Edmund Weitz

MATHEMATIK

(Skript für den Studiengang *Media Systems* an der HAW Hamburg)

5. Dezember 2025, 14:43

Dieses Skript wird ab und zu aktualisiert. Den jeweils letzten Stand (siehe Datum oben) finden Sie unter der Adresse `https://weitz.de/files/skript.pdf`.

Falls Sie Fehler entdecken (auch „kleine“ Tippfehler), freue ich mich über eine E-Mail an `edmund.weitz@haw-hamburg.de`. Für bereits entdeckte Fehler bedanke ich mich bei Adem Aksu, Lemuel Amoah, Tjark Andresen, Jörg Balzer, Célina Berbig, Tillmann Bewer, Florian Christoph, Frank Conrad, Christina Dargers, Karl Diedrichsen, Ulrich Dorobeck, Max Gansel, Pawel Gitlevich, Till Iversen, Cedric Johanson, Paul Kappmeyer, Oktay Kjasimov, Pascal Klintworth, Krischan Knauer, Dorothea Koch, Finn Lunderup, Lucy Mäge, Ronny Manjang, Fabian Matischok, Andreas Menschen, Oliver Moran, Vu Thanh Tung Paeper, Nick Petersen, Dominik Rappaport, Jan Reese, Laura Reinermann, Erik Sanjurjo-Gudehus, Thomas Schneider, Erik Schoppe, Canan Simsek, Sriraam Sinnarajah, Vanessa Staggenborg, Satyanarayan Stepponat, Simon Stroetenga, Erja Tebartz, Tres Thoenen, Jade Voß, Anna-Lena Wagner, Zanna Wahedi und Jonathan Wübbe. Für diverse Hinweise auf Pannen in den Videos zum Skript danke ich Marvin Behrmann.

Der gesamte Text ist unter der Creative-Commons-Lizenz BY-NC-ND 3.0 DE verfügbar. Eine vereinfachte Zusammenfassung dieser Lizenz findet man unter der folgenden Adresse: `https://creativecommons.org/licenses/by-nc-nd/3.0/de/`

Inhaltsverzeichnis

Gebrauchsanweisung **1**

I Grundlagen **5**

1 Logik . . . 5

2 Mengen . . . 25

II Elementare Kombinatorik **37**

3 Komplexere Mengenstrukturen . . . 37

4 Abzählende Kombinatorik . . . 46

III Relationen und Funktionen **61**

5 Relationen . . . 61

6 Funktionen . . . 71

IV Algebraische Strukturen **93**

7 Eigenschaften von inneren Verknüpfungen . . . 93

8 Gruppen . . . 97

9 Permutationsgruppen . . . 107

10 Ringe und Körper . . . 117

V Zahlentheorie **125**

11 Teilbarkeit . . . 125

12 Primzahlen . . . 133

13 Modulare Arithmetik . . . 138

14 Der chinesische Restsatz . . . 148

VI Die reellen und die komplexen Zahlen **153**

15 Ordnungsrelationen und geordnete Körper . . . 153

16 Die reellen Zahlen . . . 161

17 Die komplexen Zahlen . . . 169

18 Etwas Topologie (in metrischen Räumen) . . . 180

VII Folgen und Reihen **191**

19 Folgen . . . 191

20 Die Landau-Notation . . . 205

21 Reihen . . . 208

VIII Unendliche Mengen **233**

22 Vergleich von Mächtigkeiten . . . 233

23 Abzählbare Mengen . . . 237

24 Überabzählbare Mengen . . . 240

IX Reelle und komplexe Funktionen **245**

25 Stetige Funktionen 245
26 Differenzierbare Funktionen 251
27 Potenzreihen 258
28 Exponentialfunktionen und Logarithmen 261
29 Die trigonometrischen Funktionen 270
30 Polarkoordinaten und Arkusfunktionen 277

X Lineare Algebra 285

31 Vektorräume 285
32 Matrizen 298
33 Geometrische Interpretation linearer Abbildungen 303
34 Homogene Koordinaten 313
35 Das Skalarprodukt 315
36 Normalenvektoren 324

Lösungen zu ausgewählten Aufgaben 331

Literatur 431

Index 433

Mathematische Symbole 443

Gebrauchsanweisung

Dass Sie diesen Satz lesen, ist schon mal ein guter Anfang!

Leider lehrt die Erfahrung, dass viele Studierende nicht gerne lesen und Bücher oder Skripte meiden wie der Teufel das Weihwasser. Das ist allerdings keine gute Idee, wenn man erfolgreich studieren will. Menschen, für die Lesen eine Qual ist, rate ich dringend von einem Studium ab!

Vorlesung oder Skript? Beides!

Brauchen Sie überhaupt ein Skript, wenn Sie regelmäßig in der Vorlesung sitzen und mitschreiben? Oder umgekehrt: Müssen Sie noch (eventuell frühmorgens und im Wintersemester womöglich im Dunkeln und bei Minusgraden) in die Vorlesung kommen, wenn Sie das Skript haben? Ich behaupte, dass für fast alle Studierenden die Antwort auf diese beiden Fragen *ja* ist. Vorlesung und Skript decken zwar dieselben Themen ab und theoretisch können Sie mit einem von beiden auskommen. Aber dafür brauchen Sie entweder (nur Skript) sehr viel Selbstdisziplin oder (nur Vorlesung) eine besonders gut ausgeprägte Auffassungsgabe.

Die wöchentliche Vorlesung sorgt für Regelmäßigkeit und gibt damit gleichsam den „Takt“ für das Semester vor. Sie können dem Prof live dabei zusehen, wie man mathematisch arbeitet (und Fehler macht). Sie haben die Gelegenheit, Fragen zu stellen. Sie treffen die anderen Studierenden Ihres Semesters und können sich mit Ihnen austauschen. (Wenn Sie meinen, dass Sie auf all das verzichten können, dann hätten Sie sich vielleicht besser für ein Fernstudium entscheiden sollen, oder?)

Im Skript haben Sie alles noch einmal schwarz auf weiß. Sie können sich die Stellen heraussuchen und nacharbeiten, die Sie nicht gleich verstanden haben. (In der Mathematik versteht so gut wie niemand alles gleich beim ersten Mal!) Sie können Dinge aus den vergangenen Wochen, an die Sie sich nicht mehr so genau erinnern, nachschlagen. Sie können sich auf die kommende Vorlesung vorbereiten, indem Sie ein paar Seiten vorab lesen oder zumindest überfliegen. Und Sie finden evtl. Materialien, die über den in der Vorlesung durchgenommenen Stoff hinausgehen.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Für die Prüfungen gehen wir jedenfalls davon aus, dass Ihnen die Inhalte des Skripts bekannt sind!

Das wichtigste Werkzeug

Wie liest man so ein Skript? Das ist eigentlich schon die falsche Frage. Man *liest* es nicht wie einen Roman im Sessel, sondern man *arbeitet* es durch. Um an einer Mathevorlesung mit Gewinn teilzunehmen, braucht es zwei Zutaten: Verständnis und Routine. Sie können auf Dauer nicht folgen, wenn Sie die Inhalte der Vorwochen nicht verstanden haben, denn in der Regel baut das, was folgt, auf ihnen auf. Deshalb müssen Sie *langsam* lesen, sich dabei quasi selbst ständig über die Schulter schauen und sich immer wieder hinterfragen, ob sie „nur“ gelesen haben oder ob Sie das Gelesene auch mit Ihren eigenen Worten wiedergeben könnten.

Aber selbst dann, wenn Sie alles verstanden haben, brauchen Sie auch Routine. Sie dürfen nicht nur passiv rezipieren, sondern Sie müssen auch aktiv am Stoff arbeiten. Das ist wie mit dem Fahrradfahren oder mit dem Schwimmen: Sie beherrschen es nicht dadurch, dass Sie ein Buch darüber gelesen oder ein Video darüber gesehen haben. Oder wie es der Mathematiker Carl Runge mal formulierte: „Man lernt das Klavierspielen nicht durch den Besuch von Konzerten.“ Aus diesem Grund sollten Zettel und Bleistift Ihre wichtigsten Werkzeuge werden und beim Durcharbeiten des Skripts immer zur Hand sein. Machen Sie sich Notizen. Fertigen Sie eigenständig Zusammenfassungen der Kapitel an. Gehen Sie Beispiele aus dem Skript selbst durch und glauben Sie nicht einfach, was Sie lesen. Zeichnen Sie eigene Skizzen. Und vor allem: Bearbeiten Sie die Aufgaben! Dafür sind Sie da: die Aufgaben sind ein Service, um Sie beim Lernprozess zu unterstützen. Aber sie helfen Ihnen nur dann, wenn Sie sich mit ihnen beschäftigen.[1]

Die Aufgaben

Wenn Sie Abschnitte des Skripts zur Vorbereitung auf die Vorlesung vorab lesen, dann sollten Sie die Aufgaben zu lösen versuchen, *bevor* Sie weiterlesen. Häufig werden Sie die Lösung im folgenden Text finden oder am Ende des Skripts. Aber wenn Sie nicht selbst über die Fragen nachgedacht haben, lernen Sie nichts.

Wenn Sie hingegen das Skript *nach* dem Besuch der Vorlesung noch einmal durcharbeiten, dann kann es sicherlich nicht schaden, sich erneut mit den Aufgaben zu beschäftigen, auch wenn die vielleicht schon besprochen wurden. Versuchen Sie, die Aufgaben zu lösen, ohne Ihre Notizen aus der Vorlesung zur Hilfe zu nehmen.

Unabhängig davon, wie Sie an die Aufgaben herangehen, sollten Sie auf jeden Fall nach getaner Arbeit die Lösungen durchlesen – auch dann, wenn Sie sich sicher sind, dass Ihr Ergebnis korrekt ist. In den Lösungen finden Sie evtl. noch weitere Hinweise oder „Tricks“ bzw. Warnungen.

[1] Die Aufgaben sind aber nicht als „Probeprüfungen“ misszuverstehen. Sie werden in Testaten und Klausuren mit Sicherheit mit Aufgaben konfrontiert werden, die in diesem Skript nicht zu finden sind, denn Sie sollen ja nicht nur wiederkäuen …

Videos und Links

Die QR-Codes in der Randspalte kann man scannen oder im PDF einfach anklicken. Sie führen zu Videos von der Vorlesung zu diesem Skript, die vom Sommersemester 2023 bis zum Sommersemester 2024 aufgenommen wurden. Eine sortierte Liste aller Videos findet man unter der URL `https://weitz.de/haw-videos/`. Text in blauer Schrift ist ebenfalls anklickbar und verlinkt zu anderen Teilen des Skripts oder auf weiterführende Videos und Wikipedia-Artikel.

Beweise

Viele Aussagen in diesem Skript werden bewiesen. Da es sich um eine Vorlesung für Medieninformatiker an einer Fachhochschule handelt, geht es jedoch nicht darum, zu lernen, selbst Beweise zu führen. Die Beweise sollen vielmehr beim Verstehen des Stoffes unterstützen und eine Gelegenheit geben, sich mit der mathematischen Denkweise vertraut zu machen und die Fachsprache lesen zu lernen. Sollten Sie zu den Leserinnen und Lesern gehören, die nicht in einer meiner Vorlesung sitzen, dann weise ich vorsichtshalber darauf hin, dass das Skript nicht „beweisvollständig“ in dem Sinne ist, dass jeweils nur vorausgesetzt wird, was vorher definiert und bewiesen wurde. Wenn Sie Mathematik als Hauptfach studieren, dann eignet sich das Skript für Sie nur bedingt und Sie sollten es höchstens als ergänzende Lektüre betrachten.

Eine alternative Version des Skripts (für einen anderen Studiengang) mit anderen Schwerpunkten und teilweise anderen Inhalten findet man übrigens unter der URL `https://weitz.de/files/mi-skript.pdf`.

I

Grundlagen

Wer sich ernsthaft mit Musik beschäftigen will, wird nicht umhinkommen, die Notenschrift zu erlernen und die Bedeutung von Begriffen wie *Quinte* oder *Triole* zu verstehen. Das ist die Fachsprache, mit der Musikerinnen und Musiker miteinander kommunizieren. Auch die Mathematik hat eine Fachsprache. Dazu gehören die Objekte, die gemeinhin als *Formeln* bezeichnet werden. Darüber hinaus hat die Mathematik auch eine ihr eigene Sprech- und Denkweise. Das wird unser Thema auf den nächsten Seiten sein.

Dieses Kapitel legt das Fundament für alles, was danach folgen wird, und ist deswegen besonders wichtig. Wenn Sie die Sprache des Landes, in dem Sie Ihren Urlaub verbringen, nicht beherrschen, dann können Sie vielleicht mit Händen und Füßen einen Kaffee bestellen, Sie werden sich jedoch nicht mit den Einheimischen unterhalten können. Und wenn Sie die Sprache der Mathematik nicht verstehen, dann sind mathematische Formeln für Sie unverständliche Hieroglyphen, bei deren Anblick Sie regelmäßig verzweifeln.

Man könnte Mathematik auch ohne Formeln betreiben. In früheren Jahrhunderten hat man das gemacht. Aber die Sache wird dadurch nicht einfacher, sondern schwerer, weil natürliche Sprachen wie Deutsch oder Englisch für diesen Zweck zu umständlich sind. Mathematik ohne Formeln führt zu unhandlichen Bandwurmsätzen, die Missverständnisse geradezu herausfordern.

1. Logik

Zuerst sollten wir darüber sprechen, was Mathematikerinnen und Mathematiker eigentlich machen. Womit beschäftigt sich die Mathematik als Wissenschaft?

Es gibt keine allgemein anerkannte Definition dafür, was Wissenschaft ist. Es dürfte jedoch nicht besonders umstritten sein, wenn man sagt, dass in den *Natur*wissenschaften versucht wird, wahre und möglichst allgemeingültige Aussagen über die uns umgebende Welt zu formulieren. Das grundlegende Problem dieses Unterfangens ist, dass man sich so gut wie nie völlig sicher darüber sein kann, ob solche Theorien *wahr* sind. Man kann sie noch so oft durch Beobachtungen bestä-

tigen, sie können jederzeit durch neue Fakten widerlegt werden, die der Theorie widersprechen.

Beispielsweise ist man bis vor gut hundert Jahren davon ausgegangen, dass die Newtonsche Theorie der Gravitation das Verhalten von Himmelskörpern korrekt beschreibt. Inzwischen wurde diese jedoch durch die allgemeine Relativitätstheorie von Einstein abgelöst. Dass die „wahrer“ ist als ihr Vorgänger, lässt sich unter anderem damit begründen, dass ohne sie Satellitennavigation nicht funktionieren würde. Andererseits besteht in der Physik Einigkeit, dass auch die Relativitätstheorie noch nicht das letzte Wort ist, weil sie nicht mit der Quantentheorie vereinbar ist.[1]

Mathematik ist ganz anders. Insbesondere ist Mathematik *keine* Naturwissenschaft, obwohl sie diesen oft fälschlicherweise zugeschlagen wird. Die Mathematik untersucht nicht die reale Welt um uns herum, sondern Objekte wie Zahlen, Funktionen oder geometrische Figuren, die nur in unseren Köpfen existieren. Und im Gegensatz zu den Naturwissenschaften ist sie in der Lage, über diese Objekte allgemeingültige Aussagen zu machen, die *mit Sicherheit* wahr sind.

Vergegenwärtigen wir uns den Unterschied an einem einfachen Beispiel. Sie könnten, nachdem Sie jahrelang Vögel beobachtet haben, zu dem Schluss kommen, dass alle Raben schwarz sind. Aber können Sie sich vollkommen sicher sein, dass das stimmt? Es ist gut möglich, dass Sie in Ihrem ganzen Leben nur Raben zu Gesicht bekommen, die schwarz sind. Sie werden es jedoch niemals schaffen, alle Raben auf der Welt zu überprüfen – erst recht nicht die, die noch gar nicht geschlüpft sind.[2]

Betrachten wir nun zum Vergleich die mathematische Aussage, dass es unmöglich ist, positive ganze Zahlen a, b und c zu finden, für die $a^3 + b^3 = c^3$ gilt. Man könnte durch Herumprobieren versuchen, ein Gegenbeispiel zu finden. Da wir heutzutage Computer zur Verfügung haben, kann man in kurzer Zeit sehr viele Kombinationen von drei Zahlen durchrechnen. Finden wir nur eine einzige, die die besagte Gleichung erfüllt, dann haben wir unseren „weißen Raben“ gefunden – das „Experiment“, das die Aussage widerlegt. Finden wir jedoch nach sehr langer Suche kein Gegenbeispiel, so kann das eventuell als Indiz für die Korrektheit der Aussage interpretiert werden, aber faktisch ist die Unsicherheit noch größer als bei den Raben: unabhängig davon, wie viele Zahlen wir durchprobiert haben, es gibt immer noch unendlich viele Kombination, die auf uns warten.

Trotzdem sind sich die Mathematiker absolut sicher, dass man die Gleichung $a^3 + b^3 = c^3$ unter den gegebenen Bedingungen nicht erfüllen kann. Diese Si-

[1] Hier noch ein weiteres Beispiel: Über einen langen Zeitraum ging die Medizin davon aus, dass „Übersäuerung des Magens“ und psychische Ursachen verantwortlich für Magengeschwüre seien. Seit Ende der 1980er Jahre weiß man, dass der Hauptverursacher ein Bakterium namens *Helicobacter pylori* ist, dessen Entdecker dafür 2005 den Nobelpreis erhielten.

Auch in der Geschichte der Geologie findet man diverse Theorien, die lange aufrechterhalten wurden, inzwischen aber als widerlegt gelten.

[2] Und tatsächlich ist die Aussage falsch, da es beispielsweise in Afrika sogenannte *Schildraben* gibt, die eine weiße Brust haben.

cherheit liefern *Beweise*.[3] Beweise sind Argumentationsketten, die auf logischen Schlussfolgerungen beruhen. Sie haben große Ähnlichkeit mit den Beweisen, die in Krimis die Täter überführen. Allerdings werden an mathematische Beweise noch höhere Anforderungen gestellt, weil sie über jeglichen Zweifel erhaben sein müssen.

Beweise

Wir werden nicht lernen, selbst Beweise zu führen. Dafür muss man Mathematik als Hauptfach studieren. Aber wir werden uns mit den Basics der Logik beschäftigen und mit den damit zusammenhängenden Konventionen, weil man das für das Verständnis mathematischer Texte dringend braucht.

Aussagenlogik

Im letzten Abschnitt war die Rede von *wahr* und *falsch*. Einen Satz, der wahr oder falsch sein kann, nennt man eine *Aussage*. Überspitzt formuliert geht es in der Mathematik einzig und allein um Aussagen und um die Frage, ob diese Aussagen wahr oder falsch sind.

Hier ein paar Beispielsätze:

(i) Hamburg hat mehr als eine Million Einwohner.
(ii) Jazz ist besser als Punk.
(iii) Wie spät ist es?
(iv) Am 21.12.1940 hat es in Baltimore geregnet.
(v) Jetzt sei doch bitte mal ruhig!
(vi) Hoffentlich ist bald Herbst.
(vii) Nachts ist es kälter als draußen.

Aufgabe 1.1. Welche von diesen Sätzen würden Sie im obigen Sinne als Aussagen bezeichnen und welche nicht? Begründen Sie Ihre Entscheidungen.

Es dürfte wohl klar sein, dass (iii), (v) und (vi) keine Aussagen sind. Fragen, Aufforderungen und Wünsche können nicht wahr oder falsch sein. (vii) ist auch keine Aussage, weil der Satz zwar grammatikalisch korrekt sein mag, er aber keinen Sinn ergibt. (ii) würde man nicht als Aussage bezeichnen, weil es sich um ein subjektives Urteil handelt. Man wird keine Einigkeit darüber herstellen können, ob der Satz „wahr“ ist. (i) wirkt auf den ersten Blick so, als handele es sich um eine Aussage, aber es gibt einen Haken: Der Satz ist Anfang des 21. Jahrhunderts wahr, aber Ende des 19. Jahrhunderts war er falsch. Wir wollen nur Sätze zulassen, die entweder *immer* wahr oder *immer* falsch sind. So gesehen ist nur (iv) eine Aussage.[4] Man beachte, dass wir dafür nicht *wissen* müssen, ob es am 21. Dezember 1940 in der größten Stadt Marylands geregnet hat. Nichtsdestotrotz ist diese Aussage entweder

[3] Leider ist der Beweis für die Aussage, die hier als Beispiel fungiert, zu kompliziert für uns. Es handelt sich um einen Spezialfall eines berühmten Satzes, über den Sie z. B. in meinem Video *Der Große Satz von Fermat* mehr erfahren.

[4] Man könnte jetzt ganz kleinlich sein und beispielsweise fragen, ob der Satz besagt, dass es den ganzen Tag und in der ganzen Stadt geregnet hat. Oder darauf hinweisen, dass es mehr als einen Ort gibt, der Baltimore heißt. Aber wir wollen es nicht übertreiben.

wahr oder falsch. Und wenn wir 1940 durch 1740 ersetzen, dann gibt es höchstwahrscheinlich keine Möglichkeit, jemals zu erfahren, ob die Aussage wahr oder falsch ist. Baltimore gab es damals schon, aber es wird aus dieser Zeit wohl kaum verlässliche Wetteraufzeichnungen geben. *Trotzdem* ist die Aussage entweder wahr oder falsch.

Versuchen wir es so:

Definition

Eine **Aussage** ist ein sprachliches Gebilde, dem man einen der **Wahrheitswerte** *wahr* („trifft zu“) oder *falsch* („trifft nicht zu“) zuordnen kann. Diese Zuordnung muss objektiv und zeitlos sein. (Es ist allerdings nicht notwendig, dass der Wahrheitswert bekannt ist oder dass man ihn überhaupt ermitteln kann. Es muss lediglich sinnvoll sein, nach dem Wahrheitswert einer Aussage zu fragen.)
Die beiden Wahrheitswerte schließen sich gegenseitig aus. Eine Aussage ist also immer entweder wahr oder falsch, aber niemals beides.

Ganz schön aufwendig, oder? Wir hätten uns nicht unbedingt so viel Arbeit machen müssen, aber ich wollte gleich zu Anfang klarmachen, dass es nicht so einfach ist, sich präzise auszudrücken und Missverständnisse auszuschließen. Zum Glück werden wir uns im Wesentlichen nur mit mathematischen Aussagen befassen, wodurch sich viele der angesprochenen Probleme erledigen. Bei so etwas wie „$42 > 23$“ oder „$6 \cdot 7 = 41$“ muss man nicht darüber diskutieren, ob es sich um Aussagen handelt.[5] Ein weiteres mathematisches Beispiel, das nicht so trivial ist:

Es gibt eine ungerade vollkommene Zahl.

Das Adjektiv *vollkommen* ist ein mathematischer Fachbegriff, den Sie nicht unbedingt kennen müssen. Entscheidend sind im Moment nur zwei Dinge: Erstens handelt es sich um eine präzise formulierte Aussage im Sinne der obigen Definition. Und zweitens weiß momentan *niemand*, ob diese Aussage wahr oder falsch ist. Es handelt sich nämlich um ein ungelöstes mathematisches Problem. Als ich am Anfang des Abschnitts schrieb, dass es in der Mathematik darum geht, ob Aussagen wahr oder falsch sind, meinte ich so etwas.

Verknüpfung

Wir wollen uns aber zunächst mit viel banaleren Dingen beschäftigen. Man kann Aussagen *verknüpfen*. Dadurch entstehen *neue* Aussagen, deren Wahrheitswert nur von denen der verknüpften Aussagen abhängt.

Das klingt vielleicht komplizierter, als es gemeint ist. Also wie ist es gemeint? Nehmen wir die folgenden vier Sätze:

(i) Neil Armstrong war der erste Mensch auf dem Mond und Konrad Adenauer war der erste Kanzler der Bundesrepublik Deutschland.

(ii) Konrad Adenauer war der erste Mensch auf dem Mond und Konrad Adenauer war der erste Kanzler der Bundesrepublik Deutschland.

[5] Und es ist hoffentlich klar, dass „$6 \cdot 7$“ *keine* Aussage ist.

(iii) Neil Armstrong war der erste Mensch auf dem Mond und Neil Armstrong war der erste Kanzler der Bundesrepublik Deutschland.

(iv) Konrad Adenauer war der erste Mensch auf dem Mond und Neil Armstrong war der erste Kanzler der Bundesrepublik Deutschland.

Offensichtlich ist die erste Aussage wahr, während die anderen drei falsch sind. Das Entscheidende ist hier das Wörtchen *und*. Alle vier Beispiele bestehen aus *zwei* Aussagen, die jede für sich wahr oder falsch sind. Durch das Bindewort *und* werden sie zu einer Aussage *verknüpft* und die so entstandene verknüpfte Aussage ist nur dann wahr, wenn die beiden „Einzelteile“ wahr sind. Die zweite Aussage ist falsch, weil der erste Teilsatz falsch ist. Die dritte Aussage ist falsch, weil der zweite Teilsatz falsch ist. Die vierte Aussage ist falsch, weil beide Teilsätze falsch sind.

und

Das ist schon das Wesentliche, das man über die Bedeutung des Wortes *und* wissen muss, wenn es im mathematischen Kontext verwendet wird. Erwähnenswert ist allerdings noch, dass mathematische Texte in Lehrbüchern oder Fachartikeln in ganz normalem Deutsch oder Englisch geschrieben werden und die Ausdrucksweise dort etwas lockerer als in den obigen Beispielen ist. Einen Satz wie (ii) würde man wohl eher so formulieren: „Konrad Adenauer war der erste Mensch auf dem Mond und der erste Kanzler der Bundesrepublik Deutschland.“ Und typischerweise würde man „p und q sind Primzahlen“ schreiben und nicht etwa „p ist eine Primzahl und q ist eine Primzahl“.

Vielleicht sollte man noch ergänzen, dass im täglichen Sprachgebrauch das Wort *und* manchmal einen kausalen Zusammenhang oder eine zeitliche Abfolge andeutet. Wenn wir sagen „Sie aß Krabben *und* ihr wurde schlecht“, dann meinen wir eventuell, dass ihr schlecht wurde, *nachdem* oder gar *weil* sie Krabben gegessen hat. So wird dieses Bindewort in der mathematischen Fachsprache nicht verwendet.

Machen wir gleich weiter mit der nächsten Verknüpfung und verwenden wir als Beispiel dieselben beiden Sätze:

(i) Neil Armstrong war der erste Mensch auf dem Mond oder Konrad Adenauer war der erste Kanzler der Bundesrepublik Deutschland.

(ii) Konrad Adenauer war der erste Mensch auf dem Mond oder Konrad Adenauer war der erste Kanzler der Bundesrepublik Deutschland.

(iii) Neil Armstrong war der erste Mensch auf dem Mond oder Neil Armstrong war der erste Kanzler der Bundesrepublik Deutschland.

(iv) Konrad Adenauer war der erste Mensch auf dem Mond oder Neil Armstrong war der erste Kanzler der Bundesrepublik Deutschland.

Hier wurde lediglich *und* durch *oder* ersetzt. Die Verknüpfung *oder* hat dabei eine in der Logik klar festgeschriebene Funktion: Die verknüpfte Aussage wird dadurch wahr, dass *mindestens* eine der beiden Einzelaussagen wahr ist. In diesem Fall sind also alle Aussagen bis auf die letzte wahr. Auch hier gilt, dass man sich nicht immer so umständlich wie in dem Beispiel ausdrückt.

oder

exklusives Oder

Wie bei *und* gibt es auch noch eine kleine Tücke. Das Wort *oder* wird in der deutschen Sprache manchmal *exklusiv* verwendet, ohne dass das explizit gesagt wird. Damit ist gemeint, dass sich die beiden Alternativen gegenseitig ausschließen. Ein Beispiel wäre: „Am Eingang bekommen Sie ein rotes oder ein blaues Armband." Die meisten Menschen, die das lesen, werden wohl davon ausgehen, dass sie nur *ein* Armband bekommen.[6] Augenzwinkernd könnte man sagen, dass Mathematiker jedoch nicht überrascht wären, wenn sie *zwei* verschiedenfarbige Armbänder erhielten. Wenn man sich präzise ausdrücken will, dann sollte man für das exklusive Oder Formulierungen wie „*entweder* ein rotes oder ein blaues Armband" oder „ein rotes oder ein blaues Armband, *aber nicht beide*" verwenden. Sollten Sie in einem Lehrbuch eine Formulierung wie „p oder q sind gerade" lesen, dann müssen Sie jedenfalls davon ausgehen, dass p und q auch beide gerade sein können.

Die dritte Verknüpfung ist die Verneinung. Dabei geht es nicht wie in den anderen Fällen darum, dass zwei Aussagen zusammengesetzt werden; vielmehr wird hier einfach der Wahrheitswert *einer* Aussage umgekehrt – aus wahr wird falsch, aus falsch wahr. Banaler kann's kaum sein. Im Deutschen wird das mit den Wörtern *nicht* oder *kein* gemacht: „p ist keine Primzahl" ist die Verneinung von „p ist eine Primzahl", „Franks Auto ist nicht grün" ist die Verneinung von „Franks Auto ist grün".

Implikation

Die für mathematische Argumentationen wohl wichtigste Verknüpfung ist die sogenannte *Implikation*, die man üblicherweise in Sätzen mit *wenn* und *dann* verpackt, z. B.: „Wenn es geregnet hat, dann ist die Straße nass." Damit ist gemeint, dass aus der Wahrheit der ersten Aussage (es hat geregnet) die der zweiten (die Straße ist nass) folgt.

Eigentlich ganz einfach; Implikationen sind jedoch eine Quelle von Missverständnissen. Beispielsweise sind Nicht-Mathematiker häufig verwundert, wenn sie erfahren, dass Aussagen wie die folgenden beiden wahr sind:

(i) Wenn 6 eine Primzahl ist, dann ist die Erde eine Scheibe.

(ii) Wenn ich morgen einen Sechser im Lotto habe, dann ist 5 eine Primzahl.

Um das richtig zu verstehen, sollten Sie sich klarmachen, dass es bei der Implikation um einen rein logischen Zusammenhang geht. Anders als im täglichen Sprachgebrauch geht es *nicht* um kausale Zusammenhänge (Ursache und Wirkung) oder um zeitliche Abläufe. Eine Implikation im Sinne der Logik kann nur dann falsch sein, wenn die erste Aussage wahr und die zweite falsch ist. Beispiel (i) ist deshalb wahr, weil 6 *keine* Primzahl ist. Es ist in diesem Zusammenhang völlig irrelevant, ob die Erde eine Scheibe ist. Und Beispiel (ii) ist deshalb wahr, weil 5 eine Primzahl *ist*. Unabhängig von der morgigen Lottoziehung ist die Aussage schon heute wahr und sie wird immer wahr bleiben. Anders ausgedrückt: Das Lottospiel, die Form der Erde und Primzahlen haben miteinander nichts zu tun, auf die Korrektheit der Implikation hat das jedoch keinen Einfluss.

Noch ein Beispiel. Ich verspreche meiner Tochter:

[6] Würde man die Beispiele so interpretieren, dann wäre Aussage (i) falsch!

Wenn Du eine Eins in Erdkunde schreibst, *dann* bekommst Du ein Eis.

Natürlich muss sie ein Eis bekommen, wenn sie eine Eins schreibt. Und wenn sie keine Eins schreibt, wird sie sich nicht beschweren können, wenn sie kein Eis bekommt. Sie wird aber sicher auch nicht meckern, wenn Sie ein Eis erhält, obwohl sie keine Eins geschrieben hat. Lediglich dann, wenn Sie eine Eins schreibt und ich ihr daraufhin *kein* Eis spendiere, wird sie zu Recht sagen, dass ich mein Versprechen nicht eingehalten habe. Nur dann war die Aussage *nicht wahr*.

hinreichend
notwendig

Man spricht in diesem Zusammenhang auch von *hinreichenden* und *notwendigen* Bedingungen. Der erste Teil einer Wenn-Dann-Aussage ist eine hinreichende Bedingung für den zweiten, der zweite eine notwendige Bedingung für den ersten. Um beim Beispiel zu bleiben: Eine Eins in der Erdkundeklausur ist eine *hinreichende* Bedingung dafür, ein Eis zu bekommen. Die Eins ist jedoch nicht zwingend *notwendig*, weil der Vater ja vielleicht auch ohne Eins ein Eis ausgibt. Andererseits gibt es – wenn die Aussage wahr ist – auf jeden Fall ein Eis, wenn eine Eins geschrieben wurde. In diesem Sinne ist das Eis eine notwendige Bedingung für die Eins. Damit ist gemeint: Wenn es kein Eis gab, kann die Tochter keine Eins geschrieben haben.

Kommen wir zum zweiten Missverständnis im Zusammenhang mit Implikationen: Die Reihenfolge wird umgedreht, d. h., hinreichende und notwendige Bedingung werden in der Erwartung vertauscht, dass sich dadurch am Wahrheitsgehalt der Aussage nichts ändert. Beim ersten Beispiel mit der nassen Straße wäre das der folgende Satz: „Wenn die Straße nass ist, hat es geregnet.“ Diese Aussage ist aber *nicht* wahr, denn es kann andere Gründe dafür geben, dass die Straße nass ist. Beispielsweise könnte ein LKW mit Milch umgekippt sein. Oder um ein Beispiel für so einen Fehlschluss aus der Mathematik zu liefern: Wenn x eine positive natürliche Zahl ist, dann ist x^2 positiv. Das stimmt. Die umgedrehte Aussage ist: Wenn x^2 positiv ist, dann ist x eine positive natürliche Zahl. Das ist jedoch falsch, denn unter anderem ist das Quadrat von -3 positiv, obwohl -3 keine positive natürliche Zahl ist.

Will man korrekt vorgehen, dann muss man nicht nur die Reihenfolge ändern, sondern dabei auch beide Teilaussagen verneinen:

(i) Wenn die Straße *nicht* nass ist, hat es *nicht* geregnet.
(ii) Wenn die Tochter *kein* Eis bekommt, hat sie *keine* Eins geschrieben.
(iii) Wenn x^2 *nicht* positiv ist, dann ist x *keine* positive natürliche Zahl.

Aber wieso ist das korrekt? Wie genau ist das gemeint und wie kann man das begründen? Bisher habe ich absichtlich mit Beispielen aus dem täglichen Leben gearbeitet, aber nun werden wir den in der Logik üblichen Formalismus verwenden. Ich behaupte, dass die Dinge dadurch übersichtlicher und besser nachvollziehbar werden. Hoffentlich sehen Sie das auch so.

Wir werden für Aussagen wie „Konrad Adenauer war der erste Mensch auf dem Mond“ als Platzhalter Buchstaben wie A, B, C und so weiter verwenden. (Man

Aussagenvariable

nennt das *Aussagenvariablen*.) Für die Verknüpfungen, die wir bisher kennengelernt haben, benutzen wir die in der mathematischen Logik üblichen Symbole:[7]

Konjunktion $\wedge$
Disjunktion $\vee$
Negation $\neg$
Implikation $\Rightarrow$

Verknüpfung	Fachbegriff	Symbol	Programmieren
und	Konjunktion	$\wedge$	&&
oder	Disjunktion	$\vee$	||
nicht	Negation	$\neg$	!
wenn, dann	Implikation	$\Rightarrow$	

Außerdem schreiben wir 1 für *wahr* und 0 für *falsch*. (Wie in der Informatik, in der solche Verknüpfungen unter anderem als Logikgatter eine Rolle spielen.) Damit können wir das, was wir bisher besprochen haben, ganz knapp tabellarisch zusammenfassen:

A	$\neg A$
0	1
1	0

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

Dadurch werden zwei Sachen sofort klar. Erstens ist es für den Wahrheitswert von zusammengesetzten Aussagen wie $A \wedge B$ oder $A \Rightarrow B$ völlig egal, ob wir über die Mondlandung, über Speiseeis oder über Primzahlen sprechen. Es geht einzig und allein darum, ob A bzw. B wahr oder falsch sind. Und zweitens gibt es immer nur eine kleine Anzahl von Fällen, die wir betrachten müssen. Die rechte Tabelle hat beispielsweise nur vier Zeilen, da es lediglich vier mögliche Kombinationen von wahr und falsch für A und B gibt. Links brauchen wir sogar nur zwei Zeilen, weil A nur wahr oder falsch sein kann.

Aufgabe 1.2. Wie viele Zeilen würde eine Tabelle mit drei bzw. vier Aussagen haben?

Junktor

Die obigen Tabellen sind die mathematisch exakte *Definition* für unsere logischen Verknüpfungen – die man übrigens *Junktoren* nennt. Wenn wir in Zukunft wissen wollen, ob eine Aussage wie die mit der Fünf und dem Lotto wahr ist, dann müssen wir nur in der entsprechenden Tabelle nachschauen. Genauer: Wir nennen die Aussagen „Morgen habe ich einen Sechser im Lotto“ und „5 ist eine Primzahl“ A und B, überlegen, welchen Wahrheitswert A und B haben, und suchen anschließend den zugehörigen Wahrheitswert von $A \Rightarrow B$ in der passenden Zeile der Tabelle heraus. In diesem konkreten Fall stellen wir fest, dass wir den Wahrheitswert von A

[7] Es gibt noch diverse Alternativen, z. B. $\overline{A}$ statt $\neg A$ oder $A \cdot B$ statt $A \wedge B$, aber es würde wohl nur Verwirrung stiften, die hier alle aufzuführen. Die vierte Spalte zeigt informationshalber den Operator, der in vielen weitverbreiteten Programmiersprachen wie C und Java verwendet wird.

Bitte beachten Sie, dass diese Symbole zwar in solchen *Formeln* der Logik Sinn ergeben, dass sie jedoch *nicht* als Abkürzungen für die Wörter in der ersten Spalte gedacht sind. Es wäre furchtbar schlechter Stil, so etwas wie „$p \wedge q$ sind positiv“ oder „x ist $\neg$ rational“ zu schreiben; jede Fachzeitschrift würde das ablehnen.

gar nicht wissen müssen, weil B wahr ist und in beiden Zeilen, in denen B wahr ist, auch $A \Rightarrow B$ wahr ist.

Die obige Frage nach dem „korrekten“ Umgang mit der Implikation lässt sich nun auch leicht beantworten:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$B \Rightarrow A$	$\neg B \Rightarrow \neg A$
0	0	1	1	1	1	1
0	1	1	0	1	0	1
1	0	0	1	0	1	0
1	1	0	0	1	1	1

Wir sehen, dass in der fünften und siebten Spalte immer dieselben Wahrheitswerte stehen. $A \Rightarrow B$ ist also genau dann wahr, wenn $\neg B \Rightarrow \neg A$ wahr ist. Die sechste Spalte sieht jedoch anders aus. (Solche Tabellen nennt man *Wahrheitstafeln*. Und eine Zuordnung wie $A = 0$ und $B = 1$ nennt man eine *Belegung* der Aussagenvariablen.)

Wahrheitstafel

Belegung

Aufgabe 1.3. In welcher Zeile findet man den Fall mit dem Milchlaster?

Wenn wie eben zwei Aussagen immer dieselben Wahrheitswerte haben, dann kann man das auch durch eine logische Verknüpfung ausdrücken. Der Fachbegriff dafür ist *Äquivalenz* und das zugehörige Zeichen $\Leftrightarrow$.

Äquivalenz $\Leftrightarrow$

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Entsprechende Formulierungen für $A \Leftrightarrow B$ im Deutschen sind „genau dann, wenn“ oder „dann und nur dann, wenn“.[8] Manchmal sagt man auch einfach dass die Aussagen A und B äquivalent sind. Gemeint ist damit jedenfalls immer: Ist A wahr, dann muss zwangsläufig auch B wahr sein; und ist A falsch, dann muss zwangsläufig auch B falsch sein. Ein Beispiel: n ist genau dann gerade, wenn $n+1$ ungerade ist. Noch ein Beispiel: Wir haben gerade gesehen, dass die Aussagen $A \Rightarrow B$ und $\neg B \Rightarrow \neg A$ äquivalent sind.

Aufgabe 1.4. Wir wissen inzwischen, dass $A \Rightarrow B$ und $B \Rightarrow A$ nicht dasselbe aussagen. Der mathematische Fachbegriff dafür ist, dass die Verknüpfung $\Rightarrow$ nicht *kommutativ* ist, d. h., man darf nicht einfach links und rechts vertauschen. Machen Sie sich anhand der Tabellen klar, dass die Junktoren $\wedge$, $\vee$ und $\Leftrightarrow$ kommutativ sind.

Kommutativität

Junktoren machen mit den Wahrheitswerten von Aussagen das, was Operationen wie Addition und Multiplikation mit Zahlen machen. Wir können damit auch

[8] Im Englischen *if and only if*, was gerne mit *iff* abgekürzt wird. Wenn Sie das in einem Mathebuch lesen, dann ist das also höchstwahrscheinlich kein Druckfehler.

komplexere Ausdrücke bilden und werden das gleich tun. Wie beim Rechnen mit Zahlen sind allerdings ein paar Konventionen hilfreich. $(3\cdot 4)+2$ ist nicht dasselbe wie $3\cdot(4+2)$. Es kommt darauf an, in welcher Reihenfolge man die Operationen durchführt, und die Klammern geben vor, was zuerst berechnet werden muss. Außerdem haben wir Regeln wie "Punkt- vor Strichrechnung", mit denen wir Klammern sparen. Multiplikation (Punktrechnung) hat eine höhere Priorität als Addition (Strichrechnung) und daher ist $3\cdot 4+2$ eine Abkürzung für $(3\cdot 4)+2$.

Für die Priorität der Junktoren nehmen wir die Reihenfolge von links nach rechts in der Tabelle auf Seite 12, gefolgt von $\Leftrightarrow$. $\wedge$ hat also z. B. höhere Priorität als $\vee$ und $\vee$ hat höhere Priorität als $\Leftrightarrow$. Damit ist $A\wedge B\vee C$ eine Abkürzung für $(A\wedge B)\vee C$.

Assoziativität

Aufgabe 1.5. Erstellen Sie eine Tabelle, mit der Sie sich überzeugen, dass die Konjunktion *assoziativ* ist, dass also $(A\wedge B)\wedge C$ immer denselben Wahrheitswert wie $A\wedge(B\wedge C)$ hat. Es ist in so einem Fall also unproblematisch, die Klammern wegzulassen. Sind die Verknüpfungen Disjunktion, Implikation und Äquivalenz auch assoziativ? (Hinweis: Die Tabelle fängt mit drei Spalten für A, B und C an und besteht aus acht Zeilen. Siehe Aufgabe 1.2.)

Aufgabe 1.6. Ein altes Sprichwort lautet: „Wenn der Hahn kräht auf dem Mist, dann ändert sich das Wetter oder es bleibt, wie es ist.“ Wie sieht das als Formel der Aussagenlogik aus?

Angesichts der oben angesprochenen Missverständnisse bezüglich der Implikation ist es ganz instruktiv, sich die folgende Tabelle anzuschauen.

A	B	$\neg A$	$\neg B$	$A\Rightarrow B$	$\neg A\vee B$	$\neg(A\wedge\neg B)$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	0
1	1	0	0	1	1	1

Die drei letzten Spalten sind identisch. Man erkennt, dass man $A\Rightarrow B$ auch schlicht und einfach als Abkürzung für $\neg A\vee B$ oder $\neg(A\wedge\neg B)$ lesen kann. Diese Sichtweise hilft hoffentlich gegen die durch die Formulierung „wenn-dann“ hervorgerufene falsche Assoziation mit Kausalität oder zeitlichem Ablauf.

Aufgabe 1.7. Machen Sie sich mit einer Tabelle klar, dass $A\Leftrightarrow B$ dieselben Wahrheitswerte wie $(A\Rightarrow B)\wedge(B\Rightarrow A)$ hat.

Aufgabe 1.8. Geben Sie eine Formel an, die dieselben Wahrheitswerte wie $\neg(A\wedge B)$ hat, in der aber nur die Junktoren $\neg$ und $\vee$ verwendet werden. Überprüfen Sie Ihr Ergebnis mit einer Wahrheitstafel. Stellen Sie dann $\neg(A\vee B)$ ohne $\vee$ dar.

de-morgansche Regeln

Die Zusammenhänge aus Aufgabe 1.8 nennt man übrigens auch *de-morgansche Regeln* nach dem englischen Mathematiker Augustus De Morgan aus dem 19. Jahrhundert.

Aufgabe 1.9. In der Schule lernt man, dass für reelle Zahlen x und y immer genau eine der drei Aussagen $x < y$, $x = y$ oder $x > y$ wahr ist. Begründen Sie, warum deshalb $x \geq y$ äquivalent zur Negation von $x < y$ ist.

Zum Üben der gerade vorgestellten Begriffe und Techniken können Logikrätsel ganz hilfreich sein.[9] Wir gehen eines exemplarisch durch: Vor Ihnen stehen zwei verschlossene Kisten. Sie wissen, dass sich in jeder der Kisten genau ein Stück Obst befindet, und zwar jeweils ein Apfel oder eine Orange. Sie wissen aber natürlich nicht, welche Sorte Obst sich in welcher Kiste befindet, und es kann auch sein, dass in beiden Kisten ein Apfel oder in beiden eine Orange ist. Ferner klebt auf jeder Kiste ein Schild. Auf dem Schild auf der ersten Kiste steht: „In dieser Kiste ist eine Orange und in der anderen ist ein Apfel." Auf dem Schild auf der zweiten Kiste steht: „Es befindet sich nicht in beiden Kisten dieselbe Sorte Obst." Schließlich wird Ihnen noch mitgeteilt, dass eine der beiden Aussagen wahr und die andere falsch ist, aber Ihnen wird natürlich nicht gesagt, welche der beiden Aussagen die wahre ist. Sie lieben Orangen. Welche Kiste sollten Sie öffnen, wenn Sie nur eine öffnen dürfen? (Oder können Sie vielleicht schließen, dass in beiden Kisten Äpfel sind?)

Aufgabe 1.10. Versuchen Sie es erst einmal selbst und arbeiten Sie möglichst mit Aussagenlogik, Junktoren und Wahrheitstafeln.

Man könnte das Rätsel folgendermaßen lösen: A sei die Aussage, dass sich in der ersten Kiste eine Orange befindet, und B die entsprechende Aussage für die zweite Kiste. Das Schild auf der ersten Kiste besagt somit $A \wedge \neg B$ und das auf der zweiten $(A \wedge \neg B) \vee (\neg A \wedge B)$. Das liefert die folgende Tabelle:

A	B	$\neg A$	$\neg B$	$A \wedge \neg B$	$(A \wedge \neg B) \vee (\neg A \wedge B)$
0	0	1	1	0	0
0	1	1	0	0	1
1	0	0	1	1	1
1	1	0	0	0	0

Nur in der zweiten Zeile sind die Wahrheitswerte für die beiden Schilder unterschiedlich. Die muss es sein und deshalb ist B wahr: Sie finden in der zweiten Kiste eine Orange.

Aufgabe 1.11. Haben Sie das Schild auf der zweiten Kiste anders übersetzt? Wie könnte man es noch machen?

Aufgabe 1.12. Zwei der folgenden vier Sätze machen (abgesehen von grammatikalischen Feinheiten) rein logisch exakt dieselbe Aussage . Welche beiden sind es?

(i) Wenn der HSV die Champions League gewinnt, dann springe ich in die Alster.

[9] Die sind in manchen Kreisen offenbar so beliebt, dass es regelmäßig erscheinende Zeitschriften mit solchen Aufgaben gibt.

(ii) Wenn der HSV nicht die Champions League gewinnt, dann springe ich nicht in die Alster.

(iii) Wenn ich nicht in die Alster springe, dann hat der HSV die Champions League nicht gewonnen.

(iv) Wenn der HSV die Champions League gewinnt, dann springe ich nicht in die Alster.

Aufgabe 1.13. Sie haben eine Druckerei beauftragt, Spielkarten nach den folgenden Regeln zu bedrucken:

(i) Auf einer Seite steht ein Buchstabe, auf der anderen eine natürliche Zahl.

(ii) Wenn auf der Buchstabenseite ein Vokal steht, dann muss auf der Zahlenseite eine gerade Zahl stehen.

Vor Ihnen liegen vier Probedrucke, auf denen Sie die Zeichen `U`, `4`, `P` und `7` sehen. Sie sind sich sicher, dass die Druckerei die erste Regel bei allen vier Karten befolgt hat, aber Sie wollen überprüfen, ob auch die zweite Regel immer eingehalten wurde. Wie viele und welche der vier Karten müssen Sie dafür umdrehen? (Sie sind faul und wollen möglichst wenige Karten umdrehen!)

Aufgabe 1.14. Kommissar Gödel muss einen Mordfall lösen und hat drei Tatverdächtige: Gauß, Euler und Hilbert. Aufgrund der bisherigen Ermittlungen weiß er die folgende Dinge mit Sicherheit:

(i) Es kann einen, aber auch mehrere Täter gegeben haben.

(ii) Ist Hilbert schuldig, so war auch Euler einer der Täter.

(iii) Stellen sich Gauß oder Hilbert als Täter heraus, dann ist Euler unschuldig.

(iv) Sind aber Euler oder Hilbert unschuldig, dann muss Gauß an der Tat beteiligt gewesen sein.

Helfen Sie dem Kommissar mit Methoden der Aussagenlogik.

erfüllbar

Tautologie

Aufgabe 1.15. Eine Formel der Aussagenlogik wird *erfüllbar* genannt, wenn es (mindestens) eine Belegung der in ihr vorkommenden Variablen gibt, die die Formel wahr macht. Eine Formel, die für *alle* möglichen Belegungen wahr ist, wird *Tautologie* genannt. Begründen Sie, dass $(A \Rightarrow B) \Leftrightarrow (B \Rightarrow A)$ erfüllbar, aber keine Tautologie ist.

Aufgabe 1.16. Überprüfen Sie mit einer Wahrheitstafel, ob

$$(A \vee B \Rightarrow C) \Leftrightarrow (A \Rightarrow C) \wedge (B \Rightarrow C)$$

erfüllbar oder sogar eine Tautologie ist.

Aufgabe 1.17. Wir betrachten die Formel $(\neg A \vee B) \wedge P \Rightarrow (A \Leftrightarrow B)$. Wie kann man aus dieser eine Tautologie machen?

(i) Indem man P durch $(B \Rightarrow A)$ ersetzt.

(ii) Indem man P durch $(\neg A \wedge B)$ ersetzt.

(iii) Indem man P durch $\neg(B \wedge \neg A)$ ersetzt.

Aufgabe 1.18. Wenn Sie noch Übung im Umgang mit Wahrheitstafeln brauchen, dann überzeugen Sie sich, dass $F \wedge (F \vee G) \Leftrightarrow F$ und $F \vee (G \wedge H) \Leftrightarrow (F \vee G) \wedge (F \vee H)$ Tautologien sind und dass das auch dann noch gilt, wenn man in den beiden Formeln die Rollen von $\wedge$ und $\vee$ vertauscht.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Aufgabe 1.19. Eine Astronautin besucht einen Planeten, dessen Bewohner – die sich *Froods* nennen – entweder blau oder grün sind. Die blauen Froods sagen immer die Wahrheit, die grünen Froods lügen immer. Die Astronautin trifft die beiden Froods Andrew und Bert, aber es ist zu dunkel, um ihre Farben zu erkennen. Sie fragt Andrew, ob er und Bert beide blau seien. Andrew antwortet, aber die Astronautin weiß danach noch nicht, welche Farbe die beiden haben. Darauf fragt sie Andrew, ob er und Bert dieselbe Farbe haben. Nachdem Andrew auch diese Frage beantwortet hat, kennt sie die Farben der beiden. Sie auch?

Prädikatenlogik

Die Sprache der Aussagenlogik ist für manche Zwecke hilfreich, aber sie ist für die Mathematik nicht reichhaltig genug. Das liegt daran, dass die meisten mathematischen Aussagen Behauptungen über bestimmte *Objekte* (Zahlen, Vektoren, Funktionen, Mengen und so weiter) sind und dass so etwas in der Aussagenlogik gar keine Rolle spielt. Nehmen wir ein Beispiel aus dem letzten Abschnitt:

Wenn x eine positive natürliche Zahl ist, dann ist x^2 positiv.

Aus Sicht der Aussagenlogik hat dieser Satz die Struktur $A \Rightarrow B$. An der ist aber nicht mehr zu erkennen, dass es in A und B um dasselbe Objekt x geht und dass die Wahrheitswerte von A und B davon abhängen, wofür genau dieses x steht.[10] Deshalb erweitert man die Sprache:

Definition

Eine **Aussageform** ist ein sprachliches Gebilde, in dem **Individuenvariablen** vorkommen können und das dadurch, dass man für diese Variablen konkrete Werte einsetzt, zu einer Aussage wird.

Dazu ein Beispiel: „x ist negativ“ ist eine Aussageform mit der Individuenvariable x. In dieser Form handelt es sich nicht um eine Aussage, denn es ergibt keinen Sinn, über die Wahrheit von „x ist negativ“ zu sprechen. Setzt man für x jedoch die Zahlen -3 oder 42 ein, so ergibt sich in beiden Fällen eine Aussage; im ersten Fall eine wahre, im zweiten eine falsche. Man würde für so eine Aussageform eine Abkürzung wie $A(x)$ verwenden, an der man die Individuenvariable erkennt.[11]

Das kann man nun mit der Aussagenlogik verbinden, indem man Aussageformen wie Aussagen verknüpft. Das Beispiel vor der Definition hat in diesem Sinne die Struktur $B(x) \Rightarrow C(x)$.

Ein paar Anmerkungen dazu:

- Auch so etwas wie $m > n$ ist eine Aussageform, nämlich eine mit *zwei* Individuenvariablen, für die man dann z. B. $A(m, n)$ schreiben würde. Eine Aussage wird daraus erst, indem man für *beide* Variablen Werte einsetzt.

[10] Oder: Alle Menschen sind sterblich. Sokrates ist ein Mensch. Mit den Mitteln der Aussagenlogik kann man daraus nicht schließen, dass Sokrates sterblich ist.

[11] Wir werden in diesem Abschnitt für Individuenvariablen kleine Buchstaben wie x und y verwenden und für Aussagen und Aussageformen große wie A und B. Das ist aber nur eine Konvention und keine feste Regel, die in der gesamten Mathematik eingehalten wird.

- Aussagen sind auch Aussageformen, und zwar solche mit null Individuenvariablen.
- In einer Aussageform können Variablen auch mehrfach auftreten, beispielsweise in $x \cdot x = x$. Setzt man für so eine Variable einen Wert ein, dann ist das natürlich so gemeint, dass man überall *dasselbe* einsetzt.
- Umgekehrt ist es jedoch nicht verboten, für *verschiedene* Variablen denselben Wert einzusetzen.[12] Zum Beispiel kann man aus $m > n$ durch Einsetzen die wahre Aussage $7 > 3$ machen, aber auch die falsche $4 > 4$.
- In der Regel kann man für die Individuenvariablen nur bestimmte Objekte einsetzen, etwa nur Zahlen oder nur Matrizen. Es wäre z. B. sinnlos, in „x ist negativ“ für x das Wort *Apfel* einzusetzen. In der Prädikatenlogik gibt es dafür klare Regeln. So tief wollen wir aber nicht in die Materie einsteigen. Wir werden uns darauf verlassen, dass üblicherweise aus dem Kontext hervorgeht, was sinnvoll ist.

Aufgabe 1.20. Drücken Sie die Aussageform $x \leq y$ mithilfe der beiden Aussageformen $x < y$ und $x = y$ aus, indem Sie sie durch einen Junktor verbinden.

Aufgabe 1.21. Im 1582 eingeführten *gregorianischen Kalender* ist ein Jahr dann ein Schaltjahr, wenn die Jahreszahl durch 4, aber *nicht* durch 100 teilbar ist. Eine Ausnahme von dieser Regel bilden die durch 400 teilbaren Jahreszahlen: die gehören zu Schaltjahren. (Beispiele: 1940, 1984 und 2000 sind Schaltjahre; 1900 und 1993 sind keine Schaltjahre.) Wir führen die folgenden Aussageformen ein, wobei die Individuenvariable n jeweils für eine Jahreszahl ab 1582 stehen kann.

$$A_4(n) : n \text{ ist durch 4 teilbar.}$$
$$A_{100}(n) : n \text{ ist durch 100 teilbar.}$$
$$A_{400}(n) : n \text{ ist durch 400 teilbar.}$$

Basteln Sie daraus mithilfe von Junktoren eine Aussageform mit der Individuenvariable n, die genau dann wahr ist, wenn n ein Schaltjahr ist.

Quantor

Aussageformen erhalten ihre expressive Kraft durch sogenannte *Quantoren*. Um deren Gebrauch zu verstehen, schauen wir uns vier Aussageformen an, bei denen die Individuenvariable x jeweils für eine ganze Zahl steht.

$A(x)$	$B(x)$	$C(x)$	$D(x)$
$x - x = 0$	$x + x > 0$	$x \cdot x = 0$	$x + 1 = x$

Allquantor $\forall$

Beim ersten Beispiel ist $A(x)$ immer wahr – unabhängig davon, welche Zahl Sie für x einsetzen. Man sagt dann, dass $A(x)$ *für alle* x wahr ist, und schreibt das mit dem umgedrehten Anfangsbuchstaben des Wortes *alle*: $\forall x\, A(x)$. Wenn man – wie in diesem Beispiel – deutlich machen will, dass es um ganzen Zahlen geht, dann schreibt man[13] $\forall x \in \mathbb{Z}\, A(x)$ und liest das als: „Für alle ganzen Zahlen x gilt $A(x)$.“

[12] Wenn man dieses Verbot aus dem letzten Punkt folgern würde, dann hätte man $\neg A \Rightarrow \neg B$ aus $A \Rightarrow B$ geschlossen.

[13] Das Zeichen $\in$ ist ein Vorgriff auf den folgenden Abschnitt über Mengenlehre. Das Symbol $\mathbb{Z}$ für die Menge der ganzen Zahlen sollten Sie aus der Schule kennen. Siehe auch Seite 27.

(Dass eine Aussage *gilt*, ist also lediglich eine andere Formulierung dafür, dass sie wahr ist.) gelten

$B(x)$ ist hingegen nicht immer wahr, z. B. ist $B(0)$ falsch und $B(-3)$ ist auch falsch. Allerdings wird die Aussageform für manche x wahr, etwa $B(1)$ oder $B(42)$. In der Mathematik sagt man in so einem Fall: „Es gibt ein x, für das $B(x)$ wahr ist." Die Abkürzung dafür ist $\exists x\, B(x)$ bzw. $\exists x \in \mathbb{Z}\, B(x)$.[14] Diese Sprechweise ist typisch, aber gewöhnungsbedürftig. Man meint damit eigentlich, dass es *mindestens* ein x gibt, das $B(x)$ wahr macht, aber das Wort *mindestens* wird so gut wie immer weggelassen. Wenn man so etwas liest oder hört, muss man also aufpassen, dass man das Wörtchen *ein* nicht überbewertet. Existenzquantor $\exists$

Was beide Quantoren gemeinsam haben: Sie machen aus Aussageformen Aussagen. $x + x > 0$ ist eine Aussageform, die weder wahr noch falsch sein kann. $\forall x\,(x + x > 0)$ und $\exists x\,(x + x > 0)$ sind jedoch beides Aussagen; die erste ist falsch, die zweite ist wahr.

Ich habe im letzten Absatz Klammern gesetzt, obwohl sie rein technisch nicht nötig wären. Üblicherweise vereinbart man, dass Quantoren eine höhere Priorität als Junktoren haben, so dass beispielsweise $\forall x\, A_1(x) \wedge A_2(x)$ eine Abkürzung für $(\forall x\, A_1(x)) \wedge A_2(x)$ ist. Beachten Sie aber, dass diese Formel zwar formal korrekt ist, jedoch zu Missverständnissen führen kann. $(\forall x\, A_1(x)) \wedge A_2(x)$ ist eine Aussage*form* und keine Aussage, weil das x in $A_2(x)$ nicht im „Einflussbereich" des Quantors steht (der bei der Klammer endet). Das x in $A_1(x)$ und das x in $A_2(x)$ spielen also ganz unterschiedliche Rollen[15] und man könnte auch andere Variablennamen nehmen: $\forall x\, A_1(x) \wedge A_2(y)$.

Die Aussage $\exists x\, C(x)$ ist ebenfalls wahr. Der Unterschied zum Beispiel davor ist allerdings, dass es in diesem Fall wirklich nur eine einzige Möglichkeit für x gibt, um $C(x)$ wahr werden zu lassen – nämlich die Zahl null. Wenn man das zum Ausdruck bringen will, dann sagt man, dass es „*genau* ein x" gibt. Dafür werden manchmal auch Schreibweisen wie $\exists_1 x$ oder $\exists! x$ verwendet. $\exists_1$ $\exists!$

In die letzte Aussageform kann man schließlich einsetzen, was man will, sie wird *nie* wahr werden; es gibt keine Zahl x, für die $x + 1 = x$ gilt. Um das auszudrücken, braucht man jedoch kein neues Symbol. Man kann es mit den vorhandenen Zeichen sogar auf zwei Arten hinschreiben: $\forall x \neg D(x)$ oder $\neg \exists x\, D(x)$. Die erste Formel

[14] Hier wird der Anfangsbuchstabe von *Existenz* umgedreht. An den Zeichen für die Quantoren kann man übrigens gut erkennen, dass der Fortschritt in der Mathematik nicht so geradlinig verläuft, wie man sich das vielleicht vorstellt. Die beiden Quantoren werden heute wohl in jedem Lehrbuch gleichzeitig eingeführt und man könnte denken, sie wären schon immer ein unzertrennliches Paar gewesen. Tatsächlich wurde das Symbol $\exists$ jedoch Ende des 19. Jahrhunderts von dem Italiener Giuseppe Peano „erfunden", während das Zeichen $\forall$ erst fast 40 Jahre später von dem Deutschen Gerhard Gentzen eingeführt wurde.

[15] Man sagt in der Logik, dass die Variable x in $A_2(x)$ *frei* auftritt, während sie in $\forall x\, A_1(x)$ durch den Quantor *gebunden* ist. Wir werden diese Begriffe jedoch nicht präzise definieren. Die Bedeutung ist jedenfalls, dass $A_2(x)$ etwas *über* x aussagt, während der Übergang von $\forall x\, A_1(x)$ zu $\forall y\, A_1(y)$ die Bedeutung nicht ändert – der Name x ist hier bedeutungslos. (Für die, die ganz genau aufpassen: Der letzte Satz setzt voraus, dass y in $A_2(x)$ nicht vorkommt.) frei gebunden

besagt, dass $D(x)$ für *jedes x falsch* ist, die zweite sagt aus, dass es *kein x* gibt, für das $D(x)$ *wahr* ist.

Aufgabe 1.22. Es ist ganz wesentlich, dass Ihnen klar ist, dass $\forall x\, \neg D(x)$ und $\neg \exists x\, D(x)$ wirklich dasselbe aussagen. Erfahrungsgemäß lauert an diesem Punkt oft ein Verständnisproblem. Deshalb sollten Sie darüber nicht einfach hinweglesen, sondern sich das noch einmal in Ruhe durch den Kopf gehen lassen.

Aufgabe 1.23. Jemand behauptet, alle Bremer könnten Fußball spielen. Sie wollen das Gegenteil dieser Aussage formulieren. Welchen der folgenden Sätze dürfen Sie dann *nicht* verwenden?

(i) Einige Bremer können nicht Fußball spielen.
(ii) Es gibt mindestens einen Bremer, der nicht Fußball spielen kann.
(iii) Kein Bremer kann Fußball spielen.
(iv) Nicht alle Bremer können Fußball spielen.

Formalisieren Sie die Sätze mit Quantoren!

Zum Verständnis der Quantoren $\forall$ und $\exists$ kann vielleicht noch die folgende Sichtweise beitragen. Dass $A(x)$ für jedes x wahr ist, könnte man theoretisch auch so aufschreiben:

$$A(0) \wedge A(1) \wedge A(-1) \wedge A(2) \wedge A(-2) \wedge A(3) \wedge \dots$$

Aber eben nur theoretisch, denn man müsste unendlich viele Aussagen durch die Konjunktion verbinden. In diesem Sinne kann man sich den Allquantor $\forall$ jedoch als ein „großes $\wedge$“ vorstellen.[16]

Aufgabe 1.24. Kann man analog den Existenzquantor $\exists$ auch durch (unendlich) viele aussagenlogische Junktoren ersetzen?

Aufgabe 1.25. Schreiben Sie die Aussagen $\forall x\, W(x)$ und $\exists x\, W(x)$ aus der Lösung von Aufgabe 1.22 ohne Quantoren auf.

Mit dieser Analogie zwischen $\forall$ und $\exists$ einerseits sowie $\wedge$ und $\vee$ andererseits wird klar, dass es in den Aufgaben 1.22 und 1.23 wieder um die de-morganschen Regeln ging. Weil die so wichtig sind, führe ich sie noch einmal explizit auf:

(i) $\neg \forall x\, A(x)$ und $\exists x\, \neg A(x)$ sind äquivalent.
(ii) $\neg \exists x\, A(x)$ und $\forall x\, \neg A(x)$ sind äquivalent.

Als Eselsbrücke kann man sich vielleicht merken, dass die Negation einen Quantor in einen anderen „verwandelt“, wenn sie sich auf dessen andere Seite bewegt. Außerdem sollte man im Kopf behalten, dass man eine Aussage der Form $\forall x\, A(x)$ über „viele“ Objekte bereits dadurch widerlegen kann, dass man *ein* Gegenbeispiel findet: $\exists x\, \neg A(x)$.

[16] Und in manchen Mathebüchern verwenden die Autoren statt $\forall$ auch ein Zeichen wie $\bigwedge$.

Aufgabe 1.26. Sei $p(n)$ die Aussageform „n ist gerade“ und $q(n)$ die Aussageform „n ist durch 4 teilbar“. Welche der folgenden Aussagen ist wahr? Geben Sie bei den falschen Aussagen jeweils ein Gegenbeispiel an, das begründet, warum die Aussage nicht wahr ist. (Mit $\mathbb{N}$ sind die natürlichen Zahlen gemeint. Siehe Seite 27.)

(i) $\exists n \in \mathbb{N}(\neg p(n) \wedge q(n))$
(ii) $\exists n \in \mathbb{N}(p(n) \wedge \neg q(n))$
(iii) $\forall n \in \mathbb{N}\, p(n) \Rightarrow \forall n \in \mathbb{N}\, q(n)$
(iv) $\forall n \in \mathbb{N}(p(n) \Rightarrow q(n))$
(v) $\forall n \in \mathbb{N}(q(n) \Rightarrow p(n))$
(vi) $\forall n \in \mathbb{N}(p(n) \Leftrightarrow q(n))$
(vii) $\forall n \in \mathbb{N}(\neg q(n) \Rightarrow \neg p(n))$

Schließlich müssen wir noch besprechen, was es bedeutet, wenn mehrere Quantoren direkt hintereinander stehen. Bei gleichen Quantoren ist das nicht weiter problematisch. Es ist hoffentlich sofort einsichtig, dass die hier in einer Zeile stehenden Aussagen jeweils äquivalent sind:[17]

(i) $\forall m \in \mathbb{N} \forall n \in \mathbb{N}(m+n = n+m)$ und $\forall n \in \mathbb{N} \forall m \in \mathbb{N}(m+n = n+m)$
(ii) $\exists m \in \mathbb{N} \exists n \in \mathbb{N}(m+n = 7)$ und $\exists n \in \mathbb{N} \exists m \in \mathbb{N}(m+n = 7)$

Interessant wird es jedoch, wenn man All- und Existenzquantor mischt. Nehmen wir als Beispiel ein Geschäft, das behauptet, zu jedem Smartphone eine passende Hülle anbieten zu können. Wenn die Variable s für Smartphones steht und h für Hüllen sowie $P(h,s)$ für die Aussage, dass die Hülle h zum Smartphone s passt, dann wirbt der Laden also mit der Aussage $\forall s \exists h\, P(h,s)$. Vertauscht man die Reihenfolge, so erhält man jedoch eine völlig andere Aussage: $\exists h \forall s\, P(h,s)$ besagt, dass es eine „Universalhülle“ gibt, die zu *allen* Smartphones passt! Die erste Behauptung würde man einem gut sortierten Geschäft vielleicht noch abnehmen, die zweite ist mit Sicherheit nicht wahr.

Aufgabe 1.27. Formalisieren Sie analog zum Smartphone-Beispiel das Sprichwort „Auf jeden Topf passt ein Deckel“. Wie müsste die Aussage nach Vertauschen der Quantoren lauten?

Aufgabe 1.28. Welche der folgenden Aussagen sind wahr?

(i) $\forall m \in \mathbb{N} \exists n \in \mathbb{N}(n > m)$
(ii) $\exists n \in \mathbb{N} \forall m \in \mathbb{N}(n > m)$
(iii) $\forall m \in \mathbb{Z} \exists n \in \mathbb{Z}(mn = n)$
(iv) $\exists n \in \mathbb{Z} \forall m \in \mathbb{Z}(mn = n)$

Aufgabe 1.29. Die Individuenvariablen a_1 bis a_4 stehen für vier Geheimagenten. Die Aussageform $P(x,y)$ soll bedeuten, dass Agent x das Passwort von Agent y kennt. Wer wessen Passwort kennt, kann man in der folgenden Tabelle sehen. Steht im Schnittpunkt der i-ten Zeile mit der j-ten Spalte ein Kreuz, dann kennt a_i das Passwort von a_j, sonst nicht.

[17] Man verwendet in solchen Fällen manchmal auch Abkürzungen wie $\forall m, n$ statt $\forall m \forall n$.

	a_1	a_2	a_3	a_4
a_1	×			×
a_2	×		×	×
a_3			×	×
a_4				×

Dieser Tabelle kann man z. B. entnehmen, dass niemand das Passwort von a_2 kennt, nicht einmal a_2 selbst: $\neg\exists x\, P(x, a_2)$. Und man sieht auch, dass alle das Passwort von a_4 kennen: $\forall x\, P(x, a_4)$. Verändern Sie die Tabelle durch Hinzufügen oder Entfernen von Kreuzen so, dass $\forall y\, \exists x\, P(x, y)$ wahr ist, $\exists x\, \forall y\, P(x, y)$ aber nicht. (Und was besagen diese beiden Aussagen eigentlich, wenn man sie ins Deutsche „übersetzt“?)

Aufgabe 1.30. Begründen Sie, dass man aus $\exists x \in \mathbb{N}\, A(x) \wedge \exists x \in \mathbb{N}\, B(x)$ nicht schließen kann, dass $\exists x \in \mathbb{N}\, (A(x) \wedge B(x))$ gilt, indem Sie Aussageformen $A(x)$ und $B(x)$ finden, für die diese Folgerung falsch wäre.

Aufgabe 1.31. Jemand behauptet, jede natürliche Zahl hätte eine ganzzahlige Quadratwurzel. Sie kontern, dass das für 2 oder 3 nicht stimmen könne, denn 1^2 sei 1, 2^2 sei 4 und alle anderen Quadrate von ganzen Zahlen seien logischerweise noch größer als 4, also würden 2 und 3 nie als Quadrate vorkommen. Begründen Sie mit Mitteln der Prädikatenlogik, warum dieses Argument ausreicht, um die ursprüngliche Aussage zu widerlegen.

Beweise

Am Anfang des Abschnitts wurde die Beschäftigung mit der Logik mit Beweisen motiviert. Zum Abschluss schauen wir uns daher kurz und in vereinfachter Form an, wie mathematische Beweise „funktionieren“, wenn man sie durch die Brille der Logik betrachtet.

Wie ich eingangs schrieb, sind Beweise Argumentationsketten. Damit ist gemeint, dass man sich quasi schrittweise zum Ziel „durchhangelt“. Stellen Sie sich für ein ganz banales Beispiel vor, dass Sie erstens wissen, dass x^2 positiv ist, wenn x nicht null ist, und zweitens, dass $1/x$ und x dasselbe Vorzeichen haben. Dann können Sie schließen, dass $1/x^2$ für $x \neq 0$ immer positiv ist. Formal können wir mit den Aussagen $x \neq 0$, $x^2 > 0$ und $1/x^2 > 0$ arbeiten, die wir A, B und C nennen. Dann gehen Sie von $A \Rightarrow B$ und $B \Rightarrow C$ aus und schließen daraus, dass $A \Rightarrow C$ gilt. Unabhängig davon, wofür A, B und C stehen, ist dieser Schluss immer erlaubt:

Aufgabe 1.32. Zeigen Sie mit einer Wahrheitstafel, dass die Implikation

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$$

eine Tautologie ist.

direkter Beweis

Die meisten Beweise bestehen aus vielen aneinandergereihten Implikationen wie im obigen Beispiel. Man nennt das einen *direkten Beweis*.

indirekter Beweis

Manchmal dreht man den Spieß jedoch auch um und beweist $\neg B \Rightarrow \neg A$, wenn man eigentlich $A \Rightarrow B$ beweisen will. Das wird *indirekter Beweis* genannt. Wir

wissen bereits, dass diese beiden Implikationen äquivalent sind. Es kann jedoch unter Umständen leichter sein, die zweite Variante zu beweisen. Nehmen wir als Beispiel an, Sie wollten beweisen, dass eine natürliche Zahl n ungerade ist, wenn n^2 ungerade ist. Man kann das direkt beweisen, aber einfacher ist die Argumentation, dass n^2 gerade ist, wenn n gerade ist: n hat dann die Form $2k$ und n^2 ist deshalb die offensichtlich gerade Zahl $4k^2$.

Aufgabe 1.33. Was waren in diesem Fall A und B?

Beweis durch Widerspruch

Eine häufig verwendete Variante des indirekten Beweises ist schließlich der *Beweis durch Widerspruch*. Die Idee ist, dass man eine Aussage A beweist, indem man zeigt, dass aus ihrer Negation $\neg A$ eine offensichtlich falsche Aussage folgt. Das funktioniert, weil $(\neg A \Rightarrow B \wedge \neg B) \Rightarrow A$ eine Tautologie ist. $B \wedge \neg B$ spielt dabei die Rolle des *Widerspruchs*: einer Aussage, die garantiert nicht wahr ist.

Aufgabe 1.34. Überprüfen Sie, dass $(\neg A \Rightarrow B \wedge \neg B) \Rightarrow A$ eine Tautologie ist.

Satz des Euklid

Ein über 2000 Jahre alter Klassiker des Widerspruchsbeweises ist Euklids Begründung dafür, dass es keine größte Primzahl gibt: Um das zu beweisen, nehmen wir an, es gäbe eine Zahl p, die die größte Primzahl ist. Wir bilden das Produkt m aller Zahlen von 2 bis p. Dann ist keine Primzahl, die kleiner als $m+1$ ist, ein Teiler von $m+1$,[18] also müsste $m+1$ nach Definition eine Primzahl sein. Andererseits ist $m+1$ größer als die „größte“ Primzahl p und kann daher keine Primzahl sein. Da haben wir unseren Widerspruch.

Das soll als kleiner Einblick in die Mechanik der Beweise reichen. Wenn Sie ganz genau aufgepasst haben, dann ist Ihnen aufgefallen, dass man noch viel kleinteiliger sein müsste, wenn man sich ganz sicher sein wollte. (Fußnote 18 besteht zum Beispiel aus vielen Zwischenschritten.) Insbesondere sind wir gar nicht auf die Rolle der Individuenvariablen und der Quantoren eingegangen. Das Zerlegen von Beweisen in „atomare“ (also: nicht mehr weiter zerlegbare) Einzelschritte ist mühsam, aber es wird tatsächlich gemacht und ist auch für die Informatik von Bedeutung. Unter der URL `https://www.cs.ru.nl/~freek/100/` finden Sie Beispiele dafür. Unter anderem findet man dort auch Beweise des Satzes von Euklid in maschinenlesbarer Form.

Resümee

Die Logik als Lehre vom Schlussfolgern, die die Gültigkeit von Argumenten unabhängig von ihren Inhalten untersucht, ist über 2500 Jahre alt und wurde im klassischen Griechenland hauptsächlich durch Aristoteles geprägt. Die moderne mathematische Logik entwickelte sich erst im 19. Jahrhundert unter anderem durch die wegweisenden Arbeiten des Engländers George Boole und des Deutschen Gottlob Frege. Inzwischen spielt sie auch eine wichtige Rolle in der Informatik.

[18] Im Detail: Jede Zahl von 2 bis p teilt offenbar m, also teilt keine von denen $m+1$. Da nach unserer Annahme *alle* Primzahlen unter den Zahlen von 2 bis p sind, gibt es keine Primzahl, die $m+1$ teilt; „erst recht“ keine, die kleiner als $m+1$ ist.

Wir haben hier nur einen kleinen Ausschnitt betrachtet, denn wir wollen uns nicht vertieft mit Logik beschäftigen. Wir werden Junktoren und Quantoren ab und zu verwenden, aber sie sind kein zwingender Bestandteil der mathematischen Fachsprache. Wenn Sie sich mathematische Fachartikel anschauen, werden Sie feststellen, dass viele von denen ohne solche Zeichen auskommen und dann beispielsweise in Worten „und“ oder „for all“ schreiben.[19] Entscheidend ist die hinter solchen Formulierungen stehende Logik.

Der Sinn der letzten Seiten war, Ihr Gespür für logische Zusammenhänge zu schärfen und auf typische Missverständnisse hinzuweisen. Die mathematische Logik modelliert quasi die Art und Weise, wie man in der Mathematik denkt, und häufig ist es sinnvoll, sich die logische Struktur von Argumenten klarzumachen. Dabei kann Ihnen das hier Gelernte hoffentlich helfen.

⋆ Logik im Computer

⋆ Abschnitte oder Aufgaben, die *mit einem Stern* gekennzeichnet sind, sind optional. Wenn Sie Angst haben, aus Versehen etwas zu lernen, das Sie für die Prüfung nicht brauchen, sollten Sie sie überspringen.

Ich werde zwischendurch ab und zu zeigen, wie die Mathematik, um die es in diesem Skript geht, auf dem Computer eingesetzt werden kann. Dazu verwende ich die Programmiersprache PYTHON.[20]

Wenn Sie in PYTHON

```
42 > 23
```

eingeben, dann erhalten Sie die Antwort `True`. Das ist in dieser Programmiersprache eine Konstante, die für *wahr* steht. Gleichzeitig erkennt man an der Antwort, dass `42 > 23` als Aussage aufgefasst und ihr ein Wahrheitswert zugeordnet wurde. Die Eingabe

```
not 42 > 23
```

liefert die Antwort `False`. Darin sieht man nicht nur, dass `False` die Konstante mit der Bedeutung *falsch* ist und dass `not` für die Negation steht, sondern man lernt auch gleich etwas über die Priorität der Operatoren. (Nämlich was?)

Die Eingabe `type(True)` führt zur Ausgabe `bool`.[21] Das ist der Datentyp, den `True` und `False` haben – und außer ihnen kein anderer Wert.

[19] Darum sei hier noch gesagt, dass die stilistische Anmerkung in der Fußnote auf Seite 12 auch für Quantoren gilt: Verwenden Sie die bitte *nie* als Abkürzungen außerhalb von Formeln! So etwas wie „Die Gleichung gilt ∀ natürlichen Zahlen“ sollten Sie niemandem zumuten …

[20] Das Skript kann Ihnen allerdings keine umfassende Einführung in PYTHON liefern. Es gibt dafür z. B. in der Bibliothek der HAW Hamburg genügend kostenlose Materialien. Unter anderem können Sie PYTHON auch mit meinem Buch *Konkrete Mathematik (nicht nur) für Informatiker* lernen.

[21] Benannt nach dem bereits erwähnten George Boole.

Schließlich noch ein einfaches Beispiel dafür, wie Konjunktion und Disjunktion in PYTHON aussehen.[22] Probieren Sie es aus!

```
for x in [10,30,50]:
  if x > 23 and x < 42:
    print(f"{x} > 23 UND {x} < 42")
  if x > 23 or x < 42:
    print(f"{x} > 23 ODER {x} < 42")
```

Prädikatenlogik im mathematischen Sinne spielt in der üblichen imperativen Programmierung keine Rolle. Wenn Sie sich trotzdem damit befassen wollen, dann sollten Sie sich Programmiersprachen wie PROLOG anschauen.

2. Mengen

Mengen sind heutzutage die Grundbausteine der gesamten Mathematik, obwohl sie im Vergleich zum Alter dieser Wissenschaft junge Hüpfer sind. Insbesondere ist die Mengenschreibweise ein wesentlicher Teil der mathematischen Fachsprache. Wenn man sie nicht beherrscht, wird man große Teile der Fachliteratur, auch in der Informatik, nicht verstehen können.[23] Zudem ist die Mengenlehre ein wichtiger Bestandteil der Theoretischen Informatik und Mengen können beim Programmieren eine nützliche Datenstruktur sein.

Was also ist eine Menge?

Definition

Eine **Menge** ist eine Ansammlung von Objekten.

Das ist schon alles! Es klingt total banal, aber der „Erfolg“ des Mengenkonzeptes liegt gerade darin begründet, dass es so einfach ist. Schauen wir uns ein paar Beispiele an:

(i) die Menge der Münzen in meinem Portemonnaie
(ii) die Menge der 16 Bundesländer Deutschlands
(iii) die Menge der Mitschüler Harry Potters
(iv) die Menge, die aus den drei Zahlen 1, π und 42 besteht
(v) die Menge der Geraden, die parallel zur x-Achse verlaufen

Wenn also eben von *Objekten* die Rede war, dann kann damit alles Mögliche gemeint sein: reale Objekte, die man anfassen kann, wie zum Beispiel Geldstücke, aber auch imaginäre Objekte wie Romanfiguren, die nur in unseren Köpfen existieren. In der Mathematik geht es natürlich hauptsächlich um *mathematische* Objekte.[24] Da fallen den meisten Menschen zuerst Zahlen wie im Beispiel (iv) ein.

[22] PYTHON verwendet also *nicht* die Symbole, die in der Tabelle auf Seite 12 aufgeführt sind.
[23] Das gilt auch für dieses Skript!
[24] Die ja grundsätzlich nur in unseren Köpfen existieren. Oder haben Sie schon einmal eine Zahl oder einen Vektor angefasst?

Die Menge (v) zeigt jedoch, dass auch andere Dinge infrage kommen: Geraden, Vektoren, Matrizen, Funktionen und so weiter.

Element

Die Objekte, die in einer bestimmten Menge versammelt sind, nennt man die *Elemente* dieser Menge.[25] Im Beispiel (ii) ist also Hamburg ein Element der Menge, München ist aber keins und 42 auch nicht. In der Aussagenlogik hatten wir gesagt, dass die einzig sinnvolle Frage, die man zu einer Aussage stellen kann, die ist, ob sie wahr oder falsch ist. In diesem Sinne gibt es auch nur einen Typ Frage, den man zu Mengen stellen kann: Ist M eine Menge und x irgendein Objekt, dann kann man fragen, ob x ein Element von M ist oder nicht. Mehr „weiß“ M nicht.

Mengenklammern

Besteht eine Menge nur aus einer überschaubaren Anzahl von Elementen, dann gibt es für sie eine ganz einfache Schreibweise: man schreibt die Elemente durch Kommata[26] getrennt zwischen geschwungene Klammern, sogenannte *Mengenklammern*. Nennen wir die Menge aus Beispiel (iv) X, so sieht das folgendermaßen aus:

$$X = \{1, \pi, 42\}. \tag{2.1}$$

Elementzeichen $\in$ $\notin$

Für die Aussageform „a ist ein Element von B“ ist international die Abkürzung $a \in B$ üblich.[27] In dem aktuellen Beispiel ist also $42 \in X$ wahr und $23 \in X$ falsch. Für die Negation schreibt man auch kurz $23 \notin X$. Ferner ist so etwas wie $x, y \in M$ als Abkürzung für $x \in M \wedge y \in M$ üblich.

Die meisten Mengen, mit denen man es in der Mathematik zu tun hat, sind jedoch zu groß, um alle Elemente wie in (2.1) aufzuschreiben. Manchmal behilft man sich mit Auslassungspunkten wie zum Beispiel in

$$Y = \{1, 2, 3, \ldots, 100\} \quad \text{oder} \quad Z = \{3, 5, 7, \ldots\}, \tag{2.2}$$

aber das ist problematisch. Während es bei Y relativ klar zu sein scheint, dass es um die natürlichen Zahlen von 1 bis 100 geht, kann man bei Z schon ins Grübeln kommen: Ist die nächste Zahl 9, dann sind wohl die ungeraden natürlichen Zahlen gemeint, die größer als 1 sind. Ist sie aber 11, dann sind vielleicht nur die ungeraden Primzahlen gemeint. Oder doch etwas ganz anderes? Eigentlich verlässt man sich darauf, dass die Leser *hoffentlich* verstehen, was man vorhat, denn es sind *immer* mehrere Interpretationen möglich. (Mehr dazu in meinem nicht ganz ernst gemeinten Video *Wie man JEDEN Intelligenztest besteht*.)

Daher geht man in der Regel anders vor. Man *beschreibt* die Menge; so, wie wir es bei den Beispielen (i) bis (v) am Anfang des Abschnitts gemacht haben. Etwas

[25] Man verwendet auch andere naheliegende Formulierungen, z. B., dass ein Objekt zu einer Menge gehört oder dass es in einer Menge enthalten ist.

[26] In manchen Büchern werden auch andere Trennzeichen wie z. B. Semikola verwendet. Das Komma wird wohl am häufigsten verwendet, hat aber in Ländern wie Deutschland den Nachteil, dass es mit dem Dezimalkomma verwechselt werden kann. Dazu später noch mehr.

[27] Dieses Symbol, das sogenannte *Elementzeichen*, geht ebenfalls auf den schon erwähnten Giuseppe Peano zurück. Es ist abgeleitet vom griechischen Buchstaben Epsilon, soll aber von diesem unterscheidbar sein: Man vergleiche ε und $\in$.

formaler: Man gibt eine Aussageform $A(x)$ an, die genau dann wahr ist, wenn x ein Element der Menge ist. Diese *beschreibende Mengenschreibweise* hat die Form[28]

beschreibende Mengenschreibweise

$$M = \{x : A(x)\}$$

und wird gelesen als „M ist die Menge aller x, für die $A(x)$ gilt“. Vielleicht stellen Sie sich eine Menge als einen exklusiven Club vor. Die Aussageform ist dann der Türsteher, der entscheidet, wer eingelassen wird. x darf in den Club (also $x \in M$), wenn $A(x)$ wahr ist. Ist $A(x)$ nicht wahr, dann muss x draußen bleiben: $x \notin M$. Um es etwas konkreter zu machen: Die Menge aus (ii) würde man z. B. als

$$\{x : x \text{ ist ein Bundesland}\}$$

schreiben.

Aufgabe 2.1. Schreiben Sie die folgenden Mengen in *aufzählender Mengenschreibweise* auf, also so wie in (2.1):

aufzählende Mengenschreibweise

$$A = \{n : n \text{ ist eine positive ganze Zahl und } n^2 < 100\}$$
$$B = \{m : m \text{ ist eine ganze Zahl und } |m| \leq 4\}$$

Aufgabe 2.2. Geben Sie die beiden Mengen aus (2.2) in beschreibender Mengenschreibweise an. (Bei Z können Sie sich aussuchen, was gemeint sein soll.)

Aufgabe 2.3. Kann man eine Menge wie X aus (2.1) auch in beschreibender Mengenschreibweise aufschreiben?

Einige Mengen werden so oft benötigt, dass es für sie feste Namen gibt, die sich weltweit eingebürgert haben. Dazu gehören die folgenden:[29]

Symbol	Beschreibung	
$\mathbb{N}$	Menge der natürlichen Zahlen	$\mathbb{N}$
$\mathbb{Z}$	Menge der ganzen Zahlen	$\mathbb{Z}$
$\mathbb{Q}$	Menge der rationalen Zahlen	$\mathbb{Q}$
$\mathbb{R}$	Menge der reellen Zahlen	$\mathbb{R}$
$\mathbb{P}$	Menge der Primzahlen	$\mathbb{P}$

In der Welt der Mathematik ist man sich allerdings nicht einig darüber, ob die Null zu den natürlichen Zahlen gehört. (In meinem Video *Ist eins eine Primzahl?* wird dieses Thema ausführlich behandelt.) Da müssen Sie in jedem Buch, das Sie lesen, genau hinschauen. Wir müssen auch eine Entscheidung treffen. Wir machen es folgendermaßen:

[28] In manchen Büchern findet man statt des Doppelpunkts auch andere Trennzeichen wie zum Beispiel einen senkrechten Strich.

[29] Neben der Schreibweise mit dem Doppelstrich, die ursprünglich durch Kreide und Tafel entstand, gibt es auch die Konvention, im Druck einfach fette Buchstaben zu verwenden, also etwa **N** statt $\mathbb{N}$. Der Buchstabe $\mathbb{Q}$ steht übrigens für *Quotient*, weil rationale Zahlen ja Brüche sind, und das $\mathbb{Z}$ kommt vom deutschen Wort *Zahl*.

Konvention In dieser Vorlesung ist null eine natürliche Zahl: $0 \in \mathbb{N}$.

Aufgabe 2.4. Die Symbole und die Bezeichnungen aus der obigen Tabelle sollten Ihnen eigentlich aus der Schule bekannt vorkommen, aber vielleicht gehen Sie zur Kontrolle noch einmal die folgenden Zahlen durch und überlegen für jede, zu welcher der obigen Mengen sie gehört: $-1/3$, $\sqrt{9}$, 1, $\sqrt{8}$, 42, $14/2$, π, -12, $3/8$, 0, $0.0\overline{1}$.

Aus der Tatsache, dass eine Menge außer „Ist x ein Element von Dir?“ keine weiteren Fragen beantworten kann, kann man eine ganz wesentliche Eigenschaft schließen: Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente haben – denn andere Unterscheidungsmerkmale kann es ja nicht geben. Daraus folgt erstens, dass Mengen keine Reihenfolge kennen. $\{\pi, 42, 1\}$ ist z. B. dieselbe Menge wie $\{1, \pi, 42\}$, denn beide würden auf dieselben Fragen exakt dieselben Antworten geben. Zweitens folgt, dass man so etwas wie $\{1, \pi, 42, 1\}$ zwar hinschreiben kann, dass es sich aber immer noch um dieselbe Menge handelt. Die Zahl 1 ist entweder Element der Menge oder nicht; sie kann nicht „zweimal“ Element der Menge sein.[30] (Wenn Sie Mengen als Datenstrukturen in Programmiersprachen – wo meistens die englische Bezeichnung *set* verwendet wird – einsetzen, dann sind das die beiden wesentlichen Unterschiede zu *Arrays*.)

Enthält eine Menge B mindestens alle Elemente von A, dann sagt man, dass A eine *Teilmenge* von B ist. Wir machen das zur Übung ganz formal:

Definition

> Die Menge A ist eine **Teilmenge** der Menge B, in Zeichen $A \subseteq B$, wenn die Aussage $\forall x\,(x \in A \Rightarrow x \in B)$ gilt. Man sagt auch, dass B eine **Obermenge** von A ist, und schreibt $B \supseteq A$.

Es gilt also beispielsweise $\{1, 13\} \subseteq \{1, 5, 13\}$ und $\{1, 5, 13\} \subseteq \mathbb{N}$. Beachten Sie, dass nach dieser Definition auch $A \subseteq A$ für *jede* Menge A gilt. Daher definieren wir zusätzlich das Folgende:[31]

Definition

> Gilt $A \subseteq B$ und $A \neq B$, dann nennt man A eine **echte Teilmenge** von B und schreibt $A \subset B$.

Erinnern Sie sich noch, wie man begründet, dass eine Aussage mit einem Allquantor *nicht* wahr ist? Man muss lediglich *ein* Gegenbeispiel finden. $A \subseteq B$ gilt also *nicht*, wenn es (mindestens) ein Element von A gibt, das nicht Element von B ist. Man streicht in diesem Fall wieder das Zeichen durch: $A \not\subseteq B$. Außerdem können

$\not\subseteq$

[30] Dahinter steckt auch, dass es jedes mathematisches Objekt nur einmal gibt, obwohl man es evtl. auf verschiedene Arten darstellen kann. Auch $\{1, \pi, 42, 6 \cdot 7\}$ wäre immer noch dieselbe Menge, denn $6 \cdot 7$ *ist* 42.

[31] Leider gibt es viele Bücher, in denen das Zeichen $\subset$ für die (unechte) Teilmengenbeziehung verwendet wird. Da muss man, wie bei dem Symbol $\mathbb{N}$, beim Lesen aufpassen.

Außerdem ist auch die Sprechweise ab und zu etwas ungenau. „A enthält B“ kann sowohl $B \in A$ als auch $B \subseteq A$ bedeuten. Mit dieser Mehrdeutigkeit muss man umzugehen lernen, indem man aus dem Kontext schließt, was gemeint ist. Die formale Notation ist jedenfalls unmissverständlich.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

wir festhalten, dass zwei Mengen genau dann gleich sind, wenn jede der beiden Teilmenge der anderen ist. Es gilt also:

$$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$$

Aufgabe 2.5. In der Schule lernt man, dass $\mathbb{P} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ gilt. (Obwohl man es dort vielleicht nicht so hinschreibt. Ist Ihnen die Bedeutung der Aussage klar?) Begründen Sie mit Gegenbeispielen, dass man keines der Zeichen umkehren kann, dass also z. B. $\mathbb{P} \subset \mathbb{N}$ bzw. $\mathbb{P} \not\supseteq \mathbb{N}$ gilt.

Aufgabe 2.6. Machen Sie sich klar, dass aus $A \subseteq B$ und $B \subseteq C$ folgt, dass A eine Teilmenge von C ist. Es gibt also eine gewisse Ähnlichkeit zwischen $\leq$ und $\subseteq$. Es gibt jedoch auch einen wesentlichen Unterschied: Geben Sie zwei Mengen X und Y an, für die weder $X \subseteq Y$ noch $Y \subseteq X$ gilt.

Es spricht nichts dagegen, eine Menge hinzuschreiben, die gar keine Elemente hat: $\{\}$. Man nennt das die *leere Menge* und es gibt dafür auch noch das gebräuchlichere Symbol $\emptyset$. Es heißt übrigens *die* leere Menge und nicht etwa „eine“ leere Menge, denn eine andere Menge ohne Elemente kann es nicht geben. (Erinnern Sie sich, dass Mengen genau dann gleich sind, wenn sie dieselben Elemente haben.)

leere Menge $\emptyset$

Aufgabe 2.7. Begründen Sie, warum $\emptyset \subseteq A$ für jede Menge A gilt.

Mengenverknüpfungen

Auch Mengen kann man auf verschiedene Arten verknüpfen. Die Verknüpfung von Aussagen erzeugt neue Aussagen und die Verknüpfung von Mengen erzeugt neue Mengen. Wir beginnen mit den drei wichtigsten.

Definition

Für Mengen A und B definieren wir deren **Vereinigung**, **Durchschnitt** und **(mengentheoretische) Differenz** als

$$A \cup B = \{x : x \in A \vee x \in B\}$$
$$A \cap B = \{x : x \in A \wedge x \in B\}$$
$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

Die Vereinigung $A \cup B$ ist also die Menge, die dadurch entsteht, dass man alle Elemente in einer neuen Menge versammelt, die sich in mindestens einer der beiden Mengen A und B befinden. Der Durchschnitt $A \cap B$ entsteht hingegen dadurch, dass man nur die Elemente berücksichtigt, die sich sowohl in A als auch in B befinden. Die Differenz $A \setminus B$ erhält man, indem man aus der Menge A die Elemente entfernt, die auch zu B gehören.[32] Beachten Sie die Ähnlichkeit der Symbole $\cup$ und $\vee$ sowie $\cap$ und $\wedge$. Das ist natürlich Absicht.[33]

[32] Statt $A \setminus B$ findet man in manchen Büchern auch das normale Minuszeichen $A - B$.

[33] Falls Sie eine Eselsbrücke brauchen, dann stellen Sie sich vielleicht $\cup$ als einen Topf vor, in den alles hineingeworfen wird. Oder falls Sie Latein können, dann stellen Sie sich $\vee$ als Anfangsbuchstaben von *vel* vor.

Ein einfaches Beispiel:

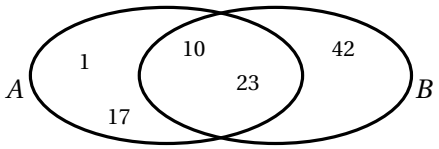
$$\{1,10,17,23\} \cup \{10,23,42\} = \{1,10,17,23,42\}$$
$$\{1,10,17,23\} \cap \{10,23,42\} = \{10,23\}$$
$$\{1,10,17,23\} \setminus \{10,23,42\} = \{1,17\}$$

Natürlich taucht in der ersten Zeile rechts vom Gleichheitszeichen das Element 10 nicht doppelt auf. Wir hatten ja bereits darüber gesprochen, dass es keine „mehrfachen Elemente“ gibt. Beachten Sie außerdem, dass in der letzten Zeile das Element 42 keine Rolle spielt. Man kann aus der linken Menge nichts entfernen, was nicht schon drin war.

Aufgabe 2.8. Es ist offensichtlich, dass Vereinigung und Durchschnitt kommutativ sind. Begründen Sie mit einem Gegenbeispiel, dass die mengentheoretische Differenz *nicht* kommutativ ist.

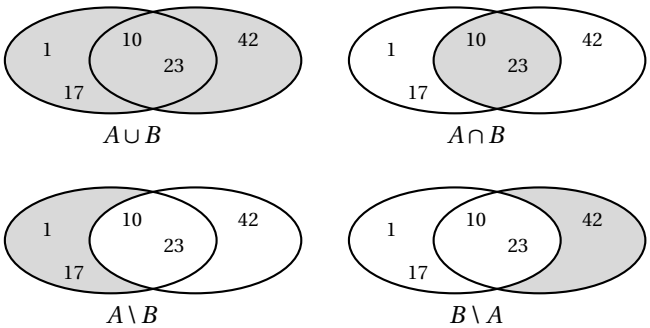
Mengendiagramm

Häufig kann man sich die Beziehungen zwischen Mengen und ihren Verknüpfungen grafisch durch sogenannte *Mengendiagramme* klarmachen. Dafür werden die einzelnen Mengen als Kreise, Ellipsen oder ähnliche geometrische Gebilde dargestellt und man stellt sich vor, dass die Elemente der Mengen sich im Inneren dieser Figuren befinden.



Dabei ist wesentlich, dass jedes Objekt in so einem Diagramm nur einmal vorkommt. Die Zahl 10 darf also beispielsweise nicht sowohl links als auch rechts auftauchen, sondern sie muss in der Mitte im gemeinsamen Gebiet beider Mengen zu finden sein.

Die gerade eingeführten Verknüpfungen kann man dann wie in der folgenden Grafik visualisieren.[34]



Aufgabe 2.9. Im Folgenden sind eine Reihe von Aussagen aufgeführt, die jeweils für *alle* Mengen A, B und C gelten. Einige davon wurden im Text schon behandelt, die meisten aber nicht.

[34] Das „funktioniert“ auch dann noch, wenn es sich um unendliche Mengen handelt, die man sich als Flächen und nicht als aus einzelnen Punkten bestehend vorstellen kann.

(i) $A \subseteq A$
(ii) $\emptyset \subseteq A$
(iii) $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
(iv) $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$
(v) $A \cap A = A$
(vi) $A \cup A = A$
(vii) $A \cap B = B \cap A$
(viii) $A \cup B = B \cup A$
(ix) $A \cap (B \cap C) = (A \cap B) \cap C$
(x) $A \cup (B \cup C) = (A \cup B) \cup C$
(xi) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(xii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(xiii) $A \cup B = A \Leftrightarrow B \subseteq A$
(xiv) $A \cap B = A \Leftrightarrow A \subseteq B$
(xv) $A \cap \emptyset = \emptyset$
(xvi) $A \cup \emptyset = A$
(xvii) $A \cap B \subseteq A$
(xviii) $A \subseteq A \cup B$
(xix) $A \subseteq C \wedge B \subseteq C \Rightarrow A \cup B \subseteq C$
(xx) $A \subseteq B \wedge A \subseteq C \Rightarrow A \subseteq B \cap C$
(xxi) $A \setminus \emptyset = A$
(xxii) $A \setminus A = \emptyset$
(xxiii) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
(xxiv) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
(xxv) $B \subseteq C \Rightarrow A \setminus C \subseteq A \setminus B$
(xxvi) $A \setminus B = \emptyset \Leftrightarrow A \subseteq B$
(xxvii) $B \cup C \subseteq A \Rightarrow B \setminus C = B \cap (A \setminus C)$

Machen Sie sich jeweils klar, ob Sie die Aussagen verstanden haben. Überzeugen Sie sich außerdem durch Beispiele oder Mengendiagramme von der Korrektheit der Aussagen. Erkennen Sie in (xxiii) und (xxiv) die de-morganschen Regeln?

Aufgabe 2.10. Da in diesem Skript die Null ein Element von $\mathbb{N}$ ist, führen wir das Symbol $\mathbb{N}^+$ für die *positiven* natürlichen Zahlen ein, also für die, die größer als null sind. Definieren Sie $\mathbb{N}^+$ einmal durch die beschreibende Mengenschreibweise und einmal mithilfe von Mengenverknüpfungen. $\mathbb{N}^+$

Aufgabe 2.11. Geben Sie (analog zu den Darstellungen in Aufgabe 2.9) eine Formel für $A \cap B$ an, in der nur die mengentheoretische Differenz verwendet wird.

Abkürzungen

Wenn man die beschreibende Mengenschreibweise verwendet, besteht die die Menge definierende Aussageform (der „Türsteher“) meistens aus einer Konjunktion und eine der Teilaussagen ist die Angabe einer Grundmenge; zum Beispiel $\mathbb{N}^+ = \{n : n \in \mathbb{N} \wedge n > 0\}$ aus Aufgabe 2.10, wobei hier $\mathbb{N}$ die Grundmenge ist. In

solchen Fällen hat es sich eingebürgert, diesen Teil *vor* den Doppelpunkt zu ziehen: $\{n \in \mathbb{N} : n > 0\}$. Allgemein formuliert:

Konvention

Ist M eine Menge und $A(x)$ eine Aussageform, dann ist $\{x \in M : A(x)\}$ eine Abkürzung für $\{x : x \in M \wedge A(x)\}$.

Sie werden wahrscheinlich denken, dass man kaum von einer „Abkürzung“ sprechen kann, weil man gerade mal ein Zeichen spart. Diese Schreibweise hat aber den Vorteil, dass man sofort sieht, um welche Objekte es geht. Man liest $\{n \in \mathbb{N} : n > 0\}$ als „Menge aller natürlichen Zahlen, die größer als 0 sind“ und das lässt sich besser verstehen als „Menge aller Objekte, die natürliche Zahlen und größer als 0 sind“.

Außerdem gibt es noch eine weitere, sehr hilfreiche Abkürzung. Wie würden Sie die Menge

$$M = \{0, 1, 4, 9, 16, 25, \ldots\}$$

aufschreiben? Offenbar sind die Quadrate 0^2, 1^2, 2^2 und so weiter der natürlichen Zahlen gemeint. Jedes Element der Menge M entsteht also dadurch, dass man sich ein Element von $\mathbb{N}$ herausgreift und damit etwas macht: man quadriert es. Das könnte man als

$$M = \{k : \exists n\,(n \in \mathbb{N} \wedge k = n^2)\}$$

notieren. Man spart sich aber in der Regel den „Zwischenschritt“ der Einführung einer weiteren Variablen und schreibt stattdessen so etwas wie

$$M = \{n^2 : n \in \mathbb{N}\}. \tag{2.3}$$

Ganz allgemein kann man das so formulieren:

Konvention

Ist $A(x_1, \ldots, x_n)$ eine Aussageform und $t(x_1, \ldots, x_n)$ ein von den Variablen x_1 bis x_n abhängender Term, dann ist

$$\{t(x_1, \ldots, x_n) : A(x_1, \ldots, x_n)\}$$

eine Abkürzung für $\{y : \exists x_1 \ldots \exists x_n (A(x_1, \ldots, x_n) \wedge y = t(x_1, \ldots, x_n))\}$.

Wir haben natürlich nicht definiert, was ein „Term“ sein soll,[35] aber das wird hoffentlich durch die folgenden Beispiele klarer werden. $t(x)$ wird im Allgemeinen etwas sein, das man „ausrechnen“ kann, wenn man x kennt; so etwas wie $3x$, $x^2 - 7$ aber auch $x \cup \{42\}$, denn x muss nicht unbedingt eine Zahl sein. In (2.3) ist der Term $t(n)$ beispielsweise n^2 und die Aussageform $A(n)$ ist $n \in \mathbb{N}$. Die Variable n „durchläuft“ quasi alle Objekte, die $A(n)$ wahr machen (in diesem Fall die natürlichen Zahlen) und in M werden die zugehörigen Werte $t(n)$ (also die Quadrate) gesammelt.

[35] Man kann das präzise machen, dafür müssten wir jedoch tief in die Prädikatenlogik einsteigen.

Die Definition wurde absichtlich so allgemein formuliert, dass auch mehrere Variablen involviert sein können. Ein Beispiel dafür könnte folgendermaßen aussehen:

$$X = \{1,2,3,4\}$$
$$Y = \{10,20,30\}$$
$$Z = \{\, y - x : x \in X \wedge y \in Y \,\} = \{9,8,7,6,19,18,17,16,29,28,27,26\}$$

Hier ist der Term $t(x,y)$ die Differenz $y-x$ und die Aussageform $A(x,y)$ ist die Konjunktion $x \in X \wedge y \in Y$. Das ist so gemeint, dass *alle* Kombinationen von x und y, die $A(x,y)$ wahr machen, durchlaufen werden. Unter anderem sind $A(1,10)$ und $A(2,20)$ wahr, aber auch $A(2,10)$ oder $A(1,20)$.

Das ist fürs Erste alles zur Sprache der Mengenlehre. Es bleibt nur noch zu ergänzen, dass Sie die beiden in diesem Abschnitt vorgestellten Abkürzungen vorerst bitte *nicht gleichzeitig* verwenden sollten! So etwas wie

$$\{\, n - 7 \in \mathbb{N} : n < 10 \,\}$$

ist bestenfalls verwirrend und meistens sogar falsch. Wahrscheinlich ist

$$\{\, n - 7 : n \in \mathbb{N} \wedge n < 10 \,\}$$

gemeint. Dann ergibt aber $n-7 \in \mathbb{N}$ keinen Sinn, denn zu dieser Menge gehört auch $6-7=-1$ und das ist keine natürliche Zahl. Sie werden in manchen Büchern (und vielleicht sogar auch weiter hinten im Skript) Varianten dieser Schreibweisen sehen. Mit etwas Erfahrung versteht man, was gemeint ist, aber erst einmal muss man sich langsam daran gewöhnen.

Aufgabe 2.12. Welche Beziehung besteht zwischen $\{\, n^2 : n \in \mathbb{N} \,\}$ und $\{\, n^2 : n \in \mathbb{Z} \,\}$?

Aufgabe 2.13. Man kann $\mathbb{Z}$ durch $\mathbb{Z} = \mathbb{N} \cup \{\, -n : n \in \mathbb{N} \,\}$ definieren. Definieren Sie $\mathbb{Q}$ mithilfe von $\mathbb{N}$, $\mathbb{N}^+$ und $\mathbb{Z}$.

Aufgabe 2.14. Die Definition von $\mathbb{Z}$ aus Aufgabe 2.13 wird von Studierenden manchmal *fälschlicherweise* (!) auch als $\{\, n, -n : n \in \mathbb{N} \,\}$ geschrieben. Was ist daran falsch?

Aufgabe 2.15. Konstruieren Sie einen Ausdruck für die Menge aller Schaltjahre seit Einführung des gregorianischen Kalenders (siehe Aufgabe 1.21), in dem nur die vier Mengen

$$G = \{\, n \in \mathbb{N} : n \geq 1582 \,\},$$
$$A_4 = \{\, n \in G : 4 \text{ teilt } n \,\},$$
$$A_{100} = \{\, n \in G : 100 \text{ teilt } n \,\} \text{ und}$$
$$A_{400} = \{\, n \in G : 400 \text{ teilt } n \,\}$$

sowie die Verknüpfungen Vereinigung, Durchschnitt und Differenz vorkommen.

Aufgabe 2.16. Finden Sie für die folgenden Mengen, die alle absichtlich kompliziert aufgeschrieben wurden, jeweils möglichst einfache Darstellungen:

$$A = \{n \in \mathbb{N} : n^2 < 1\} \qquad B = \{n \in \mathbb{N} : n^2 \geq 0\}$$
$$C = \{x \in \mathbb{Q} : x \in \mathbb{R}\} \qquad D = \{x \in \mathbb{R} : x \in \mathbb{Q}\}$$
$$E = \mathbb{N} \cup \mathbb{Q} \qquad F = \mathbb{N} \setminus \mathbb{Q}$$
$$G = \{|z| : z \in \mathbb{Z}\} \qquad H = \{-z : z \in \mathbb{Z}\}$$

Aufgabe 2.17. Jeweils zwei der unten aufgeführten Mengen sind gleich. Finden Sie die entsprechenden Paare.

$$A = \mathbb{R} \cap \mathbb{R} \qquad B = \{x \in \mathbb{Q} : x^2 = 8\} \cup \mathbb{N}$$
$$C = \mathbb{R} \cup \mathbb{R} \qquad D = \{x \in \mathbb{Q} : x^2 = x \wedge x < 1\}$$
$$E = \mathbb{N} \cup \{42\} \qquad F = \{x \in \mathbb{R} : x^2 = x \wedge x < 0\}$$
$$G = \{2\sqrt{2}\} \qquad H = \{x \in \mathbb{R} : x^2 = 8 \wedge x > 0\}$$
$$I = \{n \in \mathbb{N} : n^2 \leq 0\} \qquad J = \{x \in \mathbb{Q} : x^2 = 8 \wedge x > 0\}$$

Aufgabe 2.18. Jeweils zwei der unten aufgeführten Mengen sind gleich. Finden Sie die entsprechenden Paare.

$$A = \{\tfrac{m}{n} : m \in \mathbb{N} \wedge n \in \mathbb{N}^+\} \qquad B = \mathbb{Z} \cap \mathbb{N}$$
$$C = \{r \in \mathbb{R} : \exists z \in \mathbb{Z}\,(z < 0 \wedge r = |z|)\} \qquad D = \{1, 2, 3, 4, \ldots\}$$
$$E = \{r \in \mathbb{R} : r < 0 \wedge r^2 = r\} \qquad F = \mathbb{N} \setminus \{\sqrt{2}, \pi, -42\}$$
$$G = \{5y : y \in \mathbb{Q} \wedge y \geq 0\} \qquad H = \{s \in \mathbb{R} : s < 1 \wedge 1 - s < 0\}$$

Aufgabe 2.19. Schreiben Sie die folgenden Mengen in beschreibender Mengenschreibweise auf:

(i) Die ganzen Zahlen, deren Quadrat kleiner als 100 ist.
(ii) Die natürlichen Zahlen, die durch 3 teilbar und nicht größer als 300 sind.
(iii) Die positiven Brüche, deren Zähler in gekürzter Form 2 ist.

Aufgabe 2.20. A sei die Menge der natürlichen Zahlen, deren Quadrat kleiner als 400 und durch 12 teilbar ist. B sei die Menge der natürlichen Zahlen, deren Quadrat kleiner als 400 ist und die durch 12 teilbar sind. Geben Sie die beiden Mengen in beschreibender Mengenschreibweise an. Gilt $A = B$?

Resümee

Das mathematische Teilgebiet der Mengenlehre wurde erst nach 1870 von dem Deutschen Georg Cantor begründet, entwickelte sich dann aber ziemlich stürmisch. Der faszinierendste Aspekt der Mengenlehre sind die von Cantor entdeckten unterschiedlichen Unendlichkeiten. Mit denen werden wir uns allerdings erst wesentlich später und nur kurz beschäftigen.

Die Wichtigkeit der Mengenlehre rührt daher, dass man *alles andere*,[36] was in der Mathematik benötigt wird, mithilfe von Mengen aufbauen kann – sogar Zahlen![37] Mengen sind die Legobausteine, aus denen man sich mit genügend Geduld den gesamten Rest der Mathematik zusammenbasteln kann. Insbesondere kann man mit ihnen alle anderen mathematischen Objekte präzise beschreiben. Die große Mehrheit der Mathematikerinnen und Mathematiker befasst sich in der täglichen Arbeit nicht mit Fragen der Mengenlehre, aber alle kennen und nutzen die *Sprache* der Mengenlehre.

Schließlich muss noch erwähnt werden, dass wir – wie es in so einem Rahmen üblich ist – sogenannte *naive Mengenlehre* betreiben. Damit ist gemeint, dass wir den Begriff der Menge nicht genau genug abgegrenzt haben und damit theoretisch Gefahr laufen, auf Widersprüche zu stoßen. In der *axiomatischen Mengenlehre* geht man wesentlich vorsichtiger vor. Das ist jedoch etwas für die „Profis“ und würde das Niveau dieser Vorlesung deutlich überschreiten.

naive Mengenlehre

axiomatische Mengenlehre

⋆ Mengen im Computer

PYTHON hat einen eigenen Datentyp `set` für Mengen und man kann „kleine“ Mengen so eingeben, wie man sie auch von Hand schreiben würde:[38]

```
A = {1,10,17,23}
B = {10,23,42}
```

Nach den obigen Zuweisungen können Sie z. B. das Folgende ausprobieren:

```
10 in A     # Element
{10} <= A   # Teilmenge
A | B       # Vereinigung
A & B       # Durchschnitt
A - B       # mengentheoretische Differenz
```

Vielleicht gehen Sie Aufgabe 2.9 mal mit PYTHON durch?

PYTHON bietet außerdem eine *comprehension* genannte Syntax, die der beschreibenden Mengenschreibweise sehr ähnlich ist und von dieser inspiriert wurde.[39] Dazu hier nur zwei einfache Beispiele:

```
C = {x for x in A if x**2 > 100}
D = {x**2 for x in B}
```

[36] Für die, die es ganz genau wissen wollen: Im Video *Abstrakter Unsinn?* wird erläutert, warum diese Aussage auf Teile der sogenannten Kategorientheorie nicht ganz zutrifft.

[37] Wie das geht, wird am Ende des Videos *Das Zermelo-Fraenkel-Axiomensystem der Mengenlehre* erklärt.

[38] Lediglich für die leere Menge muss man `set()` schreiben, weil `{}` in PYTHON eine andere Bedeutung hat.

[39] Man findet diese angenehme Syntax nur in wenigen anderen Programmiersprachen wie JULIA oder HASKELL.

Damit hätte man $C = \{x \in A : x^2 > 100\}$ sowie $D = \{x^2 : x \in B\}$ definiert.

Man kann auch Elemente zu Mengen hinzufügen bzw. vorhandene entfernen:

```
A.add(100)
B.remove(42)
```

Damit macht man allerdings etwas, was in der Mathematik tabu ist. Wenn dort eine Bezeichnung wie B vergeben wird, dann wird sich diese Zuordnung nicht wieder ändern. Es wird in einem Fachtext *nie* so sein, dass beispielsweise B erst für $\{10,23,42\}$ steht und etwas später dann auf einmal für $\{10,23\}$.[40] Mengen in PYTHON sind *mutable* (veränderlich), mathematische Objekte nicht.

Dadurch werden Mengen im Computer jedoch zur Datenstruktur der Wahl, wenn es darum geht, in einem Programm zu speichern, ob bestimmte Objekte schon einmal untersucht oder bearbeitet wurden. Sie eignen sich dafür besser als beispielsweise Arrays.

[40] Natürlich kann wie im Skript A erst für eine Aussage und dann ein paar Seiten später in einem anderen Abschnitt für eine Menge stehen. Aber so eine „Transformation“ findet nicht innerhalb ein und desselben Gedankengangs statt.

III

Elementare Kombinatorik

Es ist nicht so einfach, kurz und knapp zu beschreiben, was genau mit dem Wort *Kombinatorik* aus der Überschrift gemeint ist. Auf jeden Fall geht es in dem Teil der Kombinatorik, mit dem wir uns zunächst beschäftigen wollen, oft darum, Dinge zu *zählen*. Das klingt banal, kann aber ziemlich kompliziert werden. Gleichzeitig ist es in vielen Fällen von Bedeutung für die Informatik, weil man dort oft abschätzen muss, welchen Ressourcenverbrauch bestimmte Algorithmen oder Datenstrukturen haben. Auch für die Stochastik – und damit für die statistischen Methoden, die heutzutage in fast allen Wissenschaften eine Rolle spielen – ist die Kombinatorik eine wichtige Grundlage.

3. Komplexere Mengenstrukturen

In den Beispielen im letzten Abschnitt haben wir uns auf Mengen von Zahlen beschränkt. Wir haben jedoch von Anfang an vorgesehen, dass Mengen nicht nur Zahlen, sondern beliebige (mathematische) Objekte enthalten können. Wesentliche Beispiele dafür, was Mengen außer Zahlen noch so enthalten können, werden auf den nächsten Seiten vorgestellt. Parallel dazu werden wir uns mit der Frage beschäftigen, wie „groß“ gewisse Mengen sind.

Mengen von Mengen

Wir hatten Mengen sehr allgemein als Ansammlungen von *Objekten* definiert. Mengen selbst sind auch Objekte, also können auch Mengen Elemente von Mengen sein,[1] z. B.

$$A = \{1, 2, \{3, 4\}\}. \tag{3.1}$$

Diese Menge besteht aus drei Objekten: den beiden Zahlen 1 und 2 sowie der Menge $\{3,4\}$. Es gilt also insbesondere $\{1,2\} \subseteq A$ und $\{3,4\} \in A$. Aber es gilt *nicht*

[1] Man könnte die spitzfindige, aber völlig legitime Frage stellen, ob eine Menge ein Element von sich selbst sein kann. In der axiomatischen Mengenlehre „verbietet“ man das in der Regel durch das sogenannte *Fundierungsaxiom*. Aber es würde auch nicht schaden und für die Praxis außerhalb der Grundlagenforschung ist es nicht relevant.

$\{1,2\} \in A$ und auch *nicht* $3 \in A$ oder $\{3,4\} \subseteq A$. Eigentlich sollte das allein durch das Betrachten von (3.1) klar sein, denn dort werden die drei Elemente von A ja – durch Kommata getrennt – aufgezählt. Aber die Erfahrung lehrt, dass es an dieser Stelle oft Verständnisprobleme gibt.

Dagegen hilft wohl nur, sich die Bedeutung von $\in$ und $\subseteq$ noch einmal klarzumachen. Und vielleicht hilft es auch, die Elemente der Menge im Geiste durch Variablen zu ersetzen. Schreibt man x und y für 1 und 2 sowie B für $\{3,4\}$, dann ist A die Menge $\{x, y, B\}$. Jetzt *sieht* man, dass B ein Element von A ist, oder? Und dass 3 kein Element von A ist (und deshalb B auch keine Teilmenge von A sein kann), liegt daran, dass 3 weder x noch y noch B ist. Sollten Sie mit dem Konzept immer noch Schwierigkeiten haben, dann lesen Sie eventuell zu schnell. Vielleicht noch einmal die Gebrauchsanweisung anschauen?

Aufgabe 3.1. Denken Sie sich zwei Mengen A und B mit $A \in B$ und $A \subseteq B$ aus.

Wir führen nun eine spezielle Menge von Mengen ein:

Definition

Die **Potenzmenge** einer Menge A ist die Menge aller Teilmengen von A: $\mathscr{P}(A) = \{X : X \subseteq A\}$.

Wie muss man sich das vorstellen? Fangen wir ganz klein an. Wie sieht die Potenzmenge der leeren Menge aus? Die leere Menge ist – siehe Aufgabe 2.7 – Teilmenge *jeder* Menge. Und andere Teilmengen kann $\emptyset$ natürlich nicht haben. Also ergibt sich $\mathscr{P}(\emptyset) = \{\emptyset\}$. Achtung! $\{\emptyset\}$ ist *nicht* dasselbe wie $\emptyset$. Die erste Menge hat genau ein Element, nämlich $\emptyset$, während die zweite *kein* Element hat. Es gilt also $\emptyset \in \{\emptyset\}$ und $\emptyset \notin \emptyset$. Darum sind die beiden Mengen nicht gleich, denn zwei Mengen sind – Sie erinnern sich? – dann und nur dann gleich, wenn sie dieselben Elemente haben.

Vielleicht kommen Ihnen solche Feinheiten pedantisch vor. Wen interessiert der Unterschied zwischen $\emptyset$ und $\{\emptyset\}$? Für einen erfolgreichen Umgang mit der Mathematik ist es jedoch wichtig, sich an eine Ausdrucksweise zu gewöhnen, die präziser als die Alltagssprache ist. Sie müssen Ihre Gedanken eindeutig und unmissverständlich artikulieren können. Und Sie müssen in der Lage sein, in mathematischen Texten nur das zu lesen, was dort wirklich steht, ohne etwas hineinzuinterpretieren. Beides gelingt nur durch Übung.

Singleton

Aber zurück zur Potenzmenge. Die nächstgrößere Menge ist eine, die nur aus einem Element besteht, z. B. $\{42\}$. Das liest man übrigens als *Singleton* 42.[2] Es ist wohl offensichtlich, dass es in diesem Fall zwei Teilmengen gibt, also

$$\mathscr{P}(\{42\}) = \{\emptyset, \{42\}\}.$$

Und wenn wir eine Menge wie $\{23,42\}$ mit zwei Elementen haben, dann ergibt sich als Potenzmenge

$$\mathscr{P}(\{23,42\}) = \{\emptyset, \{23\}, \{42\}, \{23,42\}\}.$$

[2] Es wäre falsch, einfach „42“ zu sagen, weil die Menge $\{42\}$ nicht dasselbe wie die Zahl 42 ist.

Ich zeige auch noch ein Beispiel für eine dreielementige Menge und hebe dabei das Element hervor, das gegenüber dem letzten Beispiel hinzugekommen ist:

$$\mathscr{P}(\{7,23,42\}) = \{\emptyset,\{7\},\{23\},\{7,23\},\{42\},\{7,42\},\{23,42\},\{7,23,42\}\}. \tag{3.2}$$

Aufgabe 3.2. Können Sie ein Muster erkennen? Welcher Zusammenhang besteht zwischen der Anzahl der Elemente von A und der Anzahl der Teilmengen von A?

Vielleicht sind Sie beim Nachdenken über die letzte Aufgabe von selbst darauf gekommen: Wenn man zu einer Menge ein Element hinzufügt, dann verdoppelt sich die Anzahl der Teilmengen.[3] Den Grund kann man am Beispiel (3.2) erkennen: Die Teilmengen von $\{23,42\}$ sind auch Teilmengen von $\{7,23,42\}$, aber zu jeder dieser „alten“ Teilmengen kommt durch Ergänzen des Elements 7 eine „neue“ Teilmenge hinzu – aus $\emptyset$ wird $\{7\}$, aus $\{23\}$ wird $\{7,23\}$ und so weiter.

Dieses Ergebnis wollen wir festhalten und führen dafür eine Schreibweise ein.[4]

Definition

Für eine endliche Menge A bezeichnen wir mit $|A|$ die Anzahl ihrer Elemente. Man nennt das die **Mächtigkeit** von A.

Was wir uns vor dieser Definition überlegt haben, können wir nun kurz und knackig so aufschreiben:[5]

Satz 3.1

Mächtigkeit der Potenzmenge
Für jede endliche Menge A gilt $|\mathscr{P}(A)| = 2^{|A|}$.

Hier sehen wir zum ersten Mal einen wichtigen Begriff der Mathematik. Darum sollte ich darüber ein paar Worte verlieren, bevor wir fortfahren. Am Anfang des Abschnitts über Aussagenlogik hatte ich geschrieben, dass es in der Mathematik darum geht, welche Aussagen wahr oder falsch sind.[6] Ist man sich bei einer Aussage sicher, dass sie wahr ist, dann spricht man von einem *Satz*. Wenn Sie also in einem Lehrbuch oder in einem Skript wie diesem etwas sehen, das als Satz markiert ist, dann können Sie davon ausgehen, dass es wahr ist.

Satz

In einem Studium der Mathematik muss auf einen Satz immer der Beweis folgen. Da wir hier die Mathematik aus einer etwas anderen Perspektive betrachten, werden wir das nicht so streng halten. In vielen Fällen werden Sie mir einfach glauben müssen, dass eine Aussage wahr ist. Ich werde Ihnen jedoch häufig eine *Begründung* (quasi einen nicht so streng ausgearbeiteten Beweis) anbieten,

[3] Vorsicht! Das gilt nur für endliche Mengen. Lesen Sie weiter!

[4] Wir setzen eine intuitive Vorstellung davon voraus, wann eine Menge *endlich* ist. Wenn man Mengenlehre „ernsthaft“ betreibt, dann muss man erstens präzise definieren, was man mit *endlich* meint, und man kann zweitens auch für unendliche Mengen deren *Kardinalität* (ein anderes Wort für Mächtigkeit) angeben. Übrigens findet man statt $|A|$ in manchen Büchern auch die Notation $\#A$.

[5] Wegen dieses Zusammenhangs wird für die Potenzmenge von A in manchen Büchern auch 2^A statt $\mathscr{P}(A)$ geschrieben. Wir werden diese Schreibweise nicht verwenden.

[6] Natürlich geht es nicht um beliebige Aussagen wie $2+3=5$, sondern um *interessante*.

wenn ich das didaktisch für geboten halte. Im Falle von Satz 3.1 finden Sie den relevanten Teil der Begründung *vor* dem Satz: Wir hatten uns bereits überlegt, dass die Potenzmenge der leeren Menge aus einem Element besteht und dass bei Hinzunahme eines Elements sich die Anzahl der Teilmengen verdoppelt. Das war's schon. Für ein Lehrbuch über Mengenlehre müsste man genauer vorgehen, aber für uns soll es reichen. Erwähnenswert ist noch, dass wir in diesem Rahmen nur etwas über endliche Mengen aussagen können; darum steht das auch explizit in der Formulierung des Satzes. Außerdem haben wir stillschweigend vorausgesetzt, dass die Anzahl der Teilmengen von A nur von der Anzahl der Elemente von A abhängt. $\{3\}$ hat also nicht mehr oder weniger Teilmengen als die Menge $\{\pi\}$ oder eine Menge, die nur aus einem Vektor besteht. Das ist zwar hoffentlich klar, sollte aber ruhig auch ausgesprochen werden.

Proposition
Theorem
Lemma

Statt *Satz* sind auch andere Bezeichnungen gebräuchlich, unter anderem *Proposition* und *Theorem*. Ein Satz, der für sich genommen nicht so interessant ist, der jedoch für den Beweis anderer Sätze hilfreich sein kann, wird gerne auch *Lemma* genannt. Ein Satz, der aus einem anderen Satz ohne große Arbeit direkt folgt, wird oft als *Korollar* bezeichnet. Diese Einteilung ist jedoch subjektiv. In allen Fällen handelt es sich um Aussagen, von denen man beweisen kann, dass sie wahr sind.

Korollar

Definition

Nicht beweisen kann man hingegen *Definitionen*. Definitionen sind lediglich Festlegungen der Fachsprache und sie können nicht wahr oder falsch sein, höchstens sinnvoll oder weniger sinnvoll. (Das Video *Ist eins eine Primzahl? Ist null eine natürliche Zahl?* erklärt das anhand von einfachen Beispielen.) Zum Glück sind die meisten Definitionen inzwischen allseits akzeptierter Standard. Wir haben aber auch schon Beispiele gesehen, bei denen Uneinigkeit besteht.[7] Definitionen und Konventionen sind für das Verständnis eines mathematischen Textes wichtig, aber sie sind nicht in Stein gemeißelt.

Konvention

Aufgabe 3.3. Sei A die Menge $\{\emptyset, \{\emptyset\}\}$ und $B = \{1,2\}$. Geben Sie die vier Mengen $A \setminus \emptyset$, $A \setminus \{\emptyset\}$, $B \setminus \emptyset$ und $B \setminus \{\emptyset\}$ an.

Aufgabe 3.4. Welche der folgenden Aussagen ist wahr? Geben Sie bei den falschen Aussagen jeweils ein Element an, das in der einen, aber nicht in der anderen Menge enthalten ist.

(i) $\{1,\{2\}\} = \{2,\{1\}\}$
(ii) $\{1,\{2\}\} \cup \{2,\{1\}\} = \{1,2\}$
(iii) $\{1,\{2\}\} \cup \{2,\{1\}\} = \{\{1,2\}\}$
(iv) $\{1,\{2\}\} \cup \{2,\{1\}\} = \{\{1\},\{2\}\}$
(v) $\{1,\{2\}\} \setminus \{2,\{1\}\} = \{2,\{1\}\} \setminus \{1,\{2\}\}$
(vi) $\{\emptyset\} \cup \emptyset = \{\emptyset\}$
(vii) $\{1\} \cup \emptyset = \{1,\emptyset\}$
(viii) $\{1\} \cup \{\emptyset\} = \{1\}$
(ix) $\mathscr{P}(\mathbb{N}) \setminus \{\{0\}\} = \mathscr{P}(\mathbb{N}^+)$

[7] Schreibt man lieber $\overline{A}$ statt $\neg A$? Soll null eine natürliche Zahl sein?

Aufgabe 3.5. Sei $A = \{n \in \mathbb{N}^+ : n < 4\}$ und $B = \{mn : m, n \in A\}$. Geben Sie $|B|$ an. Worauf müsste man zusätzlich achten, wenn in der Aufgabenstellung statt 4 zum Beispiel 7 stünde?

Aufgabe 3.6. Sei $A = \{n \in \mathbb{N}^+ : n < 7\}$ und $B = \{mn : m, n \in A\}$. Geben Sie die Mächtigkeit von $\mathscr{P}(\{B\})$ an.

Aufgabe 3.7. Wenn A und B Mengen mit $A \cap B = \emptyset$ sind, dann ist auch der Durchschnitt von $\mathscr{P}(A)$ und $\mathscr{P}(B)$ leer.[8] Stimmt das oder stimmt das nicht? Oder stimmt es nur für bestimmte Mengen?

Aufgabe 3.8. Die Aussageformen $\mathscr{P}(A \setminus B) = \mathscr{P}(A) \setminus \mathscr{P}(B)$ und $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$ sind beide nicht für beliebige Mengen A und B wahr. Finden Sie jeweils konkrete Beispiele für A und B, die sie zu falschen Aussagen machen.

Aufgabe 3.9. Seien a, b und c ganze Zahlen. Was kann man über die Mächtigkeit von $X = \{a, b, c\} \setminus \{a\}$ aussagen?

Aufgabe 3.10. Sortieren Sie die folgenden Mengen nach Mächtigkeit:

$$A = \{n \in \mathbb{N} : n^2 = 42\} \qquad B = \{n \in \mathbb{N} : n^2 + 1 < 42\}$$
$$C = \{n \in \mathbb{N} : n^2 - 7 = 42\} \qquad D = \{n \in \mathbb{N} : (n+1)^2 < 42\}$$
$$E = \{n \in \mathbb{N} : n \text{ teilt } 42\} \qquad F = \{n \in \mathbb{N} : 2n < 42\}$$

Aufgabe 3.11. Wie viele Teilmengen von $A = \{n \in \mathbb{N} : n < 20\}$ enthalten mindestens eine Primzahl?

Aufgabe 3.12. Wie viele Teilmengen von $A = \{k \in \mathbb{N} : 3 \leq k \leq 30\}$ gibt es, die mindestens eine durch 3 teilbare Zahl enthalten?

⋆ Mengen von Mengen im Computer

PYTHON bietet zusätzlich zu Mengen „gefrorene Mengen“ an. Damit kann man Mengen als Elemente von Mengen speichern, was mit dem Datentyp `set` nicht möglich ist:[9]

```
X = frozenset({1,2,3})
Y = {1,2,3,X}
X <= Y, X in Y
```

Eine Aufgabe wie 3.5 würde man für größere Zahlen wohl lieber bequem mit Computerhilfe lösen. Das könnte so aussehen:

[8] Das ist wieder so eine typische Sprechweise, die sich eingebürgert hat. Wenn man sagt, dass eine Menge *leer* ist, meint man damit natürlich, dass es sich um die leere Menge handelt. leer

[9] Wenn Sie in dem folgenden Beispiel `frozenset({1,2,3})` durch `{1,2,3}` ersetzen, erhalten Sie eine Fehlermeldung. In Mengen kann man nur Objekte speichern, die nicht *mutable* (siehe Seite 36) sind, und gefrorene Mengen sind solche Objekte: `add` und `remove` erlauben sie nicht. In diesem Sinne sind sie „mathematischer“ als die normalen Mengen von PYTHON. (Für die PYTHON-Experten: Eigentlich geht es darum, ob die Objekte *hashable* sind.)

```
A = set(range(1,7))
len({m*n for m in A for n in A})    # Mächtigkeit einer Menge
```

Die folgende Funktion ist ein Generator, der rekursiv durch die Potenzmenge einer Menge iteriert.[10]

```
def powerSet(M):                    # engl. Wort für Potenzmenge
  if M == set():
    yield set()
  else:
    S = {next(iter(M))}             # {x} für ein x aus M
    for A in powerSet(M - S):
      yield A
      yield A | S
```

Dass Satz 3.1 zumindest für die ersten zehn natürlichen Zahlen stimmt, kann man so überprüfen:

```
all(2**n == sum(1 for A in powerSet(set(range(n))))
    for n in range(10))
```

Will man wirklich die Potenz*menge* haben, dann muss man auf die eben erwähnten gefrorenen Mengen zurückgreifen:

```
{frozenset(X) for X in powerSet({1,23,42})}
```

Mengen von Tupeln

Weil Mengen weder Reihenfolge noch Dopplung kennen, sind $\{1,2\}$ und $\{2,1\}$ identisch und $\{1,1\}$ ist dasselbe wie $\{1\}$. Manchmal braucht man jedoch gerade diese Eigenschaften. Dafür gibt es sogenannte *geordnete Paare* und *Tupel*.

Definition

Sind a und b irgendwelche (mathematischen) Objekte (die nicht notwendig verschieden sein müssen), dann bezeichnet man deren Zusammenfassung (a,b) als **geordnetes Paar** von a und b. a und b nennt man die **Komponenten** des Paares.
Die definierende Eigenschaft von geordneten Paaren ist, dass (a,b) und (c,d) dann und nur dann identisch sind, wenn sowohl $a=c$ als auch $b=d$ gelten.

Nach dieser Definition sind $(1,2)$ und $(2,1)$ zwei verschiedene geordnete Paare und $(2,2)$ ist ein geordnetes Paar, dessen linke und rechte Komponente jeweils die Zahl 2 ist.

[10] In der kommentierten Zeile wird ein beliebiges Element von `M` ausgewählt. Die Konstruktion ist etwas umständlich, weil man nicht einfach so etwas wie `M[0]` schreiben kann.

⋆**Aufgabe 3.13**. Im letzten Kapitel konnte man lesen, dass man alle mathematischen Objekte aus Mengen zusammenbasteln kann. Dann müsste das auch für geordnete Paare gelten. Aber wie bringt man Reihenfolge und Dopplung in die Welt der Mengen, die so etwas nicht kennen? Eine Möglichkeit[11] ist, Paare durch

$$(a,b) = \{\{a\},\{a,b\}\}$$

zu definieren. Begründen Sie, warum die so konstruierten Paare wirklich das tun, was sie tun sollen.

Mithilfe von geordneten Paaren können wir das *Mengenprodukt* definieren:[12]

Definition

Das **kartesische Produkt** oder **Mengenprodukt** der Mengen A und B ist die Menge $A \times B = \{(a,b) : a \in A, b \in B\}$. Für $A \times A$ schreibt man auch A^2.

$A \times B$ ist also die Menge aller Paare, bei denen die erste Komponente ein Element von A und die zweite eines von B ist. Nebenbei habe ich in der Definition absichtlich ein Komma an der Stelle verwendet, wo eigentlich $\wedge$ stehen müsste. Das ist eine weit verbreitete Konvention, an die Sie sich gewöhnen sollten.

Mengenprodukte kann man sich ganz gut in Tabellenform vorstellen. Mit den Mengen $A = \{1,10,17,23\}$ und $B = \{10,23,42\}$ sieht $A \times B$ so aus:

	10	23	42
1	(1,10)	(1,23)	(1,42)
10	(10,10)	(10,23)	(10,42)
17	(17,10)	(17,23)	(17,42)
23	(23,10)	(23,23)	(23,42)

Man beachte, dass nach Definition des geordneten Paares alle Einträge in dieser Tabelle zwangsläufig verschieden sein müssen. Es kann keine Dopplungen geben. Deshalb können wir sofort folgern:

Lemma 3.2

Sind A und B endliche Mengen, dann gilt $|A \times B| = |A| \cdot |B|$.

Aber wie sieht es mit unendlichen Mengen aus? Wie kann man sich deren kartesisches Produkt vorstellen? Dazu zwei wichtige Beispiele.

Ein Produkt wie $\mathbb{N} \times \mathbb{N}$ ist auch nichts anderes als eine Tabelle, aber eine mit unendlich vielen Zeilen und Spalten, die jeweils mit den Zahlen 0, 1, 2 und so weiter durchnummeriert sind. Es geht nach rechts und nach unten jeweils – durch Auslassungspunkte angedeutet – immer weiter.

[11] Diese Idee stammt von dem polnischen Mathematiker Kazimierz Kuratowski. Es gibt jedoch noch diverse andere Möglichkeiten.

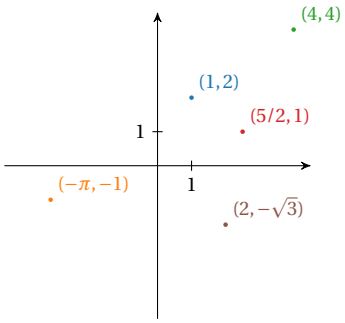
[12] Das Adjektiv *kartesisch* bezieht sich auf den latinisierten Namen des französischen Philosophen und Mathematikers René Descartes.

	0	1	2	3	…
0	(0,0)	(0,1)	(0,2)	(0,3)	…
1	(1,0)	(1,1)	(1,2)	(1,3)	…
2	(2,0)	(2,1)	(2,2)	(2,3)	…
3	(3,0)	(3,1)	(3,2)	(3,3)	…
⋮	⋮	⋮	⋮	⋮	⋱

Das Produkt $\mathbb{R}^2$ kennen Sie schon aus der Schule, obwohl Sie es bisher vielleicht nicht unter diesem Blickwinkel betrachtet haben. Man stellt sich dafür die Menge $\mathbb{R}$ der reellen Zahlen als Zahlengerade vor,[13] legt zwei solche Geraden senkrecht zueinander so auf die Ebene, dass sie sich an der Stelle treffen, wo jeweils die Null sitzt, und erhält dadurch eine eindeutige Zuordnung zwischen den Punkten der Ebene und deren „Adressen“ (Koordinaten), die geordnete Paare reeller Zahlen sind. Das ist ein sogenanntes *kartesisches Koordinatensystem*.

Zahlengerade

kartesisches Koordinatensystem



Stellen Sie sich nun vor, wo die Elemente der Menge $\mathbb{N} \times \mathbb{N}$ in diesem Koordinatensystem zu finden sind. Sie erhalten ein Gitter aus Punkten.

Aufgabe 3.14. Die Menge B aus Aufgabe 3.5 könnte man auch als

$$B = \{ mn : (m,n) \in A^2 \}$$

schreiben. Machen Sie sich klar, warum B weniger Elemente als A^2 hat.

Aufgabe 3.15. Sei $M = \{23, 42, \pi\}$. Wie sehen $\{0\} \times M$ und $\emptyset \times M$ aus?

Aufgabe 3.16. Ist das Mengenprodukt kommutativ?

Aufgabe 3.17. Können Sie eine Menge A angeben, für die $|A \times A| = 42$ gilt? Können Sie Mengen A und B angeben, für die $|A \times B| = 42$ gilt?

Aufgabe 3.18. Sei $A = [6]$, $B = \mathscr{P}(A)$, $C = B \times B$ und $D = C \setminus \{\emptyset\}$. Geben Sie $|D|$ an.

Aufgabe 3.19. Sei $A_q = \{ p \in \mathbb{P} : p < q \}$. Für welche Primzahl q gilt $|A_q \times A_q| = 100$?

[13] Diese Identifikation der Zahlengerade mit der aus einzelnen Punkten bestehenden Menge $\mathbb{R}$ ist philosophisch umstritten, in der Mathematik aber gängige Praxis. Zu den Hintergründen gibt es weitere Informationen im Video "Das Rätsel des Kontinuums".

Wir verallgemeinern nun die Definition des geordneten Paares auf mehr als zwei Komponenten:[14]

Definition

Sind a_1 bis a_n irgendwelche Objekte, dann bezeichnet man deren Zusammenfassung $(a_1,\dots,a_n)$ als das **n-Tupel** aus diesen Objekten und nennt die a_i die **Komponenten** des n-Tupels.
Die definierende Eigenschaft von n-Tupeln ist, dass $(a_1,\dots,a_n)$ und $(b_1,\dots,b_n)$ dann und nur dann identisch sind, wenn $a_i = b_i$ für alle i von 1 bis n gilt.

Geordnete Paare sind damit ein Spezialfall dieser Definition, nämlich 2-Tupel. Zu 3-Tupeln sagt man manchmal auch *Tripel* und es gibt auch Namen wie *Quadrupel* oder *Quintupel* für $n = 4$ oder $n = 5$, aber wir werden die wohl nicht brauchen. Der Vollständigkeit halber seien noch die relativ nutzlosen 1-Tupel der Form (23) erwähnt.

Tripel
Quadrupel
Quintupel

Aufgabe 3.20. Gibt es 0-Tupel?

⋆**Aufgabe 3.21**. Wie würden Sie 3-Tupel mithilfe von 2-Tupeln konstruieren, damit sie die gewünschten Eigenschaften haben?

Natürlich wird nun auch das Mengenprodukt verallgemeinert und wir können Lemma 3.2 entsprechend anpassen.

Definition

Das **kartesische Produkt** oder **Mengenprodukt** der Mengen A_1 bis A_n ist die Menge

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Für $A \times \cdots \times A$ mit n Faktoren schreibt man auch A^n.

Lemma 3.3

Für endliche Mengen gilt $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$.

⋆ Tupel im Computer

Auch in PYTHON gibt man Tupel mit Klammern und Kommata ein.[15] Lediglich bei 1-Tupeln muss man ein „überflüssiges“ Komma hinzufügen.

```
(42,23,1) == (1,23,42)   # vergleiche mit {42,23,1} == {1,23,42}
type((42,))              # vergleiche mit type((42))
```

[14] *Indizierte* Buchstaben wie a_1 sind nichts weiter als praktische Namen für Variablen. Noch im 19. Jahrhundert hätte man statt $a_1,\dots,a_n$ so etwas wie $A, B, C, \dots, K$ geschrieben und musste dann ergänzend hinzufügen, dass man eigentlich n verschiedene Namen meint – und nicht etwa zehn, weil K zufällig der zehnte Buchstabe des Alphabets ist.

[15] In vielerlei Hinsicht sind die Tupel von PYTHON das „gefrorene“ Pendant der Listen.

Das Mengenprodukt zweier Mengen könnte man so definieren:

```
product = lambda A,B: {(a,b) for a in A for b in B}
```

Die Standardbibliothek ITERTOOLS bietet allerdings eine flexiblere und effizientere Funktion `product`. Mehr dazu auf Seite 60.

4. Abzählende Kombinatorik

Auf den folgenden Seiten wird es in der einen oder anderen Form immer darum gehen, Dinge zu *zählen*. Vieles davon ist in der Schule bereits behandelt worden, wird hier jedoch noch einmal wiederholt und in der Fachsprache der Mengenlehre ausgedrückt.

Das Inklusions-Exklusions-Prinzip

Lemma 3.3 ist eine Aussage über die Mächtigkeit von Produkten von Mengen. Wie sieht es mit der Vereinigung aus? Es stellt sich heraus, dass es da leider keine so einfache Formel gibt.

> **Aufgabe 4.1**. Unter welcher Bedingung gilt $|A \cup B| = |A| + |B|$ für endliche Mengen A und B?

Auch ohne exakten mathematischen Beweis sollte hoffentlich nach einigem Nachdenken klar sein, dass die Behauptung aus Aufgabe 4.1 dann und nur dann gilt, wenn A und B kein gemeinsames Element haben, wenn also $A \cap B = \emptyset$ gilt. Man sagt dazu auch, dass A und B *disjunkt* sind.

disjunkt

Sind A und B nicht disjunkt, dann haben wir es mit einem Fall wie diesem zu tun, der aus didaktischen Gründen absichtlich redundant aufgeschrieben wurde:

$$\{1,2,3,4,5\} \cup \{4,5,6,7\} = \{1,2,3,4,4,5,5,6,7\} = \{1,2,3,4,5,6,7\}$$

Würden wir die Mächtigkeiten der beiden Mengen, die vereinigt werden, einfach addieren, so würden wir die Elemente, die in beiden Mengen vorkommen, „doppelt zählen“. (Im Beispiel wären das also die Zahlen 4 und 5.) Um das zu korrigieren, müssen wir die wieder abziehen:

Lemma 4.1 Für beliebige endliche Mengen A und B gilt $|A \cup B| = |A| + |B| - |A \cap B|$.

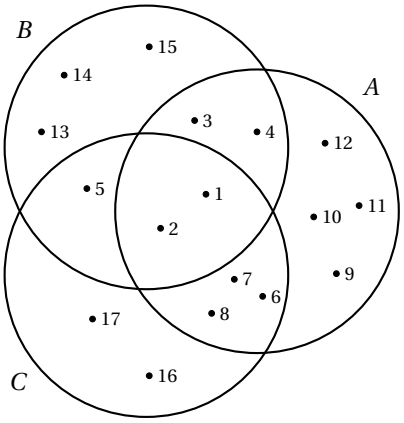
Beachten Sie, dass dieses Lemma den vorab behandelten Spezialfall zweier disjunkter Mengen umfasst, denn für die gilt $|A \cap B| = 0$.

> **Aufgabe 4.2**. Machen Sie sich mit einem Mengendiagramm klar, dass die Aussage von Lemma 4.1 korrekt ist.

Bei der Vereinigung zweier Mengen behält man eventuell auch ohne Mengendiagramm den Überblick. Spätestens bei drei Mengen ist es jedoch hilfreich, wenn

man grafisch an die Sache herangeht. Hier ein Beispiel für die folgenden drei Mengen:

$A = \{1,2,3,4,6,7,8,9,10,11,12\}$
$B = \{1,2,3,4,5,13,14,15\}$
$C = \{1,2,5,6,7,8,16,17\}$



Überzeugen Sie sich anhand der Skizze, dass die folgende Überlegung korrekt ist: Wenn wir die Elemente in jeder Menge separat zählen, dann werden die Elemente im Durchschnitt $A \cap B$ doppelt gezählt und müssen daher (wie in Lemma 4.1) abgezogen werden. Das gilt natürlich auch für $A \cap C$ und $B \cap C$. Die Elemente, die im gemeinsamen Schritt $A \cap B \cap C$ aller drei Mengen liegen, werden dann jedoch erst dreimal gezählt und dann dreimal abgezogen. Darum müssen sie zur Korrektur am Ende noch einmal gezählt werden. Wenn man das sauber aufschreibt, erhält man den folgenden Satz, den man das *Inklusions-Exklusions-Prinzip* (für drei Mengen) nennt.

Inklusions-Exklusions-Prinzip

Inklusions-Exklusions-Prinzip für drei Mengen **Satz 4.2**
Für beliebige endliche Mengen A, B und C gilt

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Aufgabe 4.3. In einem kleinen Dorf gibt es den Fußball-, den Kleingärtner- und den Kaninchenzüchterverein, die 98, 76 bzw. 55 Mitglieder haben. Bis auf den alten Sonderling Albert ist jeder Einwohner des Dorfes Mitglied in mindestens einem dieser Vereine. Sieben Mitglieder des Fußballvereins sind auch Kleingärtner, fünf Mitglieder des Kleingärtnervereins sind gleichzeitig Kaninchenzüchter und ebenfalls fünf Kaninchenzüchter spielen auch im Fußballverein mit. Die Bürgermeisterin und ihr Ehemann sind die einzigen Personen im Dorf, die Mitglieder in allen drei Vereinen sind. Wie viele Menschen leben in diesem Dorf?

Aufgabe 4.4. Wenn Sie Satz 4.2 verstanden haben, sollte es Ihnen nicht schwerfallen, eine entsprechende Formel für *vier* Mengen aufzuschreiben.

Aufgabe 4.5. A, B und C sind Mengen, die jeweils 30 Elemente haben. $A \cap B$ hat fünf Elemente, $A \cap C$ hat sechs Elemente. Ferner sind $A \cap B$ und $A \cap C$ disjunkt und es gilt $|A \cup B \cup C| = 70$. Wie viele Elemente hat $B \cap C$?

Aufgabe 4.6. Berechnen Sie mithilfe des Inklusions-Exklusions-Prinzips, wie viele natürliche Zahlen es gibt, die kleiner als 100 und weder durch 2 noch durch 3 noch durch 5 teilbar sind.

Weitere Aufgaben zum Inklusions-Exklusions-Prinzip finden Sie am Ende dieses Abschnitts ab Seite 58.

Permutationen

Da wir für die nächsten Schritte eine bestimmte Sorte Mengen öfter brauchen werden, definieren wir die Abkürzung[16]

$$[n] = \{k \in \mathbb{N} : 1 \leq k \leq n\} = \{1, \ldots, n\}.$$

$[n]$ für $n \in \mathbb{N}$.

Aufgabe 4.7. Verständnisfrage: Welche Mengen sind nach dieser Definition mit $[0]$ und $[\pi]$ gemeint?

Wir wollen uns nun überlegen, auf wie viele Arten man eine vorgegebene Menge X von Objekten sortieren kann.[17] Das kann man mit Tupeln ausdrücken. Ist X beispielsweise die Menge $\{7, 23, 42\}$, dann erhalten wir

$$\{(7,23,42), (7,42,23), (23,7,42), (23,42,7), (42,7,23), (42,23,7)\}$$

Permutationen als Menge aller möglichen Anordnungen von X, die wir die *Permutationen* von X nennen. Hat X allgemein n Elemente, dann sind die Permutationen von X also alle n-Tupel, deren Komponenten genau die Elemente von X sind. Die Menge P_X aller Permutationen von X sieht demnach so aus:

P_X

$$P_X = \{(a_1, \ldots, a_{|X|}) : \{a_1, \ldots, a_{|X|}\} = X\}$$

Aufgabe 4.8. Stellen Sie sicher, dass Sie die Definition von P_X verstanden haben, indem Sie sie für eine konkrete (kleine) Menge X durchgehen.

Aufgabe 4.9. Wie sieht $P_\emptyset$ aus?

[16] Obwohl es ähnlich aussieht, hat diese Schreibweise nichts mit den Intervallen zu tun, die Sie aus der Schule kennen. Da stehen zwischen den eckigen Klammern immer *zwei* Zahlen und es geht um Mengen von *reellen* Zahlen. Wir kommen später noch auf Intervalle zurück.

[17] Im Rest des Kapitels wird es immer um endliche Mengen gehen. Darum wird das im Folgenden nicht immer explizit erwähnt werden.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Uns interessiert die Mächtigkeit von P_X. Offenbar kommt es dabei nur auf die Mächtigkeit von X und nicht auf den Inhalt dieser Menge an.[18] Es reicht somit, wenn wir uns auf Mengen der Form $P_n = P_{[n]}$ konzentrieren,[19] deren Mächtigkeit wir mit $p_n = |P_n|$ bezeichnen. Einfache Beispiele sind

P_n
p_n

$$P_0 = \{()\},$$
$$P_1 = \{(1)\},$$
$$P_2 = \{(1,2),(2,1)\} \text{ und}$$
$$P_3 = \{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)\},$$

woraus wir $p_0 = 1$, $p_1 = 1$, $p_2 = 2$ und $p_3 = 6$ schließen können.

Aufgabe 4.10. Schreiben Sie alle Elemente von P_4 auf. Wie viele sind es?

Wenn Sie die letzte Aufgabe bearbeitet haben, dann sollten Sie auf $p_4 = 24$ gekommen sein. Für $n = 4$ ist das schon recht mühsam und für größere Zahlen erst recht. Einfacher ist es, systematisch vorzugehen. Wie stellt man beispielsweise sicher, dass man alle Elemente von P_3 erhält?[20] Jede der Zahlen 1 bis 3 kann vorne stehen. Und nachdem man sich für eine von denen entschieden hat, können die restlichen beiden dahinter irgendwie angeordnet werden. Dafür gibt es jeweils p_2 Möglichkeiten. Das macht insgesamt $3 \cdot p_2$ Permutationen von $[3]$. Bei P_4 läuft es ebenso. Jede der vier Zahlen 1 bis 4 kann vorne stehen und es bleiben jeweils drei Zahlen dahinter, die man auf p_3 verschiedene Arten anordnen kann, wodurch sich insgesamt $4 \cdot p_3$ Möglichkeiten ergeben. Verallgemeinert man das, so erhält man immer $(n+1) \cdot p_n$ Permutationen von $[n+1]$. Mithilfe der aus der Schule bekannten Fakultät $n! = 1 \cdot 2 \cdot \cdots \cdot n$ sieht das folgendermaßen aus:

Fakultät $n!$

$$p_0 = 1 = 0!,$$
$$p_1 = 1 \cdot p_0 = 1 \cdot 0! = 1!,$$
$$p_2 = 2 \cdot p_1 = 2 \cdot 1! = 2!,$$
$$p_3 = 3 \cdot p_2 = 3 \cdot 2! = 3! \text{ und so weiter.}$$

Wir haben damit, zumindest informell, diese Aussage bewiesen:

Anzahl der Permutationen **Satz 4.3**
Gilt $|X| = n$, so gibt es $n!$ Permutationen von X, d. h., P_X hat $n!$ Elemente.

Als Nächstes gehen wir einen Schritt weiter und schauen uns Anordnungen von Objekten an, die nicht unbedingt alle verschieden sind. Man kann dazu ebenfalls mit

[18] Mit anderen Worten: Es gibt genauso viele Permutationen von $\{0,-4,\pi\}$ wie es Permutationen von $\{1,2,3\}$ gibt.

[19] Eine typische „Abkürzung“, mit der man nicht viel Schreibarbeit spart, die aber die Ausdrucksweise etwas prägnanter macht.

[20] Speziell für diesen Abschnitt werden Sie in den am Rande verlinkten Videos teilweise aufwendigere Grafiken als hier im Skript finden, die hoffentlich helfen, falls etwas unklar ist.

Tupeln arbeiten und sich beispielsweise fragen, auf wie viele Arten man $(1,1,1,2,2)$ umsortieren kann. Mit etwas Rumprobieren kommt man auf zehn Möglichkeiten:

$$(1,1,1,2,2),(1,1,2,1,2),(1,1,2,2,1),(1,2,1,1,2),(1,2,1,2,1),$$
$$(1,2,2,1,1),(2,1,1,1,2),(2,1,1,2,1),(2,1,2,1,1),(2,2,1,1,1)$$

Wie kann man das systematisieren, um auf eine Formel zu kommen? Wären alle fünf Komponenten verschieden gewesen, dann hätte es 5!, also 120 Permutationen gegeben. Wir können das „simulieren“, in dem wir die zunächst die Einsen durch Farben künstlich unterscheidbar machen. Dann erhalten wir z. B. die sechs Permutationen

$$(1,1,1,2,2),(1,1,1,2,2),(1,1,1,2,2),$$
$$(1,1,1,2,2),(1,1,1,2,2),(1,1,1,2,2),$$

die ohne Färbung für uns alle gleich aussehen und zu der einen $(1,1,1,2,2)$ „verschmelzen“. Warum sind es sechs? Weil es $3! = 6$ Permutationen der drei unterschiedlich gefärbten Einsen gibt. Für jeden dieser sechs Fälle gibt es aber jeweils noch $2! = 2$ Varianten, wenn wir auch noch die Zweien färben. Aus $(1,1,1,2,2)$ werden dann $(1,1,1,2,2)$ und $(1,1,1,2,2)$, so dass wir auf diese Art insgesamt $3! \cdot 2!$ „bunte Versionen“ des Tupels $(1,1,1,2,2)$ erhalten. Rechnet man nun „rückwärts“, so wird klar, dass sich die Zahl zehn von oben dadurch ergibt, dass wir die 120 „theoretisch möglichen“ Permutationen durch $3! \cdot 2! = 12$ dividieren müssen.

Permutationen mit Wiederholungen

Man spricht in so einem Fall von *Permutationen mit Wiederholungen*. Wie schreiben wir das korrekt und konzis auf? Da die möglichen Dopplungen eine zentrale Rolle spielen, müssen wir mit Tupeln statt mit Mengen arbeiten. Die Menge der möglichen Umordnungen eines Tupels $(b_1,\dots,b_n)$ kann man so aufschreiben:

$P_{(b_1,\dots,b_n)}$

$$P_{(b_1,\dots,b_n)} = \{(b_{a_1},\dots,b_{a_n}) : (a_1,\dots,a_n) \in P_n\}$$

Aufgabe 4.11. Können Sie mit Ihren eigenen Worten beschreiben, wie diese mengentheoretische Definition „funktioniert“?

Die obigen Überlegungen zum Umsortieren von $(1,1,1,2,2)$ haben Sie hoffentlich überzeugt, dass der folgenden Satz wahr ist.

Satz 4.4

Anzahl der Permutationen mit Wiederholungen
Sei $(b_1,\dots,b_n)$ ein Tupel mit r *verschiedenen* Komponenten, also $|\{b_1,\dots,b_n\}| = r$. Nennt man diese unterschiedlichen Objekte a_1 bis a_r, so soll a_i k_i-mal im Tupel auftreten, d. h. $\{b_1,\dots,b_n\} = \{a_1,\dots,a_r\}$ und $|\{j \in [n] : b_j = a_i\}| = k_i$ für $i = 1,\dots,r$. Dann gilt

$$|P_{(b_1,\dots,b_n)}| = \frac{n!}{k_1!\,k_2!\cdots k_r!}.$$

Leider lässt sich dieser Satz nicht wesentlich einfacher formulieren. Haben Sie seine Aussage verstanden?

Aufgabe 4.12. „Übersetzen“ Sie das konkrete Beispiel $(1,1,1,2,2)$ in die allgemeine Formulierung von Satz 4.4. Welche Werte haben n, r, b_2 und so weiter?

Aufgabe 4.13. Wie viele Permutationen hat $(2,3,2,3,7,2,2)$?

Aufgabe 4.14. Satz 4.4 ist eine *Verallgemeinerung* von Satz 4.3 in dem Sinne, dass man Satz 4.3 eigentlich vergessen kann, wenn man Satz 4.4 kennt. Wie ist das gemeint?

Der Ausdruck, der in Satz 4.4 vorkommt, hat in der Mathematik einen Namen. Wir werden ihn nicht verwenden, aber der Vollständigkeit halber notieren wir ihn.

Definition

Sind k_1 bis k_r und n natürliche Zahlen mit $k_1 + \cdots + k_r = n$, dann nennt man die Zahl

$$\binom{n}{k_1,\ldots,k_r} = \frac{n!}{k_1!\cdots k_r!}$$

den **Multinomialkoeffizienten** dieser Zahlen.

In gewissem Sinne ist die Zahl n in dieser Definition überflüssig, weil sie zwangsläufig die Summe der Zahlen k_1 bis k_r sein muss. Für den fehlerfreien Umgang mit solchen Berechnungen ist diese Beobachtung allerdings ganz hilfreich: Wenn Sie Permutationen mit Wiederholungen ausrechnen, dann sollten Sie vorsichtshalber auch die Komponenten in die Berechnung einbeziehen, die nur einmal auftreten, obwohl der Term 1! eigentlich nichts ändert. In der Lösung von Aufgabe 4.13 sieht man beispielsweise, dass die Zahlen 4, 2 und 1, die im Nenner vor den Ausrufezeichen stehen, in der Summe die Zahl $n = 7$ ergeben.

Variationen

Bei den Permutationen ging es darum, dass wir eine feste Sequenz von Objekten hatten und uns fragten, auf wie viele Arten wir sie umsortieren können. Jetzt erweitern wir die Fragestellung etwas und lassen zu, dass wir die Objekte, deren mögliche Sortierungen uns interessieren, erst aus einem gewissen Vorrat auswählen. Das ist zwar eine allgemeinere Frage, aber die Antwort wird dadurch leichter werden.

Fangen wir mit einer Menge X der Mächtigkeit n an und fragen uns, wie viele k-Tupel es geben kann, bei denen die Komponenten Elemente von X und alle *verschieden* sind. (Offensichtlich ergibt diese Frage nur Sinn, wenn $k \leq n$ gilt.) Uns interessiert die Mächtigkeit der Menge

$$V_{X,k} = \{(x_1,\ldots,x_k) \in X^k : |\{x_1,\ldots,x_k\}| = k\} \qquad V_{X,k}$$

Variationen

und man spricht in diesem Fall von *Variationen*.[21]

Auch hier reicht hoffentlich ein Beispiel, um Sie davon überzeugen, dass es ein allgemeines Prinzip gibt, das die Frage beantwortet. Wie kann man systematisch die Elemente von $V_{[7],3}$ erzeugen? Ein Element dieser Menge ist ein 3-Tupel und hat drei Komponenten. Für die erste Komponente kann man ein beliebiges Element von [7] auswählen und dafür gibt es sieben Möglichkeiten. *Nachdem* man diese Wahl getroffen hat, verbleiben für die zweite Komponente jedoch nur noch sechs Alternativen, weil die Komponenten alle verschieden sein sollen. Und für die dritte Komponente hat man entsprechend nur noch fünf Möglichkeiten, weil die beiden vorher gewählten Elemente von X nicht erneut auftauchen dürfen. Anders ausgedrückt enthält $V_{[7],3}$ fünf Tripel der Form $(2,6,n)$, denn n muss eine der Zahlen 1, 3, 4, 5 oder 7 sein. Und es gibt in dieser Menge $6\cdot 5 = 30$ Tupel der Form $(2,m,n)$. Insgesamt gibt es $7\cdot 6\cdot 5 = 210$ Variationen dieser Art. Verallgemeinert wird daraus:

Satz 4.5

Anzahl der Variationen
Unter der Voraussetzung $|X| = n \geq k$ hat die Menge $V_{X,k}$ die Mächtigkeit

$$n\cdot(n-1)\cdot(n-2)\cdot\dots\cdot(n-k+1) = \frac{n!}{(n-k)!}.$$

Zu der sich ergebenden Formel sind noch ein paar Anmerkungen angebracht. Erstens sollten Sie sich klarmachen, dass dort wirklich „plus eins“ stehen muss. Wenn man das vergisst, dann ist das ein Beispiel für den auch beim Programmieren sehr „beliebten“ *Off-by-one-Error*. (Zählen Sie nach: Es müssen k Faktoren sein.) Zweitens ist der Ausdruck rechts mit den beiden Fakultäten kürzer und für theoretische Überlegungen evtl. besser geeignet, aber für das Rechnen von Hand sollte man den linken Term verwenden. Drittens wird $n!/(n-k)!$ in manchen Büchern als $n^{\underline{k}}$ oder $(n)_k$ geschrieben und als *fallende Faktorielle* bezeichnet. Und viertens verbirgt sich die entsprechende Funktion auf Taschenrechnern häufig hinter der Taste $\boxed{n\mathrm{P}r}$, wobei der Buchstabe P für das Wort *permutation* steht, denn Variationen nennt man im Englischen auch *k-permutations*.

fallende Faktorielle
$n^{\underline{k}}$ $(n)_k$

Aufgabe 4.15. Überzeugen Sie sich anhand von Beispielen, dass die beiden Ausdrücke in Satz 4.5 tatsächlich denselben Wert beschreiben. (Nicht einfach alles glauben!)

Aufgabe 4.16. Wie viele Elemente hat $V_{[8],5}$?

Aufgabe 4.17. Wie viele dreistellige natürliche Zahlen gibt es, bei denen alle Ziffern verschieden sind? (Es geht natürlich um die Darstellung im Dezimalsystem, also um Zahlen wie 123 oder 813. Zahlen wie 42 oder 7 sind keine dreistelligen Zahlen.)

Variationen mit Wiederholungen

Der Vollständigkeit halber erwähnen wir auch noch *Variationen mit Wiederholungen*. Da geht es darum, wie viele k-Tupel man bilden kann, wenn die Komponenten

[21] In der Stochastik nennt man Variationen auch *Stichproben* oder in diesem Fall präziser *Stichproben ohne Zurücklegen unter Berücksichtigung der Reihenfolge*. Stellen Sie sich ein Experiment vor, bei dem nacheinander k „Dinge“ aus der Menge X entnommen und notiert werden. Das Versuchsprotokoll ist dann ein Element von $V_{X,k}$.

beliebige Elemente einer vorgegebenen Menge X sein dürfen, also darum, welche Mächtigkeit X^k hat. Diese Frage haben wir im Prinzip schon beantwortet und können daher einfach die Antwort festhalten:

Anzahl der Variationen mit Wiederholungen **Satz 4.6**
Für alle endlichen Mengen X gilt $|X^k| = |X|^k$.

Aufgabe 4.18. Auf welcher Aussage aus diesem Kapitel basiert Satz 4.6?

Kombinationen

Bei den Permutationen hatten wir ein vorgegebenes Tupel und fragten uns, auf wie viele Arten man es umsortieren kann. Bei Variationen ging es auch um Tupel, die allerdings zunächst „bestückt“ wurden, d. h., wir konnten sozusagen auswählen. In beiden Fällen war die Reihenfolge relevant. Nun schauen wir uns den Fall an, dass wir zwar auswählen, uns die Reihenfolge jedoch nicht interessiert. Das bedeutet technisch einen Wechsel von Tupeln zu Mengen: Wie viele k-elementige Teilmengen hat eine Menge X? (X muss natürlich mindestens k Elemente haben, damit die Frage einen Sinn ergibt.) In der Kombinatorik spricht man von *Kombinationen*.[22] Kombinationen

Zum Glück haben wir in den vorherigen Abschnitten die wesentliche Vorarbeit bereits geleistet. Nehmen wir als Beispiel $X = [7]$ und $k = 3$. Eine 3-elementige Teilmenge von X ist $A = \{2,5,7\}$. Wir können A durch das Tripel $(2,5,7)$ repräsentieren, aber z. B. auch durch $(5,2,7)$. Wie viele solche Tripel gibt es, deren Komponenten genau die Elemente von A sind? Die Frage beantwortet Satz 4.3: Es sind 3!. Und wie viele Tripel gibt es, die 3-elementigen Teilmengen von X entsprechen? Diese Antwort liefert Satz 4.5: Es sind $7!/(7-3)!$. Wir müssen nur noch diese Zahl durch 3! teilen und das war's. Bevor wir daraus eine allgemeine Aussage machen, definieren wir noch ein paar praktische Begriffe.

Für natürliche Zahlen k und Mengen X verwenden wir die Abkürzungen **Definition**

$$\begin{aligned}\mathscr{P}_k(X) &= \{Y \in \mathscr{P}(X) : |Y| = k\},\\ \mathscr{P}_{<k}(X) &= \{Y \in \mathscr{P}(X) : |Y| < k\} \text{ und}\\ \mathscr{P}_{\leq k}(X) &= \{Y \in \mathscr{P}(X) : |Y| \leq k\}.\end{aligned}$$

Das hier sollten Sie aus der Schule noch kennen:

Für $n, k \in \mathbb{N}$ mit $n \geq k$ definieren wir den **Binomialkoeffizienten** durch **Definition**

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

[22] Und in der Stochastik nennt man so etwas eine *ungeordnete Stichprobe*.

Man liest das als „n über k“. Im Englischen sagt man „*n choose k*“ und deswegen ist $\boxed{nCr}$ oft die Taschenrechnertaste für den Binomialkoeffizienten.

Wir können die Konsequenz der obigen Vorüberlegungen nun kurz und knapp als Satz formulieren:[23]

Satz 4.7

Anzahl der Kombinationen

Mit $|X| = n \geq k$ gilt $|\mathscr{P}_k(X)| = \binom{n}{k}$.

Wie Sie sich vielleicht schon gedacht haben, fehlen noch Kombinationen *mit Wiederholungen*. Dazu überlegen wir uns zunächst eine andere Methode, Kombinationen darzustellen, die auch für die Informatik relevant ist:

Jede Teilmenge A von $[n]$ können wir als n-Tupel repräsentieren, dessen Komponenten nur Nullen und Einsen sind, wenn wir es so interpretieren, dass eine Eins als i-te Komponente für $i \in A$ steht, während eine Null an dieser Stelle $i \notin A$ bedeutet. In diesem Sinn steht $(0,1,0,0,1,0,1)$ für die Teilmenge $\{2,5,7\}$ von $[7]$. Das ergibt insbesondere:

Korollar 4.8

Mit $|X| = n \geq k$ gilt $|\{(x_1,\dots,x_n) \in \{0,1\}^n : x_1 + \cdots + x_n = k\}| = \binom{n}{k}$.

Aufgabe 4.19. Mithilfe von Satz 4.6 erhalten wir durch diese Darstellung einen alternativen Beweis für Satz 3.1. Nämlich wie?

Aufgabe 4.20. Was kommt heraus, wenn man die Summe

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}$$

berechnet? (Hinweis: Satz 4.7.)

Aufgabe 4.21. Wie viele Elemente hat die Menge

$$\{(x_1,\dots,x_k) \in X^k : x_1 < x_2 < \cdots < x_k\},$$

wenn $|X| = n \geq k$ gilt?

Kombinationen mit Wiederholungen

Nun aber zu den *Kombinationen mit Wiederholungen*. Bei denen soll es darum gehen, Elemente aus einer Menge auszuwählen, ohne auf die Reihenfolge zu achten. Der Zusatz *mit Wiederholungen* bedeutet, dass wir Elemente auch mehrfach entnehmen dürfen. Wir erweitern dafür die „0-1-Schreibweise“ aus Korollar 4.8 und betrachten Tupel, deren Komponenten beliebige natürliche Zahlen sein können. Eine Zahl r als i-te Komponente soll dann bedeuten, dass das Element i r-mal entnommen wurde. Wir wollen wissen, welche Mächtigkeit die Menge

$C_{n,k}$

$$C_{n,k} = \{(x_1,\dots,x_n) \in \mathbb{N}^n : x_1 + \cdots + x_n = k\}$$

[23] Wegen dieses Satzes ist mancherorts auch die Schreibweise $\binom{X}{k}$ für $\mathscr{P}_k(X)$ üblich.

hat; wie viele Möglichkeiten es also gibt, k-mal ein Element von $[n]$ auszuwählen, wenn die Reihenfolge irrelevant ist. Da wir die Elemente nach dem Auswählen wieder „zurücklegen“, kann k dabei ruhig größer als n sein.

Während die bisherigen kombinatorischen Formeln vergleichsweise naheliegend waren, verwenden wir für die Herleitung in diesem Fall einen cleveren Trick, der zwar einfach zu verstehen ist, auf den man aber erst einmal kommen muss. Er ist gleichzeitig ein gutes Beispiel dafür, dass man in der Mathematik oft anstrebt, ein neues Problem auf ein bereits bekanntes zurückzuführen, um sich Arbeit zu ersparen.[24]

Nehmen wir als Beispiel $n = 4$ und $k = 6$. Einige Elemente von $C_{4,6}$ sehen so aus:

$(x_1, \ldots, x_4)$	x_1	x_2	x_3	x_4
$(1,1,4,0)$	1	1	4	0
$(2,0,3,1)$	2	0	3	1
$(1,1,2,2)$	1	1	2	2
$(0,0,1,5)$	0	0	1	5

Der besagte Trick ist nun, die Tabelle als „Strichliste“ aufzuschreiben. Zahlen stellen wir durch eine entsprechende Anzahl von Kreuzen dar (also × × × statt 3), die Tabellenspalten trennen wir durch senkrechte Striche:

×	|	×	|	×	×	×	×	|
×	×	|	|	×	×	×	|	×
×	|	×	|	×	×	|	×	×
|	|	×	|	×	×	×	×	×

Nach kurzem Nachdenken sollte klar sein, dass man zu jedem Eintrag aus $C_{4,6}$ so einen „Code“ erstellen kann und dass sich aus dem das ursprüngliche Tupel eindeutig wieder rekonstruieren lässt. Die Anzahl der Kreuze ist dabei immer 6 und man kommt immer mit 3 Strichen aus (einem weniger als der Mächtigkeit 4 der Grundmenge), weil die Striche zwischen den Spalten ausreichen. Um die Mächtigkeit von $C_{4,6}$ zu bestimmen, können wir somit alternativ herausfinden, wie viele „Kreuz-Strich-Zeilen“ sich nach diesen Regeln bilden lassen. Das wissen wir aber schon, denn dafür können wir einfach Satz 4.4 verwenden. Die Antwort ist $9!/(3!6!) = 84$. Verallgemeinert sieht das so aus:

Anzahl der Kombinationen mit Wiederholungen **Satz 4.9**

Die Menge $C_{n,k}$ hat $\dfrac{(n-1+k)!}{(n-1)!\,k!} = \binom{n+k-1}{k}$ Elemente.

Man kann eine Auswahl wie $(2,0,3,1)$ aus der Menge $\{1,2,3,4\}$ übrigens auch als eine mengenähnliche Struktur interpretieren, in der Elemente mehr als einmal vorkommen können. Dafür sind Schreibweisen wie $\{|1,1,3,3,3,4|\}$ oder $\{1,1,3,3,3,4\}_b$

[24] Das haben wir bereits beim Abzählen der Kombinationen ohne Wiederholungen gemacht, indem wir es auf „Variationen geteilt durch Permutationen“ zurückführten.

Multimenge

gebräuchlich[25] und man spricht dann von *Multimengen*. Für die in Satz 4.9 berechnete Anzahl der k-elementigen „Multiteilmengen“ einer n-elementigen Menge schreibt man in diesem Zusammenhang auch $\left(\binom{n}{k}\right)$. Für die Informatik spielen Multimengen als Datenstrukturen eine Rolle, aber wir werden das nicht weiter verfolgen.

Resümee

Den Begriff *Kombinatorik* prägte Gottfried Wilhelm Leibniz 1666, als er sich – in dem Büchlein *Dissertatio de arte combinatoria* – mit Permutationen beschäftigte. Was wir bisher gesehen haben, sind nur die Grundlagen der sogenannten *abzählenden Kombinatorik*. Dieser „klassische“ Teil der Kombinatorik war im Wesentlichen bereits im 17. Jahrhundert bekannt und wurde ursprünglich für die Untersuchung der Wahrscheinlichkeiten bei Glücksspielen entwickelt. Einer der Pioniere in diesem Bereich war, bereits vor Leibniz, der Franzose Blaise Pascal.

Auch über 300 Jahre später spielt die Kombinatorik als Teildisziplin der Mathematik allerdings immer noch eine gewissen Außenseiterrolle gegenüber den dominanten Bereichen Algebra, Geometrie und Analysis. Gleichzeitig hat ihre Bedeutung für die Anwendung – z. B. in der Informatik – in den letzten Jahrzehnten immer weiter zugenommen. Für uns soll es aber fürs Erste reichen.

Die folgende Tabelle kann vielleicht als informelle Gedächtnisstütze für die letzten drei Abschnitte dienen.

	ohne Wdh.	mit Wdh.
Permutationen	$(1,2,3,4,5) \to (3,2,4,5,1)$	$(1,2,2,3,3) \to (3,2,2,1,3)$
Variationen	$\{1,2,3,4,5\} \to (3,2,5)$	$\{1,2,3,4\} \to (3,2,2,4,3)$
Kombinationen	$\{1,2,3,4,5\} \to \{2,3,5\}$	$\{1,2,3,4\} \to \{\vert 1,1,2,3,3,3 \vert\}$

Es ist allerdings eine Sache, die abstrakten kombinatorischen Überlegungen aus den letzten Abschnitten zu verstehen. Eine ganz andere ist die Fähigkeit, diese Überlegungen auf konkrete Probleme anzuwenden. Dazu muss man realisieren, wann und in welcher Form die gerade analysierten Tätigkeiten des Auswählens und Sortierens in Anwendungsfragen auftauchen und wie sie sich in die Sprache der Mathematik übersetzen lassen. Die folgenden Aufgaben sollen Ihnen helfen, das zu üben.

Aufgabe 4.22. Kombinatorische Auswahl- und Anordnungsverfahren werden insbesondere in der Stochastik gerne auch mit einem sogenannten *Urnenmodell* erklärt. In einer Urne befinden sich Kugeln, die mit Zahlen beschriftet sind. Nun wird eines der folgenden „Experimente“ durchgeführt, bei denen die Kugeln jeweils „blind“ der Urne entnommen werden.

(i) Die Urne enthält für jede Zahl von 1 bis n genau eine Kugel. Es werden gleichzeitig k Kugeln entnommen und die Zahlen der entnommenen Kugeln werden notiert.

[25] Der Buchstabe *b* steht für das englische Wort *bag*.

(ii) Die Urne enthält für jede Zahl von 1 bis n (mindestens) k Kugeln. Es werden nacheinander k Kugeln entnommen und die abgelesenen Zahlen werden in der Reihenfolge der Entnahme notiert.

(iii) Die Urne enthält für jede Zahl von 1 bis n genau eine Kugel. Es werden nacheinander k Kugeln entnommen und die abgelesenen Zahlen werden in der Reihenfolge der Entnahme notiert.

(iv) Die Urne enthält n Kugeln mit natürlichen Zahlen. Es können jedoch evtl. manche Zahlen mehrfach vorkommen. Es werden nacheinander alle Kugeln entnommen und die abgelesenen Zahlen werden in der Reihenfolge der Entnahme notiert.

(v) Die Urne enthält für jede Zahl von 1 bis n genau eine Kugel. Es werden nacheinander alle Kugeln entnommen und die abgelesenen Zahlen werden in der Reihenfolge der Entnahme notiert.

(vi) Die Urne enthält für jede Zahl von 1 bis n (mindestens) k Kugeln. Es werden gleichzeitig k Kugeln entnommen und die Zahlen der entnommenen Kugeln werden zusammen mit ihrer Häufigkeit notiert.

Welches kombinatorische Verfahren wird jeweils beschrieben und wie berechnet man in den einzelnen Fällen die Anzahl der möglichen Ausgänge des Experiments?

Aufgabe 4.23. Beim Pokern (*Five Card Draw*) erhält jeder Spieler am Anfang fünf von insgesamt 52 Karten. Wie viele Möglichkeiten für so ein Blatt gibt es?

Aufgabe 4.24. Beim Spiel *Mastermind* legt ein Spieler zu Beginn einen vierstelligen Farbcode fest, bei dem an jeder Position (Stelle) eine von sechs Farben stehen kann und Farben auch mehrfach vorkommen können. Wie viele Möglichkeiten für diesen Farbcode gibt es?

Aufgabe 4.25. An der Fakultät Mathematik der Universität Freedonia gibt es zwölf Professoren. Besonders beliebt sind die Einzelbüros mit Fenstern nach Süden im Elfenbeinturm. Davon gibt es jedoch nur fünf Stück. Wie viele Möglichkeiten hat die Dekanin, diese fünf (übrigens sehr unterschiedlichen) Büros unter den zwölf Mathematikern zu verteilen?

Aufgabe 4.26. Der feindliche Nachrichtendienst hat das Passwort der Geheimagentin 042 fast geknackt. Mit cleveren statistischen Methoden hat man herausgefunden, dass es aus elf Großbuchstaben besteht und dass exakt dieselben Zeichen wie in dem Wort *MISSISSIPPI* verwendet werden. Dummerweise hat man keinerlei Anhaltspunkte dafür, in welcher Reihenfolge die Buchstaben eingegeben werden müssen. Wie viele Möglichkeiten müsste man durchprobieren, wenn man genügend Zeit hätte?

Aufgabe 4.27. Sie haben eine Muffin-Form, mit der Sie zwölf Muffins auf einmal backen können. Sie haben drei Sorten Teig angerührt – für Blaubeermuffins, für Kokosmuffins und für Schokomuffins. Die Teigmengen würden jeweils reichen, um alle zwölf Mulden zu füllen. Wie viele verschiedene Möglichkeiten gibt es, die Form zu befüllen, wenn es Ihnen nur auf die Anzahl der Blaubeer-, Kokos- und Schokomuffins ankommt?

Aufgabe 4.28. Beim *Gummibärchen-Orakel* werden aus einer vollen Tüte mit Gummibärchen zufällig fünf Bärchen entnommen. Für die Aussage des Orakels ist nur die Verteilung der Farben (z.B. zweimal rot, zweimal grün, einmal weiß), nicht jedoch die

Reihenfolge relevant. Wie viele verschiedene Ergebnisse sind möglich, wenn es fünf Geschmacksrichtungen (also Farben) gibt?

Aufgabe 4.29. Der Kegelclub „Meinungsvielfalt“ plant einen Ausflug nach Hamburg. Dabei sollen auf jeden Fall die folgenden fünf Sehenswürdigkeiten besichtigt werden: Der alte Elbtunnel, *Planten un Blomen*, die Reeperbahn, die Elbphilharmonie sowie der Kunst- und Mediencampus Finkenau. Leider besteht keine Einigkeit darüber, in welcher Reihenfolge diese Orte besucht werden sollen. Jedes Clubmitglied darf daher drei Vorschläge für die Tour machen. Bei der Auszählung der Stimmen wird dann allerdings festgestellt, dass alle Mitglieder tatsächlich drei Vorschläge abgegeben haben und dass alle abgegebenen Vorschläge paarweise verschieden[26] sind. Wie viele Mitglieder kann der Club höchstens haben?

Aufgabe 4.30. Die Post in Taka-Tuka-Land benutzt zur Kennzeichnung der Postleitzahlen auf Briefen und Paketen Strichcodes, die immer aus genau sieben schwarzen Strichen bestehen, die durch sechs identisch breite weiße Lücken getrennt sind. Jeder der sieben Striche kann entweder breit oder schmal sein. Zwei mögliche Strichcodes sehen also so aus:

Wie viele verschiedene Strichcodes dieser Art gibt es?

Sie haben alle Fragen korrekt beantwortet? Herzlichen Glückwunsch! Vergessen Sie aber nicht, dass es immer auch Fälle wie Aufgabe 4.17 geben kann, bei denen nicht einfach eine der sechs Formeln passt. Durch entsprechende Nebenbedingungen kann jede Fragestellung noch etwas komplizierter werden. Dafür folgen nun noch weitere Beispiele.

Aufgabe 4.31. Um die Arbeit der Lesegeräte aus Aufgabe 4.30 zu vereinfachen, werden zwei Strichcodes als identisch angesehen, wenn sie sich nur durch die Lesereihenfolge (von rechts nach links oder von links nach rechts) unterscheiden.[27] Die beiden Strichcodes in dem Bild von oben codieren also z. B. dieselbe Postleitzahl. Wie viele verschiedene Postleitzahlen kann es in Taka-Tuka-Land höchstens geben?

Aufgabe 4.32. Wie ändert sich das Ergebnis von Aufgabe 4.27, wenn der Schokomuffinteig nur für maximal sechs Mulden reicht?

Aufgabe 4.33. Was wäre, wenn man bei Aufgabe 4.24 fordern würde, dass für den Farbcode höchstens drei der sechs Farben verwendet werden dürfen?

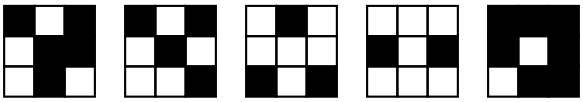
paarweise

[26] Das Adverb *paarweise* ist typischer „Mathematikerschnack“. An dieser Stelle ist es so gemeint, dass immer dann, wenn man sich zwei Vorschläge (also ein *Paar*) herausgreift, sie verschieden sind. Umgangssprachlich würde man einfach sagen, dass die Vorschläge alle unterschiedlich sind.

[27] Mit anderen Worten: Zwei Strichcodes gelten als gleich, wenn sich der eine aus dem anderen durch Drehung um 180 Grad ergibt. Alternativ können Sie sich das auch als Spiegelung am mittleren schwarzen Strich vorstellen.

Aufgabe 4.34. Bei einer Matheklausur gab es eine Aufgabe mit einer Multiple-Choice-Frage und sechs Antwortkästchen. Beim Korrigieren der Klausur stellt der Professor fest, dass tatsächlich alle Teilnehmer unterschiedliche Antworten abgegeben haben. Allerdings gab es keinen, der alle sechs Kästchen angekreuzt hat, und auch keinen, der gar kein Kästchen angekreuzt hat. Außerdem hat leider auch niemand die richtige Lösung (die ersten fünf Kästchen) abgegeben. Wie viele Personen können maximal an der Klausur teilgenommen haben?

Aufgabe 4.35. Die folgende Abbildung zeigt fünf Beispiele für 3×3-Matrizen, die mit schwarzen und weißen Pixeln gefärbt sind. Wie viele verschiedene Muster gibt es, bei denen sowohl *mindestens* zwei Pixel schwarz als auch *mindestens* zwei Pixel weiß sind?



Aufgabe 4.36. Wie viele verschiedene Zeichenketten der Länge 4, die *mindestens* eine der folgenden Bedingungen erfüllen, kann man aus den 8 Buchstaben `A` bis `H` konstruieren?

(i) Der erste Buchstabe ist `A`.
(ii) Der zweite Buchstabe ist `B`.
(iii) Der dritte Buchstabe ist `C`.

Erlaubt sind also z.B. die Zeichenketten `ADBH` oder `DBDH`, aber auch `AHCC` oder `ABCA`.

Aufgabe 4.37. Stellen Sie sich selbst Aufgaben nach dem Muster von Aufgabe 4.36, indem Sie beispielsweise die dritte Bedingung abändern und stattdessen eine der folgenden Eigenschaften fordern:

- Die ersten beiden Buchstaben sind unterschiedlich.
- Die letzten beiden Buchstaben sind gleich.
- Alle vier Buchstaben sind verschieden.

⋆ Kombinatorik im Computer

PYTHON kann selbstverständlich die Fakultät berechnen:

```
from math import factorial
factorial(6)
```

Den Multinomialkoeffizienten kann man in einer Zeile programmieren:

```
from math import prod
multi = lambda L: factorial(sum(L))//prod(map(factorial, L))
multi([4,2,1])
```

Beachten Sie, dass die Summe, die hinter der Definition des Multinomialkoeffizienten als „überflüssig“ bezeichnet wurde, hier nicht eingegeben wird.

Wenn Sie programmieren können, dann ist es eine hervorragende Übung, Funktionen zu schreiben, die zu einer vorgegebenen Menge alle Permutationen, Variationen oder Kombinationen (mit oder ohne Wiederholungen) ausgeben können. Dabei bietet sich oft die Technik der Rekursion an. Exemplarische Lösungen finden Sie beispielsweise in Kapitel 17 des bereits erwähnten Buchs *Konkrete Mathematik (nicht nur) für Informatiker*. Und in Kapitel 18 wird gezeigt, wie man diese durch die Verwendung von Generatoren effizienter macht.

Aber Sie *müssen* das natürlich nicht selbst schreiben, sondern können auch die Funktionen verwenden, die bereits im „Lieferumfang“ enthalten sind:

```
from itertools import product, permutations, combinations, \
                      combinations_with_replacement
permutations((1,2,3))        # Permutationen
permutations((1,2,2,2))      # Permutationen mit Wiederholungen
permutations((1,2,3),2)      # Variationen
product((1,2,3,4),repeat=2)  # Variationen mit Wiederholungen
combinations((1,2,3,4),2)    # Kombinationen
combinations_with_replacement((1,2,3,4),2) # Kombinationen mit W.
```

Diese Funktionen geben alle Iteratoren zurück. Um etwas zu sehen, kann man so etwas wie `set(permutations((1,2,3)))` eingeben. Man muss auch nicht unbedingt Tupel verwenden. `combinations({1,2,3,4},2)` würde z. B. auch funktionieren.

Für Multimengen gibt es in PYTHON die Klasse `Counter`:

```
from collections import Counter
c = Counter(x1=2, x2=0, x3=3, x4=1)
sorted(c.elements())
```

Manche Menschen verstehen übrigens nicht, wieso $0!$ den Wert 1 hat (obwohl man z. B. bei der Formel für die Anzahl der Permutationen sieht, dass das gut passt). Vielleicht überzeugt Sie die folgende kleine Funktion, die die Fakultät korrekt berechnet:

```
def fact(n):
  f = 1
  while n > 0:
    f = f * n
    n = n - 1
  return f
```

Die Zeile `f=1` ist einerseits nötig, damit das Programm funktioniert, und gleichzeitig ist das der Rückgabewert für die Eingabe `fact(0)`. 1 ist das, was herauskommt, wenn man *gar nicht* multipliziert. Ist es nicht logisch, dass es nur so und nicht anders sein kann? Siehe dazu auch den Wikipedia-Artikel zum leeren Produkt.

leeres Produkt

III

Relationen und Funktionen

Wir sind immer noch dabei, uns die grundlegenden Klassen von Objekten zu erarbeiten, um die es in der Mathematik geht. Eine davon ist die der *Funktionen*, die Sie aus der Schule bereits kennen, die wir aber in diesem Kapitel unter einem etwas anderen Blickwinkel unter die Lupe nehmen werden. Vorher schauen wir uns jedoch *Relationen* an, die man rein strukturell als Verallgemeinerung von Funktionen betrachten kann, die aber inhaltlich eine ganz andere Bedeutung (um nicht zu sagen: *Funktion*) haben.

5. Relationen

Wir fangen gleich mit einer Frage an:

> **Aufgabe 5.1**. Was haben die vier Ausdrücke $x \in \{y^n : n \in \mathbb{N}\}$, $x^2 + y^2 = 1$, $x \subseteq y$ und $x < y$ gemeinsam?

Eine Aussageform $A(x, y)$ mit zwei Individuenvariablen x und y kann man so interpretieren, dass sie eine Beziehung zwischen x und y ausdrückt: Ist $A(x, y)$ wahr, dann stehen x und y in einer bestimmten Beziehung zueinander; ist sie falsch, dann tun sie das nicht. Solche Beziehungen werden wir in diesem Abschnitt untersuchen. Man kann sie durch Mengen ausdrücken.

Definition

Eine Menge R von Paaren nennt man eine **Relation**.[1] Für $(x, y) \in R$ schreibt man in so einem Fall auch oft xRy. Ist R eine Teilmenge von $A \times B$, dann spricht man von einer Relation **zwischen** A und B. Ist R eine Teilmenge von A^2, dann spricht man von einer Relation **auf** A.

Aus der Aussageform $x < y$ können wir also nun z. B. die Relation

$$R = \{(x, y) \in \mathbb{R}^2 : x < y\}$$

[1] In manchen Situationen ist es sinnvoll, auch ganz allgemein Mengen von n-Tupeln als sogenannte *n-stellige Relationen* zu betrachten. Das brauchen wir aber nicht. In diesem Sinne beschäftigen wir uns ausschließlich mit *zweistelligen* Relationen, lassen das Adjektiv *zweistellig* jedoch weg.

auf $\mathbb{R}$ machen. Und rein formal können wir uns vorstellen, dass wir es mit dieser Menge R von Paaren zu tun haben, ohne zu wissen, wie sie definiert wurde. Wir nehmen uns die Freiheit heraus, diese Menge mit dem Zeichen $<$ statt mit einem Buchstaben zu bezeichnen, und schreiben $x < y$ als Abkürzung dafür, dass (x, y) zu der Menge gehört. In diesem Sinne *definiert* die Menge die Relation – im konkreten Fall die sogenannte *Kleiner-Relation*.

Kleiner-Relation

Die vielleicht wichtigste Relation überhaupt ist die, für die wir das Gleichheitszeichen verwenden. Rein technisch erhalten wir für jede Menge eine andere Relation, der wir einen eigenen Namen und gleich zwei Schreibweisen verpassen.

Definition

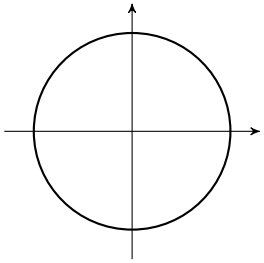
Für jede Menge A definieren wir die **Identität** auf A als die Menge

$$\mathrm{id}_A = \Delta_A = \{(x, y) \in A^2 : x = y\} = \{(x, x) : x \in A\}.$$

Aufgabe 5.2. Machen Sie sich klar, dass durch $\{(x, y) \in A^2 : x = y\}$ und $\{(x, x) : x \in A\}$ tatsächlich dieselbe Menge beschrieben wird.

Relationen auf $\mathbb{R}$ kann man mithilfe des kartesischen Koordinatensystems visualisieren, weil dann die Elemente der Relation (also die Paare) Punkten in der Ebene entsprechen. Aus der Relation $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ wird beispielsweise ein Kreis mit Radius 1 um den Ursprung, der sogenannte *Einheitskreis*.

Einheitskreis



Aufgabe 5.3. Wie sehen $\Delta_{\mathbb{R}}$ und die Kleiner-Relation aus?

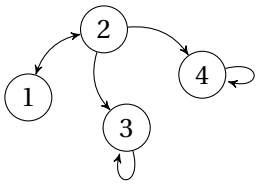
Wir fangen jedoch zunächst mit „kleinen“ Relationen an: mit endlichen Mengen von Paaren. Die haben den Vorteil, dass man sie besser überblicken kann. Außerdem bieten sie uns weitere Möglichkeiten der Visualisierung. Nehmen wir als Beispiel die Menge $A = [4]$ und die folgende Relation auf A:

$$R = \{(1,2), (2,1), (2,3), (2,4), (3,3), (4,4)\}$$

Man kann das übersichtlich als Tabelle darstellen:

	1	2	3	4
1		×		
2	×		×	×
3			×	
4				×

Oder auch in der folgenden Form, die wohl selbsterklärend ist:[2]



Aufgabe 5.4. Erstellen Sie für die Relation $\{(x, M) \in [3] \times \mathscr{P}([3]) : x \in M\}$ eine Tabelle.

Aufgabe 5.5. Zeichnen Sie für die Relation $\{(A, B) \in \mathscr{P}([3])^2 : A \subset B\}$ einen gerichteten Graphen.

Die Gleichheitsrelation, die wir unter dem Namen Identität formalisiert haben, ist das Muster für eine große Klasse von Relationen, die in der Mathematik eine zentrale Rolle spielen. Sie ahmen gleichsam drei wesentliche Eigenschaften der Identität nach, die wir folgendermaßen formulieren können.

(i) Für alle a gilt $a = a$.
(ii) Aus $a = b$ folgt $b = a$.
(iii) Aus $a = c$ und $c = b$ folgt $a = b$.

Diese Merkmale verallgemeinern wir nun und geben ihnen Namen.

Definition

Sei R eine Relation. R wird **reflexiv auf** A genannt, wenn das Paar (a, a) für alle $a \in A$ ein Element von R ist. R wird **symmetrisch** genannt, wenn für alle $(a, b) \in R$ auch (b, a) ein Element von R ist. R wird **transitiv** genannt, wenn aus $(a, c) \in R$ und $(c, b) \in R$ immer $(a, b) \in R$ folgt.

Die Begriffe sind so definiert, dass die Identität sie zwangsläufig erfüllt. Für jede Menge A ist id_A offenbar reflexiv auf A, symmetrisch und transitiv.

Aufgabe 5.6. Fällt Ihnen außer id_A noch eine andere Relation auf A ein, die garantiert reflexiv auf A, symmetrisch und transitiv ist? Dabei soll A nach wie vor eine beliebige Menge sein, über die Sie nichts weiter wissen. [Tipp: id_A ist in dem Sinne minimal, dass man von dieser Relation nichts mehr wegnehmen kann. Würde auch nur ein Paar fehlen, wäre das Ergebnis nicht mehr reflexiv auf A. Überlegen Sie sich stattdessen, wie eine besonders „große“ Relation aussehen würde.]

Aufgabe 5.7. Ist $\mathrm{id}_{\mathbb{N}}$ reflexiv auf $\mathbb{Z}$?

Aufgabe 5.8. Ist der Einheitskreis, also die Relation $E = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, symmetrisch? Was bedeutet Symmetrie in Sinne unserer Definition geometrisch?

Aufgabe 5.9. Ist der Einheitskreis transitiv?

[2] Man kann das als *gerichteten Graphen* interpretieren, dessen *Ecken* oder *Knoten* die Elemente von A und dessen *Kanten* die Elemente von R sind. Das ist aber momentan nicht unser Thema.

Aufgabe 5.10. Sei L die Menge der 16 Bundesländer Deutschlands. Ist die Relation

$$\{(x,y) \in L^2 : x \text{ und } y \text{ haben eine gemeinsame Grenze}\}$$

transitiv?

⋆**Aufgabe 5.11**. Wenn man eine Relation auf $\mathbb{R}$ als geometrische Figur in der Ebene darstellt, dann ist sie offenbar genau dann reflexiv auf $\mathbb{R}$, wenn die Hauptdiagonale Teil der Figur ist. Was die Symmetrie geometrisch bedeutet, haben wir uns in Aufgabe 5.8 überlegt. Fällt Ihnen zur Transitivität von solchen Relationen auch eine geometrische Entsprechung ein?

Aufgabe 5.12. Geben Sie bei den drei folgenden Relationen jeweils an, ob sie reflexiv auf [4], symmetrisch und transitiv sind. Begründen Sie Ihre Antworten.

	1	2	3	4
1	×	×	×	
2	×	×	×	
3	×	×	×	
4				

	1	2	3	4
1	×		×	×
2		×		×
3	×		×	
4	×	×		×

	1	2	3	4
1	×			×
2		×		
3			×	
4				×

Definition

Man kann auch etwas anders an die Sache herangehen, indem man die folgenden Operationen für Relationen definiert.

Ist R eine Relation, so definieren wir die **Umkehrrelation** zu R durch

$$R^{-1} = \{(y,x) : (x,y) \in R\}.$$

Sind R und S Relationen, so definieren wir deren **Komposition** durch

$$R \circ S = \{(x,y) : \exists z\,(xSz \wedge zRy)\}.$$

R^{-1} entsteht ganz simpel dadurch, dass wir alle Paare „umdrehen“:

$$R = \{(1,2),(2,7),(4,4),(5,6),(6,5)\}$$
$$R^{-1} = \{(2,1),(4,4),(5,6),(6,5),(7,2)\}$$

Die Komposition ist ein bisschen komplizierter. Hier werden immer Paare aus den beiden Relationen „verschmolzen“, wenn sie „zusammenpassen“. Dabei ist die Reihenfolge gewöhnungsbedürftig, weil sie einem anfangs „falsch“ vorkommt. Wieso wir es so machen, wird klar werden, wenn wir uns mit Funktionen befassen.[3] Außerdem wird es durchaus passieren, dass Paare bei der Komposition entweder keinen oder mehrere „Partner“ finden. Ein Beispiel, das nebenbei zeigt, dass die Komposition nicht kommutativ ist:

$$R = \{(2,4),(5,3),(5,4)\}$$

[3] Und in manchen Büchern macht man es auch andersherum. Leider wieder so eine Sache, bei der man beim Lesen aufpassen muss …

$$S = \{(1,2),(2,7),(3,5)\}$$
$$R \circ S = \{(1,4),(3,3),(3,4)\}$$
$$S \circ R = \{(5,5)\}$$

Aufgabe 5.13. Wenn R die Kleiner-Relation $\{(x,y) \in \mathbb{R}^2 : x < y\}$ ist, wie sieht dann R^{-1} in beschreibender Mengenschreibweise aus?

Aufgabe 5.14. Sei $R = \{(m,n) \in \mathbb{N}^+ \times \mathbb{N}^+ : 2m \text{ teilt } n\}$. Wie sieht $R \circ R$ in beschreibender Mengenschreibweise aus?

Mithilfe der neuen Begriffe können wir die drei uns interessierenden Eigenschaften von Relationen nun rein mengentheoretisch formulieren.

Satz 5.1

Sei R eine Relation auf A. Dann gilt:

(i) R ist genau dann reflexiv auf A, wenn $\mathrm{id}_A \subseteq R$ gilt.
(ii) R ist genau dann symmetrisch, wenn $R^{-1} \subseteq R$ gilt.
(iii) R ist genau dann transitiv, wenn $R \circ R \subseteq R$ gilt.

Aufgabe 5.15. Ich erspare mir einen Beweis für Satz 5.1. Sie sollten sich jedoch klarmachen, dass es da eigentlich nichts zu beweisen gibt, sondern dass es sich jeweils nur um unterschiedliche Formulierungen desselben Sachverhalts handelt.

Äquivalenzrelationen

Wir sind jetzt endlich so weit, dass wir formulieren können, was mit „verhält sich im Wesentlichen so wie die Gleichheitsrelation“ gemeint ist.

Definition

Eine Relation R auf A wird **Äquivalenzrelation auf** A genannt, wenn R reflexiv auf A, symmetrisch und transitiv ist.

Auf jeden Fall ist id_A immer eine Äquivalenzrelation auf A. Das war ja auch der Sinn der Definition. Außerdem hatten wir uns bereits in Aufgabe 5.6 überlegt, dass A^2 auch immer eine Äquivalenzrelation auf A ist. Eine Mathematikerin würde sagen, dass das „triviale“ Exemplare sind. Wäre das alles, dann wäre die Definition ziemlich sinnlos. Es gibt jedoch unzählige weitere Beispiele. Davon schauen wir uns nun ein paar an. Fangen wir in Anlehnung an Aufgabe 5.12 mit übersichtlichen Tabellen an.

	1	2	3	4
1	×	×	×	
2	×	×	×	
3	×	×	×	
4				×

	1	2	3	4
1	×	×		
2	×	×		
3			×	×
4			×	×

	1	2	3	4
1	×		×	
2		×		×
3	×		×	
4		×		×

Sie werden inzwischen geübt genug sein, um zu sehen, dass es sich in allen drei Fällen um Äquivalenzrelationen handelt. Weitere Beispiele folgen in den Aufgaben. Wir werden dabei übrigens öfter die Formulierung verwenden, dass durch eine Aussageform $A(x,y)$ eine Relation auf einer Menge M definiert wird. Gemeint ist damit die Relation $\{(x,y) \in M^2 : A(x,y)\}$. (Wir kehren damit in gewissem Sinne zurück zum Anfang des Abschnitts, in dem Relationen über Aussageformen motiviert wurden.)

Quersumme

Aufgabe 5.16. Die (dezimale) *Quersumme* $q(n)$ einer natürlichen Zahl n ist die Summe ihrer Ziffern (im Dezimalsystem), also ist z. B. $q(945) = 18$. Die *einstellige* oder *iterierte Quersumme* $Q(n)$ von n erhält man, indem man so lange die Quersumme bildet, bis das Ergebnis einstellig ist. Also ist z. B. $Q(945) = q(q(945)) = q(18) = 9$. Durch $Q(m) = Q(n)$ wird eine Relation $\sim$ auf $\mathbb{N}$ definiert. Handelt es sich um eine Äquivalenzrelation?

Aufgabe 5.17. Warum wird durch „x und y wurden am selben Wochentag geboren“ eine Äquivalenzrelation auf der Menge aller Einwohner Hamburgs definiert?

Aufgabe 5.18. Wird durch $x - y \in \mathbb{Z}$ eine Äquivalenzrelation auf $\mathbb{R}$ definiert? Was ändert sich, wenn man $\mathbb{Z}$ durch $\mathbb{N}$ ersetzt?

Aufgabe 5.19. $R = \{(a,a) : a \in A\} \cup \{(1,2),(1,3),(1,4),(2,1),(2,4),(4,2)\}$ ist eine Relation auf $A = [4]$. Man kann aus R eine Äquivalenzrelation auf A machen, indem man ein Element von R entfernt und stattdessen ein Element von $A \times A$ hinzufügt. Geben Sie an, welches Paar man entfernen und welches man hinzufügen muss, damit sich eine Äquivalenzrelation auf A ergibt.

Durch die Relation aus Aufgabe 5.17 werden die Einwohner Hamburgs in sieben „Clubs“ aufgeteilt. Jeder gehört zu einem der Clubs, aber auch nur zu einem. Äquivalenzrelationen teilen ihre Grundmenge immer auf diese Art auf. Das wird nun formalisiert.

Definition

Sei R eine Äquivalenzrelation auf A. Für $a \in A$ definieren wir die **Äquivalenzklasse** von a (bezüglich R) als[4]

$$[a]_R = \{b \in A : aRb\}$$

und die **Faktor-** oder **Quotientenmenge** von A nach R durch

$$A/R = \{[a]_R : a \in A\}.$$

Wegen der Reflexivität gilt offenbar immer $a \in [a]_R$. Insbesondere ist damit jedes Element von A Element einer Äquivalenzklasse. Außerdem sieht man leicht, dass $[a]_R = [b]_R$ dann und nur dann gilt, wenn aRb gilt, und dass unterschiedliche Äquivalenzklassen disjunkt sein müssen. Letzteres impliziert, dass jedes Element von A Element von genau einer Äquivalenzklasse ist.

[4] Nicht zu verwechseln mit der Notation $[n]$ aus dem Kapitel über Kombinatorik!

Aufgabe 5.20. Wie sehen die Äquivalenzklassen und Faktormengen zu den drei durch Tabellen definierten Relationen auf Seite 65 aus?

Aufgabe 5.21. Durch $R = \mathrm{id}_A \cup \{(1,2),(2,1),(3,4),(4,3)\}$ wird eine Äquivalenzrelation auf $A = [7]$ definiert. Geben Sie die Faktormenge A/R an.

Aufgabe 5.22. Wie sehen die Äquivalenzklassen und Faktormengen zu den Äquivalenzrelationen aus den Aufgaben 5.16 und 5.18 aus?

Das, was Äquivalenzrelationen mit ihrer Grundmenge machen, kann man auch anders – unabhängig von Relationen – beschreiben. Dafür brauchen wir allerdings noch ein paar Begriffe.

Definition

Ist $\mathscr{A}$ eine Menge von Mengen, dann definieren wir die **Vereinigungsmenge** von $\mathscr{A}$ als

$$\bigcup\mathscr{A} = \bigcup_{M\in\mathscr{A}} M = \{x : \exists M \in \mathscr{A}\ x \in M\}.$$

Ist $\mathscr{A}$ nicht leer,[5] dann definieren wir außerdem die **Schnittmenge** von $\mathscr{A}$ als

$$\bigcap\mathscr{A} = \bigcap_{M\in\mathscr{A}} M = \{x : \forall M \in \mathscr{A}\ x \in M\}.$$

Wir haben es hier mit drei „Stufen“ zu tun: Objekte, Mengen von Objekten und Mengen von solchen Mengen. Aus didaktischen Gründen verwenden wir in diesem Abschnitt unterschiedliche Symbole für diese Stufen: Kleinbuchstaben, Großbuchstaben und kalligraphische Buchstaben. Diese Unterscheidung werden wir jedoch später wieder aufgeben.

x ist nach dieser Definition ein Element der Vereinigungsmenge $\bigcup\mathscr{A}$, wenn x Element mindestens einer Menge aus $\mathscr{A}$ ist. Ist $\mathscr{A}$ endlich, so ergibt sich eigentlich nichts Neues, z. B.

$$\begin{aligned}
\bigcup\{A\} &= \{x : \exists X \in \{A\}\ x \in X\} = \{x : x \in A\} = A,\\
\bigcup\{A,B\} &= \{x : \exists X \in \{A,B\}\ x \in X\} = \{x : x \in A \vee x \in B\} = A \cup B,\\
\bigcup\{A,B,C\} &= \{x : \exists X \in \{A,B,C\}\ x \in X\}\\
&= \{x : x \in A \vee x \in B \vee x \in C\} = A \cup B \cup C
\end{aligned}$$

und so weiter. Für die Schnittmenge $\bigcap\mathscr{A}$ sieht das analog ebenso aus.

Interessant wird es erst, wenn $\mathscr{A}$ unendlich ist. Und dafür sollte man sich vielleicht an Aufgabe 1.24 und den Absatz davor erinnern. In diesem Sinne kann man sich Vereinigungs- und Schnittmenge informell als

$$\bigcup\{A_1, A_2, A_3, \ldots\} = A_1 \cup A_2 \cup A_3 \cup \cdots$$

[5] Würden wir $\bigcap\emptyset$ erlauben, so würden wir so etwas wie „die Menge *aller* Objekte“ erhalten. Das führt auf einen der am Ende von Abschnitt 2 erwähnten Widersprüche.

$$\bigcap\{A_1, A_2, A_3, \ldots\} = A_1 \cap A_2 \cap A_3 \cap \cdots$$

vorstellen, obwohl dieser Vergleich etwas hinkt, weil erstens die rechten Seiten dieser beiden „Gleichungen“ nicht definiert sind und weil zweitens die in der obigen Definition auftretende Menge $\mathscr{A}$ nicht notwendig in der Form A_1, A_2 und so weiter „sortiert“ sein muss.[6]

Aufgabe 5.23. Sei $\mathscr{A} = \{[n] : n \in \mathbb{N}^+\}$. Geben Sie $\bigcup\mathscr{A}$ und $\bigcap\mathscr{A}$ an. Was ändert sich, wenn wir $\mathbb{N}^+$ durch $\mathbb{N}$ ersetzen?

Aufgabe 5.24. Sei $\mathscr{A} = \{\mathbb{N} \setminus \{n\} : n \in \mathbb{N}\}$. Geben Sie $\bigcup\mathscr{A}$ und $\bigcap\mathscr{A}$ an.

Aufgabe 5.25. Was ist $\bigcup\emptyset$?

Aufgabe 5.26. Dies ist quasi eine Fortsetzung von Aufgabe 2.14: Begründen Sie, warum die beiden folgenden „Definitionen“ von $\mathbb{Z}$ mithilfe von $\mathbb{N}$ *beide falsch* (!) sind:

$$\mathbb{Z} = \{(n, -n) : n \in \mathbb{N}\}$$
$$\mathbb{Z} = \{\{n, -n\} : n \in \mathbb{N}\}$$

Wie könnte man die zweite Variante durch das Hinzufügen eines einzigen Symbols „retten“?

Aufgabe 5.27. Fällt Ihnen eine Menge $\mathscr{A}$ mit den drei Eigenschaften $\mathbb{R} \in \mathscr{A}$, $\bigcup\mathscr{A} \in \mathscr{A}$ und $\bigcap\mathscr{A} \in \mathscr{A}$ ein? [Tipp: Probieren Sie mit einfachen Beispielen herum.]

$\bigcup_{n\in\mathbb{N}^+}[n]$

Für eine Vereinigungsmenge wie in Aufgabe 5.23 werden wir in Zukunft auch Schreibweisen wie $\bigcup_{n\in\mathbb{N}^+}[n]$ verwenden und analog auch für die Schnittmenge. Das sollte hoffentlich selbsterklärend sein.

Definition

Eine Menge $\mathscr{P}$ von Mengen wird **Partition** der Menge M genannt, wenn sie die folgenden drei Bedingungen erfüllt:

(i) $\bigcup\mathscr{P} = M$

(ii) $\emptyset \notin \mathscr{P}$

(iii) Die Elemente von $\mathscr{P}$ sind paarweise disjunkt, d. h., für $A, B \in \mathscr{P}$ mit $A \neq B$ gilt $A \cap B = \emptyset$.

So etwas haben wir u. a. in der Lösung von Aufgabe 5.20 gesehen: $\{\{1,2,3\},\{4\}\}$ und $\{\{1,2\},\{3,4\}\}$ und $\{\{1,3\},\{2,4\}\}$ sind drei Beispiele für Partitionen der Menge $[4]$. Die bildliche Vorstellung, die Sie dabei haben sollten, ist die, dass eine Partition die gegebene Menge in getrennte Gebiete aufteilt.

Aufgabe 5.28. Wie unterscheiden sich Partitionen in der Mathematik und Partitionen in der Informatik?

[6] Genauer: Sie muss nicht *abzählbar* sein.

Aufgabe 5.29. Welche der folgenden Mengen sind *keine* Partitionen von $\mathbb{N}$? Geben Sie in diesen Fällen jeweils ein konkretes Gegenbeispiel als Begründung an.

$$\mathscr{A} = \{\{2n, 2n+1, 2n+2\} : n \in \mathbb{N}\}$$
$$\mathscr{B} = \{\{2n+1, 2n+2\} : n \in \mathbb{N}\}$$
$$\mathscr{C} = \{\{k \in \mathbb{N} : 2^n \leq 3^k < 2^{n+1}\} : n \in \mathbb{N}\}$$
$$\mathscr{D} = \{\{0\}, \{1\}, \mathbb{N} \setminus \{0,1\}\}$$

Äquivalenzklassen sind natürlich eine der Motivationen für den Begriff der Partition. Den angekündigten Zusammenhang können wir nun formulieren.

Satz 5.2

Für jede Menge $A \neq \emptyset$ gilt:

(i) Ist R eine Äquivalenzrelation auf A, dann ist A/R eine Partition von A. Man nennt sie die von R *induzierte* Partition.

(ii) Ist $\mathscr{P}$ eine Partition von A, dann ist

$$R = \{(x,y) \in A^2 : \exists C \in \mathscr{P}\,(x \in C \wedge y \in C)\}$$

eine Äquivalenzrelation auf A und A/R ist $\mathscr{P}$. Man nennt R die von $\mathscr{P}$ *induzierte* Äquivalenzrelation.

Dass (i) gilt, hatten wir uns bereits im Anschluss an die Definition des Begriffs der Äquivalenzklasse überlegt. Dass (ii) gilt, will ich nicht formal beweisen, aber es ist hoffentlich anschaulich klar, was passiert: Zwei Elemente von A stehen genau dann in der Relation R zueinander, wenn sie bezüglich der Partition im selben „Gebiet“ liegen. Man kann es auch so sehen: Weil $\mathscr{P}$ eine Partition von A ist, gibt es für jedes Element x von A genau ein „Gebiet“ $P_x \in \mathscr{P}$, in dem es liegt, für das also $x \in P_x$ gilt. Damit hat man eine Funktion, die den Elementen ihre Gebiete zuordnet, und zwei Elemente stehen in der Relation R zueinander, wenn sie denselben Funktionswert haben. Mit der Argumentation aus der Lösung von Aufgabe 5.16 ist dann klar, dass R eine Äquivalenzrelation ist.

Aufgabe 5.30. Denken Sie sich eine Äquivalenzrelation auf der Menge [6] aus (nicht gerade eine der beiden trivialen) und zeichnen Sie sie als Graph wie auf Seite 63. Welche Gestalt müssen Graphen von Äquivalenzrelationen zwangsläufig immer haben? Können Sie an dem Bild die Aussage von Satz 5.2 *sehen*?

Aufgabe 5.31. $\mathscr{P} = \{\{2^n, \ldots, 2^{n+1}-1\} : n \in \mathbb{N}\}$ ist eine Partition von $\mathbb{N}^+$. Wie sehen die Elemente von $\mathscr{P}$ aus? Beschreiben Sie mit Worten die von $\mathscr{P}$ induzierte Äquivalenzrelation. (Hinweis: Das sollten Sie aus der Informatik kennen.)

Aufgabe 5.32. Wie viele verschiedene Äquivalenzrelationen kann man auf der Menge [4] definieren? (Hinweis: Das ist nicht schwer, sondern eher eine Fleißarbeit. Verwenden Sie Satz 5.2.)

Resümee

In gewissem Sinne hat schon Euklid in den legendären *Elementen* vor über zwei Jahrtausenden das Konzept der Äquivalenzrelation vorweggenommen. Die heutzutage übliche Definition ist jedoch ein Produkt des 20. Jahrhunderts. Und aus diesem Jahrhundert stammt auch die vielleicht wichtigste Anwendung von Relationen in der Informatik: relationale Datenbanken.

Satz 5.2 mag Ihnen vielleicht nicht besonders spektakulär vorkommen (und er ist es auch nicht), er ist jedoch ein einfaches Beispiel für ein wiederkehrendes Thema in der Mathematik: Man ist bestrebt, interessante Strukturen aus unterschiedlichen Blickwinkeln zu betrachten und mit unterschiedlichen Methoden zu untersuchen. Wir haben gesehen, dass wir zu einer gegebenen Menge A einerseits Mengen von Paaren aus A^2 mit bestimmten Eigenschaften betrachten können, die wir *Äquivalenzrelationen* genannt haben, und andererseits Mengen von Teilmengen von A mit bestimmten Eigenschaften, die wir *Partitionen* genannt haben – und dass beides exakt dieselben Phänomene beschreibt. Aufgabe 5.32 war eine simple Demonstration dafür, inwiefern so eine Korrespondenz hilfreich sein kann. (Es wäre wesentlich schwieriger gewesen, die Anzahl der Äquivalenzrelationen direkt – ohne den „Umweg“ über die Partitionen – zu berechnen.)

⋆ Relationen im Computer

Rein technisch sind einige der Operatoren von PYTHON Relationen; nämlich die, die einen Wert vom Typ `bool` zurückgeben, z. B. == oder <. Auch manche Schlüsselwörter wie `in` sind in diesem Sinne Relationen.

Man kann aber Relationen auch wie in der Mathematik als Mengen von Paaren interpretieren und die Definitionen aus dem Skript „nachbauen“. Die Syntax von PYTHON macht das im Vergleich zu vielen anderen Programmiersprachen besonders angenehm. Hier zunächst Identität, Umkehrrelation und Komposition.

```
identity = lambda A: {(x,x) for x in A}
inv = lambda R: {(y,x) for (x,y) in R}
comp = lambda R,S: {(x,y) for (x,z) in S for (w,y) in R if z==w}
```

Die Tests auf Reflexivität, Symmetrie und Transitivität könnten so aussehen:

```
refl = lambda R,A: identity(A) <= R
symm = lambda R: inv(R) <= R
trans = lambda R: comp(R,R) <= R
```

Man könnte es aber auch „direkt“ programmieren. So kann man besonders gut erkennen, dass Satz 5.1 wirklich nur eine Umformulierung der Definitionen ist:

```
refl = lambda R,A: all((x,x) in R for x in A)
symm = lambda R: all((y,x) in R for (x,y) in R)
```

```
trans = lambda R: all((x,y) in R for (x,z) in R
                                 for (w,y) in R if z==w)
```

In beiden Fällen hat man dann jedenfalls einen einfachen Test für die Eigenschaft, eine Äquivalenzrelation auf einer bestimmten Menge zu sein:

```
eqRel = lambda R,A: refl(R,A) and symm(R) and trans(R)
```

Vereinigungs- und Schnittmenge könnte man folgendermaßen definieren:

```
def Union(A):
  R = set()
  for M in A:
    R |= M
  return R
def Intersection(A):
  R = next(iter(A))
  for M in A:
    R &= M
  return R
```

`Intersection` wird automatisch „meckern“, wenn `A` leer ist. Anderenfalls wäre auch nicht klar, wie man anfangen sollte, d. h., welchen Wert die Variable `R` initial haben sollte.

6. Funktionen

Aus der Schulzeit dürften Sie eine ungefähre Vorstellung davon mitbringen, was man in der Mathematik unter einer *Funktion* versteht. Wenn Sie das präzise beschreiben sollen, werden Sie aber vielleicht Probleme haben. Dieser Abschnitt liefert eine moderne und exakte Definition dieses Begriffs auf mengentheoretischer Basis und führt gleichzeitig diverse Konzepte ein, die wir in den folgenden Kapiteln immer mal wieder brauchen werden.

In der Schule verbindet man mit dem Funktionsbegriff im Allgemeinen eine Rechenvorschrift, die Zahlen andere Zahlen zuordnet. Ein „Klassiker“ ist die Wurzelfunktion, die einer Zahl x ihre Quadratwurzel $\sqrt{x}$ zuordnet. Ein anderes Beispiel ist eine Gerade mit der Steigung m und dem Achsenabschnitt b, die einer Zahl x die Zahl $mx+b$ zuordnet.[7]

Anhand solcher Beispiele wollen wir herausarbeiten, was alle Funktionen im mathematischen Sinne gemeinsam haben, inwieweit diese Beispiele jedoch zu speziell sind und nicht den gesamten Funktionsbegriff umfassen:

(i) Man kann sich Funktionen als „Vorrichtungen“ oder „Maschinen“ vorstellen, die eine Eingabe erhalten und dazu eine Ausgabe liefern. Die Wurzelfunktion

[7] In der Schule wird so etwas oft als „lineare Funktion“ bezeichnet, was sich aber leider mit der Hochschulmathematik beißt. Besser wäre das Adjektiv *affin-linear*.

liefert z. B. bei der Eingabe 4 die Ausgabe 2 und bei der Eingabe 9 die Ausgabe 3. In diesem Sinne haben Funktionen große Ähnlichkeit mit Funktionen in Programmiersprachen.

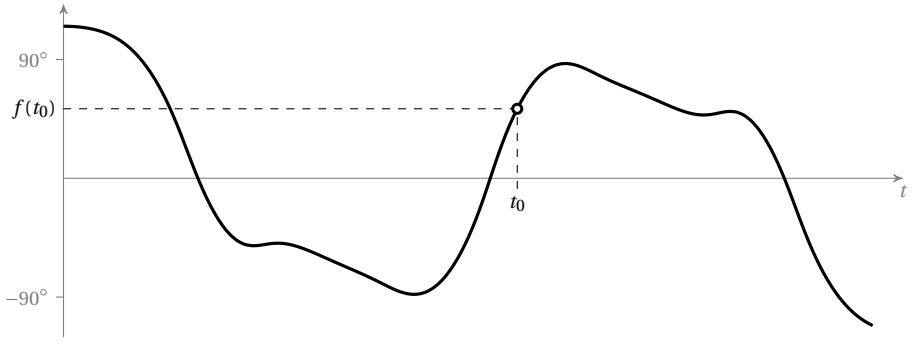
(ii) Mathematische Funktionen sind „verlässlich“: Für dieselbe Eingabe liefern sie immer dieselbe Ausgabe.[8] Das unterscheidet sie von Funktionen in Programmiersprachen, die u.a. auch zufällige Werte ausgeben, je nach Uhrzeit unterschiedliche Dinge tun oder ein „Gedächtnis“ haben können.

(iii) Nicht jeder Eingabewert ist zulässig. Die erwähnte Wurzelfunktion akzeptiert etwa keine negativen Zahlen als Eingabe. Das kennen Sie aus der Schule als *Definitionsbereich* der Funktion.

(iv) Es muss nicht um Zahlen gehen. Sowohl die Eingabewerte als auch die Ausgabewerte von Funktionen können beliebige mathematische Objekte wie Mengen, Tupel, Vektoren, Matrizen und so weiter sein. Wir werden dafür schon bald Beispiele sehen.

(v) Anders als in den genannten Beispielen muss es keine *Rechenvorschrift* geben, die festlegt, wie die Ausgabe aus der Eingabe generiert wird. Es geht einzig und allein darum, *dass* es zu jeder möglichen Eingabe eine klar definierte Ausgabe gibt. (Beispielsweise könnte diese einer vorher festgelegten Tabelle entstammen, die „ausgewürfelt“ wurde.)

Besonders der letzte Punkt ist wohl erklärungsbedürftig. Warum belässt man es nicht einfach bei Funktionen, die man berechnen kann? Eine Antwort darauf liefert die Physik. Dort ist man häufig auf der Suche nach Funktionen – meistens nach solchen, die bestimmte Werte in Abhängigkeit von der Zeit liefern: Welche Position hat ein Himmelskörper zu einem bestimmten Zeitpunkt? Welche Geschwindigkeit hat ein Elementarteilchen zu einem bestimmten Zeitpunkt? Und in der Regel kann die Physik mit sogenannten Differentialgleichungen die gesuchten Funktionen so beschreiben, dass man mathematisch beweisen kann, dass sie existieren und eindeutig bestimmt sind. Gleichzeitig kann man aber auch beweisen, dass man die Funktionswerte nicht exakt berechnen kann. Man kann mit anderen Worten kein Computerprogramm schreiben, das sie auswirft, indem es sie durch eine Formel berechnet. Die folgende Grafik zeigt ein Beispiel für so eine Funktion: den zeitlichen Verlauf eines der Winkel des in der Vorlesung vorgeführten Doppelpendels.



[8] Man kann es auch so sehen, dass Mathematik „zeitlos“ ist, was teilweise schon im Abschnitt über Logik angeklungen ist. Es ist egal, *wann* man die Funktion mit einer Eingabe füttert.

Die grafische Darstellung wurde zwar durch einen Computer erzeugt, aber die dafür benötigten Zahlen konnten nur näherungsweise durch eine Simulation ermittelt werden. Wir sehen die Visualisierung der Funktion und wir können uns vorstellen, wie wir für einen Zeitpunkt t_0 den Winkel $f(t_0)$ ablesen. Aber es ist eben nur so wie das Ablesen der Zahlen aus einer Tabelle.[9]

Die moderne Vorstellung einer Funktion ist daher auch die einer Tabelle mit zwei Spalten: einer für die Eingabe und einer für die Ausgabe. Und solche „Tabellen" kennen wir schon, nämlich Relationen! Die Relation

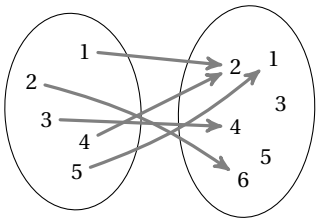
$$R = \{(1,2),(2,6),(3,4),(4,2),(5,1)\} \tag{6.1}$$

ist die mengentheoretische Repräsentation der folgenden Tabelle:

Eingabe	Ausgabe
1	2
2	6
3	4
4	2
5	1

R können wir beispielsweise entnehmen, dass der Eingabe 3 die Ausgabe 4 zugeordnet wird. Und wir können an R auch sehen, dass als Eingaben nur die natürlichen Zahlen von 1 bis 5 zugelassen sind. Aus mathematischer Sicht *ist* R eine Funktion, weil man mehr über eine Funktion nicht wissen muss.

Manchmal ist es auch hilfreich, sich eine solche Zuordnung mittels eines Pfeildiagramms zu visualisieren:[10]



Bevor wir daraus eine Definition machen, müssen wir jedoch noch klären, dass nicht *jede* Relation sich als Funktion eignet. Wenn wir eine kleine Änderung vornehmen und statt R die Relation

$$S = \{(1,2),(2,6),(3,4),(4,2),(4,1)\}$$

betrachten, dann ist nicht mehr klar, was bei der Eingabe 4 geschehen soll: Soll 2 oder 1 ausgegeben werden? So etwas darf nicht passieren. Das halten wir jetzt fest:

[9] Es hätte auch so sein können, dass die Punkte, aus denen die Grafik zusammengesetzt ist, Messwerte sind. Die hätten dann ja ebenfalls einmal in einer Tabelle gestanden.

[10] Das ist allerdings *kein* Mengendiagramm im Sinne des Abschnitts über Mengen, denn hier werden Objekte ja mehrfach gezeichnet. Bis auf die Sechs tauchen alle Zahlen links und rechts auf.

Definition

Eine Relation R – also eine Menge von Paaren – wird **rechtseindeutig** genannt, wenn aus $(x, y_1) \in R$ und $(x, y_2) \in R$ immer $y_1 = y_2$ folgt.[11] Eine **Funktion** ist eine rechtseindeutige Relation.

Funktionen werden oft auch *Abbildungen* genannt.[12]

Aufgabe 6.1. Was bedeutet Rechtseindeutigkeit für Pfeildiagramme wie das obige? Was darf man in so einem Diagramm also nicht sehen?

Aufgabe 6.2. Welche der folgenden Mengen ist eine Funktion?

$f_1 = \{(n, n/3) : n \in \mathbb{N}\}$ $\quad$ $f_2 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$

$f_3 = \{(1,2), 3, (4,5)\}$ $\quad$ $f_4 = \{(1,3), (3,5), (4,5)\}$

$f_5 = \{(1,2), (1,3), (4,5)\}$ $\quad$ $f_6 = \emptyset$

Definition

Ist f eine Relation, dann nennen wir die Menge $\mathrm{dom}(f) = \{x : (x, y) \in f\}$ den **Definitionsbereich** der Relation und $\mathrm{rng}(f) = \{y : (x, y) \in f\}$ ihren **Wertebereich** bzw. ihre **Bildmenge**.[13]

Der Definitionsbereich ist also einfach die Menge aller ersten Komponenten der Paare der Relation und der Wertebereich die Menge aller zweiten Komponenten. In einem Pfeildiagramm wie auf Seite 73 ist der Definitionsbereich die Menge der Objekte, von denen ein Pfeil ausgeht, und der Wertebereich die Menge der Objekte, auf die mindestens ein Pfeil zeigt. Beachten Sie, dass nach unserer Definition jede Relation (und damit insbesondere jede Funktion) ihren Definitions- und Wertebereich „mit sich herumträgt“: die beiden Mengen sind fest in die Relation „hineincodiert“.

Aufgabe 6.3. Geben Sie Definitions- und Wertebereich der Relationen an, die in Aufgabe 6.2 vorkamen.

Die Menge f_1 aus Aufgabe 6.2 ist das „klassische“ Beispiel für eine Funktion. Hier wird jeder Eingabe n eine Ausgabe durch die Rechenvorschrift $n/3$ zugeordnet. Solche Funktionen schreibt man ganz ausführlich in der folgenden Form:

$$f_1 : \begin{cases} \mathbb{N} \to \mathbb{Q} \\ n \mapsto n/3 \end{cases} \tag{6.2}$$

[11] R darf also keine zwei Paare (x_1, y_1) und (x_2, y_2) mit $x_1 = x_2$ und $y_1 \neq y_2$ enthalten. Im Englischen wird so eine Relation auch *univalent* genannt.

[12] In manchen Büchern wird aus didaktischen Gründen zwischen Funktionen und Abbildungen unterschieden. Wir werden das aber nicht tun. Es ist allerdings so, dass bestimmte Funktionen aus historischen Gründen eher als Abbildungen bezeichnet werden, z. B. die linearen Abbildungen der linearen Algebra.

[13] Wir verwenden dabei die internationalen Bezeichnungen *domain* und *range*. In der Schule schreibt man für den Definitionsbereich von f oft auch D_f und für den Wertebereich W_f.

D_f W_f

Vor dem Doppelpunkt steht optional der Name der Funktion. In der oberen Zeile steht links der Definitionsbereich und rechts eine sogenannte *Zielmenge*. In der unteren Zeile steht links ein Platzhalter für ein Element des Definitionsbereichs und rechts die Rechenvorschrift angewandt auf diesen Platzhalter. (Linke und rechte Seite der unteren Zeile sind also die beiden Komponenten eines Paares der Funktion, wenn man sie als Relation betrachtet.) Beachten Sie, dass die beiden Pfeile unterschiedlich aussehen.[14]

Zielmenge

Verwechseln Sie die Zielmenge (engl. *codomain*) nicht mit dem Wertebereich![15] Der Wertebereich ist eine durch die Funktion eindeutig bestimmte Menge, während die Zielmenge irgendeine Obermenge des Wertebereichs ist. Wir hätten in (6.2) statt $\mathbb{Q}$ beispielsweise auch $\mathbb{R}$ schreiben können und hätten damit *dieselbe* Funktion definiert![16]

Aufgabe 6.4. Bei der Angabe der Zielmenge kann man also irgendeine Obermenge des Wertebereichs angeben. Warum ist man da so „liberal“? Es wäre doch präziser, wenn man in der Schreibweise (6.2) statt der Zielmenge den Wertebereich angeben würde. Haben Sie eine Idee, warum man es so macht?

Ist f eine Funktion mit Definitionsbereich A und Zielmenge B, dann sagt man auch, dass f eine Funktion *von A nach B* ist und schreibt als Abkürzung dafür $f\colon A \to B$. Ebenso sagt man dann, dass f *auf A* definiert ist.

$f\colon A \to B$

Durch die Rechtseindeutigkeit ist sichergestellt, dass es für jedes Element x des Definitionsbereichs einer Funktion f genau ein y mit $(x, y) \in f$ gibt. Für dieses eindeutig bestimmte y schreibt man $f(x)$ und nennt es das *Bild von x unter f*. Man sagt auch, dass die Funktion x *auf $f(x)$ abbildet* und schreibt dafür auch $x \mapsto f(x)$. x und $f(x)$ entsprechen also dem, was wir am Anfang des Abschnitts Ein- und Ausgabe genannt haben. Weitere verbreitete Bezeichnungen sind *Argument* für x und *Funktionswert* für $f(x)$.

$f(x)$
$x \mapsto f(x)$

Argument
Funktionswert

Manchmal werden auch informelle Sprechweisen wie „die Funktion $x \mapsto x^2$“ oder „die Funktion $f(x) = x^2$“ verwendet. Das sollte jedoch nur geschehen, wenn aus dem Kontext der Definitionsbereich der Funktion hervorgeht, weil sie nur dann vollständig beschrieben ist.

Aufgabe 6.5. Welche der folgenden Relationen sind Funktionen? Begründen Sie bei den Relationen, die keine Funktionen sind, Ihre Antwort jeweils durch ein konkretes Gegenbeispiel. Geben Sie in allen Fällen auch Definitions- und Wertebereich an.

$$g_1 = \mathrm{id}_{\mathbb{N}} \qquad g_2 = \{(\mathscr{P}(A), A) : A \subseteq \mathbb{N}\}$$
$$g_3 = \{(B, A) : A \subseteq B \subseteq \mathbb{N}\} \qquad g_4 = \{(A, \mathscr{P}(A)) : A \subseteq \mathbb{N}\}$$
$$g_5 = \{(\mathbb{R} \setminus \{a, b\}, \mathbb{R} \setminus \{a\}) : a, b \in \mathbb{R}\} \qquad g_6 = \{(\mathbb{R} \setminus \{a\}, \mathbb{R} \setminus \{a, b\}) : a, b \in \mathbb{R}\}$$

[14] Der untere Pfeil wird *maplet* genannt.

[15] Sie wussten aus Aufgabe 6.3 bereits, dass $\mathbb{Q}$ nicht der Wertebereich von f_1 ist.

[16] Auch hier muss ich leider wieder darauf hinweisen, dass in der Mathematik nicht immer Einigkeit besteht. Es gibt auch Bücher, in denen die Zielmenge fester Bestandteil der Funktionsdefinition ist. In diesem Fall würden wir beim Wechsel von $\mathbb{Q}$ nach $\mathbb{R}$ tatsächlich eine *andere* Funktion erhalten. In solchen Büchern ist eine Funktion aber auch nicht mehr einfach eine Menge von Paaren.

Bilder, Urbilder, Restriktionen

Es lässt sich leider nicht vermeiden, dass Sie in diesem Kapitel mit diversen neuen Begriffen bombardiert werden …

Definition

Für $f\colon A \to B$ und $C \subseteq A$ bzw. $D \subseteq B$ definieren wir

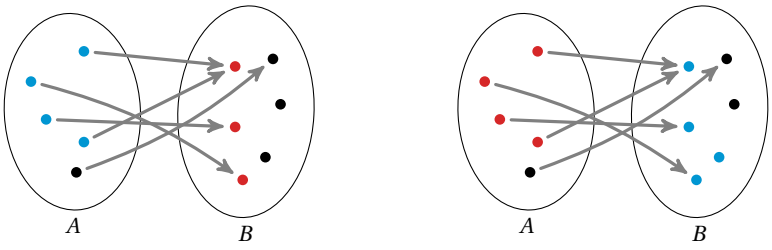
$$f[C] = \{f(c) : c \in C\} \text{ und}$$
$$f^{-1}[D] = \{c \in A : f(c) \in D\}.$$

$f[C]$ wird als **Bild von C unter f** bezeichnet, $f^{-1}[D]$ entsprechend als **Urbild von D unter f**.

Bild

$f[C]$ ist also die Menge aller möglichen Funktionswerte, wenn das Argument ganz C durchläuft. $f^{-1}[D]$ ist die Menge aller Argumente, die auf Funktionswerte in D abgebildet werden. Insbesondere ist dann natürlich $f[A]$ – manchmal auch kurz *Bild* von f genannt – dasselbe wie die Bildmenge $\operatorname{rng}(f)$ und $f^{-1}[B]$ dasselbe wie der Definitionsbereich von f.

Im folgenden Pfeildiagramm sehen wir zweimal dieselbe Funktion f von A nach B. Links ist in blauer Farbe eine Teilmenge C von A hervorgehoben und in Rot sieht man dazu die Elemente von $f[C]$. Rechts ist in Blau eine Teilmenge D von B markiert, während man in roter Farbe die Elemente von $f^{-1}[D]$ sieht. Beachten Sie, dass links die Menge $f[C]$ weniger Elemente als C hat und dass rechts ein Element von D für zwei Elemente in $f^{-1}[D]$ verantwortlich ist, während ein anderes gar keine Auswirkungen hat.



Ist f beispielsweise die durch $n \mapsto n+1$ auf $\mathbb{N}$ definierte Funktion, G die Menge der geraden und U die Menge der ungeraden natürlichen Zahlen, dann haben wir u. a. $f[\{0\}] = \{1\}$, $f[G] = U$, $f[\mathbb{N}] = \mathbb{N}^+$ und $f^{-1}[U] = G$.

Aufgabe 6.6. Sei f die auf $\mathbb{R}$ durch $x \mapsto x^2$ definierte Funktion sowie $A = \{0,1\}$. Geben Sie $f[A]$, $f^{-1}[A]$, $f[\emptyset]$ und $f^{-1}[\{-1\}]$ an.

Aufgabe 6.7. Sei f die auf $\mathbb{R}$ durch $x \mapsto x^2 - 7$ definierte Funktion und $A = \{-7,2,9\}$. Geben Sie $f[A]$, $f^{-1}[A]$, $f[f^{-1}[A]]$ und $f^{-1}[f[A]]$ an.

Aufgabe 6.8. Sei g die Funktion $\{(0,23),(\{0\},42)\}$. Geben Sie $\operatorname{dom}(g)$, $\operatorname{rng}(g)$, $g(\{0\})$ und $g[\{0\}]$ an.

Leider gibt es auch die Unsitte, $f(C)$ bzw. $f^{-1}(D)$ statt $f[C]$ bzw. $f^{-1}[D]$ zu schreiben. Aufgabe 6.8 sollte gezeigt haben, dass das keine gute Idee ist, weil es zu Missverständnissen führen kann. Diese Schreibweise ist aber so weit verbreitet, dass ich sie hier erwähnen muss, weil sie Ihnen sicher einmal begegnen wird.

Aufgabe 6.9. Sei f wie in (6.1) die Funktion

$$f = \{(1,2),(2,6),(3,4),(4,2),(5,1)\}.$$

Geben Sie eine Menge $M \subseteq [5]$ an, für die $f^{-1}[f[M]] = M$ *nicht* gilt. Kann man auch eine Teilmenge N von $\operatorname{rng}(f)$ mit $f[f^{-1}[N]] \neq N$ finden?

Aufgabe 6.10. Sei f die Funktion aus Aufgabe 6.9. Geben Sie Teilmengen M und N von $[5]$ mit $f[M \cap N] \neq f[M] \cap f[N]$ an.

⋆**Aufgabe 6.11**. Schauen Sie sich die Lösung von Aufgabe 5.16 noch einmal an. Wir hatten dort eine Funktion Q, die auf der Menge $\mathbb{N}$ definiert war und die dadurch eine Äquivalenzrelation definiert hat, dass sie quasi die Gleichheitsrelation von ihrem Wertebereich auf $\mathbb{N}$ „übertragen“ hat. Können Sie das als allgemeine Aussage definieren in dem Sinne, dass jede Funktion auf diese Art eine Äquivalenzrelation generiert?

⋆**Aufgabe 6.12**. Wie sehen für die Relation R aus der Lösung von Aufgabe 6.11 die Äquivalenzklassen aus?

Manchmal ist es sinnvoll, den Definitionsbereich einer Funktion einzuschränken:

Definition

Für $f\colon A \to B$ und $C \subseteq A$ definiert man die **Restriktion** (**Einschränkung**) von f auf C durch

$$f|_C = \{(x,y) \in f : x \in C\}.$$

$f|_C$ ist also selbst wieder eine Funktion, und zwar eine Funktion mit Definitionsbereich C. Es ist die Funktion, die man erhält, wenn man aus f alle Paare entfernt, deren erste Komponente nicht in C liegt. Auf C „macht“ $f|_C$ aber dasselbe wie f. Eine weitere übliche Schreibweise für die Restriktion ist $f \restriction C$.

$f \restriction C$

Aufgabe 6.13. Sei R die in (6.1) definierte Funktion und $X = \{1,2,3\}$. Wie sieht die Menge $R|_X$ aus?

Aufgabe 6.14. Sei f die Funktion aus Aufgabe 6.6 und $M = \{x \in \mathbb{R} : x \leq 0\}$. Geben Sie die Definitions- und Wertebereiche von f und von $f|_M$ an.

Injektivität, Surjektivität, Bijektivität

Eine der angenehmsten Eigenschaften, die Funktionen haben können, ist die Injektivität. Dann kann man sie nämlich umkehren und zum „Zählen“ verwenden. Darum geht es in diesem Abschnitt.

Definition

Eine Funktion f wird **injektiv** genannt, wenn für alle $x, y \in \mathrm{dom}(f)$ aus $x \neq y$ immer $f(x) \neq f(y)$ folgt.

Injektivität bedeutet in Worten, dass für unterschiedliche Eingaben (Argumente) auch unterschiedliche Ausgaben (Funktionswerte) herauskommen. Am Pfeildiagramm von Seite 73 kann man das ganz gut nachvollziehen. Die dort dargestellte Funktion ist nicht injektiv, denn die Zahl 2 wird von zwei Pfeilen getroffen.[17]

Ein „klassisches“ Beispiel, an dem man sich dieses neue Konzept ebenfalls gut vergegenwärtigen kann, ist die Funktion

$$f\colon \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto x^2 \end{cases} . \tag{6.3}$$

Sie ist *nicht* injektiv, denn beispielsweise gilt $f(2) = 4 = f(-2)$, obwohl 2 und -2 natürlich zwei verschiedene Argumente sind.

Aufgabe 6.15. Fällt Ihnen eine ganz einfache Klasse von Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ ein, die alle injektiv sind?

Aufgabe 6.16. Im Lösungshinweis für Aufgabe 6.15 habe ich absichtlich etwas unpräzise formuliert. Ist Ihnen aufgefallen, was man noch hätte hinzufügen müssen?

Aufgabe 6.17. Machen Sie sich klar, dass eine Funktion f genau dann injektiv ist, wenn aus $f(x) = f(y)$ immer $x = y$ folgt.

Aufgabe 6.18. Die folgenden Funktionen sind alle nicht injektiv. Begründen Sie das jeweils mit konkreten Gegenbeispielen.

$$f = \{(x, \lfloor x \rfloor) : x \in \mathbb{R}\}$$
$$g = \{(A, |A|) : A \subseteq [6]\}$$
$$h = \{(n, Q(n)) : n \in \mathbb{N}\}$$

Dabei soll Q die iterierte Quersumme aus Aufgabe 5.16 sein. Die untere Gaußklammer kennen Sie aus der Lösung zu Aufgabe 5.22.

Die Bedeutung der Injektivität steckt in der folgenden Aussage, die ich nicht formal beweisen werde, die man sich aber leicht anhand eines Pfeildiagramms klarmachen kann.

Satz 6.1

Eine Funktion f ist genau dann injektiv, wenn f^{-1} eine Funktion ist.

Umkehrfunktion

Injektive Funktionen sind also die, die man *umkehren* kann. Die Umkehr*relation* ist in diesem Fall eine Funktion, die man dann auch *Umkehrfunktion* nennt. Jede

[17] Erinnern Sie sich, dass Rechtseindeutigkeit bedeutet, dass von jedem Objekt links nur ein Pfeil ausgeht. Injektivität bedeutet, dass bei jedem Objekt rechts (höchstens) ein Pfeil ankommt. Man nennt Injektivität daher manchmal auch *Linkseindeutigkeit*.

linkseindeutig

Funktion ordnet jedem Argument eindeutig einen Funktionswert zu. Injektive Funktionen ordnen zusätzlich auch jedem Funktionswert eindeutig ein Argument zu. Häufig kann man – wie in Aufgabe 6.20 – auch eine Rechenvorschrift für die Umkehrfunktion angeben, die dann gleichzeitig ein Beleg dafür ist, dass man es tatsächlich mit einer injektiven Funktion zu tun hat. Mit anderen Worten: Wenn Sie ein Verfahren angeben können, wie man aus jeder Ausgabe *eindeutig* die zugehörige Eingabe rekonstruieren kann, dann ist die Funktion injektiv.

Aufgabe 6.19. Wenn f injektiv ist, was ist dann der Definitionsbereich der Umkehrfunktion f^{-1}?

Aufgabe 6.20. Begründen Sie für die folgenden Funktionen, dass sie injektiv sind, indem Sie jeweils eine Rechenvorschrift für die Umkehrfunktion angeben.

$$f = \{(x, 2x+8) : x \in \mathbb{R}\}$$
$$g = \{(A, [6] \setminus A) : A \subseteq [6]\}$$
$$h = \{(n, n^2) : n \in \mathbb{N}\}$$

Aufgabe 6.21. In Aufgabe 6.20 kam eine Funktion vor, die ihre eigene Umkehrfunktion war. Können Sie noch ein (ganz einfaches) Beispiel für so eine Funktion angeben?

Aufgabe 6.22. Sei $A = \{x \in \mathbb{R} : x \geq 0\}$ und f die Funktion, die jedes $x \in \mathbb{R}$ auf den Absolutbetrag $|x|$ abbildet. Ist f injektiv? Ist $f|_A$ injektiv?

⋆**Aufgabe 6.23**. Wie sieht die Relation R aus der Lösung von Aufgabe 6.11 aus, wenn die Funktion f injektiv ist?

Wenn eine Funktion nicht injektiv ist, dann wird das offenbar dadurch verhindert, dass sie „zu viele“ Paare enthält. Das kann man immer dadurch „reparieren“, dass man solche Paare entfernt. Dafür verwendet man die weiter oben eingeführte Restriktion. Ein Beispiel dafür haben Sie gerade in Aufgabe 6.22 gesehen. Durch die Restriktion erhält man eine Funktion, die eine Umkehrfunktion hat.

Diese Vorgehensweise kennen Sie auch schon länger, allerdings vielleicht nicht unter diesem Namen: Beispielsweise ist die durch (6.3) definierte Funktion f nicht injektiv. Die Restriktion von f auf $\{x \in \mathbb{R} : x \geq 0\}$ ist jedoch injektiv und deren Umkehrfunktion kennen Sie als die *Wurzelfunktion*, die als Beispiel schon erwähnt wurde. Erst durch die Einschränkung von f wird klar, dass durch $\sqrt{9}$ eindeutig der Wert 3 (und nicht etwa die Zahl -3) bezeichnet wird.

Wurzelfunktion

⋆**Aufgabe 6.24**. Fallen Ihnen weitere Funktionen aus der Schule ein, die als Umkehrfunktionen von Restriktionen definiert sind?

Ein zur Injektivität gleichsam komplementäres Konzept ist das der Surjektivität.

Definition

Man sagt, dass eine Funktion f die Menge A **surjektiv**[18] auf die Menge B abbildet, wenn es für jedes $y \in B$ ein $x \in A$ mit $f(x) = y$ gibt.

Das bedeutet informell, dass alle „möglichen“ Ausgaben auch wirklich vorkommen. Wir können dazu wieder das Pfeildiagramm von Seite 73 betrachten. Die dort visualisierte Funktion bildet nicht surjektiv auf [6] ab, denn die Zahl 3 wird z. B. nicht „getroffen“. Die Funktion bildet jedoch surjektiv auf $\{1,2,4,6\}$ ab. Und die in (6.3) definierte Funktion f eignet sich auch hier als „klassisches“ Beispiel. f bildet $\mathbb{R}$ *nicht* surjektiv auf $\mathbb{R}$ ab, weil es u. a. kein Argument gibt, das den Funktionswert -1 liefert.

Man erkennt hier auch, dass Injektivität eine Eigenschaft ist, die eine Funktion entweder hat oder nicht hat, während Surjektivität nur im Zusammenhang mit der Angabe einer Menge Sinn ergibt.[19] Obige Funktion f bildet nämlich $\mathbb{R}$ surjektiv auf die Zielmenge $\{x \in \mathbb{R} : x \geq 0\}$ ab. Trotzdem werden Sie im informellen Sprachgebrauch öfter hören, dass eine Funktion einfach als surjektiv bezeichnet wird. Dann sollte aber aus dem Kontext hervorgehen, welche Zielmenge gemeint ist. Wenn man beispielsweise f durch (6.3) definiert und dann sagt, dass f nicht surjektiv ist, dann sollte wohl klar sein, dass als Zielmenge implizit die gemeint war, die in (6.3) steht.

Aufgabe 6.25. Begründen Sie die folgenden Aussagen jeweils mit konkreten Gegenbeispielen.

(i) f aus Aufgabe 6.18 bildet $\mathbb{R}$ nicht surjektiv auf $\mathbb{R}$ ab.

(ii) g aus Aufgabe 6.18 bildet $\mathscr{P}([6])$ nicht surjektiv auf $\mathbb{N}$ ab.

(iii) $h = \{(x, x^2) : x \in \mathbb{Q}\}$ bildet $\mathbb{Q}$ nicht surjektiv auf $\{q \in \mathbb{Q} : q \geq 0\}$ ab.

Aufgabe 6.26. Die folgenden vier Funktionen haben alle sowohl als Definitionsbereich als auch als Zielmenge die Menge $\mathbb{N}$ der natürlichen Zahlen. Welche sind injektiv, welche bilden $\mathbb{N}$ surjektiv auf $\mathbb{N}$ ab? Begründen Sie negative Antworten jeweils mit konkreten Gegenbeispielen.

$$f_1 = \{(n, n+1) : n \in \mathbb{N}\}$$
$$f_2 = \{(n, \lfloor n/2 \rfloor) : n \in \mathbb{N}\}$$
$$f_3 = \{(n, \lfloor n/2 \rfloor + 1) : n \in \mathbb{N}\}$$
$$f_4 = \{(n, n) : n \in \mathbb{N}\}$$

Auch die Surjektivität kann man etwas anders charakterisieren als durch die Definition und wie bei Satz 6.1 sollte hoffentlich auch hier ohne strengen Beweis klar sein, dass die folgende Aussage korrekt ist.

[18] Das wird „sürjektiv“ ausgesprochen, weil es aus dem Französischen kommt. Die Begriffe in diesem Abschnitt stammen alle von dem legendären Mathematiker Nicolas Bourbaki – den es gar nicht gab. (Der Name war ein Pseudonym einer Gruppe französischer Mathematiker im 20. Jahrhundert.)

[19] Das ist so wie mit der Symmetrie und der Reflexivität bei Relationen. Eine Relation ist entweder symmetrisch oder nicht, aber es ergibt keinen Sinn, von einer reflexiven Relation zu sprechen, wenn man nicht hinzufügt, welche Grundmenge gemeint ist.

Sei f eine Funktion von A nach B. f bildet A genau dann surjektiv auf B ab, wenn B der Wertebereich von f ist, wenn also $f[A] = B$ gilt. **Satz 6.2**

Für den Fall, dass die Begriffe noch nicht „sitzen“, schlage ich noch die folgende Eselsbrücke vor: Wenn die Eintrittskarten eines Kinos mit Platznummern versehen sind, dann kann man sie als Abbildung der Menge der Besucher auf die Menge der Sitzplätze betrachten. Die Besucher möchten, dass diese Funktion injektiv ist, denn sonst könnte es passieren, dass jemand anders denselben Platz wie sie hat. Der Kinobesitzer möchte, dass die Funktion surjektiv auf die Menge der Plätze abbildet, weil dann das Kino ausverkauft ist.

Man sagt, dass eine Funktion f die Menge A **bijektiv** bzw. **eineindeutig** auf die Menge B abbildet, wenn f injektiv ist und die Menge A surjektiv auf B abbildet. **Definition**

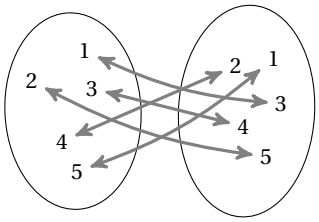
Das ist also eigentlich kein neuer Begriff, sondern lediglich eine Zusammenfassung der beiden vorherigen. Informell steht *bijektiv* einfach für *injektiv und surjektiv*. Bijektivität ist eine wichtige Eigenschaft im Zusammenhang mit der Mächtigkeit von Mengen:

Seien A und B endliche Mengen. Dann sind die beiden folgenden Aussagen äquivalent: **Satz 6.3**

(i) $|A| = |B|$

(ii) Es gibt eine Funktion, die A bijektiv auf B abbildet.

Dass aus der zweiten Aussage die erste folgt, wird intuitiv klar, wenn man ein Pfeildiagramm einer bijektiven Funktion zeichnet.



Dass die Funktion injektiv ist, bedeutet, dass man Pfeile in beide Richtungen zeichnen kann, und die Surjektivität sorgt dafür, dass von jedem Element rechts ein Pfeil in die linke Menge zeigt. Wenn man nun die Elemente einer der beiden Mengen zählt, dann zählt man durch die Zuordnung automatisch die der anderen mit. Das ist so, als würden Sie überprüfen wollen, ob in einer Tüte mit Gummibärchen dieselbe Anzahl von roten und gelben Bärchen enthalten ist, Sie aber keine Lust zum Zählen haben: Sie legen die Bärchen einfach immer paarweise hin. Wenn das möglich ist, dann haben Sie eine Bijektion[20] generiert. Und damit sollte wohl auch

[20] Wie Sie sich schon gedacht haben, ist *Bijektion von A auf B* einfach ein anderes Wort für eine Funktion, die A bijektiv auf B abbildet. Bijektion

klar sein, wieso aus der ersten Aussage von Satz 6.3 die zweite folgt, wie man also so eine Funktion erhält.

Aufgabe 6.27. Gilt Satz 6.3 auch für den Fall $A = B = \emptyset$?

Aufgabe 6.28. Sie erinnern sich sicher aus dem Abschnitt über Prädikatenlogik, dass mit Aussage (ii) im Satz 6.3 gemeint ist, dass es *mindestens* eine Funktion mit dieser Eigenschaft gibt. Geben Sie zwei verschiedene Funktionen an, die $A = [5]$ bijektiv auf $B = \{23, 42, \pi, 0, \sqrt{3}\}$ abbilden. Wie viele solche Funktionen gibt es insgesamt?

Aufgabe 6.29. In Aufgabe 6.28 ist von „verschiedenen" Funktionen die Rede. Wann sind denn zwei Funktionen überhaupt gleich? Liefern unsere bisherigen Definitionen darauf eine klare Antwort?

Aufgabe 6.30. Sei $A = [3]$ und $B = \{2, 3, 5, 7, 11\}$. Wie viele injektive Funktionen von A nach B gibt es?

⋆**Aufgabe 6.31**. Können Sie analog zu Satz 6.3 eine hinreichende und notwendige Bedingung für $|A| \leq |B|$ angeben?

⋆**Aufgabe 6.32**. Sei f eine Funktion mit der Eigenschaft, dass $f^{-1}[f[M]] = M$ für alle $M \subseteq \mathrm{dom}(f)$ gilt.[21] Was kann man dann über f sagen?

Mehrstellige Funktionen und Definition durch Fallunterscheidung

In diesem kurzen Abschnitt definieren wir keine neuen Begriffe, aber wir lernen weitere Arten kennen, wie in der Praxis Funktionen eingesetzt werden. Eine davon ist, dass die Argumente der Funktion Tupel sind. Das ist nichts Neues und durch die Definitionen der vorherigen Seiten bereits abgedeckt, aber es wird häufig anders notiert. Hier ein Beispiel:

$$f\colon \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (m, n) \mapsto m^2 + n^2 \end{cases} \tag{6.4}$$

Diese Funktion bildet z. B. das Argument $(1,5)$ auf $1^2 + 5^2 = 26$ ab und das Argument $(4,4)$ auf $4^2 + 4^2 = 32$. Man müsste also eigentlich $f((1,5)) = 26$ schreiben. In der Regel wird man sich jedoch die „überflüssigen" Klammern sparen und einfach $f(1,5)$ schreiben. Man spricht dann auch von einer *zweistelligen* Funktion[22] und verwendet manchmal auch das Wort *Verknüpfung* statt Funktion. Wenn Sie schon ein bisschen programmiert haben, wird Ihnen das nicht neu vorkommen. Man beachte jedoch die Feinheiten:

zweistellige Funktion

Verknüpfung

– Der Prototyp des Arguments links vom Zeichen $\mapsto$ muss zu den Elementen des Definitionsbereichs passen. Im Beispiel ist (m, n) in Ordnung, weil die Elemente von $\mathbb{N} \times \mathbb{N}$ Paare sind. (m, m) wäre *nicht* in Ordnung gewesen, weil die Paare aus $\mathbb{N} \times \mathbb{N}$ typischerweise nicht zwei gleiche Komponenten haben.

[21] Aufgabe 6.9 hat gezeigt, dass das nicht für jede Funktion der Fall ist.

[22] Analog gibt es natürlich auch dreistellige oder allgemein *mehrstellige* Funktionen, deren Argumente Tripel bzw. n-Tupel sind. Man schreibt dann so etwas wie $f(x, y, z)$.

mehrstellige Funktion

– Man *interpretiert* einen Ausdruck wie $f(1,5)$ oft so, dass die Funktion *zwei* Eingaben – nämlich 1 und 5 – bekommt. Aber formal bekommt sie nur *eine* Eingabe: das Paar $(1,5)$.
– Der letzte Punkt ist insbesondere für die Frage relevant, ob so eine Funktion injektiv ist. Unser Beispiel ist nämlich *nicht* injektiv, weil auch $f(5,1) = 26$ gilt und $(1,5)$ und $(5,1)$ verschiedene Paare sind.

Mit dieser Sichtweise kann man auch ganz „alltägliche“ Operationen wie Addition oder Multiplikation als Funktionen betrachten – und so sieht man sie in der Mathematik auch: Ist M irgendeine Menge, dann bezeichnet man eine Funktion von $M \times M$ nach M als (zweistellige) *innere Verknüpfung* auf M. In diesem Sinne ist beispielsweise die Funktion, die (x, y) auf $x + y$ abbildet, eine innere Verknüpfung auf $\mathbb{N}$ (und auch auf $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$). innere Verknüpfung

Aufgabe 6.33. Wenn man Multiplikation als innere Verknüpfung auf $\mathbb{R}$ betrachtet, ist diese Funktion dann injektiv?

Aufgabe 6.34. Ist die Funktion, die jedem Tupel (m, n) aus $\mathbb{N}^2$ die Zahl $m - n$ zuordnet, eine innere Verknüpfung auf $\mathbb{N}$?

Aufgabe 6.35. Welche der folgenden Funktionen ist injektiv? Begründen Sie negative Antworten jeweils mit einem konkreten Gegenbeispiel.

$$f_1 \colon \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (m,n) \mapsto m \end{cases} \qquad f_2 \colon \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N} \\ (m,n) \mapsto (n,m) \end{cases} \qquad f_3 \colon \begin{cases} \mathbb{N} \to \mathbb{N} \times \mathbb{N} \\ n \mapsto (n,n) \end{cases}$$

⋆**Aufgabe 6.36**. Ist es möglich, dass eine Funktion von $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$ injektiv ist? Geben Sie entweder ein Beispiel für eine solche Funktion an oder begründen Sie, warum das nicht geht.

Manchmal definiert man Funktionen auch durch eine *Fallunterscheidung*. Das sieht dann beispielsweise so aus: Fallunterscheidung

$$f \colon \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} \end{cases} \tag{6.5}$$

Für den Funktionswert $f(x)$ stehen hier die beiden Alternativen x und $-x$ zur Verfügung und dahinter steht jeweils, unter welcher Bedingung eine der beiden Alternativen gewählt wird.[23] Das Prinzip ist hoffentlich nicht schwer zu verstehen und das Gleiche kann man natürlich auch mit mehr als zwei Fällen machen. Da Funktionen eigentlich Relationen sind, lässt sich unser Beispiel auch leicht als

$$\{(x,x) : x \in \mathbb{R} \wedge x \geq 0\} \cup \{(x,-x) : x \in \mathbb{R} \wedge x < 0\}$$

übersetzen. Daran kann man besonders gut sehen, worauf man achten muss: Es werden zwei Funktionen vereinigt und damit die Vereinigung immer noch eine

[23] Das entspricht offenbar einer Verzweigung beim Programmieren.

Funktion ist, müssen die beiden Definitionsbereiche (wie hier) disjunkt sein oder im Schnitt der Definitionsbereiche müssen die Funktionswerte übereinstimmen. Siehe dazu die folgenden Aufgaben.

Aufgabe 6.37. Was wäre, wenn man in (6.5) die Bedingung $x < 0$ durch $x \le 0$ ersetzen würde?

Aufgabe 6.38. Nur in einem der beiden folgenden Fälle wird wirklich eine Funktion definiert. Wo liegt beim anderen der Fehler?

$$f_1 : \begin{cases} \mathbb{N} \to \mathbb{N} \\ n \mapsto \begin{cases} \lfloor n/10 \rfloor & n \le 9 \\ \lfloor (n-4)/10 \rfloor & n \ge 4 \end{cases} \end{cases} \qquad f_2 : \begin{cases} \mathbb{N} \to \mathbb{N} \\ n \mapsto \begin{cases} \lfloor n/10 \rfloor & n \le 9 \\ \lfloor (n+4)/10 \rfloor & n \ge 4 \end{cases} \end{cases}$$

Aufgabe 6.39. Unter welchem Namen kennt man die in (6.5) definierte Funktion?

Aufgabe 6.40. Schreiben Sie die Funktion

$$f : \begin{cases} [6] \to \mathbb{N} \\ n \mapsto \begin{cases} n & n \text{ ist gerade} \\ 6-n & n \text{ ist ungerade} \end{cases} \end{cases}$$

als Menge von Paaren auf. Was ist der Wertebereich von f?

Komposition und arithmetische Verknüpfung von Funktionen

Wir kennen bereits die *Komposition*, die aus zwei Relationen eine neue Relation generiert. Funktionen kann man natürlich auch komponieren, weil die ja nach Definition Relationen sind.

Satz 6.4 Sind f und g Funktionen, dann ist die Relation $f \circ g$ ebenfalls eine Funktion und für alle x aus dem Definitionsbereich von $f \circ g$ gilt $(f \circ g)(x) = f(g(x))$.

Wir wollen uns in diesem Fall wirklich einmal einen Beweis „gönnen“, weil das nicht sehr aufwendig ist. Um zu zeigen, dass die Relation $R = f \circ g$ eine Funktion ist, greifen wir uns zwei Paare (x, z_1) und (x, z_2) aus R heraus und müssen zeigen, dass $z_1 = z_2$ gilt. Weil die beiden Paare zu R gehören, gibt es nach Definition der Komposition Objekte y_1 und y_2 mit $(x, y_i) \in g$ und $(y_i, z_i) \in f$ für $i = 1, 2$. Weil g nach Voraussetzung eine Funktion ist, gilt $y_1 = y_2$. Und weil f nach Voraussetzung ebenfalls eine Funktion ist, folgt daraus $z_1 = z_2$. Das war's schon. Und den zweiten Teil des Satzes haben wir damit auch schon bewiesen, denn wir haben offenbar $z_1 = R(x)$, $z_1 = f(y_1)$ und $y_1 = g(x)$ und damit $R(x) = f(g(x))$.

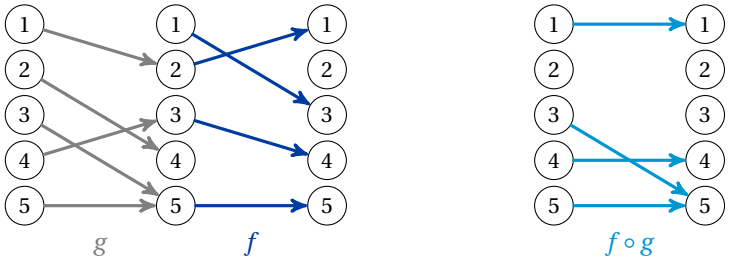
Die Komposition $f \circ g$ ist also das Hintereinanderausführen der beiden Funktionen: Die Ausgabe von g wird als Eingabe von f verwendet. Damit wird nun auch klar, warum die Komposition scheinbar „verkehrt herum“ definiert wurde. Es liegt daran, dass in der Schreibweise $g(x)$ für den Funktionswert die Funktion g links

vom Argument x steht. Wenn wir diesen Wert als Argument in eine Funktion f einsetzen wollen, dann wird daraus $f(g(x))$. f kommt quasi *nach* g „dran“, steht aber links davon, obwohl wir ansonsten von links nach rechts schreiben.[24]

Als übersichtliches Beispiel betrachten wir die Funktionen

$$f = \{(1,3),(2,1),(3,4),(5,5)\} \quad \text{und} \quad g = \{(1,2),(2,4),(3,5),(4,3),(5,5)\}$$

und erhalten die Komposition $f \circ g = \{(1,1),(3,5),(4,4),(5,5)\}$. Siehe dazu auch die folgende Grafik.



Wenn diese Begriffe neu für Sie sind, dann sollten Sie das Beispiel im Detail nachvollziehen und überprüfen. Dabei sind Ihnen vielleicht zwei Dinge aufgefallen:

(i) Die Zahl 2 gehört zum Definitionsbereich von g, aber nicht zum Definitionsbereich der Komposition $f \circ g$. Das liegt daran, dass g diese Zahl auf die Zahl 4 abbildet, die aber nicht zum Definitionsbereich von f gehört.

(ii) Die Zahl 3 gehört zum Wertebereich von f, aber nicht zum Wertebereich der Komposition $f \circ g$. Das liegt daran, dass f die Zahl 1 auf 3 abbildet, 1 jedoch nicht zum Wertebereich von g gehört.

Aufgabe 6.41. Berechnen Sie auch $g \circ f$. Was fällt Ihnen auf?

In der Praxis wird man zumindest die Situation (i) von oben in der Regel vermeiden und nur Kompositionen $f \circ g$ bilden, bei denen der Wertebereich von g eine Teilmenge des Definitionsbereichs von f ist. Grafisch gesprochen soll also jeder Pfeil von g eine „Fortsetzung“ durch einen von f bekommen. Dann haben g und $f \circ g$ denselben Definitionsbereich. So werden wir es im Folgenden auch halten (wenn wir nicht explizit nach seltsamen Gegenbeispielen suchen).

Haben wir für die Funktionen, die komponiert werden, Rechenvorschriften, dann brauchen wir nicht mühsam passende Paare zusammenzusuchen, sondern wir können Satz 6.4 anwenden und eine Rechenvorschrift in die andere „einsetzen“. Haben wir z. B. die durch $f(x) = x^2$ und $g(x) = 3 + 2x$ jeweils auf ganz $\mathbb{R}$ definierten Funktionen, dann ergibt sich die Rechenvorschrift für $f \circ g$ durch

$$(f \circ g)(x) = f(g(x)) = f(3+2x) = (3+2x)^2 = 9 + 12x + 4x^2.$$

[24] Aus diesem Grund wird $f \circ g$ auch als „f nach g“ gelesen; manchmal aber auch als „f komponiert mit g“, „f Kuller g“ oder „f Kringel g“.

Ganz einfach, wenn man nicht den leider recht häufigen Fehler macht, Klammern zu vergessen. Der Ausdruck für $g(x)$ wird in die Rechenvorschrift für $f(x)$ anstelle von x eingesetzt, aber *als Ganzes*. Vorsichtshalber sollte man ihn dort immer zuerst *mit* Klammern einsetzen. Sollten die sich als unnötig herausstellen, kann man sie immer noch entfernen. Hier wäre die Alternative $3+2x^2$ ohne Klammern auf jeden Fall falsch gewesen!

Aufgabe 6.42. Die Funktionen $f(x)=x^2$ und $g(x)=2^x$ sind auf ganz $\mathbb{R}$ definiert. Geben Sie die Rechenvorschriften für $f\circ g$ und $g\circ f$ an. Begründen Sie mit einem konkreten Gegenbeispiel, dass die beiden Kompositionen nicht gleich sind.

Aufgabe 6.43. Geben Sie zu den Funktionen

$$f:\begin{cases}\mathbb{N}\times\mathbb{N}\to\mathbb{N}\\(x,y)\mapsto x\end{cases}\qquad\text{und}\qquad g:\begin{cases}\mathbb{N}\to\mathbb{N}\times\mathbb{N}\\x\mapsto(x,x)\end{cases}$$

die Kompositionen $f\circ g$ und $g\circ f$ in derselben ausführlichen Schreibweise wie in der Aufgabenstellung an.

Was in der Lösung von Aufgabe 6.42 schon anklang, sei hier noch einmal explizit ausgesprochen. Dass die Komposition nicht kommutativ ist, dass also nicht *immer* $f\circ g=g\circ f$ gilt, heißt natürlich nicht, dass $f\circ g=g\circ f$ *nie* gilt.[25] Der typische Mathematikerschnack für so eine Situation ist, dass $f\circ g=g\circ f$ „im Allgemeinen nicht“ gilt; eine andere Formulierung dafür, dass es mindestens eine Ausnahme gibt. Man kann das also auch mit „nicht immer“ übersetzen.

im Allgemeinen nicht

Aufgabe 6.44. Fallen Ihnen zwei Funktionen f und g mit $f\circ g=g\circ f$ ein? (Gemeint sind wirklich *zwei* Funktionen, d. h., es soll $f\neq g$ gelten. Sonst wäre die Lösung „trivial“, wie eine Mathematikerin sagen würde.)

Mithilfe der Komposition können wir Aussagen über die Rolle der Identität und der Umkehrfunktion formulieren, die leicht zu beweisen sind, wenn man sich einfach die jeweiligen Definitionen vergegenwärtigt:

Satz 6.5

Sei f eine Funktion mit Definitionsbereich A und Wertebereich B. Dann gilt:

(i) $\mathrm{id}_B\circ f=f=f\circ\mathrm{id}_A$

(ii) $f\circ f^{-1}=\mathrm{id}_B$ und $f^{-1}\circ f=\mathrm{id}_A$, falls f injektiv ist.

Man kann das so interpretieren, dass $\circ$ eine Art Multiplikation von Funktionen ist und die Identität die Rolle der Eins spielt, während die Umkehrfunktion quasi der Kehrwert ist.[26] (Das erklärt auch die Schreibweise mit dem Exponenten -1.)

Es dürfte offensichtlich sein, dass $f\circ g$ injektiv ist, wenn f und g beide injektiv sind. (Machen Sie sich das ggf. mit Pfeildiagrammen klar.) Ist mindestens eine der

[25] Erinnern Sie sich an Aufgabe 1.23.

[26] Natürlich ist die Analogie nicht vollständig, weil es hier viele verschiedene „Einsen“ gibt und weil die Komposition anders als die Multiplikation reeller Zahlen nicht kommutativ ist. Mehr dazu in Abschnitt 7.

beiden Funktionen nicht injektiv, dann ist ihre Komposition das im Allgemeinen auch nicht mehr. Nehmen Sie als Beispiel $f(x) = x$ und $g(x) = x^2$ auf den reellen Zahlen: Keine der Funktionen $f \circ g$, $g \circ f$ und $g \circ g$ ist injektiv.

Aufgabe 6.45. Versuchen Sie Funktionen f und g von $\mathbb{N}$ nach $\mathbb{N}$ zu finden, für die eine der folgenden Aussagen gilt.

(i) f ist nicht injektiv, aber $f \circ g$ ist injektiv.

(ii) g ist nicht injektiv, aber $f \circ g$ ist injektiv.

Sie werden feststellen, dass das für eine der beiden Aussagen möglich ist und für die andere nicht. Können Sie begründen, warum das so ist?

⋆**Aufgabe 6.46**. Finden Sie Funktionen f und g, so dass f und g beide nicht injektiv sind, $f \circ g$ aber injektiv ist. Wieso steht das nicht im Widerspruch zu Aufgabe 6.45? [Tipp: Arbeiten Sie mit ganz einfachen Funktionen, die nur aus wenigen Paaren bestehen.]

Aufgabe 6.47. Welche der vier Funktionen aus Aufgabe 6.43 sind injektiv? Denken Sie wie üblich daran, dass für negative Antworten konkrete Gegenbeispiele am überzeugendsten sind.

Aufgabe 6.48. Welche der vier Funktionen

$$f: \begin{cases} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ (x,y) \mapsto y+1 \end{cases}, \qquad g: \begin{cases} \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \\ x \mapsto (x-1, x+1) \end{cases},$$

$f \circ g$ und $g \circ f$ sind injektiv?

Aufgabe 6.49. Welche der vier Funktionen

$$f: \begin{cases} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \\ (x,y) \mapsto (x+y, x-y) \end{cases}, \qquad g: \begin{cases} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \\ (x,y) \mapsto (y-1, x+1) \end{cases},$$

$f \circ g$ und $g \circ g$ sind injektiv?

Mit Funktionen, deren Funktionswerte Zahlen[27] sind, kann man „rechnen“:

Definition

Sind f und g Funktionen von einer Menge A nach $\mathbb{R}$, dann definieren wir die folgenden Funktionen:

$$f+g: \begin{cases} A \to \mathbb{R} \\ x \mapsto f(x)+g(x) \end{cases} \qquad f-g: \begin{cases} A \to \mathbb{R} \\ x \mapsto f(x)-g(x) \end{cases}$$

$$f \cdot g: \begin{cases} A \to \mathbb{R} \\ x \mapsto f(x) \cdot g(x) \end{cases} \qquad f/g: \begin{cases} \{x \in A : g(x) \neq 0\} \to \mathbb{R} \\ x \mapsto f(x)/g(x) \end{cases}$$

[27] Wir definieren das hier zunächst für reelle Zahlen. Später führen wir noch andere Objekte ein, mit denen man rechnen kann, z. B. komplexe Zahlen, Vektoren oder ganz allgemein Elemente von algebraischen Strukturen. Die Definitionen übertragen sich dann sinngemäß.

Wenn Sie so etwas zum ersten Mal sehen, kommt es Ihnen vielleicht komplizierter vor, als es ist. Haben wir es z. B. mit $f(x) = x^2$ und $g(x) = 5x$ zu tun, dann ist $f + g$ einfach die Funktion, die x auf $x^2 + 5x$ abbildet, und $f \cdot g$ bildet x auf $5x^3$ ab. Zu beachten ist bei diesen Definitionen lediglich:

- $f + g$, $f - g$ und so weiter sind wieder Funktionen.
- f und g müssen denselben Definitionsbereich haben.
- Wie üblich wird $f \cdot g$ oft auch als fg abgekürzt.
- Bei der Definition von f/g wird der Definitionsbereich ggf. eingeschränkt, damit nicht durch null dividiert wird.

Aufgabe 6.50. Die Funktionen

$$f : \begin{cases} \mathbb{Z} \to \mathbb{R} \\ n \mapsto 2n+4 \end{cases} \qquad \text{und} \qquad g : \begin{cases} \mathbb{Z} \to \mathbb{R} \\ n \mapsto 4-2n \end{cases}$$

sind zweifelsohne beide injektiv. Was ist mit $f + g$, $f - g$ und fg?

Aufgabe 6.51. Was würde sich bei Aufgabe 6.50 ändern, wenn man überall $\mathbb{Z}$ durch $\mathbb{N}$ ersetzen würde?

⋆**Aufgabe 6.52**. Sei f eine Bijektion von A auf B und g eine Bijektion von B auf C. Begründen Sie oder machen Sie sich zumindest mit Pfeildiagrammen klar, warum f^{-1} eine Bijektion von B auf A und $g \circ f$ eine Bijektion von A auf C ist.

Funktionen als Tupel, Folgen oder Familien

Im letzten Abschnitt des Kapitels geht es darum, dass man Funktionen je nach Kontext auch ganz anders verwenden kann, nämlich als Mechanismen zum Aufzählen bzw. Sortieren ihres Wertebereichs.

Schauen wir uns noch einmal eine ganz simple Funktion wie

$$f = \{(1,2),(2,6),(3,4),(4,2),(5,1)\}$$

an, die wir schon mehrfach betrachtet haben. Als Tabelle könnte man das folgendermaßen notieren:

Eingabe:	1	2	3	4	5
Ausgabe:	2	6	4	2	1

Wenn wir wissen, dass der Definitionsbereich $[5]$ ist, dann können wir uns die erste Zeile dabei auch sparen, wenn wir uns darauf einigen, die Funktionswerte in der „richtigen“ Reihenfolge aufzuschreiben: $(2,6,4,2,1)$. Das kann man offenbar folgendermaßen verallgemeinern:

Lemma 6.6

Sei n eine natürliche Zahl. Jede Funktion f mit $\mathrm{dom}(f) = [n]$ determiniert eindeutig ein n-Tupel, nämlich

$$(f(1), f(2), f(3), \ldots, f(n)).$$

Umgekehrt wird durch jedes n-Tupel $(a_1, a_2, a_3, \ldots, a_n)$ eindeutig eine Funktion mit Definitionsbereich $[n]$ festgelegt, nämlich

$$\{(1, a_1), (2, a_2), (3, a_3), \ldots, (n, a_n)\}.$$

In diesem Sinne *identifiziert* man in der Mathematik häufig auch n-Tupel mit solchen Funktionen und verwendet die Tupel als abkürzende Schreibweise. Diese Idee wird auch auf unendliche Definitionsbereiche übertragen. Beispielsweise kann man das „unendliche Tupel“

$$(0, 1, 4, 9, 16, 25, \ldots)$$

als die Funktion lesen, die jeder natürlichen Zahl n den Funktionswert n^2 zuordnet. Man würde das typischerweise als

$$\left(n^2 : n \in \mathbb{N}\right) \quad \text{oder} \quad \left(n^2\right)_{n\in\mathbb{N}}$$

schreiben.

Konvention

Eine Funktion f mit Definitionsbereich I kann man auch in einer der Formen

$$\left(f(i) : i \in I\right) \quad \text{oder} \quad \left(f(i)\right)_{i\in I}$$

aufschreiben. Das macht man insbesondere dann, wenn es für die Menge I eine „kanonische Ordnung“ gibt, wodurch die Menge der Funktionswerte „sortiert“ wird. Man spricht dann manchmal auch von einer **Familie** statt von einer Funktion. Ist I die Menge $\mathbb{N}$ oder $\mathbb{N}^+$, dann nennt man solche Funktionen auch **Folgen**.

Aufgabe 6.53. Schreiben Sie die Folge

$$: \begin{cases} \mathbb{N}^+ \to \mathbb{R} \\ n \to 1/n \end{cases}$$

in der gerade vorgestellten Schreibweise auf.

Definition

Sind A und B Mengen, so schreiben wir B^A für die Menge aller Funktionen von A nach B.[28]

[28] In der axiomatischen Mengenlehre schreibt man stattdessen ${}^AB$, um Verwechslungen mit der kardinalen Exponentiation zu vermeiden.

Man beachte, dass B in dieser Definition die Rolle der Zielmenge (und nicht die des Wertebereichs) spielt. Die Funktion $\{(1,42)\}$ ist z. B. ein Element von $\mathbb{N}^{[1]}$.

Aufgabe 6.54. Wenn A und B endliche Mengen sind, wie viele Elemente hat B^A dann?

⋆**Aufgabe 6.55**. Sei $n \in \mathbb{N}$. Geben Sie eine Bijektion von $\mathscr{P}([n])$ auf $[2]^{[n]}$ an.

Resümee

Das Wort *Funktion* stammt von dem bereits erwähnten Leibniz aus dem 17. Jahrhundert. Die Schreibweise $f(x)$ geht auf den berühmten Schweizer Mathematiker Leonhard Euler zurück, der sie 1734 zum ersten Mal verwendete. Bis zum heutigen Funktionsbegriff war es allerdings ein weiter Weg. Noch bis ins 19. Jahrhundert hinein bestanden nur recht schwammige Vorstellungen davon, was genau als Funktion gelten sollte, und sie waren eng mit dem Konzept einer Rechenvorschrift verbunden. Erst durch diverse pathologische Beispiele, die u.a. von Bernard Bolzano, Peter Gustav Lejeune Dirichlet und Karl Weierstraß entwickelt wurden, wurde nach und nach klar, dass man ein allgemeineres Konzept benötigte. Wie im Falle der Relationen konnte die inzwischen übliche Definition erst im 20. Jahrhundert entstehen, weil sie auf der Mengenlehre basiert.

⋆ Funktionen im Computer

Ob ein Objekt eine Funktion ist, kann man in PYTHON z. B. so überprüfen:

```
def rightUnique(R):
  return all(x1!=x2 or y1==y2 for (x1,y1) in R for (x2,y2) in R)
def isRelation(A):
  return all(type(x) is tuple and len(x)==2 for x in A)
def isFunction(A):
  return type(A) is set and isRelation(A) and rightUnique(A)
```

Und an den Definitionsbereich einer Funktion kommt man folgendermaßen heran:

```
def dom(f):
  return {x for (x,y) in f}
```

Vielleicht schreiben Sie als Übung noch PYTHON-Funktionen für den Wertebereich oder für das Testen auf Injektivität.

Natürlich ging es hier um *mathematische* Funktionen im Sinne dieses Kapitels. Die Kompositionen zweier PYTHON-Funktionen lässt sich aber auch recht elegant realisieren:

```
def comp(f, g):
  return lambda x: f(g(x))
```

```
f, g = lambda x: 3 * x, lambda x: x + 2
comp(f,g)(42)
```

Dass man wie in (6.4) das Argument einer Funktion vorab bereits in seine Einzelteile (im Beispiel sind das m und n) „zerlegt“, nennt man in der Informatik *Destrukturierung*. In PYTHON würden Sie die besagte Funktion typischerweise sicher so schreiben:

```
def f(m,n):
  return m**2+n**2
```

Dann würden Sie sie in der Form `f(1,5)` aufrufen. Man könnte das aber auch näher am „Original“ so schreiben:

```
def f(p):
  (m,n) = p
  return m**2+n**2
```

Der Aufruf wäre nun `f((1,5))`, d. h., `f` wird mit einem *Paar* als Argument aufgerufen und das Destrukturieren findet in der ersten Zeile der Funktion statt.[29] In Programmiersprachen wie HASKELL, in denen mit *Pattern Matching* gearbeitet wird, wird diese Vorgehensweise besonders deutlich.

Das Addieren von Funktionen könnte man in PYTHON so erreichen:

```
def plus(f,g):
  return lambda x: f(x)+g(x)
```

Für das Beispiel aus Aufgabe 6.50 sähe es dann so aus:

```
f, g = lambda n: 2*n+4, lambda n: 4-2*n
plus(f,g)(10)
```

In der Sprache JULIA könnte man sogar die mathematische Syntax verwenden:

```
import Base:+
+(f::Function, g::Function) = x -> f(x)+g(x)

f(n) = 2n+4
g(n) = 4-2n
(f+g)(10)
```

In dieser Sprache wird auch deutlicher, dass Operationen wie Addition und Multiplikation „ganz normale Funktionen“ sind, weil man dort z. B. statt `40+2` auch `+(40,2)` schreiben kann.

[29] Die Klammern sind in diesem Fall nicht nötig und stehen dort aus didaktischen Gründen.

IV

Algebraische Strukturen

Die Algebra ist eines der größten und wichtigsten Teilgebiete der Mathematik. Wir werden nicht besonders tief in diese teilweise sehr abstrakte Materie einsteigen, aber zumindest sollen einige grundlegende Strukturen eingeführt werden. Das wird uns später beim präzisen Formulieren helfen und es wird hoffentlich auch den Blick dafür schärfen, worum es beim „Rechnen“ eigentlich geht.

Wenn man in der Mathematik von *Strukturen* redet, dann meint man damit heutzutage fast immer Mengen mit weiteren „Zutaten“. In Abschnitt 5 waren die Zutaten Relationen. In diesem Kapitel werden es innere Verknüpfungen sein.

Wir werden ab jetzt häufiger Beweise sehen. Nach meiner Erfahrung kann man die Aussagen so besser verstehen und sie sich besser merken. Außerdem sind die meisten Beweise, die wir brauchen, nicht besonders umfangreich.

7. Eigenschaften von inneren Verknüpfungen

Aufgabe 7.1. Im Internet kursieren Aufgaben wie $6 \div 2(1+2)$, über die sich viele Menschen in den Haaren liegen. Was kommt denn bei dieser Aufgabe heraus?

Zur Erinnerung: Eine innere Verknüpfung auf einer Menge M ist eine Funktion von $M \times M$ nach M. „Typische“ Beispiele, die auch die Vorbilder für die Themen dieses Kapitels sind, sind Addition und Multiplikation von Zahlen, also z. B.

$$: \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (m,n) \mapsto m+n \end{cases} \quad \text{oder} \quad : \begin{cases} \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \\ (r,s) \mapsto r \cdot s \end{cases} .$$

Wir werden für solche Funktionen in diesem Kapitel immer die sogenannte *Infixnotation* verwenden, d. h., wenn im Folgenden f eine innere Verknüpfung ist, dann schreiben wir für die Funktionswerte $x\,f\,y$ statt $f(x,y)$. Allerdings bezeichnen wir solche Funktionen dann nicht mit Buchstaben wie f, g und h, sondern mit Operatorsymbolen wie $\oplus$ oder $\otimes$.

Infixnotation

Definition

Eine innere Verknüpfung $\otimes$ auf einer Menge M heißt **assoziativ**, wenn

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

für alle $a, b, c \in M$ gilt.

Wir fangen mit einem Beispiel für eine Verknüpfung an, die *nicht* assoziativ ist:

$$\otimes\colon \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (m,n) \mapsto m(n+1) \end{cases} \tag{7.1}$$

Unter anderem haben wir dann

$$(1 \otimes 2) \otimes 3 = (1 \cdot (2+1)) \otimes 3 = 3 \otimes 3 = 3 \cdot (3+1) = 12 \quad \text{und}$$
$$1 \otimes (2 \otimes 3) = 1 \otimes (2 \cdot (3+1)) = 1 \otimes 8 = 1 \cdot (8+1) = 9$$

und wie immer reicht ein Gegenbeispiel.

Verknüpfungen, die assoziativ sind, sind die übliche Addition und Multiplikation von Zahlen.[1] Es gilt also $a+(b+c) = (a+b)+c$ und $a(bc) = (ab)c$ und Sie haben sich darüber vielleicht noch nie Gedanken gemacht. Das Beispiel davor hat aber gezeigt, dass so etwas keine Selbstverständlichkeit ist. Innere Verknüpfungen sind immer nur für *zwei* Argumente definiert. Wenn man es mit mehr als zwei Argumenten zu tun hat, muss man Klammern setzen, um festzulegen, was zuerst berechnet werden soll. Nur dann, wenn eine Verknüpfung assoziativ ist, kann man die Klammern weglassen. Es ist also OK, wenn man $3 \cdot 7 \cdot 5$ schreibt,[2] aber im obigen Beispiel wäre $3 \otimes 7 \otimes 5$ ein undefinierter Ausdruck gewesen.

Aufgabe 7.2. Welche der folgenden Verknüpfungen sind assoziativ?

(i) $(a,b) \mapsto a^b$ für $a, b \in \mathbb{N}$
(ii) $(x,y) \mapsto x \oplus y = (x+1)(y+1)$ für $x, y \in \mathbb{N}$
(iii) $(x,y) \mapsto x \otimes y = 2xy$ für $x, y \in \mathbb{N}$
(iv) $(x,y) \mapsto x/y$ für $x, y \in \mathbb{Q} \setminus \{0\}$
(v) $(M,N) \mapsto M \cap N$ für $M, N \subseteq \mathbb{N}$
(vi) $(f,g) \mapsto f \circ g$ für $f, g \in \mathbb{N}^{\mathbb{N}}$

Aufgabe 7.3. Geben Sie das hier in PYTHON ein:[3]

[1] Kann man das beweisen? Ja, aber dafür müsste man ganz tief in den Keller der Grundlagenmathematik hinabsteigen. Wir belassen es hier dabei, dass wir das einfach glauben bzw. es aus der Schule „wissen“.

[2] Wenn Sie so etwas im Kopf ausrechnen, fangen Sie aber sicher trotzdem immer mit zwei der drei Zahlen an, weil Sie das kleine Einmaleins nicht für Produkte von drei Faktoren auswendig gelernt haben. Auch die ALU und die FPU Ihres Rechners können immer nur zwei Argumente verknüpfen.

[3] Oder probieren Sie es mit einer anderen Programmiersprache. In jeder Sprache, die sich an den Standard IEEE 754 hält, werden Sie vergleichbare Ergebnisse bekommen.

```
(1.111111111111111+0.000000000000001)+0.000000000000001
1.111111111111111+(0.000000000000001+0.000000000000001)
```

Was kann man daraus schließen?

Aufgabe 7.4. Geben Sie die folgenden beiden Ausdrücke aus der Lösung von Aufgabe 7.2 in PYTHON ein (oder probieren Sie das mit einer anderen Programmiersprache):

```
2**3**2   # ** ist der Operator für die Potenz in Python
1/2/3
```

Was kann man daraus schließen?

Wie in Aufgabe 7.4 muss man sich auch in der Mathematik bei manchen Ausdrücken für eine Reihenfolge entscheiden, wenn keine durch Klammern vorgegeben wird. Dabei gilt zunächst einmal immer die bekannte und schon am Anfang des Skripts erwähnte Regel "Punkt- vor Strichrechnung", aus der folgt, dass Multiplikation und Division Vorrang vor Addition und Subtraktion haben. Daher wird so etwas wie $4+3\cdot 2$ wie $4+(3\cdot 2)=10$ interpretiert. Zudem hat Potenzierung eine noch höhere Priorität. $5\cdot 2^3$ ist deshalb 40 und -2^4 ist -16 und nicht 16.

linksassoziativ

rechtsassoziativ

Stehen hintereinander mehrere gleichwertige Operatoren ohne Klammern, dann werden diese in der Regel als *linksassoziativ* behandelt, womit gemeint ist, dass von links nach rechts ausgewertet wird. $10-5+2$ würde man also wie $(10-5)+2$ und $1/2/3$ wie $(1/2)/3$ behandeln.[4] Man sollte so etwas aber besser ganz vermeiden. Eine Ausnahme von der Linksassoziativität bildet die Potenz, die als *rechtsassoziativ* angesehen wird: 2^{3^2} wird als $2^{(3^2)}$ ausgewertet.

Aufgabe 7.5. Was kommt denn nun bei Aufgabe 7.1 heraus?

Definition

Eine innere Verknüpfung $\otimes$ auf einer Menge M heißt **kommutativ**, wenn

$$a\otimes b = b\otimes a$$

für alle $a, b\in M$ gilt.

Ein Beispiel für eine Verknüpfung, die *nicht* kommutativ ist, ist $\otimes$ aus (7.1): $2\otimes 3=8$, $3\otimes 2=9$. Addition und Multiplikation sind aber kommutativ.

Aufgabe 7.6. Welche der Verknüpfungen aus Aufgabe 7.2 sind kommutativ?

Aufgabe 7.7. Die *symmetrische Differenz* zweier Mengen A und B ist definiert als

symmetrische Differenz $A\triangle B$

$$A\triangle B = (A\setminus B)\cup(B\setminus A) = (A\cup B)\setminus(A\cap B). \tag{7.2}$$

[4] Man könnte an dieser Stelle noch erwähnen, dass es natürlich egal ist, ob man für die Division das Zeichen / oder das in der Schule gebräuchlichere : verwendet.

Machen Sie sich mit Mengendiagrammen klar, dass diese Verknüpfung assoziativ und kommutativ ist und dass die beiden alternativen Definitionen aus (7.2) dieselbe Menge beschreiben.

Vorsichtshalber sei an dieser Stelle noch angemerkt, dass zwar klar sein sollte, was gemeint ist, wenn man sagt, dass $\cap$, $\cup$ oder $\triangle$ assoziativ oder kommutativ sind, dass es sich aber rein technisch nur dann um innere Verknüpfungen handelt, wenn man wie in Punkt (v) von Aufgabe 7.2 eine *Menge* angibt, auf der die Verknüpfung definiert ist. Siehe dazu die Bemerkungen über naive und axiomatische Mengenlehre am Ende des ersten Kapitels.

Definition

Ist $\otimes$ eine innere Verknüpfung auf einer Menge M, so nennt man $e \in M$ ein **neutrales Element** für $\otimes$, wenn

$$e \otimes a = a = a \otimes e$$

für alle $a \in M$ gilt.

Die „typischen“ Beispiele für neutrale Elemente sind die Null für die Addition und die Eins für die Multiplikation. Für $\otimes$ aus (7.1) gibt es hingegen *kein* neutrales Element. Damit immer $a \otimes e = a$ gilt, müssten wir $e = 0$ wählen, aber $0 \otimes a$ ist immer 0 und im Allgemeinen nicht a.[5]

Aufgabe 7.8. Welche der Verknüpfungen aus Aufgabe 7.2 haben neutrale Elemente?

Bei den Beispielen, bei denen wir neutrale Elemente gefunden haben, haben wir immer nur eines gefunden. Das war kein Zufall (und man kann daher auch von *dem* neutralen Element für eine bestimmte Verknüpfung sprechen).

Lemma 7.1

Ist $\otimes$ eine innere Verknüpfung auf M und e ein neutrales Element für $\otimes$, dann ist e das einzige Element von M mit dieser Eigenschaft.

Beweis. Was nun folgt, ist einer der wohl einfachsten Beweise in der gesamten Mathematik. Seien e und e' neutrale Elemente für $\otimes$. Dann gilt $e = e \otimes e' = e'$. Dabei gilt die erste Gleichheit, weil e' neutrales Element ist, und die zweite, weil e neutrales Element ist. ■

Ist Ihnen das schwarze Quadrat am rechten Rand aufgefallen? Damit wird in der Mathematik das Ende eines Beweises markiert. Die Tradition, explizit auszusprechen, dass ein Beweis beendet ist, ist über zweitausend Jahre alt. Das schwarze Quadrat – scherzhaft auch *Grabstein* genannt – wurde erst 1950 von Paul Halmos eingeführt, ist inzwischen jedoch sehr weit verbreitet.

linskneutral
rechtsneutral

An diesem Beweis sieht man übrigens nebenbei, dass es ausreicht, wenn e nur *linksneutral* und e' nur *rechtsneutral* ist, d. h., wenn lediglich $e \otimes a = a$ und $a \otimes e' = a$

[5] In der fortgeschrittenen Algebra würde man von einem *rechtsneutralen* Element sprechen, aber das werden wir nicht benötigen.

für alle $a \in M$ gilt. Man erhält dann trotzdem, dass $e = e'$ gelten muss, und hat damit ein (beidseitig) neutrales Element gefunden.

Definition

Sei $\otimes$ eine innere Verknüpfung auf einer Menge M, e das neutrale Element für $\otimes$ und $a \in M$. Ein Element b von M mit

$$a \otimes b = e = b \otimes a$$

nennt man ein **inverses Element zu** a (bezüglich $\otimes$) oder einfach **invers zu** a.

Man beachte, dass nach dieser Definition das neutrale Element immer invers zu sich selbst ist. Interessant wird die Sache also erst, wenn es auch für andere Elemente Inverse[6] gibt. Dabei kann die Menge, auf der die Verknüpfung definiert ist, durchaus eine Rolle spielen:

- Für die Addition auf $\mathbb{N}$ gibt es nur zum neutralen Element 0 ein Inverses. Für die Addition auf $\mathbb{Z}$ hat hingegen jede ganze Zahl a ein Inverses, nämlich $-a$.
- Für die Multiplikation auf $\mathbb{N}$ hat nur das neutrale Element 1 ein Inverses. Für die Multiplikation auf $\mathbb{Q}$ hat hingegen jeder Bruch $a/b \neq 0$ ein Inverses, nämlich b/a. Und die Null hat natürlich kein Inverses, weil es keine Zahl gibt, die mit null multipliziert eins ergibt.

Aufgabe 7.9. Wie sieht es bei der Multiplikation mit inversen Elementen aus, wenn sie auf $\mathbb{Z}$ definiert ist?

Aufgabe 7.10. Wenn man $(x, y) \mapsto x \otimes y = 2xy$ als Verknüpfung auf $\mathbb{Q}$ definiert, dann hat diese Verknüpfung das neutrale Element $1/2$, wie wir uns schon in Aufgabe 7.8 überlegt haben. Wie steht es mit inversen Elementen?

Aufgabe 7.11. Wenn b invers zu a ist, gibt es dann auch ein inverses Element zu b?

Aufgabe 7.12. Wie vereinfachen sich die Definitionen für das neutrale Element und für die inversen Elemente, wenn die Verknüpfung kommutativ ist?

8. Gruppen

Die Methoden der Gruppentheorie haben inzwischen fast alle Bereiche der Mathematik durchdrungen und die Entwicklung dieses Begriffs kann im Nachhinein wohl als einer der wichtigsten konzeptionellen Fortschritte in der Mathematik in Richtung Abstraktion bezeichnet werden. Wir haben leider nicht die Zeit, ausführlich auf die historische Motivation einzugehen. Eine allgemeinverständliche Darstellung finden Sie in den ersten circa 25 Minuten des zweiteiligen Videos "Der längste Beweis aller Zeiten".

[6] Wie Sie sehen, benutzt man den Begriff auch als Substantiv.

Definition

Ist M eine Menge und $\otimes$ eine innere Verknüpfung auf M, dann nennt man das Paar $(M,\otimes)$ eine **Gruppe**, wenn die folgenden drei Bedingungen erfüllt sind:

(i) $\otimes$ ist assoziativ.

(ii) Es gibt ein neutrales Element für $\otimes$.

(iii) Zu jedem Element von M gibt es bezüglich $\otimes$ ein inverses Element.

Sind zumindest die ersten beiden Bedingungen erfüllt, spricht man von einem **Monoid**. Ist wenigstens die erste Bedingung erfüllt, so handelt es sich um eine **Halbgruppe**. Ist $\otimes$ zusätzlich kommutativ, so nennt man die Struktur **kommutativ** oder **abelsch**.[7]

Es würde rein technisch reichen, nur $\otimes$ als die Gruppe zu bezeichnen, weil man aus $\otimes$ ja M rekonstruieren kann. Üblicherweise macht man es jedoch sogar andersherum und nennt die Grundmenge M die Gruppe, wenn aus dem Kontext hervorgeht, welche Verknüpfung gemeint ist.

Zunächst ein paar Beispiele aus der Welt der Zahlen, die sich größtenteils bereits aus den Überlegungen des letzten Abschnitts ergeben.

- Die natürlichen Zahlen bilden mit der Addition ein Monoid mit dem neutralen Element 0. Und mit der Multiplikation bilden sie auch ein Monoid mit dem neutralen Element 1. Weil es sich um Monoide handelt, handelt es sich „erst recht“ um Halbgruppen. In beiden Fällen hat jedoch keine Zahl außer dem neutralen Element inverse Elemente, es handelt sich also nicht um Gruppen.
- Wenn man die Addition stattdessen auf $\mathbb{Z}$ betrachtet, hat man eine Gruppe, weil man nun immer Inverse findet. Bei der Multiplikation hat man es aber nach wie vor nur mit einem Monoid zu tun.
- Geht man über zu $\mathbb{Q}$, so liefert die Addition immer noch eine Gruppe. Durch die Multiplikation erhält man nun auch eine Gruppe, wenn man statt $\mathbb{Q}$ als Grundmenge $\mathbb{Q}\setminus\{0\}$ nimmt. Nur durch das Entfernen der Null kann man erreichen, dass jedes Element ein Inverses hat.
- Schließlich bilden auch die reellen Zahl mit der Addition eine Gruppe und mit der Multiplikation bildet $\mathbb{R}\setminus\{0\}$ eine.

Bei all diesen Überlegungen muss man natürlich darauf achten, dass die jeweiligen Operationen auch wirklich innere Verknüpfungen sind: Die Addition zweier natürlicher Zahlen ergibt wieder eine natürliche Zahl, die Multiplikation zweier von null verschiedener rationaler Zahlen liefert wieder eine von null verschiedene rationale Zahl und so weiter.

Aufgabe 8.1. In welchen der folgenden Fälle ist $(M,\otimes)$ eine Gruppe oder ein Monoid? Überprüfen Sie jeweils alle Eigenschaften und begründen Sie negative Antworten durch konkrete Gegenbeispiele.

(i) $M=\{x\in\mathbb{R}: x\geq 0\}$ mit $x\otimes y=\sqrt{x^2+y^2}$

(ii) $M=\mathbb{Z}$ mit $x\otimes y=x+2y$

[7] Benannt nach dem Norweger Niels Henrik Abel.

(iii) $M = \mathbb{N}$ mit $x \otimes y = \begin{cases} x & x \geq y \\ y & x < y \end{cases}$

Aufgabe 8.2. Wir definieren eine Verknüpfung $\oplus$ auf $\mathbb{R}^2$ durch[8]

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Überzeugen Sie sich, dass es sich um eine Gruppe handelt und geben Sie an, wie das neutrale Element bzw. die inversen Elemente aussehen. Ist diese Gruppe abelsch?

Aufgabe 8.3. Bildet die Menge $M = \{q \in \mathbb{Q} : 0 < |q| \leq 1\}$ mit der üblichen Multiplikation ein Monoid oder eine Gruppe?

Aufgabe 8.4. Bildet die Menge $\mathbb{R}^+ = \{q \in \mathbb{R} : q > 0\}$, also das Intervall $(0, \infty)$, mit der üblichen Addition bzw. Multiplikation ein Monoid oder eine Gruppe? $\mathbb{R}^+$

Aufgabe 8.5. Bildet die Menge $\mathscr{P}(\mathbb{N})$ mit der Vereinigung eine Gruppe oder ein Monoid? Und was ist mit dem Durchschnitt?

⋆**Aufgabe 8.6.** Wenn man die Bedingungen (ii) und (iii) in der Definition einer Gruppe durch die folgenden, schwächeren Bedingungen ersetzt, beschreibt man damit trotzdem immer noch eine Gruppe:

(ii') Es gibt ein linksneutrales Element e für $\otimes$.

(iii') Zu jedem Element a von M gibt es bezüglich $\otimes$ ein *linksinverses* Element b. Damit ist gemeint, dass $b \otimes a = e$ gilt. linksinvers

Können Sie begründen, warum das stimmt? (Das ist ein bisschen Knobelei, aber nicht wirklich schwer. Man muss lediglich aufpassen, dass man nicht etwas verwendet, das gar nicht vorausgesetzt wurde. Beispielsweise kann man Lemma 7.1 nicht verwenden, solange nicht klar ist, dass e auch rechtsneutral ist.)

Es gibt auch *endliche* Gruppen. Deren Erforschung hat sich im 20. Jahrhundert sogar als besonders schwierig und aufwendig erwiesen. Aber keine Angst, wir schauen uns nur ein paar einfache Beispiele an.

Die einfachste Gruppe, die es überhaupt gibt, besteht nur aus einem Element. Um welches Element es sich handelt, spielt keine Rolle. Nennen wir es einfach e, denn es muss ja in Ermangelung anderer Alternativen das neutrale Element sein. Die Grundmenge ist also $M = \{e\}$ und die Verknüpfung, die wir $\otimes$ nennen werden, steht damit auch fest: $e \otimes e$ muss e sein und damit ist der Definitionsbereich $M \times M$ bereits erschöpft. Es sollte hoffentlich klar sein, dass dieses seltsame Konstrukt alle Bedingungen für eine Gruppe erfüllt. Das ist alles trivial und darum nennt man diese Gruppe auch die *triviale Gruppe*. triviale Gruppe

Aufgabe 8.7. Was ist denn mit unserer Freundin, der leeren Menge, die doch alle möglichen Eigenschaften hat? Erhält man mit der als Grundmenge nicht eine Gruppe, die noch kleiner als die triviale ist?

[8] Wenn Sie in der Schule mit Vektoren zu tun hatten, sollte Ihnen das bekannt vorkommen.

In Gruppen sind nicht nur die neutralen, sondern auch die inversen Elemente eindeutig bestimmt.

Lemma 8.1 Ist $(M, \otimes)$ eine Gruppe, dann gibt es zu jedem Element von M genau ein inverses Element.

⋆**Aufgabe 8.8**. Der Beweis für Lemma 8.1 verläuft analog zu dem für die Eindeutigkeit des neutralen Elements (Lemma 7.1). Probieren Sie's mal selbst!

Aufgabe 8.9. Geben Sie für jedes der Gleichheitszeichen in (L-2) an, warum die jeweilige Umformung erlaubt ist.

Konvention Man schreibt abstrakte Gruppen oft *multiplikativ*. Damit ist gemeint, dass man die Verknüpfung mit $\cdot$ bezeichnet und sie häufig auch weglässt, dass man also ab statt $a \cdot b$ schreibt. Das neutrale Element wird dann in der Regel 1 genannt und das zu a inverse Element schreibt man a^{-1} oder (seltener) $1/a$. Man schreibt außerdem abkürzend a^2 für aa, a^3 für aaa und so weiter.[9] Abelsche Gruppen schreibt man auch *additiv*: Als Verknüpfungszeichen wird dann + verwendet, für das neutrale Element das Symbol 0 und für das zu a inverse Element die Schreibweise $-a$.

a^{-1} $1/a$

$-a$

Bei dieser Konvention ist das Wort *abstrakt* hervorzuheben. Dass man für ein Element 0 oder 1 schreibt, heißt *nicht*, dass es sich um die gleichnamige *Zahl* handelt, sondern lediglich, dass es in der jeweiligen Gruppe eine bestimmte „Sonderrolle" einnimmt. Wir wenden diese Konvention gleich für eine wichtige generelle Aussage über Gruppen an.

Aufgabe 8.10. Man kann die Aussage aus Aufgabe 8.2 verallgemeinern und dabei gleich diese Konvention verinnerlichen: Sind G_1 bis G_n Gruppen, dann wird auf der Menge $G = G_1 \times \cdots \times G_n$ durch

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 \cdot y_1, \ldots, x_n \cdot y_n) \tag{8.1}$$

eine innere Verknüpfung definiert, durch die man eine Gruppe erhält.[10] Sind zudem alle G_i abelsch, dann ist auch G abelsch. Stellen Sie sicher, dass Sie verstanden haben, was hier behauptet wird, und begründen Sie die Korrektheit der Aussage, indem Sie die Argumentation aus Aufgabe 8.2 kopieren.

Aufgabe 8.11. Auch Aufgabe 8.10 kann man noch einmal verallgemeinern, nämlich so: Ist G eine Gruppe und M irgendeine Menge, dann wird auf der Funktionsmenge G^M durch die Verknüpfung $f \cdot g$ eine Gruppe definiert.[11] Überprüfen Sie die Assoziativität und geben Sie das neutrale Element an.

[9] Dabei ist zu beachten, dass diese Form der „Exponentiation" keine neue Operation, sondern lediglich eine Abkürzung ist. Sie ergibt in diesem Zusammenhang nur Sinn, wenn der Exponent eine natürliche Zahl ist. Dann passt aber auch a^0 für 1 und $a^1 = a$ und es gilt $a^{m+n} = a^m a^n$.

direktes Produkt

[10] Man nennt diese Gruppe das *direkte Produkt* der G_i.

[11] Hier ist die Multiplikation von Funktionen im Sinne der Definition auf Seite 87 gemeint. Wie in der dortigen Fußnote 27 bereits angekündigt wurde, sind die Funktionswerte nun keine „Zahlen" im klassischen Sinne mehr.

Satz 8.2

Ist G eine Gruppe, dann kann man für alle $a, b \in G$ die beiden Gleichungen $ax = b$ und $ya = b$ eindeutig nach x bzw. y auflösen. Die Lösungen sind $x = a^{-1}b$ und $y = ba^{-1}$. Ist die Gruppe abelsch, dann sind die beiden Lösungen offenbar identisch.

Beweis. Dass $a^{-1}b$ die erste Gleichung löst, bestätigt man einfach durch Einsetzen. Dass es die einzige Lösung ist, ergibt sich durch Multiplikation der Gleichung mit a^{-1}. Für die zweite Gleichung argumentiert man analog. Das war's schon.

Zu beachten ist hier lediglich, dass wir das Zeichen $\cdot$ nicht fälschlicherweise so interpretieren dürfen, als wäre die Verknüpfung kommutativ. Wenn wir beispielsweise $ax = b$ mit a^{-1} multiplizieren, dann müssen wir „von links" multiplizieren; und zwar *auf beiden Seiten*, denn es soll dort ja dasselbe gemacht werden und Multiplikation von links ist evtl. nicht dasselbe wie Multiplikation von rechts. ■

Korollar 8.3

Ist $(G, \cdot)$ eine Gruppe und $a \in G$, dann sind die Abbildungen $x \mapsto ax$ und $x \mapsto xa$ bijektive Funktionen von G auf G.

Beweis. Die Surjektivität von $x \mapsto ax$ folgt daraus, dass man die Gleichung $ax = b$ für jedes $b \in G$ lösen kann. Die Injektivität folgt daraus, dass die Lösung eindeutig bestimmt ist. Beides liefert Satz 8.2. Für $x \mapsto xa$ verläuft der Beweis analog mit der anderen Gleichung aus dem Satz. ■

Korollar 8.3 hilft bei der Konstruktion weiterer Gruppen. Die nach der trivialen nächstgrößere Gruppe könnte eine mit zwei Elementen sein. Schreiben wir die Grundmenge als $G = \{1, a\}$. Die Verknüpfung können wir als *Verknüpfungstabelle* aufschreiben:[12]

Verknüpfungstabelle

$\cdot$	1	a
1	1	a
a	a	1

Mit etwas Nachdenken sieht man, dass die Tabelle so wie oben aussehen *muss*. Weil 1 das neutrale Element ist, ergibt sich zwangsläufig, was in der ersten Zeile und Spalte stehen muss. Und Korollar 8.3 besagt, dass es in keiner Zeile oder Spalte zu Dopplungen kommen darf. Es muss somit $a \cdot a = 1$ gelten, anders geht es nicht. Damit ist klar, dass a zu sich selbst invers ist.

Aufgabe 8.12. Ist damit auch schon klar, dass wir eine Gruppe vor uns haben?

Aufgabe 8.13. Die Beispielgruppe mit zwei Elementen ist abelsch. Wie kann man einer Verknüpfungstabelle allgemein ansehen, dass die Verknüpfung kommutativ ist?

Aufgabe 8.14. Erinnert Sie diese Gruppe mit zwei Elementen an etwas?

[12] Das ist natürlich so gemeint, dass im Schnittpunkt der Zeile zum Element x und der Spalte zum Element y der Wert $x \cdot y$ stehen soll.

Aufgabe 8.15. Wir haben nun gelernt, dass es nur eine Gruppe mit zwei Elementen gibt. Es gibt auch nur eine mit drei Elementen. Erstellen sie eine entsprechende Verknüpfungstabelle. Dabei werden Sie feststellen, dass Ihnen gleichsam „aufgezwungen“ wird, welche Einträge Sie machen müssen.

Aufgabe 8.16. In der Lösung von Aufgabe 8.15 steht, dass die Verknüpfungstabelle einer Gruppe nach ähnlichen Regeln wie Sudoku befüllt werden muss. Wie kann man diese Regeln noch etwas präziser formulieren?

Aufgabe 8.17. Was kann man über die Positionen des neutralen Elements in einer Verknüpfungstabelle sagen?

Aufgabe 8.18. Wenn man außer einer Verknüpfungstabelle nichts hat, kann man die Assoziativität nur durch systematisches Probieren nachprüfen. Angenommen, Sie würden ein Computerprogramm schreiben, das alle möglichen Fälle für die Gruppe aus Aufgabe 8.15 durchgeht. Wie viele Fälle wären das?

In der Gruppentheorie würde man sagen, dass die oben definierte Gruppe mit den zwei Elementen 1 und a die *einzige* Gruppe mit zwei Elementen ist. Diese Sichtweise liegt einerseits nahe, weil wir gar keine andere Wahl für die Verknüpfung hatten, andererseits klingt es aber auch falsch, weil in Aufgabe 8.14 mehrere *andere* Gruppen mit zwei Elementen vorkamen. Inwieweit diese Gruppen „nicht wirklich anders“ sind, lässt sich mit den nun folgenden Begriffen beschreiben.

Definition

Seien $(G,\oplus)$ und $(H,\otimes)$ Gruppen.[13] Eine Abbildung $f\colon G\to H$ heißt **Gruppenhomomorphismus**, wenn $f(a\oplus b)=f(a)\otimes f(b)$ für alle $a,b\in G$ gilt. Wenn aus dem Kontext hervorgeht, dass es um Gruppen geht, spricht man auch kürzer einfach von einem **Homomorphismus**.

Man kann das so interpretieren, dass f die Gruppenstruktur von G derart nach H überträgt, dass sie mit der Struktur am Ziel übereinstimmt.

Eine Reihe von Beispielen für diesen neuen Begriff:

- Es ist immer eine gute Idee, zunächst mit ganz einfachen Beispielen anzufangen. Wenn G irgendeine Gruppe ist und $\{e\}$ die triviale Gruppe, dann ist die Abbildung, die alle Elemente von G konstant auf e abbildet, ein Homomorphismus.
- Ein ebenso einfaches Beispiel ist die Identität id_G, wenn $(G,\oplus)$ und $(H,\otimes)$ dieselbe Gruppe sind.
- Etwas weniger banal ist die Abbildung von $(\mathbb{Z},+)$ nach $(\mathbb{Q}\setminus\{0\},\cdot)$, die n auf 2^n abbildet.

Aufgabe 8.19. Schreiben Sie für diese Beispiele jeweils die Bedingung dafür auf, dass es sich bei den genannten Abbildungen um Homomorphismen handelt, und überzeugen Sie sich, dass die Bedingungen erfüllt sind.

[13] Wir verwenden hier aus didaktischen Gründen wieder Zeichen wir $\oplus$ und $\otimes$, um zu verdeutlichen, dass es typischerweise um verschiedene Verknüpfungen gehen wird.

Lemma 8.4 Jeder Homomorphismus von G nach H bildet das neutrale Element von G auf das neutrale Element von H ab. Ferner ist für jedes $a \in G$ das Bild von a^{-1} invers zum Bild von a.

Beweis. Sei f der Homomorphismus. Nach Definition muss für $a \in G$ einerseits $f(a) = f(1 \cdot a) = f(1) \cdot f(a)$ gelten. Andererseits hat die Gleichung $f(a) = y \cdot f(a)$ nach Satz 8.2 eine eindeutige Lösung in H und diese Lösung ist offenbar $y = 1$. Also muss $f(1) = 1$ gelten.[14] Weiter gilt $1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$. Erneut mit Satz 8.2 folgt $f(a^{-1}) = f(a)^{-1}$. ∎

Aufgabe 8.20. Sei $f : \mathbb{R} \to \mathbb{R}$ durch $f(x) = \lfloor x \rfloor$ definiert. Begründen Sie mit einem konkreten Gegenbeispiel, dass f kein Homomorphismus von $(\mathbb{R}, \cdot)$ nach $(\mathbb{R}, \cdot)$ ist.

Aufgabe 8.21. Wenn $(G, \oplus)$ die Gruppe aus Aufgabe 8.2 ist und die Funktion f auf G durch $f(x, y) = x$ definiert wird, was ist dann der Wertebereich von f und welche Verknüpfung muss man auf diesem Wertebereich definieren, damit f ein Homomorphismus ist?

Sowohl die Menge der rationalen Zahlen als auch die Menge der rellen Zahlen bilden mit der Addition jeweils eine Gruppe. Die Grundmenge der einen Gruppe ist eine Teilmenge der anderen Grundmenge und die Verknüpfungen sind in gewissem Sinne identisch, obwohl es sich rein technisch um zwei unterschiedliche Funktionen handelt. Das formalisieren wir nun.

Definition Man nennt eine Gruppe $(G, \oplus)$ eine **Untergruppe** der Gruppe $(H, \otimes)$, wenn G eine Teilmenge von H und $\oplus$ die Restriktion von $\otimes$ auf $G \times G$ ist.

Das klingt komplizierter, als es ist. Beispielsweise ist $(\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Q}, +)$, wobei mit dem Zeichen + einmal eine Abbildung von $\mathbb{Z} \times \mathbb{Z}$ nach $\mathbb{Z}$ und einmal eine von $\mathbb{Q} \times \mathbb{Q}$ nach $\mathbb{Q}$ gemeint ist.

In der Regel nimmt man es mit der Sprache nicht so genau: Man bezeichnet oft nur die Menge G als die Untergruppe und verwendet wie im Beispiel eben in beiden Gruppen dasselbe Verknüpfungszeichen. Entscheidend ist, dass sich durch die Einschränkung der Verknüpfung wieder eine Gruppe ergeben muss. Das heißt insbesondere, dass $a \otimes b = a \oplus b$ für alle $a, b \in G$ wieder ein Element von G sein muss.[15] Außerdem muss das neutrale Element von G wegen der Eindeutigkeit das neutrale Element von H sein.

Aufgabe 8.22. Unabhängig davon, wie eine Gruppe $(G, \cdot)$ konkret aussieht, bieten sich zwei *triviale Untergruppen* an. Welche sind es?

triviale Untergruppen

[14] Sie haben bemerkt, dass in der Gleichung $f(1) = 1$ die Eins links für das neutrale Element von G und die Eins rechts für das neutrale Element von H steht, oder? Auch das Verknüpfungszeichen $\cdot$ bedeutet mal dies und mal das. Wir verwenden dieselben Symbole für G und H und verlassen uns darauf, dass aus dem Kontext jeweils ersichtlich ist, in welcher Gruppe wir uns gerade befinden. Das ist eine „Nachlässigkeit“, die in der Algebra weitverbreitet ist.

[15] Man sagt dann auch, dass G *abgeschlossen* bezüglich $\otimes$ ist.

abgeschlossen

Aufgabe 8.23. Ist $\mathbb{N}$ eine Untergruppe von $(\mathbb{Z},+)$?

Aufgabe 8.24. Ist die Menge der ungeraden ganzen Zahlen eine Untergruppe von $(\mathbb{Z},+)$? Ist die Menge der geraden ganzen Zahlen eine Untergruppe von $(\mathbb{Z},+)$?

Aufgabe 8.25. Ist $\{q \in \mathbb{Q} : 0 < |q| < 1\}$ eine Untergruppe von $(\mathbb{Q}\setminus\{0\},\cdot)$?

Aufgabe 8.26. Fällt Ihnen eine Untergruppe von $(\mathbb{R}\setminus\{0\},\cdot)$ ein, die nicht trivial ist? Gehen Sie ggf. die Aufgaben aus diesem Kapitel noch einmal durch.

Aufgabe 8.27. Auf der Menge $G = \{1, a, b, c\}$ wird durch

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

eine Gruppe definiert. Wie viele nichttriviale Untergruppen können Sie finden?

Das folgende Lemma gibt ein einfaches Kriterium dafür an, wann man es mit einer Untergruppe zu tun hat.

Lemma 8.5

Eine nichtleere Teilmenge G von H ist genau dann eine Untergruppe von H, wenn $ab^{-1} \in G$ für alle $a, b \in G$ gilt.

Beweis. Die eine Richtung dieser Äquivalenz ist einfach: Ist G eine Gruppe, dann müssen für $a, b \in G$ natürlich b^{-1} und damit auch ab^{-1} Elemente von G sein. Gehen wir also nun umgekehrt davon aus, dass G eine Teilmenge von H mit dieser Eigenschaft ist. Wegen $G \neq \emptyset$ gibt es mindestens ein Element $a \in G$ und nach Voraussetzung ist dann auch $1 = aa^{-1}$ ein Element von G. Damit ist aber für jedes $b \in G$ auch $1 \cdot b^{-1} = b^{-1}$ Element von G. Da die Assoziativität von H „vererbt“ wird, fehlt nur noch, dass G abgeschlossen bezüglich $\cdot$ ist: Sind $a, b \in G$, dann wissen wir bereits, dass $b^{-1} \in G$ gilt, und es folgt $ab = a(b^{-1})^{-1} \in G$. ■

Wir wenden dieses Lemma gleich an, um die nächste Aussage zu beweisen:

Lemma 8.6

Ist f ein Homomorphismus von G nach H, dann ist $f[G]$ eine Untergruppe von H und $f^{-1}[\{1\}]$ eine Untergruppe von G.

Beweis. Sind a und b Elemente von $f[G]$, dann gibt es c und d aus G mit $f(c) = a$ und $f(d) = b$. Mit Lemma 8.4 folgt

$$ab^{-1} = f(c)f(d)^{-1} = f(c)f(d^{-1}) = f(cd^{-1}) \in f[G].$$

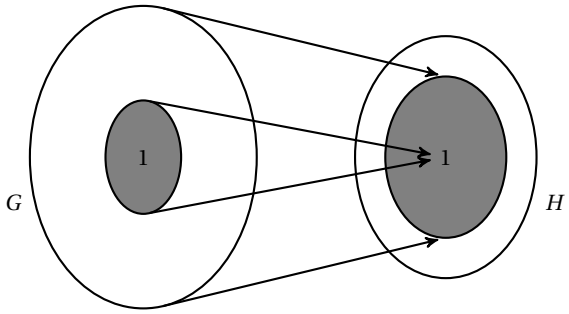
Sind andererseits a und b Elemente von $K = f^{-1}[\{1\}]$, dann gilt $f(a) = f(b) = 1$ und wir haben

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1 \cdot 1^{-1} = 1 \cdot 1 = 1$$

und damit $ab^{-1} \in K$. ■

Die Menge $f^{-1}[\{1\}]$ wird auch als *Kern* von f bezeichnet. In der folgenden Skizze wird durch Pfeile schematisch angedeutet, was f macht. Alle vier Ellipsen sind Gruppen. Die rechte graue Ellipse ist $f[G]$, die linke graue Ellipse ist der Kern von f.

Kern



⋆**Aufgabe 8.28**. Man kann den Kern von f als „Maß für die Injektivität“ von f betrachten. Das werden wir hier nicht weiter ausarbeiten, aber versuchen Sie zumindest einmal, die folgende Aussage zu beweisen: Ein Homomorphismus f ist genau dann injektiv, wenn der Kern von f die Menge $\{1\}$ ist.

⋆**Aufgabe 8.29**. Sei U eine Untergruppe von G. Begründen Sie, warum durch $a^{-1}b \in U$ für $a, b \in G$ eine Äquivalenzrelation auf G definiert wird.

⋆**Aufgabe 8.30**. Begründen Sie, dass die Äquivalenzklassen zur Relation aus Aufgabe 8.29 die Form $aU = \{au : u \in U\}$ für ein $a \in G$ haben.

aU

Ist G eine endliche Gruppe, so nennt man $|G|$ auch die **Ordnung** der Gruppe.

Definition

Satz von Lagrange
Ist U Untergruppe einer endlichen Gruppe G, dann ist die Ordnung von U ein Teiler der Ordnung von G.

Satz 8.7

Beweis. Die Mengen aU aus Aufgabe 8.30 nennt man *Nebenklassen*[16] von U. Nach Satz 5.2 sind für $a, b \in G$ die Nebenklassen aU und bU entweder identisch oder disjunkt. Außerdem wird durch $au \mapsto bu$ offenbar eine Bijektion von aU auf bU definiert. Nach Satz 6.3 haben daher alle Nebenklassen dieselbe Mächtigkeit. Da $U = 1U$ eine der Nebenklassen ist, wird G somit in gleich große „Portionen“ der Größe $|U|$ aufgeteilt. ■

Nebenklasse

Damit folgt beispielsweise sofort, dass eine Gruppe der Ordnung 5 keine nichttrivialen Untergruppen haben kann. (Das gilt für jede Gruppe, deren Ordnung eine Primzahl ist.) Außerdem ist damit klar, dass man in Aufgabe 8.27 nicht nach dreielementigen Untergruppen suchen muss. Die naheliegende Umkehrung des Satzes

[16] Genauer eigentlich *Linksnebenklassen*. Im Englischen nennt man sie *(left) cosets*.

von Lagrange gilt übrigens nicht: Es gibt nicht für jeden Teiler der Ordnung von G eine Untergruppe dieser Ordnung. Das kleinste Gegenbeispiel ist eine Gruppe der Ordnung 12, die keine Untergruppe der Ordnung 6 hat.

Lemma 8.8

Ist f ein injektiver Homomorphismus von G nach H, dann ist f^{-1} ein Homomorphismus von $f[G]$ nach G.

Beweis. Wir greifen uns zwei Elemente a und b der Gruppe $f[G]$ heraus. Dazu gibt es c und d mit $f(c) = a$ und $f(d) = b$ bzw. (siehe Satz 6.5) $f^{-1}(a) = c$ und $f^{-1}(b) = d$. Damit haben wir sofort

$$f^{-1}(a \cdot b) = f^{-1}(f(c) \cdot f(d)) = f^{-1}(f(cd)) = cd = f^{-1}(a) \cdot f^{-1}(b).$$

Wie man sieht, folgt die Aussage direkt daraus, dass f ein Homomorphismus ist. Man braucht die Injektivität lediglich, damit f^{-1} eine Funktion ist. ■

Definition

Ein Homomorphismus von G nach H wird **Isomorphismus** genannt, wenn es sich um eine bijektive Abbildung von G auf H handelt. Gibt es so eine Abbildung, dann sagt man, dass G **isomorph** zu H ist.

Nach Lemma 8.8 folgt sofort, dass f^{-1} ein Isomorphismus von H auf G ist, wenn f einer von G auf H ist. Isomorphie ist also symmetrisch,[17] d. h., wenn G isomorph zu H ist, ist H auch isomorph zu G. Darum kann man kürzer auch einfach sagen, dass G und H isomorph sind.

Aufgabe 8.31. Isomorphie ist auch reflexiv in dem Sinne, dass jede Gruppe isomorph zu sich selbst ist. Wieso?

⋆**Aufgabe 8.32**. Wieso ist Isomorphie auch transitiv?

Dass jede Gruppe isomorph zu sich selbst ist, ist natürlich nicht so spannend. Ein einfaches Beispiel für Isomorphie zwischen zwei *verschiedenen* Gruppen liefern die Gruppen $G = \{1, a\}$ und $H = \{0, b\}$, deren Verknüpfungen $\otimes$ und $\oplus$ durch die folgenden Tabellen definiert werden.

$\otimes$	1	a
1	1	a
a	a	1

$\oplus$	0	b
0	0	b
b	b	0

Es lässt sich leicht nachprüfen, dass $\{(1,0),(a,b)\}$ ein Isomorphismus von G auf H ist. Man *sieht* ja, dass die beiden Gruppen „gleich“ sind. Aber sie sind eben nicht identisch im mathematischen Sinne, sondern nur „als Gruppen gleich“. Genau dafür ist der Begriff der Isomorphie gedacht. Die Wörter Homomorphismus und

[17] Vorsichtshalber sei hier gesagt, dass Begriffe wie Symmetrie oder Transitivität hier etwas informeller als auf Seite 63 interpretiert werden müssen, weil es so etwas wie „die Menge aller Gruppen“ nicht gibt, auf der man eine Relation definieren könnte. Siehe dazu die Bemerkungen über naive und axiomatische Mengenlehre am Ende des ersten Kapitels.

Isomorphismus kommen beide aus dem Altgriechischen und bedeuten ungefähr dasselbe, nämlich „von gleicher Gestalt“. Isomorphie ist aber offensichtlich der stärkere Begriff. Informell sind zwei Gruppen dann isomorph, wenn sie sich nur durch Umbenennung unterscheiden. Der Isomorphismus $f\colon G \to H$ ordnet die unterschiedlichen Namen einander zu: $f(a)$ verhält sich in der Gruppe H genau so, wie sich a in der Gruppe G verhält. Man sagt auch, dass G und H „bis auf Isomorphie gleich“ sind. Obwohl also in Aufgabe 8.14 diverse Gruppen mit zwei Elementen genannt wurden, würde eine Mathematikerin sagen, dass es „bis auf Isomorphie“ nur *eine* Gruppe mit zwei Elementen gibt.

Aufgabe 8.33. Begründen Sie, warum im obigen Beispiel $\{(1,b),(a,0)\}$ *kein* Isomorphismus wäre.

Aufgabe 8.34. Geben Sie für die Gruppe aus Aufgabe 8.15 einen Isomorphismus auf sich selbst[18] an, der nicht die Identität ist.

Aufgabe 8.35. Die Gruppen $(\mathbb{R},+)$ und $(\mathbb{R}^+,\cdot)$ sind isomorph. Können Sie einen Isomorphismus angeben?

Aufgabe 8.36. Im Folgenden sieht man rechts (bis auf Isomorphie) die Gruppe aus Aufgabe 8.27. Links sieht man eine andere Gruppe.

$\otimes$	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

$\oplus$	0	x	y	z
0	0	x	y	z
x	x	0	z	y
y	y	z	0	x
z	z	y	x	0

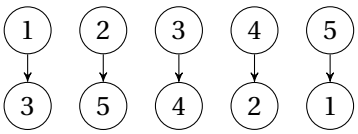
Es handelt sich wirklich um eine *andere* Gruppe, d. h., die beiden sind *nicht* isomorph. Das bedeutet, dass man keinen Isomorphismus zwischen den beiden finden kann. Können Sie das begründen?

9. Permutationsgruppen

Definition

Eine bijektive Abbildung einer Menge X auf sich selbst, nennt man **Permutation** von X. Für die Menge aller Permutationen von X schreiben wir S_X.

Den Begriff kennen wir schon aus dem Kapitel über Kombinatorik und er liegt auch nahe: Stellt man sich die Elemente einer Menge sortiert vor, dann bewirkt eine bijektive Abbildung der Menge auf sich selbst eine Umordnung dieser Elemente.[19]



[18] Falls Sie Fachbegriffe sammeln: So etwas nennt man einen *Automorphismus*.

Automorphismus

[19] Man vergleiche dazu auch den Abschnitt über Funktionen als Tupel sowie Aufgabe 6.28.

Die Komposition zweier Permutationen von X ist wieder eine Permutation von X und die Umkehrfunktion einer solchen Permutation ist ebenfalls eine.[20] S_X bildet also zusammen mit der Komposition eine Gruppe. Untergruppen von S_X nennt man *Permutationsgruppen*.

Permutationsgruppe

Aufgabe 9.1. Was ist das neutrale Element der Gruppe S_X?

Es gibt einen wichtigen Grund dafür, sich mit solchen Gruppen zu beschäftigen:

Satz 9.1

Satz von Cayley
Jede Gruppe G ist isomorph zu einer Permutationsgruppe, nämlich zu einer Untergruppe von S_G.

Beweis. Für $a \in G$ sei π_a die Abbildung von G nach G, die x auf ax abbildet. Nach Korollar 8.3 ist π_a eine Permutation von G. Ist $b \in G$ mit $a \neq b$, dann gilt natürlich $\pi_a \neq \pi_b$, weil bereits $\pi_a(1)$ und $\pi_b(1)$ verschieden sind. Ferner gilt für $a, b, x \in G$ immer

$$(\pi_a \circ \pi_b)(x) = \pi_a(\pi_b(x)) = \pi_a(bx) = a(bx) = (ab)x = \pi_{ab}(x)$$

und damit ist die durch $a \mapsto f(a) = \pi_a$ definierte Funktion f ein injektiver Homomorphismus von G nach S_G. G ist also isomorph zu $f[G]$ und das ist nach Lemma 8.6 eine Untergruppe von S_G. ■

Aufgabe 9.2. Wenn G die Gruppe $(\mathbb{Z}, +)$ ist, was ist dann die Permutation π_a aus dem Beweis des Satzes von Cayley für $a = 42$?

Aufgabe 9.3. Geben Sie eine Permutation von $\mathbb{Z}$ an, die nicht von der Form π_a für ein $a \in \mathbb{Z}$ wie in Aufgabe 9.2 ist.

Aufgabe 9.4. Geben Sie für die Gruppe aus Aufgabe 8.15 alle drei Elemente der Permutationsgruppe an, die man durch den Satz von Cayley erhält.

Aufgabe 9.5. Eine der Motivationen für die Gruppentheorie ist die Untersuchung von Symmetrien. Beispielsweise bilden die Rotationen um den Mittelpunkt, die ein Quadrat auf sich selbst abbilden, zusammen mit der Hintereinanderausführung eine Gruppe. (Dreht man etwa erst um 180 und dann um 270 Grad, dann ergibt das zusammen eine Drehung um 90 Grad.) Stellen Sie diese Gruppe als Permutationsgruppe der vier Eckpunkte des Quadrats dar.

⋆**Aufgabe 9.6**. Fügen Sie zu den Drehungen aus Aufgabe 9.5 noch die Achsenspiegelungen hinzu, die das Quadrat ebenfalls auf sich selbst abbilden, und führen Sie die Aufgabe dann erneut durch.

Permutationsgruppen werden wir in diesem Abschnitt etwas näher betrachten. Dabei wollen wir uns allerdings auf endliche Grundmengen X beschränken und dann reicht es offenbar, wenn wir Mengen der Form $[n]$ für $n \in \mathbb{N}$ betrachten.

[20] Siehe Aufgabe 6.52.

Definition

Für die Menge $S_{[n]}$ schreiben wir abkürzend S_n. Die Gruppe $(S_n, \circ)$ wird die **symmetrische Gruppe** vom Grad n genannt.

Aufgabe 9.7. Wie viele Elemente hat S_n?

Für Elemente von S_n werden häufig griechische Buchstaben wie σ, τ und so weiter verwendet. Wir verwenden außerdem die Konvention von Seite 100, d. h., wir schreiben gelegentlich $\sigma\tau$ für $\sigma \circ \tau$, σ^0 für $\mathrm{id}_{[n]}$, σ^2 für $\sigma\sigma$ et cetera. In diesem Sinne spricht man manchmal auch von *Produkten* statt von Kompositionen von Permutationen.

Zweizeilenform

Eine übliche Notation für eine Permutation σ ist die *Zweizeilenform*, bei der man die Elemente von $[n]$ zweimal jeweils horizontal aufschreibt und dabei unter dem Element i der ersten Zeile jeweils sein Bild $\sigma(i)$ in der zweiten Zeile einträgt:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Dabei muss die erste Zeile nicht notwendig aufsteigend sortiert sein.

Aufgabe 9.8. Schreiben Sie die Permutation

$$\tau\colon \begin{cases} [8] \to [8] \\ n \to \begin{cases} n+1 & n \text{ ungerade} \\ n-1 & n \text{ gerade} \end{cases} \end{cases}$$

aus S_8 in Zweizeilenform auf.

Aufgabe 9.9. Schreiben Sie die Permutationen

$$\sigma = \{(1,3),(2,1),(3,4),(4,2)\}, \quad \tau = \{(1,1),(2,4),(3,2),(4,3)\}$$

und $\sigma\tau$ aus S_4 in Zweizeilenform auf.

Aufgabe 9.10. Ein Vorteil der Zweizeilenform ist, dass man ohne Mühe das inverse Element zu einer so notierten Permutation erhält. Nämlich wie?

Aufgabe 9.11. Begründen Sie mit einem konkreten Beispiel, dass S_3 nicht abelsch ist.

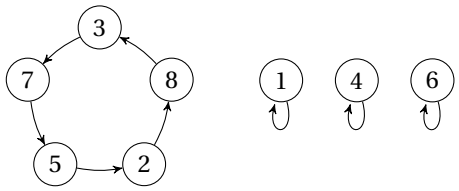
Aufgabe 9.12. Warum folgt aus Aufgabe 9.11, dass für $n \geq 3$ keine der Gruppen S_n abelsch sein kann?

Aufgabe 9.13. Seien σ und τ die Permutationen aus Aufgabe 9.9. Gibt es eine Permutation $\rho \in S_4$ mit $\sigma\rho = \tau$?

Eine Permutation wie

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 7 & 4 & 2 & 6 & 5 & 3 \end{pmatrix} \tag{9.1}$$

kann man als gerichteten Graphen so darstellen:



Entscheidend ist dabei, dass ein Teil des Graphen ein Kreis wie der links ist und alle anderen Pfeile Schleifen sind, die direkt auf den Ausgangspunkt zurückzeigen. Solche Permutationen nennt man *Zyklen*:

Definition

Eine Permutation $\sigma \in S_n$ nennt man **Zyklus** (der Länge m), wenn es für ein $m \geq 1$ eine Menge $M = \{k_1, \ldots, k_m\} \subseteq [n]$ mit $|M| = m$ sowie $\sigma(k_i) = k_{i+1}$ für $i \in [m-1]$, $\sigma(k_m) = k_1$ und $\sigma(k) = k$ für $k \notin M$ gibt.[21] Dafür schreibt man kurz $\sigma = (k_1\ k_2\ \ldots\ k_m)$.

Aufgabe 9.14. Ist die auf Seite 107 abgebildete Permutation ein Zyklus?

Aufgabe 9.15. Schreiben Sie σ aus (9.1) in der gerade definierten Schreibweise für Zyklen auf.

Aufgabe 9.16. Ist die Zyklenschreibweise eindeutig?

Aufgabe 9.17. Auf wie viele verschiedene Arten kann man den Zyklus (2 8 3 7 5) aufschreiben?

Aufgabe 9.18. Schreiben Sie den Zyklus (3 6 1 7 5) $\in S_7$ in Zweizeilenform auf.

Aufgabe 9.19. Ist der Zyklus (1 2 3) ein Element von S_3 oder von S_4?

Aufgabe 9.20. Was ist mit dem Zyklus (1) gemeint?

Aufgabe 9.21. Wie sieht in Zyklenschreibweise die Umkehrfunktion eines Zyklus aus?

Aufgabe 9.22. Ist die Menge der Zyklen eine Untergruppe von S_n?

Definition

Für $\sigma \in S_n$ bezeichnen wir die Menge $\operatorname{supp}(\sigma) = \{k \in [n] : \sigma(k) \neq k\}$ als den **Träger**[22] von σ. Zwei Permutationen werden **disjunkt** genannt, wenn ihre Träger disjunkt sind.

Im Träger von σ befinden sich also die Zahlen, die von σ „bewegt“ werden. Und sind zwei Permutationen disjunkt, dann „bewegt“ jede von ihnen nur Elemente, die von der anderen „festgehalten“ werden. Sie kommen sich quasi nicht „ins Gehege“.

[21] Beachten Sie, dass die Bedingung $|M| = m$ dafür sorgt, dass die k_i paarweise verschieden sind.
[22] Die Abkürzung steht für das englische Wort *support*.

Aufgabe 9.23. Geben Sie für die auf Seite 107 abgebildete Permutation und für den Zyklus aus Aufgabe 9.15 jeweils den Träger an.

Aufgabe 9.24. Was kann man über eine Permutation sagen, deren Träger die leere Menge ist?

Aufgabe 9.25. Was kann man über eine Permutation sagen, deren Träger aus genau einem Element besteht?

Aufgabe 9.26. Was kann man über eine Permutation sagen, deren Träger die Mächtigkeit zwei hat?

Aufgabe 9.27. Geben Sie zwei Zyklen der Länge 3 an, deren Produkt die Identität ist.

Das folgende Lemma sammelt ein paar einfache Eigenschaften von Permutationen und Zyklen, die durch die Beschäftigung mit den Aufgaben hoffentlich größtenteils schon klar geworden sind.

Lemma 9.2

In der symmetrischen Gruppe S_n gelten die folgenden Aussagen:

(i) Die Identität ist ein Zyklus (der Länge eins) und die einzige Permutation, deren Träger die leere Menge ist. Wir werden sie als *trivialen Zyklus* bezeichnen.

trivialer Zyklus

(ii) Disjunkte Permutationen *kommutieren*, d. h., es gilt $\sigma\tau = \tau\sigma$, wenn σ und τ disjunkt sind.

kommutieren

(iii) Sind σ und τ disjunkte Permutationen, dann ist $\operatorname{supp}(\sigma\tau)$ die Vereinigung der (disjunkten) Mengen $\operatorname{supp}(\sigma)$ und $\operatorname{supp}(\tau)$.[23]

(iv) Der Träger eines nichttrivialen Zyklus $(k_1\ k_2\ \ldots\ k_m)$ ist die Menge $\{k_1, k_2, \ldots, k_m\}$.

(v) Ist σ ein Zyklus der Länge m und k ein Element von $\operatorname{supp}(\sigma)$, dann gilt $\sigma = \big(\sigma^0(k)\ \sigma^1(k)\ \sigma^2(k)\ \ldots\ \sigma^{m-1}(k)\big)$.

(vi) Ist σ ein Zyklus der Länge m, dann ist σ^k die Identität, wenn k ein Vielfaches von m ist.

(vii) Zyklen unterschiedlicher Länge sind verschieden.

(viii) Ein Zyklus σ lässt sich nicht als Produkt disjunkter Zyklen darstellen, die alle eine geringere Länge als σ haben.

Aufgabe 9.28. Stellen sie für jede der Aussagen aus Lemma 9.2 sicher, dass Sie sie verstanden haben, und machen Sie sich anhand von Beispielen auch klar, dass sie stimmt. (Evtl. versuchen Sie sich ja auch daran, einen Beweis zu formulieren?)

⋆**Aufgabe 9.29**. Was passiert bei Punkt (vi) von Lemma 9.2, wenn k kein Vielfaches von m ist? Probieren Sie herum und versuchen Sie, eine Antwort zu finden, die alle Fälle abdeckt.

[23] Man beachte, dass diese Aussage und die davor nach den Aufgaben 9.12 und 9.27 im Allgemeinen nicht gelten.

Aussage (viii) von Lemma 9.2 zeigt, dass es bezüglich der „Multiplikation“ in S_n eine gewisse Analogie zwischen Zyklen und Primzahlen gibt. Das werden wir nun ausarbeiten. Dadurch wird die Bedeutung der Zyklen für die symmetrischen Gruppen klar werden.

Lemma 9.3 Jede Permutation $\sigma \in S_n \setminus \{(1)\}$ „enthält“ einen nichttrivialen Zyklus in dem Sinne, dass es einen Zyklus $\tau \neq (1)$ und ein $\rho \in S_n$ gibt, so dass $\sigma = \tau\rho$ gilt und τ und ρ disjunkt sind.

Beweis. Weil σ nicht die Identität ist, gibt es ein $k \in [n]$ mit $\sigma(k) \neq k$. Man bildet nun nacheinander $\sigma^0(k)$, $\sigma^1(k)$, $\sigma^2(k)$, $\sigma^3(k)$ und so weiter. Da $[n]$ nur endlich viele Elemente hat, muss es irgendwann zum ersten Mal zu einer Wiederholung kommen, also zu $m_1 < m_2$ mit $\sigma^{m_1}(k) = \sigma^{m_2}(k)$. Dabei muss $m_1 = 0$ gelten, denn sonst hätten wir $\sigma^{m_1-1}(k) = \sigma^{m_2-1}(k)$, weil σ injektiv ist, und bei m_2 wäre nicht die *erste* Wiederholung aufgetreten. Dann ist

$$\tau = \left(\sigma^0(k)\ \sigma^1(k)\ \sigma^2(k)\ \ldots\ \sigma^{m_2-1}(k)\right)$$

ein Zyklus. Setzen wir $T = \operatorname{supp}(\tau)$ und $\rho = \mathrm{id}_T \cup \sigma|_{[n]\setminus T}$, dann erfüllen τ und ρ die Bedingung des Lemmas. ∎

Wir gehen das am Beispiel der Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 2 & 7 & 1 & 11 & 4 & 5 & 8 & 6 & 12 & 3 & 10 \end{pmatrix}$$

aus S_{12} durch. Als Startwert k können wir jede Zahl außer 2 und 8 wählen. Wir beginnen mit $k = 1$. Dann erhalten wir $\sigma^0(k) = 1$, $\sigma^1(k) = 9$, $\sigma^2(k) = 6$, $\sigma^3(k) = 4$ und schließlich $\sigma^4(k) = 1 = k$. Damit ergibt sich $\tau = (1\,9\,6\,4)$ und wir setzen

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 2 & 7 & 4 & 11 & 6 & 5 & 8 & 9 & 12 & 3 & 10 \end{pmatrix},$$

wobei die grauen Zahlen die Elemente des Trägers von τ sind.

Der folgende Satz ist eine Analogie zum Fundamentalsatz der Arithmetik.

Satz 9.4 Jede Permutation lässt sich als Produkt paarweise disjunkter nichttrivialer Zyklen schreiben. Diese Darstellung ist bis auf die Reihenfolge eindeutig.

Eventuell haben Sie sich gefragt, wie man einen Zyklus als Produkt von Zyklen darstellen soll. Wenn man sich an die Denkweise der Mathematik gewöhnt hat, ist das jedoch kein Problem: ein Zyklus lässt sich als ein Produkt darstellen, das aus *einem* Faktor besteht. Und wenn wir schon einmal dabei sind: Was ist mit der Identität? Die kann man doch nun wirklich nicht als Produkt von *nichttrivialen* Zyklen darstellen, oder? Da würde jede professionelle Mathematikerin mit den

Schultern zucken und sagen: „Doch, die Identität ist das Produkt von *null* nichttrivialen Zyklen.“ Das passt zu der (sinnvollen) Festlegung, dass σ^0 immer für die Identität steht.

Beweis. Nach dieser Vorbemerkung können wir uns auf nichttriviale Zyklen beschränken. Nach Lemma 9.3 enthalten die immer einen nichttrivialen Zyklus als Faktor. Außerdem ist klar, dass der Träger des anderen Faktors (ρ) eine geringe Mächtigkeit als der Träger des ursprünglichen Zyklus (σ) hat. Ist der „Rest“ ρ nicht die Identität, dann können wir auf diesen erneut das Lemma anwenden. Diesen Vorgang wiederholen wir, bis wir als Rest die Identität erhalten. Das muss irgendwann passieren, weil die Träger der Reste immer kleiner werden.

Dass die Reihenfolge dieser Darstellung nicht eindeutig sein kann, ergibt sich aus Punkt (ii) in Lemma 9.2. Dass andererseits die Faktoren eindeutig bestimmt sind, folgt auch aus diesem Lemma. Ich werde das jedoch hier nicht ausführlich beweisen, weil es hoffentlich durch die folgenden Beispiele ausreichend illustriert wird. ■

Wir setzen das hinter Lemma 9.3 angefangene Beispiel fort und wenden das Lemma auf den Rest ρ an. Wenn wir mit der Zahl 3 anfangen, erhalten wir den Zyklus (3 7 5 11). Der neue Rest ist nun

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 2 & 7 & 4 & 11 & 6 & 5 & 8 & 9 & 12 & 3 & 10 \end{pmatrix}$$

und für den ergibt eine dritte Anwendung des Lemmas die Darstellung (10 12) ∘ (1). Insgesamt haben wir damit

$$\sigma = (1\,9\,6\,4)\,(3\,7\,5\,11)\,(10\,12) \tag{9.2}$$

erhalten.

Aufgabe 9.30. Stellen Sie die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 5 & 12 & 7 & 1 & 4 & 13 & 2 & 6 & 3 & 11 & 10 & 9 \end{pmatrix}$$

aus S_{13} als Produkt disjunkter Zyklen dar.

Aufgabe 9.31. Stellen Sie sich selbst ähnliche Aufgaben wie 9.30, indem Sie z. B. in Wolfram Alpha so etwas wie `RandomPermutation[13]` eingeben. Das generiert eine zufällige Permutation und zeigt zur Kontrolle auch gleich die Zerlegung in disjunkte Zyklen an.

Aufgabe 9.32. Schreiben Sie das Produkt

(1 4 2 3 8) (6 7) (9 11 14 13 12 10)

aus S_{15} in Zweizeilenform auf.

Aufgabe 9.33. Geben Sie die Permutation

$$\sigma = (1\,2\,4)\,(1\,2\,3)\,(1\,3\,5)\,(1\,3)$$

aus S_5 in Zweizeilenform und als Produkt disjunkter Zyklen an.

Aufgabe 9.34. Auf wie viele verschiedene Arten kann man das Produkt aus (9.2) hinschreiben?

Aufgabe 9.35. Wie viele verschiedene Zyklen gibt es zu einer vorgebenen Trägermenge der Mächtigkeit m?

Transposition

Einen Zyklus der Länge 2 bezeichnet man als *Transposition*. Aufgrund der Aufgaben 9.25 und 9.26 wissen wir, dass Transpositionen die einfachsten Permutationen nach der Identität sind. Erstaunlicherweise reichen sie als „Bausteine“ für *alle* Permutationen bereits aus:

Lemma 9.5

Jede Permutation aus S_n lässt sich als Produkt von Transpositionen darstellen.

Beweis. Wegen Satz 9.4 reicht es, Zyklen als Produkte von Transpositionen darzustellen. Das geht aber immer durch

$$(k_1\ k_2\ k_3\ \ldots\ k_m) = (k_1\ k_2)\,(k_2\ k_3)\cdots(k_{m-1}\ k_m),$$

wie man leicht nachrechnet. ■

Aufgabe 9.36. Was ist mit der Identität? Lässt die sich auch als Produkt von Transpositionen darstellen?

Aufgabe 9.37. Stellen Sie die Permutation σ aus Aufgabe 9.30 als Produkt von Transpositionen dar.

Aufgabe 9.38. Begründen Sie, warum man für $n \geq 2$ jede Permutation auf unendlich viele verschiedene Arten als Produkt von Transpositionen darstellen kann.

Aufgabe 9.39. Stellen Sie $\sigma = (1\,3)\,(3\,4)\,(2\,4)\,(1\,4)\,(2\,3)$ als Produkt von drei Transpositionen dar.

Nachbartransposition

⋆**Aufgabe 9.40**. Eine *Nachbartransposition* ist eine Permutation aus S_n, die die Form $(k\ k+1)$ für $k \in [n-1]$ hat. Begründen Sie, warum man jede Permutation als Produkt von Nachbartranspositionen darstellen kann.

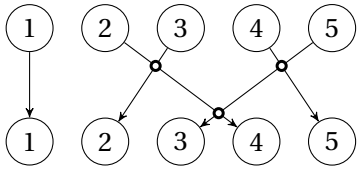
⋆**Aufgabe 9.41**. In Lemma 9.5 wird nicht (wie in Satz 9.4) gefordert, dass die Transpositionen paarweise disjunkt sind. Das geht auch gar nicht: Geben Sie eine Permutation an, die man nicht als Produkt paarweise disjunkter Transpositionen darstellen kann.

Wie man an den Aufgaben 9.37 und insbesondere 9.38 gesehen hat, ist die Darstellung durch Transpositionen im Gegensatz zu der durch disjunkte Zyklen nicht eindeutig. Man kann aber trotzdem eine Aussage darüber machen, welche Darstellungen möglich sind und welche nicht.

Definition

Ein **Fehlstand** bzw. eine **Inversion** einer Permutation $\sigma \in S_n$ ist ein Paar (i, j) aus $[n]^2$ mit $i < j$ und $\sigma(i) > \sigma(j)$.

Fehlstände kann man visualisieren, indem man die Permutationen anders als üblich aufschreibt. Die Menge $[n]$ wird zweimal horizontal aufgeschrieben, aber anders als bei der Zweizeilenform jeweils *sortiert*. Pfeile von oben nach unten verbinden jeweils Argument und zugehörigen Funktionswert. Jeder Schnittpunkt zweier Pfeile führt zu einem Fehlstand, wenn man die Pfeile zu ihren Anfangspunkten zurückverfolgt. In der folgenden Grafik sieht man in S_5 die Permutation $\sigma = \{(1,1),(2,4),(3,2),(4,5),(5,4)\}$ mit den drei Fehlständen $(2,3)$, $(2,5)$ und $(4,5)$.



Wir haben bereits gesehen, dass es für ein und dieselbe Permutation unterschiedliche Darstellungen als Produkt von Transpositionen gibt, bei denen sich die Anzahl der Transpositionen unterscheidet. Wir werden aber nun begründen, warum sich zumindest die *Parität* dieser Zahl nicht ändert – damit meint man, dass die Zahl entweder immer gerade oder immer ungerade ist. Wenn es um solche Unterscheidungen geht, dann nutzt man in der Mathematik oft aus, dass $(-1)^n$ für gerade n positiv und für ungerade n negativ ist.

Parität

Definition

Die Menge aller Fehlstände einer Permutation $\sigma \in S_n$ wird

$$\operatorname{inv}(\sigma) = \{(i,j) \in [n]^2 : i < j \wedge \sigma(i) > \sigma(j)\}$$

geschrieben. Das **Signum** von σ ist die Zahl $\operatorname{sgn}(\sigma) = (-1)^{|\operatorname{inv}(\sigma)|}$.

Das Signum ist also genau dann 1 bzw. -1, wenn die Anzahl der Fehlstände gerade bzw. ungerade ist. Man unterteilt gemäß der Parität von $|\operatorname{inv}(\sigma)|$ auch in *gerade* und *ungerade* Permutationen.

(un)gerade Permutation

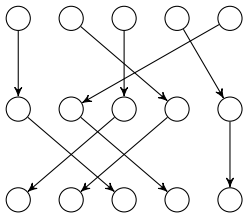
Aufgabe 9.42. Berechnen Sie für einige Permutationen das Signum. Sie können dabei wie in Aufgabe 9.31 vorgehen. Die Website wird Ihnen nämlich auch das Signum ausgeben und als Bonus ein Pfeildiagramm generieren, dem man die Fehlstände entnehmen kann.

Offensichtlich hat die Identität keine Fehlstände und daher das Signum $(-1)^0 = 1$. Transpositionen haben immer das Signum -1, denn eine Transposition vertauscht immer zwei Zahlen k und m mit $k < m$ und daraus ergibt sich auf jeden Fall der Fehlstand (k,m). Hinzu kommen für jede Zahl j zwischen k und m jeweils *zwei* Fehlstände, nämlich (k,j) und (j,m). Die Zahlen vor k und hinter m sind an Fehlständen offenbar nicht beteiligt. Die folgende Skizze zeigt dafür zwei Beispiele: $(k\ m) = (2\,3)$ und $(k\ m) = (2\,5)$.

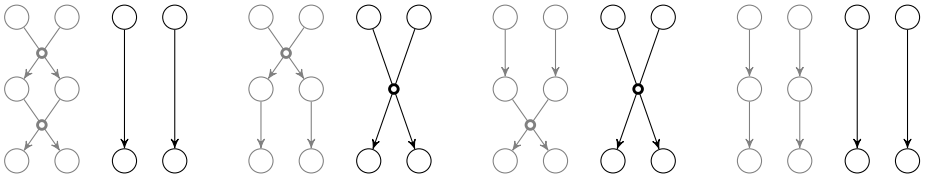
Die zentrale Aussage über die Parität von Permutationen ist die folgende:

Satz 9.6 Für alle Permutationen $\sigma, \tau \in S_n$ gilt $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

Beweis. Den Beweis führt man am einfachsten grafisch, indem man für die Komposition zwei der obigen Visualisierungen kombiniert. Als Beispiel folgt die Darstellung von $\{(1,3),(2,4),(3,1),(4,2),(5,5)\} \circ \{(1,1),(2,4),(3,3),(4,5),(5,2)\}$.



Für das Zählen der Fehlstände muss man immer nur zwei Pfeile betrachten. Die schneiden sich entweder (Fehlstand) oder sie schneiden sich nicht (kein Fehlstand). Durch das „Hintereinanderhängen“ zweier Diagramme gibt es vier Möglichkeiten:



In den drei Fällen rechts ergibt sich die Anzahl der Fehlstände der Komposition immer durch die Addition der Fehlstandzahlen der beiden Faktoren. Den Fall ganz links kann man so zählen, als würde auch addiert, danach aber zwei subtrahiert. Insgesamt ergibt das

$$|\operatorname{inv}(\sigma\tau)| = |\operatorname{inv}(\sigma)| + |\operatorname{inv}(\tau)| - 2k,$$

wobei die Zahl k angibt, wie oft der linke Fall eintritt. Das spielt aber keine Rolle, weil $2k$ auf jeden Fall gerade ist und die Parität von $|\operatorname{inv}(\sigma\tau)|$ daher nicht beeinflusst. Damit ist der Satz bewiesen. ■

Korollar 9.7 Wenn eine Permutation durch ein Produkt von m Transpositionen dargestellt wird, dann ist m genau dann gerade, wenn die Permutation gerade ist.

Beweis. Da alle Transpositionen das Signum -1 haben, hat das Produkt von m Transpositionen nach Satz 9.6 das Signum $(-1)^m$. ■

Aufgabe 9.43. Ist der Zyklus $\sigma = (1\,2\,3\,4\,5\,6)$ gerade oder ungerade?

Aufgabe 9.44. In Informatik-Vorlesungen wird gerne der Algorithmus *Bubblesort* vorgeführt. Was sagt Korollar 9.7 über dieses Sortierverfahren?

Bubblesort

Korollar 9.8

Die Menge der geraden Permutationen bildet für $n \geq 2$ eine Untergruppe der symmetrischen Gruppe S_n mit der Ordnung $|S_n|/2 = n!/2$.

alternierende Gruppe

Die Gruppe aus Korollar 9.8 wird *alternierende Gruppe* vom Grad n genannt.

Aufgabe 9.45. Wenn $\sigma = \tau_1\tau_2\ldots\tau_m$ ein Produkt von m Transpositionen ist, wie sieht dann σ^{-1} als Produkt von Transpositionen aus?

⋆**Aufgabe 9.46**. Beweisen Sie Korollar 9.8.

⋆**Aufgabe 9.47**. Wenn Sie Aufgabe 9.6 bearbeitet haben, dann schreiben Sie alles noch einmal in der Form von Zyklen und Transpositionen auf und identifizieren Sie eine nichttriviale Untergruppe, die nicht aus den vier Drehungen besteht.

10. Ringe und Körper

In Gruppen gibt es immer nur *eine* innere Verknüpfung. Beim täglichen Umgang mit Zahlen hantieren wir jedoch in der Regel mit Addition, Multiplikation, Subtraktion und Division. Die Strukturen, die dieses „Alltagsrechnen“ abstrahieren, sind *Ringe* und *Körper*. Wir werden uns mit ihnen nicht so lange beschäftigen, wie mit Gruppen, aber wir wollen uns zumindest mit den Begriffen und den wichtigsten Beispielen vertraut machen. Viele Konzepte sind einfach sinngemäße Übertragungen der entsprechende Konzepte für Gruppen.

Der „Prototyp“ für einen Ring sind die ganzen Zahlen. Der Prototyp für einen Körper sind die rationalen Zahlen.

Definition

Ist R eine Menge und sind $\oplus$ und $\otimes$ innere Verknüpfungen auf R, dann nennt man das Tripel $(R, \oplus, \otimes)$ einen **Ring**, wenn die folgenden drei Bedingungen erfüllt sind:

(i) $(R, \oplus)$ ist eine abelsche Gruppe.

(ii) $(R, \otimes)$ ist eine Halbgruppe.

(iii) Es gilt $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$ für alle $a, b, c \in R$.

Ist $(R, \otimes)$ sogar ein Monoid, dann spricht man von einem **unitären** Ring. Ist $\otimes$ kommutativ, dann spricht man von einem **kommutativen** Ring.

Distributivität

Eigenschaft (iii) wird *Distributivität* genannt. Sie stellt einen Zusammenhang zwischen den beiden Verknüpfungen her. (Sonst wären es einfach zwei Strukturen auf

derselben Grundmenge, die „nebeneinanderher leben“.) Die Ringe, mit denen wir arbeiten, werden so gut wie immer unitär und kommutativ sein.[24]

Aufgabe 10.1. Wie vereinfacht sich Eigenschaft (iii) für kommutative Ringe?

Konvention

Die Gruppe $(R,\oplus)$ schreibt man meistens additiv im Sinne der Konvention von Seite 100, während man die Verknüpfung $\otimes$ multiplikativ schreibt. Dabei beachtet man zur Klammerersparnis auch immer die Regel „Punkt- vor Strichrechnung“, d. h., dass beispielsweise $a+bc$ eine Abkürzung für $a+(b\cdot c)$ ist.

Bekannte Beispiele für (kommutative und unitäre) Ringe sind $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ und $(\mathbb{R},+,\cdot)$. Dass alle Eigenschaften erfüllt sind, ist (unbewiesenes) Schulwissen.

Für zwei weitere Beispiele haben wir die Grundidee bereits bei den Gruppen kennengelernt:

direktes Produkt

- Sind R_1 bis R_n Ringe, so erhält man auf dem Mengenprodukt $R_1\times\cdots\times R_n$ einen Ring, indem man beide Verknüpfungen komponentenweise wie in (8.1) definiert. Sind alle R_i unitär bzw. kommutativ, dann hat auch das Produkt (das man auch wieder *direktes Produkt* nennt) diese Eigenschaften. Die Begründung verläuft völlig analog wie in Aufgabe 8.10 durch simples Nachrechnen.
- Ist M irgendeine Menge und R ein Ring, dann erhält man auf R^M einen Ring, indem man Addition und Multiplikation analog zu Aufgabe 8.11 definiert. Auch hier ist der Ring der Funktionen unitär bzw. kommutativ, wenn der Ausgangsring R es ist.

Aus der Definition geht bereits hervor, dass Addition und Multiplikation in Ringen nicht gleichberechtigt sind. Man erkennt das auch an der folgenden Aussage, die in gewissem Sinne bemerkenswert ist, weil diese spezielle Eigenschaft der Null nicht etwa gefordert wird, sondern sich automatisch ergibt.

Lemma 10.1

In *jedem* Ring R gilt $a\cdot 0=0=0\cdot a$ für alle $a\in R$.

Beweis. Weil 0 das neutrale Element der Addition ist, gilt $0=0+0$. Und wegen der Distributivität folgt $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$. Damit ist $a\cdot 0$ eine Lösung der Gleichung $a\cdot 0=x+a\cdot 0$. 0 löst diese Gleichung aber auch. Und weil es nach Satz 8.2 nur *eine* Lösung gibt, folgt $a\cdot 0=0$. Für $0\cdot a$ verläuft der Beweis natürlich völlig analog. ■

Ich weise immer gerne darauf hin, dass die im Deutschen übliche Formulierung „vier Grundrechenarten“ irreführend ist. Die daraus resultierende Vorstellung führt häufig zu Denkfehlern bei einfachen Umformungen. Anhand von Ringen und

[24] Und wie so oft muss man beim Lesen von Büchern aufpassen, da manchmal nur unitäre oder sogar nur unitäre und kommutative Ringe als Ringe bezeichnet werden.

Körpern wird klar, dass es mathematisch sinnvoller ist, von *zwei* Grundrechenarten zu sprechen: Addition und Multiplikation. Subtraktion und Division sind „nur“ abgeleitete Operationen. Über die Division sprechen wir demnächst. Die Subtraktion ist gleichsam die Umkehrung der Addition:[25]

Konvention

Im Folgenden schreiben wir abkürzend $a-b$ für $a+(-b)$.

Beachten Sie, dass rechts gemäß der bereits verabredeten Konventionen das Minuszeichen im Ausdruck $-b$ für das zu b inverse Element bezüglich der Addition steht. Das Zeichen bildet zusammen mit dem Symbol b eine Einheit. Hingegen ist das Minuszeichen links neu und bekommt seine Bedeutung erst durch diese Konvention. Es steht *zwischen* a und b.

Wenn es um konkrete Zahlen geht, kann man das Minuszeichen noch auf eine dritte Art interpretieren: Mit -42 kann das inverse Element zu 42 gemeint sein, aber auch die negative Zahl -42. „Zum Glück“ ist es natürlich egal, wie es gemeint ist; sonst wäre diese Schreibweise auch sehr dumm.

Außerdem muss noch erwähnt werden, dass das Minuszeichen in beiderlei Form als „Strichrechnung“ gilt. Das impliziert, dass beispielsweise $-ab$ eine Abkürzung für $-(ab)$ ist und $a-bc$ eine Abkürzung für $a-(bc)$. Schließlich sei an die Linksassoziativität erinnert. So etwas wie $a-b-c$ wird als $(a-b)-c$ interpretiert und auch $a-b+c$ als $(a-b)+c$, weil es zwischen Addition und Subtraktion im Bezug auf die Priorität keinen Unterschied gibt.

Aufgabe 10.2. Studieren Sie die Dokumentation einer gängigen Programmiersprache und machen Sie sich klar, wie dort mit dem Minuszeichen umgegangen wird.

Es folgen ein paar einfache und aus der Schule bekannte Regeln für das Minuszeichen, von denen man hier sieht, dass (und warum) sie in *jedem* Ring gelten. Außerdem eignen sich diese Aussagen vielleicht ganz gut als Wiederholung, wenn Umformen von Termen nicht Ihre Stärke ist …

Lemma 10.2

Ist R ein Ring, dann gilt für alle $a,b,c \in R$:

(i) $0-a=-a$
(ii) $(-a)\cdot b = a\cdot(-b) = -ab$
(iii) $(-a)\cdot(-b) = ab$
(iv) $a\cdot(b-c) = ab-ac$
(v) $(b-c)\cdot a = ba-ca$
(vi) $-(a-b) = b-a$
(vii) $a-(b-c) = a-b+c$

[25] Übrigens sollten Sie beim Aufschreiben mathematischer Ausdrücke durch Klammerung dafür sorgen, dass nie zwei Rechenzeichen direkt aufeinanderfolgen. Das ist erstens unästhetisch und zweitens kann es missverständlich sein. Schreiben Sie also nicht „$3+-2$“ oder „$3\cdot-2$“, sondern $3+(-2)$ und $3\cdot(-2)$.

Beweis. Die erste Aussage ist sofort klar, wenn man sich die unterschiedliche Bedeutung der Minuszeichen vor Augen führt. Links steht nämlich die Abkürzung für $0+(-a)$ und das ist $-a$, weil 0 das neutrale Element der Addition ist.

Für die zweite Aussage berechnet man

$$a\cdot b+(-a)\cdot b=\big(a+(-a)\big)\cdot b=0\cdot b=0.$$

Dabei folgt die erste Gleichheit wegen der Distributivität, die zweite, weil $-a$ invers zu a ist, und die dritte nach Lemma 10.1. Insgesamt hat man damit gezeigt, dass $(-a)\cdot b$ bezüglich der Addition invers zu $a\cdot b$ ist.[26] Weil die Inversen nach Lemma 8.1 eindeutig bestimmt sind, ist $(-a)\cdot b$ also $-ab=-(ab)$. Für $a\cdot(-b)$ verläuft der Beweis natürlich analog.

Der Beweis der vierten Aussage verläuft so:

$$a\cdot(b-c)=a\cdot\big(b+(-c)\big)=a\cdot b+a\cdot(-c)=ab+(-ac)=ab-ac.$$

Ganz links und ganz rechts wurde lediglich die Konvention für das Minuszeichen verwendet. Die zweite Gleichheit folgt aus der Distributivität und die dritte wurde im letzten Absatz begründet.

Die fünfte Aussage beweist man analog zur vierten. Vielleicht schreiben Sie das zur Übung noch einmal hin.

Für die sechste Aussage berechnen wir

$$(a-b)+(b-a)=\big(a+(-b)\big)+\big(b+(-a)\big)=a+(-a)+b+(-b)=0$$

und sie folgt dann wegen der Eindeutigkeit der Inversen. (Ist Ihnen klar, warum die Zwischenschritte erlaubt sind?) ■

Aufgabe 10.3. Sie glauben, den Beweis der dritten und der siebten Aussage von Lemma 10.2 hätte ich vergessen? Aber nein, das sollen Sie machen!

Aufgabe 10.4. Ich habe oben geschrieben, dass die Interpretation der Subtraktion als abgeleitete Operation mathematisch sinnvoller ist. Sie ist auch für das Rechnen vorteilhafter. Warum ist es „besser“, sich $b-a$ als $b+(-a)$ vorzustellen?

Analog zu den Untergruppen kann man auch Unterringe definieren.

Definition

Ist R ein Ring, dann nennt man eine Teilmenge U von R einen **Unterring** von R, wenn U zusammen mit der auf U eingeschränkten Addition und Multiplikation selbst wieder ein Ring ist.

Beispielsweise ist $(\mathbb{Z},+,\cdot)$ ein Unterring von $(\mathbb{Q},+,\cdot)$ und $(\mathbb{Q},+,\cdot)$ ein Unterring von $(\mathbb{R},+,\cdot)$.

[26] Weil + in Ringen immer kommutativ ist, müssen wir nur eine Bedingung nachweisen.

Zusammen mit Lemma 8.5 liefert die folgende Aussage ein vergleichsweise einfach zu überprüfendes Kriterium dafür, wann man es mit einem Unterring zu tun hat. Auf den (unkomplizierten) Beweis verzichte ich.

Lemma 10.3

$U \subseteq R$ ist ein Unterring von R, wenn $(U,+)$ eine Untergruppe von $(R,+)$ und U abgeschlossen bzgl. der Multiplikation ist, d. h., wenn $ab \in U$ für alle $a, b \in U$ gilt.

Aufgabe 10.5. Ist die Menge $2\mathbb{Z}$ aller geraden ganzen Zahlen ein Unterring von $\mathbb{Z}$? $2\mathbb{Z}$

Ist R ein unitärer und kommutativer Ring, dann erhält man einen interessanten Ring folgendermaßen: Eine Funktion der Form

$$: \begin{cases} R \to R \\ x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \end{cases}$$

wird *Polynomfunktion* über R vom *Grad* n genannt, wenn n eine natürliche Zahl ist, alle a_i Elemente von R sind und $a_n \neq 0$ gilt.[27] Die a_i nennt man die *Koeffizienten* der Polynomfunktion. Ergänzend wird die Funktion von R nach R, die x konstant auf 0 abbildet, als Polynomfunktion vom Grad $-\infty$ bezeichnet. Für die Menge aller Polynomfunktionen über R schreibt man $R[x]$.

Polynomfunktion

Koeffizient

$R[x]$

Polynomfunktionen werden oft auch einfach als *Polynome* bezeichnet. Zwischen beiden Begriffen gibt es im Gebrauch zwar subtile Unterschiede, aber auf die werden wir vorerst nicht eingehen. In der Schule werden Polynomfunktionen manchmal auch *ganzrationale Funktionen* genannt.

Polynom

Aufgabe 10.6. Begründen Sie, dass $R[x]$ ein Unterring von R^R ist.

Wie versprochen kommt nun noch die Division dran. Analog zur Subtraktion, die die Addition umkehrt, werden wir die Division als Umkehrung der Multiplikation interpretieren. Da jedoch zur Multiplikation in Ringen nicht die Existenz von inversen Elementen gefordert wird, brauchen wir „mehr Struktur“, wenn wir dividieren wollen.

Definition

Ein Ring $(R,+,\cdot)$ wird **Körper** genannt, wenn er kommutativ und unitär ist und wenn zusätzlich $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.

Wegen Lemma 10.1 ist es unmöglich, dass es ein multiplikativ Inverses der Null gibt. Daher kann $(R,\cdot)$ keine Gruppe sein. Die Forderung, dass $(R \setminus \{0\}, \cdot)$ eine Gruppe ist, beinhaltet insbesondere, dass $R \setminus \{0\}$ abgeschlossen bezüglich der Multiplikation ist. Daher folgt:

[27] Zur Erklärung von Ausdrücken wie x^n sei an die Konvention von Seite 100 erinnert.

Lemma 10.4 Ist K ein Körper und sind $a, b \in K$ mit $ab = 0$, dann muss $0 \in \{a, b\}$ gelten.

nullteilerfrei

Hat ein Ring diese Eigenschaft, dann nennt man ihn *nullteilerfrei*. Körper haben die Eigenschaft immer.

Die „Standardbeispiele“ für Körper sind $\mathbb{Q}$ und $\mathbb{R}$. Der Ring $\mathbb{Z}$ ist hingegen offenbar kein Körper.

Aufgabe 10.7. Wie viele Elemente muss ein Körper mindestens haben?

Aufgabe 10.8. Das direkte Produkt $\mathbb{R} \times \mathbb{R}$ ist ein Ring. Ist es auch ein Körper?

Aufgabe 10.9. Wir definieren auf der Menge[28] $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ dieselbe Addition wie beim direkten Produkt, aber eine andere Multiplikation durch

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Überprüfen Sie, dass man dadurch einen Körper erhält.

Aufgabe 10.10. Ist der Polynomring $\mathbb{R}[x]$ ein Körper?

Konvention In Körpern kürzt man ba^{-1} oft als b/a bzw. $\frac{b}{a}$ ab. Das erklärt auch die alternative Schreibweise $1/a$ für a^{-1}.

Wie die Subtraktion ist die Division aus mathematischer Sicht also keine eigenständige Rechenoperation, sondern lediglich eine Abkürzung. Die alternative Schreibweise $b : a$ für b/a wird in der Schule gerne verwendet, kommt in der wissenschaftlichen Mathematik aber selten vor.

Analog zu Lemma 10.2 könnte man nun diverse Aussagen über die Division beweisen. Zum Beispiel, dass b/a bezüglich der Division invers zu a/b ist, oder dass $(a + b)/c$ dasselbe wie $a/c + b/c$ ist. Vielleicht überlegen Sie sich das selbst zur Übung einmal. Wir belassen es an dieser Stelle bei der Bemerkung, dass man in jedem Körper so rechnen kann, wie man es von den rationalen Zahlen gewohnt ist, solange man nur Addition, Subtraktion, Multiplikation und Division verwendet.

Aufgabe 10.11. Welche der folgenden Aussagen gelten in jedem Körper K, wenn a und b Elemente von K sind?

(i) $(a + b)^2 = a^2 + ab + ab + b^2$
(ii) $(a + b)(a - b) = a^2 - b^2$
(iii) $a^2 \geq 0$

Wir sparen es uns, Homomorphismen und Isomorphismen für Ringe und Körper formal zu definieren. Es sollte klar sein, dass sie sowohl die Addition als auch die Multiplikation erhalten müssen. Was es bedeutet, dass beispielsweise zwei Körper isomorph sind, wird Ihnen hoffentlich intuitiv auch so klar sein.

[28] Das Symbol $\mathbb{C}$ steht hier im Vorgriff für die komplexen Zahlen, die wir später im Detail behandeln werden. Für diese Aufgabe muss man über komplexe Zahlen nichts wissen.

Resümee

Heutzutage kommt man um algebraische Strukturen in der Mathematik nicht mehr herum. Ihre moderne Darstellung hat sich jedoch erst im 20. Jahrhundert entwickelt. Die deutsche Mathematikerin Emmy Noether war die vielleicht einflussreichste Person in diesem Zusammenhang.

Einer der wichtigsten Vorreiter war Anfang des 19. Jahrhunderts der Franzose Évariste Galois, der bereits mit 20 Jahren verstarb, vorher aber schon die Grundideen für Gruppen und Körper entwickelt hatte. Bereits vor Galois lebte der italienische Mathematiker Joseph-Louis Lagrange. Er bewies den nach ihm benannten Satz nicht in der Form, in der er heute rezipiert wird, aber er hatte die wesentliche Idee, auf der dann andere aufbauten. Mit dem nach dem Engländer Arthur Cayley benannten Satz verhält es sich ähnlich. Überlegungen zu den Eigenschaften von Permutationen stellten bereits Leibniz und der Japaner Seki Takakazu im 16. Jahrhundert im Zusammenhang mit Determinanten an, aber auch das war weit entfernt von der heutigen Theorie.

V

Zahlentheorie

Wir werden uns nun mit den Grundzügen der sogenannten *Zahlentheorie* befassen. Abgesehen davon, dass es sich einfach um ein spannendes Thema handelt, ist die Zahlentheorie auch für die Anwendung relevant, weil sie eine zentrale Rolle in der Kryptographie spielt. Zudem kann man einige ihrer Techniken wie z. B. die modulare Arithmetik gewinnbringend in der Informatik einsetzen.

Das Wort *Zahlentheorie* (engl. *number theory*) stammt aus einer Zeit, als man nur als Zahlen ansah, was wir heutzutage als positive natürlichen Zahlen bezeichnen (während man Brüche oder irrationale Zahlen *Größen* nannte). Wir werden das etwas ausweiten und teilweise auch mit negativen Zahlen arbeiten, aber andere Zahlen werden auf den folgenden Seiten keine Rolle spielen.

Konvention

In diesem Kapitel geht es ausschließlich um ganze Zahlen. Wenn eine Variable für eine Zahl steht und nichts weiter über sie gesagt wird, dann wird implizit immer vorausgesetzt, dass sie ein Element von $\mathbb{Z}$ ist. Und wenn von *Zahlen* ohne weiteren Zusatz die Rede ist, dann sind damit ganze Zahlen gemeint.

11. Teilbarkeit

Wir brauchen zunächst eine ganz grundlegende Eigenschaft von $\mathbb{N}$. Wenn man die Mathematik auf der Mengenlehre aufbaut, dann handelt es sich um einen Satz, für dessen Beweis uns allerdings die technischen Voraussetzungen fehlen. Betreibt man die Zahlentheorie „klassisch“ ohne Mengenlehre, dann ist die folgende Aussage etwas, das man einfach – als Axiom – „glaubt“.

Satz 11.1

Wohlordnung der natürlichen Zahlen
Jede nichtleere Menge A von natürlichen Zahlen hat ein kleinstes Element.

Minimum $\min A$

Dieses Element wird als *Minimum von A* bezeichnet und $\min A$ geschrieben. Das Minimum von $\{42, 23, 1000\}$ ist beispielsweise 23 und das Minimum der Menge aller ungeraden natürlichen Zahlen ist 1.

Der Satz wird Ihnen vielleicht selbstverständlich erscheinen, aber es sind trotzdem ein paar Anmerkungen angebracht.

- Mit einem Minimum einer Menge meint man ein Element dieser Menge. Darum wird die leere Menge in der Formulierung auch ausgeschlossen, denn sie kann kein Minimum haben.
- Die Aussage gilt beispielsweise *nicht* für die ganzen Zahlen. Mengen wie $\{-5,-10,-15,\dots\}$ oder $\mathbb{Z}$ selbst haben kein Minimum.
- Auch eine Menge wie $\{1/n : n \in \mathbb{N}^+\}$ hat kein Minimum. (Falls Sie an die Null gedacht hatten: die ist kein Element dieser Menge!)
- Das größte Element einer Menge A (wenn es existiert) nennt man das *Maximum von A* und schreibt dafür $\max A$. Satz 11.1 gilt offensichtlich nicht mehr, wenn man Minima durch Maxima ersetzt: Beispielsweise hat die Menge der ungeraden natürlichen Zahlen kein Maximum.

Maximum $\max A$

Aufgabe 11.1. Geben Sie $\min\{42n : n \in \mathbb{N}\}$ und $\max\{42n : n \in \mathbb{N}\}$ an, sofern sie existieren.

Aufgabe 11.2. Begründen Sie mithilfe von Satz 11.1, dass es keine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von natürlichen Zahlen mit $a_{n+1} < a_n$ für alle $n \in \mathbb{N}$ geben kann.

Aufgabe 11.3. Begründen Sie mithilfe von Satz 11.1, warum jede nichtleere *endliche* Menge von *reellen* Zahlen ein Minimum und ein Maximum hat.

Aufgabe 11.4. Warum funktioniert das Verfahren aus der Lösung von Aufgabe 11.3 nicht für unendliche Mengen von reellen Zahlen?

⋆**Aufgabe 11.5**. Satz 11.1 haben wir implizit bereits verwendet, z. B. im Abschnitt über Permutationsgruppen. Finden Sie dort die entsprechend Stelle?

Für Minima und Maxima sind auch andere Schreibweisen gebräuchlich, die aber selbsterklärend sein sollten. Das Minimum aus Aufgabe 11.1 kann man beispielsweise auch als

$$\min_{n\in\mathbb{N}} 42n$$

schreiben.

Wir kommen nun zur Teilbarkeit, die das zentrale Thema der Zahlentheorie ist. Vieles davon sollte Ihnen aus Ihrer Schulzeit bekannt vorkommen. Neu ist evtl., dass wir teilweise mit ganzen statt mit natürlichen Zahlen arbeiten.

Satz 11.2

Division mit Rest
Ist $m \in \mathbb{Z} \setminus \{0\}$, so gibt es zu jedem $a \in \mathbb{Z}$ eindeutig bestimmte Zahlen $k \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $r < |m|$ und $a = km + r$.

Beweis. Zu vorgegebenen Zahlen m und a definieren wir $R = \{a - km : k \in \mathbb{Z}\}$. Es ist hoffentlich offensichtlich, dass die Elemente von R ganze Zahlen sind, die im

Abstand m auf der Zahlengeraden liegen. Außerdem erhält man beliebig große Elemente von R, wenn man k groß genug oder – je nach Vorzeichen von m – klein genug wählt.[1] Insbesondere enthält R nicht nur negative Zahlen, d. h., $A = R \cap \mathbb{N}$ ist nicht leer und hat nach Satz 11.1 ein Minimum r. r muss kleiner als m sein, denn sonst wäre $r - |m|$ auch eine natürliche Zahl aus R und r nicht das Minimum von A. Nach Definition von R gilt außerdem $a = km + r$.

Dass r eindeutig bestimmt ist, folgt daraus, dass alle Werte, die für r infrage kommen, in R liegen und dass der nächstgrößere Wert $r + |m|$ nicht mehr kleiner als $|m|$ ist. Dass k dann auch eindeutig bestimmt ist, folgt aus der Gleichung $a = km + r$, die nur eine Lösung hat, wenn r feststeht. ■

Definition

Die Zahl r aus Satz 11.2 wird als **Rest** bei der Division von a durch m bezeichnet und $a \bmod m$ geschrieben.

$a \bmod m$ wird „*a modulo m*“ gelesen und $\bmod$ ist damit quasi eine innere Verknüpfung auf $\mathbb{Z}$ wie Addition oder Multiplikation.

Beispielsweise haben wir:

$$\begin{aligned} 14 \bmod 5 &= 4 & 14 &= 2 \cdot 5 + 4 \\ 14 \bmod -5 &= 4 & 14 &= -2 \cdot (-5) + 4 \\ -14 \bmod 5 &= 1 & -14 &= -3 \cdot 5 + 1 \\ -14 \bmod -5 &= 1 & -14 &= 3 \cdot (-5) + 1 \end{aligned}$$

Die erste Zeile dürfte Ihnen bekannt vorkommen. Die anderen drei sollten Sie sich genau anschauen, weil $\bmod$ sich auf den ersten Blick etwas überraschend verhält, wenn negative Zahlen ins Spiel kommen. Nach unserer Definition ist das Ergebnis $a \bmod m$ nie negativ. Da besteht jedoch leider mal wieder keine Einigkeit. Zum Glück ist zumindest der Gebrauch für positive m in der Mathematik einheitlich und nur für solche werden wir das auch verwenden.[2]

Aufgabe 11.6. Rechnen Sie ein paar Beispiele durch, um sich mit dieser Operation vertraut zu machen. Sie können Ihre Ergebnisse unter `https://weitz.de/mod.html` überprüfen.

Aufgabe 11.7. Wenn Sie (wie in der Klausur) nur einen einfachen Taschenrechner zur Verfügung haben, wird der höchstwahrscheinlich keine Taste für den Rest haben. Beherrscht er jedoch das Rechnen mit Brüchen, so kann man trotzdem Reste berechnen lassen. Wie?

Aufgabe 11.8. Warum steht oben „quasi“? Warum ist $\bmod$ nicht wirklich eine innere Verknüpfung im Sinne von Seite 83?

[1] Stellen Sie sich die durch $y = -mx + a$ beschriebene Gerade vor.

[2] In vielen Programmiersprachen wird für $\bmod$ das Zeichen % verwendet. Auch dort ist man sich nicht einig. Details dazu findet man hier.

Aufgabe 11.9. Für die Zahl k aus Satz 11.2 gibt es keine allgemein übliche Schreibweise. Wie kann man k aus a und m berechnen, wenn m positiv ist?

Definition

Für $a, b \in \mathbb{Z}$ bezeichnet man a als **Teiler** von b bzw. b als **Vielfaches** von a, wenn es ein $k \in \mathbb{Z}$ mit $b = ka$ gibt. Man sagt auch, dass a die Zahl b **teilt**, und schreibt dafür $a \mid b$. Die Abkürzung für $\neg(a \mid b)$ ist $a \nmid b$. Die Zahlen 1, -1, b und $-b$ nennt man **triviale Teiler** von b, alle anderen Teiler von b werden **echte Teiler** genannt.

Wie aus der Definition schon hervorgeht, sind die Zahlen 1, -1, a und $-a$ immer Teiler von a. Das folgt aus den Gleichungen $a = 1 \cdot a$ bzw. $a = (-1) \cdot (-a)$, wobei jeder der Faktoren die Rolle von k in der Definition spielen kann. Außerdem sind zwei weitere Punkte offensichtlich:

- Weil die Aussagen $b = ka$, $b = (-k)(-a)$, $-b = (-k)a$ und $-b = k(-a)$ alle äquivalent sind, kann man sich bei Teilbarkeitsfragen auf die nichtnegativen Zahlen konzentrieren.
  Konkretes Beispiel: Wenn man die positiven Teiler von 35 – also 1, 5, 7 und 35 – kennt, dann kennt man auch die negativen. Man erhält sie, indem man zu den positiven Teilern jeweils die negativen Gegenstücke hinzunimmt: -1, -5, -7 und -35. Und dann kennt man auch die Teiler von -35: es sind dieselben wie die von 35.
- Für $a \neq 0$ gilt $a \mid b$ genau dann, wenn b mod a null ist, wenn man also b ohne Rest durch a *teilen* kann.

Aufgabe 11.10. Stimmt es, dass jede Zahl mindestens vier verschiedene Teiler hat?

Aufgabe 11.11. Ist 7 ein Teiler von 0? Ist 0 ein Teiler von 7?

Aufgabe 11.12. Fallen Ihnen aus der Schule noch ein paar Regeln ein, mit denen man einer Zahl schnell ansehen kann, ob sie durch bestimmte Zahlen teilbar ist?

gerade ungerade

Aufgabe 11.13. Was sind gerade bzw. ungerade Zahlen? Das wissen Sie doch, oder?

Es folgen zwei ganz wesentliche Eigenschaften, die häufig gebraucht werden.

Lemma 11.3

Die Teilbarkeitsrelation ist transitiv, d. h., aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

Beweis. Wenn $a \mid b$ und $b \mid c$ gilt, dann gibt es nach Definition ganze Zahlen k_1 und k_2 mit $b = k_1 a$ und $c = k_2 b$. Setzt man die eine Gleichung in die andere ein, dann erhält man $c = k_2(k_1 a) = (k_2 k_1)a$. $k_2 k_1$ ist eine ganze Zahl, die „bezeugt“, dass a ein Teiler von c ist. ■

Lemma 11.4

Wenn a sowohl b als auch c teilt, dann teilt a auch $xb + yc$, wobei x und y beliebige (ganze) Zahlen sind.

Beweis. Wenn $a \mid b$ und $a \mid c$ gilt, dann gibt es nach Definition ganze Zahlen k_1 und k_2 mit $b = k_1 a$ und $c = k_2 a$. Nun kann man wieder einsetzen und erhält $xb + yc = xk_1 a + yk_2 a = (xk_1 + yk_2)a$. Die ganze Zahl $xk_1 + yk_2$ „bezeugt“ die zu beweisende Aussage. ■

Einen Ausdruck der Form $xb+yc$ nennt man eine *Linearkombination* von b und c.[3] Beachten Sie, dass u. a. auch Fälle wie $x = y = 1$ oder $x = 1$ und $y = -1$ durch Lemma 11.4 abgedeckt werden. Die Summe $b + c$ und die Differenz $b - c$ sind also insbesondere auch durch a teilbar, wenn b und c es sind.

Linearkombination

Wenn c Teiler von a ist, folgt aus der Definition offenbar $|c| \leq |a|$, wenn a nicht null ist. Zwei beliebige Zahlen a und b haben also erstens immer mindestens einen *gemeinsamen* positiven Teiler (nämlich 1) und zweitens können ihre gemeinsamen Teiler nicht größer als $\min\{|a|, |b|\}$ sein.[4] Daher ergibt die folgende Definition Sinn.

Definition

Der **größte gemeinsame Teiler** $\mathrm{ggT}(a, b)$ von a und b ist die größte Zahl, die a und b teilt, wenn $\{a, b\} \neq \{0\}$ gilt.[5] Zur Vervollständigung der Definition setzen wir außerdem $\mathrm{ggT}(0, 0) = 0$.

Beispielsweise hat 20 die positiven Teiler 1, 2, 4, 5, 10 und 20 und 35 hat die positiven Teiler 1, 5, 7 und 35. Die größte Zahl, die in beiden Aufzählungen vorkommt, ist 5. Also gilt $\mathrm{ggT}(20, 35) = 5$. Offenbar ist der größte gemeinsame Teiler zweier Zahlen nie negativ und nur dann null, wenn beide Zahlen verschwinden.[6]

Aufgabe 11.14. Welchen Wert haben $\mathrm{ggT}(-20, 35)$, $\mathrm{ggT}(20, -35)$ und $\mathrm{ggT}(-20, -35)$?

Aufgabe 11.15. Und was ist mit $\mathrm{ggT}(42, 42)$ und $\mathrm{ggT}(0, 42)$?

Wie berechnet man den größten gemeinsamen Teiler? Man könnte erst alle Teiler der beiden Zahlen ermitteln und dann den größten herauspicken, der sich in beiden Mengen befindet. Das wäre aber sehr ineffizient. Zum Glück kennt man seit der Zeit von Euklid ein cleveres Verfahren, das erstaunlicherweise auch zwei Jahrtausende später noch immer der beste bekannte Algorithmus für diese Aufgabe ist und das in dieser Form auch von Computern eingesetzt wird. Es ist der *euklidische Algorithmus* zur Berechnung von $\mathrm{ggT}(a, b)$:[7]

euklidischer Algorithmus

(i) Setze `A` und `B` auf die Werte a und b.

(ii) Gilt `A` $= 0$, dann ist das Ergebnis `B` und der Algorithmus ist beendet.

(iii) Ist `B` $= 0$, dann ist das Ergebnis `A` und der Algorithmus ist beendet.

[3] Genauer: eine Linearkombination mit ganzzahligen Koeffizienten.

[4] Auch hier wieder mit der Ausnahme, dass nicht $a = b = 0$ gelten darf.

[5] Manchmal wird statt $\mathrm{ggT}(a, b)$ auch einfach (a, b) geschrieben.

[6] *Verschwinden*? Was soll das denn bedeuten? Das ist mal wieder Mathematikerschnack. Wenn man sagt, dass etwas verschwindet, dann meint man damit, dass es null ist.

[7] Falls Sie sich an Seite 36 erinnern, auf der man lesen kann, dass sich in der Mathematik die Werte von Variablen nie ändern: `A` und `B`, die sich absichtlich typographisch von a und b unterscheiden, sind keine Variablen, sondern so etwas wie Speicherplätze in einem Computer.

(iv) Ist `A` > `B`, dann ersetze `A` durch `A` − `B`, anderenfalls ersetze `B` durch `B` − `A`.

(v) Fahre fort mit Schritt (iii).

Schauen wir uns zunächst ein Beispiel an. Hier wird in jeder Zeile der Stand eines Durchlaufs am Punkt (iii) gezeigt.

`A`	`B`
400	225
175 = 400 − 225	225
175	50 = 225 − 175
125 = 175 − 50	50
75 = 125 − 50	50
25 = 75 − 50	50
25	25 = 50 − 25
25	0 = 25 − 25

Am Ende haben wir ggT(400, 225) = 25 errechnet.

Aufgabe 11.16. Rechnen Sie selbst ein paar Beispiele durch. Ruhig auch mit größeren Zahlen. Der Algorithmus wird trotzdem immer nach recht wenigen Schritten zu einem Ergebnis kommen. Sie können Ihre Resultate überprüfen, indem Sie z. B. in Wolfram Alpha so etwas wie `gcd(400,225)` eingeben.[8]

Satz 11.5 Der euklidische Algorithmus liefert für jede Eingabe $a, b \geq 0$ immer den größten gemeinsamen Teiler von a und b.

Beweis. Zunächst einmal wird durch (ii) und (iii) dafür gesorgt, dass das Ergebnis korrekt ist, wenn mindestens eine der beiden Zahlen null ist. Für den Rest des Beweises nennen wir nun die Werte, die `A` und `B` nach dem n-ten Schritt annehmen, a_n und b_n. (Wir starten also mit $a_0 = a$ und $b_0 = b$.)

Nach dem n-ten Schritt haben wir $a_{n+1} = a_n - b_n$ und $b_{n+1} = b_n$ oder $a_{n+1} = a_n$ und $b_{n+1} = b_n - a_n$. In beiden Fällen folgt aus Lemma 11.4 bzw. der Bemerkung dahinter, dass jeder gemeinsame Teiler von a_n und b_n auch einer von a_{n+1} und b_{n+1} ist. Umgekehrt kann man jedoch auch argumentieren: Wir haben entweder $a_n = a_{n+1} + b_{n+1}$ und $b_n = b_{n+1}$ oder $a_n = a_{n+1}$ und $b_n = a_{n+1} + b_{n+1}$. Mit derselben Begründung folgt, dass jeder gemeinsame Teiler von a_{n+1} und b_{n+1} auch einer von a_n und b_n ist. Mit anderen Worten: Den ganzen Algorithmus über bleibt die Menge der gemeinsamen Teiler von `A` und `B` gleich und damit auch deren größter gemeinsamer Teiler. Da es mit den Werten a und b losgeht und am Ende `A` korrekterweise als größter gemeinsamer Teiler von `A` und 0 ausgegeben wird, ist das Resultat richtig.

Wir sind aber noch nicht fertig! Wir müssen uns noch überzeugen, dass der Algorithmus auch immer terminiert.[9] Das kann man sich folgendermaßen klarmachen: a_n

[8] Im Englischen (und vielen Programmiersprachen) heißt es *greatest common divisor*.

[9] Siehe dazu auch die Bemerkung im Lösungshinweis für Aufgabe 11.3.

und b_n können nie negative Werte annehmen und in jedem Schritt ist $a_{n+1} + b_{n+1}$ kleiner als $a_n + b_n$. Das kann nicht immer so weitergehen, denn sonst stünde die Folge $(a_n + b_n : n \in \mathbb{N})$ im Widerspruch zu Aufgabe 11.2. ■

Weil wir gerade gesehen haben, dass sich die Menge der gemeinsamen Teiler von A und B die ganze Zeit nicht ändert und da A und B am Ende die Werte $d = \text{ggT}(a,b)$ und 0 haben, besteht diese Menge aus den Teilern von d. Damit folgt:[10]

Korollar 11.6

Es gilt genau dann $d = \text{ggT}(a,b)$, wenn d Teiler von a und b ist und jeder gemeinsame Teiler von a und b auch d teilt.

Wir wissen nach Lemma 11.4 bereits, dass jeder gemeinsame Teiler von a und b jede Linearkombination von a und b teilt. Aus dem euklidischen Algorithmus ergibt sich zusätzlich noch das Folgende:

Korollar 11.7

Lemma von Bézout
ggT(a,b) lässt sich als Linearkombination von a und b darstellen.

Die Begründung für diese Aussage ist, dass sowohl A als auch B in jedem Schritt Linearkombinationen von a und b sind. Denn am Anfang sind sie es[11] und in jedem Schritt danach werden Linearkombinationen der vorherigen Werte gebildet, die wieder Linearkombinationen der Ausgangswerte sind:

$$x(x_1 a + y_1 b) + y(x_2 a + y_2 b) = (xx_1 + yx_2)a + (xy_1 + yy_2)b$$

Darum ist auch der letzte Wert, also das Ergebnis des Algorithmus, eine solche Linearkombination.

Hier sieht man das noch einmal am Beispiel von vorhin:

A	B
$400 = a$	$225 = b$
$175 = a - b$	$225 = b$
$175 = a - b$	$50 = b - (a-b) = 2b - a$
$125 = (a-b) - (2b-a) = 2a - 3b$	$50 = 2b - a$
$75 = (2a-3b) - (2b-a) = 3a - 5b$	$50 = 2b - a$
$25 = (3a-5b) - (2b-a) = 4a - 7b$	$50 = 2b - a$
$25 = 4a - 7b$	$25 = (2b-a) - (4a-7b) = -5a + 9b$
$25 = -5a + 9b$	0

Aufgabe 11.17. Rechnen Sie für die Werte aus Aufgabe 11.16 auch solche Linearkombinationen aus. Ob die Ergebnisse richtig sind, lässt sich ja leicht überprüfen.

[10] Daher ist die Setzung ggT$(0,0) = 0$ auch nicht willkürlich, sondern die einzige, die zu dieser Charakterisierung passt.

[11] A ist $1 \cdot a + 0 \cdot b$, B ist $0 \cdot a + 1 \cdot b$.

⋆**Aufgabe 11.18**. Ist die Linearkombination, die der euklidische Algorithmus liefert, eindeutig bestimmt? (Hinweis: Wenn man $3 \cdot 14$ Schritte vorwärts und dann $14 \cdot 3$ Schritte rückwärts macht, ist man wieder am Ausgangspunkt.)

Aufgabe 11.19. Im Beispiel mit 400 und 225 wurde dreimal nacheinander 50 subtrahiert. Das hätte man auch einfacher haben können, oder? Mit anderen Worten: Man hätte doch gleich sehen können, dass 50 in 175 dreimal „reinpasst“ und dass es eigentlich um etwas anderes geht. Formulieren Sie eine verbesserte Form des euklidischen Algorithmus, die das berücksichtigt.

Definition

Zwei Zahlen werden **teilerfremd** genannt, wenn ihr größter gemeinsamer Teiler eins ist.

Aufgabe 11.20. Nach dem Lemma von Bézout gibt es zu teilerfremden Zahlen a und b Zahlen x und y mit $1 = xa + yb$. Begründen Sie die umgekehrte Aussage: Wenn es Zahlen x und y mit $1 = xa + yb$ gibt, dann sind a und b teilerfremd.

Wenn eine Zahl ein Produkt teilt, muss sie nicht notwendig einen der Faktoren teilen. Beispielsweise teilt 6 die Zahl $30 = 3 \cdot 10$, aber 6 teilt weder 3 noch 10. Es gilt jedoch:

Lemma 11.8

Aus $a \neq 0$, $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$ folgt $a \mid c$.

Beweis. Nach dem Lemma von Bézout gibt es x und y mit $1 = xa + yb$. Multiplikation mit c liefert $c = (xc)a + y(bc)$. Nun stehen rechts zwei Summanden, die durch a teilbar sind. (Der zweite nach Lemma 11.3.) Nach Lemma 11.4 ist auch ihre Summe, also c, durch a teilbar. ■

⋆**Aufgabe 11.21**. Kann man natürliche Zahlen x und y finden, für die $x!y! = x! + y! + 2$ gilt? Begründen Sie Ihre Antwort.

⋆**Aufgabe 11.22**. Eine Knobelaufgabe, mit der man viele Teilbarkeitsregeln üben kann: Finden Sie eine neunstellige Zahl mit der folgenden Eigenschaft: Die aus den ersten beiden Ziffern gebildete Zahl ist durch 2 teilbar, die aus den ersten drei Ziffern gebildete Zahl ist durch 3 teilbar, die aus den ersten vier Ziffern gebildete Zahl ist durch 4 teilbar und so weiter – schließlich soll die gesamte Zahl durch 9 teilbar sein. Außerdem soll jede der Ziffern 1 bis 9 in der Dezimaldarstellung der Zahl genau einmal vorkommen.

⋆ Teilbarkeit im Computer

In PYTHON wird das Zeichen `%` für mod verwendet. Die Zahl k aus Satz 11.2 kann man mit `a//m` berechnen. In beiden Fällen wird man jedoch nicht immer dieselben Ergebnisse wie in diesem Kapitel erhalten, wenn negative Zahlen ins Spiel kommen. Da sollten Sie vorsichtshalber die Dokumentation lesen. Den Test auf Teilbarkeit könnte man jedenfalls so programmieren:

```
divides = lambda a,b: b==0 or a!=0 and b%a==0
```

Die wortwörtliche Übersetzung des euklidischen Algorithmus von oben sieht folgendermaßen aus:

```
def ggT(a,b):
  if a==0:
    return b
  while b!=0:
    if a>b:
      a = a-b
    else:
      b = b-a
  return a
```

Aber man muss das nicht selbst machen:

```
from math import gcd
gcd(400,225)
```

Sogar für die Faktoren aus dem Lemma von Bézout kann man sich eine fertige Funktion laden, wenn man die Bibliothek SymPy installiert hat.[12]

```
from sympy import gcdex
gcdex(400,225)
```

Und in Kapitel 5 von *Konkrete Mathematik (nicht nur) für Informatiker* sowie in den zugehörigen Lösungshinweisen findet man diverse Beispiele dafür, wie man das auch selbst programmieren kann.

12. Primzahlen

Nun kommen wir zu den Hauptakteuren der Zahlentheorie.

Definition

Eine ganze Zahl, die größer als 1 ist, heißt **Primzahl**,[13] wenn sie außer den trivialen Teilern keine weiteren hat. Positive Zahlen, die mehr als zwei positive Teiler haben, werden **zusammengesetzt** genannt.

Damit haben wir drei Kategorien für positive natürlichen Zahlen. Jede dieser Zahlen landet in genau einer dieser Kategorien.

– Die Primzahlen sind die, die nur zwei positive Teiler – nämlich die trivialen – haben, z. B. 2, 3 oder 104 729.

[12] Das Kürzel `ex` steht für *extended*. Wenn man nicht nur den größten gemeinsamen Teiler, sondern nebenbei noch diese Faktoren ausrechnet, spricht man auch vom *erweiterten* euklidischen Algorithmus.

[13] Man verwendet auch das Adjektiv *prim*. prim

- Die zusammengesetzten Zahlen sind die, die mehr als zwei positive Teiler haben, also außer den trivialen noch mindestens einen weiteren. Beispiele sind 4 (durch 2 teilbar) oder 161 051 (u. a. durch 11 teilbar).
- Die Zahl 1.

Viele Menschen finden es verwunderlich, dass die Eins eine eigene Kategorie bekommt. Hat sie nicht wie die Primzahlen keine Teiler außer den trivialen und sollte sie deswegen nicht auch eine Primzahl sein? In der Tat hat man das früher teilweise so gesehen. Es hat sich jedoch herausgestellt, dass die obige Unterteilung wesentlich praktischer ist. Ich erinnere noch einmal an die Anmerkung auf Seite 40, in der erklärt wird, dass Definitionen nicht wahr oder falsch sein können, sondern bestenfalls sinnvoll oder weniger sinnvoll. Inzwischen ist sich die Mathematikerzunft einig, dass die aktuelle Definition die sinnvollste ist.

Aufgabe 12.1. Zwischendurch mal wieder etwas Mengenlehre. Wie kann man die Menge der zusammengesetzten Zahlen möglichst kurz und knapp hinschreiben?

Definition

Ein Teiler einer Zahl a, der eine Primzahl ist, wird **Primteiler** oder **Primfaktor** von a genannt.

42 hat also z. B. die Primteiler 2, 3 und 7, aber auch noch die Teiler 1, 6, 14, 21 und 42, die alle *keine* Primteiler sind.

Lemma 12.1

Jede Zahl, die größer als 1 ist, hat (mindestens) einen Primteiler.

Beweis. Wir führen einen Beweis durch Widerspruch durch und nehmen dafür an, dass es Zahlen gibt, die größer als 1 sind und keinen Primteiler haben. Nach Satz 11.1 gibt es dann eine *kleinste* Zahl a mit dieser Eigenschaft. Wegen $a > 1$ hat a mindestens einen Teiler, der größer als 1 ist, nämlich a. Wenn das der einzige Teiler dieser Art wäre, dann wäre a eine Primzahl und damit gleichzeitg ein Primteiler von a. Das kann nicht sein, also gibt es einen weiteren Teiler b zwischen 1 und a. Weil a minimal gewählt wurde und b kleiner ist, hat b jedoch einen Primteiler, der nach Lemma 11.3 auch ein Primteiler von a ist. Da haben wir den Widerspruch. ■

Da jede Primzahl p nur die zwei positiven Teiler 1 und p hat, ist der größte gemeinsame Teiler von p und irgendeiner anderen Zahl a eine dieser beiden Zahlen. Entweder sind p und a also teilerfremd oder p teilt a. Damit hat man nach Lemma 11.8 sofort:

Korollar 12.2

Wenn eine Primzahl p ein Produkt $a_1 a_2 \cdots a_n$ teilt, dann teilt p (mindestens) einen der Faktoren a_1 bis a_n.

Aufgabe 12.2. Formulieren Sie eine etwas ausführlichere Begründung für Korollar 12.2.

Die Menge der zusammengesetzten Zahlen hat offensichtlich unendlich viele Elemente, denn bereits die Menge der geraden Zahlen ist unendlich und bis auf 2 sind alle geraden Zahlen zusammengesetzte Zahlen. Der Menge der Primzahlen hatten wir bereits das Symbol $\mathbb{P}$ spendiert und wir wissen, dass sie so aussieht:

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}.$$

Aber bedeuten die Auslassungspunkte, dass es immer so weiter geht? Ja! Das besagt ein Satz, der schon vor Beginn der Zeitrechnung bewiesen wurde.

Satz des Euklid **Satz 12.3**
Es gibt unendlich viele Primzahlen, d. h., $\mathbb{P}$ ist eine unendliche Menge.

Beweis. Damals hätte man das allerdings nicht so formuliert, weil man mit dem Begriff des Unendlichen sehr vorsichtig war. In der ursprünglichen Form besagt der Satz: Zu jeder endlichen Menge M von Primzahlen kann man (mindestens) eine finden, die nicht in M enthalten ist. So werden wir das jetzt auch beweisen.[14] Wir betrachten die ersten n Primzahlen, die wir p_1, p_2 und so weiter bis p_n nennen und begründen, warum das nicht *alle* Primzahlen sind.

Dazu setzen wir $Q = 1 + p_1 p_2 \cdots p_n$. Offenbar erhält man, wenn man Q durch eine der Primzahlen p_1 bis p_n dividiert, als Rest immer 1. Also ist keine dieser Zahlen ein Teiler von Q. Nach Lemma 12.1 muss Q jedoch einen Primteiler haben. Das ist dann zwangsläufig eine Primzahl, die nicht in der Ausgangsmenge $\{p_1, p_2, \ldots, p_n\}$ enthalten ist. ■

Aufgabe 12.3. Ein häufiges Missverständnis ist, dass die im Beweis von Satz 12.3 definierte Zahl Q selbst eine Primzahl sei. Und Zahlen wie $2+1=3$, $2\cdot 3+1=7$ und $2\cdot 3\cdot 5+1=31$ sind in der Tat Primzahlen. Begründen Sie mit einem konkreten Gegenbeispiel, dass diese Annahme trotzdem falsch ist.

Die folgende Aussage erklärt, warum die Primzahlen so wichtig sind. Sie sind gleichsam die „Bausteine“ der Zahlenwelt, aus denen die anderen Zahlen zusammengesetzt sind. Man könnte fast von den „Atomen der Arithmetik“ sprechen: Ein Kohlenstoffmonoxid-Molekül besteht beispielsweise immer aus einem Kohlenstoff- und einem Sauerstoffatom. Da wird nicht auf einmal ein zweites Sauerstoffatom auftauchen oder der Kohlenstoff durch Natrium ersetzt werden.[15] So ist das auch mit den Primzahlen.

Fundamentalsatz der Arithmetik **Satz 12.4**
Jede positive ganze Zahl lässt sich eindeutig (bis auf die Reihenfolge) als Produkt von Primzahlen darstellen.

[14] Wir haben diesen Satz auf Seite 23 übrigens schon bewiesen. Die hier gezeigte Variante ist jedoch näher am Original.

[15] Allerdings hinkt der Vergleich etwas, weil es nur endlich viele chemische Elemente gibt, während wir gerade bewiesen haben, dass es unendlich viele Primzahlen gibt.

Beweis. Zunächst sollten wir klären, was mit „eindeutig (bis auf die Reihenfolge)“ gemeint ist. Die Reihenfolge eines Produktes kann bei unterschiedlichen Faktoren gar nicht eindeutig festliegen, weil die Multiplikation kommutativ ist. $2\cdot 2\cdot 7$ ist nun einmal dasselbe wie $2\cdot 7\cdot 2$. Aber bei der Auswahl der Faktoren und der Häufigkeit ihres Auftretens gibt es nach diesem Satz nur eine Möglichkeit: Weil man 28 als Produkt von zwei Zweien und einer Sieben darstellen kann, gibt es keine andere Möglichkeit – weder durch Ersetzen einzelner Faktoren durch andere Primzahlen noch durch Erhöhen oder Verringern der Anzahl der Faktoren kann man 28 darstellen: es geht nur mit zwei Zweien und einer Sieben.

Dass sich überhaupt jede positive Zahl a als Produkt von Primzahlen darstellen lässt, ist aufgrund der bereits bewiesenen Aussagen einfach zu begründen. Man findet nach Lemma 12.1 einen Primfaktor p von a, wenn a nicht gerade eins ist. Dann schaut man sich a/p an. Das ist eine ganze Zahl und ein Teiler von a. Jeder Teiler dieser Zahl ist auch ein Teiler von a. Für diese Zahl findet man wieder einen Primteiler und verfährt dann ebenso. Weil die Zahlen in jedem Schritt kleiner werden, muss dieser Prozess nach Satz 11.1 bzw. Aufgabe 11.2 irgendwann aufhören. Das kann nur daran liegen, dass sich durch die Division die Zahl 1 eins ergeben hat. Das Produkt aller bis dahin erhaltenen Primteiler ist das gesuchte.[16]

Ein bisschen aufwendiger ist der Beweis der Eindeutigkeit. Das erledigen wir wieder mit einem Widerspruch und nehmen an, es gäbe Beispiele von Zahlen, die sich auf mindestens zwei unterschiedliche Arten als Produkt von Primzahlen darstellen lassen. Dann gibt es nach Satz 11.1 Beispiele, bei denen die Gesamtanzahl der Faktoren minimal ist.[17] So ein Beispiel greifen wir uns heraus. Wir haben also

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m, \tag{12.1}$$

wobei alle Faktoren p_i und q_j Primzahlen sind, die links und rechts der Größe nach sortiert sind und für die $(p_1,\dots,p_n) \neq (q_1,\dots,q_m)$ gilt – entweder wegen $m \neq n$ oder weil die Einträge nicht alle übereinstimmen. Nach Korollar 12.2 teilt p_1 einen Faktor q_j des rechten Produkts. Weil beides Primzahlen sind, folgt $p_1 = q_j$. Man kann daher in Gleichung (12.1) auf beiden Seiten durch p_1 dividieren und erhält eine neue Gleichung, die ebenfalls ein Gegenbeispiel zum Fundamentalsatz ist. Das ist jedoch ein Widerspruch, weil in dieser neuen Gleichung insgesamt zwei Faktoren weniger als in (12.1) auftreten. ■

⋆**Aufgabe 12.4**. Wie genau ist das mit der Minimalität am Ende des Beweises von Satz 12.4 gemeint?

⋆**Aufgabe 12.5**. Vielleicht schauen Sie sich nun Aufgabe 6.36 und die Lösung dazu noch einmal an, falls Ihnen vorher nicht ganz klar war, worum es ging.

[16] Z. B. könnten Sie für $a = 63$ den Primteiler 3 finden. Division ergibt 21. Zu dieser Zahl finden Sie vielleicht den Primteiler 7. Division ergibt 3 und hier können Sie nur noch den Primteiler 3 finden. Erneute Division führt auf 1 und der Prozess ist damit beendet. Insgesamt haben Sie die Primteiler 3, 7 und noch einmal 3 gesammelt und kommen damit auf $63 = 3\cdot 3\cdot 7$.

[17] Siehe dazu die auf den Beweis folgende Aufgabe 12.4.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Eventuell haben Sie sich gefragt, wie man eine Primzahl oder die Zahl eins als Produkt von Primzahlen darstellen soll. Das lässt sich aber wie in Anmerkung hinter Satz 9.4 beantworten: Eine Primzahl lässt sich als ein Produkt darstellen, das aus *einem* Faktor besteht, und die Eins ist das Produkt von *null* Primzahlen. (Siehe dazu auch die Anmerkung zu 0! auf Seite 60.)

Die Reihenfolge spielt zwar für das Ergebnis keine Rolle, aber man kann die an einem Produkt beteiligten Faktoren natürlich trotzdem sortieren und gleiche Faktoren zu Potenzen zusammenfassen. Damit erhält man dann die sogenannte *kanonische Primfaktorzerlegung*, für die wir hier ein paar Beispiele sehen:

kanonische Primfaktorzerlegung

$$16 = 2^4 \qquad 27 = 3^3$$
$$42 = 2 \cdot 3 \cdot 7 \qquad 43 = 43$$
$$96 = 2^5 \cdot 3 \qquad 1\,320\,574\,363 = 29^2 \cdot 31 \cdot 37^3$$

Aufgabe 12.6. Berechnen Sie zur Übung ein paar Primfaktorzerlegungen. Sie können Ihre Ergebnisse z. B. kontrollieren, indem Sie so etwas wie `factor 1320574363` in Wolfram Alpha eingeben.

Aufgabe 12.7. Wenn Sie (wie in der Klausur) nur einen einfachen Taschenrechner zur Verfügung haben und die Primfaktorzerlegung einer großen Zahl wie 32 892 berechnen sollen, wie gehen Sie dann „strategisch“ am besten vor?

Aufgabe 12.8. In Aufgabe 12.7 kommt die Zahl 2 741 vor, von der Sie sicher nicht aus dem Kopf wissen, dass es eine Primzahl ist. Wie kann man sich mit möglichst wenigen Divisionen sicher sein, dass eine Zahl prim ist?

Aufgabe 12.9. Welcher Zusammenhang besteht zwischen dem größten gemeinsamen Teiler zweier Zahlen und deren Primfaktorzerlegungen?

Aufgabe 12.10. Sie haben sicher schon einmal etwas vom *kleinsten gemeinsamen Vielfachen* zweier Zahlen a und b gehört: Zwei beliebige Zahlen a und b, die beide nicht verschwinden, haben immer mindestens ein gemeinsames positives Vielfaches, nämlich $|a| \cdot |b|$. Nach Satz 11.1 gibt es daher ein *kleinstes positives* Vielfaches, das beide gemeinsam haben. Dafür schreibt man $\mathrm{kgV}(a, b)$. (Und ergänzend setzt man $\mathrm{kgV}(a, b) = 0$, wenn $ab = 0$ gilt.)

kleinstes gemeinsames Vielfaches

$\mathrm{kgV}(a, b)$

Berechnen Sie das kleinste gemeinsame Vielfache für ein paar Zahlenpaare oder lassen Sie es berechnen, z. B. in Wolfram Alpha mit einer Eingabe wie `lcm(400,225)`.[18]

Aufgabe 12.11. Erkennen Sie einen Zusammenhang zwischen $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ sowie a und b?

⋆ Primzahlen im Computer

Die schon erwähnte Bibliothek SymPy enthält diverse zahlentheoretische Funktionen, zum Beispiel diese drei:

[18] Im Englischen *least common multiple*.

```
from sympy import prime,isprime,factorint

prime(424242)           # n-te Primzahl
factorint(4200420042)   # Primfaktorzerlegung
isprime(4242424243)     # Test, ob Argument prim ist
```

Grundsätzlich ist allerdings zu beachten, dass das Finden von Teilern bzw. das Zerlegen in Primfaktoren ein schwieriges mathematisches Problem ist, für das bisher keine effizienten Algorithmen bekannt sind. Auf diesem „Mangel“ basieren diverse kryptographische Verfahren.

Auch ein verlässlicher Test, ob eine Zahl eine Primzahl ist, ist für große Argumente recht zeitaufwendig. Funktionen wie `isprime` arbeiten deshalb in der Regel probabilistisch und liefern Ergebnisse, die mit einer geringen Wahrscheinlichkeit auch falsch sein können. In Kapitel 9 von *Konkrete Mathematik (nicht nur) für Informatiker* wird der in der Praxis am häufigsten eingesetzte Primzahltest ausführlich besprochen und auch in PYTHON implementiert. Im 10. Kapitel wird das weit verbreitete RSA-Kryptosystem erläutert, das die gerade angesprochene Schwierigkeit bei der Faktorisierung ausnutzt. Damit Sie diese beiden Kapitel verstehen, sollten Sie aber erst den folgenden Abschnitt über modulare Arithmetik durcharbeiten.

13. Modulare Arithmetik

Viele Fragestellungen der Zahlentheorie lassen sich dadurch vereinfachen, dass man mit *Resten* arbeitet.

Definition

Sei $n > 1$. Durch $a \bmod n = b \bmod n$ wird eine Äquivalenzrelation[19] auf $\mathbb{Z}$ definiert. Man sagt dazu: a **ist kongruent zu** b **modulo** n.
Für die Äquivalenzklasse der Zahl a schreiben wir $[a]_n$ und für die Faktormenge $\mathbb{Z}/n\mathbb{Z}$. Diese Menge nennt man den **Restklassenring modulo** n und ihre Elemente **Restklassen**.

Beachten Sie, dass hier unendlich viele Äquivalenzrelationen definiert wurden – für jedes n eine. Wir werden im Folgenden zwar meistens allgemein für alle n argumentieren, aber im konkreten Anwendungsfall arbeiten wir dann mit einem festen n und entsprechend nur mit einer Äquivalenzrelation zur Zeit. Warum von *Ringen* die Rede ist, wird noch klar werden.

> **Aufgabe 13.1**. Wie sehen die Äquivalenzklassen und die Faktormenge für ein konkretes Beispiel wie $n = 6$ aus?

Dass zwei Zahlen in der gerade definierten Relation zueinander stehen, kann man auch anders ausdrücken:

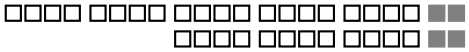
[19] Dass es sich um eine Äquivalenzrelation handelt, folgt aus Aufgabe 6.11, weil wir es mit einer Funktion zu tun haben, die dem Argument a den Funktionswert $a \bmod n$ zuordnet.

Für $n > 1$ und $a, b \in \mathbb{Z}$ gilt $[a]_n = [b]_n$ genau dann, wenn $n \mid a - b$ gilt. **Lemma 13.1**

Beweis. Haben a und b denselben Rest r bei Division durch n, dann gibt es Zahlen k_1 und k_2 mit $a = k_1 n + r$ und $b = k_2 n + r$. Das liefert die Differenz $a - b = (k_1 - k_2)n$, was gleichbedeutend mit $n \mid a - b$ ist.

Ist umgekehrt die Differenz $a - b$ durch n teilbar, dann gibt es ein k mit $a - b = kn$. Hat nun b den Rest r, wenn man durch n teilt, dann bedeutet das $b = jn + r$ für eine ganze Zahl j. Damit ergibt sich $a = b + (a - b) = jn + r + kn = (j + k)n + r$, d. h., auch a hat diesen Rest. ■

Weil ein Bild angeblich mehr als tausend Worte sagt, hier eine Illustration für das konkrete Beispiel $n = 4$, $a = 22$ und $b = 14$. Rechts jeweils in grau der Rest 2, der sich bei der Division durch 4 ergibt, und links daneben Gruppen zu je 4 Blöcken. Ich glaube, man *sieht* den Zusammenhang, den Lemma 13.1 behauptet.



Die durch die Relation induzierte Partition zerlegt also $\mathbb{Z}$ in n Mengen, die jeweils aus Zahlen bestehen, die gleichmäßig auf der Zahlengeraden verteilt sind. Diese Zahlen haben zu ihren beiden direkten „Nachbarn“ aus derselben Äquivalenzklasse den Abstand n. In der folgenden Grafik sieht man das für $n = 3$ an einem Ausschnitt von $\mathbb{Z}$ dargestellt. Die Farben stehen dabei für

$$[0]_3 = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\},$$
$$[1]_3 = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, \ldots\} \text{ und}$$
$$[2]_3 = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Nun der entscheidende Grund für die Nützlichkeit der Restklassenringe:

Sei $n > 1$. Gilt $[a]_n = [c]_n$ und $[b]_n = [d]_n$, dann gelten auch[20] **Satz 13.2**

$$[a \pm b]_n = [c \pm d]_n \text{ und}$$
$$[a \cdot b]_n = [c \cdot d]_n.$$

Beweis. Wir verwenden für die Argumentation die Darstellung aus Lemma 13.1. Wegen $[a]_n = [c]_n$ und $[b]_n = [d]_n$ gibt es k_1 und k_2 mit $a - c = k_1 n$ und $b - d = k_2 n$. Daraus folgt

$$(a \pm b) - (c \pm d) = (a - c) \pm (b - d) = k_1 n \pm k_2 n = (k_1 \pm k_2)n$$

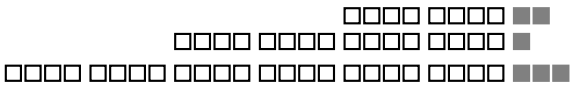
[20] Das Zeichen ± in der ersten Zeile ist eine gelegentlich verwendete Abkürzung. Gemeint sind eigentlich zwei Zeilen, eine für + und eine für −, und ± steht durchgehend für einen der beiden Operatoren, aber immer für denselben.

und das war's schon: die Differenz ganz links ist durch n teilbar. Wie in der Formulierung des Satzes kann $\pm$ sowohl für Addition als auch für Subtraktion stehen. $k_1 \pm k_2$ ist in beiden Fällen eine ganze Zahl.

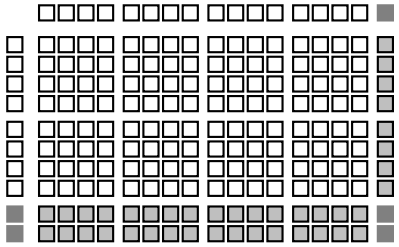
Für die Multiplikation muss man ein kleines bisschen mehr rechnen, aber auch in diesem Fall kommt am Ende ein Vielfaches von n heraus:

$$\begin{aligned} ab - cd &= ab - cb + cb - cd = (a-c)b + c(b-d) \\ &= k_1 nb + ck_2 n = (k_1 b + ck_2)n. \end{aligned}$$ ■

Auch von diesem Satz kann man sich durch Grafiken überzeugen lassen. In der folgenden Skizze sieht man die beiden Zahlen $a = 10$ und $b = 17$ und darunter deren Summe 27. Entscheidend sind jedoch die rechts grau dargestellten Reste bei Division durch $n = 4$. Zeichnen Sie ein vergleichbares Bild für Zahlen c und d, die kongruent zu a bzw. b modulo 4 sind, z. B. $c = 18$ und $d = 5$. Sie werden sehen, dass der rechte Teil der Grafik identisch ist.



Schließlich noch eine Grafik für das Produkt von 10 (vertikal) und 17 (horizontal), wo Sie ebenfalls selbst ein bisschen kritzeln und nachdenken sollten, wenn Ihnen nicht ohnehin schon alles klar ist.



Aufgabe 13.2. Was bisher in diesem Abschnitt passiert ist, erfordert keine großen Rechenkünste, aber haben Sie die Konzepte dahinter verstanden? Lesen Sie nicht einfach weiter, sondern stellen Sie sicher, dass Sie Fragen wie die folgenden beantworten können: Was ist $[3]_7$? Was ist $\mathbb{Z}/7\mathbb{Z}$? Welcher Zusammenhang besteht zwischen diesen beiden Objekten? Besteht ein Zusammenhang zwischen $[3]_7$ und $[7]_3$? Können Sie zwei verschiedene Methoden angeben, mit denen man begründen kann, warum $[424242]_{11}$ und $[424341]_{11}$ identisch sind?

Aufgabe 13.3. Warum kommen in Satz 13.2 nur drei der vier Grundrechenarten vor? Was ist mit der Division?

Wir können nun definieren, wie man mit Restklassen rechnet:

Definition

Sei $n > 1$. Wir definieren

$$[a]_n \pm [b]_n = [a \pm b]_n \text{ und}$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n.$$

Es mag sein, dass Ihnen das sowohl banal als auch sinnlos vorkommt. Nach dieser Definition haben wir beispielsweise $[4]_5 + [3]_5 = [7]_5$ und $[4]_5 \cdot [3]_5 = [12]_5$. Was soll das? Dass $4 + 3 = 7$ und $4 \cdot 3 = 12$ gilt, wissen Sie schon seit der Grundschule. Nun soll durch das Hinzufügen von eckigen Klammern etwas Neues entstanden sein? Das ist in der Tat so:

- Zunächst einmal handelt es sich um eine *Definition* und nicht um einen *Satz*. Es wird festgelegt, was Ausdrücke wie $[a]_n + [b]_n$ bedeuten sollen.
- Und was wird definiert? Auf der linken Seite der Gleichungen stehen jeweils zwei Äquivalenzklassen und rechts steht auch eine. Hier werden also innere Verknüpfungen auf $\mathbb{Z}/n\mathbb{Z}$ definiert.
- Das bedeutet, dass die Zeichen $+$, $-$ und $\cdot$ links und rechts von den Gleichheitszeichen für *unterschiedliche* Funktionen stehen, denn rechts ist einfach die Verknüpfung ganzer Zahlen gemeint. Diese Art von Operatorüberladung kennen Sie vielleicht schon vom Programmieren und auf jeden Fall aus dem letzten Kapitel. Hier wird es aber noch konkreter und die Gefahr von Verwechslungen wird größer.

  Der französische Mathematiker Henri Poincaré hat einmal gesagt: „Mathematik ist die Kunst, unterschiedlichen Dingen denselben Namen zu geben.“ Das war zwar etwas allgemeiner gemeint, aber es beschreibt auch gut, dass in dieser Wissenschaft häufig dieselben Symbole für verschiedene Dinge verwendet werden. Das ist im Endeffekt auch ganz gut so, weil man sonst vielleicht schon mehr mathematische Zeichen als chinesische Schriftzeichen hätte. Aber man muss sich daran gewöhnen und sich klarmachen, dass Dinge, die gleich *aussehen*, nicht unbedingt gleich *sind*.
- Ein wichtiges Detail, das Anfängern oft nicht klar ist: Ist diese Definition überhaupt eindeutig? Es wird z. B. festgelegt, dass $[4]_5 + [3]_5$ den Wert $[7]_5$ bekommen soll. Man kann der Definition jedoch auch entnehmen, dass $[9]_5 + [3]_5$ der Wert $[12]_5$ zugewiesen wird und $[4]_5$ und $[9]_5$ sind *dasselbe* Objekt. Damit hier wirklich eine Funktion definiert wird, muss $[7]_5$ auch dasselbe wie $[12]_5$ sein, denn anderenfalls würde keine Rechtseindeutigkeit vorliegen. Zum Glück ist $[7]_5$ dasselbe wie $[12]_5$. Dass das immer funktioniert, besagt Satz 13.2. Deswegen haben wir ihn bewiesen.

  Die grundsätzliche Eigenschaft, um die es hier geht, nennt man *Wohldefiniertheit*. Man muss sie immer überprüfen, wenn es für Objekte mehr als eine Darstellung gibt und man etwas auf der Basis dieser Darstellungen definiert.

  wohldefiniert
- Letzte Anmerkung: Dass die Zeile mit dem Symbol $\pm$ für zwei Definitionen ($+$ und $-$) steht, haben Sie natürlich bemerkt …

Aufgabe 13.4. Machen Sie sich mit diesen Operationen vertraut, indem Sie ein paar Beispiele berechnen: $[8]_{11} + [5]_{11}$, $[4]_{12} - [7]_{12}$, $[4]_{12} + [-7]_{12}$, $[10]_{15} \cdot [6]_{15}$ und so weiter. Finden Sie für das Ergebnis immer eine möglichst einfache Darstellung (in dem Sinne, dass die Zahl a in $[a]_n$ nichtnegativ und klein ist).

Aufgabe 13.5. Was ist $[3]_7 + [7]_3$?

⋆**Aufgabe 13.6**. Inwieweit spielt Wohldefiniertheit eine Rolle bei der „ganz normalen“ Bruchrechnung, die Sie aus der Schule kennen?

Es ergibt sich nun eine interessante neue Klasse von algebraischen Strukturen.

Lemma 13.3

Sei $n > 1$. Dann ist mit den gerade definierten Verknüpfungen $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer und unitärer Ring. Die neutralen Elemente für Addition und Multiplikation sind $[0]_n$ und $[1]_n$, das bzgl. der Addition zu $[a]_n$ inverse Element $-[a]_n$ ist $[-a]_n$. Insbesondere entspricht die Definition der Subtraktion auch der Konvention von Seite 119.

Aufgabe 13.7. Für den Beweis von Lemma 13.3 muss man eine ganze Reihe von Eigenschaften nachweisen. Das ist jedoch nicht schwer, weil der Ring $\mathbb{Z}/n\mathbb{Z}$ diese Eigenschaften aufgrund der Definition der Addition und Multiplikation von $\mathbb{Z}$ „erbt“. Vielleicht machen Sie das mal für ein oder zwei Punkte, um sich klarzumachen, dass Sie alles verstanden haben.

Aufgabe 13.8. Begründen Sie, dass die Gruppe aus Aufgabe 8.15 isomorph zur Gruppe $(\mathbb{Z}/3\mathbb{Z}, +)$ ist.

Aufgabe 13.9. Eine der beiden Gruppen aus Aufgabe 8.36 ist isomorph zu $(\mathbb{Z}/4\mathbb{Z}, +)$. Welche ist es?

Wir wollen nun mit Restklassen rechnen und werden uns zunächst etwas Schreibarbeit sparen.

Konvention

Wenn durch eine Formulierung wie „wir rechnen in $\mathbb{Z}/n\mathbb{Z}$“ oder „wir rechnen modulo n“ klar ist, dass mit einem festen n gerechnet wird, schreiben wir statt $[a]_n$ abkürzend die Zahl a mod n. $\mathbb{Z}/n\mathbb{Z}$ wird dadurch zu $\{0, \ldots, n-1\}$.

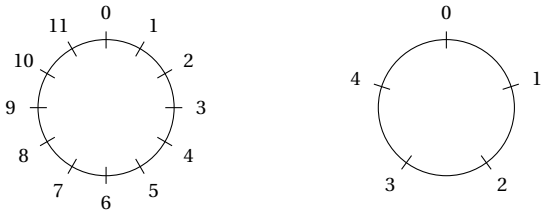
Beim Rechnen modulo 5 haben wir es dann also z. B. mit der Menge $\{0,1,2,3,4\}$ zu tun. Statt $[4]_5$ schreiben wir nun also einfach 4. Beachten Sie, dass damit *nicht* die ganze Zahl 4 gemeint ist.[21] Insbesondere gelten dann ganz neue und „seltsame“ Rechenregeln: $4+3$ ist nun 2, denn es gilt ja $[4]_5 + [3]_5 = [2]_5$. Und $4+3$ ist *nicht* 7, obwohl auch $[4]_5 + [3]_5 = [7]_5$ nicht falsch ist. Nach der obigen Konvention wird für $[7]_5$ jedoch 2 geschrieben.

Aufgabe 13.10. Berechnen Sie $10+9$, $3-8$ und $6\cdot 6$ in $\mathbb{Z}/11\mathbb{Z}$. Berechnen Sie danach $10+9$, $3-8$ und $6\cdot 6$ in $\mathbb{Z}/12\mathbb{Z}$.

Aufgabe 13.11. Denken Sie daran, dass mit $-a$ das inverse Element zu a bezüglich der Addition gemeint ist. Konkret ist also -3 die „Zahl“ 5, wenn wir modulo 8 rechnen. Was ist -3, wenn wir modulo 9 rechnen? Und was ist -7, wenn wir uns in $\mathbb{Z}/20\mathbb{Z}$ befinden?

[21] Damit wird die Konvention von Seite 125 natürlich temporär außer Kraft gesetzt.

Diese Form der Arithmetik ist gewöhnungsbedürftig, aber Sie praktizieren sie eigentlich schon seit Jahren. Es ist die übliche Art und Weise, in der wir alle auf dem Ziffernblatt einer Uhr rechnen. Wenn jemand Ihnen sagt, dass er um zehn Uhr morgens ankam und fünf Stunden blieb, dann wissen Sie ohne großes Nachdenken, dass er um drei Uhr nachmittags gegangen ist. Implizit haben Sie $10+5=15$ gerechnet und dann 12 abgezogen. Oder Sie haben es „visuell“ ausgerechnet, indem Sie den „Zeiger“ auf 10 stellten und dann fünf Schritte vorwärts bewegten. Sie rechnen dabei *modulo 12*. Wenn Sie stattdessen modulo 5 rechnen, dann ist das dasselbe Prinzip, nur mit einer anderen „Uhr“.



Aufgabe 13.12. Beim Programmieren haben Sie es auch manchmal (häufig eher ungewollt) mit dieser sogenannten *modularen Arithmetik* zu tun. Wenn ich auf meinem Rechner mit der folgenden C-Funktion die Fakultät von 13 berechnen will, dann erhalte ich als Ausgabe die Zahl 1 932 053 504.

```
int fact (int n) {
  int f = 1;
  while (n > 0) {
    f = f * n;
    n = n - 1;
  }
  return f;
}
```

Aber die korrekte Antwort wäre 6 227 020 800 gewesen. Woran liegt das?

Aufgabe 13.13. Nebenbei bemerkt kann man übrigens *ohne Rechnen* sofort sehen, dass die Antwort 1 932 053 504 aus Aufgabe 13.12 nicht richtig sein kann. Wieso?

Aufgabe 13.14. Erinnern Sie sich an die Teilbarkeitsregeln mit den Quersummen aus Aufgabe 11.12. Begründen Sie an einem konkreten Beispiel wie 7164, warum das klappt, indem Sie in $\mathbb{Z}_9$ bzw. $\mathbb{Z}_3$ rechnen. (Welche Reste erhalten Sie, wenn Sie 1, 10, 100, 1000 und so weiter durch 9 bzw. 3 teilen?)

Aufgabe 13.15. Um auf Teilbarkeit durch 11 zu testen, geht man wie bei der Teilbarkeit durch 9 vor, berechnet jedoch die *alternierende Quersumme*, indem man – bei der kleinsten Stelle beginnend – die Ziffern abwechselnd addiert und subtrahiert. Die alternierende Quersumme von 97364 ist also $4-6+3-7+9=3$. Und weil 3 nicht durch 11 teilbar ist, ist auch 97364 nicht durch 11 teilbar. Finden Sie analog zu Aufgabe 13.14 eine Begründung dafür, warum diese Regel funktioniert.

alternierende Quersumme

⋆**Aufgabe 13.16**. Für die Sieben gibt es eine weitere Teilbarkeitsregel, die allerdings etwas komplizierter als die bisherigen ist. Um festzustellen, ob eine Zahl durch 7

teilbar ist, verdoppeln Sie die letzte Ziffer und subtrahieren das Ergebnis vom Rest der Zahl (ohne die letzte Ziffer). Wiederholen Sie das so lange, bis Sie dem Ergebnis ansehen können, ob es durch 7 teilbar ist. Das ist genau dann der Fall, wenn auch die ursprüngliche Zahl durch 7 teilbar ist.

Um z. B. zu sehen, ob 35581 durch 7 teilbar ist, berechnen wir $3558 - 2 \cdot 1 = 3556$. Aus diesem Ergebnis machen wir $355 - 2 \cdot 6 = 343$. Daraus wird $34 - 2 \cdot 3 = 28$. Und dass 28 durch 7 teilbar ist, wissen wir. Darum ist auch 35581 durch 7 teilbar.

Können Sie begründen, warum das immer klappt?

Ein großer Unterschied zwischen der modularen Arithmetik und der „normalen“ in $\mathbb{Z}$ ist, dass $\mathbb{Z}/n\mathbb{Z}$ nur endlich viele Elemente hat. Man kann also theoretisch alles, was es dort überhaupt auszurechnen gibt, einmal aufschreiben und dann auf das Rechnen verzichten und stattdessen Verknüpfungstabellen konsultieren. Für $n = 6$ würde das so aussehen:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Die beiden farblich hervorgehobenen Zahlen stehen für $5 + 2 = 1$ und $3 \cdot 4 = 0$.

Aufgabe 13.17. Vergegenwärtigen Sie sich noch einmal, welche Ringeigenschaften man solchen Tabellen direkt ansehen kann.

Aufgabe 13.18. Für die Subtraktion muss man keine eigene Tabelle aufstellen, sondern kann die für die Addition „zweckentfremden“. Wie würde man das machen?

Aufgabe 13.19. Nach Satz 8.2 kann man in $\mathbb{Z}/6\mathbb{Z}$ jede Gleichung der Form $x + a = b$ nach x auflösen. Wie kann man das der linken Tabelle entnehmen?

Aufgabe 13.20. Stellen Sie zu Übung solche Tabellen wie auf Seite 144 für $n = 5$ oder $n = 7$ auf. Können Sie bei der Multiplikation einen signifikanten Unterschied zum Fall $n = 6$ erkennen?

Die Multiplikationstabelle zu $\mathbb{Z}/6\mathbb{Z}$ ist *kein* lateinisches Quadrat (siehe Aufgabe 13.19). Auch dann nicht, wenn man die Zeile und die Spalte für die Null ignoriert. $\mathbb{Z}/6\mathbb{Z}$ ist also *kein* Körper. Man kann der Tabelle noch weitere „Merkwürdigkeiten“ entnehmen, die wir von der üblichen Arithmetik mit rationalen oder reellen Zahlen nicht gewohnt sind:

- Man kann die Gleichung $x \cdot 2 = 3$ nicht lösen.
- Es gilt $5 \cdot 2 = 2 \cdot 2$, obwohl 5 und 2 zwei verschiedene Elemente von $\mathbb{Z}/6\mathbb{Z}$ sind.
- Es gilt $3 \cdot 2 = 0$, obwohl beide Faktoren von null verschieden sind.[22]

[22] Siehe Lemma 10.4.

Alle drei Beispiele lassen sich darauf zurückführen, dass 2 in diesem Ring kein Inverses bzgl. der Multiplikation hat. Wenn Sie Aufgabe 13.20 bearbeitet haben, werden Sie jedoch gesehen haben, dass $\mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/7\mathbb{Z}$ Körper sind. Das liegt an der folgenden wichtigen Aussage:

Satz 13.4

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Beweis. Um Verwechslungen zu vermeiden, verwenden wir im Beweis wieder die „umständliche“ Schreibweise $[a]_n$ für Elemente von $\mathbb{Z}/n\mathbb{Z}$, so dass klar ist, dass wir „normale“ ganze Zahlen meinen, wenn wir a schreiben.

Es geht um die Frage, wann die Gleichung $[a]_n \cdot [x]_n = [1]_n$ eine Lösung $[x]_n$ hat, wenn $[a]_n$ nicht $[0]_n$ ist. In den ganzen Zahlen ist das äquivalent zu der Gleichung $ax \bmod n = 1$, die für $0 < a < n$ gelöst werden soll. Und das kann man wiederum als $ax = kn + 1$ bzw. $ax - kn = 1$ für ein $k \in \mathbb{Z}$ ausdrücken.

Sind a und n teilerfremd, dann kann man nach dem Lemma von Bézout x und k mit dieser Eigenschaft finden. Gibt es umgekehrt solche Zahlen, dann teilt nach Lemma 11.4 jeder gemeinsame Teiler von a und n auch 1 und daher sind a und n nach Korollar 11.6 teilerfremd.

Für *alle* a, die infrage kommen, lässt sich die besagte Gleichung also dann und nur dann lösen, wenn in jedem Fall a und n teilerfremd sind. Die Zahlen n mit dieser Eigenschaft sind genau die Primzahlen. ■

Konvention

Ist p eine Primzahl, dann schreibt man auch $\mathbb{Z}_p$ statt $\mathbb{Z}/p\mathbb{Z}$ und spricht dann auch vom **Restklassenkörper modulo** p. Wir würden also beispielsweise $\mathbb{Z}_5$ oder $\mathbb{Z}_{19}$ schreiben, aber *nicht* $\mathbb{Z}_{16}$.

$\mathbb{Z}_p$

Kehrwert

Wie findet man nun konkret ein multiplikativ Inverses (auch *Kehrwert* genannt) zu einem vorgegebenen Element eines Restklassenkörpers? Nehmen wir als Beispiel $\mathbb{Z}_{97}$ und das Element $[67]_{97}$. Spielen wir den Beweis des Satzes durch, dann haben wir $n = 97$ und $a = 67$. Da wir das Lemma von Bézout anwenden wollen, müssen wir den euklidischen Algorithmus durchspielen:[23]

A	B
$97 = n$	$67 = a$
$30 = n - a$	$67 = a$
$30 = n - a$	$7 = a - 2(n-a) = 3a - 2n$
$2 = (n-a) - 4(3a-2n) = 9n - 13a$	$7 = 3a - 2n$
$2 = 9n - 13a$	$1 = (3a-2n) - 3(9n-13a) = 42a - 29n$

Wir haben den Prozess in diesem Fall etwas abgekürzt. (Siehe dazu Aufgabe 11.19.) Entscheidend ist die Zahl 42, die am Ende als Faktor vor a steht (während der

[23] Obwohl wir schon wissen, dass das Ergebnis $\mathrm{ggT}(67,97) = 1$ sein wird, weil 97 eine Primzahl ist. Uns interessiert die rechte Spalte.

zweite Faktor 29 nicht weiter interessant ist). Die Antwort wäre also $[42]_{97}$ und Sie können (z. B. mit dem Tool aus Aufgabe 11.6) nachrechnen, dass in $\mathbb{Z}_{97}$ tatsächlich $42 \cdot 67 = 1$ gilt. Gemäß der Konvention für Körper würden wir $1/67 = 42$ schreiben.

Aufgabe 13.21. Berechnen Sie so wie eben $1/106$ in $\mathbb{Z}_{173}$. Ermitteln Sie außerdem den Kehrwert von 5 in $\mathbb{Z}_{13}$.

Aufgabe 13.22. Stellen Sie sich selbst entsprechende Aufgaben. Sie können Ihre Ergebnisse überprüfen, indem Sie in Wolfram Alpha so etwas wie

```
inverse of 67 modulo 97
```

eingeben.

Aufgabe 13.23. Was ist $4/5$ in $\mathbb{Z}_{13}$?

Zum Abschluss dieses Abschnitts beweisen wir noch einen Satz, der in der Zahlentheorie häufig verwendet wird. Dabei geht es um Potenzen in Restklassenringen, die wir gemäß der Konvention von Seite 100 interpretieren. x^3 ist also einfach eine Abkürzung für $x \cdot x \cdot x$ und allgemein betrachten wir nur Ausdrücke der Form x^n, bei denen n eine natürliche Zahl ist.

Solche Potenzen lassen sich oft auch dann erstaunlich einfach berechnen, wenn der Exponent sehr groß ist. Wollen wir beispielsweise 10^{200} in $\mathbb{Z}_{11}$ berechnen, so können wir ausnutzen, dass $10 = -1$ gilt. Nach Punkt (iii) von Lemma 10.2 gilt $(-1)^2 = 1$ und damit haben wir

$$10^{200} = \left(10^2\right)^{100} = \left((-1)^2\right)^{100} = 1^{100} = 1.$$

Aufgabe 13.24. Berechnen Sie mit möglichst geringem Rechenaufwand 4^{100} in $\mathbb{Z}_{13}$. (Hinweis: Berechnen Sie zuerst 4^3.)

Aufgabe 13.25. Moment mal! Es gilt $[100]_{13} = [9]_{13}$ und daher hätte in Aufgabe 13.24 doch $4^{100} = 4^9 = \left(4^3\right)^3 = (-1)^3 = -1$ herauskommen müssen, oder? Wo ist hier der Denkfehler?

Der angekündigte Satz besagt, dass in jedem Restklassenkörper für einen bestimmten Exponenten die Potenz immer dieselbe ist.

Satz 13.5

Kleiner Satz von Fermat
Ist p prim, so gilt in $\mathbb{Z}_p$ die Gleichung $a^{p-1} = 1$ für alle $a \in \mathbb{Z}_p \setminus \{0\}$.

Beweis. Wir schreiben abkürzend $\mathbb{Z}_p^\times$ für $\mathbb{Z}_p \setminus \{0\}$ und rechnen die ganze Zeit modulo p. Sei $a \in \mathbb{Z}_p^\times$ fest gewählt. Weil $(\mathbb{Z}_p^\times, \cdot)$ eine Gruppe ist, bildet die zugehörige Verknüpfungstabelle ein lateinisches Quadrat. (Siehe Aufgabe 8.16.) Das bedeutet, dass die Mengen $\mathbb{Z}_p^\times$ und $\{ka : k \in \mathbb{Z}_p^\times\}$ identisch sind. Weil die Multiplikation

außerdem kommutativ ist, folgt, dass die Produkte über diese Mengen ebenfalls gleich sein müssen. Es gilt also

$$1 \cdot 2 \cdot 3 \cdots (p-1) = a \cdot 2a \cdot 3a \cdots (p-1)a.$$

Diese Gleichung können wir nun sukzessive auf beiden Seiten erst durch 1, dann durch 2 und so weiter dividieren. Nachdem wir schließlich durch $p-1$ dividiert haben, steht links nur noch 1 und rechts a^{p-1}. ■

Dieser Satz ist die Grundlage für diverse in der Praxis relevante Primzahltests. Seinen etwas seltsamen Namen trägt er übrigens, weil es auch einen „großen“ Satz von Fermat gibt. (Siehe dazu die Fußnote 3 auf Seite 7.)

Aufgabe 13.26. Wenn in einem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ für ein Element $a \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ die Gleichung $a^{n-1} = 1$ gilt, dann folgt daraus *nicht* notwendig, dass n prim ist. Finden Sie ein nichttriviales Beispiel dafür.

Aufgabe 13.27. Wir wissen bereits, dass man Kehrwerte in Restklassenkörpern mittels des erweiterten euklidischen Algorithmus berechnen kann. Der kleine Satz von Fermat liefert noch eine weitere (zumindest theoretische) Möglichkeit zur Berechnung von Kehrwerten. Sehen Sie sie?

Restklassenkörper werden in vielen Fehlererkennungs- und Fehlerkorrekturverfahren eingesetzt. So wird die Prüfziffer für Buchnummern im System ISBN-10 z. B. in $\mathbb{Z}_{11}$ berechnet[24] und das Verfahren, das verhindern soll, dass Sie beim Online-Banking aus Versehen eine falsche IBAN eingeben, rechnet in $\mathbb{Z}_{97}$.

Dass $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist, wenn n keine Primzahl ist, heißt übrigens nicht notwendig, dass es keinen Körper mit genau n Elementen gibt. Es gibt beispielsweise Körper mit 9, 32 oder 125 Elementen und solche sogenannten Galoiskörper werden unter anderem für die automatische Korrektur von Fehlern bei DVDs und anderen digitalen Medien eingesetzt. Mehr dazu im Video *Fehlerkorrektur mit Reed-Solomon-Codes*.

⋆ Modulare Arithmetik im Computer

Viele Berechnungen, die mit modularer Arithmetik zu tun haben, lassen sich in PYTHON einfach mit dem Operator % durchführen. Es gibt jedoch zusätzlich in SYMPY eine spezielle Funktion zur Berechnung der Kehrwerte:

```
from sympy import mod_inverse
mod_inverse(67,97)
```

Außerdem hat PYTHON eine Standardfunktion `pow` für Potenzen (nicht zu verwechseln mit der gleichnamigen Funktion aus der MATH-Bibliothek), die man mit einem dritten Argument dazu bringen kann, modular zu rechnen:

[24] Siehe dazu Kapitel 6 in *Konkrete Mathematik (nicht nur) für Informatiker*.

```
4**100, pow(4,100), pow(4,100,13)
```

Durch den Einsatz der sogenannten *binären Exponentiation* ist diese Funktion auch für große Exponenten sehr schnell.

14. Der chinesische Restsatz

In diesem Kapitel behandeln wir kurz einen Algorithmus, der in der Kryptographie an verschiedenen Stellen benutzt wird.[25] Das Verfahren basiert auf Ideen, die schon dem chinesischen Mathematiker Sun Zi im dritten Jahrhundert bekannt waren.

Definition

$a \equiv b \pmod m$ ist lediglich eine andere, in der Zahlentheorie häufig verwendete, Schreibweise für $[a]_m = [b]_m$ bzw. $a \bmod m = b \bmod m$.[26] Solche Aussagen werden auch als **Kongruenzen** bezeichnet.

Satz 14.1

Chinesischer Restsatz
Ein Kongruenzsystem der Form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

hat für beliebige vorgegebene natürliche Zahlen a_i eine Lösung, wenn m_1 bis m_n paarweise teilerfremde natürlichen Zahlen sind.

Kongruenzsystem

Bevor wir diese Aussage beweisen, klären wir, was mit einem *Kongruenzsystem* gemeint ist: Wie bei einem (linearen) Gleichungssystem (das Sie aus der Schule kennen) wird *eine* Zahl x gesucht, die alle Kongruenzen gleichzeitig simultan erfüllt. Und natürlich geht es wie im gesamten Kapitel um eine ganze Zahl. (Sonst würden die Kongruenzen auch gar keinen Sinn ergeben.)

Die Beweis*idee* können wir ebenfalls vorwegnehmen, indem wir uns das einfache System

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \end{aligned} \tag{14.1}$$

anschauen. Markieren Sie ein paar Lösungen der ersten Kongruenz auf der Zahlengeraden: 1, 4, 7, 10, −2, −5 und so weiter. Markieren Sie dann ein paar Löungen

[25] Unter anderem für *Geheimnisteilungsverfahren* sowie für die Steigerung der Effizienz des RSA-Kryptosystems, das in Kapitel 10 von *Konkrete Mathematik (nicht nur) für Informatiker* ausführlich beschrieben wird.

[26] Man muss allerdings beachten, dass mod in einem Ausdruck wie $a \bmod b$ ein Operator wie + ist, während die Zeichenfolge $(\bmod m)$ nur zusammen mit dem Teil $a \equiv b$ davor Sinn ergibt.

der zweiten Kongruenz in einer anderen Farbe. Sie werden schnell merken, dass es Zahlen gibt, die beide Kongruenzen lösen, zum Beispiel 7. Aber wie kommt man ohne Probieren auf so eine Lösung?

Der Trick ist, nach einer Lösung x_1 der ersten Kongruenz zu suchen, die durch 5 teilbar ist. Warum? Weil wir die zu einer Lösung der zweiten Kongruenz addieren könnten und das Ergebnis wieder eine Lösung der zweiten Kongruenz wäre. Ebenso können wir eine Lösung x_2 der zweiten Kongruenz, die durch 3 teilbar ist, „gefahrlos“ zu einer Lösung der ersten Kongruenz addieren. Insbesondere muss, wenn wir solche Zahlen finden, $x_1 + x_2$ eine Lösung des Systems (14.1) sein. Und das war's schon! (Im konkreten Fall könnten $x_1 = 10$ und $x_2 = 12$ diese Rollen spielen und die Lösung 22 liefern.)

Der komplette Beweis begründet nun, warum man Zahlen wie x_1 und x_2 immer finden kann und warum das auch mit mehr als zwei Kongruenzen klappt.

Beweis. Weil die Zahlen m_i paarweise teilerfremd sind, ist jede von ihnen auch teilerfremd zum Produkt der anderen. Wären beispielsweise m_1 und das Produkt $m_2 m_3 \cdots m_n$ nicht teilerfremd, so gäbe es nach dem Lemma von Bézout Zahlen k_1 und k_2 mit

$$k_1 \cdot m_1 + k_2 \cdot m_2 m_3 \cdots m_n > 1.$$

Diese Gleichung würde aber gleichzeitig nach Lemma 11.4 ein Beleg dafür sein, dass m_1 und m_2 nicht teilerfremd sind, weil man den rechten Summanden auch als $(k_2 m_3 \cdots m_n) \cdot m_2$ lesen kann. Und das wäre ein Widerspruch.

Wiederum nach dem Lemma von Bézout gibt es also Zahlen r_1 und s_1 mit

$$r_1 \cdot m_1 + s_1 \cdot m_2 m_3 \cdots m_n = 1.$$

Multipliziert man diese Gleichung mit a_1, dann erhält man die Zahl

$$x_1 = a_1 s_1 \cdot m_2 m_3 \cdots m_n,$$

die ein Vielfaches von $m_2 m_3 \cdots m_n$ ist und gleichzeitig die erste Kongruenz löst. Analog findet man für jedes i eine Zahl x_i, die die i-te Kongruenz löst und ein Vielfaches von $m_1 m_2 \cdots m_n / m_i$ ist.

Die Summe $x = x_1 + \cdots + x_n$ löst offenbar das Kongruenzsystem: x_1 löst die erste Kongruenz und die anderen Summanden sind Vielfache von m_1, also löst x die erste Kongruenz. Ebenso überzeugt man sich, dass x die anderen $n-1$ Kongruenzen löst. ■

Aufgabe 14.1. Lösen Sie das folgende Kongruenzsystem, indem Sie den Schritten des obigen Beweises folgen:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

Aufgabe 14.2. Stellen Sie sich selbst solche Aufgaben und lösen Sie sie – auch welche mit mehr als drei Kongruenzen. Man kann bei solchen Aufgaben offensichtlich sofort eine Probe machen und damit die eigenen Ergebnisse überprüfen. Wenn Sie Ihren Rechenkünsten nicht trauen, können Sie aber auch in Wolfram Alpha so etwas wie `ChineseRemainder[{1,2,4},{3,5,7}]` eingeben.

Aufgabe 14.3. Ihnen wird bereits aufgefallen sein, dass Kongruenzsysteme, die die Voraussetzungen des chinesischen Restsatzes erfüllen, mehr als eine Lösung haben. Wie viele sind es und welcher Zusammenhang besteht zwischen verschiedenen Lösungen?

Aufgabe 14.4. Auf die Voraussetzung, dass die m_i paarweise teilerfremd sind, kann man nicht verzichten. Begründen Sie das, indem Sie ein Kongruenzsystem angeben, für das man garantiert keine Lösung finden kann.

Aufgabe 14.5. Diese Aufgabe eignet sich sehr gut, um eine Reihe von Begriffen zu wiederholen bzw. zu vertiefen. Wir definieren die Abbildung f durch

$$f\colon \begin{cases} \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}_3 \times Z_5 \\ [x]_{15} \mapsto ([x]_3, [x]_5) \end{cases} .$$

Damit ist gemeint, dass f beispielsweise 7 auf $(1,2)$ abbildet und 11 auf $(2,1)$ (wobei wie üblich die eckigen Klammern weggelassen werden).

- Überlegen Sie sich zunächst, dass f wohldefiniert ist, dass es also z. B. keinen Unterschied macht, wenn man $[52]_{15}$ statt $[7]_{15}$ in die Definition von f einsetzt.
- Machen Sie sich dann klar, dass $f(a+b) = f(a) + f(b)$ und $f(ab) = f(a)f(b)$ für alle $a, b \in \mathbb{Z}/15\mathbb{Z}$ gilt.
- Begründen Sie mithilfe des chinesischen Restsatzes, dass f bijektiv ist.

Insgesamt haben Sie damit gezeigt, dass der Ring $\mathbb{Z}/15\mathbb{Z}$ isomorph zum direkten Produkt $\mathbb{Z}_3 \times \mathbb{Z}_5$ ist.

⋆ Der chinesische Restsatz im Computer

In der schon mehrfach erwähnten Bibliothek SymPy gibt es eine Funktion für den chinesischen Restsatz:

```
from sympy.ntheory.modular import crt
crt([3,5,7],[1,2,4])
```

Sie können sich sicher denken, welche Bedeutung der zweite Rückgabewert hat.

Resümee

Die Zahlentheorie ist eines der ältesten Gebiete der Mathematik. Einige der Resultate, die in diesem Kapitel vorgestellt wurden, waren bereits in der griechischen Antike bekannt und wurden in den schon erwähnten *Elementen* von Euklid bewiesen. Im Mittelalter verfiel die Zahlentheorie jedoch in einen „Dornröschenschlaf“ und wurde erst durch Mathematiker wie Pierre de Fermat im 17. Jahrhundert wiederbelebt. Die modulare Arithmetik stammt wie unzählige weitere Beiträge von

Carl Friedrich Gauß, der die Mathematik als „Königin der Wissenschaften“ und die Zahlentheorie als „Königin der Mathematik“ bezeichnete. Bis Mitte des 20. Jahrhunderts behielt die Zahlentheorie ihren Status als spannendes, aber nutzloses „Spielzeug“ der Mathematiker. Inzwischen ist sie allerdings ein unverzichtbares Hilfsmittel in der Kryptographie und der Kodierungstheorie geworden. Der amerikanische Geheimdienst NSA soll aus diesem Grund der weltweit größte Arbeitgeber für promovierte Mathematiker sein.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

VI

Die reellen und die komplexen Zahlen

Mit den reellen Zahlen rechnet man eigentlich schon regelmäßig während des größten Teils der Schulzeit, aber man macht sich über sie kaum wirklich Gedanken. Dabei handelt es sich bei ihnen nach wie vor um sehr rätselhafte Objekte. Auf den folgenden Seiten wollen wir sie ein wenig genauer unter die Lupe nehmen. Außerdem führen wir die komplexen Zahlen ein, die in der Schule selten eine Rolle spielen, die aber für die moderne Mathematik und auch für viele Anwendungen unverzichtbar sind.

15. Ordnungsrelationen und geordnete Körper

Was die reellen Zahlen von anderen Körpern, derer es ja viele gibt, unterscheidet, sind ihre topologischen bzw. ordnungstheoretischen Eigenschaften. Diese Adjektive werden Ihnen momentan voraussichtlich nicht viel sagen. Die kommenden Abschnitte sollen diese Begriffe mit Leben füllen.

Definition

Eine Relation R auf einer Menge A heißt **total auf** A, wenn für alle $a, b \in A$ (mindestens) eine der Aussagen aRb oder bRa wahr ist. R heißt **antisymmetrisch**, wenn aus aRb und bRa immer $a = b$ folgt. Eine Relation, die auf A reflexiv, antisymmetrisch und transitiv ist, wird **Halbordnung** auf A genannt. Ist eine Halbordnung zusätzlich total, so spricht man von einer **Totalordnung** bzw. einer **linearen Ordnung** auf A.

Der Prototyp für lineare Ordnungen ist die Relation $\leq$ auf den uns bekannten Zahlenmengen.

Aufgabe 15.1. Geben Sie bei den drei folgenden Relationen jeweils an, ob sie (auf der Menge $[4]$) reflexiv, transitiv, total und antisymmetrisch sind. Begründen Sie Ihre Antworten.

	1	2	3	4
1	×		×	
2	×	×		
3		×	×	
4	×	×	×	×

	1	2	3	4
1	×	×	×	×
2	×	×	×	×
3	×	×	×	×
4	×	×	×	×

	1	2	3	4
1	×			
2		×		
3			×	
4				×

Aufgabe 15.2. Sei A eine Menge. Wird durch $\subseteq$ eine Halbordnung auf $\mathscr{P}(A)$ definiert? Handelt es sich um eine lineare Ordnung?

Aufgabe 15.3. Wird durch $T = \{(m,n) \in \mathbb{N}^+ \times \mathbb{N}^+ : m \mid n\}$ eine Halbordnung auf $\mathbb{N}^+$ definiert? Handelt es sich um eine lineare Ordnung?

Aufgabe 15.4. Wird durch $T = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} : m \mid n\}$ eine Halbordnung auf $\mathbb{Z}$ definiert?

Aufgabe 15.5. Beachten Sie, dass Antisymmetrie *nicht* das Gegenteil von Symmetrie ist! Geben Sie als Begründung für diese Warnung eine Relation auf [3] an, die weder symmetrisch noch antisymmetrisch ist.

Definition

Eine Relation R auf einer Menge A wird **strenge Totalordnung** auf A genannt, wenn für alle $a, b \in A$ *genau eine* der drei Aussagen

$$aRb \quad \text{oder} \quad bRa \quad \text{oder} \quad a = b \tag{15.1}$$

gilt[1] und sie außerdem transitiv ist. R wird **irreflexiv auf** A genannt, wenn aRa für *kein* $a \in A$ gilt.

Der Prototyp für strenge Totalordnungen ist die Relation $<$ auf den uns bekannten Zahlenmengen.

Die folgende Aussage ist es eigentlich gar nicht wert, in ein eigenes Lemma „verpackt“ zu werden, aber aus didaktischen Gründen und zum Einüben der Begriffe habe ich es doch gemacht.

Lemma 15.1

Jede strenge Totalordnung auf einer Menge A ist irreflexiv auf A.

Beweis. Ist R eine Relation auf A, die *nicht* irreflexiv ist, dann gibt es ein $a \in A$ mit aRa. Aber natürlich gilt auch $a = a$ und damit gelten zwei der drei Aussagen aus (15.1). R ist somit keine Totalordnung auf A. ■

Aufgabe 15.6. Fällt Ihnen eine Relation ein, die für jede Menge A transitiv und irreflexiv auf $\mathscr{P}(A)$ ist? (Tipp: Schauen Sie sich noch einmal Aufgabe 15.2 an.)

Aufgabe 15.7. Analog zu Aufgabe 15.5 sei davor gewarnt, dass Irreflexivität *nicht* das Gegenteil von Reflexivität ist. Wie Sie sich schon gedacht haben, sollen Sie eine Relation (auf einer möglichst kleinen Menge) angeben, die weder reflexiv noch irreflexiv auf dieser Menge ist.

Trichotomie

[1] Diese Eigenschaft nennt man auch *Trichotomie*.

asymmetrisch

⋆**Aufgabe 15.8**. Eine Relation R auf einer Menge A heißt *asymmetrisch* auf A, wenn aus aRb immer $\neg bRa$ folgt. Beweisen Sie, dass so eine Relation sowohl irreflexiv als auch antisymmetrisch auf A ist. Ist jede Relation, die nicht symmetrisch ist, asymmetrisch?

Einige der bisher definierten Begriffe hängen eng zusammen. In gewissem Sinne sind sie sogar austauschbar:

Lemma 15.2

Sei A eine Menge.

(i) Ist R eine lineare Ordnung auf A, dann wird durch

$$S = \{(a,b) \in A^2 : aRb \wedge a \neq b\} = R \setminus \mathrm{id}_A$$

eine strenge Totalordnung auf A definiert.

(ii) Ist S eine strenge Totalordnung auf A, dann wird durch

$$R = \{(a,b) \in A^2 : aSb \vee a = b\} = S \cup \mathrm{id}_A$$

eine lineare Ordnung auf A definiert.

Beweis. Wir beginnen mit dem ersten Teil und setzen voraus, dass R eine lineare Ordnung auf A ist.

- **Transitivität von S:** Es gelte aSb und bSc. Wir müssen aSc zeigen, also aRc und $a \neq c$. Nach Definition von S gilt aRb und bRc und damit aRc, weil R transitiv ist. Würde $a = c$ gelten, dann hätten wir cRa wegen der Reflexivität von R und somit auch bRa wegen der Transitivität von R und schließlich $a = b$ wegen der Antisymmetrie von R. Das widerspricht jedoch aSb.
- **Trichotomie von S:** Seien a und b Elemente von A. Gilt $a = b$, dann ist aSb und bSA nach Definition von S nicht möglich. Es gelte also nun $a \neq b$. Wir müssen zeigen, dass aSb oder bSa, aber nicht beides gilt. Das ist aber klar, weil wegen der Totalität von R mindestens eine der Aussagen aRb oder bRa gilt und da wegen $a \neq b$ und der Antisymmetrie von R nicht beide gelten können.

Nun der zweite Teil, S sei eine strenge Totalordnung auf A.

- **Reflexivität von R:** Die ist in die Definition von R „eingebaut“.
- **Transitivität von R:** Es gelte aRb und bRc. Wir müssen aRc zeigen, also aSc oder $a = c$. Gilt $a = b$ oder $b = c$, dann gilt aRc trivialerweise. Wir können also $a \neq b$ und $b \neq c$ annehmen, was aSb und bSc nach Definition von R liefert. Mit der Transitivität von S folgt aSc.
- **Antisymmetrie von R:** Es gelte aRb und bRa. Würde $a \neq b$ gelten, dann würde aSb und bSa aus der Definition von R folgen, was der Trichotomie widerspricht.
- **Totalität von R:** Seien a und b Elemente von A. Gilt $a = b$, so folgt aRb wegen der bereits bewiesenen Reflexivität von R. Gilt $a \neq b$, so folgt aus der Trichotomie von S, dass eine der Aussagen aSb oder bSa gelten muss, und das bedeutet aRb oder bRa nach Definition von R. ■

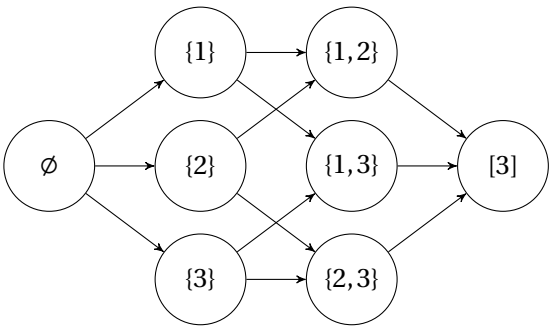
Konvention

Für abstrakte Halbordnungen verwendet man häufig suggestive Symbole wie $\preceq$ statt Buchstaben und analog Zeichen wie $\prec$ für irreflexive und transitive Relationen. Insbesondere soll mit $\prec$ die strenge Totalordnung aus dem ersten Teil von Lemma 15.2 gemeint sein, wenn $\preceq$ eine lineare Ordnung ist. Und umgekehrt soll $\preceq$ die lineare Ordnung aus dem zweiten Teil dieses Lemma sein, wenn $\prec$ eine strenge Totalordnung ist.
Zudem verwenden wir $a \succeq b$ und $a \succ b$ als Abkürzungen für $b \preceq a$ bzw. $b \prec a$.

In manchen Büchern nimmt man es mit den Begriffen nicht so genau und nennt beispielsweise auch $\prec$ eine lineare Ordnung, wenn $\preceq$ eine ist. Das ist aber nicht so schlimm, weil diese beiden Relationen nach Lemma 15.2 ja sozusagen immer im Tandem auftreten.

Hasse-Diagramm

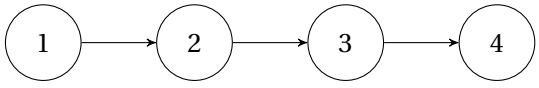
Ist A aus Aufgabe 15.2 zum Beispiel die Menge $[3]$, dann kann man die Relation folgendermaßen als sogenanntes *Hasse-Diagramm* visualisieren:



Die Pfeile sind dabei wie in den Grafiken in Abschnitt 5 (z. B. Seite 63) gemeint, wobei wie dort wegen der Reflexivität und der Transitivität diverse Pfeile weggelassen werden. Man sieht unter anderem, dass $\{1\}$ und $\{2\}$ nicht in Relation zueinander stehen.

Aufgabe 15.9. Sei $A = \{n \in \mathbb{N} : n \mid 12\}$ und $T = \{(m,n) \in A^2 : m \mid n\}$. Zeichnen Sie ein Hasse-Diagramm für diese Halbordnung.

Ich zeige das hauptsächlich deshalb, um klarzumachen, woher das Adjektiv *linear* für lineare Ordnungen kommt. Wegen der geforderten Totalität ergibt sich bei solchen Ordnungen als Hasse-Diagramm immer eine durchgehende *Linie*. Die Totalordnung $\mathrm{id}_{[4]} \cup \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$ auf $[4]$ sieht beispielsweise so aus:



Uns interessieren Ordnungsrelationen in Zukunft hauptsächlich im Zusammenhang mit algebraischen Operationen.

Definition

Ein Körper $(K,+,\cdot)$ wird **geordneter** oder **angeordneter Körper** genannt, wenn es eine lineare Ordnung $\preceq$ auf K gibt, die sich im folgenden Sinne mit den Rechenoperation „verträgt“:[2]

- **GK1:** $\forall a,b,c \in K\ (a \preceq b \Rightarrow a+c \preceq b+c)$
- **GK2:** $\forall a,b \in K\ (0 \preceq a \wedge 0 \preceq b \Rightarrow 0 \preceq ab)$

In so einem Körper nennt man Elemente a mit $0 \prec a$ **positiv** und Elemente b mit $b \prec 0$ **negativ**.

Auch hier gibt es natürlich einen naheliegenden Prototypen: den Körper $\mathbb{Q}$ der rationalen Zahlen mit der üblichen Relation $\leq$. So ziemlich alle Rechengesetze, die Sie aus der der Schule für $<$ und $\leq$ kennen, gelten in *jedem* geordneten Körper und das folgt schon aus den beiden simplen Eigenschaften **GK1** und **GK2** in der Definition. Im folgenden Lemma habe ich einige wichtige aufgezählt.

Lemma 15.3

In jedem geordneten Körper K gelten die folgenden Aussagen für alle Elemente a,b,c von K:

(i) $a \prec b \Rightarrow a+c \prec b+c$
(ii) $0 \prec a \wedge 0 \prec b \Rightarrow 0 \prec ab$
(iii) $0 \prec a \Leftrightarrow -a \prec 0$
(iv) $0 \preceq a \wedge 0 \preceq b \Rightarrow 0 \preceq a+b$
(v) $0 \preceq a^2$
(vi) $0 \prec 1$
(vii) $a \prec b \Leftrightarrow 0 \prec b-a$
(viii) $a \prec b \wedge 0 \prec c \Rightarrow ac \prec bc$
(ix) $a \prec b \wedge c \prec 0 \Rightarrow bc \prec ac$
(x) $1 \prec a \wedge 0 \prec b \Rightarrow b \prec ab$
(xi) $a \prec 1 \wedge 0 \prec b \Rightarrow ab \prec b$
(xii) $0 \prec ab \Leftrightarrow (0 \prec a \wedge 0 \prec b) \vee (a \prec 0 \wedge b \prec 0)$
(xiii) $0 \prec a \Rightarrow 0 \prec 1/a$
(xiv) $1 \prec a \Rightarrow 0 \prec 1/a \prec 1$
(xv) $0 \prec a \prec b \Rightarrow 0 \prec 1/b \prec 1/a$

Beweis. Ich picke mir einige Punkte heraus und überlasse Ihnen den Rest als Übung – siehe Aufgabe 15.10.

(iii) Das folgt aus (i), indem man auf beiden Seiten $-a$ bzw. a addiert.

[2] Wenn man es ganz genau nimmt, dann muss man das Tupel $(K,+,\cdot,\preceq)$ als den angeordneten Körper bezeichnen. Auf solche Feinheiten verzichten wir jedoch. Es wird jeweils aus dem Kontext hervorgehen, welche Relation und welche Verknüpfungen gemeint sind.

(iv) O. B. d. A.[3] (wegen der Totalität) gelte $a \preceq b$. Aus $0 \preceq a$ folgt $b = 0 + b \preceq a + b$ mit **GK1** und wegen der Transitivität von $\preceq$ haben wir $0 \preceq a \preceq b \preceq a + b$.

(v) Für $0 \preceq a$ ist das eine direkte Folgerung aus **GK2** (mit $b = a$). Gilt hingegen $a \prec 0$, so wissen wir nach (iii), dass daraus $0 \prec -a$ folgt. Die Aussage folgt dann, weil $a^2 = (-a)^2$ nach Lemma 10.2 in jedem Ring gilt. ■

⋆**Aufgabe 15.10**. Ergänzen Sie die fehlenden Beweise in Lemma 15.3. Beweisen Sie dabei die Aussagen in der angegebenen Reihenfolge, die absichtlich so gewählt wurde. Was bereits bewiesen ist, dürfen Sie für die folgenden Beweise natürlich verwenden.

Satz 15.4

Jeder angeordnete Körper enthält eine isomorphe[4] Kopie von $\mathbb{Q}$. Insbesondere hat jeder angeordnete Körper unendlich viele Elemente.

Beweis. Wir wissen bereits, dass $0 \prec 1$ gelten muss. Durch sukzessive Addition von 1 folgt daraus $1 \prec 1 + 1$, $1 + 1 \prec 1 + 1 + 1$ und so weiter. Die Körperelemente 0, 1, $1 + 1$, $1 + 1 + 1$ et cetera sind also also verschieden und aus den Rechengesetzen für Körper folgt, dass sie sich so wie die natürlichen Zahlen verhalten. Es ist daher legitim, sie als „Kopien“ der natürlichen Zahlen 0, 1, 2, 3 und so weiter zu betrachten. Nimmt man die additiv Inversen hinzu, so findet man auf diese Art auch alle ganzen Zahlen wieder. Und bildet man dann Kehrwerte und multipliziert, so kommt man zu „Kopien“ der Brüche.

Das war nur eine Beweisskizze, aber das soll reichen. Entscheidend ist dies: Ist K ein angeordneter Körper, dann ist $\mathbb{Q}$ natürlich im Allgemeinen keine Teilmenge von K, aber K hat einen Teilkörper, der sich bezüglich der Rechenoperationen und Relationen von K genauso *verhält* wie $\mathbb{Q}$. ■

Wir haben damit sofort einen großen „Vorrat“ an Körpern, die garantiert keine geordneten Körper sein können:

Korollar 15.5

Endliche Körper können *nicht* angeordnet werden. Das gilt insbesondere für Körper der Form $\mathbb{Z}_p$ wie in Abschnitt 13.

Da solche Körper endlich sind, gibt es nichts mehr zu beweisen. Aber es sei noch einmal darauf hingewiesen, woran es scheitert: Im Körper $\mathbb{Z}_2$ gilt $1 + 1 = 0$, in $\mathbb{Z}_3$ gilt $1 + 1 + 1 = 0$ und so weiter. In einem angeordneten Körper darf so etwas nicht

[3] Diese Abkürzung steht für *ohne Beschränkung der Allgemeinheit* und damit ist gemeint, dass man – in der Regel zur Vermeidung von Schreibarbeit – eine Einschränkung vornimmt, die aber faktisch keine ist. Im konkreten Fall gilt $a \preceq b$ *oder* $b \preceq a$. Im zweiten Fall würde man aber bis auf Vertauschung von a und b denselben Beweis erhalten und spart sich daher die Arbeit, das noch einmal aufzuschreiben.

[4] Machen Sie sich nicht zu viele Gedanken über den Begriff der Isomorphie. Wenn Ihnen die Aussage des Satzes durch den Beweis intuitiv klar wird, dann reicht das. Siehe dazu auch die Anmerkung auf Seite 122 direkt vor dem Resümee.

Zur Formulierung „enthält“ siehe die Fußnote 31 auf Seite 28. Hier ist natürlich gemeint, dass die Kopie eine *Teilmenge* des Körpers ist.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

passieren. Das heißt aber auch, dass Sie nicht der Versuchung erliegen dürfen, so etwas wie „1 ist kleiner als 2“ zu denken, wenn Sie in einem Körper der Form $\mathbb{Z}_p$ arbeiten!

Aufgabe 15.11. Auf dem mathematischen Niveau, auf dem wir uns hier bewegen, ist es schwer, Beispiele für angeordnete Körper außer $\mathbb{Q}$ und $\mathbb{R}$ zu finden. Aber einen sollen Sie zumindest einmal gesehen haben. Wenn man die Menge

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\},$$ $\mathbb{Q}(\sqrt{2})$

die eine echte Teilmenge von $\mathbb{R}$ und eine echte Obermenge von $\mathbb{Q}$ ist, mit den üblichen Bedeutungen von $+$, $\cdot$ und $\leq$ betrachtet, dann erhält man einen angeordneten Körper. Wenn Sie es sich zutrauen, dann versuchen Sie, das zu beweisen (wobei Sie natürlich voraussetzen dürfen, dass Sie „wissen“, dass $\mathbb{R}$ ein angeordneter Körper ist). Wenn Sie es sich nicht zutrauen, dann lesen Sie sich vielleicht wenigstens die Lösung durch.

Ein wichtiges Zwischenziel dieses Kapitels wird eine eindeutige Charakterisierung der reellen Zahlen sein. Wie wir gesehen haben, bilden sie einen angeordneten Körper, aber nicht den einzigen. Wir brauche noch eine weitere Eigenschaft und dafür noch ein paar Begriffe.

Definition

Sei $\preceq$ eine Halbordnung auf einer Menge A und $B \subseteq A$. Ein Element m von B heißt **Maximum** bzw. **größtes Element** von B, wenn $b \preceq m$ für alle $b \in B$ gilt. Analog werden **Minimum** und **kleinstes Element** definiert.

Beachten Sie, dass diese Definition natürlich nicht der von Seite 125 widerspricht. Das wäre ja sonst auch ziemlich dumm. Und wir übernehmen auch die Schreibweise $\min B$ bzw. $\max B$ aus Abschnitt 11. Mit der üblichen Ordnung $\leq$ haben wir also beispielsweise $1 = \min \mathbb{N}^+$ oder $42 = \max\{-17, 23, 42\}$. $\min B$ $\max B$

Aufgabe 15.12. Wir betrachten $\mathbb{Q}$ mit der üblichen Halbordnung $\leq$. Geben Sie eine Menge von rationalen Zahlen an, die kein Minimum hat.

Aufgabe 15.13. Sei $A = [4]$ und $\subseteq$ die Halbordnung auf $B = \mathscr{P}(A)$, die wir aus Aufgabe 15.2 kennen. Geben Sie eine Teilmenge von B an, die kein Maximum hat.

Aufgabe 15.14. Begründen Sie, dass eine Menge nicht zwei verschiedene Maxima (bzw. Minima) haben kann. (Darum spricht man auch von *dem* Maximum und nicht von *einem*.)

Maxima und Minima müssen Elemente der jeweiligen Menge sein. Für die nun definierten *Schranken* gilt das nicht.

Definition

Sei $\preceq$ eine Halbordnung auf einer Menge A und $M \subseteq A$. Ein Element $a \in A$ heißt **obere Schranke** von M, wenn $m \preceq a$ für alle $m \in M$ gilt. Gibt es eine obere Schranke, dann nennt man M **nach oben beschränkt**. Analog werden die Begriffe **untere Schranke** und **nach unten beschränkt** definiert. Eine Menge, die nach oben und unten beschränkt ist, wird **beschränkt** genannt.

Mit der üblichen Relation $\leq$ ist beispielsweise 12 eine obere Schranke von $\{1,2,3\}$ aber 3 ist auch eine. 0 ist eine untere Schranke der Menge $\{1/n : n \in \mathbb{N}^+\}$. Beide Mengen sind beschränkt. $\mathbb{N}$ ist nach unten, aber nicht nach oben beschränkt und daher auch nicht beschränkt. Hat eine Menge ein Maximum bzw. ein Minimum, so ist dieses natürlich eine obere bzw. untere Schranke der Menge.

Aufgabe 15.15. Wir betrachten die Halbordnung $\subseteq$ auf der Menge $A = \mathscr{P}(\mathbb{N}) \setminus \{\mathbb{N}\}$. Seien B_1, B_2 und B_3 drei endliche Teilmengen von $\mathbb{N}$. Geben Sie eine obere Schranke von $\{B_1, B_2, B_3\}$ an. Geben Sie eine nach oben unbeschränkte Teilmenge von A an.

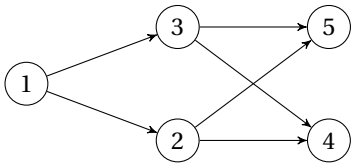
Definition

Sei $\preceq$ eine Halbordnung auf einer Menge A und $M \subseteq A$. Ist M nach oben beschränkt und hat die Menge der oberen Schranken ein Minimum, dann bezeichnet man dieses als **Supremum** von M und schreibt dafür $\sup M$. Analog wird das Maximum der unteren Schranken (wenn es existiert) einer nach unten beschränkten M das **Infimum** von M genannt und $\inf M$ geschrieben.

Mit anderen Worten: Das Supremum ist die *kleinste* obere Schranke, das Infimum ist die *größte* untere Schranke.

Aufgabe 15.16. Geben Sie für die Mengen $\{x \in \mathbb{Q} : x < 2\}$ und $\{x \in \mathbb{Q} : x \leq 2\}$ jeweils das Supremum an.

Aufgabe 15.17. Gegeben sei die folgende, durch ein Hasse-Diagramm dargestellte Relation $\preceq$ auf $[5]$:



Geben Sie eine Teilmenge von $[5]$ an, die nach oben beschränkt ist, aber kein Supremum hat.

Lemma 15.6

Ist $\preceq$ eine Halbordnung auf A und m das Maximum von A, dann ist m das Supremum von A. Ist umgekehrt das Supremum von A ein Element von A, dann handelt es sich um das Maximum.[5]

Beweis. Dass m eine obere Schranke von A ist, hatten wir uns bereits überlegt. Ist m' ebenfalls eine obere Schranke von A, dann gilt insbesondere $m \preceq m'$, weil m ein Element von A ist. Und das war schon der erste Teil. Ist umgekehrt s das Supremum von A (oder sogar irgendeine obere Schranke) und gleichzeitig ein Element von A, dann erfüllt s offenbar die Eigenschaften, die das Maximum erfüllen muss. ■

[5] Natürlich gilt das alles auch, wenn man stattdessen Infima und Minima betrachtet.

⋆ Ordnungsrelationen im Computer

Aufbauend auf dem Code von den Seiten 45 und 70 kann man auch Antisymmetrie, Totalität und Irreflexivität implementieren.

```
antisymm = lambda R,A: R&inv(R) <= identity(A)
total = lambda R,A: product(A,A) <= R|inv(R)
irr = lambda R,A: identity(A)&R == set()
```

PYTHON bietet außerdem die Funktionen `max` und `min` zum effizienten Ermitteln von Maxima und Minima von z. B. Listen und Mengen und ganz allgemein Iteratoren.

```
S = set([-17,23,42])
min(S)
max(-x**2+5*x-3 for x in range(-10,11))
```

Da man in PYTHON Operatoren wie `<=` überladen kann, kann man sich mit eigenen Klassen natürlich auch eigene Interpretationen dieser Relationen bauen.

16. Die reellen Zahlen

Die „Lebensberechtigung“ für die reellen Zahlen ist, dass den rationalen Zahlen etwas „fehlt“. Betrachtet man nur den angeordneten Körper der rationalen Zahlen, dann ist beispielsweise die Menge $C = \{q \in \mathbb{Q} : q^2 < 2\}$ nach oben beschränkt, hat aber kein Supremum. (Siehe dazu Aufgabe 16.2.) Wenn man sich diese linear geordnete Menge als Punkte auf einer Geraden vorstellt, dann gibt es *Lücken*.[6] Wie müsste ein Körper aussehen, der solche Lücken nicht aufweist?

Definition

Ein angeordneter Körper K heißt **vollständig angeordnet**, wenn jede nichtleere, nach oben beschränkte Teilmenge von K ein Supremum hat.

Die Menge der reellen Zahlen hat diese Eigenschaft:

Satz 16.1

Der Körper $\mathbb{R}$ der reellen Zahlen ist vollständig angeordnet. Bis auf Isomorphie ist es der einzige dieser Art.

Uns fehlen die mathematischen Hilfsmittel, um diesen Satz zu beweisen,[7] und es würde davon abgesehen auch zu viel Zeit kosten. (Wenn Sie einen Eindruck davon

[6] Allerdings ist es schwierig, das mit unseren Alltagsvorstellungen in Übereinstimmung zu bringen, denn zwischen je zwei rationalen Zahlen a und b liegt immer noch eine weitere rationale Zahl, nämlich ihr Mittelwert $(a+b)/2$, und daher liegen zwischen ihnen unendlich viele Zahlen. (Zwischen dem Mittelwert und a bzw. b liegt wieder eine Zahl und immer so weiter.) Wo sollen da denn „Lücken“ sein? Aber es gibt sie offenbar …

[7] Auch in Uni-Vorlesungen für Studierende der Mathematik wird der Satz in den Einführungsvorlesungen oft nicht bewiesen, sondern als Axiom an den Anfang gestellt. Auf die Hintergründe geht man dann ggf. später in Spezialvorlesungen ein.

bekommen wollen, wie man vorgeht, dann schauen Sie sich das Video "Dedekindsche Schnitte" an.) Aber es ist wichtig, sich über diese grundlegende Eigenschaft der reellen Zahlen im Klaren zu sein. Die gesamte Analysis basiert darauf und es ist keine große Übertreibung, wenn man sagt, dass die Mathematikerzunft zwei Jahrhunderte lang um saubere Begriffe gerungen hat, bis man an diesem Punkt angelangt war.

Aufgabe 16.1. Begründen Sie, dass in $\mathbb{R}$ jede nichtleere, nach unten beschränkte Menge ein Infimum hat.

⋆**Aufgabe 16.2**. Begründen Sie, dass $C = \{q \in \mathbb{Q} : q^2 < 2\}$ in $\mathbb{Q}$ kein Supremum hat, ohne die Vollständigkeit der reellen Zahlen zu verwenden. Es gibt also nur Brüche und insbesondere gibt es die „Zahl“ $\sqrt{2}$ nicht. (Hinweis: Wissen Sie, wie "babylonisches Wurzelziehen" funktioniert?)

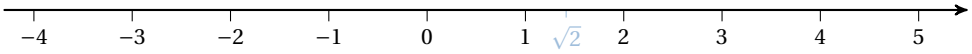
Nach Satz 15.4 muss $\mathbb{R}$ eine Kopie von $\mathbb{Q}$ enthalten. Wir ignorieren die technischen Feinheiten und betrachten $\mathbb{Q}$ als Teilmenge von $\mathbb{R}$, wie wir es schon die ganze Zeit gemacht haben. Jede rationale Zahl ist also eine reelle Zahl. Damit haben wir jetzt „offiziell“ den Stand erreicht, mit dem wir inoffiziell schon seit der Tabelle auf Seite 27 arbeiten und den ich hier noch einmal wiederhole:[8]

$$\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \tag{16.1}$$

irrational

Die reellen Zahlen, die *nicht* rational sind, also die Elemente von $\mathbb{R} \setminus \mathbb{Q}$, nennt man *irrational*. Die Menge C vom Anfang des Abschnitts hat im Reellen ein Supremum. Es handelt sich um die Zahl, die man gewöhnlich als $\sqrt{2}$ bezeichnet.[9] Dass Wurzeln wie diese irrational sind, weiß man bereits seit weit über zweitausend Jahren. Beweise für die Irrationalität anderer Zahlen ergaben sich erst in der Neuzeit.

Die mathematisch idealisierte Vorstellung von $\mathbb{R}$ ist also, dass diese Menge die Menge der Punkte der (lückenlosen) Zahlengeraden *ist*.



Lemma 16.2

Archimedisches Axiom
Zu beliebigen positiven reellen Zahlen x und y gibt es immer eine natürliche Zahl n mit $nx > y$.

Beweis. Wir führen einen Widerspruchsbeweis und nehmen an, dass es Zahlen $x, y > 0$ mit der Eigenschaft gibt, dass $nx \leq y$ für alle $n \in \mathbb{N}$ gilt.[10] Dann ist y eine obere Schranke für die Menge $X = \{nx : n \in \mathbb{N}\}$. Wegen der Vollständigkeit von $\mathbb{R}$ muss X ein Supremum s haben. Der „Witz“ ist nun, dass auch $s - x$ eine obere

[8] Erinnern Sie sich an Aufgaben wie 2.4 und 2.5.

[9] Dass das Quadrat dieser Zahl tatsächlich 2 ist, werden wir allerdings erst später richtig beweisen können.

[10] Wir benutzen ab jetzt die ordnungstheoretischen Eigenschaften aus dem letzten Abschnitt, ohne darauf jeweils im Einzelnen einzugehen. Eben wurde z. B. verwendet, dass wegen der Trichotomie $nx < y$ oder $nx = y$ gelten muss, wenn $nx > y$ *nicht* gilt.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Schranke von X ist: Ist nx irgendein Element von X, dann gilt $(n+1)x \leq s$ und damit $nx \leq s - x$. Aber $s - x$ ist kleiner als s und das ist ein Widerspruch dazu, dass s die *kleinste* obere Schranke von X ist. ■

Dass man hier von einem Axiom spricht, obwohl man die Aussage beweisen kann, hat historische Gründe. Die Aussage des Satzes verdeutlicht man sich am besten, wenn man sich x als eine sehr kurze Strecke (vielleicht wenige Millimeter) vorstellt und y als sehr lang (vielleicht Lichtjahre). Trotzdem kann man die Länge y übertreffen, wenn man nur genügend viele Stücke (nämlich n) der Länge x aneinanderlegt.

Nebenbei folgt aus diesem Lemma auch, dass $\mathbb{N}$ nach oben unbeschränkt ist: Mit $x = 1$ zeigt man, dass keine reelle Zahl y eine obere Schranke von $\mathbb{N}$ sein kann.

Häufig werden wir das archimedische Axiom in der folgenden Form verwenden:

Korollar 16.3

Zu jeder positiven reellen Zahl x gibt es ein $n \in \mathbb{N}^+$ mit $1/n < x$.

Beweis. Nach Lemma 16.2 (mit $x = 1$ und $y = 1/x$) gibt es ein $n \in \mathbb{N}$ mit $n \cdot 1 > 1/x$. Mit den Rechenregeln für angeordnete Körper ergibt sich $1/n < x$. ■

Lemma 16.4

Jede nichtleere, nach oben beschränkte Menge von ganzen Zahlen hat ein Maximum.

Beweis. Sei M so eine Menge. Weil $\mathbb{R}$ vollständig ist, hat sie ein Supremum s. $s - 1$ ist dann keine obere Schranke von M, weil $s - 1$ kleiner als s ist. Also gibt es ein $m \in M$ mit $s - 1 < m$. Addiert man auf beiden Seiten 1, so folgt $s < m + 1$ und damit kann (die ganze Zahl) $m + 1$ kein Element von M sein. Das gilt „erst recht“ für alle noch größeren ganzen Zahlen. Also ist m die größte Zahl in M und es gilt $s = m$. ■

Damit können wir nun eine Operation begründen, die wir schon verwendet haben, nämlich das Runden auf ganze Zahlen.

Korollar 16.5

Zu jeder reellen Zahl x gibt es eine größte ganze Zahl z_1 mit $z_1 \leq x$ und eine kleinste ganze Zahl z_2 mit $x \leq z_2$.

Beweis. Nach dem archimedischen Axiom gibt es eine natürliche Zahl n, für die $n > -x$ bzw. $-n < x$ gilt.[11] Die Menge $\{z \in \mathbb{Z} : z \leq x\}$ ist also nicht leer und nach oben beschränkt. Nach Lemma 16.4 hat sie ein größtes Element. Die andere Hälfte beweist man analog. ■

[11] Das archimedische Axiom braucht man nur, wenn x negativ ist. Ansonsten kann man einfach $n = 1$ wählen.

Definition

Für die eindeutig bestimmten Zahlen aus Korollar 16.5 schreibt man $\lfloor x \rfloor$ bzw. $\lceil x \rceil$. Das sind die sogenannten **unteren** und **oberen Gaußklammern**.

Beispielsweise gilt $\lfloor 7/2 \rfloor = 3 = \lceil 27/10 \rceil$ und $\lfloor -7/2 \rfloor = -4 = \lceil -47/10 \rceil$. Man beachte das Verhalten bei negativen Zahlen!

Aufgabe 16.3. Begründen Sie mit Gegenbeispielen, dass die beiden folgenden „Rechenregeln“ falsch sind: $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ und $\lfloor xy \rfloor = \lfloor x \rfloor \cdot \lfloor y \rfloor$. (Und wie ist das mit den oberen Gaußklammern?)

Wir definieren noch eine wichtige (und aus der Schule bekannte) Funktion durch Fallunterscheidung und beweisen einige ihrer Eigenschaften.

Definition

Der **Absolutbetrag** bzw. **Betrag** ist die Funktion von $\mathbb{R}$ nach $\mathbb{R}$, die jede reelle Zahl x auf den folgenden Wert abbildet:

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Für später ist der folgende Zusammenhang besonders wichtig:

Lemma 16.6

Für alle $x, \varepsilon \in \mathbb{R}$ mit $\varepsilon > 0$ gilt $|x| < \varepsilon$ genau dann, wenn $-\varepsilon < x < \varepsilon$ gilt.

⋆**Aufgabe 16.4**. Wahrscheinlich (bzw. hoffentlich) ist Ihnen klar, dass Lemma 16.6 gilt. Aber versuchen Sie ruhig einmal, einen präzisen Beweis dafür aufzuschreiben.

⋆**Aufgabe 16.5**. Beweisen Sie, dass $-|x| \leq x \leq |x|$ für alle $x \in \mathbb{R}$ gilt.

Lemma 16.7

Für alle $x, y \in \mathbb{R}$ gilt:

(i) $|x| \geq 0$

(ii) $|x| = 0 \Leftrightarrow x = 0$

(iii) $|xy| = |x| \cdot |y|$ (*Multiplikativität*)

(iv) $|x+y| \leq |x| + |y|$ (*Dreiecksungleichung*)

Beweis. Die ersten beiden Punkte sollten wohl offensichtlich sein. Der dritte Punkt folgt mit einer Fallunterscheidung aus den Rechenregeln für angeordnete Körper. Nach Aufgabe 16.5 gilt schließlich $-|a| \leq a \leq |a|$ und $-|b| \leq b \leq |b|$. Addiert man diese beiden Ungleichungen, dann erhält man $-(|a|+|b|) \leq a+b \leq |a|+|b|$. Daraus folgt die Dreiecksungleichung nach Lemma 16.6. ■

Aufgabe 16.6. Begründen Sie mit einem Gegenbeispiel, dass man in der Dreiecksungleichung $\leq$ nicht durch $=$ ersetzen kann.

Die folgenden Aussagen hätte man im Prinzip auch gleich zum letzten Lemma hinzufügen können. Aus Gründen, die später noch klar werden, führen wir sie jedoch explizit als Folgerungen aus diesem Lemma auf.

Korollar 16.8

Für alle $x, y \in \mathbb{R}$ gilt:

(i) $|x/y| = |x|/|y|$ für $y \neq 0$

(ii) $|x - y| \leq |x| + |y|$

(iii) $||x| - |y|| \leq |x \pm y|$

Beweis. Aus der Multiplikativität folgt $|y| \cdot |x/y| = |x|$ und durch Multiplikation mit $|x/y|$ folgt der erste Punkt. Der zweite Punkt folgt aus der Dreiecksungleichung, wenn man y durch $-y$ ersetzt, weil natürlich $|-y| = |y|$ gilt.

Für den dritten Punkt liefert die Dreiecksungleichung zunächst

$$|x| = |(x - y) + y| \leq |x - y| + |y|$$

und damit $|x| - |y| \leq |x - y|$. Vertauscht man die Rollen von x und y, so erhält man $-(|x| - |y|) = |y| - |x| \leq |y - x| = |x - y|$. Beides zusammen liefert $||x| - |y|| \leq |x - y|$. Ersetzt man y durch $-y$, so erhält man analog $||x| - |y|| \leq |x + y|$. ■

Manchmal ist auch die folgende Funktion ganz hilfreich.

Definition

Die **Vorzeichen-** oder **Signumfunktion** wird für alle $x \in \mathbb{R}$ definiert durch[12]

$$\operatorname{sgn}(x) = \begin{cases} 1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}.$$

Aus der Definition der beiden Funktionen durch Fallunterscheidung folgt sofort ein Zusammenhang zwischen Betrags- und Signumfunktion:

Lemma 16.9

Für alle $x \in \mathbb{R}$ gilt $x = \operatorname{sgn}(x) \cdot |x|$.

Obwohl wir noch sehen werden, dass die rationalen Zahlen eine kleine Minderheit innerhalb der Menge der reellen Zahlen bilden, sind sie in gewissem Sinne deren Rückgrat, weil sie gleichsam „überall“ sind:

Satz 16.10

$\mathbb{Q}$ liegt *dicht* in $\mathbb{R}$. Das bedeutet: Zu beliebigen reellen Zahlen r_1 und r_2 mit $r_1 < r_2$ gibt es eine[13] rationale Zahl q mit $r_1 < q < r_2$.

[12] Wir hatten dasselbe Zeichen auch für das Signum einer Permutation verwendet. Es besteht allerdings keine Gefahr von Verwechslungen, weil Permutationen und reelle Zahlen offensichtlich unterschiedliche Dinge sind.

Beweis. Zu $\varepsilon = r_2 - r_1$ gibt es nach Lemma 16.3 ein $n \in \mathbb{N}^+$ mit $1/n < \varepsilon$. Nach Lemma 16.4 gibt es ein größtes $a \in \mathbb{Z}$ mit $a \le nr_1$ und ein kleinstes $b \in \mathbb{Z}$ mit $nr_2 \le b$. Es folgt

$$\frac{a}{n} \le r_1 < r_2 \le \frac{b}{n} \quad \text{und damit} \quad \frac{b-a}{n} = \frac{b}{n} - \frac{a}{n} \ge r_2 - r_1 > \frac{1}{n}.$$

Also gibt es mindestens eine ganze Zahl c zwischen a und b. Die rationale Zahl c/n liegt nach Konstruktion zwischen r_1 und r_2. ■

Den Prozess kann man natürlich beliebig fortsetzen. Zwischen r_1 und q bzw. zwischen q und r_2 muss nach dem Satz wieder eine rationale Zahl liegen und so weiter …

Aufgabe 16.7. Begründen Sie: Ist q rational und r irrational, dann ist $q + r$ irrational. Außerdem ist qr irrational, wenn $q \neq 0$ gilt.

Aufgabe 16.8. Geben Sie zwei irrationale Zahlen an, deren Summe *und* Produkt rational sind.

Es gilt allerdings auch die „Umkehrung“ von Satz 16.10:

Lemma 16.11

Zwischen zwei verschiedenen rationalen Zahlen liegt immer eine irrationale Zahl, d. h., zu $q_1, q_2 \in \mathbb{Q}$ mit $q_1 < q_2$ existiert ein $r \in \mathbb{R} \setminus \mathbb{Q}$ mit $q_1 < r < q_2$.

Beweis. Sei $n \in \mathbb{N}^+$ beliebig. $n^2 + 1$ ist offensichtlich kein Quadrat einer natürlichen Zahl. Völlig analog zu Aufgabe 16.2 kann man zeigen, dass das Supremum s der Menge $\{q \in \mathbb{Q} : q^2 < n^2 + 1\}$ irrational sein muss.[14] Es gilt dann $s^2 \ge n^2 + 1 > n^2$ und damit $s > n$. Da mit s auch $1/s$ irrational ist (weil $\mathbb{Q}$ ein Körper ist), haben wir gerade gezeigt, dass wir zu $n \in \mathbb{N}^+$ eine irrationale Zahl r mit $0 < r < 1/n$ finden können.

Sind nun q_1 und q_2 wie in der Formulierung des Lemmas gegeben, dann stellen wir sie als Brüche mit gemeinsamen Nenner $n \in \mathbb{N}^+$ dar: $q_1 = m_1/n$ und $q_2 = m_2/n$ mit $q_2 - q_1 \ge 1/n$. Wir wählen eine irrationale Zahl r zwischen 0 und $1/n$ und erhalten mit $m_1/n + r$ eine Zahl zwischen q_1 und q_2, die nach Aufgabe 16.7 irrational ist. ■

Definition

Eine Menge I von reellen Zahlen wird **Intervall** genannt, wenn für alle $r_1, r_2 \in I$ und alle $x \in \mathbb{R}$ aus $r_1 < x < r_2$ immer $x \in I$ folgt.

unechte/echte Intervalle

Ein Intervall ist also ein „lückenloses Stück der Zahlengeraden“. Die einfachsten Intervalle sind die leere Menge und alle Singletons. (Siehe Aufgabe 16.9.) Diese Mengen werden auch als *unechte Intervalle* bezeichnet, während man Intervalle mit mehr als einem Element *echt* nennt. Die sind die eigentlich interessanten.

[13] Sie sind inzwischen mit der mathematischen Sprechweise natürlich vertraut genug, dass Sie diesen Satz nicht so interpretieren, dass zwischen r_1 und r_2 *nur eine* rationale Zahl liegt.

[14] Es handelt sich um die Zahl $\sqrt{n^2+1}$. In Aufgabe 16.2 ging es um den Spezialfall $n = 1$.

Lemma 16.12

Ist eine nichtleere Menge I von reellen Zahlen ein Intervall, dann erfüllt sie eine der folgenden vier Bedingungen, die sich gegenseitig ausschließen:

(i) I ist beschränkt und $\{x \in \mathbb{R} : \inf I < x < \sup I\} \subseteq I$

(ii) I ist nur nach unten beschränkt und $\{x \in \mathbb{R} : \inf I < x\} \subseteq I$

(iii) I ist nur nach oben beschränkt und $\{x \in \mathbb{R} : x < \sup I\} \subseteq I$

(iv) $I = \mathbb{R}$

Insbesondere enthalten alle echten Intervalle unendlich viele Zahlen.

Beweis. Für den ersten Teil wählen wir uns eine Zahl $x \in \mathbb{R}$ mit $\inf I < x < \sup I$. Weil x größer als das Infimum von I ist, ist x keine untere Schranke von I. Also muss es ein $r_1 \in I$ mit $r_1 < x$ geben. Analog muss es wegen $x < \sup I$ ein $r_2 \in I$ mit $x < r_2$ geben. Weil I ein Intervall ist, folgt $x \in I$.

Die Formulierung „*nur* nach unten beschränkt“ im zweiten Teil soll natürlich bedeuten, dass I nach unten beschränkt und nach oben unbeschränkt ist. Gilt $\inf I < x$ für eine beliebige reelle Zahl, dann findet man wie im ersten Teil ein $r_1 \in I$ mit $r_1 < x$. Außerdem kann nach Voraussetzung x keine obere Schranke von I sein. Also gibt es ein $r_2 \in I$ mit $x < r_2$. Damit haben wir wieder dieselbe Situation wie eben. Die anderen beiden Fälle beweist man analog.

Hat ein Intervall I mindestens zwei Elemente r_1 und r_2, so liegen nach Definition alle Zahlen zwischen r_1 und r_2 in I. Aus Satz 16.10 und Lemma 16.11 folgt dann, dass I unendlich viele Zahlen enthalten muss. ■

Intervalle können also nur bestimmte Formen annehmen, für die wir eine Schreibweise einführen, die aus der Schule bekannt sein sollte.

Definition

Für $a, b \in \mathbb{R}$ definieren wir die folgenden Mengen:

$$
\begin{aligned}
[a,b] &= \{x \in \mathbb{R} : a \le x \le b\} & [a,b) &= \{x \in \mathbb{R} : a \le x < b\} \\
(a,b] &= \{x \in \mathbb{R} : a < x \le b\} & (a,b) &= \{x \in \mathbb{R} : a < x < b\} \\
[a,\infty) &= \{x \in \mathbb{R} : a \le x\} & (a,\infty) &= \{x \in \mathbb{R} : a < x\} \\
(-\infty,b] &= \{x \in \mathbb{R} : x \le b\} & (-\infty,b) &= \{x \in \mathbb{R} : x < b\} \\
(-\infty,\infty) &= \mathbb{R}
\end{aligned}
$$

Dazu ein paar Anmerkungen:

(i) Es gibt in jedem Semester ein paar Studierende, die berichten, dass man in der Schule $[a,b[$ statt $[a,b)$ geschrieben habe. Wenn Sie das unbedingt so schreiben wollen, dann machen Sie das. (Dann aber konsistent und nicht mal so und mal so!) Ich persönlich finde solche „verdrehten“ Klammern ausgesprochen häßlich und werde sie in diesem Skript nicht verwenden.

(ii) Das Zeichen ∞ in Ausdrücken wie $[a,\infty)$ ist nur ein Symbol. ∞ ist *keine* reelle Zahl! Daher würde auch so etwas wie „$[a,\infty]$“ keinen Sinn ergeben.[15]

(iii) Wir verwenden dieselbe Schreibweise (a,b) für Intervalle und für geordnete Paare. Solche Überschneidungen werden sich nie ganz vermeiden lassen. In der Praxis wird sich die Verwechslungsgefahr als sehr gering herausstellen und zur Not kann man durch eine Formulierung wie „das Intervall (a,b)“ klarstellen, was gemeint ist.

$\mathbb{R}_{\geq 0}$ (iv) Wir werden manchmal auch Schreibweisen wie $\mathbb{R}_{\geq 0}$ für $[0,\infty)$ oder $\mathbb{R}_{<0}$ für $(-\infty,0)$ verwenden. Die sollten hoffentlich suggestiv genug sein, um nicht explizit definiert werden zu müssen.

Aufgabe 16.9. Wer noch nicht so viel Erfahrung mit der Denkweise der Mathematik hat, wundert sich evtl. darüber, dass Mengen wie $\emptyset$ oder $\{42\}$ Intervalle sind. Begründen Sie diese Aussage, indem Sie die Definition in eine Formel der Prädikatenlogik übersetzen und anhand derer nachweisen, dass sie auf unechte Intervalle zutrifft.

Aufgabe 16.10. Mit der oben definierten Intervallschreibweise sind wirklich *alle* Intervalle abgedeckt. Wie kann man mit dieser Notation unechte Intervalle aufschreiben?

Aufgabe 16.11. Wie viele Elemente hat die Menge $[1,5]$?

Aufgabe 16.12. Machen Sie sich klar, dass aus der Definition folgt, dass der Durchschnitt von zwei Intervallen wieder ein Intervall ist. Geben Sie zur Übung $[1/2,5)\cap(3,7]$, $(1/2,5]\cap[3,7)$, $[1/2,\infty)\cap(3,7]$, $[1/2,3]\cap[3,7]$ und $[1/2,3)\cap[3,7]$ an.

Aufgabe 16.13. Geben Sie zwei Intervalle an, deren Vereinigung ein Intervall ist. Geben Sie dann zwei Intervalle an, deren Vereinigung *kein* Intervall ist.

Aufgabe 16.14. Ist $I_1 \setminus I_2$ immer ein Intervall, wenn I_1 und I_2 Intervalle sind?

Aufgabe 16.15. Jeweils zwei der unten aufgeführten Mengen sind gleich. Finden Sie die entsprechenden Paare.

$$A = (-2,4]\cap[-4,2) \qquad B = \{x\in\mathbb{R} : x>0 \vee x<2\}$$
$$C = (-2,2)\cap\mathbb{Q} \qquad D = \{x\in\mathbb{R} : x\leq 0 \wedge x\geq 2\}$$
$$E = \{x\in\mathbb{Q} : x^2<4\} \qquad F = \{x\in\mathbb{R} : |x|<4\}$$
$$G = (-\infty,2]\cup[-2,\infty) \qquad H = \{x\in\mathbb{R} : x^2<4\}$$
$$I = (-\infty,-2]\cap[2,\infty) \qquad J = (-4,4)$$

Aufgabe 16.16. Welche der folgenden Mengen sind echte Intervalle?

$$[40,42]\setminus[40,41) \qquad [40,41]\setminus\mathbb{N} \qquad [40,42]\setminus[40,42)$$
$$[40,41]\setminus\mathbb{Q} \qquad [40,41]\cap[41,43] \qquad (40,42)\setminus\mathbb{N}$$

[15] Es gibt verschiedene Möglichkeiten, unendliche Elemente zu $\mathbb{R}$ hinzuzufügen. Das werden wir in diesem Rahmen jedoch nicht behandeln.

⋆ Betrag, Signumfunktion und Gaußklammern im Computer

Der Absolutbetrag heißt in PYTHON, wie in vielen Programmiersprachen, `abs`. Die Signumfunktion gibt es in PYTHON nicht, aber man kann sie nach Lemma 16.9 leicht selbst bauen.

```
sgn = lambda x: 0.0 if x==0 else x/abs(x)
```

Diese Funktion gibt immer Fließkommazahlen zurück. Falls Sie lieber ganzzahlige Ergebnisse haben möchten oder sich wegen der Division Gedanken ob der Effizienz machen, können Sie es etwas kryptischer auch so programmieren:

```
sgn = lambda x: (x>0)-(x<0)
```

Die Gaußklammern erhält man folgendermaßen:

```
from math import floor, ceil
floor(-7/2), ceil(-47/10)
```

17. Die komplexen Zahlen

Komplexe Zahlen haben sich im 16. Jahrhundert gleichsam in die Mathematik "eingeschlichen". Inzwischen sind sie aber ein unverzichtbarer Bestandteil nicht nur der Mathematik, sondern auch der Naturwissenschaften und der Informatik. So kann man z. B. die Programmierung von Quantencomputern ohne komplexe Zahlen nicht verstehen.

In Aufgabe 10.8 haben wir gesehen, dass das direkte Produkt $\mathbb{R} \times \mathbb{R}$ kein Körper ist. Es gibt jedoch eine andere Möglichkeit, auf dieser Menge einen Körper zu definieren.

Definition

Auf der Menge $\mathbb{R} \times \mathbb{R}$ definieren wir die inneren Verknüpfungen $+$ und $\cdot$ durch

$$(a,b)+(c,d) = (a+c, b+d) \quad \text{und}$$
$$(a,b)\cdot(c,d) = (ac-bd, ad+bc).$$

Wenn wir so rechnen, schreiben wir $\mathbb{C}$ statt $\mathbb{R} \times \mathbb{R}$ und bezeichnen die Elemente von $\mathbb{C}$ als **komplexe Zahlen**.

Wir wissen bereits (Aufgabe 8.2), dass wir durch diese Definition eine abelsche Gruppe $(\mathbb{C}, +)$ erhalten, deren neutrales Element $(0,0)$ ist. Wir werden nun sehen, dass auch die Multiplikation alle Anforderungen für einen Körper erfüllt. Teilweise ist das einfach Rechenarbeit.

Aufgabe 17.1. Überprüfen Sie durch Einsetzen in die Definition, dass die gerade definierte Multiplikation assoziativ, kommutativ und zudem distributiv über der Addition ist und dass $(1,0)$ das neutrale Element der Multiplikation ist.

Satz 17.1

$\mathbb{C}$ ist ein Körper, der eine Kopie von $\mathbb{R}$ enthält.

Beweis. Der größte Teil der Arbeit wurde bereits in Aufgabe 17.1 erledigt. Es fehlt noch der Kehrwert zu einer komplexen Zahl $(a,b) \neq (0,0)$. Da wenden wir einen ähnlichen Rechentrick an wie in der Lösung von Aufgabe 15.11:

$$(a,b)\cdot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=\left(\frac{a\cdot a-b\cdot(-b)}{a^2+b^2},\frac{a\cdot(-b)+b\cdot a}{a^2+b^2}\right)=(1,0)$$

Was ist mit der Kopie von $\mathbb{R}$? Dafür betrachten wir die komplexe Zahlen, deren zweite Komponente verschwindet. Für die gilt nach den Rechenregeln in $\mathbb{C}$:

$$(a,0)+(b,0)=(a+b,0) \quad \text{und} \quad (a,0)\cdot(b,0)=(a\cdot b,0).$$

Eine komplexe Zahl von der Form $(a,0)$ verhält sich beim Rechnen also exakt so wie die reelle Zahl a. ■

Es bietet sich daher die folgende Konvention an:

Konvention

Für komplexe Zahlen der Form $(a,0)$ schreiben wir einfach a und behandeln sie wie reelle Zahlen.

In diesem Sinne ist $\mathbb{R}$ eine Teilmenge von $\mathbb{C}$ (d. h., reelle Zahlen sind komplexe Zahlen) und wir können (16.1) folgendermaßen erweitern:

$$\mathbb{P}\subset\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}.$$

i (imaginäre Einheit)

Wir geben nun der komplexen Zahl $(0,1)$, die *keine* reelle Zahl ist, einen Namen, nämlich i. Man nennt sie auch die *imaginäre Einheit*. Mit i und der obigen Konvention ergeben sich zwei grundlegende Gleichungen:

$$\begin{aligned} a+b\cdot\mathrm{i}=(a,0)+(b,0)\cdot(0,1)=(a,b) \quad &\text{für alle } a,b\in\mathbb{R} \text{ und}\\ \mathrm{i}^2=(0,1)\cdot(0,1)=(-1,0)=-1. \quad &(17.1)\end{aligned}$$

Die Tupel (a,b) haben damit ihre Schuldigkeit getan und wir können komplexe Zahlen in Zukunft so schreiben, wie man es üblicherweise macht.

Konvention

Für komplexe Zahlen (a,b) schreiben wir ab jetzt $a+b\cdot\mathrm{i}$ oder kürzer $a+b\mathrm{i}$.

Definition

Ist z die komplexe Zahl $a+b\mathrm{i}$, so nennt man a den **Realteil** von z und b den **Imaginärteil**. Man schreibt dafür $\mathrm{Re}(z)$ bzw. $\mathrm{Im}(z)$.[16] Komplexe Zahlen der Form $b\mathrm{i}$ werden **rein imaginär** genannt. Elemente von $\mathbb{C}\setminus\mathbb{R}$, also komplexe Zahlen, die *nicht* reell sind, nennt man man **echt komplex**.

[16] In manchen Büchern auch $\Re(z)$ und $\Im(z)$ in Fraktur.

Bei reellen Zahlen verschwindet also der Imaginärteil, bei rein imaginären der Realteil. Echt komplexe Zahlen sind solche, bei denen der Imaginärteil nicht verschwindet. Das Adjektiv *imaginär* stammt aus einer Zeit, zu der man den komplexen Zahlen noch die Existenzberechtigung absprach und sie als „nur imaginiert“ ansah. Das Adjektiv *komplex* – nicht zu verwechseln mit *kompliziert* – kommt daher, dass diese Zahlen aus reellen und imaginären Zahlen zusammengesetzt sind. Nebenbei haben wir hier zum ersten Mal gesehen, dass man für komplexe Zahlen die Variablennamen z und w bevorzugt, während man für reelle eher x und y verwendet. Das ist aber lediglich eine Konvention und keine feste Regel.

Weil wir es mit einem Körper zu tun haben und i sowie die reellen Zahlen Körperelemente sind, können wir wie gewohnt rechnen, dabei aber gemäß (17.1) immer i^2 durch -1 ersetzen. Hier ein Beispiel:[17]

$$(2-3\mathrm{i})\cdot(4+\mathrm{i}) = 2\cdot 4 - 3\mathrm{i}\cdot 4 + 2\mathrm{i} - 3\mathrm{i}\cdot\mathrm{i} = 8 - 12\mathrm{i} + 2\mathrm{i} - 3\cdot(-1) = 11 - 10\mathrm{i}$$

Aufgabe 17.2. Geben Sie Real- und Imaginärteil von $z = 3 - 4\mathrm{i}$ an.

Aufgabe 17.3. Wenn eben alles mit rechten Dingen zuging, dann müsste sich nach der „alten“ Schreibweise $(2,-3)\cdot(4,1) = (11,-10)$ ergeben. Vielleicht rechnen Sie das vorsichtshalber noch einmal nach.

Addition, Subtraktion und Multiplikation von komplexen Zahlen sollten damit klar sein. Für die Division kann man sich die Vorgehensweise aus dem Beweis von Satz 17.1 wohl am besten so merken: Will man durch $c + d\mathrm{i}$ teilen, so erweitert man mit $c - d\mathrm{i}$. Im Nenner ergibt sich dann die reelle Zahl $c^2 + d^2$. Zum Beispiel so:

$$\frac{4+\mathrm{i}}{2-5\mathrm{i}} = \frac{4+\mathrm{i}}{2-5\mathrm{i}}\cdot\frac{2+5\mathrm{i}}{2+5\mathrm{i}} = \frac{3+22\mathrm{i}}{2^2+5^2} = \frac{3}{29} + \frac{22}{29}\mathrm{i}$$

Aufgabe 17.4. Wenn die komplexen Zahlen neu für Sie sind, dann sollten Sie das Rechnen mit ihnen auf jeden Fall üben. In Wolfram Alpha können Sie Ausdrücke wie `(4+i)/(2-5i)` direkt eingeben und damit Ihre Ergebnisse überprüfen.

Bevor wir dazu kommen, wozu die komplexen Zahlen eigentlich gut sind, zunächst eine schlechte Nachricht.

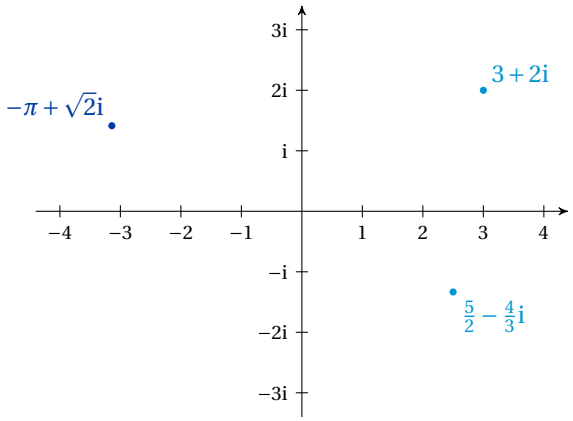
Lemma 17.2. Die komplexen Zahlen lassen sich nicht anordnen.

Beweis. Aus Lemma 15.3 wissen wir über angeordnete Körper, dass 1 immer positiv und -1 daher immer negativ ist. Und wir wissen, dass Quadrate nie negativ sind. Aber nach (17.1) ist das Quadrat von i negativ. Das war's schon. ∎

Es ergibt also keinen Sinn, sich die komplexen Zahlen analog zu den reellen auf so etwas wie einer „komplexen Zahlengeraden“ vorzustellen. So eine Anordnung würde jedenfalls nicht zu den Rechenoperationen passen. Komplexe Zahlen können

[17] Es ist hoffentlich klar, dass $2-3\mathrm{i}$ eine Abkürzung für $2+(-3)\mathrm{i}$ ist, also für die Zahl, die gerade eben noch $(2,-3)$ hieß.

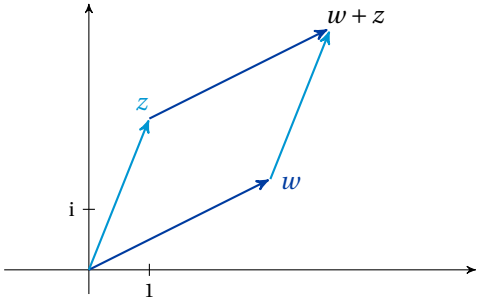
deswegen auch nicht „positiv“ oder „negativ“ sein.[18] Es gibt jedoch eine geometrische Interpretation der komplexen Zahlen, die sehr hilfreich ist: Man trägt die Zahlen $a+b\mathrm{i}$ als Punkte (a,b) in ein kartesisches Koordinatensystem ein.



gaußsche Zahlenebene

Die reelle Zahlengerade bildet die horizontale Achse und der Rest der Ebene ist mit echt komplexen Zahlen bedeckt. Auf der vertikalen Achse liegen die rein imaginären Zahlen. Man nennt das die *gaußsche Zahlenebene*.

Das ist nicht nur eine hübsche Darstellung, sondern sie liefert auch sinnvolle geometrische Gegenstücke zu den Rechenoperationen. Für die Addition zweier komplexer Zahlen w und z stellt man sich beide als Pfeile vor, die von 0 (also vom Ursprung des Koordinatensystems) auf diese Zahlen zeigen. Verschiebt man den z-Pfeil so, dass sein Anfang auf der Spitze des w-Pfeils landet, so zeigt seine Spitze auf $w+z$.[19] Das kennen Sie aus der Schule vom Rechnen mit Vektoren bzw. vom Kräfteparallelogramm.



Aufgabe 17.5. Wenn Sie die Lage einer komplexen Zahl z in der gaußschen Zahlenebene kennen, wo liegt dann $-z$?

Aufgabe 17.6. Zeichnen Sie eine ähnliche Skizze wie oben für die Subtraktion zweier komplexer Zahlen.

[18] Das hat u. a. die Konsequenz, dass Sie, wenn Sie in einem Mathebuch so etwas wie $x>0$ lesen, sich sicher sein können, dass x *nicht* komplex ist.

[19] Und mit vertauschten Rollen erhält man dasselbe Ergebnis, wodurch man gleich eine visuelle Bestätigung der Kommutativität der Addition erhält.

Wie gesagt sollten Ihnen die graphische Addition und Subtraktion komplexer Zahlen (wenn auch nicht unter diesem Namen) vertraut sein. Aber wie kann man sich die Multiplikation vorstellen? Dafür müssen wir noch ein wenig Vorarbeit leisten, die wir ohnehin brauchen werden. Wie berechnet man den Abstand eines Punktes (a, b) vom Ursprung? Genau, mit dem Satz des Pythagoras. Der Abstand ist die Quadratwurzel von $a^2 + b^2$. Dieser Zahl geben wir einen Namen.

Definition

Der **Absolutbetrag** bzw. **Betrag** ist die Funktion von $\mathbb{C}$ nach $\mathbb{R}$, die jede komplexe Zahl $z = a + b\mathrm{i}$ auf den Wert $|z| = \sqrt{a^2 + b^2} = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}$ abbildet.

Man beachte, das z zwar irgendeine komplexe Zahl sein kann, $a^2 + b^2$ aber immer eine nichtnegative reelle Zahl ist. Die Quadratwurzel ist also immer definiert und ebenfalls eine nichtnegative reelle Zahl (wie es sich für einen Abstand gehört.)

Aufgabe 17.7. Berechnen Sie $|\mathrm{i}|$.

Aufgabe 17.8. Sei $z = a + b\mathrm{i}$. Vergleichen Sie $|z|$ und $|-z|$.

Aufgabe 17.9. Welcher Zusammenhang besteht zwischen dem komplexen Betrag und dem auf Seite 164 definierten reellen Betrag?

Aufgabe 17.10. Sei $w = a + b\mathrm{i}$ und $z = c + d\mathrm{i}$. Berechnen Sie $|wz|$ und $|w| \cdot |z|$. Was fällt Ihnen auf?

Lemma 17.3

Für alle $w, z \in \mathbb{C}$ gilt:

(i) $|w| \geq 0$

(ii) $|w| = 0 \Leftrightarrow w = 0$

(iii) $|wz| = |w| \cdot |z|$ (*Multiplikativität*)

(iv) $|w + z| \leq |w| + |z|$ (*Dreiecksungleichung*)

Beweis. Die ersten beiden Punkte sollten wohl offensichtlich sein. Der dritte Punkt wurde in Aufgabe 17.10 bewiesen. Der vierte Punkt erfordert etwas Rechnerei. Für beliebige reelle Zahlen a, b, c und d gilt $0 \leq (bc - ad)^2$, weil Quadrate nie negativ sind. Berechnet man das Quadrat mit der zweiten binomischen Formel und subtrahiert dann einen der drei Summanden, so ergibt sich $2abcd \leq b^2c^2 + a^2d^2$. In der folgenden Kette von Ungleichungen folgt nun jeweils eine aus der nächsten, indem entweder umgeformt oder auf beiden Seiten dasselbe addiert oder ausgenutzt wird, dass aus $0 \leq x \leq y$ immer $\sqrt{x} \leq \sqrt{y}$ folgt.

$$
\begin{aligned}
2abcd &\leq b^2c^2 + a^2d^2 \\
a^2c^2 + 2abcd + b^2d^2 &\leq a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\
(ac + bd)^2 &\leq (a^2 + b^2)(c^2 + d^2) \\
2(ac + bd) \leq 2\sqrt{(ac + bd)^2} &\leq 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
a^2 + 2ac + c^2 + b^2 + 2bd + d^2 &\leq a^2 + b^2 + 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} + c^2 + d^2
\end{aligned}
$$

$$(a+c)^2+(b+d)^2 \le \left(\sqrt{a^2+b^2}+\sqrt{c^2+d^2}\right)^2$$
$$\sqrt{(a+c)^2+(b+d)^2} \le \sqrt{a^2+b^2}+\sqrt{c^2+d^2}$$

Setzt man nun $w = a+b\mathrm{i}$ und $z = c+d\mathrm{i}$, so steht in der letzten Zeile die zu beweisende Dreiecksungleichung. ■

Aufgabe 17.11. In Wolfram Alpha können Sie mit Eingaben wie `|3+5i|` Beträge von komplexen Zahlen ausrechnen. Berechnen Sie $|w|+|z|$ und $|w+z|$ für $w = 3+\mathrm{i}$ und $z = 1+2\mathrm{i}$, um sich zu überzeugen, dass man in der Dreiecksungleichung $\le$ nicht durch $=$ ersetzen kann. (Siehe auch Aufgabe 16.6.) Zeichnen Sie eine Skizze, in der man w, z und $w+z$ sieht, und erklären Sie daran den Namen *Dreiecksungleichung*.

Blättern Sie zurück und Sie werden sehen, dass das gerade bewiesene Lemma 17.3 exakt dieselben Aussagen macht wie Lemma 16.7. Daher können wir auch dieselben Dinge folgern wie in Korollar 16.8 und müssen das nicht mehr beweisen (denn wir könnten den Originalbeweis wortwörtlich abschreiben).

Korollar 17.4

Für alle $w, z \in \mathbb{C}$ gilt:

(i) $|w/z| = |w|/|z|$ für $z \neq 0$

(ii) $|w-z| \le |w|+|z|$

(iii) $||w|-|z|| \le |w \pm z|$

Vielleicht ist Ihnen aufgefallen, dass der „Pythagoras“-Term, der im Betrag unter der Wurzel auftaucht, bei der Division bereits vorkam und wie wir dort auf ihn gekommen sind. Das wollen wir noch aufschreiben, weil dahinter eine unscheinbare, aber wichtige Funktion steht.

Definition

Die zu $z = a+b\mathrm{i}$ **konjugiert komplexe** Zahl ist $a-b\mathrm{i}$ und wird $\overline{z}$ geschrieben.

Beim *Konjugieren* (man verwendet das Wort auch als Verb) wird also einfach das Vorzeichen des Imaginärteils umgedreht. Einfacher geht's kaum.

Aufgabe 17.12. Wenn Sie die Lage einer komplexen Zahl z in der gaußschen Zahlenebene kennen, wo liegt dann $\overline{z}$?

Aufgabe 17.13. Sei $w = a+b\mathrm{i}$ und $z = c+d\mathrm{i}$. Berechnen Sie $\overline{w+z}$ und $\overline{w}+\overline{z}$. Was fällt Ihnen auf? Und wie ist es mit $\overline{w\cdot z}$ und $\overline{w}\cdot\overline{z}$?

Aufgabe 17.14. Was kommt heraus, wenn man $z+\overline{z}$ bzw. $z-\overline{z}$ berechnet?

In Anbetracht dessen, was wir schon wissen, müssen wir die wichtigsten Eigenschaften der Konjugation nur noch zusammenfassen und nichts mehr beweisen.

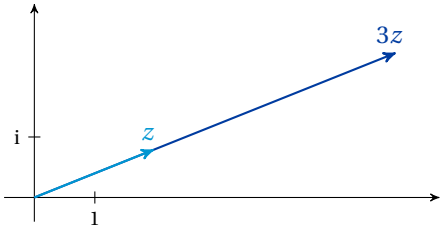
Lemma 17.5

Für alle $w, z \in \mathbb{C}$ gilt:

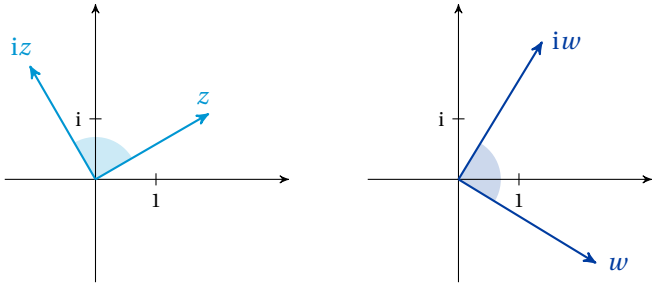
(i) $|z| = \sqrt{z\overline{z}}$

(ii) $\overline{w+z} = \overline{w} + \overline{z}$
(iii) $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$
(iv) $z + \overline{z} = 2\,\mathrm{Re}(z)$
(v) $z - \overline{z} = 2\mathrm{i}\,\mathrm{Im}(z)$

Nun kommen wir zur Multiplikation und schauen uns zunächst zwei besonders einfache Fälle an, von denen der erste auch eine Entsprechung beim Rechnen mit Vektoren hat. Multipliziert man nämlich eine komplexe Zahl $z = a + b\mathrm{i}$ mit einer positiven *reellen* Zahl r, so erhält man $rz = ra + rb\mathrm{i}$. Das entspricht offenbar einfach einer Streckung ($r > 1$) bzw. Stauchung ($r < 1$) des entsprechenden Pfeils um diesen Faktor. Bei Vektoren nennt man das skalare Multiplikation. Insbesondere hat rz den Abstand $|rz| = r \cdot |z|$ von null, ist also r-mal so „lang“ wie z.[20]



Multipliziert man $z = a + b\mathrm{i}$ mit i, so ergibt sich $\mathrm{i}z = -b + a\mathrm{i}$. Die Komponenten des zugehörigen Punktes in der gaußschen Zahlenebene werden also vertauscht und bei der hinteren ändert sich zudem bei diesem Tausch das Vorzeichen. Geometrisch ist das eine Drehung um einen rechten Winkel (wobei sich der Abstand von der Null nicht ändert, weil i den Betrag eins hat).

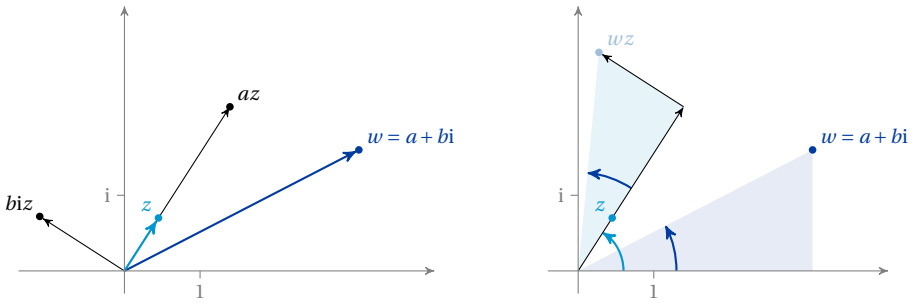


Jetzt schauen wir uns die Multiplikation einer beliebigen komplexen Zahl z mit irgendeiner anderen komplexen Zahl $w = a + b\mathrm{i}$ an. (Der Einfachheit halber gehen wir von positiven Zahlen a und b aus. Den Fall, dass a oder b oder beide negativ sind, sollten Sie danach zur Kontrolle selbst skizzieren.) Wir zerlegen das Produkt als $wz = (a + b\mathrm{i})z = az + b\mathrm{i}z$. Wir haben uns vorher überlegt:

(i) az entspricht einer Streckung von z um den Faktor a.
(ii) $\mathrm{i}z$ entspricht einer Drehung von z um einen rechten Winkel.
(iii) $b\mathrm{i}z$ entspricht einer Streckung von $\mathrm{i}z$ um den Faktor b.
(iv) Die Resultate aus dem ersten und dritten Schritt werden addiert.

[20] Ist r negativ, so ändert sich außerdem noch die Richtung und rz ist $|r|$-mal so „lang“ wie z.

Das sieht im Ergebnis so aus:



Mit Schulkenntnissen aus der Elementargeometrie können wir nun die folgenden Beobachtungen machen:

- Wir sehen zwei rechtwinklige Dreiecke.
- Das rechte hat die Kathetenlängen a und b.
- Das linke hat die Kathetenlängen $a|z|$ und $b|z|$.
- Also sind die beiden Dreiecke ähnlich und das linke ist aus dem rechten durch Streckung (oder Stauchung) um den Faktor $|z|$ hervorgegangen.
- Darum sind erstens alle Winkel in den Dreiecken gleich und zweitens hat die Hypotenuse des linken Dreiecks die Länge $|z||w|$ (weil die Hypotenuse des rechten Dreiecks die Länge $|w|$ hat).

Dass $|w||z|$ der Betrag des Produktes wz ist, wussten wir bereits, aber es ist beruhigend, das noch einmal bestätigt zu bekommen. Neu ist jedoch die sehr wichtige Erkenntnis über die Winkel, für die wir einen Begriff einführen.

Definition

Für $z \in \mathbb{C}\setminus\{0\}$ sei das **Argument** von z, geschrieben $\arg(z)$, der Winkel zwischen der positiven reellen Achse und der Verbindunglinie von z mit dem Nullpunkt. Um eine eindeutige Angabe zu garantieren, legen wir fest, dass das Argument (in Bogenmaß) immer ein Winkel aus dem Intervall $(-\pi, \pi]$ sein soll.

Damit können wir festhalten: *Das Argument von wz ist die Summe der Argumente von w und z.* Wir erhalten dadurch übrigens auch eine schöne geometrische Begründung für die Regel „minus mal minus ist plus“, die wir schon aus der Schule kennen.[21] Negative reelle Zahlen haben das Argument π (also 180 Grad). Multipliziert man zwei solche Zahlen, so hat das Ergebnis das Argument 2π bzw. 360 Grad, was bedeutet, dass es auf der positiven Hälfte der reellen Achse liegen muss.

Aufgabe 17.15. Sei $z = -a + b\mathrm{i}$ mit $a, b > 0$. In welcher Hälfte der gaußschen Zahlenebene liegt z^2 mit Sicherheit *nicht*?

Aufgabe 17.16. Sei $z \in \mathbb{C}$ mit $\mathrm{Re}(z) > 0$ und $\mathrm{Im}(z) < 0$. Was kann man über die Lage von z^3 in der gaußschen Zahlenebene aussagen?

[21] Nach Lemma 10.2 gilt das in jedem Ring. Damit ist die Aussage aber nicht unbedingt „klar“.

Das Argument von z^2 erhält man also, indem man das Argument von z verdoppelt. Daraus folgt, wie man eine Zahl w mit $w^2 = z$ findet: Der Betrag von w muss $\sqrt{|z|}$ sein und das Argument von w muss die Hälfte des Arguments von z betragen. Zumindest geometrisch ist also klar, dass es so eine „Wurzel“ immer geben muss. Da beweisen wir nun auch algebraisch.

Satz 17.6

Für jede komplexe Zahl $z \in \mathbb{C} \setminus \{0\}$ hat die Gleichung $w^2 = z$ genau zwei verschiedene Lösungen, wobei die zweite Lösung sich durch $-w_1$ ergibt, wenn w_1 die erste ist.

Beweis. Bevor wir zu eigentlichen Berechnung einer Lösung kommen, klären wir die einfachen Punkte. Dass mit w_1 auch $-w_1$ eine Lösung ist, folgt aus Lemma 10.2. Ist eine Lösung w_1 bekannt, so können wir die Gleichung $w^2 = z$ außerdem als $w^2 = w_1^2$ schreiben. Durch Umformen (dritte binomische Formel) wird daraus $(w - w_1)(w + w_1) = 0$. Nach Lemma 10.4 kann das Produkt auf der linken Seite nur verschwinden, wenn einer der Faktoren verschwindet, wenn also $w - w_1 = 0$ oder $w + w_1 = 0$ gilt. Daher kann es außer w_1 und $-w_1$ keine weiteren Lösungen geben.

Um auf eine Lösung zu kommen, gehen wir nun von $z = a + b\mathrm{i}$ aus und machen den Ansatz $w_1 = c + d\mathrm{i}$. $w_1^2 = z$ bedeutet ausgeschrieben

$$c^2 - d^2 + 2cd\mathrm{i} = a + b\mathrm{i}$$

und damit $c^2 - d^2 = a$ und $2cd = b$. Beachten Sie, dass wir ab hier nur noch im Reellen arbeiten. a, b, c und d stehen für reelle Zahlen!

Die zweite Gleichung formen wir zu $d = b/(2c)$ um und setzen das in die erste ein. Das liefert die folgenden Gleichungen, die jeweils durch einfache Umformungen der vorherigen entstanden sind:

$$\begin{aligned} c^2 - b^2/(4c^2) &= a \\ 4c^4 - b^2 &= 4ac^2 \\ c^4 - ac^2 - b^2/4 &= 0 \\ x^2 - ax - b^2/4 &= 0 \end{aligned}$$

Die letzte Gleichung ergab sich, indem wir eine neue Variable x für c^2 substituiert haben. Mit der bekannten p-q-Formel erhält man

$$x_{1,2} = a/2 \pm \sqrt{a^2/4 + b^2/4} = a/2 \pm |z|/2.$$

Wegen $x = c^2$ kann x nicht negativ sein. Wir wählen daher die positive der beiden Lösungen[22] und nennen sie x_1. Daraus ergeben sich zwei mögliche Werte für c, die mit $d = b/(2c)$ zwei zugehörige Werte für d liefern. ■

Aufgabe 17.17. Gehen Sie den Beweis von Satz 17.6 für den konkreten Fall $z = 3 + 4\mathrm{i}$ durch und geben Sie die beiden Lösungen an.

[22] Wegen $|a/2| \leq |z|/2$ *muss* eine von beiden Lösungen positiv sein.

Aufgabe 17.18. Wolfram Alpha kann natürlich auch Gleichungen wie `w^2=-7+24i` lösen. Wenn Sie aber einfach irgendwelche komplexen Zahlen einsetzen, werden die Ergebnisse selten „schön“ sein. Zum Üben würde ich das folgende Vorgehen vorschlagen: Berechnen Sie für ein paar komplexe Zahlen z_1 bis z_n die Quadrate z_1^2 bis z_n^2 und schreiben Sie die beiden Listen auf zwei verschiedene Zettel. Am nächsten Tag haben Sie die Zahlen sicher vergessen. Sie können dann aus der zweiten Liste eine Zahl z_k^2 entnehmen, die Aufgabe $w^2 = z_k^2$ lösen und danach Ihr Ergebnis w mit dem Wert z_k aus der ersten Liste vergleichen. Arbeiten Sie ruhig auch ab und zu mit Brüchen und nicht nur mit ganzen Zahlen!

⋆**Aufgabe 17.19**. Im Beweis von Satz 17.6 habe ich (absichtlich) etwas gepfuscht. Können Sie das Problem erkennen (und beheben)?

Ist es nun also OK, $2+\mathrm{i} = \sqrt{3+4\mathrm{i}}$ zu schreiben? Leider ist die Sache etwas kompliziert. Wenn a eine positive reelle Zahl ist, dann hat die Gleichung $x^2 = a$ zwei Lösungen, von denen eine positiv und eine negativ ist. Mit $\sqrt{a}$ ist dann *per definitionem* immer die positive der beiden Lösungen gemeint! Man muss es irgendwie festlegen, damit durch die Zuordnung $x \mapsto \sqrt{x}$ eine Funktion von $\mathbb{R}$ nach $\mathbb{R}$ definiert wird.[23] Wenn die komplexen Zahlen ins Spiel kommen, kann man aber nicht mehr von positiv oder negativ reden. Man könnte nun willkürlich etwas festlegen (z. B. die Lösung, die in der rechten Hälfte der gaußschen Zahlenebene liegt), aber keine solche Festlegung liefert eine Funktion, die für alle komplexen Zahlen definiert ist und „angenehme“ mathematische Eigenschaften wie Stetigkeit oder Differenzierbarkeit hat. Auf weitere Details kann ich hier nicht eingehen und belasse es bei dem Hinweis, dass Sie *nicht* $\sqrt{z}$ schreiben sollten, wenn z eine beliebige komplexe Zahl ist.

Auf jeden Fall können wir aber nun jede Gleichung der Form $w^2 = z$ lösen und wir können sogar noch mehr.

Satz 17.7

Sind a, b und c beliebige komplexe Zahlen mit $a \neq 0$, dann hat die Gleichung $aw^2 + bw + c = 0$ immer mindestens eine Lösung (und höchstens zwei verschiedene).

Beweis. Man kann die gesamte Gleichung offenbar durch a dividieren, ohne ihre Lösungsmenge zu ändern. Es reicht daher, sich mit Gleichungen der Form

$$w^2 + pw + q = 0 \tag{17.2}$$

zu beschäftigen, wobei p und q beliebige komplexe Zahlen sind.

Wir begründen zunächst, warum es nicht mehr als zwei Lösungen geben kann. Ist w_1 eine Lösung, dann kann man die Gleichung als

$$w^2 + pw + q = w_1^2 + pw_1 + q$$

[23] Ich habe schon öfter die falsche Vorstellung gehört, $\sqrt{a}$ stehe für *beide* Lösungen. Das ist aber schlicht und einfach falsch und wäre auch nicht sehr hilfreich. $\sqrt{a}$ wäre dann nicht einmal eine Zahl …

schreiben und zu $w^2 - w_1^2 + pw - pw_1 = 0$ umformen. Mit der dritten binomischen Formel wird daraus $(w - w_1)(w + w_1 + p) = 0$. Wie im Beweis von Satz 17.6 ist klar, dass es nur noch eine weitere Lösung, nämlich die von $w + w_1 + p = 0$, geben kann.

Man verschafft sich nun eine Lösung z_1 von $z^2 = p^2/4 - q$, die es nach Satz 17.6 gibt. $w_1 = -p/2 + z_1$ und $w_2 = -p/2 - z_1$ sind dann zwei (evtl. identische) Lösungen von (17.2), wie man durch Einsetzen leicht nachprüft. ■

Aufgabe 17.20. Berechnen Sie beide Lösungen von $2w^2 + (2+2\mathrm{i})w + (12+36\mathrm{i}) = 0$.

Aufgabe 17.21. Wie in Aufgabe 17.18 sollten Sie sich selbst Aufgaben stellen und diese dann später lösen. Aufgaben generiert man, indem man sich zwei komplexe Zahlen w_1 und w_2 (die Lösungen) ausdenkt und dann den Term $(w - w_1)(w - w_2)$ ausmultipliziert.

Abschließend sei darauf hingewiesen, dass wir die geometrische Interpretation der komplexen Zahlen bisher nur zur Illustration und Motivation der Konzepte verwendet haben. In den Beweisen kam sie nicht vor. In Abschnitt 29 werden wir auf das Thema zurückkommen und diese Sichtweise präzisieren.

⋆ Komplexe Zahlen im Computer

PYTHON bietet als Standard bereits komplexe Zahlen. Fügt man direkt hinter einer Zeichenkette, die als Zahl erkennbar ist, den Buchstaben `j` (klein oder groß) an, so wird das als rein imaginäre Zahl erkannt.[24] Ein alleinstehendes `j` wird jedoch als die Variable mit diesem Namen interpretiert. Beliebige komplexe Zahlen gibt man als Summe von Real- und Imaginärteil ein oder mit der Funktion `complex`.

```
42J, 42j, 2.3j, 23e-1j
2+3j, complex(2,3)
(5+3j)*(3+2j)
z = 5+3j
abs(z), z.real, z.imag
```

Das letzte Beispiel zeigt, dass Real- und Imaginärteil intern grundsätzlich als Fließkommazahlen gespeichert werden.[25] Für das Rechnen mit komplexen Zahlen sollte in der Regel die Standardbibliothek CMATH benutzt werden.

```
import cmath
# würde mit dem "normalen" sqrt nicht funktionieren:
cmath.sqrt(-15-8j), cmath.sqrt(-4)
cmath.phase(-42)                    # das Argument
```

[24] PYTHON übernimmt hier die in den Ingenieurwissenschaften übliche Bezeichnung j für die imaginäre Einheit.

[25] Sprachen wie JULIA oder COMMON LISP bieten auch Typen an, in denen die beiden Teile einer komplexen Zahl intern als ganze Zahl oder als Bruch gespeichert werden können.

18. Etwas Topologie (in metrischen Räumen)

Die Topologie ist ein wichtiges Teilgebiet der Mathematik, in dem vereinfacht gesagt die Lage und die Anordnung geometrischer Objekte abstrakt untersucht wird – wobei *Geometrie* in einem sehr allgemeinen Sinne gemeint ist, der mit der Schulgeometrie nicht mehr viel gemeinsam hat. Wir werden diesen großen Bereich nur streifen und es kann auch sehr schnell ziemlich kompliziert werden, aber ein paar wichtige Begriffe werden immer wieder eine Rolle spielen und darum sollen sie in diesem Abschnitt definiert und erklärt werden.

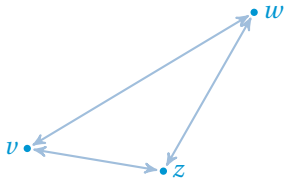
Wir hatten die Betragsfunktion so definiert, dass $|z|$ anschaulich der Abstand der Zahl z von der Zahl 0 in der gaußschen Zahlenebene ist. Daraus folgt sofort (siehe die Skizze zur Lösung von Aufgabe 17.6), dass $|w-z|$ der Abstand der Zahlen w und z ist. Es ist offensichtlich, dass der Abstand von w und z nur null sein kann, wenn $w=z$ gilt, und dass der Abstand von w und z dasselbe wie der Abstand von z und w ist. Zudem zeigt ein simpler „Rechentrick“, dass die folgende Aussage gilt:

Lemma 18.1

Dreiecksungleichung für Abstände
Für alle $v, w, z \in \mathbb{C}$ gilt $|w-z| \leq |w-v| + |v-z|$.

Aufgabe 18.1. Sehen Sie, wieso Lemma 18.1 aus der Dreiecksungleichung in Lemma 17.3 folgt?

Weil diese Ungleichung so wichtig ist, spendiere ich noch einmal eine Skizze. Es ist hoffentlich evident, dass die direkte Verbindung von w und z nicht länger sein kann als der „Umweg“ über v. Und auch, dass sich an der Korrektheit der Aussage nichts ändert, wenn wir die Namen der Punkte vertauschen.



Die Idee des Abstands wird nun abstrahiert.

Definition

Ist X irgendeine Menge und d eine Funktion von X^2 nach $\mathbb{R}$, die die folgenden drei Eigenschaften für alle $x, y, z \in X$ hat, dann nennt man d eine **Metrik** auf X und (X, d) einen **metrischen Raum**.[26]

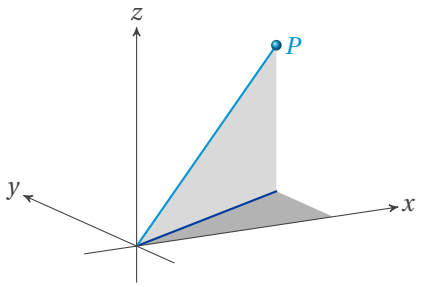
- **M1:** $d(x,y) \geq 0 \wedge (d(x,y) = 0 \Leftrightarrow x = y)$ (*positive Definitheit*)
- **M2:** $d(x,y) = d(y,x)$ (*Symmetrie*)
- **M3:** $d(x,y) \leq d(x,z) + d(z,y)$ (*Dreiecksungleichung*)

[26] Häufig geht aus dem Zusammenhang hervor, was d ist, und man bezeichnet dann einfach X als metrischen Raum. Wir haben das schon bei Gruppen gemacht, wenn wir statt $(G, \otimes)$ einfach G geschrieben haben.

Eine Metrik ist also ein verallgemeinerter Abstandsbegriff. Zwei Objekten x und y wird ein „Abstand“ $d(x,y)$ zugeordnet, wobei gefordert wird, dass Abstände nichtnegative Zahlen sind, dass zwei Objekte dann und nur dann den Abstand null haben, wenn sie identisch (also *ein* Objekt) sind, dass der Abstand von x und y dasselbe wie der Abstand von y und x ist und dass „Umwege“ keine Abkürzungen sein können.

Nach unseren Vorüberlegungen ist klar, dass $\mathbb{C}$ ein metrischer Raum ist, wenn wir als Metrik $d(x,y) = |x-y|$ festsetzen. Ebenso ist natürlich $\mathbb{R}$ mit dieser Metrik ein metrischer Raum, weil $\mathbb{R}$ eine Teilmenge von $\mathbb{C}$ ist. (Wir messen dann einfach Abstände auf der Zahlengeraden.) Es gibt jedoch noch viele weitere Beispiele, von denen wir uns nun ein paar anschauen wollen.

– Mit Geometrie werden wir uns später noch beschäftigen. Im Vorgriff können wir jedoch schon einmal das Berechnen von Abständen im Raum $\mathbb{R}^3$ betrachten. Um herauszufinden, wie weit der Punkt P in der folgenden Skizze vom Ursprung entfernt ist, berechnet man zunächst die Länge der dunkelblauen Strecke, die den Nullpunkt mit der Projektion von P in die x-y-Ebene verbindet. Das macht man mithilfe des Satzes von Pythagoras in dem dunkelgrauen rechtwinkligen Dreieck, das komplett in dieser Ebene liegt. Danach wendet man den Satz erneut auf das hellgraue (ebenfalls rechtwinklige) Dreieck an.



Das liefert eine Formel für die sogenannte *Norm* $\|P\|$ des Punktes (bzw. seines Ortsvektors). Mit $d(P,Q) = \|P-Q\|$ erhält man eine Metrik auf $\mathbb{R}^3$ (und kann das sogar auf $\mathbb{R}^n$ für beliebige $n \in \mathbb{N}$ verallgemeinern).

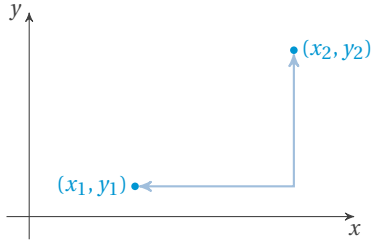
Norm

Diese Metrik (die mit den obigen für $\mathbb{C}$ und $\mathbb{R}$ übereinstimmt, wenn man diese Zahlenmengen als $\mathbb{R}^2$ bzw. $\mathbb{R}^1$ interpretiert), bezeichnet man auch als *euklidischen Abstand*.

euklidischer Abstand

– Man kann aber vertraute geometrische Räume auch ganz anders metrisieren. Durch $d\big((x_1,y_1),(x_2,y_2)\big) = |x_1-x_2| + |y_1-y_2|$ wird beispielsweise die sogenannte *Manhattan-Metrik* auf $\mathbb{R}^2$ definiert.

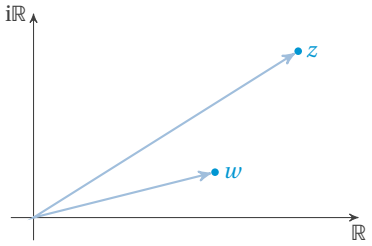
Manhattan-Metrik



Ihren Namen erhält sie daher, dass man sich vorstellen kann, dass der Abstand gemessen wird, den man zurücklegen müsste, wenn man nur auf „Straßen“ fahren darf, die parallel zu den Achsen verlaufen.

französische Eisenbahnmetrik

– Eine weitere „lustige“ Metrik in der Ebene ist die *französische Eisenbahnmetrik*. Am einfachsten kann man sie hinschreiben, wenn man die Punkte der Ebene als komplexe Zahlen betrachtet. Der Abstand von z und w wird in dieser Metrik als $d(z,w) = |z-w|$ definiert, falls z und w auf derselben Gerade durch den Nullpunkt liegen, und als $d(z,w) = |z| + |w|$ für andere Paare von Punkten.



Die scherzhafte Bezeichnung kommt daher, dass es angeblich im 19. Jahrhundert im Eisenbahnnetz Frankreichs keine direkten Verbindungen zwischen größeren Städten gab, sondern man immer über Paris (den Nullpunkt) fahren musste.

Hamming-Abstand

– Eine Anwendung dieses Konzepts aus der Informationstheorie ist der nach einem amerikanischen Mathematiker aus dem 20. Jahrhundert benannte *Hamming-Abstand*. Dabei geht es z. B. um Tupel aus der Menge $B = \{0,1\}^n$, die man als Nachrichten betrachten kann, die aus n Bits bestehen. Der Abstand zweier solcher Tupel ist definiert als die Anzahl der Komponenten, an denen sie *nicht* übereinstimmen. Das ist eine Metrik auf B. Für $n = 4$ wäre der Hamming-Abstand von $(0,1,1,0)$ und $(1,1,0,0)$ beispielsweise 2, weil die erste und die dritte Komponente sich unterscheiden. Wenn man es nun etwa mit einem Code zu tun hat, bei dem der Abstand zweier Codewörter immer mindestens drei ist, dann bedeutet das, dass man auch dann, wenn zwei Bits falsch übertragen wurden, noch erkennen kann, dass es Fehler gab.

Levenshtein-Distanz

– Eine Anwendung im Bereich der Informatik und gleichzeitig eine Verallgemeinerung des Hamming-Abstands ist die nach einem russischen Mathematiker benannte *Levenshtein-Distanz*. Dabei geht es um Wörter, für die drei Operationen definiert sind: einen beliebigen Buchstaben des Wortes entfernen, einen beliebigen Buchstaben des Wortes durch einen anderen ersetzen, einen Buchstaben an einer beliebigen Position des Wortes hinzufügen. Der Abstand zweier Wörter ist die *minimale* Anzahl solcher Operationen, die man benötigt, um aus dem einen Wort das andere zu machen. Man kann z. B. `HUMBUG` aus `HAMBURG` machen, indem man erst `A` und `R` entfernt und dann hinter dem `H` ein `U` einfügt. Das sind drei Operationen. Man kann aber auch das `R` entfernen und das `A` direkt durch ein `U` ersetzen. Die Levenshtein-Distanz der beiden Wörter ist daher zwei. Eingesetzt wird das u. a. bei der Autokorrektur: Es sollen Wörter vorgeschlagen werden, die im Sinne dieser Metrik möglichst „nahe“ an den getippten liegen.

Aufgabe 18.2. Rechnen Sie nach, dass die Manhattan-Metrik die Bedingung **M3** der Dreiecksungleichung erfüllt.

Aufgabe 18.3. Überprüfen Sie **M3** auch für die französische Eisenbahnmetrik.

⋆**Aufgabe 18.4**. Wie ändert sich die Formel für die Eisenbahnmetrik, wenn Paris nicht im Nullpunkt, sondern an der Stelle $p \in \mathbb{C}$ liegt? Ist das dann immer noch eine Metrik?

Aufgabe 18.5. Geben Sie eine möglichst große Teilmenge von $B = \{0,1\}^3$ an, für die der Hamming-Abstand zweier Elemente von B immer mindestens 2 ist.

Aufgabe 18.6. Können Sie einen Zusammenhang zwischen dem Hamming-Abstand und der Manhattan-Metrik erkennen?

⋆**Aufgabe 18.7**. Überlegen Sie sich einen Algorithmus (oder programmieren Sie ihn), mit dem man die Levenshtein-Distanz zweier vorgegebener Wörter berechnen kann. Sie werden feststellen, dass das gar nicht so einfach ist, wenn das Verfahren effizient sein soll.

Viele der folgenden Begriffe werden gleich ganz allgemein für metrische Räume definiert. Wir werden sie jedoch zunächst hauptsächlich auf den euklidischen Abstand in $\mathbb{R}$ und $\mathbb{C}$ anwenden. Zumindest für diese beiden Räume sollten Sie jeweils Beispiele vor Ihrem inneren Auge parat haben.

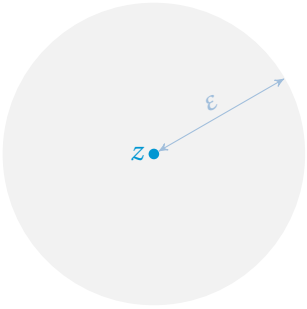
Definition

Sei (X,d) ein metrischer Raum, $x \in X$ und $\varepsilon > 0$. Die Menge

$$U_\varepsilon(x) = \{\, y \in X : d(x,y) < \varepsilon \,\}$$

wird als **(offene) ε-Kugel** oder **ε-Umgebung um** x bezeichnet.[27]

In der gaußschen Zahlenebene ist $U_\varepsilon(z)$ also eine Kreisscheibe mit dem Radius ε um den Mittelpunkt z, wobei – weil in der Definition $<$ und nicht $\leq$ steht – der Kreisrand *nicht* dazugehört. $U_1(0)$ ist der Einheitskreis und zu dieser Menge gehören unter anderem die Zahlen 0, 1/2 oder $(1+\mathrm{i})/10$, aber z. B. *nicht* -1 und i und „erst recht“ nicht 42 oder $2-7\mathrm{i}$.



[27] Eigentlich müsste am U noch irgendwo das d stehen, damit man weiß, um welche Metrik es geht. Das lässt man aber üblicherweise weg und verlässt sich darauf, dass die Leser schon verstehen werden, was gemeint ist. Im Englischen nennt man diese Kugeln übrigens *ball* und verwendet die Schreibweise $B_\varepsilon(x)$.

Die Bezeichnung Kugel kommt daher, dass die offenen Kugeln im Raum $\mathbb{R}^3$ mit dem euklidischen Abstand tatsächlich Kugeln (ohne Oberfläche) sind. In diesem Sinne sind Mengen der Form $U_\varepsilon(x)$ in beliebigen metrischen Räumen „verallgemeinerte Kugeln“. In der Mathematik abstrahiert man eben gerne …

Umgebung

Außerdem bezeichnet man auch oft eine Menge $U \subseteq X$ einfach als *Umgebung* von $x \in X$, wenn es ein $\varepsilon > 0$ mit $U_\varepsilon(x) \subseteq U$ gibt. Jede ε-Umgebung ist damit automatisch eine Umgebung, aber auch Mengen, die nicht genau diese Form haben, können Umgebungen sein.[28]

Aufgabe 18.8. Wie sehen die offenen ε-Kugeln in $\mathbb{R}$ aus?

Aufgabe 18.9. Seien a, b reelle Zahlen mit $a < b$. Begründen Sie, dass das Intervall (a, b) eine offene ε-Kugel ist.

Aufgabe 18.10. Wie sehen die offenen ε-Kugeln bezüglich der Manhattan-Metrik aus?

Aufgabe 18.11. Endliche Zeichenketten (oder *Strings*, wie sie beim Programmieren genannt werden) bezeichnen wir für diese Aufgabe als *Wörter*. X sei die (unendliche) Menge aller Wörter, die man mit den drei Buchstaben `A`, `B` und `C` bilden kann. Zu X gehören also Wörter wie `B`, `CC`, `ABBA`, `ABCABC` und so weiter.[29] Wie sieht $U_2(\texttt{AC})$ bezüglich der Levenshtein-Metrik auf X aus?

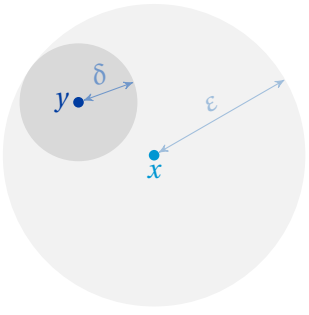
Lemma 18.2 Ist (X, d) ein metrischer Raum, $x \in X$ und $\varepsilon > 0$, dann gibt es zu jedem $y \in U_\varepsilon(x)$ ein $\delta > 0$ mit $U_\delta(y) \subseteq U_\varepsilon(x)$.

Beweis. Wegen $y \in U_\varepsilon(x)$ gilt $r = d(x, y) < \varepsilon$. Wir setzen $\delta = \varepsilon - r$. Für $y' \in U_\delta(y)$ gilt dann nach der Dreiecksungleichung

$$d(y', x) \leq d(y', y) + d(y, x) = d(y', y) + r < \delta + r = \varepsilon$$

und damit $y' \in U_\varepsilon(x)$. ∎

Das schematische Bild zur Aussage von Lemma 18.2 sieht so aus:



[28] Auch hier sind sich leider die Bücher nicht einig. Manchmal werden nur offene Mengen als Umgebungen bezeichnet.

[29] Für diese Aufgabe ist es nicht relevant, aber da Sie diesem Konzept in der Theoretischen Informatik erneut begegnen werden, sei darauf hingewiesen, dass auch das *leere Wort* zu X gehört, also ein String der Länge null.

Jeder Punkt y aus der Menge $U_\varepsilon(x)$ hat dort also ein bisschen „Platz“ um sich herum. Er kann sich etwas „bewegen“, ohne $U_\varepsilon(x)$ zu verlassen (solange die neue Position weniger als δ von seiner alten entfernt ist). ε-Kugeln sind nicht die einzigen Mengen, die diese Eigenschaft haben. Weil sie wichtig ist, geben wir ihr einen Namen.

Definition

Sei (X,d) ein metrischer Raum. Eine Menge $A \subseteq X$ heißt **offen**, wenn es zu jedem $y \in A$ ein $\delta > 0$ mit $U_\delta(y) \subseteq A$ gibt.

In Lemma 18.2 haben wir also bewiesen, dass ε-Kugeln das Adjektiv *offen*, das ihnen bereits in der Definition angeheftet wurde, tatsächlich verdienen.

Fangen wir gleich mit einem Beispiel für eine Menge an, die *nicht* offen ist. Das Intervall $I = [0,1)$ ist nicht offen in $\mathbb{R}$, denn egal wie klein $\delta > 0$ ist, in der δ-Kugel um 0 werden sich immer negative Zahlen befinden, die nicht zu I gehören. Ein anderes einfaches Beispiel sind endliche Mengen wie $\{42\}$ oder $\{1,2,3\}$, die weder in $\mathbb{R}$ noch in $\mathbb{C}$ offen sind.

Und noch ein triviales Beispiel: In jedem metrischen Raum (X,d) sind $\emptyset$ und X offen. Sie haben sich inzwischen hoffentlich genügend an die mathematische Denkweise gewöhnt, um einzusehen, warum das so ist.

Aufgabe 18.12. Fallen Ihnen außer den Mengen aus Aufgabe 18.9 noch andere offene Mengen in $\mathbb{R}$ ein?

Aufgabe 18.13. Ist das Intervall $I = (0,1)$ offen in $\mathbb{C}$?

Aufgabe 18.14. Sei X irgendeine Menge. Definiert man d durch

$$d(x,y) = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases}$$

für $x, y \in X$, dann erhält man die sogenannte *diskrete Metrik* auf X. Wie sehen die offenen Mengen bezüglich dieser Metrik aus?

diskrete Metrik

Lemma 18.3

Sei (X,d) ein metrischer Raum und $\mathscr{A} \neq \emptyset$ eine Menge von offenen Teilmengen von X. Dann ist $\bigcup \mathscr{A}$ offen. Ist $\mathscr{A}$ endlich, dann ist auch $\bigcap \mathscr{A}$ offen.

Beweis. Ist $y \in \bigcup \mathscr{A}$, dann gibt es eine Menge $A \in \mathscr{A}$ mit $y \in A$. Weil A offen ist, gibt es ein $\delta > 0$ mit $U_\delta(y) \subseteq A$. Wegen $A \subseteq \bigcup \mathscr{A}$ ist der erste Teil des Lemmas damit bereits bewiesen.

Für den zweiten Teil sei $\mathscr{A}$ die Menge $\{A_1, \ldots, A_n\}$. Gilt $y \in \bigcap \mathscr{A} = A_1 \cap \cdots \cap A_n$, dann gibt es positive Zahlen δ_1 bis δ_n mit $U_{\delta_i}(y) \subseteq A_i$ für $i = 1, \ldots, n$. Setzt man $\delta = \min\{\delta_1, \ldots, \delta_n\}$, dann gilt offenbar $U_\delta(y) \subseteq \bigcap \mathscr{A}$. ∎

Der obige Beweis des zweiten Teils von Lemma 18.3 funktioniert nicht mehr bei unendlich vielen Mengen, weil dann das Minimum, das dort vorkommt, nicht existieren muss. Und tatsächlich stimmt die Aussage für unendlich viele offene Mengen

im Allgemeinen auch nicht mehr. Ein Standardbeispiel für $\mathbb{R}$ sind die Intervalle $(-1/n, 1/n)$, die für $n \in \mathbb{N}^+$ alle offen sind. Ihre Schnittmenge $\bigcap_{n\in\mathbb{N}^+}(-1/n, 1/n)$ ist jedoch $\{0\}$ und das ist keine offene Menge.

Definition

Sei (X, d) ein metrischer Raum, $A \subseteq X$, $x \in X$ und $a \in A$. a heißt **innerer Punkt** von A, wenn es eine offene Menge $B \subseteq X$ mit $a \in B \subseteq A$ gibt. a heißt **isolierter Punkt** von A, wenn es eine offene Menge $B \subseteq X$ mit $B \cap A = \{a\}$ gibt. x heißt **Berührungspunkt** von A, wenn $B \cap A \neq \emptyset$ für jede offene Menge $B \subseteq X$ mit $x \in B$ gilt. x heißt **Randpunkt** von A, wenn x Berührungspunkt von A und von $X \setminus A$ ist. Der **Rand** ∂A von A ist die Menge der Randpunkte von A. Das **Innere** A° von A ist die Menge der inneren Punkte von A. Der **Abschluss** $\overline{A}$ von A ist die Menge der Berührungspunkte von A. A heißt **abgeschlossen**, wenn $\overline{A} = A$ gilt.

Das sind zugegebenermaßen ziemlich viele Begriffe auf einmal. Man sollte sich diese am besten anhand von schematischen Skizzen merken, statt abstrakte Definitionen auswendig zu lernen. Im linken Teil der folgenden Grafik soll die Menge A aus der grauen Fläche sowie dem Punkt a_1 bestehen. a_1 ist damit ein isolierter Punkt von A und a_2 ein innerer Punkt. a_3 ist ein Randpunkt von A und zusammen mit der schwarzen Linie Teil des Randes ∂A. Dafür ist es unerheblich, ob die Punkte auf dieser Linie Elemente von A sind oder nicht. (Das „sieht“ man anhand so einer Zeichnung ja ohnehin nicht.) Alle drei Punkte sind Berührungspunkte von A. Die gestrichelten Kreise sollen jeweils offene Mengen um die Punkte darstellen.

Im mittleren Teil sieht man das Innere A°. a_1 gehört nicht dazu und auch keiner der Randpunkte – auch dann nicht, wenn diese Randpunkte Elemente von A waren. Rechts sieht man schließlich den Abschluss $\overline{A}$. a_1 gehört dazu und der gesamte Rand auch. Auch dabei ist es irrelevant, welche Randpunkte Elemente von A waren.

Ein Versuch einer anschaulichen Interpretation: Wie wir uns oben bereits überlegt hatten, haben Elemente von offenen Mengen in diesen Mengen immer ein bisschen „Platz“ um sich herum; sie können sich kleine Bewegungen in alle Richtungen „leisten“, ohne die offene Menge zu verlassen. Das gilt auch für die inneren Punkte einer Menge. Berührungspunkte einer Menge A sind Elemente von X, die mit kleinen Bewegungen[30] A erreichen können. (Wenn sie schon Elemente von A sind, müssen sie sich gar nicht bewegen.) Randpunkte von A können daher „mit minimalem Aufwand“ sowohl A erreichen als auch A verlassen. (Für einen von beiden Schritten müssen sie logischerweise gar nichts machen, denn entweder

[30] Wenn hier informell von „kleinen“ Bewegungen die Rede ist, dann bedeutet das, dass das Ziel der Bewegung ein Ort ist, dessen Abstand vom Startpunkt beliebig klein sein kann, solange er positiv ist.

gehören sie zu A oder nicht.) Eine Menge ist genau dann abgeschlossen, wenn ihr Rand zur Menge gehört. (Siehe dazu auch Aufgabe 18.19.)

Ein paar Beispiele:

- Seien a und b reelle Zahlen mit $a < b$. Wir betrachten die Intervalle $I_1 = [a,b]$, $I_2 = [a,b)$, $I_3 = (a,b]$ und $I_4 = (a,b)$. a und b sind (die einzigen) Randpunkte dieser Intervalle. I_1 ist der Abschluss aller vier Intervalle und die einzige abgeschlossene Menge unter den vieren. I_4 ist das Innere aller vier Intervalle und die einzige offene Menge unter den vieren. Keines der vier Intervalle hat isolierte Punkte.
- Für $a \in \mathbb{R}$ ist $I = [a,a] = \{a\}$ abgeschlossen. a ist Randpunkt und isolierter Punkt von I. Das Innere von I ist die leere Menge.
- Im konkreten Fall der Räume $\mathbb{C}$ bzw. $\mathbb{R}^2$ mit euklidischem Abstand gilt für alle $x \in X$ und alle $\varepsilon > 0$

$$\overline{U_\varepsilon(x)} = \{y \in X : d(x,y) \leq \varepsilon\} \text{ und}$$
$$\partial U_\varepsilon(x) = \{y \in X : d(x,y) = \varepsilon\}.$$

  Dabei geht es um Kreise und der *Rand* eines solchen Kreises ist dann auch das, was wir uns anschaulich darunter vorstellen.
- Ist eine Menge X, die mit der diskreten Metrik (siehe Aufgabe 18.14) versehen ist, dann sind alle Teilmengen von X sowohl offen als auch abgeschlossen.

Aufgabe 18.15. Gehen Sie die obigen Beispiele durch und machen Sie sich jeweils klar, dass Sie verstanden haben, warum die dort stehenden Aussagen wahr sind. (Glauben Sie das nicht einfach und lernen Sie es auf keinen Fall auswendig!)

Aufgabe 18.16. Gehen Sie analog zum obigen Beispiel unbeschränkte Intervalle der Formen $[a,\infty)$, (a,∞), $(-\infty,b]$ und $(-\infty,b)$ durch.

Aufgabe 18.17. Geben Sie eine offene Teilmenge von $\mathbb{R}$ an, die kein Intervall ist.

Aufgabe 18.18. Begründen Sie, dass in jedem metrischen Raum $A^\circ \subseteq A \subseteq \overline{A}$ für alle Teilmengen A des Raumes gilt.

Aufgabe 18.19. Begründen Sie, dass in jedem metrischen Raum $\overline{A} = A \cup \partial A$ für alle Teilmengen A des Raumes gilt.

Lemma 18.4 Sei (X,d) ein metrischer Raum und $A \subseteq X$. Dann ist A genau dann offen, wenn $A = A^\circ$ gilt. Und das ist genau dann der Fall, wenn $X \setminus A$ abgeschlossen ist.

Beweis. Bei der ersten Äquivalenz geht es nur darum, die Definitionen richtig zu lesen. Sei A offen. Nach Aufgabe 18.18 gilt $A^\circ \subseteq A$ und wir müssen nur $A \subseteq A^\circ$ zeigen. Das folgt aber aus der Definition von offenen Mengen und Lemma 18.2. Nun gelte umgekehrt $A = A^\circ$. Wir wollen zeigen, dass A offen ist. Aber weil jeder Punkt von A innerer Punkt von A ist, liegt er in einer offenen Menge B, die ganz

in A liegt. Und die enthält nach Definition eine ε-Umgebung des Punktes, die „erst recht“ in A liegt.

Nun zur zweiten Äquivalenz. Sei A offen. Nach Aufgabe 18.18 müssen wir nur noch zeigen, dass $x \in X \setminus A$ aus $x \in \overline{X \setminus A}$ folgt. Wir machen das indirekt: Gilt $x \notin X \setminus A$, also $x \in A$, dann gibt es, weil A offen ist, ein $\varepsilon > 0$ mit $U_\varepsilon(x) \subseteq A$. Das ist eine offene Menge, die x enthält und disjunkt zu $X \setminus A$ ist. Daher ist x kein Berührungspunkt von $X \setminus A$.

Sei umgekehrt $X \setminus A$ abgeschlossen. Ist $a \in A$ beliebig, dann gilt $a \notin X \setminus A$ und a ist daher kein Berührungspunkt von $X \setminus A$. Also gibt es eine offene Menge B mit $x \in B$, die disjunkt zu $X \setminus A$ ist. Das heißt aber, dass B eine Teilmenge von A ist. Damit ist gezeigt, dass A offen ist (denn o. B. d. A. ist B eine ε-Umgebung von a). ■

Korollar 18.5

Sei (X, d) ein metrischer Raum und $\mathscr{A} \neq \emptyset$ eine Menge von abgeschlossenen Teilmengen von X. Dann ist $\bigcap \mathscr{A}$ abgeschlossen. Ist $\mathscr{A}$ endlich, dann ist auch $\bigcup \mathscr{A}$ abgeschlossen.

Beweis. Nach den de-morgansche Regeln (siehe KapitelI) gilt

$$\bigcap \mathscr{A} = X \setminus \bigcup \{X \setminus A : A \in \mathscr{A}\} \quad \text{und} \quad \bigcup \mathscr{A} = X \setminus \bigcap \{X \setminus A : A \in \mathscr{A}\}.$$

Mit den Lemmata 18.3 und 18.4 folgt dann sofort die Behauptung. ■

Korollar 18.6

In jedem metrischen Raum sind alle endlichen Mengen abgeschlossen. Damit sind auch alle offenen Mengen, von denen nur endlich viele Elemente entfernt wurden, offen.

Beweis. Offensichtlich sind Singletons $A = \{a\}$ immer abgeschlossen, denn für jedes $x \in A$ mit $x \neq a$ gilt $r = d(x, a) > 0$ und A und $U_r(x)$ disjunkt, d. h. x ist kein Berührungspunkt von A. Nach Korollar 18.5 sind damit auch endliche Mengen abgeschlossen. Ist schließlich B offen und sind b_1 bis b_n Elemente von B, dann ist $B \setminus \{b_1, \ldots, b_n\}$ Durchschnitt der offenen Mengen B und $X \setminus \{b_1, \ldots, b_n\}$, die beide offen sind. ■

Insbesondere sind nach Lemma 18.4 in jedem metrischen Raum (X, d) die Mengen $\emptyset$ und X offen und abgeschlossen. Anhand des Beispiels der diskreten Metrik haben wir gesehen, dass es noch viele andere Mengen mit dieser Eigenschaft geben kann. Das ist aber nicht in jedem Raum so.

Lemma 18.7

Im Raum der reellen Zahlen sind $\emptyset$ und $\mathbb{R}$ die einzigen Mengen, die sowohl offen als auch abgeschlossen sind.

Beweis. Sei $A \subseteq \mathbb{R}$ weder leer noch ganz $\mathbb{R}$. Dann gibt es Zahlen x und y mit $x \in A$ und $y \notin A$. O. B. d. A. sei $x < y$. Wir definieren $A_1 = \{r \in A : x \leq r < y\}$. Diese Menge ist nicht leer und nach oben beschränkt, hat also ein Supremum s. Ist s ein Element

von A, dann ist s das Maximum von A_1 und sicher kleiner als y. Das Intervall $(s, y]$ ist damit eine Teilmenge von $X \setminus A$. Für alle $\varepsilon < y - s$ liegen aber dann in $U = U_\varepsilon(s)$ Zahlen zwischen s und y, die nicht zu A gehören, d. h., U ist keine Teilmenge von A. Das bedeutet, A ist nicht offen. Ist s hingegen *kein* Element von A, so liegen in jeder ε-Umgebung von s Elemente von $A_1 \subseteq A$, denn sonst wäre s nicht das Supremum von A_1. Damit liegt aber keine ε-Umgebung von s ganz in $X \setminus A$ und $X \setminus A$ ist nicht offen. ■

Die obige Aussage gilt auch für $\mathbb{C}$, aber das können wir momentan noch nicht richtig begründen.

Aufgabe 18.20. Es sollte eigentlich bereits klar sein, aber wegen der Wahl der Wörter[31] gibt es ab und zu das Missverständnis, dass eine Menge, die nicht offen ist, abgeschlossen sein müsste und umgekehrt. Geben Sie daher, damit Sie das erst gar nicht denken, eine Teilmenge von $\mathbb{R}$ an, die *weder* offen *noch* abgeschlossen ist.

Der Vollständigkeit halber präzisieren wir noch die Wortwahl aus Satz 16.10.

Sei (X, d) ein metrischer Raum und $A \subseteq X$. A liegt **dicht** in X, wenn $\overline{A} = X$ gilt. **Definition**

Wenn es stimmt, dass $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt, dann muss jede reelle Zahl r Berührungspunkt von $\mathbb{Q}$ sein. Und das stimmt auch. Ist B eine offene Menge, die r enthält, dann gibt es ein $\varepsilon > 0$ mit $U_\varepsilon(x) \subseteq B$ und nach Satz 16.10 gibt es ein $q \in \mathbb{Q}$ mit $x - \varepsilon < q < x + \varepsilon$, also mit $q \in B$.

Aufgabe 18.21. Liegt $\mathbb{R} \setminus \mathbb{Q}$ auch dicht in $\mathbb{R}$?

Für die Analysis brauchen wir noch eine Verallgemeinerung des Begriffs der beschränkten Menge.

Sei (X, d) ein metrischer Raum und $A \subseteq X$. Gibt es ein $r > 0$ und ein $x \in X$ mit $A \subseteq U_r(x)$, dann wird A **beschränkt** genannt. **Definition**

Aufgabe 18.22. Begründen Sie, warum A genau dann beschränkt ist, wenn es ein $r > 0$ und ein $x \in X$ mit $A \subseteq \overline{U_r(x)}$ gibt.

Aufgabe 18.23. Begründen Sie, warum eine Menge A von reellen Zahlen im Sinne dieser Definition genau dann beschränkt ist, wenn sie im Sinne der Definition von Seite 159 beschränkt ist. (Sonst wäre es auch nicht sehr clever, denselben Begriff zu verwenden.)

Aufgabe 18.24. Identifizieren Sie unter den metrischen Räumen, die Sie schon kennengelernt haben, einen, in dem *alle* Mengen beschränkt sind.

[31] Ein Fenster oder eine Tür sind immer *entweder* offen *oder* abgeschlossen.

Anschaulich bedeutet dieser Begriff, dass die Abstände innerhalb einer beschränkten Menge nicht beliebig groß werden können:

Lemma 18.8 Sei (X,d) ein metrischer Raum und $A \subseteq X$. A ist genau dann beschränkt, wenn $\{d(a_1,a_2) : a_1, a_2 \in A\}$ nach oben beschränkt ist.

Beweis. Gilt $A \subseteq U_r(x)$ und sind a_1 und a_2 Elemente von A, dann gilt nach der Dreiecksungleichung $d(a_1,a_2) \leq d(a_1,x) + d(x,a_2) < r + r$. Ist umgekehrt b eine obere Schranke für die Abstände zweier Elemente von A und a irgendein Element von A, dann liegen alle Elemente von A in $U_{b+1}(a)$. ■

VII

Folgen und Reihen

In den folgenden Abschnitten werden Grenzwertprozesse eine zentrale Rolle spielen. Sie bilden die Basis der sogenannten Analysis und sind auch der Grund dafür, warum wir die reellen Zahlen brauchen.

19. Folgen

In Abschnitt 6 hatten wir bereits definiert, was eine *Folge* ist, nämlich eine Abbildung f, deren Definitionsbereich $\mathbb{N}$ ist und die man in Kurzform als $(f(n))_{n\in\mathbb{N}}$ schreibt. Mit Folgen werden wir uns nun ausführlich beschäftigen.

Konvention

Wir schreiben allgemeine Folgen meistens in der Form $(a_n)_{n\in\mathbb{N}}$. Damit ist gemeint, dass a_n der Funktionswert der Folge für das Argument n ist. Man nennt a_n dann auch das n-te **Folgenglied**. Häufig werden wir auch den Index weglassen und einfach (a_n) schreiben, wenn klar ist, dass von Folgen die Rede ist. Und schließlich ignorieren wir gelegentlich den Fall, dass endlich viele Folgenglieder evtl. nicht definiert sind. Wir würden beispielsweise $(1/n)$ schreiben, obwohl diese Folge eigentlich für $n = 0$ nicht definiert ist.[1]
Wir sagen, dass (a_n) eine Folge **in** der Menge M ist, wenn der Wertebereich der Folge eine Teilmenge von M ist. Folgen in $\mathbb{R}$ bzw. $\mathbb{C}$ bezeichnen wir auch als **reelle** bzw. **komplexe Folgen**.
Schließlich sei in den folgenden Aussagen in diesem Abschnitt (X, d) immer ein beliebiger metrischer Raum, wenn in den Voraussetzungen nicht explizit etwas anderes steht.

(a_n)

Definition

Eine Folge (a_n) in X **konvergiert** gegen (oder **geht** gegen) $a \in X$, wenn es für alle $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt, so dass $a_n \in U_\varepsilon(a)$ für alle $n \geq n_0$ gilt.

[1] Zur Folge $(1/n)$ siehe auch Aufgabe 6.53. Dass wir so etwas wie Division durch null einfach unter den Tisch kehren, liegt daran, dass wir in diesem Kapitel nur daran interessiert sein werden, was „am Ende“ der Folge passiert. Trotzdem darf man natürlich nicht durch null teilen.

Für reelle oder komplexe Folgen wird der Abstand zweier Zahlen bekanntlich durch den Absolutbetrag ihrer Differenz berechnet. Daher kann man für solche Folgen die Definition auch so lesen, dass für alle $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ existieren muss, so dass $|a_n - a| < \varepsilon$ für alle $n \geq n_0$ gilt.

harmonische Folge

Wir schauen uns ein Beispiel an: Die reelle Folge $(1/n)$, die man übrigens *harmonische Folge* nennt,[2] konvergiert gegen 0. Die Begründung dafür liefert Korollar 16.3. Das besagt nämlich, dass es zu jedem vorgegebenem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}^+$ mit $1/n_0 < \varepsilon$ gibt. Für alle n mit $n \geq n_0$ gilt dann $|1/n - 0| = 1/n \leq 1/n_0 < \varepsilon$.

Dass der Abstand spätestens ab einem bestimmten Index n_0 kleiner als ε sein soll, bedeutet, dass höchstens für die Indizes $0, 1, \ldots, n_0 - 1$ der Abstand *nicht* kleiner als ε ist. Es gibt also „nur“ endlich viele Ausnahmen im Vergleich zu den unendlich vielen Folgengliedern, für die die Aussage gilt.[3] Das kann man präzisieren und kommt dadurch zu einem Begriff, der das Konzept der Konvergenz evtl. etwas anschaulicher beschreibt.

Definition

Ist M eine unendliche Menge und P eine Eigenschaft, die Elemente von M haben oder nicht haben können,[4] dann sagt man, dass **fast alle** Elemente von M die Eigenschaft P haben, wenn die Menge $\{m \in M : \neg P(m)\}$ der „Ausnahmen“ endlich ist. Entsprechend sagt man, dass **fast alle** Glieder einer Folge (a_n) die Eigenschaft P haben, wenn es nur endlich viele Indizes $k \in \mathbb{N}$ gibt, für die $P(a_k)$ nicht gilt.

Aufgabe 19.1. Welche der folgenden Aussagen sind wahr?

(i) Fast alle natürlichen Zahlen sind größer als 999 999 999.
(ii) Fast alle natürlichen Zahlen sind gerade.
(iii) Fast alle natürlichen Zahlen sind zusammengesetzte Zahlen.
(iv) Fast alle Glieder der Folge $(\lfloor n/100 \rfloor)$ sind positiv.

Mit dieser Sprechweise kann man Konvergenz auch so formulieren:

Lemma 19.1

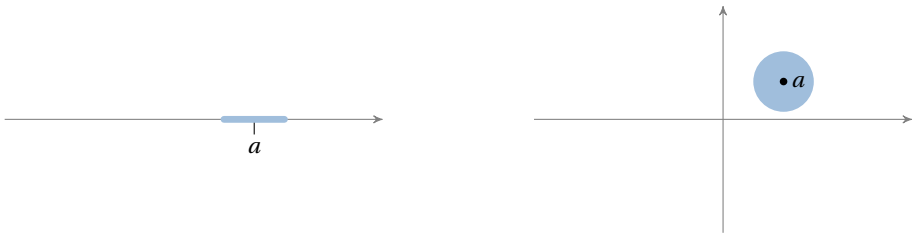
Eine Folge (a_n) konvergiert genau dann gegen a, wenn für alle $\varepsilon > 0$ fast alle Folgenglieder in $U_\varepsilon(a)$ liegen.

Für reelle Folgen heißt Konvergenz gegen a anschaulich, dass in *jedem* offenen Intervall, in dessen Mitte a liegt, auch fast alle Folgenglieder liegen. Für komplexe Zahlen gilt das entsprechend für jede offene Kreisscheibe mit Mittelpunkt a.

[2] Das hat etwas mit der Harmonik in der Musik zu tun, weil die Wellenlängen der Obertöne eines Grundtons 1/2, 1/3 und so weiter sind.

[3] Die Anführungszeichen stehen dort, weil die Menge der Ausnahmen ggf. riesengroß sein kann. Es könnte beispielsweise mehr Ausnahmen geben als es Atome im Universum gibt. Trotzdem wäre das eine verschwindend geringe Minderheit gegenüber den unendlich vielen Elementen, die keine Ausnahmen sind.

[4] Formal ist P also eine Aussageform $P(x)$, in die man für x Elemente von M einsetzen kann.



Aufgabe 19.2. Konvergiert die Folge (42) gegen 42? (Mit dieser Folge ist die Funktion gemeint, die jeder natürlichen Zahl den Funktionswert 42 zuordnet.)

Aufgabe 19.3. Konvergiert die Folge $((-1)^n)$ gegen 1, gegen -1 oder gegen 1 *und* -1?

Lemma 19.2

Wenn eine Folge (a_n) in X gegen a und gegen b konvergiert, dann gilt $a = b$.

Beweis. Würde $a \neq b$ gelten, dann müsste wegen der positiven Definitheit von Metriken $d(a,b)$ positiv sein. Nennen wir diesen Abstand ε. Wegen der Konvergenz gegen a liegen fast alle Folgenglieder in $U_{\varepsilon/2}(a)$. Wegen der Konvergenz gegen b liegen aber auch fast alle Folgenglieder in $U_{\varepsilon/2}(b)$. Das ist aber offensichtlich ein Widerspruch, weil diese beiden Umgebungen disjunkt sind. ■

Aufgabe 19.4. Warum sind $U_{\varepsilon/2}(a)$ und $U_{\varepsilon/2}(b)$ im Beweis von Lemma 19.2 disjunkt?

Wegen dieser Eindeutigkeitsaussage ergibt die folgende Definition Sinn.

Definition

Konvergiert die Folge (a_n) gegen a, so nennt man a den **Grenzwert** oder **Limes** der Folge und schreibt $a = \lim_{n\to\infty} a_n$ oder $a_n \overset{n\to\infty}{\longrightarrow} a$ oder einfach nur $a_n \to a$, wenn durch den Kontext klar wird, was gemeint ist. So eine Folge nennt man **konvergent**. Folgen, die nicht konvergent sind, nennt man **divergent**.

0 ist also z. B. der Grenzwert von $(1/n)$ bzw. $\lim_{n\to\infty} 1/n = 0$. Folgen mit dem Grenzwert 0 nennt man übrigens auch *Nullfolgen*. Dieser Begriff ist natürlich nur sinnvoll in metrischen Räumen wie $\mathbb{R}$ oder $\mathbb{C}$, in denen es eine Null gibt.

Nullfolge

Aufgabe 19.5. Wie sehen die konvergenten Folgen in einem Raum mit der diskreten Metrik aus?

Definition

Eine Folge in einem metrischen Raum nennen wir **beschränkt**, wenn ihr Wertebereich beschränkt ist.

Lemma 19.3

Jede konvergente Folge ist beschränkt.

Beweis. Sei (a_n) eine Folge, die gegen a konvergiert. Dann gibt es ein $n_0 \in \mathbb{N}$, so dass $a_n \in U_1(a)$ für alle $n \geq n_0$ gilt. Nach Aufgabe 11.3 hat die endliche Menge

$\{d(a_n,a) : n < n_0\}$ ein Maximum m. Mit $m' = \max\{m+1,1\}$ gilt dann $a_n \in U_{m'}(a)$ für alle $n \in \mathbb{N}$. ■

Aufgabe 19.6. Begründen Sie mit einem Gegenbeispiel, dass die Umkehrung von Lemma 19.3 nicht gilt, dass es also eine beschränkte Folge gibt, die nicht konvergiert.

In der folgenden Aussage geht es um Summen, Differenzen, Produkte und Quotienten von Folgen. (Erinnern Sie sich an die Definition auf Seite 87, die natürlich auch für komplexe Zahlen Sinn ergibt. $(a_n + b_n)$ ist z. B. die Summe der Funktionen (a_n) und (b_n).)

Lemma 19.4

Seien (a_n) und (b_n) konvergente komplexe Zahlenfolgen mit den Grenzwerten a und b. Dann konvergieren auch die Folgen $(a_n + b_n)$, $(a_n - b_n)$ und $(a_n \cdot b_n)$, und zwar gegen $a+b$, $a-b$ und ab. Gilt $b \neq 0$, dann konvergiert auch (a_n/b_n), und zwar gegen a/b.

Beweis. Zunächst zur Summe $(a_n + b_n)$. Sei $\varepsilon > 0$ vorgegeben. Weil (a_n) und (b_n) konvergieren, gibt es natürliche Zahlen n_a und n_b mit $|a_n - a| < \varepsilon/2$ für alle $n \geq n_a$ und $|b_n - b| < \varepsilon/2$ für alle $n \geq n_b$. Setzt man $n_0 = \max\{n_a, n_b\}$, dann gilt mit der Dreiecksungleichung

$$|(a_n + b_n) - (a+b)| \leq |a_n - a| + |b_n + b| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

für alle $n \geq n_0$. Für die Differenz verläuft der Beweis völlig analog, wobei man lediglich die „Dreiecksungleichung für Differenzen“, also Korollar 17.4, verwendet.

Nun zum Produkt $(a_n b_n)$. Nach Lemma 19.3 gibt es eine Schranke $C > 0$ mit $|a_n| \leq C$ für alle $n \in \mathbb{N}$. Ist nun $\varepsilon > 0$ vorgegeben, so findet man wie eben ein $n_0 \in \mathbb{N}$ mit $|a_n - a| < \varepsilon/(2|b|)$ und $|b_n - b| < \varepsilon/(2C)$ für alle $n \geq n_0$. Damit folgt für solche n

$$\begin{aligned} |a_n b_n - ab| &= |a_n b_n - a_n b + a_n b - ab| = |a_n(b_n - b) + (a_n - a)b| \\ &\leq |a_n| \cdot |b_n - b| + |a_n - a| \cdot |b| < C \cdot \varepsilon/(2C) + \varepsilon/(2|b|) \cdot |b| = \varepsilon. \end{aligned}$$

Für den Quotienten ist zunächst zu beachten, dass die Sache nur funktioniert, wenn b nicht verschwindet. Dann gibt es nach Definition der Konvergenz ein n_1 mit $|b_n - b| < |b|/2$ für alle $n \geq n_1$. Insbesondere heißt das $|b_n| > |b|/2$ und damit $b_n \neq 0$ für alle $n \geq n_1$. Man kann also (spätestens ab $n = n_1$) gefahrlos durch b_n dividieren. Man muss nun nur noch zeigen, dass $(1/b_n)$ gegen $1/b$ konvergiert. Der Rest folgt dann durch Multiplikation mit der Folge (a_n). Dazu wähle man sich zu vorgegebenem $\varepsilon > 0$ ein n_2 mit $|b_n - b| < \varepsilon \cdot |b|^2/2$ für alle $n \geq n_2$. Für alle $n \geq \max\{n_1, n_2\}$ gilt dann

$$\left|\frac{1}{b_n} - \frac{1}{b}\right| = \left|\frac{b - b_n}{b b_n}\right| = \frac{|b - b_n|}{|b| \cdot |b_n|} < \frac{\varepsilon \cdot |b|^2/2}{|b|^2/2} = \varepsilon.$$ ■

Aufgabe 19.7. Begründen Sie mit Lemma 19.4, dass für eine konstante Zahl λ die Folge (λa_n) gegen λa konvergiert, wenn (a_n) gegen a konvergiert.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Aufgabe 19.8. Wieso folgt im Beweis von Lemma 19.4 $|b_n| > |b|/2$ aus $|b_n - b| < |b|/2$?

Damit können wir nun einige weitere Beispiele für Grenzwerte angeben:

- Eine Folge wie $(\mathrm{i} + 1/n)$ ist die Summe der konstanten Folge (i) (die nach Aufgabe 19.2 gegen i geht) und der harmonischen Folge, von der wir wissen, dass sie eine Nullfolge ist. Die Summe hat daher den Grenzwert $\mathrm{i} + 0 = \mathrm{i}$.
- Die Folge $(1/n^2)$ kann man als Produkt der harmonischen Folge mit sich selbst betrachten und daher ist ihr Grenzwert $0 \cdot 0 = 0$. Offenbar gilt allgemein $1/n^k \to 0$ für alle $k \in \mathbb{N}^+$; man muss zur Begründung dasselbe Argument einfach mehrfach anwenden.
- Für die Folge $\big((2n+5)/(3n+2)\big)$ kann man einen „Trick“ anwenden: man multipliziert Zähler und Nenner mit $1/n$. (Das ist legitimes Erweitern von Brüchen und nur problematisch für den uninteressanten Fall $n = 0$.) Mit Anwendung der obigen Rechenregeln erhält man

$$\frac{2n+5}{3n+2} = \frac{2n+5}{3n+2} \cdot \frac{1/n}{1/n} = \frac{2+5/n}{3+2/n} \longrightarrow \frac{2+5\cdot 0}{3+2\cdot 0} = \frac{2}{3}.$$

  Dabei ist zu beachten, dass wir die Regel für den Quotienten nur anwenden durften, weil der Nenner nicht gegen null konvergierte.

Aufgabe 19.9. Berechnen Sie die Grenzwerte der Folgen

$$\big((\mathrm{i}/n)^3\big), \quad \left(\frac{3n^2+5n-10}{3-4n-6n^2}\right) \quad \text{und} \quad \left(\frac{3n^2+5n-10}{3-4n-6n^3}\right).$$

Aufgabe 19.10. Welchen Wert muss $a \in \mathbb{R}$ haben, damit die Folge

$$\left(\frac{3+4n+5n^2+6n^3}{10-7n+an^3}\right)_{n\in\mathbb{N}}$$

den Grenzwert 42 hat?

Die beiden folgenden Lemmata sind recht unscheinbar, aber bei der Ermittlung von Grenzwerten oft hilfreich.

Lemma 19.5

Majorantenkriterium für Folgen
Seien (a_n) eine komplexe Nullfolge und (b_n) irgendeine komplexe Folge. Gibt es eine komplexe Zahl b mit $|b - b_n| \le |a_n|$ für fast alle $n \in \mathbb{N}$, dann konvergiert (b_n) gegen b.

Beweis. Sei $\varepsilon > 0$ vorgegeben. Dazu gibt es nach Voraussetzung ein $n_0 \in \mathbb{N}$ mit $|a_n| = |a_n - 0| < \varepsilon$ für alle $n \ge n_0$. Für solche n folgt sofort $|b - b_n| \le |a_n| < \varepsilon$. ∎

Mithilfe des Majorantenkriteriums kann man zeigen, dass $\big((-1/n)^n\big)$ eine Nullfolge ist, indem man $b_n = (-1/n)$ und $a_n = 1/n$ nimmt. Dieses Beispiel ist deshalb anders als alle bisherigen, weil die Folgenwerte ständig das Vorzeichen wechseln

und mal auf der einen, mal auf der anderen Seite des Grenzwertes liegen. Der Pfeil in der Grenzwertschreibweise sollte also nicht so verstanden werden, dass die Folgenglieder sich dem Grenzwert in einer bestimmten Richtung nähern müssen. Siehe dazu auch Aufgabe 19.11.

Aufgabe 19.11. Geben Sie den Grenzwert von $\big((\mathrm{i}/n)^n\big)$ an und beschreiben Sie das geometrische Verhalten der Folgenglieder.

Lemma 19.6 Seien (a_n) und (b_n) konvergente reelle Folgen, für die $a_n \le b_n$ für fast alle $n \in \mathbb{N}$ gilt. Dann gilt $\lim_{n\to\infty} a_n \le \lim_{n\to\infty} b_n$.

Beweis. Wir nennen die Grenzwerte a und b. Gilt *nicht* $a \le b$, dann muss $a > b$ wegen der Trichotomie von $<$ gelten. Insbesondere ist $\varepsilon = a - b$ dann positiv und es liegen fast alle Folgenglieder von (b_n) in $I_b = (b - \varepsilon/2, b + \varepsilon/2)$ und fast alle Folgenglieder von (a_n) in $I_a = (a - \varepsilon/2, a + \varepsilon/2)$. Da aber alle Elemente von I_b kleiner als alle von I_a sind, ist das ein Widerspruch zur Voraussetzung. ■

Aufgabe 19.12. Begründen Sie mit einem Gegenbeispiel, dass man in Lemma 19.6 nicht $\le$ an beiden Stellen durch $<$ ersetzen kann.

Aufgabe 19.13. Begründen Sie mithilfe von Lemma 19.6 die folgende Aussage: Konvergiert eine Folge von positiven reellen Zahlen, dann ist ihr Grenzwert nicht negativ.

Wir haben in den vorherigen Kapiteln schon öfter die Wurzelfunktion verwendet und diese auch als Beispiel dafür angeführt, dass die rationalen Zahlen „Lücken“ aufweisen. Nun können wir beweisen, dass es in den (nichtnegativen) reellen Zahlen Wurzeln tatsächlich immer gibt.[5]

Satz 19.7 Ist y eine nichtnegative reelle Zahl und $n \in \mathbb{N}^+$, dann gibt es eine eindeutig bestimmte nichtnegative reelle Zahl x mit $x^n = y$.

Beweis. Wir können $y > 0$ voraussetzen, denn für $y = 0$ ist die Aussage trivial. Die Eindeutigkeit ist einfach zu begründen: Sind $x_1, x_2 \in [0, \infty)$ zwei verschiedene Zahlen, dann gilt o. B. d. A. $x_1 > x_2$ und damit $x_1^n > x_2^n$ wegen (ii) aus Lemma 15.3.

Um die Existenz zu beweisen, definieren wir $M = \{r \in \mathbb{R} : r \ge 0 \wedge r^n \le y\}$. Sicher gilt $M \neq 0$, denn 0 ist ein Element von M, und zwar sogar das Minimum von M. Außerdem ist M offensichtlich ein Intervall. Auch das folgt aus Lemma 15.3 bzw. der Tatsache, dass $\mathbb{R}$ ein angeordneter Körper ist. Ferner ist M beschränkt, denn für $y > 1$ gilt $r^n > y$ für $r > y$ und für $y \le 1$ gilt $r^n > y$ für $r > 1$; also ist $\max\{y, 1\}$ eine obere Schranke für M. Weil $\mathbb{R}$ sogar ein vollständig angeordneter Körper ist, existiert $x = \sup M$ und sicher gilt $x > 0$.

Wir betrachten nun die Folgen $(x - 1/k)_{k\in\mathbb{N}}$ und $(x + 1/k)_{k\in\mathbb{N}}$, die offenbar beide gegen x konvergieren. Außerdem sind fast alle Folgenglieder der ersten Folge

[5] In Abschnitt 17 haben wir gesehen, dass das deswegen auch für alle komplexen Zahlen gilt.

Elemente von M und alle Folgenglieder der zweiten Folge positiv und nicht in M enthalten. Damit folgt

$$y \le \lim_{k\to\infty} (x+1/k)^n = \big(\lim_{k\to\infty} (x+1/k)\big)^n = x^n$$
$$= \big(\lim_{k\to\infty} (x-1/k)\big)^n = \lim_{k\to\infty} (x-1/k)^n \le y$$

aus den Rechenregeln (Lemma 19.4) für Grenzwerte. ■

⋆**Aufgabe 19.14**. Wieso ist im Beweis von Satz 19.7 klar, dass das Supremum x von M positiv ist?

Definition

Die eindeutig bestimmte Zahl x aus Satz 19.7 nennt man die **n-te Wurzel** von y und schreibt dafür $\sqrt[n]{y}$. $\sqrt[2]{y}$ nennt man auch die **Quadratwurzel** von y und schreibt dafür kurz $\sqrt{y}$.

Damit wir eine Funktion erhalten, ist es wichtig, dass der Ausdruck $\sqrt[n]{y}$ durch diese Definition eindeutig bestimmt ist.[6] $\sqrt{4}$ ist z. B. 2 und *nicht* -2 oder so etwas wie „± 2“ (obwohl das Quadrat von -2 natürlich 4 ist). Außerdem kann man die Gleichung $x^n = y$ zwar auch für negative y lösen, wenn n ungerade ist (beispielsweise gilt $(-3)^3 = -27$), aber man verwendet die Wurzelschreibweise in der Regel nur für nichtnegative y.

Insbesondere für Folgen kann man eine bestimmte Beweistechnik oft einsetzen, deren Korrektheit wir nun begründen.

Satz 19.8

Vollständige Induktion
Ist P eine Eigenschaft, die natürliche Zahlen haben oder nicht haben können, und gilt einerseits $P(0)$ und andererseits $P(n) \Rightarrow P(n+1)$ für alle $n \in \mathbb{N}$, dann gilt $P(n)$ für alle $n \in \mathbb{N}$.

Beweis. Wenn $P(n)$ *nicht* für alle $n \in \mathbb{N}$ gilt, dann ist die Menge $M = \{n \in \mathbb{N} : \neg P(n)\}$ nicht leer und hat daher nach Satz 11.1 ein kleinstes Element m. m kann wegen $P(0)$ nicht null sein, es muss also $m > 0$ gelten. Nach Definition von M gilt dann aber $P(m-1)$ und nach der Voraussetzung des Satzes würde $P(m)$, also $m \notin M$ folgen. ■

Induktionsanfang
Induktionsschritt
Induktionsvoraussetzung

In Beweisen, die das Prinzip der vollständigen Induktion aus Satz 19.8 verwenden, bezeichnet man $P(0)$ als den *Induktionsanfang* und die Implikation $P(n) \Rightarrow P(n+1)$ als den *Induktionsschritt* oder *Induktionsschluss*, wobei der vordere Teil $P(n)$ als *Induktionsvoraussetzung* bezeichnet wird.

Als erstes Beispiel beweisen wir, dass $5^n + 3$ für alle $n \in \mathbb{N}$ ein Vielfaches von 4 ist. Die Aussageform $P(n)$ ist in diesem Fall also $4 \mid 5^n + 3$. Der Induktionsanfang $P(0)$ ist die Aussage, dass 4 ein Teiler von $5^0 + 3 = 4$ ist, und das stimmt offensichtlich.

[6] Wir hatten das Thema bereits auf Seite 178.

Im Induktionsschritt müssen wir zeigen, dass 4 ein Teiler von $5^{n+1}+3$ ist, *wenn* 4 ein Teiler von 5^n+3 ist. Dafür zerlegen wir den Term in der Form

$$5^{n+1}+3 = 5\cdot 5^n+3 = (4+1)\cdot 5^n+3 = 4\cdot 5^n+(5^n+3).$$

Nun haben wir es mit einer Summe zu tun und der erste Summand $4\cdot 5^n$ ist wegen des Faktors 4 offensichtlich durch 4 teilbar, während der zweite Term 5^n+3 *nach Induktionsvoraussetzung* durch 4 teilbar ist. Daher ist auch die Summe durch 4 teilbar. Das war's.

Aufgabe 19.15. Dass $4 \mid 5^n+3$ für alle $n\in\mathbb{N}$ gilt, hätte man auch mit modularer Arithmetik beweisen können. Machen Sie das bitte.

Aufgabe 19.16. Beweisen Sie mit vollständiger Induktion, dass die sogenannte gaußsche Summenformel

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

für alle $n\in\mathbb{N}$ gilt.

⋆**Aufgabe 19.17**. Im Beweis von Satz 19.7 (und nicht nur dort) wird etwas behauptet, das man eigentlich mit vollständiger Induktion beweisen müsste. Sehen Sie, was gemeint ist?

⋆**Aufgabe 19.18**. Das Prinzip der vollständigen Induktion lässt sich noch allgemeiner formulieren: Gilt

$$\forall m\in\mathbb{N}\,(m<n \Rightarrow P(m)) \;\Rightarrow\; P(n) \tag{19.1}$$

für alle $n\in\mathbb{N}$, dann gilt $P(n)$ für alle $n\in\mathbb{N}$. Können Sie das mithilfe der Wohlordnung der natürlichen Zahlen begründen? Und warum ist diese Formulierung allgemeiner als die von Satz 19.8?

Aufgabe 19.19. Vollständige Induktion lässt sich auch dann anwenden, wenn man für eine Eigenschaft P beweisen will, dass $P(n)$ nur für alle n ab einer Zahl $k\in\mathbb{N}$ gilt. Dafür wendet man Satz 19.8 einfach auf die Aussageform $P(k+n)$ statt auf $P(n)$ an. Der Induktionsanfang ist dann $P(k)$ und im Induktionsschritt müssen wir zeigen, dass $P(n+1)$ aus $P(n)$ für alle $n\geq k$ folgt.[7]

Benutzen Sie diese Technik, um zu beweisen, dass $2^n > n^2$ für alle $n>4$ gilt.

Aufgabe 19.20. Ein gerne verwendetes Beispiel an dieser Stelle ist der folgende „Beweis“ per vollständiger Induktion, dass alle Katzen dieselbe Augenfarbe haben: Wir zeigen für alle positiven natürlichen Zahlen n, dass in jeder beliebigen Menge von n Katzen alle dieselbe Augenfarbe haben. Für $n=1$ (Induktionsanfang) ist das klar. Wenn wir es nun mit einer Menge M von $n+1$ Katzen zu tun haben, dann greifen wir uns eine Katze $k_1\in M$ heraus und betrachten die Menge $M' = M\setminus\{k_1\}$. Nach Induktionsvoraussetzung haben alle Katzen in M' dieselbe Augenfarbe. Anschließend greifen wir uns eine Katze $k_2\in M'$ heraus und betrachten die Menge $\{k_1,k_2\}$. Nach Induktionsvoraussetzung haben auch k_1 und k_2 dieselbe Augenfarbe. Also hat k_1 dieselbe Augenfarbe wie k_2 und damit wie die Katzen in M'. Ergo haben alle Katzen in M dieselbe Augenfarbe. Wo ist der Denkfehler?

[7] Verwenden wir Aufgabe 19.18, dann müssen wir zeigen, dass $P(n)$ für $n\geq k$ folgt, wenn $P(m)$ für alle $m\in\mathbb{N}$ mit $k\leq m<n$ gilt.

Die folgende Abschätzung ist hilfreich, wenn man Potenzen „loswerden“ will.

Bernoullische Ungleichung **Satz 19.9**
Für alle $x \geq -1$ und alle $n \in \mathbb{N}$ gilt $(1+x)^n \geq 1+nx$.

Beweis. Für ein festes $x \geq -1$ beweisen wir die Aussage mit vollständiger Induktion über n. Für $n = 0$ (Induktionsanfang) gilt sie offensichtlich. Gehen wir für den Induktionsschritt nun also davon aus, dass sie für n gilt. Es folgt

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x) \geq (1+nx)(1+x) = 1+(n+1)x+nx^2\\ &\geq 1+(n+1)x.\end{aligned}$$

Man beachte dabei, dass die erste Ungleichung in dieser Kette nach Induktionsvoraussetzung gilt, dass das aber nur funktioniert, weil der Faktor $1+x$ nach Voraussetzung nicht negativ ist. Die zweite Ungleichung ist korrekt, weil der Ausdruck nx^2 wegen des Quadrats nie negativ ist. ■

Aufgabe 19.21. Schreiben Sie formal korrekt (als Aussageform) auf, was im Beweis von Satz 19.9 die Eigenschaft $P(n)$ ist, die wir mit vollständiger Induktion beweisen.

In den beiden folgenden Lemmata werden zwei sehr wichtige Klassen von Folgen mit ihren Grenzwerten vorgestellt. Die sollten Sie auf jeden Fall kennen.

Geometrische Folge[8] **Lemma 19.10**
Für $q \in \mathbb{C}$ mit $|q| < 1$ gilt $\lim_{n\to\infty} q^n = 0$.

Beweis. Weil $1/|q|$ größer als 1 ist, ist $1/|q|-1$ größer als 0 und wir dürfen die bernoullische Ungleichung anwenden:

$$\left(\frac{1}{|q|}\right)^n = \left(1+\frac{1}{|q|}-1\right)^n = \left(1+\frac{1-|q|}{|q|}\right)^n \geq 1+n\left(\frac{1-|q|}{|q|}\right) = \frac{|q|+n(1-|q|)}{|q|}$$

Durch Bilden der Kehrwerte erhält man:

$$|q|^n \leq \frac{|q|}{|q|+n(1-|q|)} \leq \frac{|q|}{n(1-|q|)} = \frac{|q|}{1-|q|}\cdot\frac{1}{n}$$

Nun steht aber rechts die harmonische Folge multipliziert mit einem konstanten Faktor, also eine Nullfolge. (Siehe Aufgabe 19.7.) Nach dem Majorantenkriterium steht links daher auch eine Nullfolge. ■

Aufgabe 19.22. Finden Sie den Beweis dafür, dass die geometrische Folge eine Nullfolge ist, umständlich? Ist es nicht *klar*, dass eine Folge wie $\left((3/5)^n\right)$ gegen null geht, weil jedes Folgenglied kleiner als das vorherige ist? (Man nimmt in jedem Schritt 40 % vom vorherigen Wert weg.) Geben Sie ein Beispiel für eine Folge von positiven Zahlen an, bei der jedes Folgenglied kleiner als das vorherige ist, obwohl die Folge *nicht* gegen null geht.

[8] Diese Folge heißt so, weil jedes Folgenglied das *geometrische Mittel* seiner beiden Nachbarn ist. Warum man wiederum diesen Mittelwert *geometrisch* nennt, wird in dem verlinkten Wikipedia-Artikel anhand von Beispielen ganz gut erklärt.

Lemma 19.11 Für $k \in \mathbb{N}$ und $b \in (1,\infty)$ ist (n^k/b^n) eine Nullfolge.

Beweis. Offensichtlich geht die Folge $\big((n+1)/n\big)$ gegen 1 und damit geht nach den Rechenregeln für Grenzwerte auch $\big((n+1)^k/n^k\big)$ gegen 1. Deshalb gibt es ein $n_0 \in \mathbb{N}$, so dass alle $(n+1)^k/n^k < b$ für alle $n \geq n_0$ gilt. Mit $q_n = (n+1)^k/(bn^k)$ gilt also $q_n \leq q_{n_0} < 1$ für alle $n \geq n_0$. Wir setzen $C = q_1 \cdot q_2 \cdot \dots \cdot q_{n_0-1}/b$.

Sei nun $\varepsilon > 0$ vorgegeben. Da die geometrische Folge $(q_{n_0}^m)_{m\in\mathbb{N}}$ nach Lemma 19.10 gegen null konvergiert, gibt es ein $m_0 \in \mathbb{N}$, so dass $q_{n_0}^m < \varepsilon/C$ für alle $m \geq m_0$ gilt. Für $n \geq n_0 + m_0$ (und damit $n - n_0 \geq m_0$) folgt dann

$$\begin{aligned}\frac{n^k}{b^n} &= \frac{1^k}{b} \cdot \frac{2^k}{b\cdot 1^k} \cdot \frac{3^k}{b\cdot 2^k} \cdot \dots \cdot \frac{(n-1)^k}{b(n-2)^k} \cdot \frac{n^k}{b(n-1)^k} \\ &= \frac{1}{b} \cdot q_1 \cdot q_2 \cdot \dots \cdot q_{n_0-1} \cdot q_{n_0} \cdot q_{n_0+1} \cdot \dots \cdot q_{n-2} \cdot q_{n-1} \\ &= C \cdot q_{n_0} \cdot q_{n_0+1} \cdot \dots \cdot q_{n-2} \cdot q_{n-1} \leq C \cdot q_{n_0}^{n-n_0} < \varepsilon.\end{aligned}$$

■

Lemma 19.11 besagt, dass ein Exponentialterm der Form b^n immer schneller wächst als irgendein Polynom in n. Das werden wir auch in Abschnitt 20 wieder brauchen.

Rekursion

Folgen werden häufig *rekursiv* definiert. Damit ist gemeint, dass man den Startwert der Folge vorgibt und sich die weiteren Folgenglieder dadurch ergeben, dass eine bestimmte Rechenvorschrift (allgemeiner: eine Funktion) auf den Vorgänger angewandt wird. Ein einfaches, wenn auch nicht besonders spannendes Beispiel erhält man durch $a_0 = 1$ und $a_{n+1} = (n+1)a_n$. Damit hat man $a_1 = 1\cdot 1 = 1$, $a_2 = 2\cdot 1 = 2$, $a_3 = 3\cdot 2 = 6$ und so weiter. Es ergibt sich also $a_n = n!$ und das hätte man auch ohne Rekusion gleich so hinschreiben können. Wir werden aber noch interessantere Beispiele kennenlernen.

> **Aufgabe 19.23**. Wie kann man die Folge, die rekursiv durch $a_0 = 1$ und $a_{n+1} = a_n/3$ definiert ist, kürzer hinschreiben?

Der guten Ordnung halber wollen wir festhalten, dass man so etwas überhaupt machen darf. Dafür definieren wir in Anlehnung an die Schreibweise $[n]$ aus dem Abschnitt über Permutationen

$[n]_0$

$$[n]_0 = \{k \in \mathbb{N} : k < n\} = \{0,\dots,n-1\} = \{k-1 : k \in [n]\}.$$

für $n \in \mathbb{N}$. Man beachte, dass $[0]_0$ die leere Menge ist und allgemein $|[n]_0| = n$ gilt.

Satz 19.12 Sei M irgendeine Menge und F eine Funktion von

$$\bigcup\{M^{[n]_0} : n \in \mathbb{N}\}$$

nach M. Dann gibt es genau eine Funktion f von $\mathbb{N}$ nach M (also eine Folge in M) mit der Eigenschaft, dass $f(n) = F(f|_{[n]_0})$ für alle $n \in \mathbb{N}$ gilt.

Beweis. Der Beweis ist im Prinzip nicht schwer, aber für sein Verständnis ist wesentlich, dass man mit den verwendeten Notationen und Begriffen umgehen kann, die alle in Kapitel III eingeführt wurden.

Dass es nur eine Funktion mit dieser Eigenschaft geben kann, folgt wie üblich: Gäbe es zwei verschiedene, z. B. f_1 und f_2, dann gäbe es eine kleinste natürliche Zahl n mit $f_1(n) \neq f_2(n)$. Wegen der Minimalität von n folgt dann jedoch $f_1|_{[n]_0} = f_2|_{[n]_0}$ und damit der Widerspruch $f_1(n) = F(f_1|_{[n]_0}) = F(f_2|_{[n]_0}) = f_2(n)$.

Man zeigt nun mit vollständiger Induktion, dass es für alle $n \in \mathbb{N}$ genau eine Funktion f_n von $[n+1]_0$ nach M mit der Eigenschaft $f_n(k) = F(f_n|_{[k]_0})$ für alle $k \in [n+1]_0$ gibt: Im Induktionsanfang ist f_0 durch die Forderung $f_0(0) = F(\emptyset)$ eindeutig festgelegt. Für den Induktionsschluss definiert man f_{n+1} durch $f_n \cup \{(n+1, F(f_n))\}$. Dass diese Festlegung alternativlos ist, begründet man wie im letzten Absatz.

Da nach Konstruktion immer $f_n \subseteq f_{n+1}$ gilt, ist $f = \bigcup_{n\in\mathbb{N}} f_n$ offenbar eine Funktion von $\mathbb{N}$ nach M mit den gewünschten Eigenschaften. ■

Die folgende Aussage liefert eine vereinfachte Version dieses Satzes, die für viele Fälle ausreichend ist.

Korollar 19.13

Sei M eine Menge, x ein Element von M und h eine Funktion von M nach M. Dann ist durch die Eigenschaften $a_0 = x$ sowie $a_{n+1} = h(a_n)$ für alle $n \in \mathbb{N}$ eindeutig eine Folge (a_n) in M bestimmt.

Beweis. Definiert man F durch $F(\emptyset) = x$ und $F(g) = h(g(n))$ für alle $g \in M^{[n+1]_0}$, so kann man Satz 19.12 anwenden und erhält dadurch eine Funktion f. Mit $a_n = f(n)$ gilt dann

$$a_0 = f(0) = F(f|_{[0]_0}) = F(\emptyset) = x \quad \text{und}$$
$$a_{n+1} = f(n+1) = F(f|_{[n+1]_0}) = h(f(n)) = h(a_n).$$ ■

⋆**Aufgabe 19.24**. Beweisen Sie die Eindeutigkeitsaussage aus Korollar 19.13 mithilfe des Prinzips der vollständigen Induktion.

Hier noch zwei etwas interessantere Beispiele für rekursive Definitionen:

- Die berühmte *Fibonacci-Folge* wird definiert durch $a_0 = 0$, $a_1 = 1$ sowie $a_{n+2} = a_n + a_{n+1}$ für alle $n \in \mathbb{N}$. Hier werden also immer zwei Vorgänger für die Berechnung des nächsten Wertes benötigt.
- Ähnlich wie im Beweis des Satzes von Euklid definieren wir $p_0 = 2$ und p_{n+1} für $n \in \mathbb{N}$ als den kleinsten Primteiler von $1 + p_0 \cdot p_1 \cdot \dots \cdot p_n$. In diesem Fall braucht man für die Ermittlung des nächsten Folgenglieds sogar *alle* bisher berechneten Folgenwerte.

Aufgabe 19.25. Geben Sie für die Fibonacci-Folge a_6 und a_7 an.

Aufgabe 19.26. Geben Sie p_4 für das Beispiel nach der Fibonacci-Folge an.

Aufgabe 19.27. Wie müsste die Funktion h aus Korollar 19.13 aussehen, um die Folge a_n aus Aufgabe 19.23 zu erhalten? Und wie müsste h für das Beispiel vor dieser Aufgabe ($a_n = n!$) aussehen?

Aufgabe 19.28. Wie müsste die Funktion F aus Satz 19.12 aussehen, um die Fibonacci-Folge bzw. das Beispiel danach – also die Folge (p_n) – zu erhalten?

Aufgabe 19.29. Wir definieren rekursiv $b_0 = 1$, $b_1 = 3$ und $b_{n+2} = (b_n + b_{n+1}) \bmod 5$ für alle $n \in \mathbb{N}$. Geben Sie b_{13} an.

⋆**Aufgabe 19.30**. Wäre es auch zu einer periodischen Wiederholung gekommen, wenn wir in Aufgabe 19.29 als Anfangswerte irgendwelche anderen ganzen Zahlen b_0 und b_1 genommen hätten? Wenn Ihre Antwort *ja* ist, dann begründen Sie sie. Wenn Ihre Antwort *nein* ist, geben Sie ein konkretes Gegenbeispiel an.

Wäre dies ein Skript für ein Studium der Mathematik, dann müsste die Reihenfolge der behandelten Themen eine andere sein, weil man in so einem Fall darauf achtet, nur Dinge zu verwenden, die vorher bereits definiert bzw. bewiesen wurden. Das geschieht hier aus didaktischen Gründen nicht immer. Wir haben aber nun zumindest das gesamte Handwerkszeug zusammen, um nachträglich das bekannte Schulwissen über Potenzen und Wurzeln zusammenzufassen und zu begründen, wieso das alles seine Richtigkeit hat. Würde man ganz sauber vorgehen, dann liefe es folgendermaßen ab:

(i) Man definiert zunächst rekursiv für alle $x \in \mathbb{R}$ und alle $n \in \mathbb{N}$, was x^n bedeuten soll: x^0 ist immer 1 und x^{n+1} steht für $x^n \cdot x$. Das führt zu der üblichen Bedeutung, die wir kennen: x^n ist eine Abkürzung für

$$\underbrace{x \cdot x \cdot \dots \cdot x}_{n\text{-mal}}.$$

(ii) Dann setzt man fest, dass x^{-n} für den Kehrwert von x^n steht, wenn n eine positive natürliche Zahl ist und x nicht verschwindet.

(iii) Für $x \geq 0$ definiert man im nächsten Schritt $x^{1/n}$ als die n-te Wurzel von x für $n \in \mathbb{N}^+$.

(iv) Und schließlich setzt man, ebenfalls für $x \geq 0$, fest, dass $x^{p/q}$ für $(x^{1/q})^p$ stehen soll, wenn p und q ganze Zahlen mit $q \neq 0$ sind.[9]

Damit ist der Ausdruck x^r für alle rationalen Exponenten definiert,[10] wenn x eine nichtnegative reelle Zahl ist. Man kann nun u. a. die folgenden Rechenregeln beweisen, die wie gesagt aus der Schule bekannt sein sollten, hier aber noch einmal zusammengefasst werden:

[9] Dabei muss man sich überlegen, dass dieser Ausdruck *wohldefiniert* ist, weil es mehr als eine Darstellung für den Bruch p/q gibt. Siehe Seite 141.

[10] Beachten Sie, dass wir noch nicht wissen, was x^r bedeuten soll, wenn r irrational ist. Dazu kommen wir später.

Lemma 19.14

Für alle $a, b \in [0,\infty)$ und alle $r, s \in \mathbb{Q}$ gelten die folgenden Aussagen:

(i) $a^r \cdot a^s = a^{r+s}$
(ii) $a^r / a^s = a^{r-s}$ für $a \neq 0$
(iii) $a^r \cdot b^r = (ab)^r$
(iv) $a^r / b^r = (a/b)^r$ für $b \neq 0$
(v) $(a^r)^s = a^{rs}$

Beweis. Der Beweis besteht aus vielen kleinen Schritten, die hier nicht alle vorgeführt werden sollen. Am Anfang überzeugt man sich beispielsweise mittels vollständiger Induktion, dass (i), (iii) und (v) für natürliche Zahlen r und s gelten. Dann zeigt man, dass alle fünf Regeln auch für negative Exponenten gelten. Und so hangelt man sich nach und nach durch. ■

Daraus ergeben sich sofort entsprechende Folgerungen für Wurzeln.

Korollar 19.15

Für alle $a, b \in [0,\infty)$ und alle $m, n \in \mathbb{N}^+$ gelten die folgenden Aussagen:

(i) $\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab}$
(ii) $\sqrt[n]{a} / \sqrt[n]{b} = \sqrt[n]{a/b}$ für $b \neq 0$
(iii) $\sqrt[n]{\sqrt[m]{a}} = \sqrt[mn]{a}$

Aufgabe 19.31. Wieso folgen die Regeln in Korollar 19.15 direkt aus denen in Lemma 19.14?

Aufgabe 19.32. Nach Lemma 19.14 gilt $\sqrt{a^2} = (a^2)^{1/2} = a^{2\cdot 1/2} = a^1 = a$. Geben Sie eine reelle Zahl a an, für die $\sqrt{a^2} = a$ *nicht* gilt. Wieso ist das kein Widerspruch?

Aufgabe 19.33. Berechnen Sie den Grenzwert der Folge $\big((4^{n+1} + 2^n)/(4^n + 2^{2n})\big)$. Wenden Sie dabei einen ähnlichen „Trick“ wie in Aufgabe 19.9 an.

Lemma 19.16

Sei $a > 0$.[11] Dann gilt $\sqrt[n]{a} \to 1$.

Beweis. Wir gehen zunächst von $a \geq 1$ aus. Mit $x_n = \sqrt[n]{a}$ gilt dann $x_n - 1 \geq 0$ und wir können die bernoullische Ungleichung anwenden:

$$a = x_n^n = (1 + x_n - 1)^n \geq 1 + n(x_n - 1)$$

Durch Umformen dieser Ungleichung erhält man $x_n - 1 \leq (a-1)/n$, also geht $(x_n - 1)$ nach Lemma 19.6 gegen 0 und (x_n) daher nach dem Majorantenkriterium gegen 1. Für $a < 1$ gilt nun $\sqrt[n]{1/a} \to 1$ und der Rest folgt mit den Rechenregeln für Wurzeln und Grenzwerte. ■

[11] Dies ist vielleicht eine gute Gelegenheit, noch einmal an Fußnote 18 von Seite 172 zu erinnern: Durch die Angabe $a > 0$ ist implizit klar, dass a reell sein muss.

Aufgabe 19.34. Berechnen Sie den Grenzwert der Folge $\left(\sqrt[n]{2^{n+1}}\right)$.

Aufgabe 19.35. In Wolfram Alpha kann man sich mit Eingaben wie

```
limit of (3n^3+2n-100)/(n^2-5n^3) as n to infinity
```

Grenzwerte berechnen lassen. Das kann man verwenden, um sich selbst Aufgaben zu stellen oder eigene Lösungen zu überprüfen. Man sollte nur jeweils zuerst nachschauen, ob das System die Eingabe so verstanden hat, wie sie intendiert war.

Definition

Sei (a_n) eine reelle Folge. Wenn es für alle $C > 0$ ein $n_0 \in \mathbb{N}$ mit $a_n \geq C$ für alle $n \geq n_0$ gibt, dann sagt man, dass die Folge **bestimmt gegen ∞ divergiert**. Man sagt ferner, dass eine reelle Folge (b_n) **bestimmt gegen $-\infty$ divergiert**, wenn $(-b_n)$ bestimmt gegen ∞ divergiert.

Wenn (a_n) bestimmt gegen ∞ divergiert, dann verwendet man Schreibweisen wie $\lim_{n\to\infty} a_n = \infty$ oder $a_n \to \infty$ und sagt auch manchmal, dass die Folge *gegen* ∞ *geht*. Dabei darf jedoch nicht vergessen werden, dass erstens ∞ *keine* reelle Zahl ist und dass zweitens so eine Folge *nicht* konvergiert und ∞ *kein* Grenzwert ist.

Das Standardbeispiel für eine Folge, die gegen ∞ divergiert, ist nach dem archimedischen Axiom die Folge (n). Und offensichtlich gilt das auch für Folgen wie (n^2) oder (2^n). Die Gültigkeit der folgenden Aussage sollte hoffentlich klar sein.

Lemma 19.17

Sei (a_n) eine reelle Folge, die bestimmt divergiert. Dann ist diese Folge unbeschränkt und $(1/a_n)$ ist eine Nullfolge.

Aufgabe 19.36. Geben Sie ein Beispiel für eine reelle Nullfolge (a_n) an, für die $(1/a_n)$ *nicht* bestimmt divergiert.[12]

⋆ Rekursion im Computer

Rekursion ist auch beim Programmieren eine wichtige Technik, mit der sich komplexe Algorithmen häufig klarer und kürzer formulieren lassen. Das Beispiel mit der Fakultät würde in PYTHON so aussehen:

```
def fact(n):
    if n==0:
        return 1
    return n*fact(n-1)
```

Oder in einer Zeile so:

```
fact = lambda n: 1 if n==0 else n*fact(n-1)
```

Die beiden anderen Beispiele könnte man folgendermaßen programmieren:

[12] $(1/a_n)$ soll definiert sein, d. h. fast alle Folgenglieder von (a_n) müssen von null verschieden sein.

```
fibo = lambda n: n if n<2 else fibo(n-2)+fibo(n-1)

from sympy import factorint
from math import prod
def p(n):
    if n == 0:
        return 2
    return min(factorint(1+prod(p(k) for k in range(n))).keys())
```

Rekursiv programmierte Algorithmen können jedoch aufgrund des höheren „Verwaltungsaufwands“ durch Funktionsaufrufe auch langsamer als ihre iterativen Gegenstücke sein. Partielle Abhilfe verschaffen Compiler, die sogenannte Endrekursionen automatisch erkennen und auflösen. Ein Beispiel dafür ist die Programmiersprache SCHEME.

Eine weitere Möglichkeit, rekursive Algorithmen zu beschleunigen, ist *Memoisation*. Für die Funktion p von oben könnte das so aussehen:

```
from sympy import factorint as fi
from math import prod

def p(n, memo={0:2}):
    if n in memo:
        return memo[n]
    return min(fi(1+prod(p(k,memo) for k in range(n))).keys())
```

20. Die Landau-Notation

In diesem kurzen Abschnitt führen wir eine Schreibweise ein, die in der Informatik häufig benutzt wird, um die Komplexität von Algorithmen zu beschreiben. Sie ist benannt nach dem deutschen Mathematiker Edmund Landau (obwohl sie eigentlich von Landaus Landsmann Paul Bachmann eingeführt wurde).

Definition

Ist f eine Folge reeller Zahlen, so definieren wir

$$\mathcal{O}(f) = \{g \in \mathbb{R}^{\mathbb{N}} : \text{Es gibt ein } C > 0 \text{ mit } |g(n)| \le C|f(n)| \text{ für fast alle } n \in \mathbb{N}\}.$$

Gilt $g \in \mathcal{O}(f)$, so sagt man, dass g **von der Ordnung** f oder auch **„groß-Oh“ von** f ist.[13]

In der Informatik sind die Folgen, für die diese Notation verwendet wird, in der Regel solche, die bestimmt gegen ∞ konvergieren, z. B. (2^n). Gilt $g \in \mathcal{O}(f)$, so heißt das, dass g *nicht wesentlich stärker anwächst* als f, denn es gibt ja eine feste Zahl C, für die fast immer $g(n) \le Cf(n)$ gilt. Die Folgenglieder von g sind also bis auf

[13] Im Englischen spricht man deshalb auch von der *big O notation*. Im Original war eigentlich ein Omikron gemeint, aber im Druck ist der Unterschied in der Regel nicht zu erkennen.

endlich viele Ausnahmen höchstens C-mal so groß wie die von f zum selben Index. Entsprechend bedeutet $g \notin \mathcal{O}(f)$, dass g deutlich schneller wächst als f.

Konvention

Wenn wir in diesem Abschnitt Schreibweisen wie n^2 verwenden, dann sind damit häufig die entsprechenden Folgen gemeint. Statt $3n^2 \in \mathcal{O}(n^2)$ müsste man eigentlich $(3n^2)_{n\in\mathbb{N}} \in \mathcal{O}\big((n^2)_{n\in\mathbb{N}}\big)$ schreiben, aber das wäre natürlich sehr umständlich.

Das Beispiel $3n^2 \in \mathcal{O}(n^2)$ ist korrekt, denn wir können hier $C = 3$ wählen. Andererseits gilt auch $n^2 \in \mathcal{O}(3n^2)$, weil wir in diesem Fall $C = 1/3$ verwenden können. Der Sinn der Landau-Notation ist allerdings das Vereinfachen der Terme bzw. das Weglassen „unwichtiger“ Anteile. Daher ist die erste Variante, bei der der Faktor 3 „entfernt“ wurde, die typische Verwendung dieser Schreibweise.

Satz 20.1

Seien $f_1, f_2, g_1, g_2 \in \mathbb{R}^{\mathbb{N}}$ mit $g_i \in \mathcal{O}(f_i)$ für $i = 1, 2$. Dann gilt:

(i) $\lambda g_1 \in \mathcal{O}(f_1)$ für $\lambda \in \mathbb{R}$

(ii) $g_1 + g_2 \in \mathcal{O}(f_1)$, wenn $|f_2(n)| \le |f_1(n)|$ für fast alle $n \in \mathbb{N}$ gilt.

(iii) $g_1 g_2 \in \mathcal{O}(f_1 f_2)$

(iv) $\mathcal{O}(g_1) \subseteq \mathcal{O}(f_1)$

Beweis. Nach Voraussetzung gibt es für $i = 1, 2$ ein $C_i > 0$ mit $|g_i(n)| \le C_i |f_i(n)|$ für fast alle $n \in \mathbb{N}$. Sicher gilt dann $|\lambda g_1(n)| \le |\lambda| C_1 |f_1(n)|$ für fast alle n und damit ist die erste Aussage bereits bewiesen. Und wenn $|f_2(n)| \le |f_1(n)|$ für fast alle n gilt, dann gilt

$$\begin{aligned} |g_1(n) + g_2(n)| &\le |g_1(n)| + |g_2(n)| \le C_1 |f_1(n)| + C_2 |f_2(n)| \\ &\le C_1 |f_1(n)| + C_2 f_1|(n)| \le (C_1 + C_2) |f_1(n)| \end{aligned}$$

für fast alle n. Die dritte Aussage folgt mit

$$|g_1(n) g_2(n)| = |g_1(n)||g_2(n)| \le C_1 |f_1(n)| \cdot C_2 |f_2(n)| = C_1 C_2 |f_1(n) f_2(n)|.$$

Für die vierte Aussage sei $h \in \mathcal{O}(g_1)$ und dazu $C > 0$ mit $|h(n)| \le C|g_1(n)|$ für fast alle n. Dann folgt natürlich $|h(n)| \le C C_1 |f_1(n)|$. ■

Lemma 20.2

Sind f und g Folgen von reellen Zahlen und ist $\big(g(n)/f(n)\big)$ definiert[14] und konvergent, dann gilt $g \in \mathcal{O}(f)$. Ist diese Folge sogar eine Nullfolge, dann gilt $f \notin \mathcal{O}(g)$.

Beweis. Nach Lemma 19.3 ist $\big(g(n)/f(n)\big)$ beschränkt, d. h., es gibt ein $C > 0$ mit $|g(n)/f(n)| \le C$ und damit $|g(n)| \le C|f(n)|$ für fast alle $n \in \mathbb{N}$.

[14] Damit ist gemeint, dass fast alle Folgenglieder von f von null verschieden sind, damit nicht zu oft durch null dividiert wird.

Konvergiert die Folge $\big(g(n)/f(n)\big)$ gegen null, dann gilt für alle positiven Zahlen C die Ungleichung $|g(n)/f(n)| < 1/C$ für fast alle $n \in \mathbb{N}$. Daher kann $|f(n)| \le C|g(n)|$ *nicht* für fast alle $n \in \mathbb{N}$ gelten, denn das ist die Negation dieser Ungleichung. ■

Lemma 20.3

Seien $k, m \in \mathbb{N}$ und $a, b \in (1, \infty)$. Dann gilt:

(i) Aus $k < m$ folgt $\mathcal{O}(n^k) \subset \mathcal{O}(n^m)$.

(ii) Aus $a < b$ folgt $\mathcal{O}(a^n) \subset \mathcal{O}(b^n)$.

(iii) $\mathcal{O}(n^k) \subset \mathcal{O}(a^n)$

Beweis. Wir verwenden jeweils die „Nullfolgen-Version“ von Lemma 20.2. (n^k/n^m), also (n^{k-m}), ist als Potenz der harmonischen Folge eine Nullfolge – siehe Seite 195. (a^n/b^n), also $\big((a/b)^n\big)$ ist als geometrische Folge eine Nullfolge. Und (n^k/a^n) ist nach Lemma 19.11 eine Nullfolge. ■

Mit den obigen Aussagen ergibt sich z. B. $5 \in \mathcal{O}(n^2)$ wegen $5 = 5 \cdot n^0$ und $-2n \in \mathcal{O}(n^2)$ und $8n^2 \in \mathcal{O}(n^2)$ sowie schließlich $8n^2 - 2n + 5 \in \mathcal{O}(n^2)$ für die Summe. Wie oben bereits angedeutet ist es der „Job“ der Landau-Notation, die für das asymptotische Wachstumsverhalten „unwichtigen“ Anteile zu entfernen. Mathematisch wäre natürlich auch $8n^2 - 2n + 5 \in \mathcal{O}(n^3)$ korrekt, aber in den Anwendungen ist man immer an einer möglichst „scharfen“ Schranke interessiert.

Lemma 20.3 beschreibt die wesentlichen „Stufen“, die in der Informatik eine Rolle spielen. Außer denen und deren Beziehungen untereinander, braucht man manchmal noch eine weitere, die wir jetzt noch nicht beweisen können, die hier aber der Vollständigkeit halber schon einmal erwähnt sein soll: Es gilt $\mathcal{O}(\log_a n) \subset \mathcal{O}(n)$ für alle $a > 0$. Da außerdem $\mathcal{O}(\log_a n) = \mathcal{O}(\log_b n)$ für alle $a, b > 0$ gilt, schreibt man in der Regel einfach $\mathcal{O}(\log n)$.

Aufgabe 20.1. Welche der folgenden Aussagen sind wahr?

(i) $2^{n+42} \in \mathcal{O}(3^n)$

(ii) $3^n \in \mathcal{O}(2^{n+42})$

(iii) $n^2 2^n \in \mathcal{O}(2^n)$

(iv) $n^2 2^n \in \mathcal{O}(3^n)$

(v) $(2^n)^2 \in \mathcal{O}(2^n)$

(vi) $n \log n \in \mathcal{O}(n^2)$

In Fachtexten findet man übrigens häufig Ausdrücke wie $n^2 + 5n + 2 = \mathcal{O}(n^2)$, d. h., statt $\in$ wird $=$ verwendet. Das ist leider didaktisch sehr unglücklich, weil es sich *nicht* um eine Gleichung handelt. Wenn Sie so etwas lesen, dann sollten Sie es im Geiste immer in die korrekte Schreibweise aus diesem Abschnitt „übersetzen“.

⋆ Die Landau-Notation im Computer

Die in diesem Skript bereits erwähnte Bibliothek SymPy „versteht“ auch die Landau-Notation. Details entnehmen Sie bitte der Dokumentation.

```
from sympy import *
n = symbols("n")

O(8*n**2-2*n+5,(n,oo))
2**(n+42) in O(3**n,(n,oo))
```

21. Reihen

Reihen sind so etwas wie „unendliche Summen“, allerdings kann man den Begriff der Summe nicht ohne Weiteres auf unendlich viele Summanden erweitern. Zur Erinnerung wiederholen wir zunächst die Schreibweise für endliche Summen, die aus der Schule bekannt sein sollte.

Definition

Wir definieren rekursiv, wofür der Ausdruck $\sum_{k=m}^{n} a_k$ steht, wenn m und n ganze Zahlen sind und a_k wie bei Folgen ein von k abhängende komplexe Zahl sein soll: $\sum_{k=m}^{n} a_k$ soll null sein, wenn $n < m$ gilt. Anderenfalls soll $\sum_{k=m}^{n} a_k$ den Wert $a_n + \sum_{k=m}^{n-1} a_k$ haben.

$\sum_{k=m}^{n} a_k$ steht also für

$$a_m + a_{m+1} + a_{m+2} + \cdots + a_n,$$

wobei die obige Definition im Gegensatz zu der mit Auslassungspunkten unmissverständlich ist.

Beachten Sie, dass k als sogenannte *Laufvariable* gebunden (siehe Fußnote 15 auf Seite 19) und daher in gewissem Sinne bedeutungslos ist. Der Wert $\sum_{k=m}^{n} a_k$ ändert sich nicht, wenn man stattdessen $\sum_{i=m}^{n} a_i$ schreibt.

Zur Schreibweise ist außerdem zu sagen, dass nach wie vor „Punkt- vor Strichrechnung“ gilt, so dass man bei einem Ausdruck wie $\sum_{i=2}^{8}(5i)$ die Klammern in der Regel weglassen wird, weil die Multiplikation $5i$ eine höhere Priorität als die Summe hat. Bei $\sum_{i=2}^{8}(i+5)$ gilt das jedoch nicht, weil man diese Summe ohne Klammern für $5 + \sum_{i=2}^{8} i$ halten könnte.

Aufgabe 21.1. Geben Sie den Wert $\sum_{k=3}^{5} k^2$ an. Gehen Sie dabei zur Wiederholung der Technik der Rekursion explizit nach der obigen Definition vor.

Aufgabe 21.2. Geben Sie die Summen

$$s_1 = 4 + 8 + 12 + 16 + \cdots + 404,$$
$$s_2 = 10 + 13 + 16 + 19 + \cdots + 3001,$$
$$s_3 = 1 + 1/4 + 1/9 + 1/16 + 1/25 + \cdots + 1/121,$$
$$s_4 = 1 - 2 + 3 - 4 + 5 - 6 + \cdots + 41 - 42 \quad \text{und}$$
$$s_5 = na_6 + na_9 + na_{12} + \cdots + na_{99}$$

mithilfe der eben eingeführten Schreibweise an.

Da es sich um ganz normale Addition handelt, kann man bekannte Rechenregeln anwenden, zum Beispiel die im nächsten Lemma zusammengefassten.

Lemma 21.1

Für endliche Summen gelten die folgenden Rechenregeln.

$$\sum_{k=m}^{n}(a_k \pm b_k) = \Big(\sum_{k=m}^{n} a_k\Big) \pm \sum_{k=m}^{n} b_k$$

$$\sum_{k=m}^{n} \lambda a_k = \lambda \sum_{k=m}^{n} a_k \qquad \text{für } \lambda \in \mathbb{C}$$

$$\sum_{k=m}^{n} a_k = \Big(\sum_{k=0}^{n} a_k\Big) - \sum_{k=0}^{m-1} a_k \qquad \text{für } n \geq m \geq 0$$

$$\sum_{k=m}^{n} a_k = \sum_{k=0}^{n-m} a_{k+m}$$

Aufgabe 21.3. Machen Sie sich anhand von Beispielen klar, was die Regeln in Lemma 21.1 besagen und warum sie korrekt sind.

Aufgabe 21.4. Begründen Sie mit einem einfachen Gegenbeispiel, dass die erste Regel aus Lemma 21.1 für die Multiplikation nicht stimmt, dass

$$\sum_{k=m}^{n} a_k b_k = \Big(\sum_{k=m}^{n} a_k\Big) \cdot \sum_{k=m}^{n} b_k$$

also im Allgemeinen *nicht* korrekt ist.

Für bestimmte regelmäßige Summen kann man sich das Addieren sparen, weil eine einfache Formel für den Wert bekannt ist. Die beiden wichtigsten sind die folgenden.

Satz 21.2

Gaußsche (bzw. arithmetische) und geometrische Summenformel
Für alle $n \in \mathbb{N}$ und alle $q \in \mathbb{C} \setminus \{1\}$ gilt:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

$$\sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$$

Beweis. Die erste Formel wurde bereits in Aufgabe 19.16 bewiesen. Für die zweite setzen wir $S = \sum_{k=0}^{n} q^k$. Dann ergibt sich

$$\begin{aligned}(q-1)S = qS - S &= \Big(\sum_{k=0}^{n} q^{k+1}\Big) - \sum_{k=0}^{n} q^k \\ &= q^{n+1} + q^n + \cdots + q^2 + q^1 - \big(q^n + q^{n-1} + \cdots + q^1 + q^0\big) \\ &= q^{n+1} - q^0 = q^{n+1} - 1.\end{aligned}$$

Dabei ergibt sich die vorletzte Gleichheit, weil q^1, q^2 und so weiter bis q^n jeweils links addiert und dann rechts wieder subtrahiert werden. Es bleiben nur zwei Terme übrig. Dividiert man nun auf beiden Seiten durch $q-1$ (was OK ist, weil nach Voraussetzung $q \neq 1$ gilt), so ist man fertig. ■

Aufgabe 21.5. Verwenden Sie Lemma 21.1 und Satz 21.2 zusammen, um die Summen $\sum_{n=5}^{20} 3n$ sowie $\sum_{n=3}^{8} 1/2^n$ zu berechnen.

Aufgabe 21.6. Schreiben Sie $40+50+60+\cdots+230$ mittels des Summenzeichens auf und berechnen Sie dann diese Summe.

Aufgabe 21.7. Geben Sie die Summe $7+10+13+16+\cdots+1000$ an.

Aufgabe 21.8. Es gibt außer den beiden in Satz 21.2 aufgeführten noch weitere Summenformeln. Wichtig ist z. B. die Faulhabersche Formel. Schauen Sie sich den verlinkten Wikipedia-Artikel an und berechnen Sie mithilfe dieser Formel die Summen $\sum_{n=1}^{8} n^2$ sowie $3^2+4^2+5^2+\cdots+30^2$.

Der Vollständigkeit halber definieren wir auch noch die analoge Schreibweise für Produkte.

Definition

Wir definieren rekursiv, wofür der Ausdruck $\prod_{k=m}^{n} a_k$ steht, wenn m und n ganze Zahlen sind und a_k wie bei Folgen ein von k abhängende komplexe Zahl sein soll: $\prod_{k=m}^{n} a_k$ soll eins sein, wenn $n < m$ gilt. Anderenfalls soll $\prod_{k=m}^{n} a_k$ den Wert $a_n \cdot \prod_{k=m}^{n-1} a_k$ haben.

$\prod_{k=1}^{n} k$ ist dann beispielsweise $n!$. Beachten Sie, dass bei Summen als „Startwert“ null genommen werden muss und bei Produkten eins – in beiden Fällen das neutrale Element der jeweiligen Operation.

Aufgabe 21.9. Berechnen Sie $\prod_{k=3}^{8} \frac{k}{k+1}$.

Aufgabe 21.10. Wie muss eine Rechenregel analog zu Lemma 21.1 für $\prod_{k=m}^{n} \lambda a_k$ aussehen, wenn $m \leq n$ gilt?

Aufgabe 21.11. Welche andere Schreibweise für $\prod_{i=1}^{k} \frac{n-i+1}{i}$ haben Sie in diesem Skript schon kennengelernt?

Jetzt können wir mit dem eigentlichen Thema beginnen: mit den „unendlichen Summen“. Zunächst sollte man sich klarmachen, dass es so etwas gar nicht gibt, wenn man es nicht definiert, weil Addition nur für zwei Summanden (und damit für endlich viele) definiert ist. Dass eine naive Herangehensweise nicht funktioniert, zeigt das folgende Beispiel:

$$1+(-1)+1+(-1)+1+(-1)+\ldots = (1-1)+(1-1)+(1-1)+\cdots = 0$$
$$1+(-1)+1+(-1)+1+(-1)+\ldots = 1-(1-1)-(1-1)-(1-1)-\cdots = 1$$
$$1+(-1)+1+(-1)+1+(-1)+\ldots = (-1)+1+(-1)+1+(-1)+1+\ldots$$

$$= -1 + (1-1) + (1-1) + (1-1) + \cdots = -1$$

Was kommt denn da nun heraus? 0, 1, -1 oder etwas ganz anderes? Es sieht jedenfalls so aus, als könne man nicht einfach „drauflos addieren“ und bekannte Regeln wie Assoziativität und Kommutativität ins Unendliche „übersetzen“.

Definition

Sei $(a_k)_{k\in\mathbb{N}}$ eine komplexe Folge und $m \in \mathbb{N}$. Für die Folge $\left(\sum_{k=m}^{n} a_k\right)_{n\in\mathbb{N}}$ schreiben wir $\sum_{k=m}^{\infty} a_k$ und sprechen von der **Reihe** mit den **Reihengliedern** a_k und den **Partialsummen** $\sum_{k=m}^{n} a_k$. Wenn die Reihe (also die Folge der Partialsummen) konvergiert, so nennt man den Grenzwert den **Wert** bzw. die **Summe** der Reihe und schreibt dafür $\sum_{k=m}^{\infty} a_k$.

$\sum_{k=m}^{\infty} a_k$ bezeichnet also einerseits die Reihe und anderseits den Wert der Reihe (wenn er existiert). Man kann somit sagen, dass $\sum_{k=m}^{\infty} a_k$ konvergiert, andererseits ergibt aber auch so etwas wie $\sum_{k=m}^{\infty} a_k = 42$ Sinn. Das ist zwar theoretisch missverständlich, aber historisch so gewachsen und führt erfahrungsgemäß kaum zu Problemen.

Eher problematisch ist anfangs für viele, dass in der Definition zwei Folgen vorkommen, die man auseinanderhalten muss. Geht es beispielsweise um $a_k = 1/2^k$, so haben wir erstens die Folge $1, 1/2, 1/4, 1/8, \ldots$ und zweitens die Folge

$$\begin{aligned} 1, \\ 1 + 1/2 &= 3/2, \\ 1 + 1/2 + 1/4 &= 7/4, \\ 1 + 1/2 + 1/4 + 1/8 &= 15/8 \quad \text{und so weiter.} \end{aligned}$$

Die Idee ist, dass $\sum_{k=0}^{\infty} = 1/2^k$ so etwas wie die „Summe“

$$1 + 1/2 + 1/4 + 1/8 + 1/16 + \cdots$$

darstellen soll, wobei die erste Folge die Folge der „Summanden“ (Reihenglieder) ist, während die zweite die der „Zwischenergebnisse“ (Partialsummen) ist. Die Begriffe stehen in Häkchen, weil es keine unendlichen Summen gibt, solange man nur Addition hat. Erst durch das Konzept der Reihe (für das man Folgen und Grenzwerte braucht) wird klar definiert, was damit gemeint sein soll.

Außerdem noch eine Klarstellung zum „Anfang“ einer Reihe:

Lemma 21.3

Sei (a_n) eine komplexe Folge und $m \in \mathbb{N}$. Die Reihe $\sum_{n=m}^{\infty} a_n$ konvergiert genau dann, wenn $\sum_{n=0}^{\infty} a_n$ konvergiert. Es gilt dann $\sum_{n=0}^{\infty} a_n = \left(\sum_{n=0}^{m-1} a_n\right) + \sum_{n=m}^{\infty} a_n$.

Das folgt direkt aus der Definition, denn die eine Reihe ist die Folge $\left(\sum_{k=m}^{n} a_k\right)$, die andere ist $\left(\sum_{k=0}^{n} a_k\right)$, d. h., die zweite Folge erhält man aus der ersten, indem man zu jedem Folgenglied $\sum_{n=0}^{m-1} a_n$ addiert. Für die Konvergenz ist dieses Addieren eines konstanten Wertes egal, für den Grenzwert natürlich nicht. Außerdem kann

man sicher den „Start“ $n = 0$ auch durch $n = 1$ oder einen anderen Wert ersetzen, wenn man das an beiden Stellen macht.

Aufgabe 21.12. Was ist mit dem Beispiel $1 + (-1) + 1 + (-1) + \ldots$ von eben? Wie würde man es als Reihe schreiben und was für ein Ergebnis bekommt man?

Bevor wir uns spezifischen Reihen zuwenden, machen wir uns zuerst ein paar allgemeine Gedanken über die Konvergenz von Reihen. Dafür müssen wir noch einmal auf Folgen eingehen.

Definition

Sei (a_n) eine Folge in einem metrischen Raum X. Ein Element $x \in X$ wird **Häufungspunkt** von (a_n) genannt, wenn die Menge $\{n \in \mathbb{N} : a_n \in U_\varepsilon(x)\}$ für alle $\varepsilon > 0$ unendlich ist.

Man beachte den Unterschied zur Definition des Grenzwerts. Bei Grenzwerten müssen *fast alle* n in der besagten Menge liegen, bei Häufungspunkten „nur“ unendlich viele. Daher hat jede konvergente Folge genau einen Häufungspunkt, nämlich ihren Grenzwert. Die Folgen $((-1)^n)$ und $((-1)^n + 1/n)$ haben jedoch beispielsweise beide zwei Häufungspunkte, nämlich 1 und -1, und die Folge (n) hat gar keinen Häufungspunkt.

Aufgabe 21.13. Denken Sie sich eine Folge aus, die genau einen Häufungspunkt hat, aber *nicht* konvergiert.

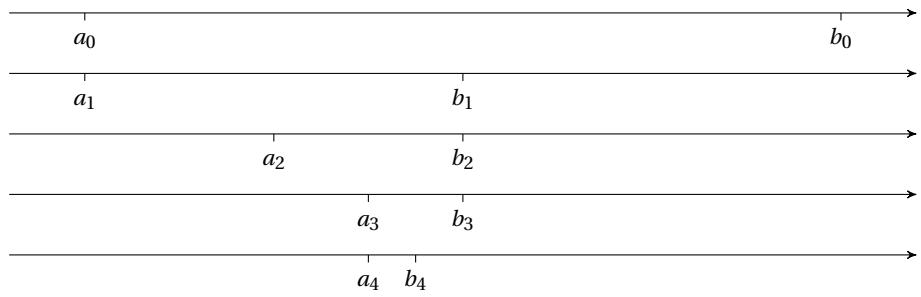
⋆**Aufgabe 21.14**. Schwere Knobelaufgabe: Denken Sie sich eine Folge aus, die unendlich viele Häufungspunkte hat. (Hinweis: Satz 16.10.)

Satz 21.4

Satz von Bolzano-Weierstraß
Jede beschränkte Folge reeller Zahlen hat einen Häufungspunkt.

Beweis. Sei (x_n) eine beschränkte Folge. Es gibt also ein Intervall $[a_0, b_0]$, in dem alle Folgenglieder liegen. Wir teilen das Intervall in der Mitte durch $c_0 = (a_0 + b_0)/2$ auf. In mindestens einer der beiden Hälften $[a_0, c_0]$ und $[c_0, b_0]$ liegen unendlich viele Folgenglieder.[15] Diese Hälfte nennen wir $[a_1, b_1]$. Dann teilen wir $[a_1, b_1]$ in zwei Hälften auf und nennen eine Hälfte, in der unendlich viele Folgenglieder liegen, $[a_2, b_2]$. Setzen wir das fort, so erhalten wir Folgen (a_n) und (b_n). Der Prozess könnte so anfangen wie in der folgenden Skizze.

[15] Die Formulierung ist hoffentlich einprägsam, allerdings etwas unpräzise. Unendlich ist die Menge der Indizes, während die Menge der Folgenglieder das nicht notwendig sein muss, z. B. im Fall einer konstanten Folge. Wenn im Folgenden von „unendlich vielen Folgengliedern“ die Rede ist, ist das immer so zu verstehen wie hier.



Weil sie in $[a_0, b_0]$ verlaufen, sind beide Folgen beschränkt. Also existieren die Zahlen $a = \sup_{n\in\mathbb{N}} a_n$ und $b = \inf_{n\in\mathbb{N}} b_n$ und es gilt $a_n \le a \le b \le b_n$ für alle $n \in \mathbb{N}$. Offenbar muss sogar $a = b$ gelten, denn sonst wäre $b_n - a_n$ für alle n größer als die positive Zahl $b - a$. Diese Zahl a ist nach Konstruktion ein Häufungspunkt der Folge. ■

Definition

Eine Folge (a_n) in einem metrischen Raum (X, d) heißt **Cauchy-Folge** oder **Fundamentalfolge**, wenn es für alle $\varepsilon > 0$ ein $k \in \mathbb{N}$ gibt, so dass $d(a_m, a_n) < \varepsilon$ für alle $m, n \ge k$ gilt.

Diese Definition hat zunächst einmal nichts mit Konvergenz zu tun. Sie klingt zwar sehr ähnlich, es kommt jedoch kein Grenzwert vor, sondern es wird lediglich gefordert, dass die Folgenwerte nach und nach immer dichter beieinander liegen. Man überlegt sich leicht, dass jede konvergente Folge eine Cauchy-Folge ist. Umgekehrt muss allerdings nicht jede Cauchy-Folge konvergieren. Ein Beispiel dafür liefert Aufgabe 16.2 für den metrischen Raum $X = \mathbb{Q}$. Es gilt aber der folgende Satz.

Satz 21.5

In den metrischen Räumen $\mathbb{R}$ und $\mathbb{C}$ konvergiert jede Cauchy-Folge.

Beweis. Sei (a_n) eine beliebige Cauchy-Folge. Man wähle ein $k \in \mathbb{N}$ derart, dass $d(a_m, a_n) < 1$ für $m, n \ge k$ gilt. Insbesondere liegen dann alle Folgenglieder ab k in $U_1(a_k)$. Da es außer diesen nur noch endlich viele weitere gibt, ist die Folge offenbar beschränkt.

Ist nun (a_n) speziell eine reelle Cauchy-Folge, so gibt es nach dem Satz von Bolzano-Weierstraß einen Häufungspunkt a. Zu vorgegebenem $\varepsilon > 0$ findet man nun einerseits ein k, so dass $|a_m - a_n| < \varepsilon/2$ für alle $m, n \ge k$ gilt, und andererseits ein $n_0 \ge k$ mit $|a - a_{n_0}| < \varepsilon/2$. ($k$ existiert, weil wir es mit einer Cauchy-Folge zu tun haben, und n_0 gibt es, weil a ein Häufungspunkt ist.) Für $n \ge k$ folgt

$$|a - a_n| \le |a - a_{n_0}| + |a_{n_0} - a_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

und damit ist a der Grenzwert der Folge.

Ist $(a_n + \mathrm{i}b_n)$ eine komplexe Cauchy-Folge, dann sind die Folgen (a_n) und (b_n) (die natürlich reell sein sollen) offenbar auch Cauchy-Folgen. Nach den vorherigen Überlegungen haben sie Grenzwerte a und b. Mit einer inzwischen üblichen Abschätzung zeigt man leicht, dass $a + \mathrm{i}b$ Grenzwert der komplexen Folge ist. ■

⋆**Aufgabe 21.15**. Vervollständigen Sie den Beweis von Satz 21.5 für komplexe Folgen.

vollständig

Satz 21.5 ist eine wichtige Aussage über $\mathbb{R}$, die daraus folgt, dass $\mathbb{R}$ vollständig angeordnet ist. Man sagt auch, dass $\mathbb{R}$ als metrischer Raum *vollständig* ist. Führt man die reellen Zahlen axiomatisch ein (siehe Fußnote 7 auf Seite 161), so wird häufig als Axiom gefordert, dass $\mathbb{R}$ ein vollständiger metrischer Raum ist.

Die folgende Aussage ist eine direkte Übersetzung von Satz 21.5 in die Sprache der Reihen. Das darauf folgende Korollar ist nichts weiter als der Spezialfall $n = m$.

Korollar 21.6

Cauchy-Kriterium
Eine Reihe[16] $\sum_{k=0}^{\infty} a_k$ konvergiert genau dann, wenn es für alle $\varepsilon > 0$ ein $N \in \mathbb{N}$ mit $|\sum_{k=m}^{n} a_k| < \varepsilon$ für alle $n \geq m \geq N$ gibt.

Korollar 21.7

Nullfolgenkriterium
Wenn $\sum_{k=0}^{\infty} a_k$ konvergiert, dann ist (a_n) eine Nullfolge.

Das Nullfolgenkriterium kann man sich anschaulich folgendermaßen klarmachen: Wenn die Reihe gegen die Zahl S konvergiert, dann liegen nach Definition der Konvergenz zu vorgegebenem $\varepsilon > 0$ fast alle Partialsummen im Intervall $(S-\varepsilon, S+\varepsilon)$. Die zugehörigen Summanden (Reihenglieder) müssen dann aber auf jeden Fall einen kleineren Betrag als 2ε haben, weil das Intervall sonst beim Übergang von einer Partialsumme s_n zur nächsten verlassen würde. Weil ε beliebig klein werden kann, müssen auch die Beträge der Summanden beliebig klein werden.[17]

harmonische Reihe

Man beachte, dass Korollar 21.7 lediglich ein notwendiges, aber kein hinreichendes Kriterium ist. Dafür schauen wir uns als wichtiges Beispiel die *harmonische Reihe* $\sum_{n=1}^{\infty} 1/n$ an. Nach einer Beweisidee von Nikolaus von Oresme aus dem 14. Jahrhundert betrachtet man dafür ausgewählte Partialsummen nach dem folgenden Muster:

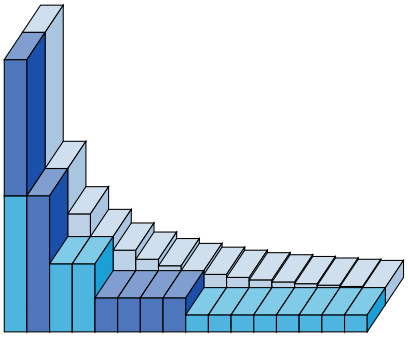
$$\sum_{k=1}^{1} \frac{1}{k} = \frac{1}{2} + \frac{1}{2} = 2 \cdot \frac{1}{2}$$
$$\sum_{k=1}^{2} \frac{1}{k} = \sum_{k=1}^{1} \frac{1}{k} + \frac{1}{2} = 3 \cdot \frac{1}{2}$$
$$\sum_{k=1}^{4} \frac{1}{k} = \sum_{k=1}^{2} \frac{1}{k} + \frac{1}{3} + \frac{1}{4} \geq 3 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} = 4 \cdot \frac{1}{2}$$

[16] Wenn hier und im Folgenden nicht explizit etwas anderes steht, sind immer komplexe Reihen gemeint.

[17] Stellen Sie sich zur Übung vor, wie die folgende Skizze im Komplexen aussehen müsste. Dort gilt das Nullfolgenkriterium ja auch.

$$\sum_{k=1}^{8}\frac{1}{k}=\sum_{k=1}^{4}\frac{1}{k}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\geq 4\cdot\frac{1}{2}+4\cdot\frac{1}{8}=5\cdot\frac{1}{2}$$
$$\sum_{k=1}^{16}\frac{1}{k}=\sum_{k=1}^{8}\frac{1}{k}+\frac{1}{9}+\frac{1}{10}+\cdots+\frac{1}{16}\geq 5\cdot\frac{1}{2}+8\cdot\frac{1}{16}=6\cdot\frac{1}{2}$$

Allgemein ist die 2^m-te Partialsumme offenbar immer mindestens so groß wie $(m+2)/2$. Daher ist die Folge der Partialsummen unbeschränkt und die Reihe konvergiert nicht, *obwohl* die Folge der Reihenglieder das Nullfolgenkriterium erfüllt!

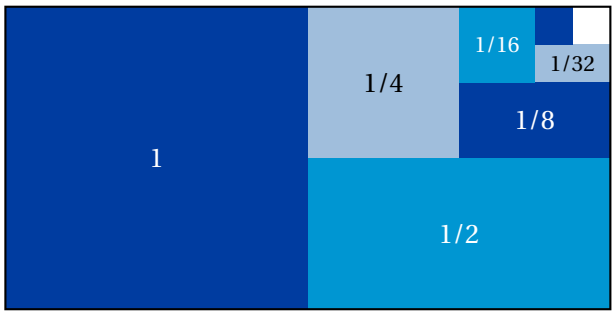


Satz 21.8

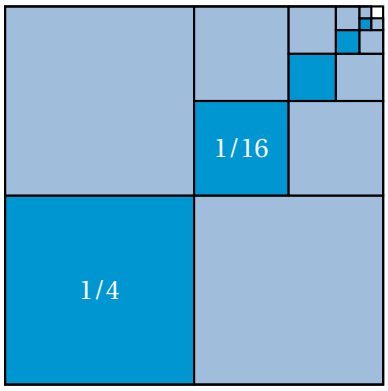
Geometrische Reihe
Sei $q\in\mathbb{C}$. Für $|q|<1$ konvergiert $\sum_{n=0}^{\infty}q^n$ gegen $(1-q)^{-1}$. Für $|q|\geq 1$ divergiert diese Reihe.

Beweis. Nach Satz 21.2 ist die Folge der Partialsummen $\big((q^{n+1}-1)/(q-1)\big)$. Da q^{n+1} nach Lemma 19.10 für $|q|<1$ eine Nullfolge ist, folgt sofort der erste Teil der Behauptung. Der zweite Teil ergibt sich aus dem Nullfolgenkriterium. ■

Für $q=1/2$ ergibt sich 2 als Reihenwert. Das kann man an der folgenden Skizze ganz gut geometrisch sehen.



Und für $q=1/4$ erhält man $\sum_{k=1}^{\infty}4^{-k}=1/3$. (Rechnen Sie es nach!) Das kann man aus der folgenden Grafik schließen, in der jeweils eines von drei gleich großen Quadraten (also ein Drittel) durch kräftiges Blau hervorgehoben ist.



Aufgabe 21.16. Wenden Sie Satz 21.8 und Lemma 21.3 an, um $\sum_{n=2}^{\infty} 3^{-n}$ zu berechnen.

Natürlich gibt es auch für Reihen ein paar Rechenregeln. Die einfachsten folgen direkt aus denen für endliche Summen.

Lemma 21.9

Seien (a_n) und (b_n) komplexe Folgen, λ eine komplexe Zahl und m eine natürliche Zahl. Dann gilt:

(i) Konvergiert $\sum_{n=m}^{\infty} a_n$ gegen a, dann konvergiert auch $\sum_{n=m}^{\infty} \lambda a_n$, und zwar gegen λa.

(ii) Konvergieren $\sum_{n=m}^{\infty} a_n$ und $\sum_{n=m}^{\infty} b_n$ gegen a bzw. b, dann konvergiert auch $\sum_{n=m}^{\infty}(a_n \pm b_n)$, und zwar gegen $a \pm b$.

Aufgabe 21.17. Den Beweis von Lemma 21.9 erspare ich mir. Es wäre für Ihr Verständnis allerdings sehr hilfreich, wenn Sie sich anhand der Definition der Reihenkonvergenz überzeugen würden, dass das Lemma korrekt ist und dass es im Wesentlichen aus Lemma 19.4 folgt.

Lemma 21.10

Die Reihe $\sum_{k=1}^{\infty}(k^2+k)^{-1}$ konvergiert gegen 1.

Beweis. Es gilt

$$\frac{1}{k^2+k} = \frac{(k+1)-k}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$$

für alle $k \in \mathbb{N}^+$ und damit erhält man mit Lemma 21.1 für die Partialsummen

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k^2+k} &= \sum_{k=1}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right) = \left(\sum_{k=1}^{n}\frac{1}{k}\right) - \sum_{k=1}^{n}\frac{1}{k+1} \\ &= \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}\right) - \left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \frac{1}{n+1}\right) \\ &= 1 - \frac{1}{n+1}\end{aligned}$$

mit dem Grenzwert 1 für $n \to \infty$. ∎

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Die beiden Reihen aus Satz 21.8 und Lemma 21.10 gehören zu den wenigen, für die man vergleichsweise einfach Grenzwerte berechnen kann. Insbesondere die geometrische Reihe spielt jedoch eine wichtige Rolle, weil man die Konvergenz vieler anderer Reihen mit ihrer Hilfe beweisen kann.

Aufgabe 21.18. Berechnen Sie

$$\sum_{n=3}^{\infty} \frac{3}{n+n^2}, \quad \sum_{n=2}^{\infty} \frac{5}{2^n} \quad \text{und} \quad \sum_{n=0}^{\infty} \frac{2\cdot 4^n + 3^{n+1}}{6^n}.$$

Definition

Ist $A \subseteq \mathbb{R}$ und $f\colon A \to \mathbb{R}$, dann nennt man f **monoton steigend**, wenn für alle $x, y \in A$ aus $x < y$ immer $f(x) \leq f(y)$ folgt. f heißt **streng monoton steigend**, wenn aus $x < y$ sogar immer $f(x) < f(y)$ folgt. Analog werden **monoton fallend** und **streng monoton fallend** definiert.

Jede Gerade der Form $x \mapsto mx+b$ ist streng monoton steigend, wenn (ihre Steigung) m positiv ist, und streng monoton fallend, wenn m negativ ist. Eine konstante Funktion wie $x \mapsto 42$ (also eine Gerade mit der Steigung 0) ist monoton steigend und fallend aber weder streng monoton steigend noch streng monoton fallend. Folgen wie (n), $(2n)$ oder (2^n) sind streng monoton steigend.

Aufgabe 21.19. Geben Sie eine Funktion an, die weder monoton steigend noch monoton fallend ist.

Aufgabe 21.20. Welche Eigenschaft aus Kapitel 6 haben alle Funktionen, die streng monoton steigen oder fallen?

Aufgabe 21.21. Formulieren Sie die Aussage von Aufgabe 11.2 mithilfe dieser neuen Begriffe.

Satz 21.11

Leibniz-Kriterium
Ist (a_n) eine monoton fallende Nullfolge,[18] so konvergiert $\sum_{n=0}^{\infty}(-1)^n a_n$.

Beweis. Für $m \leq n$ gilt immer

$$\sum_{k=m}^{n} (-1)^k a_k = (-1)^m \Big(a_m - \sum_{k=m+1}^{n} (-1)^{k-m-1} a_k \Big). \tag{21.1}$$

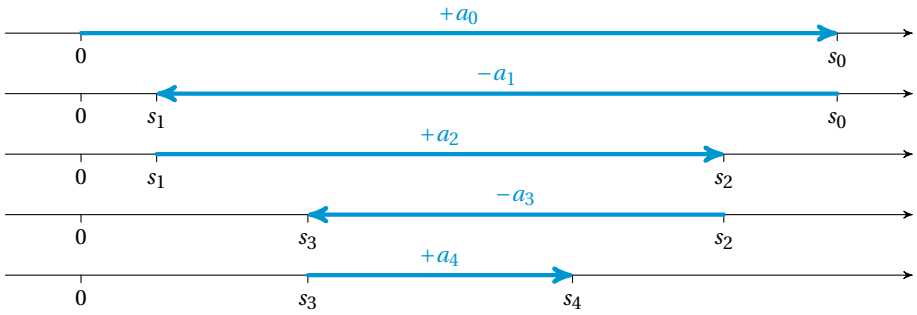
Durch vollständige Induktion über $n-m$ kann man damit zeigen, dass

$$\Big| \sum_{k=m}^{n} (-1)^k a_k \Big| \leq |a_m| \tag{21.2}$$

für alle $m \leq n$ gilt. Mit dem Cauchy-Kriterium folgt nun sofort die Behauptung, weil (a_n) eine Nullfolge ist. ■

[18] Beachten Sie, dass „monoton fallend“ für komplexe Folgen keinen Sinn ergibt. (a_n) muss eine reelle Folge sein.

Grafisch kann man sich das wie folgt vorstellen, wobei die s_k die entsprechenden Partialsummen sein sollen.



Aufgabe 21.22. Beim Beweis von Satz 21.11 muss man auf die Vorzeichen achten. Er funktioniert nur, weil alle Folgenglieder a_n nichtnegativ sind und daher in der großen Klammer in (21.1) vom nichtnegativen Wert a_m ein nichtnegativer Wert subtrahiert wird. Warum können in (a_n) keine negativen Werte vorkommen?

alternierende harmonische Reihe

Damit folgt sofort, dass die *alternierende harmonische Reihe* $\sum_{n=1}^{\infty}(-1)^{n+1}/n$ im Gegensatz zur harmonischen Reihe konvergiert.[19] Allerdings liefert uns das Leibniz-Kriterium nicht den Grenzwert. (Man kann ihn lediglich anhand der obigen Skizze eingrenzen, weil er offensichtlich immer zwischen zwei aufeinanderfolgenden Partialsummen liegt, also beispielsweise zwischen 1 und 1/2.)

Definition

Die komplexe Reihe $\sum_{n=0}^{\infty} a_n$ **konvergiert absolut**, wenn die Reihe $\sum_{n=0}^{\infty}|a_n|$ konvergiert. Eine Reihe, die konvergiert, aber nicht absolut konvergiert, wird *bedingt konvergent* genannt.

Zum Beispiel konvergiert die geometrische Reihe für $q=-1/2$ absolut, die alternierende harmonische Reihe nur bedingt. Zu beachten ist, dass man die folgende Aussage trotz der Wortwahl in der Definition tatsächlich beweisen muss!

Lemma 21.12

Wenn eine Reihe absolut konvergiert, dann konvergiert sie.

Beweis. Wegen $|\sum_{k=m}^{n} a_k| \le |\sum_{k=m}^{n}|a_k||$ (nach der Dreiecksungleichung) folgt das aus dem Cauchy-Kriterium. ■

Die (absolute) Konvergenz einer Reihe wird über die Konvergenz einer *anderen* Reihe definiert. Das wirkt seltsam. Die Definition ist jedoch sinnvoll, weil absolut konvergente Reihen viele angenehme Eigenschaften haben, die bedingt konvergente im Allgemeinen nicht haben. Hier gleich das erste Beispiel.

[19] Warum nimmt man als Exponent $n+1$ statt n? Das ist nur eine Konvention, damit das erste Reihenglied positiv ist. Ansonsten spielt das keine Rolle, weil das ja nur einer Multiplikation mit dem konstanten Faktor -1 entspricht.

Ist σ eine Permutation von $\mathbb{N}$ und konvergiert $\sum_{k=0}^{\infty} a_k$ absolut, dann konvergiert auch $\sum_{k=0}^{\infty} a_{\sigma(k)}$ absolut und hat denselben Reihenwert.

Satz 21.13

Riemannscher Umordnungssatz
Ist $\sum_{k=0}^{\infty} a_k$ eine bedingt konvergente reelle Reihe, so kann man für jede reelle Zahl S eine Permutation σ von $\mathbb{N}$ mit $\sum_{k=0}^{\infty} a_{\sigma(k)} = S$ finden.[20]

Satz 21.14

Satz 21.13 besagt also, dass für absolut konvergente Reihen die „unendliche Addition“ quasi kommutativ ist, und Satz 21.14 besagt, dass das für bedingt konvergente Reihen definitiv *nicht* der Fall ist. Diese beiden Sätzen werden hier nicht bewiesen. Das Video *Reihen, Riemannscher Umordnungssatz und komplex-analytische Funktionen* geht jedoch ausführlich auf diese Thematik ein.

Majorantenkriterium für Reihen
Ist $\sum_{k=0}^{\infty} b_k$ eine konvergente reelle Reihe (die sogenannte *Majorante*) und gilt $|a_n| \leq b_n$ für fast alle $n \in \mathbb{N}$, dann konvergiert $\sum_{k=0}^{\infty} a_k$ absolut.

Lemma 21.15

Beweis. Das folgt mit dem Cauchy-Kriterium und der Dreiecksungleichung aus

$$\left| \sum_{k=m}^{n} |a_k| \right| \leq \left| \sum_{k=m}^{n} b_k \right|$$

für $m \leq n$. ■

Wurzelkriterium
Gibt es eine Zahl $q < 1$, so dass $\sqrt[n]{|a_n|} \leq q$ für fast alle $n \in \mathbb{N}$ gilt, dann konvergiert $\sum_{k=0}^{\infty} a_k$ absolut.

Lemma 21.16

Beweis. Die Voraussetzung kann man auch als $|a_n| \leq q^n$ schreiben. Damit ist $\sum_{n=0}^{\infty} q^n$ eine Majorante und nach Lemma 21.15 und Satz 21.8 sind wir bereits fertig. ■

Quotientenkriterium
Gibt es eine Zahl $q < 1$, so dass $a_n \neq 0$ und $|a_{n+1}/a_n| \leq q$ für fast alle $n \in \mathbb{N}$ gilt, dann konvergiert $\sum_{k=0}^{\infty} a_k$ absolut.

Lemma 21.17

Beweis. O. B. d. A. gelte die Voraussetzung für *alle* $n \in \mathbb{N}$. (Siehe dazu Lemma 21.3.) Mit vollständiger Induktion zeigt man leicht, dass dann $|a_n| \leq q^n |a_0|$ für alle $n \in \mathbb{N}$. Bis auf den irrelevanten Faktor $|a_0|$ hat man nun dieselbe Situation wie im Beweis des Wurzelkriteriums. ■

[20] Und das ist auch für bestimmte Divergenz möglich, also für $S = \infty$ oder $S = -\infty$.

Die Bedingung des Wurzelkriteriums ist insbesondere dann erfüllt, wenn die Folge $\left(\sqrt[n]{|a_n|}\right)$ gegen eine Zahl konvergiert, die kleiner als 1 ist. Sie ist jedoch *nicht* durch $\sqrt[n]{|a_n|} < 1$ für fast alle $n \in \mathbb{N}$ erfüllt. Für das Quotientenkriterium und die Folge $\left(|a_{n+1}/a_n|\right)$ gilt dieselbe Anmerkung.

Aufgabe 21.23. Warum ist die Bedingung des Wurzelkriteriums erfüllt, wenn die Folge $\left(\sqrt[n]{|a_n|}\right)$ gegen eine Zahl $b < 1$ konvergiert?

Aufgabe 21.24. Geben Sie ein Beispiel für eine Reihe $\sum_{n=1}^{\infty} a_n$ an, die *nicht* konvergiert, obwohl fast immer $\sqrt[n]{|a_n|} < 1$ gilt.

Aufgabe 21.25. Wenden Sie das Wurzelkriterium auf die Reihe $\sum_{n=1}^{\infty}(1/2 - 1/n)^n$ an.

Aufgabe 21.26. Wenden Sie das Quotientenkriterium auf $\sum_{n=1}^{\infty}(3+n^2)7^{-n}$ an.

Ohne Beweis hier noch zwei Verallgemeinerungen der bereits betrachteten harmonischen Reihe, von denen man schon einmal gehört haben sollte.

allgemeine harmonische Reihe

– Die *allgemeine harmonische Reihe*

$$\sum_{k=1}^{\infty} \frac{1}{k^\alpha}$$

ist eine Verallgemeinerung der harmonischen Reihe. Sie konvergiert für $\alpha \in (1,\infty)$ und sie divergiert für $\alpha \in [0,1]$.[21] Exakte Reihenwerte können nur in speziellen Fällen angegeben werden, z. B. $\pi^2/6$ für $\alpha = 2$ oder $\pi^4/90$ für $\alpha = 4$.[22] Was es bedeutet, wenn α irrational ist, haben wir noch gar nicht geklärt. Das kommt aber noch. Lässt man für α sogar komplexe Werte zu, so erhält man die *Zeta-Funktion*, um die es in der berühmten *Riemannschen Vermutung* geht.

allgemeine alternierende harmonische Reihe

– Die *allgemeine alternierende harmonische Reihe*

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^\alpha}$$

unterscheidet sich von der vorherigen Reihe nur durch das Vorzeichen. Sie konvergiert absolut für $\alpha \in (1,\infty)$ und bedingt für $\alpha \in (0,1]$. Auch hier können Reihenwerte nur in speziellen Fällen angegeben werden, z.B. $\ln 2$ für $\alpha = 1$ oder $\pi^2/12$ für $\alpha = 2$.

Die vielleicht wichtigste Reihe überhaupt bekommt später noch ihr eigenes Kapitel.

⋆**Aufgabe 21.27**. Zeigen Sie mit dem Majorantenkriterium, dass die allgemeine harmonische Reihe $\sum_{k=1}^{\infty} k^{-2}$ konvergiert. (Hinweis: Als Majorante müssen Sie eine Reihe verwenden, von der Sie bereits vor Seite 220 wussten, dass sie konvergiert. So viele gibt es davon ja nicht.)

[21] Daran sieht man auch, dass die (spezielle) harmonische Reihe in gewissem Sinne genau an der Grenze zwischen Konvergenz und Divergenz liegt.

[22] Den Wert $\pi^2/6$ hat übrigens Leonhard Euler 1734 zum ersten Mal ermittelt, nachdem die Frage nach der Summe dieser Reihe fast hundert Jahre ungeklärt gewesen war. Diese Frage ist als *Basler Problem* bekannt geworden.

Man beachte, dass man die Konvergenz der Reihe aus Aufgabe 21.27 nicht mithilfe des Wurzel- oder Quotientenkriteriums beweisen kann. Die Folgen

$$\left(\sqrt[n]{n^{-2}}\right) \quad \text{und} \quad \left(\frac{(n+1)^{-2}}{n^{-2}}\right)$$

konvergieren beide gegen 1 und daher kann es (nach Lemma 19.6) keine Zahl $q < 1$ geben, unterhalb derer fast alle Folgenglieder liegen. Die Kriterien sind also nur hinreichende Bedingungen, aber keine notwendigen.

⋆ Summen, Produkte und Reihen im Computer

Es ist eine gute Übung, das Summenzeichen und das Produktzeichen in einfache Funktionen in einer Programmiersprache zu übersetzen. (Machen Sie das ruhig einmal!) Für die Praxis bietet PYTHON mit `sum` und `prod` allerdings bereits Funktionen für das Berechnen endlicher Summen und Produkte.

```
from math import prod

sum(k**2 for k in range(10))
prod(k for k in range(1,10))
```

Die bereits mehrfach erwähnte Bibliothek SYMPY kann auch mit Folgen und Reihen umgehen und deren Grenzwerte berechnen. Mehr dazu in *Konkrete Mathematik (nicht nur) für Informatiker* ab Kapitel 21. Und in Kapitel 18 wird gezeigt, wie man mit *Generatoren* unendliche Folgen simulieren kann.

Die Dezimaldarstellung von Zahlen

Stellenwertsystem

Durch unser Wissen über Reihen können wir an dieser Stelle noch einmal gründlich auf die inzwischen weltweit übliche Darstellung von Zahlen eingehen. Diese hat sich in Indien in den ersten Jahrhunderten nach Beginn der Zeitrechnung entwickelt und kam über den arabischen Raum nach Europa, wo sie sich erst ab dem Spätmittelalter langsam gegen die römische Zahlschrift durchsetzte. Der große Vorteil gegenüber allen früher verwendeten Methoden ist die konsequente Verwendung eines *Stellenwertsystems* inklusive der Null. Dass dabei die Zahl 10 eine besondere Rolle spielt, ist hingegen ein historischer „Zufall“.[23] Man hätte auch eine andere Zahl nehmen können.

Die Grundlagen sollten Ihnen bereits vertraut sein. Eine Zeichenfolge wie 9419 steht für

$$9419 = 9\cdot 1000 + 4\cdot 100 + 1\cdot 10 + 9\cdot 1 = 9\cdot 10^3 + 4\cdot 10^2 + 1\cdot 10^1 + 9\cdot 10^0.$$

Wir verwenden zehn verschiedene Ziffern (die Zahlzeichen 0 bis 9); die Ziffer an der n-ten Position von rechts wird mit der Zehnerpotenz 10^{n-1} multipliziert und alle Produkte werden addiert. Man nennt das ein *Stellenwertsystem*, weil der Wert einer Ziffer von der Stelle abhängt, an der sie steht.

[23] Vermutlich liegt es daran, dass Menschen zehn Finger haben.

In diesem Kapitel wird es um die Nachkommastellen gehen. Diese Ergänzung zum Dezimalsystem wurde wesentlich durch den flämischen Mathematiker Simon Stevin im 16. Jahrhundert geprägt (obwohl seine Schreibweise noch nicht die heutige war). Man schreibt dabei rechts hinter einem Trennzeichen weiter und die Werte entstehen nun durch Zehnerpotenzen mit negativen Exponenten:

$$94.19 = 9\cdot 10 + 4\cdot 1 + 1\cdot\frac{1}{10} + 9\cdot\frac{1}{100} = 9\cdot 10^1 + 4\cdot 10^0 + 1\cdot 10^{-1} + 9\cdot 10^{-2}$$

Konvention

Ab hier wird in diesem Skript als Dezimaltrennzeichen ein Punkt verwendet, obwohl in Deutschland das Komma üblicher ist.

Diese Entscheidung beruht auf ganz pragmatischen Gründen. Erstens sind Dezimalpunkte in den meisten Programmiersprachen üblich und zweitens kann es dann keine Verwechslungsgefahr mit Kommata in Mengen oder Tupeln geben. Wir werden trotzdem von Nach*komma*stellen sprechen. Offensichtlich kann man sich beim Studium dieser Stellen auf Zahlen zwischen 0 und 1 konzentrieren, weil der ganzzahlige Anteil dann uninteressant ist.

Fangen wir mit der einfachsten Variante an. Zahlen die nur endlich viele Nachkommastellen haben,[24] kann man offenbar immer als Brüche darstellen, deren Nenner eine Zehnerpotenz ist:[25]

$$\begin{aligned} 0.9419 &= \frac{9}{10} + \frac{4}{100} + \frac{1}{1000} + \frac{9}{10000} \\ &= \frac{9000}{10000} + \frac{400}{10000} + \frac{10}{10000} + \frac{9}{10000} = \frac{9419}{10000} \\ 0.445 &= \frac{455}{1000} = \frac{91}{200} \\ 0.0306 &= \frac{306}{10000} = \frac{153}{5000} \end{aligned}$$

Umgekehrt kann man für manche Brüche durch einfaches Erweitern ihre Dezimaldarstellung ermitteln:

$$\begin{aligned} \frac{3}{4} &= \frac{3\cdot 25}{4\cdot 25} = \frac{75}{100} = 0.75 \\ \frac{17}{5000} &= \frac{17\cdot 2}{5000\cdot 2} = \frac{34}{10000} = 0.0034 \end{aligned}$$

Aufgabe 21.28. Für den Fall, dass Ihnen das nicht ohnehin klar ist, sollten Sie es üben, indem Sie ein paar ausgedachte Zahlen von Hand umwandeln und dann mit einem Taschenrechner Ihre Ergebnisse überprüfen. Beachten Sie dabei insbesondere auch

[24] Wenn von endlich vielen Nachkommastellen gesprochen wird, dann ist das natürlich immer so gemeint, dass es sich um endlich viele handelt, die von null verschieden sind. Theoretisch kann man 0.5 ja auch als 0.50, 0.500000 oder $0.5\overline{0}$ schreiben.

[25] Evtl. kann man noch kürzen.

die Rolle führende Nullen wie bei den Beispielen 0.0306 und 17/5000 oben. Was passiert mit den Dezimaldarstellungen, wenn man mit Zehnerpotenzen multipliziert oder durch sie dividiert?

Damit ist aber auch klar, dass man Zahlen, die sich *nicht* in diese Form bringen lassen, nicht mit endlich vielen Nachkommastellen darstellen kann. Diese Zahlen fallen in zwei Kategorien:

- Brüche, deren Nenner in gekürzter Form außer 2 und 5 noch andere Primfaktoren hat, denn durch Erweitern wird man diese Faktoren nicht „loswerden“ und daher im Nenner keine Zehnerpotenz erhalten.
- Zahlen wie zum Beispiel $\sqrt{2}$, die gar keine Brüche sind. Zu denen kommen wir gleich.

Wie erhält man generell für beliebige Brüche die Dezimaldarstellung? Das kann man durch schriftliche Division erreichen. Analysieren wir das am Beispiel 3/7:

```
  3.0000000... : 7 = 0.4285714...
−2.8
  ---
   20
−  14
   --
    60
−   56
    --
     40
−    35
     --
      50
−     49
      --
       10
−       7
        --
        30
−       28
        --
         2
```

Die erste Nachkommastelle 4 haben wir erhalten, indem wir im Prinzip 30 durch 7 dividiert haben. Wenn wir uns nicht verrechnet haben, ist 30/7 also mindestens 4, evtl. etwas mehr (wenn es einen Rest gibt), aber weniger als 5 (denn sonst hätten wir doch einen Fehler gemacht). Da wir eine Null „geborgt“ haben, haben wir eigentlich herausbekommen, dass 3/7 mindestens 0.4 und auf jeden Fall weniger als 0.5 ist. In diesem Sinne ist 4 die „richtige“ erste Nachkommastelle. Analog sagt uns die zweite Nachkommastelle, dass 3/7 mindestens 0.42 und weniger als 0.43 ist. Und so geht es weiter. Weil dieses Vorgehen offenbar korrekt funktioniert, muss es bei Brüchen, die sich mit endlich vielen Nachkommastellen darstellen lassen, abbrechen. Das heißt, dass als Rest (das sind im Beispiel die blauen Zahlen) irgendwann null herauskommt.

Was passiert bei den anderen Brüchen? Im Beispiel kommt es zu einer Wiederholung. Ganz unten kommt der Rest 2 heraus, der weiter oben schon einmal vorkam. So eine Wiederholung *musste* sich ergeben, weil bei der Division durch 7 außer der Null nur sechs verschiedene Reste möglich sind. Und offenbar gilt das immer. Bei der Division durch 23 muss es spätestens nach 22 Divisionen zu einer Wiederholung gekommen sein und so weiter.[26] Wir können damit festhalten, dass es in der Dezimaldarstellung von rationalen Zahlen immer zu *periodischen Wiederholungen* kommen wird.[27] Die entsprechende Schreibweise mit einem Überstrich sollte Ihnen aus der Schule geläufig sein; für 3/7 ist es beispielsweise $0.\overline{428571}$.

Aber wie genau sind „unendlich viele Nachkommastellen“ zu verstehen? Als Reihe! Die Ziffer k an der n-ten Stelle hinter dem Komma steht wie im endlichen Fall für $k \cdot 10^{-n}$, aber man benötigt eine Reihe, um diese Brüche alle zu addieren. Es folgen ein paar Beispiele, die zeigen, wie das gemeint ist.

$$\begin{aligned}
0.\overline{3} &= \frac{3}{10} + \frac{3}{100} + \cdots = \sum_{n=1}^{\infty} 3 \cdot 10^{-n} = 3 \sum_{n=1}^{\infty} 10^{-n} \\
&= 3 \cdot \left(\frac{1}{1 - 1/10} - 1 \right) = 3 \cdot \frac{1}{9} = \frac{1}{3} \\
0.\overline{9} &= \frac{9}{10} + \frac{9}{100} + \cdots = \sum_{n=1}^{\infty} 9 \cdot 10^{-n} = 9 \sum_{n=1}^{\infty} 10^{-n} \\
&= 9 \cdot \left(\frac{1}{1 - 1/10} - 1 \right) = 9 \cdot \frac{1}{9} = 1 \\
0.\overline{27} &= \frac{27}{100} + \frac{27}{10000} + \cdots = \sum_{n=1}^{\infty} 27 \cdot 100^{-n} = 27 \sum_{n=1}^{\infty} 100^{-n} \\
&= 27 \cdot \left(\frac{1}{1 - 1/100} - 1 \right) = 27 \cdot \frac{1}{99} = \frac{3}{11} \\
0.0\overline{27} &= \frac{27}{1000} + \frac{27}{100000} + \cdots = \sum_{n=1}^{\infty} 27 \cdot 10^{-(2n+1)} = \frac{1}{10} \cdot \sum_{n=1}^{\infty} 27 \cdot 100^{-n} = \frac{3}{110} \\
0.4\overline{27} &= 0.4 + 0.0\overline{27} = \frac{2}{5} + \frac{3}{110} = \frac{47}{110}
\end{aligned}$$

Daran erkennt man offenbar eine allgemeine Methode, eine Zahl der Form

$$0.k_1 \ldots k_m \overline{p_1 \ldots p_n}$$

in einen Bruch umzurechnen. Der vordere Teil ist einfach die Zahl $0.k_1 \ldots k_m$ und daraus erhält man den Bruch mit dem Zähler $k_1 \ldots k_m$ und dem Nenner 10^m. Der periodische Teil hinten ist $10^{-m} \cdot 0.\overline{p_1 \ldots p_n}$ und $0.\overline{p_1 \ldots p_n}$ wiederum ist der Bruch mit dem Zähler $p_1 \ldots p_n$ und dem Nenner $10^n - 1$. Die beiden Teilergebnisse müssen dann nur noch addiert werden.

Am Beispiel $0.0012\overline{017}$ ausführlich vorgerechnet:

[26] Man kann das noch verfeinern und genauer vorhersagen, wann es zum ersten Mal passiert. Dazu gibt es ein ausführliches Video von mir.

[27] Damit der Satz auch für abbrechende Darstellungen stimmt, muss man Zahlen wie 0.32 als $0.32\overline{0}$ oder $0.31\overline{9}$ interpretieren.

– Hier haben wir $m = 4$, $k_1 \dots k_4 = 0012$, $n = 3$ und $p_1 \dots p_3 = 017$.
– Der nichtperiodische Teil ist $12/10^4 = 3/2500$.
– $0.\overline{017}$ ist $17/999$.
– $0.0000\overline{017}$ ist daher $10^{-4} \cdot 17/999 = 17/9990000$.
– Insgesamt ergibt sich $3/2500 + 17/9990000 = 2401/1998000$.

Aufgabe 21.29. Wenn Sie es noch einmal selbst probieren wollen: Geben Sie die Dezimalzahl $0.7\overline{63}$ als gekürzten Bruch an.

Aufgabe 21.30. Überprüfen Sie durch schriftliche Division, dass man für den Bruch $3/11$ tatsächlich die Dezimaldarstellung $0.\overline{27}$ erhält.

Aufgabe 21.31. Wenn Sie trotz der mathematischen Herleitung nicht so richtig „glauben“ können, dass $0.\overline{9}$ dasselbe wie 1 ist, dann schauen Sie sich das Video "Das Rätsel des Kontinuums" an.

Aufgabe 21.32. Wenn Sie den Umgang mit unendlichen Dezimaldarstellungen üben wollen, können Sie beispielsweise Wolfram Alpha verwenden, um weitere Aufgaben zu generieren. Gibt man dort etwa

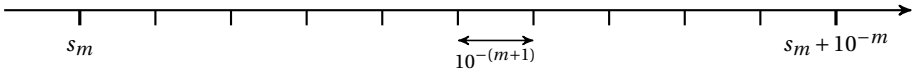
```
decimal digits of 49/660
```

ein, dann erhält man als Antwort `{{7,{4,2}},-1}`. Dabei steht der erste Teil für den nichtperiodischen Anfang, der zweite für die Periode. Hier geht es somit um die Ziffernfolge $7\overline{42}$. Die letzte Zahl gibt an, wie viele der Ziffern der Folge links vom Dezimaltrennzeichen stehen. Weil die Zahl in diesem Fall negativ ist, fängt die Sequenz erst mit einer Stelle „Verspätung“ an: es kommt also $0.07\overline{42}$ heraus.

Wie sieht es mit irrationalen Zahlen aus? Einerseits konvergiert jede Reihe der Form $\sum_{n=1}^{\infty} a_n \cdot 10^{-n}$, wobei die a_n Ziffern (also einstellige natürliche Zahlen) sind, nach dem Wurzelkriterium, denn es gilt

$$\sqrt[n]{a_n \cdot 10^{-n}} = \sqrt[n]{a_n}/10 \leq \sqrt[n]{9}/10 \leq 9/10$$

für alle $n \geq 1$. Jede endliche oder unendliche Folge von Nachkommastellen repräsentiert also eine reelle Zahl. Andererseits können wir jede reelle Zahl $r \in [0,1)$ durch eine Folge von Partialsummen der Form $s_m = \sum_{n=1}^{m} a_n \cdot 10^{-n}$ mit $a_n \in [10]_0$ annähern,[28] wobei immer $s_m \leq r < s_m + 10^{-m}$ gilt. Wie man dafür rekursiv die Folge (a_n) der Reihenglieder konstruieren müsste, wird hoffentlich durch die folgenden Skizze deutlich.



Dezimaldarstellung von Zahlen ▸ **Satz 21.18**

[28] Siehe die Definition auf Seite 200.

Ist (a_n) eine Folge von Dezimalziffern – also von Zahlen aus $[10]_0$ –, so konvergiert die Reihe $\sum_{n=1}^{\infty} a_n 10^{-n}$ gegen eine Zahl aus dem Intervall $[0,1]$, für die man

$$0.a_1 a_2 a_3 a_4 \ldots$$

schreibt. Ist umgekehrt r eine Zahl aus dem Intervall $[0,1]$, so gibt es eine Folge (a_n) von Dezimalziffern, so dass $\sum_{n=1}^{\infty} a_n 10^{-n}$ gegen r konvergiert.
Für reelle Zahlen $r \geq 1$ erhält man eine entsprechende Darstellung, indem man $\lfloor r \rfloor$ und $r - \lfloor r \rfloor$ getrennt betrachtet. Für negative Zahlen r verwendet man die Dezimaldarstellung von r mit einem Minus davor.
Eine Zahl ist genau dann rational, wenn die Ziffern in der Folge ihrer Nachkommastellen sich ab einer gewissen Stelle periodisch wiederholen. Für Zahlen, die sich in gekürzter Form als Bruch $p/q \neq 0$ darstellen lassen, wobei q außer 2 und 5 keine weiteren Primfaktoren hat, gibt es zwei verschiedene Dezimaldarstellungen.[29] Für alle anderen Zahlen ist die Dezimaldarstellung eindeutig bestimmt.

Konvention

Wenn wir in Zukunft von *der* n-ten Nachkommastelle einer Zahl sprechen und es sich um eine Zahl handelt, die zwei Darstellungen hat, dann soll immer die Darstellung mit unendlich vielen Nullen gemeint sein. Die dritte Nachkommastelle von $1/4$ ist also beispielsweise 0 und nicht 9. Durch diese Konvention sind für jede reelle Zahl die Nachkommastellen eindeutig bestimmt.

Aufgabe 21.33. Geben Sie die dritte Nachkommastelle von $10^{100}/7$ an. (Hinweis: Was passiert mit den Nachkommastellen, wenn man mit 10 oder allgemeiner mit 10^n multipliziert?)

Aufgabe 21.34. Geben Sie die dritte Nachkommastelle von $10^{5^{1000}}/7$ an. (Hinweis: Erinnern Sie sich an die modulare Arithmetik.)

Satz 21.18 gilt in entsprechend abgewandelter Form auch dann noch, wenn man statt 10 eine andere Basis wählt. Das ist insbesondere für Computer relevant, die im Dualsystem – also mit der Basis 2 – rechnen. Im Dualsystem ergibt sich beispielsweise

$$\frac{1}{10} = 0.000\overline{1100}_2 = \frac{1}{2^4} + \frac{1}{2^5} + \frac{1}{2^8} + \frac{1}{2^9} + \frac{1}{2^{12}} + \frac{1}{2^{13}} + \ldots$$

und es gibt dann noch weniger Zahlen als im Dezimalsystem, die sich mit endlich vielen Nachkommastellen darstellen lassen. (Nämlich nur die Brüche, deren Nenner in gekürzter Form eine Zweierpotenz ist.)

[29] Siehe auch Fußnote 27.

Runden und Fehlerfortpflanzung

In der Praxis rechnet man oft mit ungenauen Werten. Das kann verschiedene Gründe haben:

- Man hat Ausgangsdaten, die durch Messungen oder Schätzungen entstanden sind. Exakte Messungen von physikalischen Größen wie Länge oder Masse sind grundsätzlich unmöglich. Und bei Mengen von Objekten, die zu groß zum Erfassen aller Einzelfälle sind, kann man sich nur mit Schätzungen behelfen.
- Zahlen werden durch die Darstellung und das Rechnen im Computer ungenau. Das liegt daran, dass Computer nur ganz wenige Zahlen exakt darstellen können.[30]
- Für viele Berechnung werden numerische Verfahren eingesetzt, die nur Näherungswerte liefern. Das kann daran liegen, dass man exakte Werte gar nicht angeben kann, aber auch daran, dass die Ermittlung derselben zu aufwendig wäre.

In der Regel gibt es also einen „korrekten“ Wert x und einen Näherungswert, der sich mehr oder weniger von x unterscheiden kann. Die Anführungszeichen stehen dort, weil x typischerweise unbekannt oder nicht darstellbar ist; sonst müsste man ja nicht mit Näherungen rechnen.

Wenn die Ausgangsdaten und die Berechnung fehlerhaft sind, dann wird auch das Ergebnis nicht exakt sein. Taschenrechner, Computer und andere technische Geräte geben jedoch eine konkrete Zahl aus, die man in so einer Situation nicht kritiklos weitergeben darf. Sinnvoll wäre im Allgemeinen die Angabe von Fehlerschranken. Wir werden uns allerdings nicht ausführlich mit der sogenannten Fehlerrechnung beschäftigten. Es geht zunächst nur darum, ein Bewusstsein für „zu genaue Zahlen“ zu entwickeln.

Nehmen wir als konkretes Beispiel an, dass Sie für eine handwerkliche Arbeit die Fläche eines Kreises berechnen müssen. Sie messen als Radius 84 Zentimeter aus, geben in PYTHON

```
from math import pi

r = 0.84
pi*r**2
```

ein und erhalten als Ergebnis: `2.216707776372958`. Aber was heißt denn das? Die beiden Angaben 2.216707776372 und 2.216707776373 unterscheiden sich beispielsweise nur um einen Quadratmikrometer. Ihre Messung stimmte aber höchstwahrscheinlich nur bis auf einem Zentimeter oder maximal einen Millimeter. Daher ergibt es keinen Sinn, so viele Nachkommastellen anzugeben. Man *rundet* das Ergebnis.

[30] Ausführlich wird das in *Konkrete Mathematik (nicht nur) für Informatiker* erklärt, insbesondere in Kapitel 13 über das Format IEEE 754.

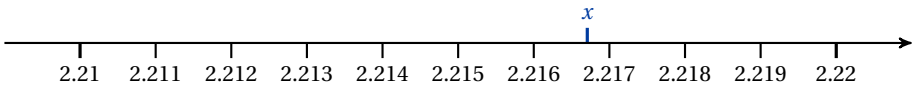
Definition

Wenn eine Zahl $x \in \mathbb{R}$ auf n Stellen nach dem Komma **gerundet** wird, dann ist damit gemeint, dass man eine Zahl $\tilde{x}$ angibt, die zwei Bedingungen erfüllt:

(i) In der Dezimaldarstellung von $\tilde{x}$ sind höchstens die ersten n Nachkommastellen von null verschieden.

(ii) Der Betrag $|\tilde{x} - x|$ der Abweichung vom richtigen Wert ist nicht größer als $5 \cdot 10^{-(n+1)}$.

Ist x die Zahl 2.216707776372958 von oben und will man auf drei Stellen nach dem Komma runden, so soll die Abweichung nicht größer als $5 \cdot 10^{-4} = 0.0005$ werden. Das ist die Hälfte des Abstands zweier Zahlen in der folgenden Skizze.



Der gerundete Wert kann also nur 2.217 sein. Offensichtlich ist durch die obige Definition der gerundete Wert nur dann nicht eindeutig bestimmt, wenn x genau zwischen zwei „Kandidaten“ liegt. Will man beispielsweise $x = 0.265$ auf zwei Stellen nach dem Komma runden, so sind sowohl 0.26 als auch 0.27 in Ordnung. Es gibt dafür jedoch zwei Konventionen:

kaufmännisches Runden

– Beim *kaufmännischen Runden* wird „nach oben“ gerundet. Im obigen Beispiel würde man sich also für 0.27 entscheiden.[31]

mathematisches Runden

– Beim *wissenschaftlichen* oder *mathematischen Runden* wird so gerundet, dass die letzte Ziffer (nach dem Runden) gerade ist. Dann käme oben 0.26 heraus.

Man beachte, dass beide Konventionen nur dann greifen, wenn es eine Wahlmöglichkeit gibt! Im ersten Beispiel kommt *immer* 2.217 heraus, egal ob man kaufmännisch oder mathematisch rundet.

Der Sinn des mathematischen Rundens, das Computer typischerweise auch intern einsetzen, ist das Vermeiden systematischer Abweichungen. Man kann sich das anhand einer Summe wie

$$0.15 + 0.25 + \cdots + 0.85 + 0.95$$

vor Augen führen. Die korrekte Summe ist 4.95. Würde man die neun Summanden vor der Addition kaufmännisch auf eine Stelle nach dem Komma runden, so käme man auf 5.4 und läge um 0.45 daneben, weil immer in dieselbe Richtung gerundet wurde. Mit mathematischem Runden kommt man auf den wesentlich besseren Wert 5.0, weil sich die Rundungsfehler größtenteils gegenseitig neutralisieren.

Aufgabe 21.35. Geben Sie den Wert von π gerundet auf drei, vier und sieben Stellen nach dem Komma an. Geben Sie den Wert von $3/80$ gerundet auf drei Stellen nach dem Komma an.

[31] Diese Regel wird im Allgemeinen nur für positive Zahlen angewendet.

Aufgabe 21.36. Warum wird man sich beim Runden von $\sqrt{2}$ niemals die Frage stellen müssen, ob man kaufmännisch oder mathematisch runden sollte?

Aufgabe 21.37. In Aufgabe 21.35 hat man gesehen, dass beispielsweise beim Runden auf drei Nachkommastellen die dritte Nachkommastelle des gerundeten Wertes nicht die dritte Nachkommastelle von π war. Geben Sie ein Beispiel für eine Zahl an, bei der nach Runden auf drei Nachkommastellen keine Nachkommastelle mehr mit dem Original übereinstimmt.

Aufgabe 21.38. Falls Sie noch nie so richtig über Runden und Näherungswerte Gedanken gemacht haben, sollten Sie sich vielleicht die Videos "Genau oder ungefähr?" und "Wenn Zahlen zu genau sind ..." anschauen.

Die Angabe von Nachkommastellen ist oft nicht zielführend. Bei physikalischen Größen hängt deren Relevanz z. B. von der Maßeinheit ab. Eine Nachkommastelle bei einer Angabe in Tonnen ist etwas ganz anderes als eine Nachkommastelle bei einer Angabe in Gramm. Daher spricht man auch von *signifikanten Stellen*, die unabhängig von solchen Skalierungen sind.

Definition

Wenn eine Zahl $x \in \mathbb{R}_{>0}$ auf n **signifikante Stellen** nach dem Komma gerundet wird, dann ist damit gemeint, dass man eine Zahl $\tilde{x}$ angibt, die folgendermaßen konstruiert wird:

(i) Es gibt ein eindeutig bestimmtes $k \in \mathbb{Z}$ mit $0 \leq 10^k x < 1 \leq 10^{k+1} x$.

(ii) $\tilde{x}$ wird so gewählt, dass $10^k \tilde{x}$ der auf n Nachkommastellen gerundete Wert von $10^k x$ ist.

Für negative x geht man entsprechend vor. Die Konventionen für kaufmännisches und mathematisches Runden sind dieselben wie oben.

Im ersten Schritt wird die erste Ziffer von x, die von null verschieden ist, direkt hinter das Dezimaltrennzeichen verschoben. Aus $x_1 = 0.000346$ wird mit $k = 3$ z. B. 0.346 und aus $x_2 = 42.81$ wird mit $k = -2$ der Wert 0.4281. Dann wird auf Nachkommastellen gerundet und anschließend die Verschiebung rückgängig gemacht. x_1 auf zwei signifikante Stellen gerundet ist 0.00035, x_2 auf zwei signifikante Stellen gerundet ist 43.

Konvention

In der Regel wird so gerundet, dass man den verbleibenden Stellen „trauen“ kann. Daher ist es üblich, „überflüssige“ Nullen auszuschreiben, wenn sie beim Runden entstanden sind.

Damit ist gemeint, dass $x = 0.198$ auf zwei Nachkommastellen gerundet 0.20 ist und *nicht* 0.2. Und $\sqrt{24}$ auf drei signifikante Stellen gerundet ist 4.90 und *nicht* 4.9. Mathematisch macht das zwar keinen Unterschied, aber die Signalwirkung beim Lesen ist eine andere. Außerdem sollte man, wenn es sich um Näherungswerte handelt, ein anderes Zeichen als = verwenden, weil das (zumindest in der Mathematik) für exakte Gleichheit steht. Üblich ist in so einem Fall das Symbol $\approx$.

$\approx$

Definition

Ist $\tilde{x}$ ein Näherungswert für die Zahl $x \in \mathbb{R}$, so bezeichnet man die Differenz $\tilde{x} - x$ als den **absoluten Fehler** von $\tilde{x}$.
Ist $\tilde{x}$ ein Näherungswert für die Zahl $x \in \mathbb{R} \setminus \{0\}$, so bezeichnet man den Quotienten $(\tilde{x} - x)/x$ als den **relativen Fehler** von $\tilde{x}$.

Runden auf n Nachkommastellen stellt also sicher, dass der Betrag des absoluten Fehlers höchstens $5 \cdot 10^{-n-1}$ ist. Runden auf signifikante Stellen sorgt hingegen dafür, dass der relative Fehler unabhängig von der Wahl der Maßeinheit immer gleich ist. Da es sich bei relativen Fehlern um Verhältnisse handelt, werden diese oft in Prozent angegeben.

Zum Thema Fehlerfortpflanzung nur zwei einfache Beispiele, um deutlich zu machen, dass auch bei fehlerfreier Rechnung einmal vorhandene Abweichungen immer größer werden können.

Lemma 21.19

Seien x und y reelle Zahlen und $\tilde{x}$ und $\tilde{y}$ Näherungswerte für diese Zahlen mit absoluten Fehlern Δ_x bzw. Δ_y und relativen Fehlern δ_x bzw. δ_y.
Betrachtet man $\tilde{x} \pm \tilde{y}$ als Näherung für $x \pm y$, so ist der Betrag des absoluten Fehlers höchstens $|\Delta_x| + |\Delta_y|$. Betrachtet man $\tilde{x} \cdot \tilde{y}$ als Näherung für $x \cdot y$, so ist der Betrag des relativen Fehlers höchstens $|\delta_x| + |\delta_y| + |\delta_x||\delta_y|$. Die angegeben Schranken lassen sich nicht verbessern, d. h., im schlimmsten Fall können die Fehler tatsächlich so groß wie angegeben sein.

Aufgabe 21.39. Geben Sie Beispiele dafür an, wie in Lemma 21.19 die Fehler maximal groß werden.

Konvention

In der (reinen) Mathematik kommt im Gegensatz zu den Natur- und Ingenieurwissenschaften die Schreibweise von Zahlen mit Nachkommastellen so gut wie nie vor. Sie sollten grundsätzlich immer Brüche verwenden, wenn dies möglich ist. Schreiben Sie also beispielsweise $3/4$ und *nicht* 0.75, weil Letzteres einen ungenauen Wert suggeriert.

Beachten Sie, dass irrationale Zahlen ohnehin in dieser Schreibweise nicht korrekt geschrieben werden können. 0.75 statt $3/4$ ist nur schlechter Stil, 1.73205 statt $\sqrt{3}$ ist jedoch schlicht und einfach falsch!

⋆ Typische Fehlerfortpflanzung im Computer

Im Folgenden will ich an zwei Beispielen Probleme mit der Arithmetik im Computer darstellen. Die Berechnung werden zwar in PYTHON vorgeführt, in anderen Programmiersprachen kommt es jedoch zu denselben Ergebnissen, da Fließkommaarithmetik von der CPU durchgeführt wird und standardisiert ist.

```
from math import sqrt

x = sqrt(2)
m = 1000000
s,S = 0,0
for k in range(m):
    s += x
for k in range(m):
    S += s
S*x - 2*m*m
```

Hier wurde $x \cdot \sum_{k=1}^{m} \left(\sum_{k=1}^{m} x \right)$ berechnet. Das ist dasselbe wie $m^2 x^2$. Der Unterschied zwischen beiden Werten im Computer ist jedoch größer als 45.

```
s0,s1 = 0,0
for k in range(0,14):
    s0 += 9*10**(-k)
    s1 += 9*10**(k-13)
s0,s1
```

Und hier wurde $\sum_{k=0}^{13} 9/10^{-k}$ auf zwei verschiedene Arten (einmal „vorwärts“ und einmal „rückwärts“) berechnet. Es kommen zwei unterschiedliche Ergebnisse heraus. (Welches ist richtig?)

Die Beispiele kommen Ihnen vielleicht konstruiert vor. Das sind sie jedoch nur, um die Probleme besonders deutlich hervorzuheben. Grundsätzlich sollten Sie davon ausgehen, dass mit dem Computer berechnete Fließkommawerte *immer* falsch sind. Exakt richtig sind sie nur in Ausnahmefällen. Daher ist es auch keine gute Idee, solche Zahlen auf Gleichheit zu testen. Probieren Sie z. B. einmal aus, welche Antwort Sie auf die Eingabe

```
6*0.1 == 0.6
```

erhalten. Für vertiefende Informationen zu diesem Thema siehe Fußnote 30.

Resümee

Folgen und Reihen spielten zwar sporadisch bereits in der Antike und im Mittelalter eine gewisse Rolle, aber erst in der Neuzeit – unter anderem durch die Arbeiten von Isaac Newton – rückten sie in den Mittelpunkt der mathematischen Forschung. Die sogenannte „Epsilontik“, mit der Grenzwerte heutzutage präzise definiert werden, geht auf Karl Weierstraß zurück, der Ende des 19. Jahrhunderts auch demonstrierte, dass man große Teile der Analysis auf der Basis von Reihen entwickeln kann.

VIII

Unendliche Mengen

Durch die Überlegungen zur Dezimaldarstellung irrationaler Zahlen wissen wir nun genug, um ein wichtiges Resultat der Mengenlehre verstehen zu können. Daher unterbrechen wir die Ausführungen zur Analysis und beschäftigen uns eine Zeit lang mit unendlichen Mengen. Die Resultate aus diesem Kapitel werden unter anderem in der Theoretischen Informatik (viertes Semester) benötigt, sind aber unabhängig davon auch einfach interessant und sollten zum mathematischen Allgemeinwissen gehören.

22. Vergleich von Mächtigkeiten

Satz 6.3 stellt einen Zusammenhang zwischen der Größe endlicher Mengen und Funktionen zwischen ihnen her. Insbesondere ermöglicht er uns, die Mächtigkeit zweier Mengen zu vergleichen, ohne dass wir zählen müssen. Stellen Sie sich zwei Kinder vor, die wissen wollen, wer von ihnen mehr Legosteine hat, die aber noch nicht zählen können. Sie könnten die Legosteine paarweise hinlegen. Dieses Konzept übertragen wir durch die folgenden Definition auf beliebige (also auch unendliche) Mengen.

Definition

Wenn es eine Bijektion von der Menge A auf die Menge B gibt, dann sagen wir, dass A und B **gleichmächtig** sind bzw. dass sie dieselbe **Mächtigkeit** haben. Wir verwenden dafür die Schreibweise $A \rightleftharpoons B$.

In Kapitel II hatten wir für endliche Mengen bereits definiert, was deren Mächtigkeit sein soll. Das war einfach die Anzahl ihrer Elemente. Dieses Konzept kann man auch auf unendliche Mengen erweitern, wenn man mit sogenannten Kardinalzahlen[1] arbeitet. Das werden wir jedoch nicht machen. Im Kontext unendlicher Mengen vergleichen wir zwar Mächtigkeiten von zwei Mengen im Sinne von „gleich groß“ oder „größer“, wir lassen jedoch offen, was die Mächtigkeit einer einzelnen Menge für ein mathematisches Objekt sein soll.

[1] Im Video *Was sind Kardinalzahlen?* erfahren Sie bei Interesse mehr darüber.

Bezeichnen wir mit $2\mathbb{N}$ die Menge aller geraden natürlichen Zahlen, so wird durch $n \mapsto 2n$ offenbar eine Bijektion von $\mathbb{N}$ auf $2\mathbb{N}$ beschrieben. Es gilt nach der obigen Definition also $\mathbb{N} \approx 2\mathbb{N}$ und wir interpretieren die beiden Mengen als „gleich groß“, obwohl eine von beiden eine echte Teilmenge der anderen ist. Das wirkt einerseits paradox, wenn man zum ersten Mal damit zu tun hat, andererseits ist es sogar eine definierende Eigenschaft unendlicher Mengen.

Aufgabe 22.1. Begründen Sie durch die Angabe einer Bijektion, dass $\mathbb{N} \approx \mathbb{N}^+$ gilt.

Aufgabe 22.2. Begründen Sie durch die Angabe einer Bijektion, dass $\mathbb{N} \approx \mathbb{Z}$ gilt.

Der folgenden Satz besagt, dass sich $\approx$ wie eine Äquivalenzrelation verhält.[2]

Lemma 22.1

Für beliebige Mengen A, B und C gilt:

(i) $A \approx A$

(ii) $A \approx B \Rightarrow B \approx A$

(iii) $A \approx B \wedge B \approx C \Rightarrow A \approx C$

Beweis. $A \approx A$ folgt mithilfe der Abbildung id_A. Die beiden anderen Aussagen wurden bereits in Aufgabe 6.52 bewiesen. ■

Gibt es eine injektive Abbildung von einer endlichen Menge A in eine endliche Menge B, so kann A offenbar nicht mehr Elemente als B haben. Auch diese Idee verwenden wir für beliebige Mengen. Die Vorstellung dahinter ist, dass A zumindest nicht „größer“ als B ist.

Definition

Wenn es eine injektive Funktion von der Menge A in die Menge B gibt, dann schreiben wir dafür $A \preceq B$.

Lemma 22.2

Für beliebige Mengen A, B und C gilt:

(i) $A \subseteq B \Rightarrow A \preceq B$

(ii) $A \preceq A$

(iii) $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$

Beweis. Den ersten Teil beweist man wieder mit id_A und der zweite folgt aus dem ersten wegen $A \subseteq A$. Der dritte Teil wird wie in Lemma 22.1 mit der Komposition der entsprechenden Funktionen bewiesen. ■

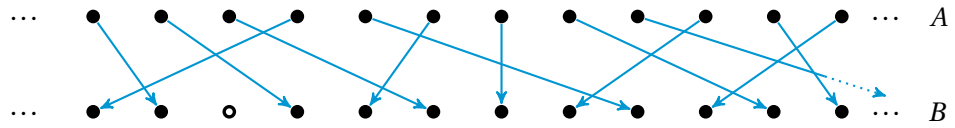
Satz 22.3

Satz von Cantor-Bernstein
Sind A und B beliebige Mengen mit $A \preceq B$ und $B \preceq A$, so gilt $A \approx B$.

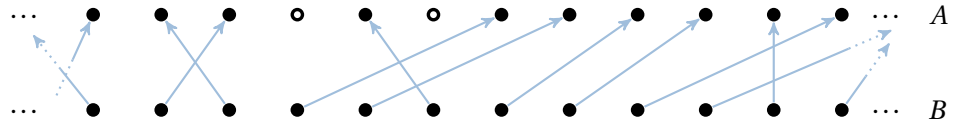
[2] Die vorsichtige Formulierung „verhält sich wie“ (statt einfach „ist“) rührt daher, dass eine Äquivalenzrelation immer auf einer Menge definiert ist und es eine "Menge aller Mengen" nicht gibt. Über solche Dinge müssen wir uns hier jedoch keine Gedanken machen.

Beweis. Wie können o. B. d. A. davon ausgehen, dass A und B disjunkt sind.[3] (Anderenfalls betrachten wir stattdessen die Mengen $A \times \{0\}$ und $B \times \{1\}$, die garantiert disjunkt sind. Finden wir eine Bijektion zwischen diese beiden Mengen, dann liefert diese uns offensichtlich eine zwischen A und B.)

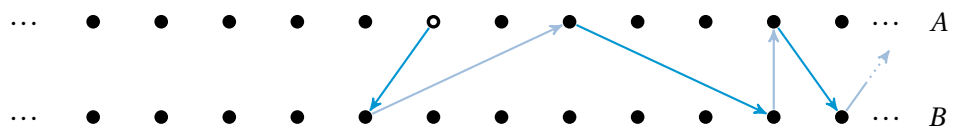
Seien f und g injektive Funktionen von A nach B bzw. von B nach A. Zur Illustration der Beweisidee zeigen die beiden folgenden Skizzen Teile dieser Abbildungen als Pfeildiagramme wie in Abschnitt 6. In der ersten Skizze (für f) geht von jedem Element von A ein Pfeil aus, aber nicht jedes Element von B wird von einem Pfeil getroffen. Auf jeden Fall zeigt jedoch auf kein Element von B mehr als eine Pfeilspitze.



In der zweiten Skizze sehen wir dasselbe für die Funktion g mit vertauschten Rollen von A und B.

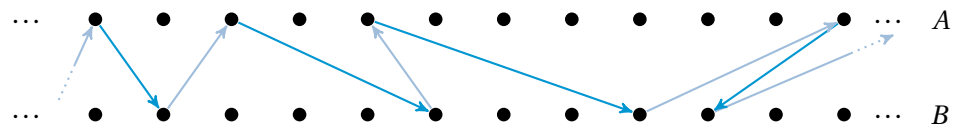


Nun betrachten wir *Ketten*. Damit ist gemeint, dass von jedem Punkt in A *oder* B genau ein Pfeil ausgeht. Dieser Pfeil zeigt auf einen Punkt, von dem wieder ein Pfeil ausgeht, und so weiter. Bei jedem Punkt startet also ein „Zick-Zack-Weg“, der zwischen den beiden Mengen hin- und her springt und nie endet. Man kann aber evtl. auch „rückwärts“ gehen: Gibt es einen Pfeil, der auf einen Punkt zeigt, dann geht man zum Ausgangspunkt dieses Pfeils und schaut dort wiederum, ob ein Pfeil auf diesen Punkt zeigt. Auch das kann man fortsetzen, aber im „Rückwärtsgang“ ist es nicht mit Sicherheit so, dass der Weg nie endet, weil man bei einem Punkt angelangen kann, auf den kein Pfeil zeigt. Die Menge aller Punkte, die man von einem Punkt aus erreicht, wird dann *Kette* genannt. Die folgende Skizze zeigt ein Beispiel. Und wenn wir davon ausgehen, dass auf den hervorgehobenen Punkt kein Pfeil zeigt, dann hat diese Kette einen definitiven Anfang.

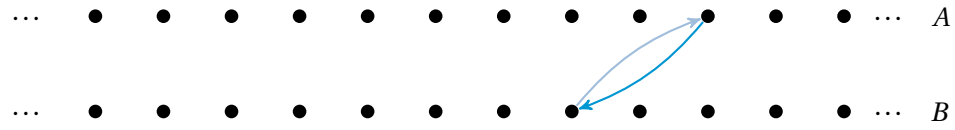


Ketten müssen aber keinen Anfang haben. Wir können uns vorstellen, dass man nicht nur immer weiter nach „vorne“, sondern auch beliebig weit „rückwärts“ gehen kann. Das soll durch die Auslassungspunkte in der folgenden Skizze angedeutet werden.

[3] Das ist gar nicht unbedingt nötig, erleichtert allerdings die Vorstellung und die Visualisierung.

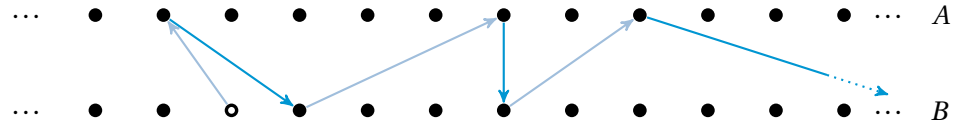


Und auch „Schleifen“, die zum Ausgangspunkt zurückkehren sind denkbar. Das sind ebenfalls Ketten ohne Anfang. Das einfachste Beispiel ist eine Schleife aus nur zwei Punkten wie in der folgenden Grafik.



Es sollte jedenfalls das Folgende klar sein: Erstens liegt jeder Punkt aus $A \cup B$ auf einer Kette, weil von ihm auf jeden Fall ein Pfeil ausgeht. Zweitens liegt kein Punkt auf mehr als einer Kette, denn von jedem Punkt geht nur ein Pfeil aus und bei jedem Punkt kommt höchstens ein Pfeil an. Ebenso gehört auch jeder Pfeil zu genau einer Kette.

Ketten, die einen Anfangspunkt haben, der in B liegt, nennen wir *B-Ketten*. Die folgende Skizze zeigt dafür ein Beispiel. Alle vorher gezeigten Ketten sind damit *keine* B-Ketten, denn sie haben entweder keinen Anfangspunkt oder dieser liegt in der Menge A.



Nun definieren wir die folgende Funktion:

$$h\colon \begin{cases} A \to B \\ x \mapsto \begin{cases} g^{-1}(x) & x \text{ liegt auf einer } B\text{-Kette} \\ f(x) & x \text{ liegt nicht auf einer } B\text{-Kette} \end{cases} \end{cases} \tag{22.1}$$

In der letzten Skizze würden wir also von den A-Punkten auf der Kette aus jeweils den hellen Pfeilen in umgekehrter Richtung folgen. In den Skizzen davor würden wir hingegen den dunklen Pfeilen vorwärts folgen.

h ist damit eine bijektive Funktion von A auf B. Zunächst einmal ist h überhaupt sinnvoll definiert: $f(x)$ existiert ohnehin für jedes $x \in A$ und $g^{-1}(x)$ existiert zumindest für $x \in A$, das auf einer B-Kette liegt, denn so eine Kette fängt nicht im Punkt x an. Dass h injektiv ist, folgt aus den obigen Überlegungen über Ketten. Es fehlt nur noch die Surjektivität: Ist $y \in B$ ein Punkt auf einer B-Kette, dann gilt nach Definition $h(g(y)) = y$. Liegt $y \in B$ nicht auf einer B-Kette, dann ist y nicht der Anfangspunkt der Kette und es gibt einen f-Pfeil, der auf y zeigt.[4] ■

[4] Die hier gezeigte Beweisidee stammt übrigens von dem ungarischen Mathematiker Julius König. Weitere Beweise und mehr über den historischen Hintergrund im Video "Der Satz von Cantor-Bernstein".

Während sich $\precneqq$ wie eine Äquivalenzrelation verhält, verhält sich $\preceq$ also wie eine Halbordnung, wenn man $\precneqq$ als Gleichheit interpretiert.[5] Man kann $A \precneqq B$ und $A \preceq B$ auch als $|A| = |B|$ bzw. $|A| \leq |B|$ verstehen. Das ist zwar korrekt, aber im Rahmen dieses Skripts wissen wir nicht, was mit $|A|$ gemeint sein soll, wenn A unendlich ist. (Siehe die Bemerkung auf Seite 233.)

Aufgabe 22.3. Mit dem Satz von Cantor-Bernstein kann man ohne großen Aufwand zeigen, dass die Intervalle $A = (0,1)$ und $B = [0,1]$ gleichmächtig sind. Haben Sie eine Idee, welche Funktionen man nehmen könnte?

⋆**Aufgabe 22.4**. Können Sie eine Bijektion von $B = [0,1]$ auf $A = (0,1)$ explizit angeben?

Aufgabe 22.5. Geben Sie für die Lösung von Aufgabe 22.3 an, ob die Zahlen $1/2$, $3/8$ und $5/16$ als Elemente von A auf einer B-Kette (im Sinne des Beweises von Satz 22.3) liegen. Welche Funktionswerte würde die Funktion h aus dem Beweis diesen drei Zahlen zuordnen.

23. Abzählbare Mengen

Wir sind bisher immer von einer intuitiven Vorstellung von „endlich“ ausgegangen. Für die folgenden Überlegungen ist es jedoch sinnvoll, das zu präzisieren.

Definition

Wir nennen eine Menge A **endlich**, wenn es eine natürliche Zahl n mit $A \precneqq [n]$ gibt. Eine Menge, die nicht endlich ist, wird **unendlich** genannt.

Aufgabe 23.1. Verständnisfrage: Ist nach der obigen Definition die leere Menge endlich? Begründen Sie Ihre Antwort.

$\mathbb{N}$ ist offenbar unendlich, denn wenn es eine Zahl $n \in \mathbb{N}$ mit $\mathbb{N} \precneqq [n]$ gäbe, dann könnten wir mit einem Algorithmus wie in Aufgabe 11.3 das größte Element M von $\mathbb{N}$ ermitteln. Aber das kann es nicht geben, denn $M+1$ ist ja ebenfalls ein Element von $\mathbb{N}$. Man kann aber noch mehr über $\mathbb{N}$ aussagen:

Lemma 23.1

$\mathbb{N}$ ist die „kleinste“ unendliche Menge in dem Sinne, dass $\mathbb{N} \succeq A$ für jede unendliche Menge A gilt.

Beweis. Sei A eine beliebige unendliche Menge. Wir definieren rekursiv eine injektive Folge (a_n) von Elementen von A: a_0 sei irgendein Element von A. (Es muss eins geben, weil A nach Aufgabe 23.1 nicht leer ist.) Sind a_0 bis a_{n-1} bereits definiert, so ist $A_n = \{a_0, \dots, a_{n-1}\}$ offenbar eine Menge mit $A_n \precneqq [n]$. Da A unendlich ist, muss $A \neq A_n$ gelten. Also gibt es ein Element $a_n \in A \setminus A_n$. ■

[5] Eine naheliegende Frage ist übrigens, ob diese „Halbordnung“ total in dem Sinne ist, dass für zwei Mengen A und B immer mindestens eine der beiden Aussagen $A \succeq B$ oder $B \succeq A$ gilt. Die Antwort hängt vom sogenannten *Auswahlaxiom* ab. Siehe dazu das Video *Das (berühmt-berüchtigte) Auswahlaxiom*.

Definition

Eine Menge, die endlich ist oder dieselbe Mächtigkeit wie $\mathbb{N}$ hat, wird **abzählbar** genannt. Abzählbare Mengen, die nicht endlich sind, werden **abzählbar unendlich** genannt.

Diese Bezeichnung rührt daher, dass man die Elemente einer abzählbaren Mengen mithilfe einer entsprechenden Bijektion der Reihe nach „abzählen“ kann: das erste, das zweite, das dritte und so weiter. Nach Aufgabe 22.2 ist beispielsweise $\mathbb{Z}$ abzählbar.

Lemma 23.2

Jede Teilmenge einer abzählbaren Menge ist abzählbar.

Beweis. Sei A abzählbar. Dann gibt es eine injektive Abbildung von A nach $\mathbb{N}$. (Entweder gilt $A \precnsim \mathbb{N}$ oder $A \precnsim [n]$ für ein $n \in \mathbb{N}$. Im zweiten Fall kann man die Bijektion von A nach $[n]$ als Injektion[6] von A nach $\mathbb{N}$ nehmen.)

Sei nun B eine Teilmenge von A. Die Restriktion auf B der Injektion aus dem letzten Absatz ist dann eine Injektion von B nach $\mathbb{N}$. O. B. d. A. sei B unendlich (denn sonst gibt es nichts mehr zu zeigen). Nach Lemma 23.1 gibt es eine Injektion von $\mathbb{N}$ nach B. Nach Satz 22.3 folgt $\mathbb{N} \precnsim B$. ■

Will man nun von einer Menge A zeigen, dass sie abzählbar ist, so reicht es nach diesem Lemma, eine injektive Abbildung f von A in irgendeine abzählbare Menge B anzugeben. A hat dann nämlich dieselbe Mächtigkeit wie die Teilmenge $f[A]$ von B.

Satz 23.3

$\mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\}$ und $\mathbb{N} \times \mathbb{N}$ sind abzählbar.

Beweis. Eine Abbildung von $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$ erhalten wir, indem wir jedes Paar (m, n) auf $2^m 3^n$ abbilden.[7] Injektiv ist diese Funktion nach dem Fundamentalsatz der Arithmetik. Und eine injektive Abbildung von $\mathbb{Q}^+$ nach $\mathbb{N} \times \mathbb{N}$ erhalten wir, indem wir jeden Bruch p/q (in gekürzter Form) auf das Paar (p, q) abbilden. ■

Obwohl wir sie wegen der Verwendung des Satzes von Cantor-Bernstein nicht benötigten, ist es doch ganz sinnvoll, sich Cantors ursprüngliche Beweisidee anzuschauen, weil man sie häufig gut gebrauchen kann. Dazu stellt man sich zunächst alle positiven Brüche in einer Tabelle wie der folgenden vor.

	1	2	3	4	5	6	⋯
1	1/1	1/2	1/3	1/4	1/5	1/6	⋯
2	2/1	2/2	2/3	2/4	2/5	2/6	⋯
3	3/1	3/2	3/3	3/4	3/5	3/6	⋯
4	4/1	4/2	4/3	4/4	4/5	4/6	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

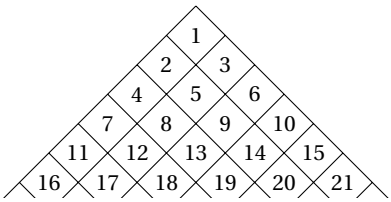
Injektion

[6] *Injektion* ist einfach ein anderes Wort für injektive Funktion.

[7] Auf derselben Idee basiert die Technik der sogenannten *Gödelisierung*.

In der m-ten Zeile stehen die Brüche mit dem Zähler m, in der n-ten Spalte die Brüche mit dem Nenner n. Damit wirklich *alle* Brüche in der Tabelle zu finden sind, muss diese natürlich unendlich viele Zeilen und unendlich viele Spalten haben. Dass hat zur Folge, dass man die Tabelle nicht zeilen- oder spaltenweise durchgehen kann, denn bereits mit dem Abzählen aller Einträge der ersten Zeile oder Spalte würde man niemals fertig werden.

Cantors clevere Idee bestand darin, stattdessen die Tabelle quasi um 45 Grad zu drehen und sich die Diagonalen der Reihe nach vorzunehmen. Die werden zwar immer länger, haben aber jede für sich nur eine endliche Länge, so dass nach und nach alle drankommen. Die Reihenfolge sieht wie folgt aus.



Für die Tabelle der Brüche würde das mit

$$1/1 \quad 2/1 \quad 1/2 \quad 3/1 \quad 2/2 \quad 1/3 \quad 4/1 \quad 3/2 \quad 2/3 \quad 1/4 \quad 5/1 \quad \dots$$

anfangen. Um daraus eine bijektive Funktion von $\mathbb{N}$ nach $\mathbb{Q}^+$ zu machen, muss man gewissermaßen Buch führen und bereits „gesehene“ Brüche überspringen. (Beispielsweise würde $2/2$ gestrichen werden, weil vorher bereits $1/1$ vorkam.) Alternativ kann man die obige Reihenfolge verwenden, um daraus eine injektive Abbildung von $\mathbb{Q}^+$ nach $\mathbb{N}$ zu konstruieren: $1/1$ wird beispielsweise auf 1 abgebildet, $1/3$ auf 6, $4/3$ auf 18 und so weiter.

⋆**Aufgabe 23.2**. Schreiben Sie eine Rechenvorschrift für die eben angedeutete injektive Abbildung von $\mathbb{Q}^+$ nach $\mathbb{N}$ auf.

$\mathbb{Q}$ ist abzählbar. **Korollar 23.4**

Beweis. Sei f eine bijektive Abbildung von $\mathbb{N}^+$ auf $\mathbb{Q}^+$. (Siehe Aufgabe 22.1.) Durch

$$n \mapsto \begin{cases} f(n) & n > 0 \\ 0 & n = 0 \\ -f(-n) & n < 0 \end{cases}$$

wird dann eine Bijektion von der abzählbaren Menge $\mathbb{Z}$ auf $\mathbb{Q}$ definiert. ■

Ist A abzählbar, dann ist A^n für alle $n \in \mathbb{N}$ abzählbar.[8] **Korollar 23.5**

[8] Mit A^1 ist natürlich A gemeint – oder etwas formaler $\{(a) : a \in A\}$ – und mit A^0 die Menge, die als einziges Element das leere Tupel (siehe Aufgabe 3.20) enthält.

Beweis. Dass A^0 und A^1 abzählbar sind, ist klar. Sei nun f eine Injektion von A nach $\mathbb{N}$ und g eine Bijektion von $\mathbb{N}\times\mathbb{N}$ auf $\mathbb{N}$. Durch $(a_1,a_2)\mapsto g(f(a_1),f(a_2))$ wird dann eine Injektion von $A^2=A\times A$ nach $\mathbb{N}$ definiert. Für A^3 zeigt man anschließend die Abzählbarkeit, indem man die Bijektion $(a_1,(a_2,a_3))\mapsto(a_1,a_2,a_3)$ von $A\times A^2$ auf A^3 verwendet.[9] Induktiv folgt die Behauptung dann für A^4 und so weiter. ■

Satz 23.6 Sind die Mengen A_n für $n\in\mathbb{N}$ alle abzählbar, dann ist auch $\bigcup_{n\in\mathbb{N}} A_n$ abzählbar.

Beweis. Nach Voraussetzung gibt es für alle $n\in\mathbb{N}$ eine Injektion f_n von A_n auf $\mathbb{N}$. Für $a\in A=\bigcup_{n\in\mathbb{N}} A_n$ sei $n_a=\min\{n\in\mathbb{N}: a\in A_n\}$. Durch $a\mapsto(n_a,f_{n_a}(a))$ wird dann eine injektive Funktion von A nach $\mathbb{N}\times\mathbb{N}$ definiert. ■

Man beachte, dass Satz 23.6 insbesondere auch für die Vereinigung von endlich vielen Mengen gilt, weil es ja nicht verboten ist, dass fast alle A_n leer sind.

Korollar 23.7 Ist A abzählbar, dann ist $\bigcup_{n\in\mathbb{N}} A^n$ abzählbar.

Korollar 23.7 ist u. a. für die Theoretische Informatik interessant, weil daraus folgt, dass es „nur“ abzählbar viele (endliche) Zeichenketten gibt, wenn man einen endlichen (oder sogar einen abzählbar unendlichen) Zeichenvorrat hat. Ist U beispielsweise die (endliche) Menge aller Unicode-Zeichen, so kann man die Menge aller Strings, die sich mit diesen Zeichen darstellen lassen, mit $\bigcup_{n\in\mathbb{N}} U^n$ identifizieren.

Aufgabe 23.3. Begründen Sie, warum $\mathbb{P}$ abzählbar unendlich ist.

Aufgabe 23.4. Begründen Sie, warum die Menge aller Polynomfunktionen über $\mathbb{Q}$ abzählbar ist. (Hinweis: Ein Polynom vom Grad n wird durch die Angabe von $n+1$ Koeffizienten eindeutig beschrieben.)

⋆**Aufgabe 23.5.** Begründen Sie die folgende Aussage: Ist A abzählbar, dann ist

$\mathscr{P}_{<\infty}(A)$ $$\mathscr{P}_{<\infty}(A)=\{Y\in\mathscr{P}(A): Y \text{ ist endlich}\}$$

ebenfalls abzählbar.

24. Überabzählbare Mengen

Durch den letzten Abschnitt könnte man den Eindruck gewinnen, alle Mengen seien abzählbar. Dem ist aber nicht so, wie das folgende berühmte Resultat von Georg Cantor zeigt.

Satz 24.1 Das Intervall $(0,1)$ ist nicht abzählbar.

[9] Dabei nutzt man aus, dass A^2 schon als abzählbar bekannt ist und dass wir im letzten Schritt eigentlich bewiesen haben, dass $A\times B$ abzählbar ist, wenn A und B abzählbar sind. (Denn man hätte a_1 und a_2 auch in unterschiedliche Injektionen einsetzen können.)

Beweis. Während es bisher immer ausreichte, eine spezifische Bijektion oder Injektion anzugeben, müssen wir nun beweisen, dass es *keine* Bijektion von $\mathbb{N}^+$ auf $(0,1)$ geben kann.[10] Das machen wir mit einem Widerspruchsbeweis, indem wir annehmen, es gäbe so eine Bijektion f. Wir bezeichnen dann mit a_n die n-te Nachkommastelle von $f(n)$. Und definieren die Folge (b_n) durch $b_n = 4$, wenn $a_n = 5$ gilt, und $b_n = 5$ für alle anderen Fälle. Die Zahl $b = \sum_{n=1}^{\infty} b_n 10^{-n}$ liegt dann im Intervall $(0,1)$, aber nicht im Wertebereich von f, denn für alle $n \in \mathbb{N}$ unterscheiden sich nach Konstruktion die n-te Nachkommastelle von $f(n)$ und die n-te Nachkommastelle von b. f ist also nicht surjektiv. ■

Cantors wesentliche Idee bei der Konstruktion von b nennt man inzwischen ein *Diagonalargument* und dieselbe Technik wurde später auch in anderen mathematischen Beweisen eingesetzt. Die folgende Tabelle illustriert die Vorgehensweise an einem Beispiel. Die unterstrichenen Ziffern sind die relevanten Nachkommastellen. b würde in diesem Fall mit $0.5454455\ldots$ anfangen.

Diagonalargument

$f(1)$	$2/3$	$0.\underline{6}6666666666666\ldots$
$f(2)$	$1/4$	$0.2\underline{5}000000000000\ldots$
$f(3)$	$1/2$	$0.50\underline{0}0000000000000\ldots$
$f(4)$	$\pi - 3$	$0.1415\underline{9}265358979\ldots$
$f(5)$	$1/7$	$0.14285\underline{7}14285714\ldots$
$f(6)$	$\sqrt{5} - 2$	$0.23606\underline{7}97749979\ldots$
$f(7)$	$\pi^2 - 9$	$0.869604\underline{4}0108936\ldots$
	$\vdots$	

Mengen, die nicht abzählbar sind, nennt man **überabzählbar**.

Definition

Jede Obermenge einer überabzählbaren Menge ist überabzählbar.

Lemma 24.2

Beweis. Sei A überabzählbar und $B \supseteq A$. Wäre B nicht überabzählbar, so wäre A nach Lemma 23.2 abzählbar. ■

Jedes echte Intervall ist überabzählbar. Insbesondere ist $\mathbb{R}$ überabzählbar.

Korollar 24.3

Beweis. Sind a und b reelle Zahlen mit $a < b$, so ist $x \mapsto (b-a)x + a$ eine Bijektion von $(0,1)$ auf (a,b). Alle Intervalle von diesem Typ sind damit nach Satz 24.1 überabzählbar. Nach Lemma 24.2 gilt die Aussage auch für unbeschränkte Intervalle oder solche mit eckigen statt runden Klammern. ■

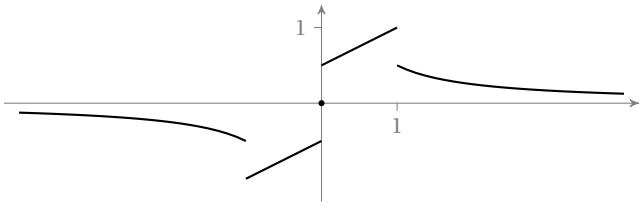
Es gilt sogar eine noch stärkere Aussage:

[10] Aus technischen Gründen nehmen wir $\mathbb{N}^+$ statt $\mathbb{N}$. Nach Aufgabe 22.1 ist das OK.

Satz 24.4 Alle echten Intervalle haben dieselbe Mächtigkeit.

Beweis. Nach Aufgabe 22.3 haben $(0,1)$ und $[0,1]$ dieselbe Mächtigkeit. Daher müssen offensichtlich auch $[0,1)$ und $(0,1]$ diese Mächtigkeit haben. Mit der im Beweis von Korollar 24.3 angegebenen Bijektion folgt dann, dass alle beschränkten echten Intervalle dieselbe Mächtigkeit haben. Um auch noch die unbeschränkten Intervalle ins Boot zu holen, reicht eine Injektion von $\mathbb{R}$ in ein beschränktes Intervall.[11] Dafür kann man beispielsweise so vorgehen:

$$: \begin{cases} \mathbb{R} \to (-1,1) \\ x \mapsto \begin{cases} 0 & x = 0 \\ (x+1)/2 & x \in (0,1) \\ (x-1)/2 & x \in (-1,0) \\ (2x)^{-1} & x \notin (-1,1) \end{cases} \end{cases}$$



Dass diese Funktion tatsächlich injektiv und ihr Wertebereich (eine Teilmenge von) $(-1,1)$ ist, kann man mit den Rechenregeln aus Lemma 15.3 nachweisen.[12] ■

Aufgabe 24.1. Begründen Sie, warum die Menge $\mathbb{R} \setminus \mathbb{Q}$ aller irrationalen Zahlen überabzählbar ist.

Satz 24.5 **Satz von Cantor**
Für keine Menge A gibt es eine surjektive Abbildung von A auf $\mathscr{P}(A)$.

Beweis. Das beweist man wieder mit einem Diagonalargument. Wir nehmen an, es gäbe eine surjektive Abbildung f von A auf $\mathscr{P}(A)$ und definieren die Menge $B = \{a \in A : a \notin f(a)\}$. Da B eine Teilmenge von A ist, muss es ein $a \in A$ geben mit $f(a) = B$. Es gilt also entweder $a \in B$ oder $a \notin B$. $a \in B = f(a)$ ist nach Definition von B jedoch äquivalent zu der Aussage $a \notin B$. Das ist offensichtlich ein unauflösbarer Widerspruch. ■

Da andererseits durch $a \mapsto \{a\}$ offenbar eine Injektion von A nach $\mathscr{P}(A)$ definiert wird, hat $\mathscr{P}(A)$ immer eine größere Mächtigkeit als A. Zu jeder Menge gibt es also eine, die noch größer ist. Es gibt unendlich viele verschiedenen Stufen der

[11] Jedes andere unbeschränkte Intervall ist eine Teilmenge von $\mathbb{R}$ und kann damit „erst recht“ injektiv in ein beschränktes Intervall abgebildet werden.

[12] Eine elegante Alternative zum „Zusammendrücken“ von $\mathbb{R}$ auf ein beschränktes Intervall ist der Arkustangens, den wir allerdings erst später einführen werden.

Unendlichkeit, die durch den Begriff *überabzählbar* nur unzureichend erfasst werden. Leider können wir das Thema hier nicht weiter vertiefen. Bei Interesse blättern Sie vielleicht mal in einem Buch wie *Introduction to Cardinal Arithmetic* nach.

Zumindest sei aber noch erwähnt, dass nach dem Satz von Cantor $\mathscr{P}(\mathbb{N})$ überabzählbar ist. Man kann sogar noch mehr zeigen:

Satz 24.6 $\mathscr{P}(\mathbb{N})$ und $\mathbb{R}$ haben dieselbe Mächtigkeit.

Beweis. Analog zu Satz 21.18 hat jede Zahl im Intervall $[0,1)$ eine Binärdarstellung, also eine Folge von Nachkommastellen, die aus Nullen und Einsen besteht.[13] Ist x eine Zahl aus diesem Intervall und a_n die n-Nachkommastelle von x, dann bildet man x auf die Menge $\{n \in \mathbb{N}^+ : a_n = 1\}$ ab. Damit erhält man eine Injektion von $[0,1)$ nach $\mathscr{P}(\mathbb{N})$.

Umgekehrt kann man zu einer Teilmenge X von $\mathbb{N}$ eine Folge (a_n) in $\{0,1\}$ dadurch definieren, dass a_n genau dann 1 ist, wenn $n \in X$ gilt. Daraus ergibt sich eine Zahl $\sum_{n=0}^{\infty} a_n 10^{-n-1}$, die im Intervall $[0,1)$ liegt. Diese Abbildung von Mengen auf Zahlen ist offenbar ebenfalls injektiv.

Nach dem Satz von Cantor-Bernstein haben $[0,1)$ und $\mathscr{P}(\mathbb{N})$ dieselbe Mächtigkeit und nach Satz 24.4 gilt das auch für $\mathbb{R}$. ■

Aufgabe 24.2. Begründen Sie, warum die Menge aller Polynomfunktionen über $\mathbb{R}$ überabzählbar ist. (Hinweis: Für die Begründung braucht man nicht einmal alle Polynomfunktionen, sondern nur einen kleinen Teil von $\mathbb{R}[x]$.)

Aufgabe 24.3. Welche der folgenden Mengen sind überabzählbar? Begründen Sie Ihre Antworten.

$$A = \{\sqrt{n} : n \in \mathbb{N}^+\} \qquad B = \{\sqrt[k]{n} : k, n \in \mathbb{N}^+\}$$
$$C = \{\lfloor r \rfloor : r \in \mathbb{R}\} \qquad D = \mathbb{R} \times \mathbb{Q}$$
$$E = \bigcup_{n \in \mathbb{N}^+} [n, n + 1/n) \qquad F = \bigcup_{n \in \mathbb{N}} \mathscr{P}([n])$$
$$G = \mathbb{R} \times \emptyset$$

Aufgabe 24.4. Ist $A = [0,1) \cup \{q\}$ abzählbar, wenn q eine rationale Zahl ist? Und was ist mit $B = \{[0,1) \cup \{q\} : q \in \mathbb{Q}\}$?

⋆**Aufgabe 24.5**. Geben Sie eine Bijektion von $\mathscr{P}(\mathbb{N})$ auf $[2]_0^{\mathbb{N}}$ an. (Zur Erinnerung: Gemeint ist die Menge aller Funktionen von $\mathbb{N}$ nach $[2]_0$.

[13] Positive Brüche, deren Nenner in gekürzter Form eine Zweierpotenz ist, haben zwei verschiedene Darstellungen. Das ist aber kein Problem. In so einem Fall entscheidet man sich einfach für eine von beiden.

Resümee

Um Mengenlehre ging es bereits ganz am Anfang des Skripts und dort wurde auch schon auf deren Bedeutung eingegangen. Erst durch die genaue Untersuchung unendlicher Mengen wird jedoch die Komplexität der Mengenlehre deutlich. Die Ergebnisse in diesem Kapitel beruhen alle auf den Forschungen von Georg Cantor, der in der zweiten Hälfte des 19. Jahrhunderts ein uraltes Denkverbot überwand und mit der sogenannten *aktualen Unendlichkeit* arbeitete. Das führte seinerzeit zu erheblichem Widerstand im Kreise seiner Kollegen. (Dabei ging es nicht darum, ob Cantors Resultate formal richtig oder falsch waren, sondern ob seine Methoden aus philosophischer Sicht überhaupt zulässig waren.) Heute werden Cantors Pionierleistungen jedoch als Geburtsstunde eines wesentlichen Teilbereichs der Mathematik betrachtet.

Zudem warf Cantor schon sehr früh eine Frage auf, die inzwischen Kontinuumshypothese genannt wird: Kann es sein, dass es eine Teilmenge von $\mathbb{R}$ gibt, die eine größere Mächtigkeit als $\mathbb{N}$ bzw. $\mathbb{Q}$, aber eine kleinere als ganz $\mathbb{R}$ hat? Diese Frage galt fast ein Jahrhundert lang als eines der wichtigsten offenen Probleme der Mathematik und stellte sich schließlich als unlösbar heraus.

IX

Reelle und komplexe Funktionen

Auf der Basis des Wissens über Grenzwerte aus dem letzten Kapitel erarbeiten wir uns weitere Ergebnisse der Analysis. Im Mittelpunkt stehen dabei die sogenannten elementaren Funktionen und ihre Eigenschaften.

25. Stetige Funktionen

Der Begriff der Stetigkeit präzisiert mathematisch in gewissem Sinne eine Grundannahme der Philosophie und Naturwissenschaft seit der Antike, die man als *Natura non facit saltus* – „Die Natur macht keine Sprünge“ – bezeichnet. Heutzutage betrachtet man Stetigkeit als eine topologische Eigenschaft, die man unabhängig von der Differenzierbarkeit einer Funktion untersuchen kann.

Definition

Sei $f\colon A \to \mathbb{C}$ mit $A \subseteq \mathbb{C}$, $a \in \overline{A}$ und $L \in \mathbb{C}$. Gilt $\lim_{n\to\infty} f(a_n) = L$ für alle Folgen (a_n) in A mit $\lim_{n\to\infty} a_n = a$, dann nennt man L den **Grenzwert** von f an der Stelle a und schreibt $\lim_{x\to a} f(x) = L$. Ist f eine reellwertige Funktion und A eine Teilmenge von $\mathbb{R}$, so verwendet man diese Schreibweise auch für die Fälle $L = \infty$ oder $L = -\infty$.

Es ist wichtig, den Unterschied zur Grenzwertdefinition für Folgen zu verstehen. Man kann eine Folge zwar als Funktion im Sinne dieser Definition interpretieren, aber ∞ ist kein Berührungspunkt ihres Definitionsbereichs. (∞ ist ja nicht einmal eine Zahl.) Es ist zwar möglich, beide Definitionen unter einen Hut zu bringen, aber das wäre zu abstrakt für das Niveau dieses Skripts.

Ganz wesentlich ist außerdem, dass a nicht notwendig im Definitionsbereich von f liegen muss. Man kann also vom Grenzwert an der Stelle a sprechen, obwohl der Funktionswert $f(a)$ evtl. gar nicht definiert ist.

Ein paar einfache Beispiele, die hoffentlich dem Verständnis dienen. Wenn nichts anderes erwähnt wird, sind f, A und a immer wie in der Definition gemeint.

- Ist f durch $f(x) = x$ definiert, dann gilt offenbar $\lim_{x\to a} f(x) = \lim_{x\to a} x = a$ für alle $a \in \overline{A}$, denn natürlich konvergiert $(f(a_n))$ immer gegen denselben Grenzwert wie (a_n), weil es sich in beiden Fällen um dieselbe Folge handelt.
- Ist f durch $f(x) = c$ für eine konstante Zahl c definiert, dann gilt natürlich $\lim_{x\to a} f(x) = \lim_{x\to a} c = c$ für alle $a \in \overline{A}$, denn $(f(a_n))$ ist dann immer die konstante Folge (c).
- Ist a ein isolierter Punkt von A, dann muss $a \in A$ gelten und es gibt außer Folgen, deren Folgenglieder fast alle den Wert a haben, keine weiteren in A, die gegen a konvergieren. Daher folgt $\lim_{x\to a} f(x) = f(a)$.
- Betrachtet man die durch $f(x) = g(x) = 0$ für $x \neq 0$ und $f(0) = 1$ definierten Funktionen $f\colon \mathbb{R} \to \mathbb{R}$ und $g\colon \mathbb{R}\setminus\{0\} \to \mathbb{R}$, dann gilt $\lim_{x\to 0} g(x) = 0$, während $\lim_{x\to 0} f(x)$ nicht existiert. Der Unterschied kommt dadurch zustande, dass für den Grenzwert nur Folgen verwendet werden können, die im Definitionsbereich der Funktion verlaufen. Für f muss man auch die Folge betrachten, die konstant null ist, während das für g nicht möglich ist.[1]

Direkt aus den Rechenregeln für Folgen (Lemma 19.4) erhält man:

Lemma 25.1

Sei f und g Funktionen von A nach $\mathbb{C}$ mit $A \subseteq \mathbb{C}$ und $a \in \overline{A}$. Existieren die Grenzwerte von f und g an der Stelle a, dann existieren auch die von $f \pm g$ und $f \cdot g$. Ist $\lim_{x\to a} g(x)$ nicht null, so existiert auch der entsprechende Grenzwert von f/g. Unter den genannten Voraussetzungen gilt dann:

$$\begin{aligned}
\lim_{x\to a}\big(f(x) \pm g(x)\big) &= \lim_{x\to a} f(x) \pm \lim_{x\to a} g(x)\\
\lim_{x\to a}\big(f(x) \cdot g(x)\big) &= \lim_{x\to a} f(x) \cdot \lim_{x\to a} g(x)\\
\lim_{x\to a}\big(f(x) / g(x)\big) &= \lim_{x\to a} f(x) / \lim_{x\to a} g(x)
\end{aligned}$$

Aufgabe 25.1. Gilt auch eine Rechenregel wie

$$\lim_{x\to a+b} f(x) = \lim_{x\to a} f(x) + \lim_{x\to b} f(x)?$$

Begründen Sie Ihre Antwort.

Definition

Sei $f\colon A \to \mathbb{C}$ mit $A \subseteq \mathbb{C}$. Man sagt, dass f **stetig** an der Stelle $a \in A$ ist, wenn $\lim_{x\to a} f(x) = f(a)$ gilt. Ist $B \subseteq A$ und f stetig an allen Stellen $a \in B$, dann nennt man f **stetig** auf B. Ist f stetig auf dem gesamten Definitionsbereich A, so nennt man f einfach **stetig**.

Wegen Lemma 25.1 hat man sofort:

[1] Für das Folgende ist das nicht wichtig, aber an dieser Stelle unterscheidet sich die „moderne“ Definition, die wir hier verwenden, von der „klassischen“, die auf den schon erwähnten Karl Weierstraß zurückgeht. Weitere Informationen dazu findet man z. B. im Wikipedia-Artikel über Grenzwerte von Funktionen.

Lemma 25.2

Sei f und g Funktionen von A nach $\mathbb{C}$ mit $A \subseteq \mathbb{C}$. Sind f und g stetig in $a \in A$, so sind $f \pm g$ und $f \cdot g$ dort auch stetig. Gilt $g(a) \neq 0$, so ist auch f/g an der Stelle a stetig.

Die ersten Beispiele haben gezeigt, dass konstante Funktionen und die Identität stetig sind. Mit Lemma 25.2 folgt, dass alle Polynomfunktionen über $\mathbb{C}$ stetig sind. Und das gilt auch noch für alle *rationalen Funktionen*, also für Quotienten von Polynomfunktionen (die natürlich an den Stellen, an denen der Nenner verschwindet, nicht definiert sind).

rationale Funktion

Einfache Beispiele für Funktionen, die an einer Stelle a ihres Definitionsbereichs *nicht* stetig sind, liefern Funktionen, die „absichtlich“ in diesem Punkt „umdefiniert“ werden oder die dort einen „Sprung“ machen. Beispiele sind die auf ganz $\mathbb{R}$ definierten Funktionen f und g mit

$$f(x) = \begin{cases} 0 & x \neq 0 \\ 1 & x = 0 \end{cases} \quad \text{und} \quad g(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases}. \tag{25.1}$$

Ein extremeres Beispiel ist die *Dirichlet-Funktion*, die durch

Dirichlet-Funktion

$$: \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases} \end{cases}$$

definiert ist. Sie ist in *keinem* Punkt $a \in \mathbb{R}$ stetig. (Das folgt aus Satz 16.10 und Lemma 16.11.)

Aufgabe 25.2. Wenn Ihnen nicht völlig klar ist, wie diese Funktionen aussehen, dann skizzieren Sie die Funktionsgraphen für die Beispiele f und g in (25.1). Überlegen Sie sich dann, warum man die Dirichlet-Funktion nicht zeichnen kann, und versuchen Sie, sich diese Funktion vorzustellen.

Die intuitive Vorstellung, dass stetige Funktionen keine "Sprünge" machen, dass sie also keine Werte „auslassen“, kann man (zumindest im Reellen) folgendermaßen präzisieren.

Satz 25.3

Zwischenwertsatz
Ist $f\colon [a,b] \to \mathbb{R}$ stetig (wobei $a < b$ gelten soll), so gibt es für alle Zahlen d zwischen $f(a)$ und $f(b)$ ein $c \in [a,b]$ mit $f(c) = d$.

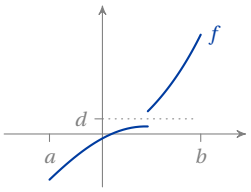
Beweis. O. B. d. A. können wir $f(a) < d < f(b)$ annehmen.[2] Wir betrachten die Menge $C = \{x \in [a,b] : f(x) < d\}$. Wegen $a \in C$ und $C \subseteq [a,b]$ besitzt diese Menge ein Supremum c, weil $\mathbb{R}$ vollständig angeordnet ist. Es gibt also eine Folge (x_n) von

[2] Für $f(b) < d < f(a)$ verläuft der Beweis analog und für $d = f(a)$ oder $d = f(b)$ ist er trivial.

Elementen von C, die gegen c konvergiert. Wegen der Stetigkeit konvergiert $(f(x_n))$ gegen $f(c)$ und mit Lemma 19.6 folgt $f(c) \leq d$.

Wegen $d < f(b)$ gilt $c \neq b$ und damit $c < b$. Für alle $x \in (c, b]$ muss $f(x) \geq d$ nach Wahl von c gelten. Und in $(c, b]$ gibt es Folgen, die gegen c konvergieren und mit denen man wie eben $f(c) \geq d$ begründen kann. ■

Die folgende Skizze zeigt, wie eine Funktion f eine Zahl d „überspringt“, sie also nicht als Funktionswert annimmt, obwohl d zwischen $f(a)$ und $f(b)$ liegt. Bei stetigen Funktionen kann so etwas nicht passieren.



⋆**Aufgabe 25.3**. Man kann den Zwischenwertsatz auch so formulieren: Das stetige Bild eines Intervalls ist ein Intervall. Begründen Sie, warum diese Aussage aus Satz 25.3 folgt.

Bisektion

Der Zwischenwertsatz sichert für viele Gleichungen die Existenz einer Lösung und liefert gleichzeitig ein Verfahren, um Näherungswerte für so eine Lösung zu bestimmen, das man *Bisektion* nennt:

- Jede Gleichung mit einer Unbekannten x lässt sich so umformen, dass auf einer Seite der Gleichung 0 steht. Interpretiert man die andere Seite als Funktion f von x, so bekommt die Gleichung die Form $f(x) = 0$. Beim Lösen der Gleichung geht es also darum, eine Nullstelle von f zu finden.
- Ist f auf einem Intervall $[a_0, b_0]$ definiert und stetig und haben $f(a_0)$ und $f(b_0)$ unterschiedliche Vorzeichen, so gibt es nach dem Zwischenwertsatz eine Zahl $c \in (a_0, b_0)$ mit $f(c) = 0$. Damit ist schon einmal klar, dass eine Lösung existiert.
- Nun setzt man $c_0 = (a_0 + b_0)/2$ und berechnet $f(c_0)$. Gilt $f(c_0) = 0$, so ist man fertig. Das ist allerdings sehr unwahrscheinlich. Anderenfalls haben aber entweder a_0 und c_0 oder c_0 und b_0 unterschiedliche Vorzeichen. Man kann dann $[a_0, b_0]$ durch $[a_0, c_0]$ oder $[c_0, b_0]$ ersetzen, dieses neue Intervall $[a_1, b_1]$ nennen und den Vorgang wiederholen, indem man die Mitte c_1 von $[a_1, b_1]$ berechnet. Und so weiter.
- Damit erhält man eine Folge (c_n), die offenbar gegen eine Nullstelle von f konvergiert. In der Praxis wird man nach endlich vielen Schritten aufhören, wenn der Abstand zwischen den Intervallgrenzen so gering ist, dass man mit der Genauigkeit der Näherung zufrieden ist.

Für die Gleichung $x^5 + 1 = x$, für die es übrigens keine Lösungsformel gibt, wäre f die durch $f(x) = x^5 - x + 1$ definierte Funktion. Es gilt $f(-2) = -29$ und $f(2) = 31$. Mit den Startwerten -2 und 2 würden die ersten Schritte so aussehen:

k	a_k	b_k
0	-2	2
1	-2	0
2	-2	-1
3	-1.5	-1
4	-1.25	-1
5	-1.25	-1.125
6	-1.1875	-1.125
7	-1.1875	-1.15625
8	-1.171875	-1.15625
9	-1.171875	-1.1640625
10	-1.16796875	-1.1640625
11	-1.16796875	-1.166015625
12	-1.16796875	-1.1669921875
13	-1.16748046875	-1.1669921875
14	-1.16748046875	-1.167236328125
15	-1.1673583984375	-1.167236328125

Eine Lösung der Gleichung[3] liegt also zwischen a_{15} und b_{15}.

Aufgabe 25.4. Greifen Sie sich einen Taschenrechner und rechnen Sie zumindest die ersten Zeilen der obigen Tabelle nach, um sicherzustellen, dass Sie das Verfahren verstanden haben.

Aufgabe 25.5. Wenn man wie in diesem Beispiel bis zum 15. Schritt gerechnet hat, wie viele Nachkommastellen der Lösung sollte man dann angeben?

Aufgabe 25.6. Berechnen Sie mit dem Bisektionsverfahren eine Näherung für die reelle Lösung der Gleichung $x^5 + 2x^2 = x + 8$ auf zwei Stellen nach dem Komma.

⋆**Aufgabe 25.7**. Programmieren Sie das Bisektionsverfahren in einer Programmiersprache Ihrer Wahl.

Aufgabe 25.8. Von einer Funktion $f\colon \mathbb{R} \to \mathbb{R}$ weiß man lediglich, dass sie stetig ist und dass $f(1/k) = (-2)^k$ für alle $k \in [5]$ gilt. Wie viele Nullstellen muss f mindestens haben?

Eine weitere Interpretation der Stetigkeit, die insbesondere für Anwendungen hilfreich ist, ist die, dass bei einer stetigen Funktion kleine Änderungen des Arguments auch nur kleine Änderungen des Funktionswertes bewirken.

Lemma 25.4

Sei $f\colon A \to \mathbb{C}$ mit $A \subseteq \mathbb{C}$. f ist genau dann stetig an der Stelle $a \in A$, wenn für alle $\varepsilon > 0$ ein $\delta > 0$ existiert, so dass $|f(a) - f(x)| < \varepsilon$ für alle $x \in U_\delta(a) \cap A$ gilt.

Beweis. Wir führen für beide Richtungen der Äquivalenz einen indirekten Beweis.

[3] Es gibt insgesamt fünf, aber die anderen vier sind echt komplex.

Ist f *nicht* stetig in a, dann gibt es eine gegen a konvergierende Folge (a_n) in A, so dass $(f(a_n))$ nicht gegen $f(a)$ konvergiert. Das bedeutet, dass es für mindestens ein $\varepsilon > 0$ unendlich viele Folgenglieder a_n gibt, für die $|f(a_n) - f(a)| \geq \varepsilon$ gilt. Weil in jeder δ-Umgebung von a fast alle Folgenglieder liegen, kann man also kein δ wie in der Formulierung des Lemmas finden.

Für die andere Richtung ist es evtl. hilfreich, sich die Aussage, um die es geht, mit Quantoren aufzuschreiben:

$$\forall \varepsilon \in (0,\infty)\ \exists \delta \in (0,\infty)\ \forall x \in A \left(x \in U_\delta(a) \Rightarrow f(x) \in U_\varepsilon(f(a))\right)$$

Negiert man diese mithilfe der de-morganschen Regeln, so heißt das, dass es ein $\varepsilon > 0$ gibt, so dass man für alle $\delta > 0$ ein $x \in A \cap U_\delta(a)$ finden kann, für das $f(x)$ nicht in $U_\varepsilon(f(a))$ liegt. Zu diesem ε kann man nun einfach für jede positive natürliche Zahl ein entsprechendes x zu $\delta = 1/n$ auswählen und es a_n nennen. Dann hat man eine Folge (a_n) konstruiert, die $\lim_{x\to a} f(x) = f(a)$ widerlegt. ■

Ein weiteres Beispiel für eine stetige Funktion ist die komplexe Konjugation: Offensichtlich gilt $|\overline{z}| = \sqrt{z\overline{z}} = |z|$ für alle $z \in \mathbb{C}$ und damit $|\overline{z} - \overline{w}| = |\overline{z - w}| = |z - w|$ für alle $z, w \in \mathbb{C}$. (Siehe Lemma 17.5.) Man kann also in Lemma 25.4 einfach $\delta = \varepsilon$ nehmen.

Definition

Ist $(a_n)_{n\in\mathbb{N}}$ eine beliebige Folge und $(n_k)_{k\in\mathbb{N}}$ eine streng monotone Folge von natürlichen Zahlen, dann nennt man $(a_{n_k})_{k\in\mathbb{N}}$ eine **Teilfolge** von $(a_n)_{n\in\mathbb{N}}$.

Beispielsweise sind $(2n)$ und $(2n+1)$ Teilfolgen von (n) – und (n) selbst ist auch eine. $(1/p)_{p\in\mathbb{P}}$ (also $1/2, 1/3, 1/5, 1/7, 1/11, \ldots$) ist eine Teilfolge der harmonischen Folge.

Eine Folge hat also genau dann einen Häufungspunkt, wenn sie eine Teilfolge hat, die gegen diesen Punkt konvergiert. Den Satz von Bolzano-Weierstraß kann man dann mit anderen Worten auch so formulieren, dass jede beschränkte Folge reeller Zahlen eine konvergente Teilfolge hat.

Satz 25.5

Satz vom Minimum und Maximum
Ist $f\colon [a,b] \to \mathbb{R}$ stetig (wobei $a < b$ gelten soll), so ist der Wertebereich $\operatorname{rng}(f)$ von f beschränkt und hat ein Minimum und ein Maximum.

Beweis. Wäre $\operatorname{rng}(f)$ nicht nach oben beschränkt, so gäbe es eine Folge (x_n) in $[a,b]$ mit $\lim_{n\to\infty} f(x_n) = \infty$. (x_n) müsste nach dem Satz von Bolzano-Weierstraß jedoch eine konvergente Teilfolge (x_{n_k}) mit einem Grenzwert x^* in $[a,b]$ haben. Wegen der Stetigkeit müsste $(f(x_{n_k}))$ aber gegen $f(x^*)$ konvergieren. Das ist ein Widerspruch zur bestimmten Divergenz von $(f(x_n))$.

$\operatorname{rng}(f)$ hat also ein Supremum S, weil $\mathbb{R}$ vollständig angeordnet ist. Daher gibt es eine Folge (y_n) in $\operatorname{rng}(f)$, die gegen S konvergiert. Zu jedem $n \in \mathbb{N}$ muss es wegen $y_n \in \operatorname{rng}(f)$ ein $x_n \in [a,b]$ mit $y_n = f(x_n)$ geben. Wir können wieder den Satz

von Bolzano-Weierstraß anwenden und erhalten eine Teilfolge (x_{n_k}) mit einem Grenzwert $x^* \in [a,b]$. $(f(x_{n_k}))$ ist dann eine Teilfolge von (y_n) und wegen der Stetigkeit folgt $S = f(x^*)$ und damit $S \in \operatorname{rng}(f)$.

Die Beschränktheit nach unten und die Existenz eines Minimums zeigt man natürlich völlig analog. ■

Die beiden folgenden Beispiele demonstrieren, dass die Aussage des Satzes vom Minimum und Maximum nicht selbstverständlich ist:

$$f\colon \begin{cases} [0,2] \to \mathbb{R} \\ x \mapsto \begin{cases} x & x \in [0,1) \\ 1/2 & x \in [1,2] \end{cases} \end{cases} \qquad g\colon \begin{cases} (0,1) \to \mathbb{R} \\ x \mapsto 1/x \end{cases}$$

f ist zwar auf einem abgeschlossenen und beschränkten Intervall definiert, aber nicht stetig. $\operatorname{rng}(f)$ hat kein Maximum. g ist zwar stetig und auf einem beschränkten Intervall definiert, aber das Intervall ist nicht abgeschlossen. $\operatorname{rng}(g)$ ist unbeschränkt und hat weder Maximum noch Minimum.

Zum Abschluss dieses Abschnitts noch eine Bemerkung über den Zusammenhang zwischen Grenzwerten und der Komposition von Funktionen.

Lemma 25.6 Sei $g\colon A \to \mathbb{C}$ mit $A \subseteq \mathbb{C}$ und $a \in \overline{A}$, so dass der Grenzwert L von g an der der Stelle a existiert. Ferner sei $f\colon B \to \mathbb{C}$ stetig mit $g[A] \subseteq B$ und $L \in \overline{B}$, so dass der Grenzwert von f an der Stelle L existiert. Dann gilt

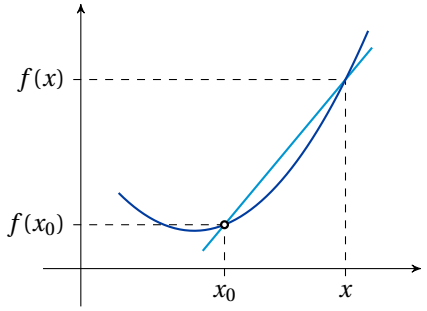
$$\lim_{x \to a} f(g(x)) = \lim_{y \to L} f(y). \tag{25.2}$$

Beweis. Sei (a_n) eine Folge in A mit $a_n \to a$. Nach der Voraussetzung über g konvergiert $(g(a_n))$ gegen L. Da alle Glieder von $(g(a_n))$ in B liegen, konvergiert $(f(g(a_n)))$ gegen die rechte Seite von (25.2). ■

Insbesondere ist unter den Voraussetzungen von Lemma 25.6 $f \circ g$ in a stetig, wenn g in a stetig und f in L stetig ist. Das bedeutet, dass die Funktion $f \circ g$ stetig ist, wenn f und g stetig sind.

26. Differenzierbare Funktionen

Die Idee der Ableitung ist (in Kombination mit der des Integrals) die wohl wichtigste Innovation der letzten tausend Jahre in der Mathematik. Motivieren kann man diese Idee dadurch, dass man an den Funktionsgraphen einer Funktion f im Punkt $(x_0, f(x_0))$ eine Tangente anlegen will, deren Steigung man ermitteln möchte.



Die in der Skizze eingezeichnete Gerade hat die Steigung $(f(x)-f(x_0))/(x-x_0)$. Sie ist *nicht* die Tangente, aber es sieht so aus, als würde man nach und nach bessere Näherungswerte für die Steigung der Tangente erhalten, wenn x näher an x_0 heranrückt.

Definition

Sei $f\colon A\to\mathbb{R}$ mit $A\subseteq\mathbb{R}$ und x_0 ein innerer Punkt von A. f ist **differenzierbar** an der Stelle a wenn der Grenzwert[4]

$$\lim_{x\to x_0}\frac{f(x)-f(x_0)}{x-x_0} \tag{26.1}$$

existiert. Für diesen Grenzwert schreibt man dann

$$\frac{df}{dx}(x_0)\quad\text{oder}\quad\frac{d}{dx}f(x_0)\quad\text{oder}\quad\frac{df(x)}{dx}\Big|_{x=x_0}$$

und nennt ihn die **Ableitung** bzw. den **Differentialquotienten** von f an der Stelle x_0. Ist klar, welche Variable gemeint ist, so verwendet man für die Ableitung auch die Kurzschreibweise $f'(x_0)$. Analog definiert man Differenzierbarkeit für den Fall, dass oben an beiden Stellen $\mathbb{R}$ durch $\mathbb{C}$ ersetzt wird.

Wie bei der Stetigkeit spricht man auch von der Differenzierbarkeit auf einer Menge von Punkten bzw. von der Differenzierbarkeit einer Funktion, wenn diese in jedem Punkt ihres Definitionsbereichs differenzierbar ist. (Dabei ist jedoch zu beachten, dass es um innere Punkte geht. Die Mengen müssen daher offen sein.)

Der geniale „Trick“ bei dieser Definition ist, dass die Funktion in (26.1) an der Stelle $x=x_0$ nicht definiert ist (weil sonst durch null dividiert würde).

Durch simples Einsetzen in die Definition kann man sich überzeugen, dass konstante Funktionen überall differenzierbar mit der Ableitung 0 sind. Ebenso ist die Identität überall differenzierbar mit der Ableitung 1.

Aufgabe 26.1. Rechnen Sie anhand der Definition nach, dass die obigen Aussagen über konstante Funktionen und die Identität korrekt sind.

[4] Wohlgemerkt ist hier eine *Zahl* und nicht etwa ∞ gemeint!

Aufgabe 26.2. Berechnen Sie nur mithilfe der obigen Definition (also ohne die Verwendung Ihres Vorwissens aus der Schule) die Ableitung der Funktion $x \mapsto x^2$ an der Stelle x_0. (Hinweis: Dritte binomische Formel.)

Konvention

Um Schreibarbeit zu sparen, sollen im Folgenden die Funktionen, um die es geht, immer solche sein, die reelle auf reelle oder komplexe auf komplexe Zahlen abbilden. Bei den Stellen, an denen differenziert wird, soll es zudem immer um innere Punkte des Definitionsbereichs gehen.

Lemma 26.1

Sind f und g an der Stelle x_0 differenzierbar und ist λ eine Konstante, so sind auch $f \pm g$ und λf an dieser Stelle differenzierbar und für die Ableitungen gilt $(f \pm g)'(x_0) = f'(x_0) \pm g'(x_0)$ und $(\lambda f)'(x_0) = \lambda f'(x_0)$.

Beweis. Das folgt direkt aus den Rechenregeln für Grenzwerte (Lemma 25.1). Zum Beispiel gilt

$$\begin{aligned}\lim_{x\to x_0} \frac{(f+g)(x)-(f+g)(x_0)}{x-x_0} &= \lim_{x\to x_0} \frac{f(x)+g(x)-(f(x_0)+g(x_0))}{x-x_0}\\ &= \lim_{x\to x_0}\Big(\frac{f(x)-f(x_0)}{x-x_0} - \frac{g(x)-g(x_0)}{x-x_0}\Big)\\ &= \lim_{x\to x_0} \frac{f(x)-f(x_0)}{x-x_0} - \lim_{x\to x_0} \frac{g(x)-g(x_0)}{x-x_0}.\end{aligned}$$

∎

Damit erhält man beispielsweise, dass die Funktion $x \to 3x+5$ überall differenzierbar mit der Ableitung 3 ist.

Lemma 26.2

f ist genau dann in x_0 differenzierbar, wenn es eine in einer Umgebung U von x_0 stetige Funktion r mit $r(x_0) = 0$ und eine Konstante L gibt, so dass

$$f(x) = f(x_0) + L(x-x_0) + r(x)(x-x_0) \tag{26.2}$$

für alle $x \in U$ gilt. Ist diese Bedingung erfüllt, so ist L die eindeutig bestimmte Ableitung von f an der Stelle x_0.

Beweis. Gleichung (26.2) kann man für $x \neq x_0$ zu

$$r(x) = \frac{f(x)-f(x_0)}{x-x_0} - L \tag{26.3}$$

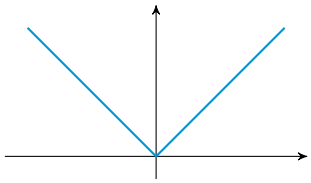
umformen. Ist f in x_0 differenzierbar und setzt man $L = f'(x_0)$, so liefert (26.3) eine Funktion r mit den gewünschten Eigenschaften. Ist umgekehrt r stetig in x_0 mit $r(x_0) = 0$, so folgt aus (26.3) die Differenzierbarkeit von f in x_0, wenn man x gegen x_0 gehen lässt. ∎

Die Bedeutung von Lemma 26.2 ist, dass sich f an der Stelle x_0 im Wesentlichen wie die Gerade $f(x_0) + L(x-x_0)$ mit der Steigung $L = f'(x_0)$ verhält. (Und diese Gerade

ist natürlich die am Anfang des Abschnitts erwähnte Tangente.) Die Abweichung von dieser Geraden ist so gering, dass ihr Verhältnis zu $x - x_0$ gegen null geht, wenn x sich x_0 nähert. Anschaulich kann man sich das so vorstellen, dass differenzierbare Funktionen „unter dem Mikroskop wie Geraden aussehen“. Grafisch wird dies in dem Video *Die Ableitung unter dem Mikroskop* demonstriert.

Aufgabe 26.3. Geben Sie die Gleichung für die Tangente an den Funktionsgraphen von $x \mapsto x^2$ an der Stelle $x_0 = -1$ an.

Ein Beispiel für eine nicht überall differenzierbare Funktion ist die Betragsfunktion $x \mapsto |x|$. An der Stelle $x_0 = 0$ ist diese Funktion nicht differenzierbar, denn der Quotient $(|x| - |0|)/(x - 0)$ ist positiv für $x > 0$ und negativ für $x < 0$. Darum würde man mit den Folgen $(1/n)$ und $(-1/n)$, die beide gegen 0 konvergieren, unterschiedliche Grenzwerte erhalten, wenn man sie in diesen Quotienten einsetzen würde. Man „sieht“ ja auch, dass es an dieser Stelle keine eindeutige Tangente gibt.



Lemma 26.2 liefert „nebenbei“ einen wichtigen Zusammenhang zwischen Differenzierbarkeit und Stetigkeit.

Korollar 26.3 Ist f an der Stelle x_0 differenzierbar, dann ist f dort auch stetig.

Beweis. Das folgt sofort aus Gleichung (26.2), denn die rechte Seite ist aus lauter Funktionen zusammengesetzt, die in x_0 stetig sind. ■

Man beachte, dass die Betragsfunktion stetig ist. Stetigkeit folgt also aus der Differenzierbarkeit, aber nicht umgekehrt. (Sonst wäre es ja auch sinnlos, zwei verschiedene Begriffe zu verwenden.) Man kann sogar mit entsprechendem Aufwand Funktionen konstruieren, die *überall* stetig und *nirgends* differenzierbar sind. Beispiele dafür finden Sie in dem Video *Die Monster der Analysis*.

Damit können wir nun weitere Ableitungsregeln beweisen.

Satz 26.4 **Leibniz- bzw. Produktregel**
Sind f und g an der Stelle x_0 differenzierbar, so ist auch ihr Produkt fg an dieser Stelle differenzierbar und es gilt $(fg)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0)$.

Beweis. Nutzt man die Stetigkeit einer der beiden Funktionen und die Rechenregeln für Grenzwerte aus, so braucht man lediglich einen „Trick“, den wir schon öfter gesehen haben, und erhält

$$\lim_{x \to x_0} \frac{(fg)(x) - (fg)(x_0)}{x - x_0} = \lim_{x \to x_0} \frac{f(x)g(x) - f(x_0)g(x_0)}{x - x_0}$$

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

$$
\begin{aligned}
&= \lim_{x\to x_0} \frac{f(x)g(x) - f(x_0)g(x) + f(x_0)g(x) - f(x_0)g(x_0)}{x - x_0} \\
&= \lim_{x\to x_0} \frac{f(x)g(x) - f(x_0)g(x)}{x - x_0} + \lim_{x\to x_0} \frac{f(x_0)g(x) - f(x_0)g(x_0)}{x - x_0} \\
&= \lim_{x\to x_0} g(x) \cdot \frac{f(x) - f(x_0)}{x - x_0} + \lim_{x\to x_0} f(x_0) \cdot \frac{g(x) - g(x_0)}{x - x_0} \\
&= g(x_0) \cdot f'(x_0) + f(x_0) \cdot g'(x_0).
\end{aligned}
$$

■

Aufgabe 26.4. Berechen Sie die Ableitung von $x \mapsto x^2$ erneut (siehe Aufgabe 26.2), indem Sie diesmal x^2 als Produkt $x \cdot x$ interpretieren und die Leibnizregel anwenden.

Aufgabe 26.5. Beweisen Sie mit vollständiger Induktion und mithilfe der Leibnizregel, dass für alle $n \in \mathbb{N}$ die Ableitung von $x \mapsto x^n$ an der Stelle x_0 den Wert nx_0^{n-1} hat.

Aufgabe 26.6. Mit Aufgabe 26.5 und Lemma 26.1 können wir nun jedes Polynom differenzieren. Wie sieht z. B. die Ableitung von $x \mapsto 3x^3 - 5x^2 + 8x - 2$ an der Stelle x_0 aus?

Definition

Ist die Funktion f auf der Menge A differenzierbar, so bezeichnet man die Funktion f', die jedem $x_0 \in A$ die Ableitung $f'(x_0)$ zuordnet, als **Ableitungsfunktion** oder manchmal auch einfach als **Ableitung** von f. Ist f' an der Stelle $x_0 \in A$ ebenfalls differenzierbar, so sagt man, dass f dort **zweimal differenzierbar** ist, und schreibt für diese sogenannte *zweite Ableitung*

$$f''(x_0) \quad \text{oder} \quad \frac{d^2 f}{dx^2}(x_0) \quad \text{oder} \quad \frac{d^2}{dx^2} f(x_0) \quad \text{oder} \quad \frac{d^2 f(x)}{dx^2}\Big|_{x=x_0}.$$

Entsprechend werden auch n-te Ableitungen definiert, für die man entweder $f^{(n)}$ schreibt oder eine der obigen Schreibweisen (mit n statt 2) verwendet. Ist eine Funktion n-mal differenzierbar für *alle* $n \in \mathbb{N}$, so spricht man auch von einer **glatten** Funktion.

Aufgabe 26.7. Geben Sie für das Polynom aus Aufgabe 26.6 die ersten vier Ableitungsfunktionen an. Wie sieht die 42. Ableitung aus?

Aufgabe 26.8. Berechnen Sie für die Funktion $f(x) = (x^2 + 3)(x^3 - x)$ die Ableitungsfunktion auf zwei Arten: einmal durch Anwendung der Leibnizregel auf das Produkt der beiden Terme und einmal, indem Sie ausmultiplizieren und das resultierende Polynom ableiten. Kommt in beiden Fällen dasselbe heraus?

Satz 26.5

Kehrwertregel
Ist f an der Stelle x_0 differenzierbar und gilt $f(x_0) \neq 0$, so ist auch der Kehrwert $1/f$ an dieser Stelle differenzierbar und es gilt $(1/f)'(x_0) = -f'(x_0)/f(x_0)^2$.

Beweis. Das ist eine simple Rechenaufgabe, bei der man lediglich geeignet erweitern muss:

$$\lim_{x\to x_0} \frac{\frac{1}{f(x)} - \frac{1}{f(x_0)}}{x - x_0} = \lim_{x\to x_0} \frac{\frac{f(x_0)-f(x)}{f(x)f(x_0)}}{x - x_0}$$
$$= \lim_{x\to x_0} \frac{1}{f(x)f(x_0)} \cdot \frac{f(x_0) - f(x)}{x - x_0} = \frac{1}{f(x_0)f(x_0)} \cdot \big(-f'(x_0)\big)$$ ■

Aufgabe 26.9. Berechnen Sie mit der Kehrwertregel die Ableitung von $f(x) = x^{-3}$.

Aufgabe 26.10. Begründen Sie, dass die Regel aus Aufgabe 26.5 auch dann noch gilt, wenn n eine beliebige ganze Zahl ist.

Korollar 26.6

Quotientenregel
Sind f und g an der Stelle x_0 differenzierbar und gilt $g(x_0) \neq 0$, so ist auch der Quotient f/g an dieser Stelle differenzierbar und es gilt

$$(f/g)'(x_0) = \frac{f'(x_0)g(x_0) - f(x_0)g'(x_0)}{g(x_0)^2}.$$

Beweis. Man wendet die Leibnizregel auf das Produkt aus f und $1/g$ an und berechnet die Ableitung des zweiten Faktors mit der Kehrwertregel. ■

Aufgabe 26.11. Es kann sicher nicht schaden, wenn Sie den Beweis von Korollar 26.6 noch einmal nachrechnen und ihn nicht einfach glauben.

Aufgabe 26.12. Berechnen Sie die Ableitung von $f(x) = (x^2 + 2x + 2)/(3x^2 - 2)$.

Aufgabe 26.13. Wenn Sie sich selbst ähnliche Aufgaben stellen und Ihre Lösungen überprüfen wollen, können Sie z. B. in Wolfram Alpha so etwas wie

```
derivative of (x^2+2x+2)/(3x^2-2)
```

eingeben. Wenn das System Terme nicht ausmultipliziert (wie in diesem Fall den Nenner), dann können Sie es mit einer Eingabe wie

```
expand (3x^2-2)^2
```

dazu „zwingen“.

Die folgende Aussage ist vielen durch die Merkregel „äußere mal innere Ableitung“ bekannt.

Satz 26.7

Kettenregel
Sei g an der Stelle x_0 differenzierbar und f an der Stelle $g(x_0)$. Dann ist $f \circ g$ an der Stelle x_0 differenzierbar und es gilt $(f \circ g)'(x_0) = f'(g(x_0))g'(x_0)$.

Beweis. Man erweitert und wendet Lemma 25.6 sowie die Stetigkeit von g an der Stelle x_0 (nach Korollar 26.3) an:

$$\lim_{x\to x_0}\frac{f(g(x))-f(g(x_0))}{x-x_0}=\lim_{x\to x_0}\frac{f(g(x))-f(g(x_0))}{g(x)-g(x_0)}\cdot\frac{g(x)-g(x_0)}{x-x_0}$$
$$=g'(x_0)\cdot\lim_{y\to g(x_0)}\frac{f(y)-f(g(x_0))}{y-g(x_0)}=g'(x_0)\cdot f'(g(x_0)).$$ ■

Aufgabe 26.14. Berechnen Sie die Ableitung von $h(x)=(3x^2-5x+2)^4$ mithilfe der Kettenregel. Sie sollen dabei weder $h(x)$ noch $h'(x)$ ausmultiplizieren.

Satz 26.8

Umkehrregel

Sei f an der Stelle x_0 differenzierbar mit $f'(x_0)\neq 0$. Ist f injektiv und die Umkehrabbildung f^{-1} stetig an der Stelle $f(x_0)$, dann ist sie an dieser Stelle auch differenzierbar mit der Ableitung

$$(f^{-1})'(f(x_0))=\frac{1}{f'(x_0)}, \tag{26.4}$$

die man auch als

$$(f^{-1})'(y_0)=\frac{1}{f'(f^{-1}(y_0))} \tag{26.5}$$

mit $y_0=f(x_0)$ schreiben kann.

Beweis. Einen ausführlichen Beweis findet man beispielsweise in dem Video *Der Satz über implizite Funktionen und der lokale Umkehrsatz*. An dieser Stelle zeige ich ersatzweise nur ein einfaches Plausibilitätsargument für (26.4), bei dem bereits vorausgesetzt wird, dass f^{-1} differenzierbar ist.

Weil f^{-1} die Umkehrfunktion von f ist, ist $f^{-1}\circ f$ die Identität, deren Ableitung konstant eins ist. Ist f^{-1} differenzierbar, so gilt somit nach der Kettenregel $(f^{-1})'(f(x_0))f'(x_0)=1$. Teilt man nun durch die Ableitung von f an der Stelle x_0, die nach Voraussetzung nicht verschwindet, so erhält man den gewünschten Zusammenhang. ■

Für Funktionen, die komplexe auf komplexe Zahlen abbilden, reicht es übrigens, wenn f auf einer offenen Menge U differenzierbar und x_0 ein Element von U mit $f'(x_0)\neq 0$ ist. Existenz und Stetigkeit der Umkehrfunktion ergeben sich dann automatisch. Das gilt ebenfalls für reelle Funktionen, wenn die Ableitungsfunktion zusätzlich stetig ist.

Aufgabe 26.15. Für $n\in\mathbb{N}^+$ ist durch $f(x)=x^n$ eine auf dem Intervall $(0,\infty)$ streng monoton steigende (und damit nach Aufgabe 21.20 injektive) Funktion definiert, deren Umkehrfunktion die n-te Wurzelfunktion $f^{-1}(x)=\sqrt[n]{x}$ ist, die ebenfalls auf $(0,\infty)$ definiert ist. Geben Sie mithilfe der Umkehrregel die Ableitung von f^{-1} an.

Aufgabe 26.16. Schreiben Sie, falls Sie das nicht bereits gemacht haben, Aufgabe 26.15 und deren Lösung so um, dass statt Wurzeln nur noch Potenzen vorkommen.

Lemma 26.9 Für alle $q \in \mathbb{Q}$ ist die auf $(0,\infty)$ definierte Funktion $x \mapsto x^q$ differenzierbar mit der Ableitung qx^{q-1}.

Beweis. Die wesentliche Arbeit wurde mit den Aufgaben 26.10 und 26.16 bereits erledigt. Man muss sie nur noch mit der Kettenregel verbinden. Sei $q \in \mathbb{Q}$ dazu der Bruch z/n mit $z \in \mathbb{Z}$ und $n \in \mathbb{N}^+$. Für die Ableitung von $f(x) = x^q = (x^{1/n})^z$ gilt dann

$$\begin{aligned} f'(x) &= z \cdot (x^{1/n})^{z-1} \cdot \frac{1}{n} \cdot x^{1/n-1} = \frac{z}{n} \cdot x^{z/n-1/n} \cdot x^{1/n-1} \\ &= \frac{z}{n} \cdot x^{z/n-1} = qx^{q-1}. \end{aligned}$$

■

Mit den Regeln aus diesem Abschnitt wissen Sie über das Ableiten elementarer Funktionen mehr oder weniger alles, was man wissen muss. Und mithilfe der besagten Regeln wird Differenzieren (leider) zu einem mechanischen Vorgang, den man ohne Nachdenken durchführen kann. Mehr dazu im Video *Wie man Computern das Ableiten beibringt*.

27. Potenzreihen

Die einfachsten Funktionen, mit denen man es in Anwendungen zu tun haben kann, sind zweifelsohne die Polynome. Die Funktionen, um die es im Folgenden gehen wird, sind so etwas wie „unendliche Polynome“. Sie haben viele angenehme Eigenschaften und verhalten sich häufig so ähnlich wie Polynome.

Definition

Ist (a_n) eine Folge komplexer Zahlen, so bezeichnet man eine Funktion wie

$$: \begin{cases} A \to \mathbb{C} \\ z \mapsto \sum_{n=0}^{\infty} a_n z^n \end{cases}$$

als **Potenzreihe**, wenn $A \subseteq \mathbb{C}$ derart gewählt ist, dass die Reihe $\sum_{n=0}^{\infty} a_n z^n$ für alle $z \in A$ konvergiert. Die Glieder der Folge (a_n) nennt man die **Koeffizienten** der Potenzreihe.

Die Menge, die in dieser Definition A heißt, kann, wie sich nun herausstellen wird, im Komplexen immer eine kreisförmige Gestalt haben (bzw. im Reellen ein Intervall sein).

Lemma 27.1 Ist (a_n) eine Folge komplexer Zahlen und q eine komplexe Zahl, für die $\sum_{n=0}^{\infty} a_n q^n$ konvergiert, dann konvergiert $\sum_{n=0}^{\infty} a_n b^n$ absolut für alle $b \in \mathbb{C}$ mit $|b| < |q|$.

Beweis. Nach dem Nullfolgenkriterium ist $(a_n q^n)$ eine Nullfolge. Also gilt $|a_n q^n| \leq 1$ für fast alle n. Für $|b| < |q|$ folgt damit

$$|a_n b^n| = |a_n q^n| \cdot |b/q|^n \leq |b/q|^n$$

für fast alle n. Wegen $|b/q| < 1$ konvergiert die geometrische Reihe $\sum_{n=0}^{\infty} |b/q|^n$ nach Satz 21.8 und nach dem Majorantenkriterium konvergiert damit die Reihe $\sum_{n=0}^{\infty} a_n b^n$ absolut. ■

Korollar 27.2

Ist (a_n) eine Folge komplexer Zahlen, so konvergiert die Reihe $\sum_{n=0}^{\infty} a_n z^n$ entweder für alle $z \in \mathbb{C}$ absolut oder es gibt ein $\rho \in \mathbb{R}_{\geq 0}$, so dass diese Reihe für alle $z \in \mathbb{C}$ mit $|z| < \rho$ absolut konvergiert und für alle $z \in \mathbb{C}$ mit $|z| > \rho$ divergiert.

Beweis. Sei A die Menge der nichtnegativen reellen Zahl r, für die die Reihe für alle $z \in \mathbb{C}$ mit $|z| < r$ konvergiert. Trivialerweise gilt $0 \in A$ und nach Lemma 27.1 ist A ein Intervall. Ist A unbeschränkt, so konvergiert die Reihe also (absolut) für alle $z \in \mathbb{C}$. Ist A beschränkt, so existiert das Supremum ρ von A, das den zweiten Teil der Aussage des Korollars erfüllt. ■

Konvergenzradius

Die Zahl ρ aus Korollar 27.2 wird als *Konvergenzradius* der Potenzreihe $\sum_{n=0}^{\infty} a_n z^n$ bezeichnet. Konvergiert die Reihe für alle $z \in \mathbb{C}$, so sagt man, dass der Konvergenzradius unendlich ist.

Man beachte, dass Korollar 27.2 nichts über die Zahlen aussagt, deren Absolutbetrag genau ρ ist. Dass das Verhalten der Reihe für solche Werte durch den Konvergenzradius tatsächlich nicht bestimmt wird, zeigen Beispiele auf der Wikipedia-Seite zum Konvergenzradius.

In gewissem Sinne darf man Potenzreihen wie „unendliche Polynome“ differenzieren, also jeden „Summanden“ einzeln:

Satz 27.3

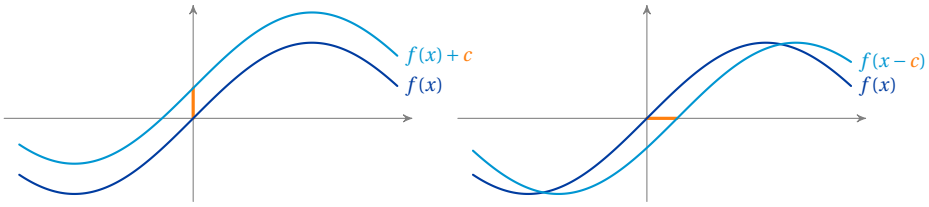
Wenn die Potenzreihe $f(z) = \sum_{n=0}^{\infty} a_z z^n$ einen Konvergenzradius ρ hat, der nicht null ist, dann hat die Potenzreihe $g(z) = \sum_{n=1}^{\infty} n a_z z^{n-1}$ denselben Konvergenzradius und für $|z| < \rho$ ist $g(z)$ die Ableitung von f an der Stelle z.

Der Beweis für diesen Satz wird im Video *Reihen, Riemannscher Umordnungssatz und komplex-analytische Funktionen* gezeigt. Man beachte jedoch, dass es sich *nicht* um eine Anwendung von Lemma 26.1 handelt, weil dieses Lemma nur für endliche Summen anwendbar ist.

Satz 27.3 besagt also, dass konvergente Potenzreihen Funktionen liefern, die differenzierbar (und damit auch stetig) sind. Und da die Ableitung eine Potenzreihe mit demselben Konvergenzradius ist, sind solche Funktionen sogar beliebig oft differenzierbar, also glatt.

Betrachtet man statt einer Funktion f die durch $g(x) = x + c$ definierte Funktion, wobei c eine Konstante ist, dann wird der Funktionsgraph nur um c vertikal verschoben und wir würden erwarten, dass g dieselben wesentlichen Eigenschaften

wie f hat. Ebenso erhält man mit $h(x) = f(x-c)$ eine lediglich horizontal verschobene Funktion, die sich nicht grundsätzlich von f unterscheiden sollte.



Entsprechend kann man auch Potenzreihen „verschieben“.

Definition

Ist (a_n) eine Folge komplexer Zahlen und $z_0 \in \mathbb{C}$, so bezeichnet man eine Funktion wie

$$: \begin{cases} A \to \mathbb{C} \\ z \mapsto \sum_{n=0}^{\infty} a_n (z-z_0)^n \end{cases} \tag{27.1}$$

als **Potenzreihe** mit **Entwicklungspunkt** z_0, wenn $A \subseteq \mathbb{C}$ derart gewählt ist, dass die Reihe $\sum_{n=0}^{\infty} a_n (z-z_0)^n$ für alle $z \in A$ konvergiert.

Die Potenzreihen, mit denen wir uns bisher beschäftigt haben, sind in diesem Sinne einfach Spezialfälle, bei denen der Entwicklungspunkt die Zahl null ist. Und selbstverständlich übertragen sich die Aussagen aus diesem Abschnitt auch auf allgemeinere Potenzreihen. Insbesondere haben auch solche Potenzreihen einen Konvergenzradius ρ, der eine nichtnegative reelle Zahl oder ∞ sein kann. Die Menge der Zahlen, für die die Reihe mit Sicherheit konvergiert, ist dann die Menge der z, für die $|z-z_0| < \rho$ gilt, wobei z_0 der Entwicklungspunkt ist. Im Komplexen ist das für $\rho \neq \infty$ eine offene Kreisscheibe mit Radius ρ und Mittelpunkt z_0, im Reellen das Intervall $(z_0-\rho, z_0+\rho)$.

Aufgabe 27.1. Die Potenzreihe $\sum_{n=0}^{\infty} a_n (z+3)^n$ habe den Konvergenzradius 2. Was kann man über die Konvergenz der Reihe an den Stellen -4, -1, 1 und 2 sagen? Was ist mit einer komplexen Zahl wie $-3+2\mathrm{i}$?

Aufgabe 27.2. Die Potenzreihe $\sum_{n=0}^{\infty} a_n (z-2+\mathrm{i})^n$ habe den Konvergenzradius 3. Zeichnen Sie die Menge der Zahlen, für die diese Reihe auf jeden Fall konvergiert.

⋆**Aufgabe 27.3**. Wie muss man Satz 27.3 wohl für Potenzreihen der Form (27.1) formulieren?

analytisch

Funktionen, die über Potenzreihen definiert sind bzw. sich über Potenzreihen definieren lassen, nennt man *analytisch*. Die meisten Funktionen, mit denen man es in Anwendungen zu tun hat, sind analytisch. Insbesondere sind auch Polynome analytisch, denn bei ihnen handelt es sich um Potenzreihen, bei denen fast alle Koeffizienten verschwinden. Auch rationale Funktionen und Wurzelfunktionen sind beispielsweise analytisch, haben aber nicht unbedingt Potenzreihen, die überall konvergieren. Mehr dazu im Video *Taylorpolynome* und den darauf folgenden.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

⋆ Potenzreihen im Computer

Potenzreihen sind die Erklärung dafür, dass Computer Funktionen wie den Sinus oder den Logarithmus berechnen können, die in den folgenden Abschnitten behandelt werden. Wenn Sie Informatik studieren, dann wissen Sie, dass es Gatter gibt, die die vier Grundrechenarten durchführen können. Damit kann man aber nur rationale Funktionen berechnen. Für andere Funktionen werden mithilfe von Reihen Approximationen ermittelt. Beispielsweise werden wir gleich sehen, dass die Funktion exp durch die Reihe (28.1) definiert ist. Man könnte diese Funktion in PYTHON also näherungsweise z. B. folgendermaßen berechnen:

```
from math import factorial, exp
exp1 = lambda x: sum(x**k/factorial(k) for k in range(42))

exp1(1), exp(1)
```

In der Realität ist es allerdings nicht ganz so simpel, weil natürlich erstens die Geschwindigkeit eine Rolle spielt und zweitens die Genauigkeit. Was tatsächlich „unter der Haube“ eingesetzt wird, ist in der Regel ein über viele Jahre optimierter Algorithmus. Wenn Sie ein bisschen herumspielen, werden Sie beispielsweise feststellen, dass der relative Fehler von `exp1` (im Vergleich zum „richtigen“ Wert `exp`) inakzeptabel groß wird, wenn der Betrag des Arguments deutlich größer als 1 ist. Das ließe sich mit einem kleinen Kunstgriff verbessern:

```
exp2 = lambda x: exp1(x) if abs(x)<=1 else exp2(x/2)**2
```

Trotzdem ist diese Implementation noch weit davon entfernt, wie `exp` tatsächlich realisiert ist.

28. Exponentialfunktionen und Logarithmen

Wir kommen nun zur wohl wichtigsten Funktion der gesamten Mathematik.

Definition

Die durch

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \tag{28.1}$$

für $z \in \mathbb{C}$ definierte Funktion wird **(natürliche) Exponentialfunktion** genannt. Für den Funktionswert $\exp(1)$ schreibt man e und nennt ihn die **eulersche Zahl**.

e ist übrigens eine irrationale Zahl, wie ihr Namenspate Leonhard Euler 1737 bewies. Einen kurzen Beweis dafür, den man verstehen kann, wenn man das Skript bis hier durchgearbeitet hat, finden Sie in dem Video *Die eulersche Zahl e ist irrational*.

Mit dem Quotientenkriterium erhält man sofort:

Lemma 28.1 Die Exponentialfunktion hat unendlichen Konvergenzradius, d. h., ihre Reihe konvergiert für alle $z \in \mathbb{C}$.

Aufgabe 28.1. Welchen Wert hat $\exp(0)$? Berechnen Sie mit einem Taschenrechner gemäß der Definition in (28.1) einen ungefähren Wert für e.

⋆**Aufgabe 28.2**. Führen Sie den Beweis von Lemma 28.1 aus.

Aus Satz 27.3 (rechnen Sie nach!) folgt:

Lemma 28.2 Die Funktion exp ist beliebig oft differenzierbar und ihre eigene Ableitung.

Aufgabe 28.3. Berechnen Sie die Ableitungen der beiden Funktionen $x \mapsto \exp(x^2)$ und $x \mapsto \exp(x)^2$.

Aufgabe 28.4. Durch Komposition mit der Exponentialfunktion kann man weitere Funktionen konstruieren, die ihre eigene Ableitung sind. Fallen Ihnen Beispiele ein?

Wie werden zwei endliche Summen multipliziert? Gemäß der Distributivität wird ausmultipliziert, so dass jeder Summand der einen Summe mit jedem der anderen multipliziert und alle Produkte danach addiert werden. Will man z. B.

$$(a_0 + a_1 + a_2)(b_0 + b_1 + b_2 + b_3)$$

berechnen, so kann man das systematisch als Tabelle folgendermaßen notieren:

	b_0	b_1	b_2	b_3
a_0	a_0b_0	a_0b_1	a_0b_2	a_0b_3
a_1	a_1b_0	a_1b_1	a_1b_2	a_1b_3
a_2	a_2b_0	a_2b_1	a_2b_2	a_2b_3

Wie bei Cantors Diagonalverfahren kann man diese Terme nun immer entlang der Diagonalen zusammenfassen. Allgemein ergibt sich

$$\Big(\sum_{k=0}^{m} a_k\Big) \cdot \Big(\sum_{k=0}^{n} b_k\Big) = \sum_{k=0}^{m+n} \sum_{j=0}^{k} a_j b_{k-j},$$

wobei man Faktoren der Form a_j mit $j > m$ bzw. b_i mit $i > n$ wie Nullen behandelt. Kann man das auch mit „unendlichen Summen“ machen?

Satz 28.3 Wenn die Reihen $\sum_{n=0}^{\infty} a_n$ und $\sum_{n=0}^{\infty} b_n$ absolut gegen A bzw. B konvergieren, dann konvergiert die Reihe

$$\sum_{n=0}^{\infty} \sum_{k=0}^{n} a_k b_{n-k} \tag{28.2}$$

absolut gegen AB.

Die Reihe (28.2) wird als *Cauchy-Produkt* der beiden anderen Reihen bezeichnet. Cauchy-Produkt

Einen Beweis für diesen Satz findet man z. B. auf der Wikipedia-Seite zum sogenannten Satz von Mertens (der besagt, dass es reicht, wenn eine der Reihen absolut konvergiert, solange die absolute Konvergenz des Cauchy-Produktes nicht benötigt wird). Dort findet man auch ein Beispiel dafür, dass die Aussage im Allgemeinen nicht mehr gilt, wenn beide Reihen nur bedingt konvergieren.

Für den nächsten Schritt benötigen wir ein grundlegendes algebraisches Resultat, das wir auch schon früher hätten beweisen können. Es handelt sich um eine Verallgemeinerung eines aus der Schule wohlbekannten Resultats.

Binomischer Lehrsatz **Satz 28.4**
Ist $(R,+,\cdot)$ ein kommutativer unitärer Ring, dann gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{28.3}$$

für alle $a, b \in R$ und alle $n \in \mathbb{N}$.[5]

Beweis. Formal beweist man das mittels vollständiger Induktion. (Siehe Aufgabe 28.6.) Man kann sich aber auch einfach kombinatorisch klarmachen, dass die Aussage stimmen muss: Wir haben n Faktoren, die jeweils aus den zwei Summanden a und b bestehen. Beim Ausmultiplizieren muss aus jedem Faktor einer der Summanden ausgewählt werden und alle Möglichkeiten müssen berücksichtigt werden. (Wie bei den binomischen Formeln, allerdings ggf. mit mehr als zwei Faktoren.) Da es wegen der Kommutativität der Multiplikation auf die Reihenfolge nicht ankommt, ist nur entscheidend, wie oft man a (bzw. b) ausgewählt hat. Ist k die Anzahl der as, dann bleiben $n-k$ bs übrig. Multiplikation ergibt $a^k b^{n-k}$. Nach Satz 4.7 gibt es für diese Auswahl $\binom{n}{k}$ Möglichkeiten. ■

Aufgabe 28.5. Setzen Sie in (28.3) $n = 2$ ein und verifizieren Sie, dass sich die bekannte binomische Formel ergibt. Überprüfen Sie auch die Korrektheit der Formel für $n = 1$ und schließlich für $n = 3$, indem Sie $(a+b)^3$ manuell ausmultiplizieren.

⋆**Aufgabe 28.6**. Beweisen Sie den binomischen Lehrsatz durch Induktion über n.

Aufgabe 28.7. Wenn man $(x+1)^{19}$ ausmultipliziert, ergibt sich ein Polynom $\sum_{k=0}^{19} a_k x^k$. Geben Sie den Koeffizienten a_{13} dieses Polynoms an.

Funktionalgleichung der Exponentialfunktion **Satz 28.5**
Für alle $z, w \in \mathbb{C}$ gilt $\exp(z+w) = \exp(z)\exp(w)$.

[5] Dabei ist das Summenzeichen natürlich so gemeint, dass es um die Addition im Ring R geht.

Beweis. Das folgt mit dem Cauchy-Produkt und dem binomischen Lehrsatz durch einfaches Nachrechnen:

$$\begin{aligned}\exp(z)\exp(w) &= \Big(\sum_{n=0}^{\infty}\frac{z^n}{n!}\Big)\Big(\sum_{n=0}^{\infty}\frac{w^n}{n!}\Big) = \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{z^k}{k!}\cdot\frac{w^{n-k}}{(n-k)!}\\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{n!}{n!}\cdot\frac{z^k w^{n-k}}{k!(n-k)!} = \sum_{n=0}^{\infty}\frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}z^k w^{n-k}\\ &= \sum_{n=0}^{\infty}\frac{(z+w)^n}{n!} = \exp(z+w)\end{aligned}$$

■

Funktionalgleichung

Als *Funktionalgleichung* bezeichnet man eine Gleichung, die man so interpretiert, dass die durch die Gleichung beschriebene Unbekannte eine Funktion ist. Man kann beweisen, dass die Exponentialfunktion im Wesentlichen die einzige stetige Funktion ist, die die Gleichung $f(z+w) = f(z)f(w)$ aus Satz (28.5) erfüllt.[6] Obwohl der Beweis aufgrund der Vorarbeit recht einfach ist, ist der Satz sehr wichtig, weil aus ihm viele grundlegende Eigenschaften der Exponentialfunktion gefolgert werden können.

Lemma 28.6

Für $x \in \mathbb{R}$ ist $\exp(x)$ reell und positiv. Außerdem ist $\exp|_{\mathbb{R}}$ streng monoton steigend und es gibt kein $z \in \mathbb{C}$ mit $\exp(z) = 0$.

Beweis. Hätte die Exponentialfunktion eine Nullstelle $z \in \mathbb{C}$, dann hätten wir mit der Funktionalgleichung

$$2 = 1+1 = \sum_{n=0}^{1}\frac{1^n}{n!} < \sum_{n=0}^{\infty}\frac{1^n}{n!} = \exp(1) = \exp(1-z+z) = \exp(1-z)\exp(z) = 0,$$

was offenbar ein Widerspruch ist.

Dass $\exp(x)$ für reelle x reell ist, folgt sofort aus der Definition (28.1). Mit der Funktionalgleichung folgt dann

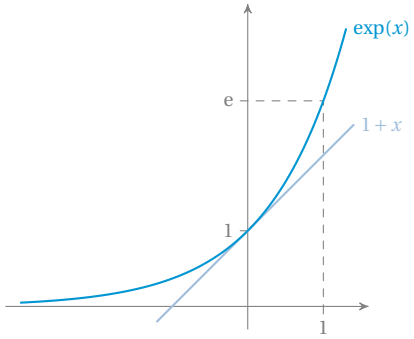
$$\exp(x) = \exp(x/2 + x/2) = \exp(x/2)^2 > 0.$$

Für $h > 0$ gilt sogar $\exp(h) > 1$, was ebenfalls direkt aus (28.1) folgt. Die Monotonie folgt damit durch $\exp(x+h) = \exp(x)\exp(h) > \exp(x)$. ■

Man kann auch $\exp(x) \geq 1 + x$ für $x \in \mathbb{R}$ zeigen, worauf wir hier verzichten. Insgesamt sieht der reelle Verlauf der Exponentialfunktion so aus wie in der folgenden Skizze. Auf der linken Seite bleibt die Kurve immer oberhalb der horizontalen Achse, nach rechts steigt sie sehr stark an.[7]

[6] Was mit „im Wesentlichen“ gemeint ist, wird bald klar werden.

[7] Nach Lemma 20.3 steigt exp stärker als jedes Polynom.



Für alle $q \in \mathbb{Q}$ und $r \in \mathbb{R}$ gilt $\exp(qr) = \exp(r)^q$. Insbesondere gilt $\exp(q) = \mathrm{e}^q$. **Satz 28.7**

Beweis. Zunächst zeigen wir $\exp(nr) = \exp(r)^n$ für alle $n \in \mathbb{N}$ mit vollständiger Induktion über n. Für $n = 0$ gilt die Aussage offensichtlich – siehe Aufgabe 28.1. Der Induktionsschluss ist dann mithilfe der Funktionalgleichung

$$\exp\big((n+1)r\big) = \exp(nr)\exp(r) = \exp(r)^n \cdot \exp(r) = \exp(r)^{n+1}.$$

Für $n \in \mathbb{N}$ folgt ebenfalls aus der Funktionalgleichung

$$1 = \exp(0) = \exp(-nr + nr) = \exp(-nr)\exp(nr)$$

und damit $\exp(-nr) = 1/\exp(nr) = 1/\exp(r)^n = \exp(r)^{-n}$. Also gilt die Behauptung für alle ganzen Zahlen.

Schließlich haben wir für $m \in \mathbb{Z}$ und $n \in \mathbb{N}^+$

$$\exp(r)^m = \exp(mr) = \exp(n \cdot m/n \cdot r) = \exp(m/n \cdot r)^n$$

bzw. $\exp(m/n \cdot r) = \sqrt[n]{\exp(r)^m} = \exp(r)^{m/n}$. ∎

Der Beweis zeigt, dass Satz 28.7 auch dann gilt, wenn r komplex und q eine ganze Zahl ist. Für beliebige rationale Zahlen q können wir das jedoch nicht formulieren, weil nicht klar ist, was *die n-te Wurzel einer komplexen Zahl* sein soll. (Siehe die Diskussion auf Seite 178.)

Für $z \in \mathbb{C}$ definieren wir e^z als $\exp(z)$. **Definition**

Wir können also nun beispielsweise sagen, was e^π oder e^i bedeuten sollen, während diese Ausdrücke vorher keinen Sinn ergeben hätten – wohingegen Terme der Form e^q mit rationalen Exponenten q definiert waren. $z \to \mathrm{e}^z$ ist damit eine auf ganz $\mathbb{C}$ definierte glatte Funktion, die nach Satz 28.7 für rationale Argumente mit der bisherigen Definition übereinstimmt.

Aufgabe 28.8. Geben Sie alle Lösungen der Gleichung $(2x-6)\mathrm{e}^{x^2+3} = 0$ an.

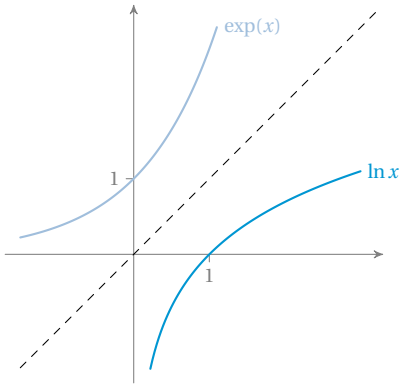
⋆**Aufgabe 28.9**. Begründen Sie, warum der Wertebereich von $\exp|_{\mathbb{R}}$ das komplette Intervall $(0,\infty)$ ist.

Wegen Aufgabe 28.9 und da die Funktion $\exp|_{\mathbb{R}}$ nach Lemma 28.6 außerdem injektiv ist, ergibt die folgende Definition Sinn.

Definition

Die auf $(0,\infty)$ definierte Umkehrfunktion von $\exp|_{\mathbb{R}}$ wird als **natürlicher Logarithmus** bezeichnet und ln geschrieben.[8]

Grundsätzlich ergeben sich die Funktionsgraphen von Umkehrfunktionen reeller Funktionen durch Spiegelung an der Hauptdiagonalen $\mathrm{id}_{\mathbb{R}}$, denn es werden (siehe Abschnitt 6) lediglich die Komponenten der Paare vertauscht. Für den Logarithmus sieht das folgendermaßen aus.



Offensichtlich ist der Logarithmus streng monoton steigend mit $\ln 1 = 0$.

⋆**Aufgabe 28.10**. Begründen Sie: Ist $A \subseteq \mathbb{R}$ und $f\colon A \to \mathbb{R}$ streng monoton steigend, dann ist die Umkehrfunktion f^{-1} ebenfalls streng monoton steigend.

Lemma 28.8

Die Ableitung des Logarithmus ist die Funktion $x \mapsto 1/x$.

Beweis. Mit der Umkehrregel und Lemma 28.2 erhält man sofort $1/\exp(\ln x)$. ■

Aufgabe 28.11. Berechnen Sie die Ableitungen von $\ln(x^2+1)$ und $(\ln x)^2+1$.

Lemma 28.9

Funktionalgleichung des Logarithmus
Für alle $x_1, x_2 \in (0,\infty)$ gilt $\ln x_1 x_2 = \ln x_1 + \ln x_2$.

Beweis. Mit der Funktionalgleichung der Exponentialfunktion erhält man

$$\exp(\ln x_1 + \ln x_2) = \exp(\ln x_1)\exp(\ln x_2) = x_1 x_2.$$

[8] In mathematischen Fachtexten wird statt ln oft auch log verwendet. Auch in vielen Programmiersprachen heißt die entsprechende Funktion `log`.

Damit ergibt sich die Behauptung sofort, wenn man auf beiden Seiten den Logarithmus anwendet. ■

Aufgabe 28.12. Begründen Sie, dass auch $\ln(x_1/x_2) = \ln x_1 - \ln x_2$ gilt.

Ihnen ist vielleicht aufgefallen, dass ich $\exp(x)$ immer mit Klammern, $\ln x$ aber manchmal ohne diese geschrieben habe. Damit folge ich einer historisch gewachsenen Tradition, bei manchen Funktionen – z. B. auch beim Sinus oder beim Kosinus – die Klammern wegzulassen. Dafür gibt es keine festen Regeln, aber üblicherweise versteht man es so, dass der „Geltungsbereich" der Funktion sich bis zum nächsten Operatorsymbol erstreckt. Das würde beispielsweise implizieren, dass $\ln xy$, $\ln x^3$ und $\ln \frac{3}{4}$ Abkürzungen für $\ln(xy)$, $\ln(x^3)$ und $\ln(\frac{3}{4})$ sind, während $\ln x + y$ oder $\ln 3/4$ im Sinne von $\ln(x) + y$ bzw. $\ln(3)/4$ gemeint sind. Besonders Letzteres lädt jedoch zu Missverständnissen ein. Im Zweifelsfall sollte man lieber Klammern verwenden. (Und natürlich dürfen Sie in typischen Programmiersprachen Funktionen wie `log` und `sin` *nie* ohne Klammern verwenden.)

Ist a eine positive reelle Zahl und $q \in \mathbb{Q}$, dann gilt nach Satz 28.7

$$a^q = \exp(\ln a)^q = \exp(q \ln a).$$

Analog zur Definition von e^z ergibt daher auch die folgende Definition Sinn, stimmt für rationale Exponenten mit der gewohnten überein, liefert nun jedoch (für festes a) eine auf ganz $\mathbb{C}$ definierte und differenzierbare Funktion.

Definition

Für $a > 0$ und $z \in \mathbb{C}$ definieren wir a^z als $\exp(z \ln a)$ bzw. $e^{z \ln a}$.

Lemma 19.14 kann damit auf komplexe Zahlen verallgemeinert werden. Bewiesen werden diese Eigenschaften ganz simpel durch Einsetzen in die Definition und Anwendung der Funktionalgleichungen für die Exponentialfunktion und den Logarithmus.

Lemma 28.10

Für alle $a, b \in (0, \infty)$ und alle $r, s \in \mathbb{C}$ gelten die folgenden Aussagen:

(i) $a^r \cdot a^s = a^{r+s}$
(ii) $a^r / a^s = a^{r-s}$
(iii) $a^r \cdot b^r = (ab)^r$
(iv) $a^r / b^r = (a/b)^r$
(v) $(a^r)^s = a^{rs}$

Aufgabe 28.13. Beweisen Sie Lemma 28.10.

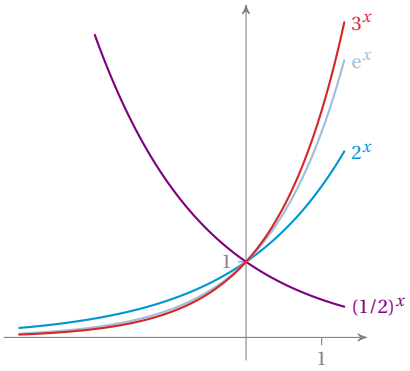
Aufgabe 28.14. Begründen Sie, warum die reelle Funktion $x \mapsto a^x$ für $a > 1$ streng monoton steigt und für $0 < a < 1$ streng monoton fällt.

Aufgabe 28.15. Geben Sie für $r \in \mathbb{R}$ die Ableitung der auf dem Intervall $(0, \infty)$ definierten Funktion $x \mapsto x^r$ an.

Aufgabe 28.16. Geben Sie für $a > 0$ die Ableitung von $x \mapsto a^x$ an.

Exponentialfunktion

Funktionen der Art $x \mapsto a^x$ werden allgemein als *Exponentialfunktionen* bezeichnet. Einige Beispiele zeigt die folgende Skizze. Beachten Sie, dass alle diese Funktionen sich im Punkt $(0,1)$ schneiden. Außerdem folgt aus den Rechenregeln in Lemma 28.10, dass der Funktionsgraph von $(1/a)^x$ sich durch Spiegelung des Graphen von a^x an der vertikalen Achse ergeben muss.



Wegen Aufgabe 28.14 kann man nun auch allgemeine Logarithmen definieren.

Definition

Sei $a > 0$ und $a \neq 1$. Die auf $(0,\infty)$ definierte Umkehrfunktion von $x \mapsto a^x$ wird als **Logarithmus zur Basis** a bezeichnet und $\log_a$ geschrieben.[9]

Da es erfahrungsgemäß oft zu gewissen Verwirrungen kommt, sei hier ein wichtiger Punkt explizit hervorgehoben. Wenn Sie Gleichungen wie $x + y = a$ oder $xy = a$ nach x auflösen, dann erhalten Sie $x = a - y$ bzw. $x = a/y$, weil Subtraktion und Division die Umkehrung von Addition und Multiplikation sind – siehe Abschnitt 10. Und wenn Sie diese Gleichungen nach y auflösen, dann ergeben sich $y = a - x$ bzw. $y = a/x$. Das ist dieselbe Rechnung, bei der nur die Rollen von x und y vertauscht wurden. Und das liegt daran, dass Addition und Multiplikation kommutativ sind.

Das Potenzieren ist aber *nicht* kommutativ – siehe z. B. Aufgabe 7.6.[10] Daher ist es bei einer Gleichung wie $x^y = a$ *nicht* egal, ob Sie nach x oder nach y auflösen. Nach x aufgelöst erhält man $x = a^{1/y}$ und beantwortet die Frage, welche Zahl zur y-ten Potenz a ergibt.[11] Nach y aufgelöst erhält man jedoch $y = \log_x a$ und beantwortet die Frage, mit was man x potenzieren muss, damit a herauskommt.

Aufgabe 28.17. Geben Sie ohne Zuhilfenahme eines Taschenrechners oder anderer Hilfsmittel die Werte $\log_2 64$ und $\log_{10} 100\,000$ an.

[9] In technischen Texten findet man auch die Abkürzungen lg für $\log_{10}$ sowie lb oder ld für $\log_2$. Und ln ist natürlich dasselbe wie $\log_e$.

[10] Siehe auch die Aufgaben 28.15 und 28.16, bei denen es offenbar um zwei sehr unterschiedliche Funktionen geht. Dafür muss man nur die Funktionsgraphen von $x \mapsto x^2$ und $x \mapsto 2^x$ vergleichen.

[11] Wenn $y \in \mathbb{N}^+$ gilt, spricht man bekanntlich auch von der y-ten Wurzel.

Die Funktionalgleichung des natürlichen Logarithmus gilt für alle Logarithmen. Und man kann noch weitere angenehme Eigenschaften beweisen.

Lemma 28.11

Für alle $a, b, x, y > 0$ mit $a, b \neq 1$ gelten die folgenden Aussagen:

(i) $\log_a x = \log_b x / \log_b a$
(ii) $\log_a xy = \log_a x + \log_a y$
(iii) $\log_a(x/y) = \log_a x - \log_a y$
(iv) $\log_a x^y = y \log_a x$

Beweis. Nach Definition gilt $\exp(\ln a \log_a x) = a^{\log_a x} = x$ und damit $\ln x = \ln a \log_a x$ bzw. $\log_a x = \ln x / \ln a$. Substitutiert man für a bzw. x andere Variablen, erhält man

$$\log_a x = \frac{\ln x}{\ln a} = \frac{\ln x / \ln b}{\ln a / \ln b} = \frac{\log_b x}{\log_b a}.$$

Das beweist den ersten Punkt und man kann damit insbesondere alle weiteren Punkte auf Eigenschaften des natürlichen Logarithmus zurückführen. ($\log_a$ „ist“ quasi der natürliche Logarithmus, der lediglich mit dem konstanten Faktor $1/\ln a$ multipliziert wird.)

Die nächsten beiden Punkte folgen daher direkt aus der Funktionalgleichung des natürlichen Logarithmus sowie aus Aufgabe 28.12. Der letzte Punkt ist für $a = \mathrm{e}$ nach Definition von x^y offensichtlich und damit auch für beliebige Logarithmen klar. ■

Aufgabe 28.18. Viele Taschenrechner kennen nur die zwei Logarithmusfunktionen ln und $\log_{10}$. Wie würden Sie mit so einem Taschenrechner $\log_7 42$ berechnen?

Aufgabe 28.19. Sei $a = 500^{-\frac{1}{2}}$ und $b = \sqrt{5}/a$. Berechnen Sie $c = \log_{10} b + \log_{10} 20$. (Arbeiten Sie mit Zettel und Bleistift. Das Ergebnis ist eine rationale Zahl und kann daher exakt angegeben werden.)

Aufgabe 28.20. Seien b und c positive reelle Zahlen und $x = \mathrm{e}^{b \ln c}$. Geben Sie einen möglichst einfachen Ausdruck für $x^{-2/b}$ an, in dem weder x und e noch Logarithmen vorkommen.

Aufgabe 28.21. Sei $a > 0$. Geben Sie die Lösung x der Gleichung $a^x = 5/a^2$ in Abhängigkeit von a in möglichst einfacher Form an.

Aufgabe 28.22. Sei $a > 0$ mit $a \neq 1$. Geben Sie die Ableitung von $x \mapsto \log_a x$ an. (Hinweis: Verwenden Sie Lemma 28.11.)

⋆ Exponentialfunktionen und Logarithmen im Computer

In PYTHON gibt es für die Exponentiation drei Möglichkeiten, die sich subtil unterscheiden.

```
import math
2**3, pow(2,3), math.pow(2,3)
```

Die dritte Version rechnet immer mit Fließkommazahlen gemäß der Definition auf Seite 267, während die anderen beiden bei ganzzahligen Argumenten auch ganzzahlige Werte zurückgeben. Außerdem können diese auch mit PYTHONs komplexen Zahlen umgehen. Man beachte die Klammern, die in diesem Fall notwendig sind:

```
(2+5j)**3j, pow(2+5j,3j)
```

Dass `pow` auch modulare Arithmetik beherrscht, wissen wir schon.

Die Standardbibliothek MATH beinhaltet die natürliche Exponentialfunktion, Logarithmen und die eulersche Zahl. Ruft man `log` mit zwei Argumenten auf, dann ist das zweite die Basis.

```
from math import *
exp(1), e, log(e), log(1000,10)
```

Wenn Sie mit komplexen Zahlen arbeiten wollen, müssen Sie die Bibliothek CMATH verwenden.[12]

```
import cmath
x=cmath.exp(2+3j)
x, cmath.log(x)
```

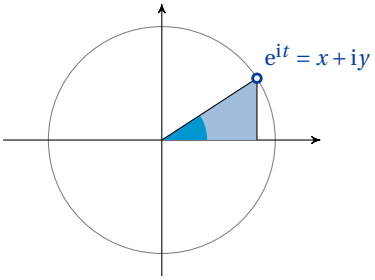
Zusätzlich gibt es Spezialfunktionen wie `expm1` oder `log10`, die in Grenzfällen genauer rechnen. Für Einzelheiten sei auf die Dokumentation verwiesen.

```
log10(1000), log(1000,10)
```

29. Die trigonometrischen Funktionen

In der Schule lernt man die trigonometrischen Funktionen als Seitenverhältnisse in rechtwinkligen Dreiecken kennen. Das ist gewissermaßen der „klassische“ geometrische Ansatz. Wir wählen in diesem Kapitel jedoch den modernen Weg der Einführung mithilfe der Exponentialfunktion, damit wir klar definierte Funktionen haben, die man mit den Mitteln der Analysis untersuchen kann. Im Zuge dessen werden wir auch präzisieren, was genau mit der Zahl π gemeint ist. Die folgende Skizze soll dabei als Motivation für die nächsten Seiten dienen.

[12] Komplexe Logarithmen haben wir in diesem Skript gar nicht definiert.



Wir werden feststellen, dass komplexe Zahlen der Form e^{it} für $t \in \mathbb{R}$ immer den Absolutbetrag 1 haben, dass sie also anschaulich auf dem skizzierten Einheitskreis liegen. Hat so eine Zahl den Realteil x und den Imaginärteil y, dann sind diese Werte die Längen der Katheten des hellblau gefüllten rechtwinkligen Dreiecks – und gleichzeitig die *Verhältnisse* dieser Längen zur Länge der Hypotenuse (weil die die Länge 1 hat). Wir definieren Funktionen, die x und y in Abhängigkeit von t ausdrücken. Und wir werden sehen, dass es Sinn ergibt, t als den hervorgehobenen Winkel (also als das Argument der Zahl e^{it}) zu betrachten.

Lemma 29.1

Für alle $z \in \mathbb{C}$ gilt $\overline{e^z} = e^{\overline{z}}$.

Beweis. Da das Konjugieren stetig ist (siehe Seite 250), gilt für jede konvergente Folge (a_n) mit Grenzwert a, dass $(\overline{a_n})$ gegen $\overline{a}$ konvergiert. $\exp(z)$ ist als Wert einer Reihe nach Definition der Grenzwert der Folge der Partialsummen. Also gilt

$$\overline{\exp(z)} = \overline{\lim_{n\to\infty} \sum_{k=0}^{n} \frac{z^k}{k!}} = \lim_{n\to\infty} \overline{\sum_{k=0}^{n} \frac{z^k}{k!}} = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{\overline{z}^k}{k!} = \exp(\overline{z}).$$

Bei der vorletzten Gleichheit wurden die Rechenregeln zum Konjugieren (Lemma 17.5) angewandt sowie die Tatsache, dass $k!$ sich als reelle Zahl durch das Konjugieren nicht ändert. ■

Korollar 29.2

Für alle $z \in \mathbb{C}$ gilt $|e^z| = e^{\mathrm{Re}(z)}$. Insbesondere gilt $|e^{it}| = 1$ für alle $t \in \mathbb{R}$.

Beweis. Erneut unter Anwendung der Regeln aus Lemma 17.5 erhält man

$$|e^z| = \sqrt{e^z \cdot \overline{e^z}} = \sqrt{e^z \cdot e^{\overline{z}}} = \sqrt{e^{z+\overline{z}}} = \sqrt{e^{2\,\mathrm{Re}(z)}} = e^{\mathrm{Re}(z)}.$$

(Man beachte, dass unter der Wurzel garantiert nur nichtnegative reelle Zahlen stehen. Die auf Seite 178 angesprochene Problematik der Wurzeln echt komplexer Zahlen spielt hier also keine Rolle.) ■

Allgemein gilt $i^n = (-1)^{n/2}$ für gerade $n \in \mathbb{N}$ und $i^n = (-1)^{(n-1)/2} i$ für ungerade n. (Siehe Aufgabe 19.11.) Damit kann man $\exp(iz)$ für $z \in \mathbb{C}$ in zwei Reihen zerlegen:

$$\exp(iz) = \sum_{n=0}^{\infty} \frac{(iz)^n}{n!} = \sum_{n=0}^{\infty} \frac{i^n z^n}{n!} = \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n}}{(2n)!} + i \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{(2n+1)!} \tag{29.1}$$

Definition

Der **Sinus** und der **Kosinus** werden folgendermaßen auf ganz $\mathbb{C}$ definiert:

$$\cos z = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} z^{2n}$$
$$\sin z = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} z^{2n+1} \tag{29.2}$$

Dass diese Reihen für alle $z \in \mathbb{C}$ konvergieren, zeigt man wieder mit dem Quotientenkriterium. Mit (29.1) folgt:

Satz 29.3

Eulersche Formel
Für alle $z \in \mathbb{C}$ gilt $\exp(\mathrm{i}z) = \cos z + \mathrm{i} \sin z$.

Man sieht zudem, dass Sinus und Kosinus für reelle Argumente reelle Funktionswerte liefern (und das insbesondere $\cos 0 = 1$ und $\sin 0 = 0$ gilt). Es folgt:

Korollar 29.4

Für alle $t \in \mathbb{R}$ sind $\cos t$ und $\sin t$ Real- und Imaginärteil von $\mathrm{e}^{\mathrm{i}t}$ (und damit gelten auch $|\cos t| \leq 1$ und $|\sin t| \leq 1$).

Damit haben wir den wesentlichen Teil des am Anfang des Abschnitts versprochenen Zusammenhangs bereits gezeigt. Wir werden die neuen Funktionen nun genauer unter die Lupe nehmen.

Satz 27.3 liefert die folgende Aussage, die man leicht durch Nachrechnen verifizieren kann.[13]

Lemma 29.5

Die Funktionen sin und cos sind beliebig oft differenzierbar mit $\sin' = \cos$ und $\cos' = -\sin$.

Aufgabe 29.1. Geben Sie die Ableitungen von $\sin(x^2+1)$ sowie von $\ln \sin x$ an.

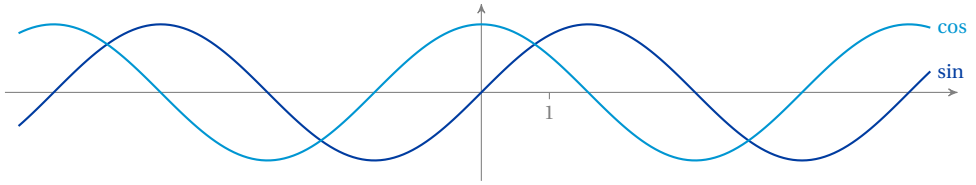
Aufgabe 29.2. Wie Sie wahrscheinlich aus der Schule wissen, ist der Tangens durch $\tan x = \sin x / \cos x$ definiert. (Natürlich nur an den Stellen, an denen $\cos x \neq 0$ gilt. Details später.) Ermitteln Sie die Ableitung des Tangens.

gerade Funktion
ungerade Funktion

Außerdem ist der Kosinus eine sogenannte *gerade* Funktion, womit gemeint ist, dass $\cos(-z) = \cos z$ für alle $z \in \mathbb{C}$ gilt. Und der Sinus ist *ungerade*, d. h., es gilt immer $\sin(-z) = -\sin z$. Der Funktionsgraph des reellen Kosinus ist also achsensymmetrisch zur vertikalen Achse und der des reellen Sinus ist punktsymmetrisch zum Ursprung des Koordinatensystems. Beides lässt sich ohne Mühe durch Einsetzen in (29.2) nachprüfen.[14]

[13] Eine geometrische Begründung für diesen Zusammenhang demonstriert das Video *Warum der Kosinus die Ableitung des Sinus ist*.

[14] Die Bezeichnungen kommen von den Funktionen der Form $x \mapsto x^n$, die genau dann gerade bzw. ungerade sind, wenn ihre Exponenten diese Eigenschaft haben.



Der folgende Satz wird sich für Sinus und Kosinus als ähnlich hilfreich herausstellen wie die Funktionalgleichung der Exponentialfunktion (mit deren Hilfe er auch bewiesen wird).

Additionstheoreme für Sinus und Kosinus **Satz 29.6**
Für alle $z, w \in \mathbb{C}$ gilt

$$\cos(z \pm w) = \cos z \cos w \mp \sin z \sin w \quad \text{und}$$
$$\sin(z \pm w) = \sin z \cos w \pm \cos z \sin w.$$

Beweis. Mit der eulerschen Formel und der Funktionalgleichung der Exponentialfunktion ergibt sich

$$\begin{aligned}\cos(z+w) \pm \mathrm{i}\sin(z+w) &= \mathrm{e}^{\pm\mathrm{i}(z+w)} = \mathrm{e}^{\pm\mathrm{i}z}\mathrm{e}^{\pm\mathrm{i}w} \\ &= (\cos z \pm \mathrm{i}\sin z)(\cos w \pm \mathrm{i}\sin w) \\ &= \cos z\cos w - \sin z \sin w \pm \mathrm{i}(\cos z \sin w + \sin z \cos w).\end{aligned}$$

Das sind zwei Gleichungen, eine für plus und eine für minus. Addiert bzw. subtrahiert man die beiden und dividiert anschließend durch 2 bzw. 2i, so ergeben sich die Additionstheoreme für plus. Die Additionstheoreme für minus folgen dann sofort, weil der Kosinus gerade ist und der Sinus ungerade. ■

Satz des Pythagoras **Korollar 29.7**
Für alle $z \in \mathbb{C}$ gilt $\sin^2 z + \cos^2 z = 1$.

Beweis. Das ergibt sich, wenn man $w = z$ im Additionstheorem für $\cos(z - w)$ einsetzt und dabei $\cos 0 = 1$ verwendet. ■

Das ist natürlich eine ganz allgemeine Aussage über zwei komplexe Funktionen und nicht der klassische Satz des Pythagoras. (Zwischen Pythagoras und der ersten Verwendung komplexer Zahlen liegen etwa zweitausend Jahre.) Aber angesichts der geometrischen Interpretation der komplexen Zahlen ergibt die Benennung durchaus Sinn.

Die Schreibweise $\sin^2 z$ ist eine weitere weitverbreitete Konvention. Es handelt sich um eine Abkürzung für $(\sin z)^2$.

Der Kosinus hat auf dem Intervall $[0, 2]$ genau eine Nullstelle. **Satz 29.8**

Beweis. Setzt man den Wert 2 in die Definition (29.2) ein, so erhält man die Reihenentwicklung

$$\cos 2 = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n}}{(2n)!} = 1 - 2 + \underbrace{\sum_{n=2}^{\infty} (-1)^n \frac{2^{2n}}{(2n)!}}_{S}.$$

Wir wissen zwar schon, dass die Reihe konvergiert, aber da die Folge der Reihenglieder eine Nullfolge ist,[15] kann man in diesem Fall auch das Leibniz-Kriterium anwenden. Dessen Beweis liefert mit (21.2) und Lemma 19.6 die Abschätzung

$$|S| \le \left|(-1)^2 \frac{2^{2\cdot 2}}{(2\cdot 2)!}\right| = \frac{2^4}{4!} = \frac{2}{3}$$

und damit $\cos 2 = 1 - 2 + S \le -1/3$. Da $\cos 0 = 1$ positiv ist, gibt es nach dem Zwischenwertsatz zwischen 0 und 2 mindestens eine Nullstelle.

Mit der Reihendarstellung

$$\frac{\sin x}{x} = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n+1)!} = 1 + \sum_{n=1}^{\infty} (-1)^n \frac{x^{2n}}{(2n+1)!}$$

kann man genau wie eben argumentieren und daraus

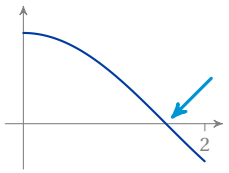
$$\frac{\sin x}{x} \ge 1 - \frac{x^2}{3!}$$

für $x > 0$ folgern. Für $x \in (0,2]$ folgt daraus $\frac{\sin x}{x} \ge \frac{1}{3}$ und damit insbesondere die Ungleichung $\sin x > 0$.

Mit den Additionstheoremen erhält man

$$\begin{aligned}\cos x - \cos y &= \cos\Big(\frac{x+y}{2} - \frac{y-x}{2}\Big) - \cos\Big(\frac{x+y}{2} + \frac{y-x}{2}\Big)\\ &= \cdots = 2\sin\Big(\frac{x+y}{2}\Big)\sin\Big(\frac{y-x}{2}\Big)\end{aligned}$$

und speziell für $x, y \in (0,2)$ mit $x < y$ folgt dann zusammen mit der vorherigen Überlegung $\cos x - \cos y > 0$. $\cos x$ ist also auf $(0,2)$ streng monoton fallend, daher insbesondere injektiv und es kann somit dort nur eine Nullstelle geben. ■



[15] Dass eine Folge der Form $(b^n/n!)$ gegen Null geht, wissen wir „offiziell“ noch nicht. Man kann das ähnlich wie Lemma 19.11 beweisen. Siehe dazu z. B. das Video *Folgen mit Polynomen und Exponentialfunktionen*.

Definition

Die Zahl, die sich ergibt, wenn man die eindeutig bestimmte Nullstelle aus Satz 29.8 verdoppelt, wird als die **Kreiszahl** π bezeichnet.[16]

Bekanntlich hat π ungefähr den Wert 3.141592. Wie e ist auch π irrational. Das hat der Schweizer Johann Heinrich Lambert 1761 bewiesen. Einen Beweis, den man mit soliden Kenntnissen der Schulmathematik verstehen kann, zeigt das Video *Die Kreiszahl Pi ist irrational*. Ein paar interessante Fakten zur Historie von π und den Versuchen, einen möglichst genauen Wert für diese Zahl zu bestimmen, präsentiert das Video *Eine kurze Geschichte der Kreiszahl Pi*.

Es gilt also $\cos(\pi/2) = 0$ und mit Korollar 29.7 folgt daraus[17] $\sin(\pi/2) = 1$. Die eulersche Formel liefert nun für $n \in \mathbb{Z}$

$$\cos\tfrac{n\pi}{2} + \mathrm{i}\sin\tfrac{n\pi}{2} = \mathrm{e}^{n\mathrm{i}\pi/2} = \left(\mathrm{e}^{\mathrm{i}\pi/2}\right)^n = \left(\cos\tfrac{\pi}{2} + \mathrm{i}\sin\tfrac{\pi}{2}\right)^n = \mathrm{i}^n.$$

Vergleich man links und rechts jeweils Real- und Imaginärteile, so ergibt sich die folgende Aussage.

Lemma 29.9

Nullstellen und Extrema von Sinus und Kosinus im Reellen
Für alle $n \in \mathbb{Z}$ gilt

$$\cos\left(\tfrac{\pi}{2} + n\pi\right) = \sin(n\pi) = 0 \quad \text{und}$$
$$\cos(n\pi) = \sin\left(\tfrac{\pi}{2} + n\pi\right) = (-1)^n.$$

Insbesondere ergibt sich $\mathrm{e}^{\mathrm{i}\pi} = \cos\pi + \mathrm{i}\sin\pi = -1$. Schreibt man das absichtlich etwas umständlich auf, dann erhält man das, was regelmäßig von Mathematikerinnen und Mathematikern als „schönste Formel der Welt“ gekürt wird.

Korollar 29.10

Eulersche Identität
$\mathrm{e}^{\mathrm{i}\pi} + 1 = 0$

Was macht diese Formel so besonders? Erstens kommen in ihr die drei wesentlichen Rechenoperationen Addition, Multiplikation und Exponentiation jeweils einmal vor und zweitens stellt sie einen Zusammenhang zwischen den fünf wichtigsten Zahlen der Mathematik her:

- 0 und 1 sind als neutrale Elemente von Addition und Multiplikation die Grundlage des Rechnens und aus ihnen kann man in gewissem Sinne alle reellen Zahlen generieren – siehe z. B. Satz 15.4.
- π ist als Verhältnis von Kreisumfang zum Durchmesser so etwas wie die „Naturkonstante“ der Geometrie.

[16] Obwohl dieser Wert in verschiedenen Kulturen schon seit Jahrtausenden verwendet wurde, stammt die heute übliche Bezeichnung mit einem griechischen Buchstaben erst aus dem 18. Jahrhundert. Sie wird dem walisischen Mathematiker William Jones zugeschrieben.

[17] Weil wir aus dem Beweis von Satz 29.8 wissen, dass nicht -1 herauskommen kann.

– e ist die Basis der natürlichen Exponentialfunktion, von deren Wichtigkeit wir schon gehört haben.
– i ist die „Keimzelle“ der komplexen Zahlen, die das Zahlenuniversum gleichsam komplettieren.

Durch einfache Anwendung der Additionstheoreme und die Werte aus Lemma 29.9 erhält man eine weitere wichtige Eigenschaft von Sinus und Kosinus.

Lemma 29.11

Periodizität von Sinus und Kosinus
Sinus und Kosinus sind *periodisch* mit der Periode 2π. Damit ist gemeint, dass die Beziehungen $\cos(z+2\pi) = \cos z$ und $\sin(z+2\pi) = \sin z$ für alle $z \in \mathbb{C}$ gelten.

Auch der folgende Zusammenhang folgt durch einfaches Ausrechnen mit den Additionstheoremen und bereits bekannte Funktionswerte. Der Sinus ist quasi nur ein „verschobener“ Kosinus.[18]

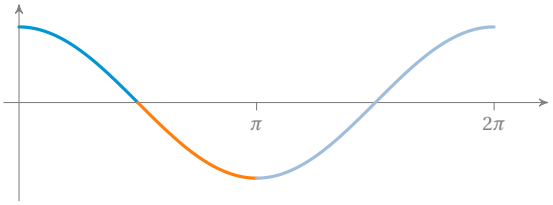
Lemma 29.12

Phasenverschiebung von Sinus und Kosinus
Für alle $z \in \mathbb{C}$ gilt $\cos(z+\pi/2) = -\sin z$ und $\sin(z+\pi/2) = \cos z$.

Die Aussagen der beiden Lemmata lassen sich in der Skizze auf Seite 273 gut erkennen. Lemma 29.11 besagt, dass man beispielsweise nur die Werte zwischen 0 und 2π kennen muss, um den gesamten reellen Verlauf von Sinus und Kosinus zu kennen. Lemma 29.12 besagt, dass es reicht, eine der beiden Funktionen zu kennen. Schließlich kann man sich noch überlegen (ein weiteres Mal mit den Additionstheoremen), dass es sogar ausreicht, die Funktionswerte in einem der vier Viertel einer Periode zu kennen. Das folgende Lemma formuliert das für den Kosinus, aber wegen der obigen Zusammenhänge kann man das natürlich auch für den Sinus machen.

Lemma 29.13

Determiniertheit durch den ersten Quadranten
Für alle $z \in \mathbb{C}$ gilt $\cos(\pi/2+z) = -\cos(\pi/2-z)$ und $\cos(\pi+z) = \cos(\pi-z)$.



Damit folgt dann auch, dass die in Lemma 29.9 genannten Nullstellen die einzigen reellen Nullstellen der beiden Funktionen sind.

Aufgabe 29.3. Sie haben einen Taschenrechner, bei dem die Kosinusfunktion nur für Eingabewerte zwischen 0 und $\pi/2$ funktioniert. Was müssen Sie eingeben, um $\cos(7\pi/6)$ zu berechnen? (Verwenden Sie Lemma 29.13.)

[18] Der Begriff *Phase* stammt aus der Physik.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Aufgabe 29.4. Der Billigtaschenrechner aus Aufgabe 29.3 hat zu allem Überfluss auch keine Taste für den Sinus. Wie können Sie trotzdem $\sin(5\pi/9)$ berechnen?

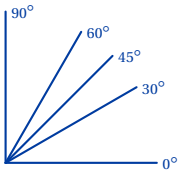
Aufgabe 29.5. Führen Sie die Beweise der Lemmata 29.11 bis 29.13 durch, indem Sie jeweils in die Additionstheoreme einsetzen.

⋆**Aufgabe 29.6**. Leiten Sie mithilfe der Additionstheoreme und mit Korollar 29.7 eine Formel für $\cos 2z$ her, in der der Sinus nicht vorkommt.

Aufgabe 29.7. Berechnen Sie mit der Formel aus der Lösung von Aufgabe 29.6 nacheinander $\cos(\pi/4)$ und $\cos(\pi/8)$.

Ein paar Werte von Sinus und Kosinus sollte man im Kopf haben.[19]

x	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
x	0°	30°	45°	60°	90°
n	0	1	2	3	4
$\sqrt{n}/2$	0	$1/2$	$1/\sqrt{2}$	$\sqrt{3}/2$	1
$\sin x$	0	$1/2$	$1/\sqrt{2}$	$\sqrt{3}/2$	1
$\cos x$	1	$\sqrt{3}/2$	$1/\sqrt{2}$	$1/2$	0
$\tan x$	0	$1/\sqrt{3}$	1	$\sqrt{3}$	–



Man kann noch diverse weitere Zusammenhänge beweisen, die Sie sich aber ohnehin nicht alle merken werden. Im Bedarfsfall kann man zum Beispiel in der Formelsammlung zur Trigonometrie auf Wikipedia nachschlagen.

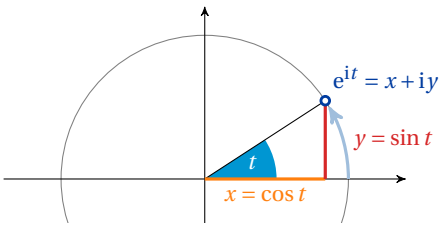
Aufgabe 29.8. Die Gleichung $\cos x = x$ hat zwischen 0 und 1 genau eine Lösung. (Wieso?) Geben Sie diese Lösung auf zwei Stellen nach dem Komma genau an.

Aufgabe 29.9. Was würde sich in Aufgabe 25.8 ändern, wenn man zusätzlich wüsste, dass f ungerade ist?

30. Polarkoordinaten und Arkusfunktionen

An dieser Stelle können wir zur Skizze vom Anfang des letzten Abschnitts zurückkommen. Es ist nun klar, dass die komplexe Zahl e^{it} gegen den Uhrzeigersinn auf dem Einheitskreis „wandert“, wenn t auf der reellen Achse nach rechts bewegt wird. Sie startet im Punkt 1 für $t = 0$, kommt bei $t = \pi/2$ bei i vorbei, bei $t = \pi$ bei -1 und ist bei $t = 2\pi$ wieder am Ausgangspunkt. Ab hier wiederholt sich der Vorgang.

[19] Die grau eingefärbten Zeilen sind als Merkhilfe für den Sinus gedacht. Man beachte, dass die Zeile für den Kosinus der für den Sinus in umgekehrter Reihenfolge entspricht. Der Tangens ergibt sich bekanntlich durch Division der beiden Zeilen darüber.



Es liegt daher nahe, den Parameter t als Maß für den Winkel zu nehmen. Sinus und Kosinus bekommen dadurch für Punkte auf dem ersten Viertel des Kreises die geometrische Bedeutung, die wir mit ihnen ohnehin schon verbinden, sind nun aber für beliebige komplexe Zahlen sinnvoll definiert.

Damit ist t auch der Wert, den wir als Argument der komplexen Zahl bezeichnet hatten. Nach den Überlegungen aus dem vorherigen Abschnitt ist

$$z = re^{it} = r(\cos t + i \sin t) \tag{30.1}$$

für $r \geq 0$ und $t \in \mathbb{R}$ eine Zahl mit dem Absolutbetrag r und dem Argument t. Setzen wir noch gemäß einer üblichen Konvention fest, dass t im Intervall $(-\pi, \pi]$ liegen soll, dann sind r und t für jede komplexe Zahl $z \neq 0$ eindeutig bestimmt. Man bezeichnet (30.1) als die *Polardarstellung* von z.[20]

Polardarstellung

Etwas gewöhnungsbedürftig ist die „Maßeinheit“ für Winkel, die hier verwendet wird und die man als *Radiant* bezeichnet. Es sollte jedoch durch die Herleitung klargeworden sein, dass diese Festlegung sich gewissermaßen von selbst ergibt und ganz natürlich ist. Man kann (mithilfe der Integralrechnung) zeigen, dass t in der obigen Skizze genau die Länge des (hellblauen) Kreisbogens ist. Deshalb spricht man auch vom *Bogenmaß*.

Radiant

Bogenmaß

Die uns vertraute Unterteilung des Kreises in 360 *Grad* führt eine Tradition fort, die vor vielen Jahrtausenden wahrscheinlich von babylonischen Astronomen begründet wurde. Sie ist im Gegensatz zum Bogenmaß willkürlich. Würden wir in Grad rechnen, würden Aussagen wie die von Lemma 29.5 komplizierter werden, weil wir dann Vorfaktoren bräuchten. Zum Glück ist die Umrechnung zwischen Grad und Bogenmaß simpel, weil eine einfache Proportionalität besteht: 360 Grad entsprechen 2π.

Bogenmaß	$\pi/6$	$\pi/4$	$\pi/2$	π	2π
Grad	30°	45°	90°	180°	360°

Man beachte dabei, dass für Grad das Einheitenzeichen ° verwendet wird, während das Bogenmaß einfach nur eine Zahl ist. Taschenrechner bieten in der Regel Tasten wie RAD und DEG für das Umschalten zwischen Radiant und Grad (engl. *degree*) an. Achtung: Das Arbeiten mit dem falschen Winkelmaß ist eine typische Fehlerquelle!

[20] Die bereits bekannte Variante $z = x + iy$ mit expliziter Angabe von Real- und Imaginärteil nennt man *kartesische Darstellung*.

kartesische Darstellung

Kennt man von einer komplexen Zahl z den Betrag r und das Argument t, so ist nach (30.1) sofort klar, wie man Real- und Imaginärteil ausrechnet, nämlich durch

$$\mathrm{Re}(z) = r\cos t \quad \text{und} \quad \mathrm{Im}(z) = r\sin t.$$

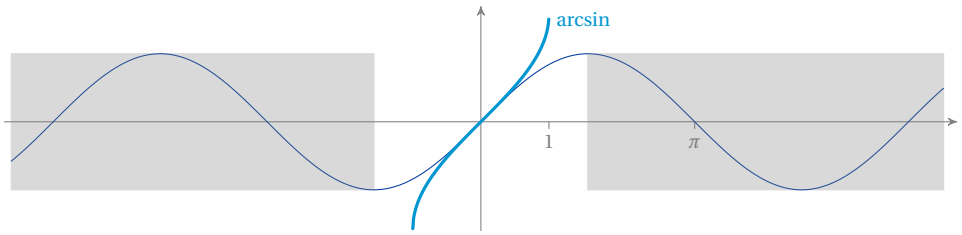
Aber wie kommt man umgekehrt von der kartesischen Darstellung $z = x+\mathrm{i}y$ zur Polardarstellung? Der Betrag r ist kein Problem: wir müssen einfach seine Definition nachschlagen und erhalten $r = \sqrt{x^2+y^2}$. Für das Argument t liefert (30.1) die Zusammenhänge $\cos t = x/r$ und $\sin t = y/r$. Aber um das nach t aufzulösen, braucht man Umkehrfunktionen der trigonometrischen Funktionen. Die sind jedoch auf direktem Wege nicht zu erhalten, weil Sinus und Kosinus wegen der Periodizität nicht injektiv sind. Man muss die Methode von Seite 79 anwenden, und entsprechend eingeschränkte Versionen dieser Funktionen betrachten. Wiederum wegen der Periodizität hat man dafür theoretisch unendlich viele Möglichkeiten. Man entscheidet sich in der Regel für eine relativ nahe bei null liegende.

Definition

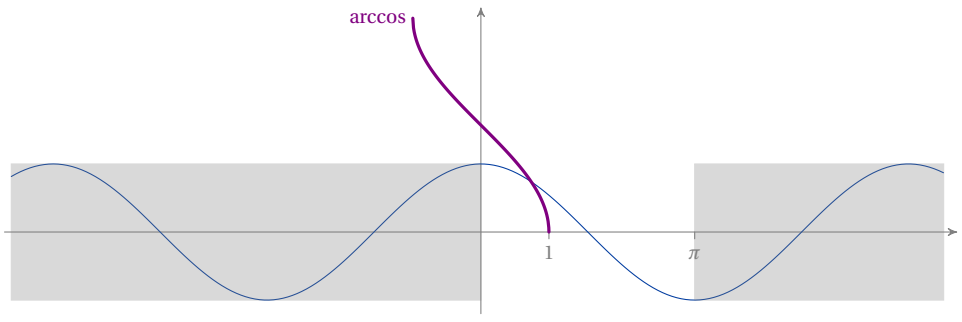
Die Umkehrfunktion von $\sin|_{[-\pi/2,\pi/2]}$ wird **Arkussinus** genannt und arcsin geschrieben. Die Umkehrfunktion von $\cos|_{[0,\pi]}$ wird **Arkuskosinus** genannt und arccos geschrieben.

Den Verlauf dieser Funktionen zeigen die beiden folgenden Grafiken. Beide sind auf dem Intervall $[-1,1]$ definiert. Sie haben als Wertebereich $[-\pi/2,\pi/2]$ bzw. $[0,\pi]$. Wegen der angesprochenen Wahlmöglichkeiten nennt man die Funktionen aus der obigen Definition auch die *Hauptzweige*.

Hauptzweige



Auf Taschenrechnern sind oft die Tasten $\boxed{\sin^{-1}}$ und $\boxed{\cos^{-1}}$ für diese Funktionen vorgesehen, während sie in vielen Programmiersprachen `asin` und `acos` heißen. Die Bezeichnung *Arkus* (lat. für *Bogen*) rührt daher, dass geometrisch betrachtet die Arkusfunktionen als Argument ein Seitenverhältnis bekommen und als Funktionswert einen Winkel – also die Länge eines Bogens – liefern.



Aufgabe 30.1. Berechnen Sie mit der Umkehrregel die Ableitungen von arcsin und arccos oder schauen Sie sich zumindest die Lösung an, damit sie die Ableitungen kennen. (Hinweis: Verwenden Sie den Satz des Pythagoras, um zwischen Sinus und Kosinus hin und her zu wechseln.)

⋆**Aufgabe 30.2**. Es ist offensichtlich, dass der Kosinus nicht injektiv ist. Aber ist eigentlich klar, dass seine Restriktion auf $[0,\pi]$ tatsächlich injektiv ist? Und was ist mit $\sin|_{[-\pi/2,\pi/2]}$?

Beim Versuch, aus der kartesischen Darstellung $z = x+\mathrm{i}y$ das Argument zu erhalten, waren wir oben bei $\cos t = x/r$ stehengeblieben. Es sieht so aus, als wäre die Lösung $t = \arccos(x/r)$. Aber leider liefert der Arkuskosinus nur Werte zwischen 0 und π. Das bedeutet, dass diese „Lösung“ für komplexe Zahlen unterhalb der reellen Achse falsche Angaben liefert. Interpretiert man das Argument jedoch wie in der Definition auf Seite 176 als eine Zahl aus dem Intervall $(-\pi,\pi]$ und nutzt aus, dass der Kosinus gerade ist, dann erhält man

$$t = \begin{cases} \arccos(x/r) & y \geq 0 \\ -\arccos(x/r) & y < 0 \end{cases}$$

für $r \neq 0$. (Für $r = 0$ ist das Argument nicht definiert.)

Aufgabe 30.3. Man kann das besagte Problem auch nicht aus der Welt schaffen, wenn man stattdessen den Zusammenhang $\sin t = y/r$ und den Arkussinus verwendet. Wie sieht dann die Fallunterscheidung aus?

Zum Abschluss führen wir noch den in Aufgabe 29.2 bereits erwähnten Tangens offiziell ein. Dabei verwenden wir ohne Beweis, dass der Kosinus auch im Komplexen außer den in Lemma 29.9 erwähnten keine weiteren Nullstellen hat.

Definition

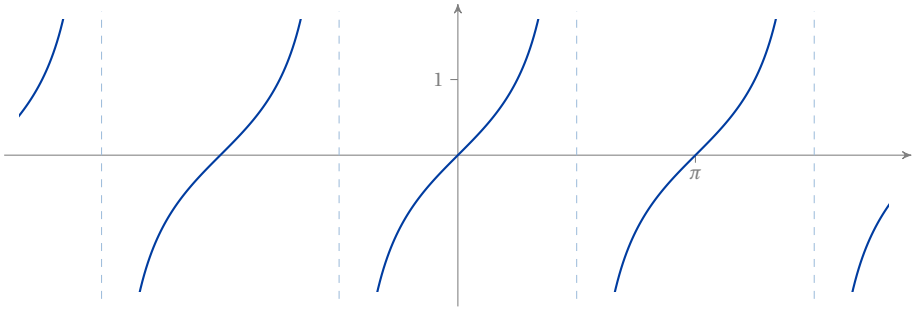
Der **Tangens** ist durch

$$\tan z = \frac{\sin z}{\cos z}$$

für alle $z \in \mathbb{C}$ definiert, für die $\cos z \neq 0$ gilt. Der Definitionsbereich dieser Funktion ist also $\mathbb{C} \setminus \{\pi/2 + n\pi : n \in \mathbb{Z}\}$.

Da Sinus und Kosinus beide periodisch, aber gegeneinander phasenverschoben sind, ist der Tangens periodisch mit der „halben“ Periode π. Der reelle Teil sieht so aus wie in der folgenden Grafik. Insbesondere ist das Bild eines Intervalls der Form $(\pi/2 + n\pi, 3\pi/2 + n\pi)$ immer ganz $\mathbb{R}$.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

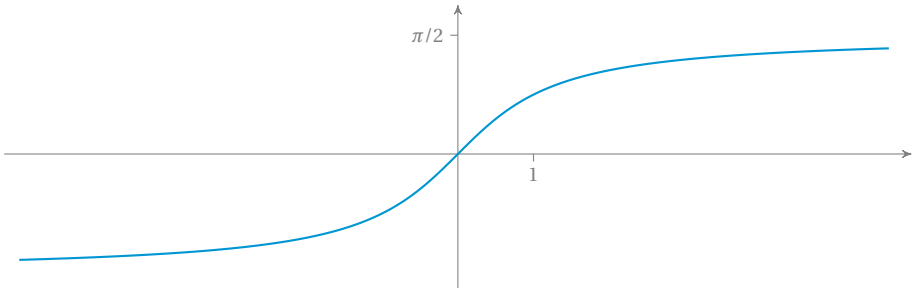


Eine Umkehrfunktion erhält man wieder durch Restriktion, indem man beispielsweise nur den mittleren „Streifen“ betrachtet.

Definition

Die Umkehrfunktion von $\tan|_{(-\pi/2,\pi/2)}$ wird **Arkustangens** genannt und arctan geschrieben.

Der Definitionsbereich des Arkustangens ist also ganz $\mathbb{R}$ und er sieht so aus wie in der folgenden Skizze.



Der Arkustangens liefert eine weitere Möglichkeit, das Argument einer komplexen Zahl $x+\mathrm{i}y$ zu berechnen. Zwar ist man aus demselben Grund wie oben auch wieder auf eine Fallunterscheidung angewiesen (und muss dabei zusätzlich noch auf die Definitionslücken achten), hat aber den Vorteil, dass man den Betrag nicht benötigt, sondern direkt mit x und y rechnen kann:[21]

$$t = \begin{cases} \arctan(y/x) & x > 0 \\ \arctan(y/x) + \pi & x < 0 \wedge y \geq 0 \\ \arctan(y/x) - \pi & x < 0 \wedge y < 0 \\ \operatorname{sgn}(y)\pi/2 & x = 0 \end{cases}$$

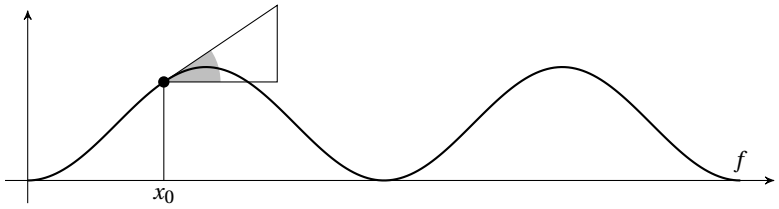
Siehe dazu auch die Bemerkung zur Hilfsfunktion `atan2` im folgenden Abschnitt über Trigonometrie im Computer.

Aufgabe 30.4. Berechnen Sie mithilfe der Lösung von Aufgabe 29.2 die Ableitung des Arkustangens.

[21] Zur Erinnerung: Die Signumfunktion wurde auf Seite 165 definiert.

Aufgabe 30.5. Geben Sie die Polardarstellung der Zahl $z = -5 + 3\mathrm{i}$ an, wobei Betrag und Argument auf drei Stellen nach dem Komma gerundet sein sollen. Wie sieht die Polardarstellung von z^3 aus?

Aufgabe 30.6. Die Funktion f ist durch $f(x) = \sin^2 x$ definiert. Geben Sie die Ableitung sowie den (grau eingezeichneten) Steigungswinkel φ des Funktionsgraphen von f an der Stelle $x_0 = 6/5$ jeweils auf zwei Stellen nach dem Komma an.



Aufgabe 30.7. Üben Sie das Umrechnen zwischen kartesischen und Polarkoordinaten. Sie können zur Kontrolle Ausdrücke wie

`2.3-5.2i in polar` oder `(-1.8,0.2) in cartesian`

in Wolfram Alpha eingeben.

⋆ Trigonometrie im Computer

In PYTHON bietet die Bibliothek MATH alle gängigen trigonometrischen Funktionen und die Konstante `pi`. Man beachte den Rundungsfehler:

```
from math import *
sin(pi), cos(pi)
```

Wie die meisten Programmiersprachen erwartet PYTHON Angaben in Bogenmaß. Obwohl die Umrechnung zwischen Grad und Radiant ganz einfach ist, gibt es dafür sogar fertige Funktionen, damit man sich das Denken abgewöhnen kann.

```
degrees(pi), radians(180)
```

Die Arkusfunktionen haben typische Kurznamen, z. B. `asin` statt arcsin.

```
asin(1/sqrt(2))/pi
```

Speziell für den Arkustangens gibt es eine sinnvolle zweistellige Erweiterung namens `atan2`. Warum es diese Funktion in vielen Programmiersprachen gibt, sollte im Laufe von Abschnitt 30 klar geworden sein. Es wird zudem in dem Video *Der "bessere" Arkustangens* noch einmal ausführlich erklärt.

```
atan(3/4),atan2(3,4),atan2(-3,-4)
```

Für das Umrechnen zwischen kartesischen Koordinaten und der Polardarstellung gibt es Funktionen in der CMATH-Bibliothek.

```
import cmath
cmath.polar(3+2j), cmath.rect(2,pi/4)/sqrt(2)
```

Resümee

Das Differenzieren von Funktionen ist ein wesentlicher Bestandteil der sogenannten *Infinitesimalrechnung*, mit der der Engländer Isaac Newton und der Deutsche Gottfried Wilhelm Leibniz Ende des 17. Jahrhunderts die Mathematik revolutionierten. Damals konnte jedoch nicht zufriedenstellend erklärt werden, *warum* die neuen Methoden funktionierten. Die moderne Herangehensweise auf der Basis von Grenzwerten wurde im 19. Jahrhundert hauptsächlich von dem Franzosen Augustin-Louis Cauchy und dem Deutschen Karl Weierstraß entwickelt.

Die Stetigkeit von Funktionen wurde erst Anfang des 19. Jahrhunderts als grundlegendes Konzept erkannt. Bis dahin hatte man diese Eigenschaft gewissermaßen als selbstverständlich vorausgesetzt, ohne sich darüber genaue Gedanken zu machen. Das lag auch daran, dass sich der Begriff der Funktion erst entwickeln musste. Dazu trugen unter anderem Beispiele wie die Dirichlet-Funktion bei, die an der hergebrachten Vorstellung davon, was eine „Funktion“ ist, rüttelten. Das Video *Was ist Nichtstandardanalysis?* geht ausführlicher auf die historische Entwicklung der Analysis ein.

Logarithmen tauchten in der Mathematik bereits Ende des 16. Jahrhunderts (und damit schon vor der Exponentialfunktion) auf. „Entdeckt“ wurden Sie von dem Schotten John Napier und dem Schweizer Jost Bürgi. Sie wurden wegen ihrer Eigenschaft, Multiplikation durch Addition ersetzen zu können, als Rechenhilfe[22] eingesetzt – zunächst in der Form von Logarithmentafeln, die später oft durch Rechenschieber ersetzt wurden. Letztere wurden erst Ende des 20. Jahrhunderts durch die Taschenrechner abgelöst. In dem Video *Was sind Logarithmen?* wird beschrieben, wie Rechenschieber funktionieren und wie Logarithmen in Technik und Wissenschaft eingesetzt werden.

Trigonometrische Funktionen wurden bereits im fünften Jahrhundert in Indien verwendet und dann später auch im arabischen Reich. Die in diesem Skript vorgestellte moderne Definition über Reihen beruht auf den Vorarbeiten des Schweizers Leonhard Euler aus dem 18. Jahrhundert. Eine geometrisch orientierte Einführung liefert das Video *Die trigonometrischen Funktionen*.

[22] Das war z. B. überlebenswichtig für die Seefahrt. Für denselben Zweck wurden auch die trigonometrischen Funktionen eingesetzt. Im Video *Wie hat man früher Sinus und Kosinus berechnet?* wird das genauer erklärt.

X

Lineare Algebra

Im Folgenden werden wir uns mit Blick auf Anwendungen wie die Computergrafik hauptsächlich mit sogenannter analytischer Geometrie beschäftigen. Dieser Bereich der Mathematik ist allerdings heutzutage in eine größere Theorie eingebettet, die man lineare Algebra nennt und die wir zumindest in Ansätzen entwickeln werden. Das wird keine Abstraktion um ihrer selbst Willen sein, denn diese allgemeinere Theorie lässt sich einerseits noch in vielen anderen mathematischen Zusammenhängen anwenden und andererseits zeigen sich durch eine erweiterte Sichtweise auch neue Anwendungen, u. a. in der Codierungstheorie.

Für das Verständnis der folgenden Seiten ist eine gewisse Vertrautheit mit der Schulgeometrie sehr hilfreich. Zum Wiederholen eignen sich unter anderem die beiden Vorkursvideos *Elementargeometrie* und *Rechtwinklige Dreiecke*.

31. Vektorräume

Für typische geometrische Anwendungen reicht es im Prinzip, die Ebene $\mathbb{R}^2$ und den Raum $\mathbb{R}^3$ (siehe Seite 44) zu betrachten. Wir werden jedoch gleich $\mathbb{R}$ durch einen beliebigen Körper K und 2 und 3 durch eine beliebige natürliche Zahl n ersetzen.

Wir wissen bereits, dass das direkte Produkt von Ringen wieder ein Ring ist. Insbesondere erhalten wir dadurch eine algebraische Struktur auf K^n, wenn K ein Körper ist. Die Addition[1] $\oplus$ ist komponentenweise durch

$$(x_1, \dots, x_n) \oplus (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n) \tag{31.1}$$

definiert und auch die Verknüpfung

$$y \odot (x_1, \dots, x_n) = (y \cdot x_1, \dots, y \cdot x_n) \tag{31.2}$$

[1] Auch eine komponentenweise Multiplikation ist definiert, aber das wird hier keine Rolle spielen. Aus Aufgabe 10.8 wissen wir bereits, dass wir dadurch im Allgemeinen keinen Körper erhalten. Man kann sogar beweisen, dass die komplexe Multiplikation, durch die $\mathbb{R}^2$ quasi eine „vollwertige“ Multiplikation erhält, eine Ausnahme ist.

ist naheliegend.

Wie es in der Algebra üblich ist, werden die Rechengesetze, die in solchen Strukturen gelten, in möglichst konzentrierter Form zusammengefasst, um zu untersuchen, auf welche anderen Bereiche sie sich anwenden lassen. Das geschieht durch die folgende Begriffsbildung.

Definition

Sei $(V, \oplus)$ eine abelsche Gruppe und K ein Körper.[2] Ferner sei $\odot$ eine Funktion von $K \times V$ nach V. Man nennt V einen **Vektorraum** über K bzw. einen **K-Vektorraum**, wenn für alle $\alpha, \beta \in K$ und alle $\mathbf{u}, \mathbf{v} \in V$ die folgenden Bedingungen erfüllt sind:

(i) $\alpha \odot (\mathbf{u} \oplus \mathbf{v}) = (\alpha \odot \mathbf{u}) \oplus (\alpha \odot \mathbf{v})$

(ii) $(\alpha + \beta) \odot \mathbf{v} = (\alpha \odot \mathbf{v}) \oplus (\beta \odot \mathbf{v})$

(iii) $(\alpha \cdot \beta) \odot \mathbf{v} = \alpha \odot (\beta \odot \mathbf{v})$

(iv) $1 \odot \mathbf{v} = \mathbf{v}$

Die Elemente von V nennt man in diesem Zusammenhang **Vektoren**, die von K **Skalare**. Die Abbildung $\odot$ wird **skalare Multiplikation** genannt.

Die ersten drei Bedingungen sehen so aus wie die Distributivität und die Assoziativität von inneren Verknüpfungen und so sind sie auch gemeint. Es ist allerdings zu beachten, dass $\odot$ *keine* innere Verknüpfung ist, weil diese Funktion einen Skalar und einen Vektor zu einem Vektor verknüpft. So etwas nennt man eine *äußere Verknüpfung*.

äußere Verknüpfung

Aus didaktischen Gründen wird in diesem Skript für Vektoren Fettdruck verwendet, also beispielsweise $\mathbf{v}$ statt v. Auch das neutrale Element von V (der sogenannte *Nullvektor*) wird entsprechend $\mathbf{0}$ statt 0 geschrieben.[3] Sie können sich jedoch nicht darauf verlassen, dass das in allen Büchern so gehandhabt wird.

Nullvektor

Schauen wir uns ein paar grundlegende Beispiele an.

- Das „Standardbeispiel“ ist der Vektorraum K^n, bei dem $\oplus$ und $\odot$ durch (31.1) und (31.2) definiert sind. Es ist eine simple Fingerübung, die entsprechenden Eigenschaften nachzuprüfen.
- Ein wichtiges Beispiel aus der Analysis sind Vektorräume von Funktionen. Ist etwa I ein Intervall, dann ist $\mathbb{R}^I$ ein Vektorraum.[4] Mit $\oplus$ ist die Addition von Funktionen gemeint und für $\alpha \in \mathbb{R}$ und $f \in \mathbb{R}^I$ soll $\alpha \odot f$ die Funktion

$$: \begin{cases} I \to \mathbb{R} \\ x \mapsto \alpha \cdot f(x) \end{cases}$$

sein. (In solchen Räumen verwendet man für die Vektoren – also die Funktionen – typischerweise keinen Fettdruck, sondern wie üblich Buchstaben wie f, g und h.)

[2] Für K verwenden wir die üblichen Schreibweisen mit $+$, $\cdot$ und so weiter.

[3] An der Tafel werde ich stattdessen einen kleinen Pfeil oberhalb der Zeichen machen.

[4] Und auch ein Ring. Erinnern Sie sich an das Beispiel auf Seite 118.

– Ist $\{\mathbf{0}\}$ die triviale Gruppe, dann erhält man dadurch für jeden Körper K einen K-Vektorraum. Dieser *triviale Vektorraum* ist zwar sehr langweilig, weil es nur einen Vektor gibt, aber es ist immer instruktiv, sich die Minimalbeispiele anzuschauen. trivialer Vektorraum
– Und wenn wir schon bei nicht so interessanten, aber trotzdem erwähnenswerten Vektorräumen sind: Setzt man im obigen „Standardbeispiel“ $n = 1$ und identifiziert K^1 mit K, so erhält man, dass jeder Körper K ein Vektorraum über K ist. $+$ und $\oplus$ sind dann identisch und ebenso $\cdot$ und $\odot$. Die Elemente von K sind sowohl Skalare als auch Vektoren.
– Das vorherige Beispiel wird auf einmal wesentlich interessanter, wenn man einen *Teilkörper* L von K betrachtet.[5] Dann ist nämlich K ein Vektorraum über L. Die Elemente von K sind immer noch die Vektoren, aber nur die von L sind auch Skalare. Insbesondere ist $\mathbb{R}$ ein Vektorraum über $\mathbb{Q}$ und $\mathbb{C}$ ein Vektorraum über $\mathbb{R}$ und über $\mathbb{Q}$. Teilkörper

Aufgabe 31.1. Überprüfen Sie durch Nachrechnen, dass die vier aufgezählten Eigenschaften für den $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ erfüllt sind.

Aufgabe 31.2. Sei K der Restklassenkörper $\mathbb{Z}_5$. Wir verwenden die Konvention von Seite 142. Berechnen Sie $(4,3) \oplus (2,4)$ und $3 \odot (2,4)$ in K^2.

Aufgabe 31.3. Verständnisfrage: Wie sieht im trivialen K-Vektorraum $\{\mathbf{0}\}$ die skalare Multiplikation aus?

Rein mathematisch formal betrachtet sind Vektoren nur als Elemente eines Vektorraums existent. Es ergibt also keinen Sinn, von „dem Vektor $(\pi, \sqrt{2})$“ zu sprechen, wenn man nicht vorher vereinbart hat, dass es um den Vektorraum $\mathbb{R}^2$ geht. Speziell für Vektorräume der Form $\mathbb{R}^n$ – und insbesondere für $\mathbb{R}^2$ und $\mathbb{R}^3$ – haben Vektoren jedoch in der Geometrie und in Anwendungen wie der Physik und den Ingenieurwissenschaften noch eine andere Bedeutung, die wir ebenfalls im Hinterkopf behalten sollten, weil sie auch der Sichtweise der Computergrafik entspricht: Vektoren des $\mathbb{R}^n$ werden in diesem Sinne durch *Pfeile* visualisiert. Im $\mathbb{R}^2$ entsprechen die Operationen $\oplus$ und $\odot$ dann dem, was wir uns bereits für die komplexen Zahlen überlegt haben – siehe Seite 172 bzw. Seite 175. Im $\mathbb{R}^3$ kann man sich das analog vorstellen. Wichtig ist dabei lediglich, dass ein Pfeil nur ein *Repräsentant* für einen Vektor ist, während der Vektor als die Menge *aller* Pfeile mit derselben Länge und derselben Richtung zu verstehen ist. Ein Vektor hat als Pfeil also gewissermaßen keinen festen Anfangspunkt, aber durch die Wahl eines Anfangspunktes ist der Pfeil eindeutig festgelegt. Diese Perspektive, die aus der Schule bekannt sein sollte, wird in dem Vorkursvideo *Was sind Vektoren?* ausführlicher dargestellt.

Wie schon bei Ringen ergeben sich aus der Definition einige Rechenregeln, die automatisch in *allen* Vektorräumen gelten. Hier seien nur ein paar exemplarisch aufgeführt.

[5] Das ist so gemeint, dass L ein Unterring von K mit $1 \in L$ und $a^{-1} \in L$ für alle $a \in L$ ist.

Lemma 31.1

Sei V ein K-Vektorraum. Dann gilt für alle $\mathbf{v} \in V$ und alle $\alpha \in K$:[6]

(i) $0 \odot \mathbf{v} = \mathbf{0}$

(ii) $\lambda \odot \mathbf{0} = \mathbf{0}$

(iii) $\lambda \odot \mathbf{v} = \mathbf{0} \Rightarrow \lambda = 0 \vee \mathbf{v} = \mathbf{0}$

(iv) $(-1) \odot \mathbf{v} = \ominus \mathbf{v}$

Beweis. Die erste Behauptung folgt aus $0 \odot \mathbf{v} = (0+0) \odot \mathbf{v} = 0 \odot \mathbf{v} + 0 \odot \mathbf{v}$ mit den bekannten Eigenschaften von Gruppen, die zweite analog mit $\lambda \odot \mathbf{0} = \lambda \odot (\mathbf{0} + \mathbf{0})$.

Gilt $\lambda \cdot \mathbf{v} = \mathbf{0}$ und $\lambda \neq 0$, dann folgt, wie gerade bewiesen,

$$\mathbf{v} = 1 \odot \mathbf{v} = (\lambda^{-1} \cdot \lambda) \odot \mathbf{v} = \lambda^{-1} \odot (\lambda \odot \mathbf{v}) = \lambda^{-1} \odot \mathbf{0} = \mathbf{0}.$$

Das beweist die dritte Behauptung. Die vierte schließlich folgt aus

$$\mathbf{0} = \mathbf{0} \odot \mathbf{v} = \big(1 + (-1)\big) \odot \mathbf{v} = (1 \odot \mathbf{v}) \oplus \big((-1) \odot \mathbf{v}\big) = \mathbf{v} \oplus \big((-1) \odot \mathbf{v}\big). \qquad \blacksquare$$

⋆**Aufgabe 31.4**. Begründung Sie im Detail jedes einzelne Gleichheitszeichen und jede einzelne Folgerung im Beweis von Lemma 31.1.

Um die Unterschiede herauszustellen, wurden bisher die Symbole $\odot$ und $\oplus$ verwendet. Wir werden jedoch in Zukunft dafür einfach $\cdot$ und $+$ schreiben,[7] z. B. $\alpha \cdot (\mathbf{u} + \mathbf{v})$ statt $\alpha \odot (\mathbf{u} \oplus \mathbf{v})$. Das heißt, dass diese Zeichen *je nach Kontext* für unterschiedliche Funktionen stehen! Es wird aber jeweils nur eine mögliche Bedeutung geben, so dass keine Verwechslungsgefahr besteht, wenn man mitdenkt. Außerdem zeigen Rechenregeln wie die in Lemma 31.1, dass man gefahrlos die beiden Multiplikationen und die beiden Additionen gleichberechtigt behandeln und im Prinzip wie in einem Ring rechnen kann.

Nach Untergruppen und Unterringen haben Sie die folgenden Definition sicher schon erwartet.

Definition

Ist V ein K-Vektorraum, dann nennt man eine Teilmenge U von V einen **Untervektorraum** von V, wenn U zusammen mit der auf U bzw. $K \times U$ eingeschränkten Addition und skalaren Multiplikation selbst wieder ein K-Vektorraum ist.

Lemma 31.2

Sei V ein K-Vektorraum und U eine nichtleere Teilmenge von V. U ist genau dann ein Untervektorraum von V, wenn $\mathbf{u} + \mathbf{v} \in U$ und $\alpha \mathbf{v} \in U$ für alle $\mathbf{u}, \mathbf{v} \in U$ und alle $\alpha \in K$ gilt.

[6] Mit $\ominus \mathbf{v}$ ist natürlich das bezüglich $\oplus$ inverse Element zu $\mathbf{v}$ gemeint.

[7] Wir werden außerdem die üblichen Konventionen beibehalten, dass das Multiplikationssymbol oft ganz weggelassen wird und dass gemäß der Regel „Punkt- vor Strichrechnung“ Klammern gespart werden.

Beweis. Durch $\alpha\mathbf{v} \in U$ für alle $\mathbf{v} \in U$ und alle $\alpha \in K$ ist sichergestellt, dass U der Wertebereich der Einschränkung der skalaren Multiplikation auf $K \times U$ ist. Da sich die vier in der Definition eines Vektorraums aufgezählten Eigenschaften wie üblich „nach unten vererben“, muss nur noch gezeigt werden, dass U bezüglich der Vektoraddition eine Untergruppe von V ist. Das folgt aus Lemma 8.5, denn es gilt mittels Lemma 31.1 $\mathbf{u} - \mathbf{v} = \mathbf{u} + (-1) \cdot \mathbf{v} \in U$ für $\mathbf{u}, \mathbf{v} \in U$. ■

Beispiele für Untervektorräume:

- Jeder Vektorraum V hat die trivialen Untervektorräume $\{\mathbf{0}\}$ und V.
- $\{(\lambda, 0) : \lambda \in \mathbb{R}\}$ ist ein Untervektorraum von $\mathbb{R}^2$. Geometrisch interpretiert ist das die horizontale Achse.
- Es geht sogar noch allgemeiner. Für feste Zahlen $a, b \in \mathbb{R}$ ist $\{(\lambda a, \lambda b) : \lambda \in \mathbb{R}\}$ ein Untervektorraum von $\mathbb{R}^2$. Geometrisch interpretiert handelt es sich um eine Gerade durch den Nullpunkt.
- Ist I ein Intervall, dann ist die Menge der stetigen Funktionen von I nach $\mathbb{R}$ ein Untervektorraum von $\mathbb{R}^I$. Das folgt aus Lemma 25.2. Und die Menge der differenzierbaren Funktionen von I nach $\mathbb{R}$ ist ein Untervektorraum dieses Untervektorraums. Das besagen Lemma 26.1 und Korollar 26.3.
- Die Menge $K[x]$ der Polynomfunktionen über dem Körper K bildet einen Untervektorraum von K^K. Insbesondere ist $\mathbb{R}[x]$ ein Untervektorraum des Vektorraums der differenzierbaren Funktionen von $\mathbb{R}$ nach $\mathbb{R}$.

Aufgabe 31.5. Prüfen Sie für die obigen Beispiele mittels Lemma 31.2 selbst nach, dass es sich um Untervektorräume handelt.

Aufgabe 31.6. Die obige Bemerkungen über Geraden durch den Nullpunkt ist nicht ganz korrekt. Wo ist der Fehler?

Definition

Sei X eine nichtleere Menge von Vektoren eines K-Vektorraums. Ist $n \in \mathbb{N}$, so nennen wir ein Tupel

$$\big((\alpha_1, \mathbf{v}_1), \ldots, (\alpha_n, \mathbf{v}_n)\big)$$

aus $(K \times X)^n$ eine **Linearkombination** von bzw. über X, wenn $\mathbf{v}_i \neq \mathbf{v}_j$ für $i \neq j$ gilt. Gilt außerdem $\alpha_i \neq 0$ für alle i, so nennen wir die Linearkombination **reduziert**. Wir sagen, dass diese Linearkombination den Vektor

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n \tag{31.3}$$

darstellt.[8] Ferner schreiben wir $\langle X \rangle$ für die Menge aller Vektoren, die durch Linearkombinationen über X dargestellt werden, und nennen diese Menge von X **erzeugt** bzw. **aufgespannt**.

[8] Für $n = 0$ (also das 0-Tupel), ist mit (31.3) natürlich die leere Summe gemeint, also der Nullvektor. Diese leere Linearkombination ist dann trivialerweise auch reduziert.

Im Vektorraum $\mathbb{R}^2$ ist z. B. $\big((3,(1,0)),(2,(0,2))\big)$ eine Linearkombination, die den Vektor $3\cdot(1,0)+2\cdot(0,2)=(3,4)$ darstellt. $\big((1/2,(6,8)),(0,(-1,1))\big)$ und $\big((2,(0,2)),(3,(1,0))\big)$ stellen ebenfalls diesen Vektor dar, aber eine von beiden ist nicht reduziert. (Welche?) Alle drei Linearkombinationen sind verschieden, die dritte unterscheidet sich von der ersten allerdings nur durch die Reihenfolge. $\big((1/8,(6,8)),(3/8,(6,8))\big)$ ist hingegen *keine* Linearkombination, weil der Vektor $(6,8)$ mehrfach vorkommt.

Die Definition wirkt umständlich, weil es knifflig ist, den Begriff der Linearkombination sauber zu formulieren, und in manchen Lehrbüchern wird das auch etwas schlampig gehandhabt. Eigentlich geht es nämlich nur um Summen der Form (31.3) und wir werden später den allgemeinen Sprachgebrauch übernehmen, Terme wie $\sum_{i=1}^n \alpha_i \mathbf{v}_i$ als Linearkombinationen zu bezeichnen. Im Zweifelsfall sind aber immer die Tupel gemeint und es ist zwischen Linearkombinationen und den durch sie dargestellten Vektoren zu unterscheiden.

Man beachte, dass die Menge X in dieser Definition nicht notwendig endlich sein muss, dass aber Linearkombinationen grundsätzlich immer nur aus endlich vielen Summanden bestehen. Etwas anderes ist auch nicht möglich, weil wir „unendliche Summen“ in beliebigen Vektorräumen gar nicht definiert haben.

Außerdem sei noch einmal wiederholt, dass nach Definition keiner der Vektoren in einer Linearkombination mehrfach vorkommt. Wenn im Folgenden also von Linearkombinationen gesprochen wird, so wird damit immer implizit vorausgesetzt, dass die beteiligten Vektoren paarweise verschieden sind!

Ist X eine endliche Menge $\{\mathbf{w}_1,\dots,\mathbf{w}_k\}$, so schreibt man für $\langle X\rangle$ auch $\langle \mathbf{w}_1,\dots,\mathbf{w}_k\rangle$. Offenbar gilt

$$\langle \mathbf{w}_1,\dots,\mathbf{w}_k\rangle = \Big\{ \sum_{i=1}^k \alpha_i \mathbf{w}_i : (\alpha_1,\dots,\alpha_k)\in K^k \Big\}. \tag{31.4}$$

Aufgabe 31.7. Wie sieht im Vektorraum $\mathbb{R}^3$ die Menge $\langle (1,0,0),(0,2,0)\rangle$ aus?

Aufgabe 31.8. Wie sieht im Vektorraum $\mathbb{R}^2$ die Menge $\langle (1,0),(2,0)\rangle$ aus?

Aufgabe 31.9. Im Vektorraum $\mathbb{R}^{\mathbb{R}}$ sei f_k für $k\in\mathbb{N}$ die Funktion $x\mapsto x^k$. Welche Menge wird von $M=\{f_k : k\in\mathbb{N}\}$ erzeugt?

Aufgabe 31.10. Verständnisfrage: Wieso ist (31.4) überhaupt erwähnenswert? Ist das nicht einfach die Definition von $\langle X\rangle$?

Lemma 31.3 Ist X Teilmenge des Vektorraums[9] V, so ist $\langle X\rangle$ ein Untervektorraum von V.

Beweis. Das zeigt man mit Lemma 31.2. Ist $\mathbf{v}=\sum_{i=1}^n \alpha_i\mathbf{v}_i$ eine Linearkombination über X und $\alpha\in K$, so ist

$$\alpha\mathbf{v}=\sum_{i=1}^n (\alpha\alpha_i)\mathbf{v}_i$$

[9] Wenn hier und im Folgenden der Körper nicht explizit erwähnt wird, dann heißt er K.

ebenfalls eine Linearkombination über X. Ist $\mathbf{w}$ ein weiteres Element von $\langle X\rangle$, so kann man o. B. d. A. annehmen, dass $\mathbf{w}$ die Form $\sum_{i=1}^{n}\beta_i\mathbf{v}_i$ hat.[10]

$$\mathbf{v}+\mathbf{w}=\sum_{i=1}^{n}(\alpha_i+\beta_i)\mathbf{v}_i$$

ist dann auch in $\langle X\rangle$. ■

Definition

Eine Menge X von Vektoren eines Vektorraums V heißt **linear unabhängig** wenn es nur *eine* reduzierte Linearkombination über X gibt, die den Nullvektor darstellt. Anderenfalls bezeichnet man X als **linear abhängig**.

Man beachte, dass es unabhängig von X immer eine reduzierte Linearkombination gibt, die den Nullvektor darstellt – siehe Fußnote 8. Die Definition besagt also, dass es keine weitere geben darf.

In $\mathbb{R}^2$ ist beispielsweise $\{(1,0),(1,1),(0,2)\}$ linear abhängig, denn es gilt

$$1\cdot(1,0)+(-1)\cdot(1,1)+1/2\cdot(0,2)=(0,0).$$

$\{(0,3),(2,0)\}$ ist hingegen linear unabhängig, denn aus

$$\alpha\cdot(0,3)+\beta\cdot(2,0)=(2\beta,3\alpha)=(0,0)$$

folgt offenbar $\alpha=\beta=0$.

Ein interessantes Beispiel für eine unendliche linear unabhängige Menge ist die Menge M aus Aufgabe 31.9.

Aufgabe 31.11. Wenn X linear unabhängig ist, dann gibt es einen Vektor, der mit Sicherheit kein Element von X ist. Welcher ist es und warum?

Aufgabe 31.12. Geben Sie im Vektorraum $\mathbb{R}^3$ zwei verschiedene Linearkombinationen über $X=\{(1,0,0),(0,2,0),(0,0,3)\}$ an, die $(6,6,0)$ darstellen.

Aufgabe 31.13. Geben Sie im Vektorraum $\mathbb{R}^2$ zwei verschiedene reduzierte Linearkombinationen über $X=\{(1,1),(2,0),(0,3)\}$ an, die $(6,6)$ darstellen.

Lemma 31.4

Ist V ein Vektorraum und $X\subseteq V$ linear unabhängig, dann gibt es für jeden Vektor $\mathbf{v}\in V$ bis auf Vertauschung der Reihenfolge höchstens eine reduzierte Linearkombination, die $\mathbf{v}$ darstellt.

Beweis. Gäbe es für ein $\mathbf{v}$ zwei verschiedene solche Darstellungen, so könnte man diese subtrahieren und würde eine Darstellung von $\mathbf{v}-\mathbf{v}=\mathbf{0}$ erhalten, die der Definition der linearen Unabhängigkeit widerspricht.

[10] Ansonsten füllt man mit Nullen auf wie in Aufgabe 31.10.

Subtrahiert man z. B. in der Lösung von Aufgabe 31.4 die ersten beiden Darstellungen in (L-6) voneinander, so erhält man

$$(0,0) = (6,6) - (6,6) = 6 \cdot (1,1) - 3 \cdot (2,0) - 2 \cdot (0,3)$$

als reduzierte Darstellung des Nullvektors. Mit den beiden Darstellungen in (L-7) hätte das nicht geklappt, weil diese bis auf Vertauschung identisch sind. ■

Definition

Eine Teilmenge B eines Vektorraums V heißt **Basis** von V, wenn B linear unabhängig ist und $\langle B \rangle = V$ gilt.

Eine Basis ist immer eine maximal linear unabhängige Menge (in dem Sinne, dass man keine weiteren Vektoren hinzufügen kann) und gleichzeitig eine minimale Menge, die V erzeugt (in dem Sinne, dass man nichts entfernen kann). Siehe dazu die Aufgaben 31.15 und 31.16. Direkt aus Lemma 31.4 folgt außerdem:

Korollar 31.5

Ist B eine Basis des Vektorraums V, dann gibt es für jeden Vektor $\mathbf{v} \in V$ bis auf Vertauschung genau eine reduzierte Linearkombination über B, die $\mathbf{v}$ darstellt.

$\{(1,0),(0,1)\}$ ist z. B. eine Basis für $\mathbb{R}^2$. Das ist hoffentlich angesichts der bisherigen Überlegungen klar. Da es sich hierbei um den prototypischen Fall handelt, wollen wir das gleich verallgemeinern. Wir werden in Zukunft $\mathbf{e}_i$ für ein Tupel schreiben, dessen i-te Komponente 1 ist, während alle anderen Komponenten 0 sind. Diesen Vektor bezeichnen wir als *i-ten Einheitsvektor*.

Einheitsvektor $\mathbf{e}_i$

Diese Definition ist nicht eindeutig, weil wir sowohl $(0,1)$ als auch $(0,1,0)$ als $\mathbf{e}_2$ bezeichnen werden und weil dabei nicht klar ist, *welche* Eins bzw. Null wir meinen. Das wird jedoch immer aus den Kontext hervorgehen. Befinden wir uns beispielsweise im Vektorraum $\mathbb{R}^3$, dann ist mit $\mathbf{e}_1$ der Vektor $(1,0,0)$ gemeint und die Komponenten sind reelle Zahlen.

Es ist nun offensichtlich, dass $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ eine Basis des Vektorraums K^n ist, wenn K ein Körper ist. Diese Basis nennt man auch die *kanonische Basis* von K^n.

kanonische Basis

Die oben bereits erwähnte Menge M aus Aufgabe 31.9 ist eine Basis für $\mathbb{R}[x]$. Sie ist ein Beispiel für eine unendliche Basis.

Man kann beweisen, dass jeder Vektorraum eine Basis hat. Das erfordert jedoch fortgeschrittene Techniken,[11] die wir im Folgenden nicht benötigen werden, weil wir uns nur mit Vektorräumen beschäftigen werden, bei denen klar ist, dass sie eine Basis haben.

Aufgabe 31.14. Begründen Sie, dass X aus Aufgabe 31.12 eine Basis für $\mathbb{R}^3$ ist.

[11] Problematisch kann es werden, wenn die Basen unendlich sind. Sie sind dann nicht immer so leicht anzugeben wie im Beispiel $\mathbb{R}[x]$. Insbesondere benötigt man im Allgemeinen das bereits in Fußnote 5 auf Seite 237 erwähnte *Auswahlaxiom*. Mehr dazu im Video *Das (berühmt-berüchtigte) Auswahlaxiom*.

⋆**Aufgabe 31.15**. Begründen Sie: Gilt $\langle B\rangle = V$ und ist $B' \subseteq V$ eine echte Obermenge von B, dann ist B' nicht linear unabhängig.

⋆**Aufgabe 31.16**. Begründen Sie: Ist $B \subseteq V$ linear unabhängig und B' eine echte Teilmenge von B, dann spannt B' nicht V auf.

Satz 31.6

Ist B eine endliche Basis des Vektorraums V und X eine Teilmenge von V, die mehr als $|B|$ Vektoren enthält, dann ist X linear abhängig.

Beweis. Um nicht in einem Wust von Indizes zu ertrinken, beschränken wir uns auf das übersichtliche Beispiel, dass B nur aus den zwei Vektoren $\mathbf{v}_1$ und $\mathbf{v}_2$ besteht. Wenn Sie das nachvollziehen können, dann sollte es Ihnen nicht schwerfallen, den Beweis auf größere Basen zu verallgemeinern.

Nach Voraussetzung enthält X mindestens drei verschiedene Vektoren $\mathbf{w}_1$ bis $\mathbf{w}_3$. O. B. d. A. ist keiner davon der Nullvektor.[12] Weil B den Raum aufspannt, gibt es $\alpha_1, \alpha_2 \in K$ mit $\mathbf{w}_1 = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2$. Und wegen $\mathbf{w}_1 \neq \mathbf{0}$ kann nicht $\alpha_1 = \alpha_2 = 0$ gelten. Geht man o. B. d. A. von $\alpha_1 \neq 0$ aus, so erhält man $\mathbf{v}_1 = 1/\alpha_1\mathbf{w}_1 - \alpha_2/\alpha_1\mathbf{v}_2$. Das bedeutet jedoch, dass auch $\mathbf{w}_1$ und $\mathbf{v}_2$ den Raum V aufspannen. Insbesondere gibt es $\beta_1, \beta_2 \in K$ mit $\mathbf{w}_2 = \beta_1\mathbf{w}_1 + \beta_2\mathbf{v}_2$.

Gilt $\beta_2 = 0$, so folgt $\mathbf{0} = \beta_1\mathbf{w}_1 - \mathbf{w}_2$ und wir sind fertig. Wir können also $\beta_2 \neq 0$ annehmen und man kann $\mathbf{v}_2$ als $1/\beta_2\mathbf{w}_2 - \beta_1/\beta_2\mathbf{w}_1$ darstellen, woraus folgt, dass auch $\mathbf{w}_1$ und $\mathbf{w}_2$ den Raum V aufspannen.

Deshalb muss es γ_1, γ_2 mit $\mathbf{w}_3 = \gamma_1\mathbf{w}_1 + \gamma_2\mathbf{w}_2$ geben. Mit $\mathbf{0} = \mathbf{w}_3 - \gamma_1\mathbf{w}_1 - \gamma_2\mathbf{w}_2$ ist der Beweis dann beendet. ■

Insbesondere kann das X aus Satz 31.6 also keine Basis sein. Es folgt, dass je zwei endliche Basen eines Vektorraums immer dieselbe Mächtigkeit haben und dass ein Vektorraum nicht sowohl eine endliche als auch eine unendliche Basis haben kann. Daher ist die folgende Definition sinnvoll.[13]

Definition

Hat der Vektorraum V eine endliche Basis B, so sagt man, dass V die **Dimension** $|B|$ hat, und schreibt dafür auch $\dim V$.

Mithilfe der oben vorgestellten kanonischen Basis folgt, dass ein Vektorraum der Form K^n die Dimension n hat. Der bereits mehrfach als Beispiel verwendete Vektorraum $\mathbb{R}[x]$ hat hingegen keine endliche Basis. Das gilt „erst recht“ für die erwähnten Räume aller stetigen Funktionen oder aller Funktionen von $\mathbb{R}$ nach $\mathbb{R}$.

Aufgabe 31.17. Welche Dimension hat der Vektorraum $\{\mathbf{0}\}$?

[12] Denn sonst ist X ohnehin linear abhängig. Siehe Aufgabe 31.11.

[13] Sie wäre auch ohne die Einschränkung auf endliche Basen sinnvoll, weil man zeigen kann, dass auch zwei unendliche Basen desselben Vektorraums dieselbe Mächtigkeit haben. Die Dimension wäre dann eine Kardinalzahl – siehe den Anfang von Abschnitt 22.

Da wir auf einen Beweis dafür verzichten, dass jeder Vektorraum eine Basis hat, müssen wir eigentlich ein paar weitere Details klären. Das geschieht im folgenden Lemma und den beiden optionalen Aufgaben dahinter.

Lemma 31.7

Ist $X \subseteq V$ endlich mit $\langle X \rangle = V$, dann gibt es eine Teilmenge von X, die eine Basis von V ist.

Beweis. Sei $X = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Ist X linear unabhängig, dann haben wir bereits eine Basis. Anderenfalls gibt es Skalare α_1 bis α_n mit $\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$, so dass nicht alle α_i verschwinden. Geht man o. B. d. A. von $\alpha_1 \neq 0$ aus, so ergibt sich

$$\mathbf{v}_1 = -\sum_{i=2}^{n} \frac{\alpha_i}{\alpha_1} \mathbf{v}_i$$

und damit $\mathbf{v}_1 \in \langle X \setminus \{\mathbf{v}_1\} \rangle$. Also spannt schon $X \setminus \{\mathbf{v}_1\}$ den ganzen Raum auf. Ist diese Menge noch keine Basis, so wiederholen wir den Prozess des Entfernens eines Vektors. Da X endlich ist, muss dieser Vorgang nach endlich vielen Schritten terminieren. ■

⋆**Aufgabe 31.18**. Begründen Sie: Hat V eine endliche Basis mit n Elementen und ist U Untervektorraum von V, dann hat U ebenfalls eine endliche Basis und diese Basis hat höchstens n Elemente.

⋆**Aufgabe 31.19**. Begründen Sie: Hat V eine endliche Basis mit n Elementen, dann gibt es zu den Dimensionen 0 bzw. n jeweils nur einen Untervektorraum, nämlich $\{\mathbf{0}\}$ bzw. V.

Die Quintessenz ist, dass ein Vektorraum der Dimension $n \in \mathbb{N}$ für jede natürliche Zahl k mit $0 \leq k \leq n$ Untervektorräume der Dimension k hat, dass das alle seine Untervektorräume sind und dass es für die Grenzfälle $k = 0$ und $k = n$ jeweils nur einen solchen Untervektorraum gibt.

Aufgabe 31.20. Verständnisfrage zur letzten Anmerkung: Wieso muss beispielsweise ein Vektorraum der Dimension 7 einen Untervektorraum der Dimension 3 haben?

In Anlehnung an die Definition für Gruppen von Seite 102 definieren wir nun:

Definition

Sind V und W K-Vektorräume, so nennt man eine Funktion f von V nach W einen **Vektorraumhomomorphismus** bzw. eine **lineare Abbildung**, wenn $f(\mathbf{v}+\mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w})$ und $f(\alpha \cdot \mathbf{v}) = \alpha \cdot f(\mathbf{v})$ für alle $\mathbf{v}, \mathbf{w} \in V$ und alle $\alpha \in K$ gilt. Ist f außerdem eine bijektive Abbildung von V auf W, dann spricht man von einem **Isomorphismus** und sagt, dass V und W **isomorph** sind.[14]

[14] Wie bei den Gruppen verwenden wir nicht die Langform *Vektorraumisomorphismus*, wenn aus dem Kontext klar wird, worum es geht.

Beispielsweise wird durch $f\big((a,b)\big) = (2a,0,3b)$ eine lineare Abbildung von $\mathbb{R}^2$ nach $\mathbb{R}^3$ definiert, wie man leicht überprüft:

$$\begin{aligned} f\big((a,b)+(c,d)\big) &= f\big((a+c,b+d)\big) = \big(2(a+c),0,3(b+d)\big) \\ &= (2a,0,3b)+(2c,0,3d) = f\big((a,b)\big)+f\big((c,d)\big) \\ f\big(\alpha\cdot(a,b)\big) &= f(\alpha a,\alpha b) \\ &= (2\alpha a,0,3\alpha b) = \alpha\cdot(2a,0,3b) = \alpha\cdot f\big((a,b)\big) \end{aligned}$$

Ein interessanteres Beispiel ist die Funktion, die jeder auf ganz $\mathbb{R}$ differenzierbaren Funktion f ihre Ableitungsfunktion f' zuordnet. Nach Lemma 26.1 ist das eine lineare Abbildung. Die Bedeutung der linearen Algebra für die Mathematik rührt daher, dass diverse Operationen aus ganz unterschiedlichen Bereichen lineare Abbildungen sind. Weitere Beispiele sind das Integrieren oder der Erwartungswert in der Stochastik.

Aufgabe 31.21. Warum gibt es keine lineare Abbildung von $\mathbb{Z}_5^3$ nach $\mathbb{Z}_3^3$?

Eine lineare Abbildung von V nach W ist natürlich insbesondere ein Gruppenhomomorphismus der additiven Gruppe von V in die von W. Analog zum Vorgehen in Abschnitt 8 (siehe die Skizze auf Seite 105) kann man nun zeigen:

Satz 31.8

Sei f eine lineare Abbildung von V nach W. Dann bildet f den Nullvektor von V auf den von W ab, $f[V]$ ist ein Untervektorraum von W und $f^{-1}[\{\mathbf{0}\}]$ ist ein Untervektorraum von V. Ist f zudem injektiv, dann ist f^{-1} eine lineare Abbildung von $f[V]$ nach V.

Beweis. Alle Teile des Beweises lassen sich ganz geradlinig ohne besondere „Tricks“ durchführen.

Es gilt $f(\mathbf{0}) = f(\mathbf{0}+\mathbf{0}) = f(\mathbf{0})+f(\mathbf{0})$ und damit muss $f(\mathbf{0})$ der Nullvektor in W sein.

Sind $\mathbf{w}_1$ und $\mathbf{w}_2$ Elemente von $f[V]$, dann gibt es $\mathbf{v}_1$ und $\mathbf{v}_2$ mit $f(\mathbf{v}_i) = \mathbf{w}_i$ für $i = 1,2$. Es folgt

$$\begin{aligned} \mathbf{w}_1+\mathbf{w}_2 = f(\mathbf{v}_1)+f(\mathbf{v}_2) = f(\mathbf{v}_1+\mathbf{v}_2) \in f[V] \quad &\text{sowie} \\ \alpha\mathbf{w}_1 = \alpha f(\mathbf{v}_1) = f(\alpha\mathbf{v}_1) \in f[V] & \end{aligned}$$

für $\alpha \in K$, womit $f[V]$ nach Lemma 31.2 ein Untervektorraum von W ist.

Sind $\mathbf{v}_1$ und $\mathbf{v}_2$ Elemente von $f^{-1}[\{\mathbf{0}\}]$, dann gilt

$$\begin{aligned} f(\mathbf{v}_1+\mathbf{v}_2) = f(\mathbf{v}_1)+f(\mathbf{v}_2) = \mathbf{0}+\mathbf{0} = \mathbf{0} \quad &\text{sowie} \\ f(\alpha\mathbf{v}_1) = \alpha f(\mathbf{v}_1) = \alpha\cdot\mathbf{0} = \mathbf{0} & \end{aligned}$$

für $\alpha \in K$ und damit sind $\mathbf{v}_1+\mathbf{v}_2$ und $\alpha\mathbf{v}_1$ Elemente von $f^{-1}[\{\mathbf{0}\}]$.

Ist f injektiv und sind $\mathbf{w}_1$ und $\mathbf{w}_2$ wie am Anfang des Beweises Elemente von $f[V]$ mit den zugehörigen $\mathbf{v}_i$, so gilt

$$f(\mathbf{v}_1+\mathbf{v}_2) = f(\mathbf{v}_1)+f(\mathbf{v}_2) = \mathbf{w}_1+\mathbf{w}_2 \quad \text{und damit}$$

$$f^{-1}(\mathbf{w}_1+\mathbf{w}_2)=\mathbf{v}_1+\mathbf{v}_2=f^{-1}(\mathbf{w}_1)+f^{-1}(\mathbf{w}_2).$$

Die zweite Eigenschaft zeigt man analog. ■

Kern

Die Menge $f^{-1}[\{\mathbf{0}\}]$ wird auch *Kern* von f genannt und $\ker f$ geschrieben.

Aufgabe 31.22. Begründen Sie: Sind f_1 und f_2 lineare Abbildungen von V_1 nach V_2 bzw. von V_2 nach V_3, so ist $f_2 \circ f_1$ eine lineare Abbildung von V_1 nach V_3.

Satz 31.9

Kern-Bild-Formel
Seien V und W Vektorräume mit endlichen Basen und f eine lineare Abbildung von V nach W. Dann gilt $\dim V = \dim f[V] + \dim\ker f$.

Beweis. $B=\{\mathbf{b}_1,\dots,\mathbf{b}_m\}$ sei eine Basis von $\ker f$ mit m Elementen und $C=\{\mathbf{c}_1,\dots,\mathbf{c}_k\}$ eine Basis von $f[V]$ mit k Elementen. Für jedes $i\in[k]$ wählen wir einen Vektor $\mathbf{a}_i\in V$ mit $f(\mathbf{a}_i)=\mathbf{c}_i$. Offenbar hat $A=\{\mathbf{a}_1,\dots,\mathbf{a}_k\}$ ebenfalls k Elemente und A und B sind disjunkt, so dass $A\cup B$ die Mächtigkeit $k+m=\dim f[V]+\dim\ker f$ hat. Wir zeigen nun, dass $A\cup B$ eine Basis von V ist.

Gilt $\sum_{i=1}^k \alpha_i\mathbf{a}_i+\sum_{i=1}^m \beta_i\mathbf{b}_i=\mathbf{0}$, so folgt

$$\mathbf{0}=f\Big(\sum_{i=1}^k \alpha_i\mathbf{a}_i+\sum_{i=1}^m \beta_i\mathbf{b}_i\Big)=\sum_{i=1}^k \alpha_i\mathbf{c}_i$$

und daher müssen alle α_i verschwinden, weil C linear unabhängig ist. Das impliziert $\sum_{i=1}^m \beta_i\mathbf{b}_i=\mathbf{0}$ und weil B ebenfalls linear unabhängig ist, müssen auch alle β_i verschwinden. Also ist $A\cup B$ linear unabhängig.

Sei nun $\mathbf{v}\in V$ beliebig. Dann gibt es Skalare α_i mit $f(\mathbf{v})=\sum_{i=1}^k \alpha_i\mathbf{c}_i$, weil C eine Basis von $f[V]$ ist. Wegen der Linearität von f folgt

$$f\Big(\mathbf{v}-\sum_{i=1}^k \alpha_i\mathbf{a}_i\Big)=\mathbf{0}$$

und damit ist $\mathbf{v}-\sum_{i=1}^k \alpha_i\mathbf{a}_i$ ein Element von $\ker f$, für das es eine Darstellung $\sum_{i=1}^m \beta_i\mathbf{b}_i$ gibt. Es folgt

$$\mathbf{v}=\sum_{i=1}^k \alpha_i\mathbf{a}_i+\sum_{i=1}^m \beta_i\mathbf{b}_i$$

und damit wurde $\langle A\cup B\rangle = V$ bewiesen. ■

Über Homomorphismen zwischen Vektorräumen gelten dieselben Bemerkungen wie bei Gruppen: Eine lineare Abbildung „überträgt“ die Eigenschaften eines Vektorraums auf ihren Wertebereich. Und sind zwei Vektorräume isomorph, dann sind sie „eigentlich gleich“ und unterscheiden sich nur durch „Umbenennung“ ihrer Vektoren.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lineare Abbildungen sind zudem bereits vollständig definiert, wenn man nur wenige Bilder kennt. Weiß man beispielsweise, dass f eine lineare Abbildung von $\mathbb{R}^2$ nach $\mathbb{R}^3$ mit $f(\mathbf{e}_1) = (3,0,0)$ und $f(\mathbf{e}_2) = (0,0,-1)$ ist, dann kennt man automatisch alle anderen Funktionswerte:

$$\begin{aligned} f(a,b) &= f(a\cdot\mathbf{e}_1 + b\cdot\mathbf{e}_2) = f(a\cdot\mathbf{e}_1) + f(b\cdot\mathbf{e}_2) \\ &= a\cdot f(\mathbf{e}_1) + b\cdot f(\mathbf{e}_2) = a\cdot(3,0,0) + b\cdot(0,0,-1) = (3a,0,-b) \end{aligned}$$

In allgemeiner Form bedeutet das:

Lemma 31.10

Seien f und g lineare Abbildungen von V nach W und B eine Basis von V. Gilt $f(\mathbf{b}) = g(\mathbf{b})$ für alle $\mathbf{b} \in B$, dann gilt $f = g$.

Beweis. Sei $\mathbf{v}$ ein beliebiger Vektor aus V. Weil B eine Basis ist, gibt es $\mathbf{b}_1, \dots, \mathbf{b}_n \in B$ und $\alpha_1, \dots, \alpha_n \in K$ mit $\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$. Wegen der Eigenschaften linearer Abbildungen folgt

$$\begin{aligned} f(\mathbf{v}) &= f\Big(\sum_{i=1}^{n} \alpha_i \mathbf{b}_i\Big) = \sum_{i=1}^{n} f(\alpha_i \mathbf{b}_i) = \sum_{i=1}^{n} \alpha_i f(\mathbf{b}_i) = \sum_{i=1}^{n} \alpha_i g(\mathbf{b}_i) \\ &= \sum_{i=1}^{n} g(\alpha_i \mathbf{b}_i) = g\Big(\sum_{i=1}^{n} \alpha_i \mathbf{b}_i\Big) = g(\mathbf{v}). \end{aligned}$$

■

Umgekehrt gilt aber auch:

Lemma 31.11

Seien V und W Vektorräume, B eine Basis von V und f^* eine Abbildung von B nach W. Dann gibt es genau eine lineare Abbildung f von V nach W mit $f(\mathbf{b}) = f^*(\mathbf{b})$ für alle $\mathbf{b} \in B$.

Beweis. Nach Lemma 31.4 gibt es für jeden Vektor $\mathbf{v} \in V$ eine eindeutig bestimmte Darstellung $\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$ durch eine reduzierte Linearkombination über B. Man definiert nun f durch $f(\mathbf{v}) = \sum_{i=1}^{n} \alpha_i f(\mathbf{b}_i)$. Es ist offensichtlich, dass f so aussehen muss, und Lemma 31.10 besagt ebenfalls, dass es keine andere Möglichkeit gibt.

Dass sich damit wirklich eine lineare Abbildung ergibt, ist leicht überprüft. Hat $\mathbf{v}$ beispielsweise die obige Darstellung, so ergibt sich $\beta\mathbf{v} = \sum_{i=1}^{n} \beta\alpha_i \mathbf{b}_i$ und wiederum wegen Lemma 31.4 muss dies die eindeutige Darstellung von $\beta\mathbf{v}$ sein. Durch simples Einsetzen in die Definition von f rechnet man dann leicht nach, dass $f(\beta\mathbf{v}) = \beta f(\mathbf{v})$ gilt. Für Summen zweier Vektoren läuft das analog. ■

Aufgabe 31.23. Die lineare Abbildung f von $\mathbb{R}^2$ nach $\mathbb{R}^2$ bildet $\mathbf{e}_1$ auf $(2,1)$ und $\mathbf{e}_2$ auf $(2,-4)$ ab. Geben Sie den Vektor $f\big((3,2)\big)$ an.

Aufgabe 31.24. Die lineare Abbildung f von $\mathbb{R}^2$ nach $\mathbb{R}^2$ bildet $\mathbf{e}_1$ auf $(2,1)$ und $2\mathbf{e}_2$ auf $(2,-4)$ ab. Geben Sie den Vektor $f\big((3,2)\big)$ an.

Aufgabe 31.25. Die lineare Abbildung f von $\mathbb{R}^2$ nach $\mathbb{R}^2$ bildet $(2,1)$ auf $(3,2)$ und $(0,2)$ auf $(1,-5)$ ab. Geben Sie den Vektor $f\big((3,1)\big)$ an. (Hinweis: Überlegen Sie zuerst, wie man $(3,1)$ als Linearkombination von $(2,1)$ und $(0,2)$ darstellen kann.)

Aufgabe 31.26. Die lineare Abbildung f von $\mathbb{R}^3$ nach $\mathbb{R}^{\mathbb{R}}$ bildet den Einheitsvektor $\mathbf{e}_k$ auf die Funktion $x \mapsto x^{k-1}$ ab. Was ist $f\big((3,-2,8)\big)$ und wie sieht der Wertebereich von f aus?

Der „krönende“ Abschluss dieses Abschnitts ist die folgende Aussage.

Korollar 31.12

Klassifikationssatz
Ist V ein K-Vektorraum mit der Dimension n, so ist V isomorph zu K^n.

Beweis. Nach Voraussetzung hat V eine Basis B, die aus n Vektoren $\mathbf{b}_1$ bis $\mathbf{b}_n$ besteht. Nach Lemma 31.11 gibt es genau eine lineare Abbildung f von V nach K^n mit $f(\mathbf{b}_i) = \mathbf{e}_i$. Da $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ eine Basis von K^n ist[15] und wegen der Eindeutigkeit der Darstellung bzgl. einer Basis überlegt man sich leicht, dass f eine bijektive Abbildung von V auf K^n ist. ■

Korollar 31.12 besagt, dass es zu jeder Dimension[16] und jedem Körper eigentlich nur einen Vektorraum gibt. (Beispielsweise ist der Wertebereich aus Aufgabe 31.26 nur eine Umbenennung von $\mathbb{R}^3$.) Darum werden wir uns ab jetzt auch meistens auf diese Vektorräume beschränken.

32. Matrizen

Im letzten Abschnitt haben wir gesehen, dass eine lineare Abbildung von einem Vektorraum V in einen Vektorraum W eindeutig festgelegt ist, wenn man die Bilder einer Basis B von V kennt. Außerdem kann man jedes dieser Bilder wiederum eindeutig durch eine Basis C von W darstellen. Ist konkret $B = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ eine Basis von V und $C = \{\mathbf{c}_1, \dots, \mathbf{c}_m\}$ eine von W, dann kann man so eine Abbildung f durch die n Gleichungen

$$f(\mathbf{b}_j) = \sum_{i=1}^{m} a_{i,j}\mathbf{c}_i \qquad (j = 1, \dots, n) \tag{32.1}$$

vollständig beschreiben. Man braucht also lediglich die mn Skalare $a_{i,j}$, die in der Darstellung (32.1) vorkommen. Es stellt sich heraus, dass es sehr vorteilhaft ist, diese Zahlen auf eine bestimmte Art anzuordnen. Dadurch erhält man nämlich einen vielseitig einsetzbaren Kalkül.

Definition

Ein rechteckiges Schema von Objekten aus einer Menge A mit m Zeilen und n Spalten nennt man eine $m \times n$-**Matrix** (bzw. eine Matrix vom **Typ** $m \times n$) über A. Die einzelnen Objekte werden **Komponenten**, **Elemente** oder **Einträge** der

[15] Das war die, die wir oben die kanonische genannt hatten.
[16] Das gilt auch für unendliche Dimensionen, aber das haben wir weder definiert noch bewiesen.

Matrix genannt. Für die Menge aller $m \times n$-Matrizen über A schreiben wir $A^{m\times n}$. Mit

$$(a_{i,j})_{\substack{i=1,\dots,m\\ j=1,\dots,n}}$$

ist die $m \times n$-Matrix gemeint, in deren i-ter Zeile und j-ter Spalte das Objekt $a_{i,j}$ steht. Wenn aus dem Kontext der Typ der Matrix hervorgeht, schreibt man oft auch nur $(a_{i,j})$ oder (a_{ij}).

A wird in der Regel der Körper K der Skalare sein, die Definition ist aber absichtlich etwas allgemeiner gehalten. Wie auch für Vektoren wird im Skript für Matrizen[17] meistens Fettdruck verwendet.

Die Einträge einer Matrix schreiben wir zwischen Klammern und ohne trennende Kommata. Eine 2×3-Matrix $\mathbf{M}$ über $\mathbb{Z}$ könnte beispielsweise so aussehen:

$$\mathbf{M} = \begin{pmatrix} 5 & -2 & 0 \\ 8 & 5 & 13 \end{pmatrix}$$

Sind $\mathbf{A}$ und $\mathbf{B}$ $m \times n$-Matrizen über einem Ring K und ist λ ein Element von K, dann werden die $m \times n$-Matrizen $\mathbf{A}+\mathbf{B}$ und $\lambda \cdot \mathbf{A}$ auf naheliegende Weise durch komponentenweise Operationen definiert. (Siehe Aufgabe 32.1.) Abgesehen von der Darstellung in Zeilen und Spalten passiert offenbar dasselbe wie in (31.1) und (31.2). Daher sollte die folgende Aussage klar sein.

Lemma 32.1 Mit den gerade definierten Verknüpfungen ist $K^{m\times n}$ ein Vektorraum über dem Körper K, der isomorph zu K^{mn} ist.

Aufgabe 32.1. Gegeben seien die 2×3-Matrizen

$$\mathbf{A} = \begin{pmatrix} 5 & 2 & 0 \\ 3 & 1 & 4 \end{pmatrix} \quad \text{und} \quad \mathbf{B} = \begin{pmatrix} 4 & 1 & 4 \\ 4 & 6 & 5 \end{pmatrix}$$

über $\mathbb{Z}_7$. Geben Sie $\mathbf{A}+\mathbf{B}$ und $5 \cdot \mathbf{A}$ an.

⋆**Aufgabe 32.2**. Wie müsste ein Isomorphismus aussehen, der Lemma 32.1 beweist?

Interessant wird der Matrizenkalkül durch das Multiplizieren von Matrizen.

Definition Sei K ein Ring, $\mathbf{A} \in K^{m\times n}$ und $\mathbf{B} \in K^{n\times p}$ mit $\mathbf{A} = (a_{ij})$ und $\mathbf{B} = (b_{jk})$. Dann ist $\mathbf{A} \cdot \mathbf{B}$ definiert als die $m \times p$-Matrix (c_{ij}) mit den Einträgen

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

[17] Wohlgemerkt, der Plural ist *Matrizen*, der Singular *Matrix* (und nicht etwa *Matrize*).

Warum das gerade so definiert wird, klären wir gleich. Zunächst einmal ist entscheidend an dieser Definition, dass man nicht beliebige Matrizen über demselben Ring oder Körper multiplizieren kann. Das Produkt ist nur definiert, wenn die Anzahl der Spalten des ersten Faktors der der Zeilen des zweiten entspricht. Und die verbleibenden beiden Größen (Zeilen des ersten und Spalten des zweiten Faktors) determinieren den Typ des Ergebnisses.

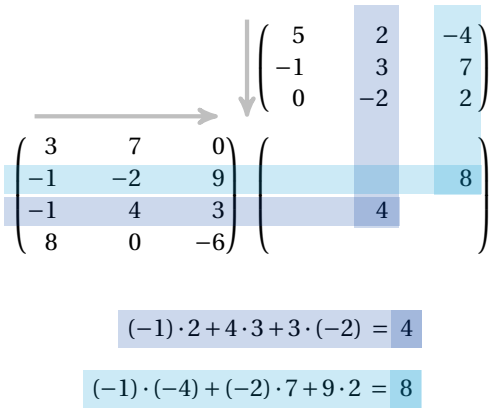
Aufgabe 32.3. Seien $\mathbf{A} \in K^{3\times 5}$, $\mathbf{B} \in K^{3\times 3}$ und $\mathbf{C} \in K^{5\times 3}$. Welche der Produkte

$$\mathbf{A}\cdot\mathbf{A},\ \mathbf{A}\cdot\mathbf{B},\ \mathbf{A}\cdot\mathbf{C},\ \mathbf{B}\cdot\mathbf{A},\ \mathbf{B}\cdot\mathbf{B},\ \mathbf{B}\cdot\mathbf{C},\ \mathbf{C}\cdot\mathbf{A},\ \mathbf{C}\cdot\mathbf{B} \text{ und } \mathbf{C}\cdot\mathbf{C}$$

kann man bilden und welchen Typ hat das Produkt dann jeweils?

Falksches Schema

Wie man Matrizen ohne die Hilfe eines Computers multipliziert, kann man sich wohl am besten mithilfe des sogenannten Falkschen Schemas merken. Das wird in der folgenden Grafik an zwei Beispielen (über $\mathbb{R}$) gezeigt.



Man schreibt die beiden zu multiplizierenden Matrizen so nebeneinander, dass der rechte Faktor nach oben versetzt wird, damit unter ihm Platz für das Produkt ist. Multiplizieren kann man nur dann, wenn die Spaltenzahl links und die Zeilenzahl oben (im Beispiel jeweils drei) übereinstimmen, wenn man also oben links gewissermaßen ein Quadrat hat. Für jeden Eintrag des Produktes betrachtet man nun die auf ihn zeigende Spalte des oberen Faktors sowie die auf ihn zeigende Zeile des linken Faktors. Die entsprechenden Einträge werden paarweise miteinander multipliziert und diese Produkte werden am Ende aufsummiert.

Aufgabe 32.4. Im obigen Beispiel wurden zwei Komponenten des Produktes bereits berechnet. Rechnen Sie die anderen zehn Einträge aus.

Aufgabe 32.5. Berechnen Sie $\mathbf{A}\cdot\mathbf{B}$ und $\mathbf{B}\cdot\mathbf{A}$ für die Matrizen

$$\mathbf{A} = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{und} \quad \mathbf{B} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}.$$

(Wenn nichts anderes erwähnt wird, können Sie immer davon ausgehen, dass über $\mathbb{R}$ gerechnet wird.)

Aufgabe 32.6. Auch Rechnen mit Matrizen kann man mit Wolfram Alpha üben. Für das Produkt $\mathbf{A}\cdot\mathbf{B}$ aus Aufgabe 32.5 gibt man z. B.

```
{{2,0},{1,1}} . {{1,2},{0,0}}
```

ein. (In der Informatik würde man das *row-major order* nennen.)

Offenbar kann man zwei quadratische Matrizen desselben Typs immer multiplizieren und erhält wieder eine Matrix desselben Typs. Die Menge der $n\times n$-Matrizen bildet mit Addition und Multiplikation sogar einen Ring. (Dass die entsprechenden Rechengesetze gelten, kann man durch Nachrechnen verifizieren, siehe Aufgabe 32.7.) Das neutrale Element der Addition ist natürlich die Matrix, deren Komponenten lauter Nullen sind, und die man deswegen als *Nullmatrix* bezeichnet.[18] Aufgabe 32.5 zeigt jedoch, dass diese Ringe nicht kommutativ sind. Allerdings sind sie, wie wir nun sehen werden, unitär.

Nullmatrix

Aufgabe 32.7. Denken Sie sich drei verschiedene 2×2-Matrizen $\mathbf{A}$, $\mathbf{B}$ und $\mathbf{C}$ aus und prüfen Sie nach, dass die Identitäten

$$(\mathbf{A}+\mathbf{B})\cdot\mathbf{C}=\mathbf{A}\cdot\mathbf{C}+\mathbf{B}\cdot\mathbf{C},$$
$$\mathbf{A}\cdot(\mathbf{B}+\mathbf{C})=\mathbf{A}\cdot\mathbf{B}+\mathbf{A}\cdot\mathbf{C}\quad\text{und}$$
$$(\mathbf{A}\cdot\mathbf{B})\cdot\mathbf{C}=\mathbf{A}\cdot(\mathbf{B}\cdot\mathbf{C})$$

gelten. (Noch besser ist es, wenn Sie allgemeine Matrizen wie $\mathbf{A}=(a_{ij})$ verwenden.)

Definition

Ist $\mathbf{A}=(a_{ij})$ eine beliebige $m\times n$-Matrix, so bilden die Einträge der Form a_{ii} für $1\le i\le\min\{m,n\}$ die sogenannte **Hauptdiagonale** von $\mathbf{A}$. Eine $n\times n$-Matrix, in deren Hauptdiagonale Einsen stehen und deren andere Komponenten Nullen sind, nennt man eine **Einheitsmatrix** und schreibt dafür $\mathbf{E}_n$ oder $\mathbb{1}_n$.

Man rechnet leicht nach, dass die folgende Aussage korrekt ist.

Lemma 32.2

Für jede Matrix $\mathbf{A}\in K^{m\times n}$ gilt $\mathbf{A}\cdot\mathbf{E}_n=\mathbf{A}=\mathbf{E}_m\cdot\mathbf{A}$.

Definition

Ein Tupel $B=(\mathbf{b}_1,\dots,\mathbf{b}_n)$ wird **geordnete Basis** des Vektorraums V genannt, wenn $\{\mathbf{b}_1,\dots,\mathbf{b}_n\}$ eine Basis von V mit n Elementen ist. Ist $\mathbf{v}$ ein Element von V mit der Darstellung $\mathbf{v}=\sum_{k=1}^{n}\beta_k\mathbf{b}_k$, dann schreiben wir $\mathbf{v}$ auch als $n\times 1$-Matrix

$$\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}_B \tag{32.2}$$

und lassen den Index unten rechts weg, wenn B die (geordnete) kanonische Basis $(\mathbf{e}_1,\dots,\mathbf{e}_n)$ ist.

[18] Offensichtlich gibt es nicht *die* Nullmatrix, sondern für jeden Typ eine.

Man beachte, dass die Matrix aus (32.2) in diesem Sinne nur eine andere Schreibweise für den Vektor $(\beta_1, \ldots, \beta_n)$ ist, wenn B die kanonische Basis ist.

Nun zeigt sich, wieso die Matrixmultiplikation so und nicht anders definiert ist. Ist nämlich eine lineare Abbildung f von V nach W wie in (32.1) gegeben, so ergibt sich die Darstellung des Funktionswertes $f(\mathbf{v})$ bzgl. der Basis C durch die Multiplikation der Matrix $\mathbf{A} = (a_{ij})$ mit der Matrix (32.2), die $\mathbf{v}$ bzgl. der Basis B darstellt.[19] (Dass das stimmt, kann man einfach nachrechnen.) Wenn wir mit den kanonischen Basen arbeiten, werden wir für dieses Produkt in Zukunft einfach $\mathbf{A} \cdot \mathbf{v}$ schreiben, d. h., wir identifizieren Vektoren mit den Matrizen, die sie darstellen.

Ein konkretes Beispiel: Die Funktion f aus Aufgabe 31.23 wird bzgl. der kanonischen Basis durch die Matrix

$$\mathbf{A} = \begin{pmatrix} 2 & 2 \\ 1 & -4 \end{pmatrix}$$

dargestellt. Eine hilfreiche Merkregel ist dabei: *In den Spalten der Matrix stehen die Bilder der Basisvektoren.* Um wie in der besagten Aufgabe $f\big((3,2)\big)$ zu berechnen, multipliziert man $\mathbf{A}$ mit der Matrix

$$\begin{pmatrix} 3 \\ 2 \end{pmatrix},$$

die stellvertretend für den Vektor $(3,2)$ steht.

Konvention

Wenn nicht explizit etwas anderes erwähnt wird, ist im Folgenden bei der Angabe von Matrizen immer die geordnete kanonische Basis $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ von K^n gemeint.

Aufgabe 32.8. Geben Sie die Matrix an, die die Abbildung aus Aufgabe 31.24 darstellt.

Aufgabe 32.9. Gegeben seien die folgenden beiden linearen Abbildungen:

$$f\colon \begin{cases} \mathbb{R}^3 \to \mathbb{R}^2 \\ (x,y,z) \to (3x-2y, 2y+x) \end{cases} \qquad g\colon \begin{cases} \mathbb{R}^2 \to \mathbb{R}^3 \\ (x,y) \to (y, x, x+y) \end{cases}$$

Geben Sie die Matrix an, die die lineare Abbildung $f \circ g$ darstellt.

Aufgabe 32.10. Die lineare Abbildung $f\colon \mathbb{Z}_5^2 \to \mathbb{Z}_5^3$ wird durch

$$\begin{pmatrix} 1 & 3 \\ 0 & 4 \\ 4 & 1 \end{pmatrix}$$

dargestellt. Geben Sie $f(\mathbf{e}_2)$ und $f\big((2,1)\big)$ an.

[19] Zu beachten ist dabei allerdings, dass dieses Vorgehen erst dadurch eindeutig wird, dass man sich auf geordnete (!) Basen B und C für V und W geeinigt hat.

Ebenfalls durch Nachrechnen verifizieren kann man das folgende Lemma, das besagt, dass die Matrixmultiplikation dem Komponieren von Funktionen entspricht.[20] (Siehe Aufgabe 31.22.)

Lemma 32.3 Sind f_1 und f_2 lineare Abbildungen von V_1 nach V_2 bzw. von V_2 nach V_3, die (bzgl. entsprechender Basen) durch die Matrizen $\mathbf{A}_1$ bzw. $\mathbf{A}_2$ dargestellt werden, dann wird $f_2 \circ f_1$ durch die Matrix $\mathbf{A}_2 \cdot \mathbf{A}_1$ dargestellt.

Aufgabe 32.11. Wie sieht die Matrix aus, die id_{K^n} darstellt?

Aufgabe 32.12. Überprüfen Sie die Korrektheit von Lemma 32.3 anhand der konkreten Matrizen aus Aufgabe 32.9.

33. Geometrische Interpretation linearer Abbildungen

In diesem Abschnitt beschäftigen wir uns hauptsächlich mit den Vektorräumen der Form $\mathbb{R}^n$. Mittels kartesischer Koordinaten kann man sich insbesondere $\mathbb{R}^2$ als Ebene und $\mathbb{R}^3$ als dreidimensionalen Raum vorstellen und in dieser Form werden sie auch in der Computergrafik verwendet. Wir werden für Beispiele in der Regel $\mathbb{R}^2$ verwenden, aber die meisten Aussagen gelten allgemeiner auch für $\mathbb{R}^n$ und manchmal sogar für K^n, wobei K irgendein Körper ist.

Die Vektoren spielen dabei eine Doppelrolle. Einerseits kann ein Vektor einen Punkt im Raum bezeichnen und wird in diesem Zusammenhang als *Ortsvektor* bezeichnet. Andererseits (siehe Seite 287) können Vektoren als nicht an einen Ort gebundene Pfeile interpretiert werden und werden dann *Richtungsvektoren* genannt. Wir werden der üblichen Praxis folgen und in den Bezeichnungen nicht zwischen Punkten, Ortsvektoren und Richtungsvektoren unterscheiden. Man sollte sich jedoch klarmachen, dass die Vektoraddition geometrisch nur in bestimmten Kombinationen Sinn ergibt:

Ortsvektor

Richtungsvektor

- Man kann einen Ortsvektor $\mathbf{p}$ und einen Richtungsvektor $\mathbf{v}$ addieren, wenn man $\mathbf{p}+\mathbf{v}$ als Ortsvektor für den Punkt interpretiert, der sich dadurch ergibt, dass $\mathbf{p}$ in Richtung $\mathbf{v}$ verschoben wurde.
- Man kann zwei Richtungsvektoren $\mathbf{v}_1$ und $\mathbf{v}_2$ addieren und erhält einen neuen Richtungsvektor, der der Verschiebung in Richtung $\mathbf{v}_1$ kombiniert mit der anschließenden Verschiebung in Richtung $\mathbf{v}_2$ entspricht.
- Auch die Multiplikation eines Richtungsvektors mit einem Skalar kann man auf naheliegende Weise interpretieren.
- Für die Addition zweier Ortsvektoren gibt es hingegen keine sinnvolle Interpretation.

Aufgabe 33.1. Sind die Operationen „Ortsvektor minus Richtungsvektor“ bzw. „Ortsvektor minus Ortsvektor“ sinnvoll und wie kann man sie ggf. interpretieren?

[20] Dadurch klärt sich auch, warum die Matrizen, die man multiplizieren will, zueinander passen müssen: Die Komposition der entsprechenden Abbildungen muss sinnvoll sein.

Definition

Sind $\mathbf{p}$ und $\mathbf{v}$ Vektoren des Raum K^n mit $\mathbf{v} \neq \mathbf{0}$, so wird die Menge

$$\mathbf{p} + K\mathbf{v} = \{\mathbf{p} + \lambda\mathbf{v} : \lambda \in K\} \tag{33.1}$$

als **Gerade** bezeichnet. Ist $\mathbf{w}$ ein weiterer Vektor und $\{\mathbf{v}, \mathbf{w}\}$ linear unabhängig, dann nennt man

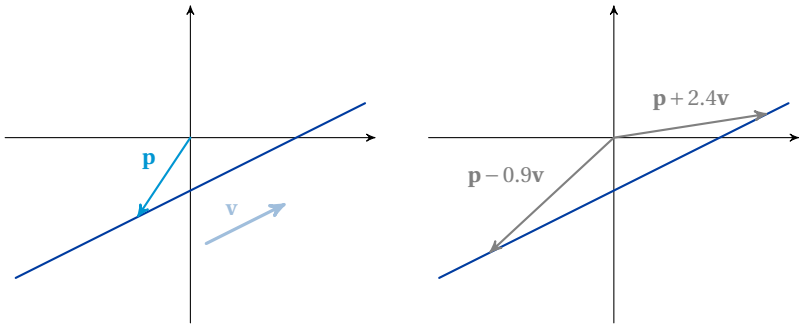
$$\mathbf{p} + K\mathbf{v} + K\mathbf{w} = \{\mathbf{p} + \lambda\mathbf{v} + \mu\mathbf{w} : \lambda, \mu \in K\}$$

eine **Ebene**.
Zwei Vektoren $\mathbf{v}, \mathbf{w} \neq \mathbf{0}$ werden als **parallel** bezeichnet, wenn es ein $\lambda \in K$ mit $\mathbf{v} = \lambda\mathbf{w}$ gibt.[21] Zwei Geraden $\mathbf{p}+K\mathbf{v}$ und $\mathbf{q}+K\mathbf{w}$ werden **parallel** genannt, wenn ihre Richtungsvektoren $\mathbf{v}$ und $\mathbf{w}$ parallel sind.

Auch wenn man das für beliebige Körper im Allgemeinen nicht visualisieren kann, so sind dies offensichtlich direkte Verallgemeinerungen der gewohnten geometrischen Begriffe. Für $\mathbb{R}^2$ bzw. $\mathbb{R}^3$ sollte eine Darstellung wie (33.1) als *Punktrichtungsform* aus der Schule bekannt sein. Man beachte, dass $\mathbf{p}$ hier als Ortsvektor aufgefasst wird, während $\mathbf{v}$ und $\mathbf{w}$ Richtungsvektoren sind. Daher sind Geraden und Ebenen im Ergebnis Mengen von Ortsvektoren bzw. Punkten.

Parameterdarstellung

Die Punktrichtungsform wird übrigens auch *Parameterform* genannt. Allgemein spricht man von einer *Parameterdarstellung*, wenn eine Menge (von Punkten) als Menge von Bildern einer Funktion beschrieben wird. Die Argumente der Funktion nennt man die Parameter. Im Falle der Geraden ist $\lambda \mapsto \mathbf{p} + \lambda\mathbf{v}$ die Funktion und λ der (einzige) Parameter.



affiner Unterraum

Nach den Überlegungen aus dem letzten Abschnitt ist klar, dass Geraden durch den Nullpunkt die einzigen nichttrivialen Untervektorräume des Raums K^2 sind. Ebenso sind Geraden und Ebenen durch den Nullpunkt die einzigen nichttrivialen Untervektorräume von K^3. Allgemeine Geraden und Ebenen sind quasi „verschobene Untervektorräume“, die man *affine Unterräume* nennt.

kollinear

[21] Parallelität ist also einfach eine andere Formulierung dafür, dass $\{\mathbf{v}, \mathbf{w}\}$ linear abhängig ist. Man sagt auch, dass $\mathbf{v}$ und $\mathbf{w}$ *kollinear* sind.

Lemma 33.1

Jede Gerade enthält mindestens zwei Punkte und umgekehrt ist durch zwei Punkte eine Gerade eindeutig bestimmt.

Beweis. Die Gerade (33.1) enthält (mit $\lambda = 0$ und $\lambda = 1$) die Punkte $\mathbf{p}$ und $\mathbf{p}+\mathbf{v}$, die tatsächlich auch verschieden sind, weil $\mathbf{v}$ nicht der Nullvektor ist.[22]

Sind nun zwei verschiedene Punkte $\mathbf{p}_1$ und $\mathbf{p}_2$ gegeben, dann ist

$$g = \mathbf{p}_1 + K(\mathbf{p}_2 - \mathbf{p}_1) \tag{33.2}$$

offenbar eine Gerade, die diese beiden Punkte enthält. Sei $h = \mathbf{p} + K\mathbf{v}$ ebenfalls eine Gerade, die $\mathbf{p}_1$ und $\mathbf{p}_2$ enthält. Dann gibt es $\lambda_1, \lambda_2 \in K$ mit $\mathbf{p}_i = \mathbf{p} + \lambda_i \mathbf{v}$. Ist nun $\mathbf{q} = \mathbf{p}_1 + \lambda(\mathbf{p}_2 - \mathbf{p}_1)$ ein Punkt von g, dann gilt

$$\mathbf{q} = (\mathbf{p} + \lambda_1\mathbf{v}) + \lambda\big((\mathbf{p} + \lambda_2\mathbf{v}) - (\mathbf{p} + \lambda_1\mathbf{v})\big) = \mathbf{p} + \big(\lambda_1 + \lambda(\lambda_2 - \lambda_1)\big)\mathbf{v} \in h.$$

Ist umgekehrt $\mathbf{q} \in h$ mit $\mathbf{q} = \mathbf{p} + \lambda\mathbf{v}$, so rechnet man leicht nach, dass

$$\begin{aligned}\mathbf{q} &= \mathbf{p}_1 + (\mathbf{p} - \mathbf{p}_1) + \lambda\mathbf{v} = \mathbf{p}_1 + (\lambda - \lambda_1)\mathbf{v} \\ &= \mathbf{p}_1 + \frac{\lambda - \lambda_1}{\lambda_2 - \lambda_1} \cdot (\lambda_2 - \lambda_1)\mathbf{v} = \mathbf{p}_1 + \frac{\lambda - \lambda_1}{\lambda_2 - \lambda_1} \cdot (\mathbf{p}_2 - \mathbf{p}_1) \in g\end{aligned}$$

gilt. Damit haben wir $g = h$ gezeigt. ∎

Lemma 33.2

Sind zwei Geraden parallel, dann sind sie identisch oder haben keinen Punkt gemeinsam. Im Raum K^2 gilt auch die Umkehrung dieser Aussage.

Beweis. Die beiden Geraden seien $g = \mathbf{p} + K\mathbf{v}$ und $h = \mathbf{q} + K\mathbf{w}$. Sind sie parallel, dann gilt $\mathbf{v} = \nu\mathbf{w}$ für ein $\nu \in K$. Gibt es einen Punkt $\mathbf{x} \in g \cap h$, so gibt es $\lambda, \mu \in K$ mit

$$\mathbf{p} + \lambda\mathbf{v} = \mathbf{x} = \mathbf{q} + \mu\mathbf{w}. \tag{33.3}$$

Für jeden Punkt $\mathbf{p} + \alpha\mathbf{v} \in g$ gilt dann

$$\mathbf{p} + \alpha\mathbf{v} = \mathbf{p} + \lambda\mathbf{v} + (\alpha - \lambda)\mathbf{v} = \mathbf{q} + \mu\mathbf{w} + (\alpha - \lambda)\nu\mathbf{w} = \mathbf{q} + \big(\mu + \nu(\alpha - \lambda)\big)\mathbf{w} \in h,$$

woraus $g \subseteq h$ folgt. $h \subseteq g$ zeigt man analog mit $\mathbf{w} = \nu^{-1}\mathbf{v}$.

Sind die Geraden nicht parallel, dann ist $\{\mathbf{v}, \mathbf{w}\}$ linear unabhängig (siehe Fußnote 21) und damit eine Basis von K^2. Insbesondere gibt es eine dann genau ein Möglichkeit, den Vektor $\mathbf{p} - \mathbf{q}$ als Linearkombination von $\mathbf{v}$ und $\mathbf{w}$ darzustellen. Das bedeutet, dass es für (33.3) genau eine Lösung gibt. Die Geraden sind daher nicht disjunkt, nach Lemma 33.1 aber auch nicht identisch. ∎

[22] Falls Sie das für Korinthenkackerei halten, dann sei darauf hingewiesen, dass in Räumen der Form $\mathbb{Z}_2^n$ Geraden tatsächlich nur aus zwei Punkten bestehen. Die Lösung von Aufgabe 18.5 zeigt beispielsweise im Prinzip den Raum $\mathbb{Z}_2^3$, der aus nur acht Punkten besteht. In $\mathbb{R}$-Vektorräumen haben Geraden aber natürlich unendlich viele Punkte.

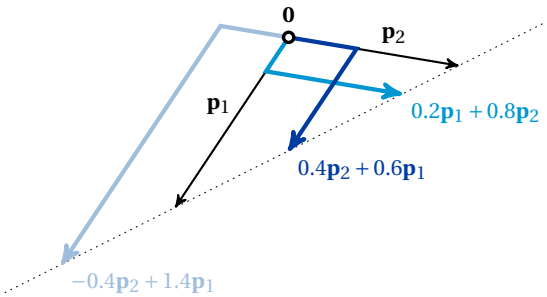
E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lemma 33.3 Ist g eine Gerade, auf der die beiden Punkte $\mathbf{p}_1$ und $\mathbf{p}_2$ liegen, dann ist $\mathbf{p}$ genau dann ein Punkt auf g, wenn es $\lambda, \mu \in K$ mit $\mathbf{p} = \lambda\mathbf{p}_1 + \mu\mathbf{p}_2$ und $\lambda + \mu = 1$ gibt.

Beweis. Setzt man in (33.2) für den Parameter μ ein, so erhält man $(1-\mu)\mathbf{p}_1 + \mu\mathbf{p}_2$ und kann nun λ für $1-\mu$ schreiben. ■

Affinkombination

Die folgende Skizze illustriert Lemma 33.3. Die Darstellung $\mathbf{p} = \lambda\mathbf{p}_1 + \mu\mathbf{p}_2$ ist eine Linearkombination von $\mathbf{p}_1$ und $\mathbf{p}_2$. Zusammen mit der Einschränkung $\lambda + \mu = 1$ spricht man auch von einer *Affinkombination*. In anderen Kontexten nennt man λ und μ manchmal auch die *baryzentrischen Koordinaten* von $\mathbf{p}$.



Strecke

Im Fall $K = \mathbb{R}$ ist anschaulich klar, dass der Punkt $\mathbf{p}$ genau dann *zwischen* $\mathbf{p}_1$ und $\mathbf{p}_2$ liegt (also auf der *Strecke* zwischen den beiden Punkten), wenn sowohl λ als auch μ nichtnegativ sind. Beide Parameter liegen dann im Intervall $[0,1]$. Außerdem kann man aus den Parametern auf die Lage des Punktes schließen. Der Punkt $0.4\mathbf{p}_2 + 0.6\mathbf{p}_1$ in der Skizze teilt die Strecke beispielsweise im Verhältnis $0.4 : 0.6$ bzw. $4 : 6$ in zwei Teile.

Aufgabe 33.2. Liegen die Punkte $(0,5)$ bzw. $(5,0)$ auf der Geraden $(1,2) + \mathbb{R}(-2,6)$?

Aufgabe 33.3. Schneiden sich die Geraden $(1,2) + \mathbb{R}(-2,6)$ und $(2,3) + \mathbb{R}(-5,2)$? Geben Sie in diesem Fall den Schnittpunkt an.

Aufgabe 33.4. Nach Lemma 33.1 ist durch die Punkte $\mathbf{p}_1 = (1,-3,2)$ und $\mathbf{p}_2 = (5,4,8)$ eindeutig eine Gerade g im Raum $\mathbb{R}^3$ bestimmt, die $\mathbf{p}_1$ und $\mathbf{p}_2$ enthält. Geben Sie eine Punktrichtungsform von g an.

Aufgabe 33.5. Analog zu Lemma 33.1 erhält man in der Regel eine Ebene im Raum $\mathbb{R}^3$, die die Punkte $\mathbf{p}_1$ bis $\mathbf{p}_3$ enthält, wenn man die Punktrichtungsform

$$\mathbf{p}_1 + \mathbb{R}(\mathbf{p}_2 - \mathbf{p}_1) + \mathbb{R}(\mathbf{p}_3 - \mathbf{p}_1) \tag{33.4}$$

wählt. Geben Sie so eine Ebene für die Punkte $\mathbf{p}_3 = (7,-1,0)$ sowie $\mathbf{p}_1$ und $\mathbf{p}_2$ aus Aufgabe 33.4 an.

Aufgabe 33.6. Geben Sie ein Beispiel für drei verschiedene Punkte $\mathbf{p}_1$ bis $\mathbf{p}_3$ an, für die (33.4) *keine* Ebene in $\mathbb{R}^3$ liefert.

Lemma 33.4 Eine lineare Abbildung von K^n nach K^m bildet Geraden auf Geraden oder auf einzelne Punkte ab. Ferner sind die Bilder zweier paralleler Geraden wieder parallel (wenn es sich nicht um Punkte handelt). Für $K = \mathbb{R}$ gilt außerdem, dass bei Abbildungen von Geraden auf Geraden die Streckenverhältnisse erhalten bleiben.

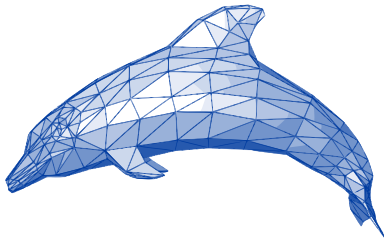
Beweis. Der Hauptteil der Aussage folgt direkt aus Lemma 33.3, denn wenn f so eine lineare Abbildung ist, dann wird ein Punkt der Form $\lambda\mathbf{p}_1 + \mu\mathbf{p}_2$ wegen der Linearität von f auf $\lambda f(\mathbf{p}_1) + \mu f(\mathbf{p}_2)$ abgebildet, die Gerade durch $\mathbf{p}_1$ und $\mathbf{p}_2$ also auf die Gerade durch $f(\mathbf{p}_1)$ und $f(\mathbf{p}_2)$. Die Parameter λ und μ ändern sich dabei nicht. Man muss lediglich den Sonderfall $f(\mathbf{p}_1) = f(\mathbf{p}_2)$ beachten. Für den Rest des Beweises siehe Aufgabe 33.7. ■

⋆**Aufgabe 33.7**. Beweisen Sie die Aussage zur Parallelität aus Lemma 33.4.

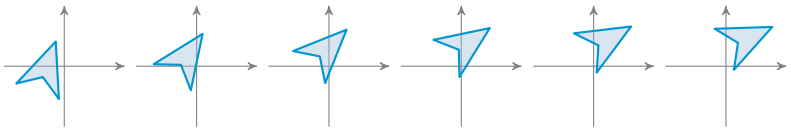
Bevor wir uns spezielle lineare Abbildungen und deren geometrische Interpretation anschauen, ein paar Vorbemerkungen:

- Geometrische Figuren wie Kreise oder Dreiecke in den Räumen $\mathbb{R}^2$, $\mathbb{R}^3$ oder allgemeineren Räumen interpretieren wir als Mengen von Punkten (oder alternativ als Menge der Ortsvektoren dieser Punkte). Das haben wir bei Geraden und Ebenen auf den letzten Seiten bereits getan.
- In diesem Sinne bilden Funktionen von $\mathbb{R}^m$ nach $\mathbb{R}^n$ geometrische Figuren auf geometrische Figuren ab. Uns interessieren im Folgenden hauptsächlich lineare Abbildungen.
- Weil eine lineare Abbildung f aus der Beziehung $\mathbf{q} = \mathbf{p} + \mathbf{v}$ die Beziehung $f(\mathbf{q}) = f(\mathbf{p}) + f(\mathbf{v})$ macht, behalten durch solch eine Funktion sowohl Orts- als auch Richtungsvektoren ihre Rolle. (Mit anderen Worten: Wenn $\mathbf{v}$ den Punkt $\mathbf{p}$ auf den Punkt $\mathbf{q}$ verschiebt, dann verschiebt $f(\mathbf{v})$ den Punkt $f(\mathbf{p})$ auf den Punkt $f(\mathbf{q})$.) Für beliebige Funktionen stimmt das im Allgemeinen nicht – siehe das Beispiel zu den Translationen am Ende des Abschnitts.
- Gilt für eine lineare Abbildung von $\mathbb{R}^m$ nach $\mathbb{R}^n$ die Beziehung $m > n$, so gibt es nach der Kern-Bild-Formel einen „Dimensionsverlust“: ein Teil des Raums $\mathbb{R}^m$ (nämlich der Kern der Abbildung) wird auf den Nullpunkt „zusammengeschrumpft“. Konkret müssen beispielsweise bei einer Abbildung von $\mathbb{R}^3$ nach $\mathbb{R}^2$ aus Kugeln oder Quadern zwei- oder vielleicht sogar eindimensionale Figuren werden.
- Gilt umgekehrt $m < n$, so wird der ganze Raum $\mathbb{R}^m$ in einen echten Untervektorraum von $\mathbb{R}^n$ abgebildet. Bei einer Abbildung von $\mathbb{R}^2$ nach $\mathbb{R}^3$ werden also z. B. alle Bildpunkte in derselben Ebene durch den Nullpunkt liegen.
- Bei „typischen“ linearen Abbildungen von $\mathbb{R}^n$ nach $\mathbb{R}^n$ kann man hingegen erwarten, dass Figuren zumindest ihre Dimension behalten. (Wie wir gleich sehen werden, können sich Größenverhältnisse und Winkel aber durchaus ändern.)

Und falls Sie es als Einschränkung empfinden, dass wir uns nur mit linearen Abbildungen und sehr einfache geometrischen Figuren beschäftigen, dann machen Sie sich klar, dass Grafikprozessoren genau dafür optimiert sind, weil Objekte in der Regel durch kleine Dreiecke approximiert werden.



Wenn wie in der folgenden Grafik eine Animation in einem Computer aus vielen Einzelbildern zusammengesetzt ist, dann lässt sich das daher am effizientesten berechnen, wenn jedes Bild aus dem vorherigen durch eine lineare Abbildung entsteht.



Wir konzentrieren uns auf lineare Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$. Wenn der Bildraum die Dimension 2 hat, dann wird nach Lemma 33.4 das Koordinatengitter, das im Urbildraum aus zwei Scharen äquidistanter paralleler Geraden besteht,[23] abgebildet auf zwei andere Scharen paralleler Geraden, die aber nicht mehr unbedingt rechtwinklig zueinander stehen. Außerdem sind die Abstände innerhalb einer der beiden Scharen zwar nach wie vor gleich, sie müssen aber nicht denen in der anderen Schar entsprechen. Anders ausgedrückt werden aus den Quadraten, in die das Koordinatengitter die Ebene zerlegt, kongruente Parallelogramme.

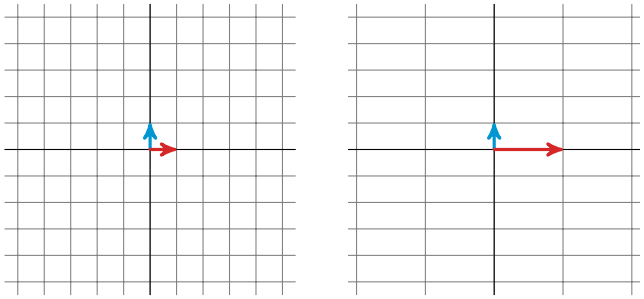
Skalierung

Das erste Beispiel sind *Skalierungen*. Die folgende Skizze zeigt den Effekt einer Matrix der Form

$$\begin{pmatrix} 2.6 & 0 \\ 0 & 1 \end{pmatrix},$$

die sich nur in einer Komponente von der Einheitsmatrix unterscheidet. Hier wird parallel zur x-Achse um den Faktor 2.6 gestreckt, während die y-Koordinaten sich nicht ändern. Selbstverständlich kann man mit Faktoren aus dem Intervall $(0,1)$ auch stauchen oder in y-Richtung skalieren.

[23] Nämlich aus den waagerechten Geraden der Form $(0,z)+\mathbb{R}(1,0)$ für $z \in \mathbb{Z}$ und den senkrechten der Form $(z,0)+\mathbb{R}(0,1)$ für $z \in \mathbb{Z}$.



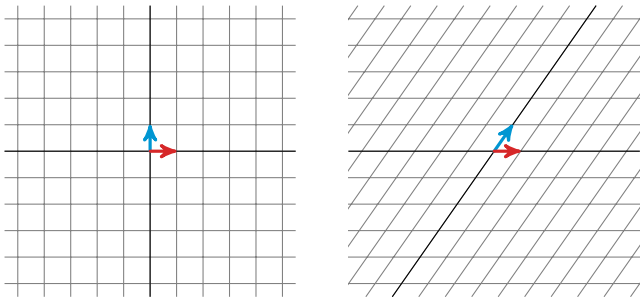
Beachten Sie, dass man anhand der farbig eingezeichneten Bilder der beiden Basisvektoren den ganzen Rest konstruieren kann und dass diese Bilder in den Spalten der Matrix stehen. Beides entspricht dem, was auf den vorherigen Seiten theoretisch erarbeitet wurde, und gilt natürlich auch für alle folgenden Beispiele.

Das zweite Beispiel sind *Scherungen*. Die Matrix zur Skizze ist

Scherung

$$\begin{pmatrix} 1 & 0.7 \\ 0 & 1 \end{pmatrix}. \tag{33.5}$$

Auch hier unterscheidet sich nur eine Komponente von der Einheitsmatrix, allerdings wurde in diesem Fall eine der Nullen modifiziert. Die Punkte behalten ebenfalls ihre y-Koordinate, anders als bei der Skalierung hängt allerdings die horizontale Verschiebung von ihrem Abstand von der x-Achse ab – und davon, ob sie oberhalb oder unterhalb derselben liegen.



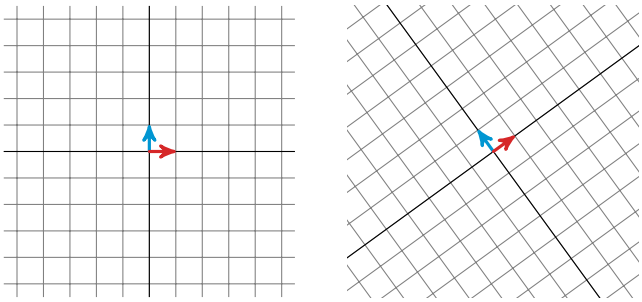
Das dritte Beispiel zeigt eine *Drehung* um den Nullpunkt um den Winkel $\pi/5$. Die Matrix dazu ist

Drehung

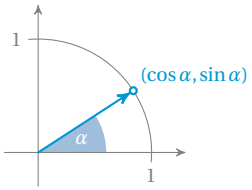
$$\begin{pmatrix} \cos(\pi/5) & -\sin(\pi/5) \\ \sin(\pi/5) & \cos(\pi/5) \end{pmatrix}.$$

Eine lineare Abbildung kann offenbar nur Drehungen um den Nullpunkt darstellen, weil dieser sich nicht bewegen darf.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE



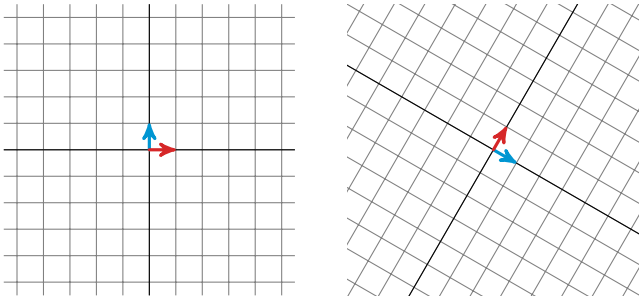
Die erste Spalte der Matrix zeigt den entsprechend gedrehten Einheitsvektor $\mathbf{e}_1$, den man mithilfe der trigonometrischen Funktionen berechnen kann. Die zweite Spalte kann man ebenso aus dem zweiten Einheitsvektor erhalten oder durch Drehung des ersten Funktionswertes um 90 Grad, wie wir es uns schon bei der Multiplikation komplexer Zahlen überlegt hatten.



Spiegelung

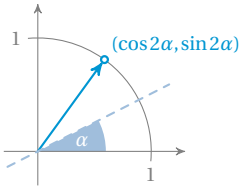
Das vierte Beispiel sieht auf den ersten Blick wie eine Drehung aus, allerdings erkennt man bei genauerem Hinsehen, dass die Bilder der Einheitsvektoren quasi ihre Rolle getauscht haben. Es handelt sich um eine *Spiegelung* an einer durch den Nullpunkt verlaufenden Achse. Die Matrix in diesem Fall ist

$$\begin{pmatrix} \cos(\pi/3) & \sin(\pi/3) \\ \sin(\pi/3) & -\cos(\pi/3) \end{pmatrix}.$$



Wieso kommen auch hier Kosinus, Sinus und Winkel vor? Die Achse, an der gespiegelt wird, ist die Gerade durch den Nullpunkt, die man erhält, wenn man die horizontale Achse um $\pi/6$ dreht. Der in der Matrix verwendete Winkel ist das Doppelte davon. Mithilfe einer kleinen Skizze kann man sich leicht davon überzeugen, wieso die erste Spalte der Matrix so aussehen muss. Die zweite ergibt sich dann durch Drehung der ersten um $-90°$. (Man beachte das Vorzeichen.)

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE



Für das fünfte Beispiel gibt es keine Skizze, weil es im Bildraum kein zweidimensionales Koordinatensystem mehr gibt. Mit einer Matrix wie

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{33.6}$$

erhält man eine *Projektion*. Alle Punkte werden auf die horizontale Achse projiziert. Sie „verlieren“ quasi ihre zweite Koordinate. Anders ausgedrückt: Alle Punkte mit gleicher x-Koordinate werden auf denselben Punkt abgebildet.

Projektion

Die gezeigten Abbildungstypen bilden einen „Baukasten“, aus dem man sich durch Komposition alle linearen Abbildungen zusammenbasteln kann. Das wird in den folgenden Aufgaben an diversen Beispielen durchexerziert.

Aufgabe 33.8. Geben Sie die Matrix für eine Skalierung an, die die gesamte Ebene um den Faktor 3.7 vergrößert.

Aufgabe 33.9. Eine Matrix, in der außerhalb der Hauptdiagonalen nur Nullen stehen, bezeichnet man als *Diagonalmatrix*. Offenbar entsprechen Diagonalmatrizen genau den allgemeinen Skalierungen, bei denen unabhängig voneinander in x- und y-Richtung skaliert wird. Überzeugen Sie sich durch Nachrechnen, dass das Produkt zweier Diagonalmatrizen eine Diagonalmatrix ist.

Diagonalmatrix

Aufgabe 33.10. Sei $\mathbf{A}$ eine $n \times n$-Matrix und λ ein Skalar. Welche Matrix $\mathbf{M}$ sorgt dafür, dass $\mathbf{M} \cdot \mathbf{A} = \lambda \cdot \mathbf{A}$ gilt?

Aufgabe 33.11. Überlegen Sie sich, wie eine Skizze für die Scherung

$$\begin{pmatrix} 1 & 0 \\ -1.2 & 1 \end{pmatrix}$$

aussehen müsste.

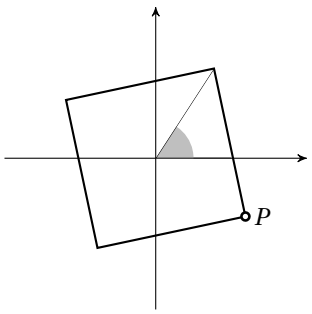
Aufgabe 33.12. Es ist anschaulich naheliegend, dass die Komposition zweier Drehungen (um den Nullpunkt) eine Drehung ist, deren Drehwinkel sich durch die Addition der Drehwinkel der komponierten Abbildungen ergibt. Überzeugen Sie sich durch eine entsprechende Matrixmultiplikation und Anwendung der Additionstheoreme, dass das auch wirklich stimmt.

Aufgabe 33.13. Welche Bewegungen werden durch diese Matrizen beschrieben?

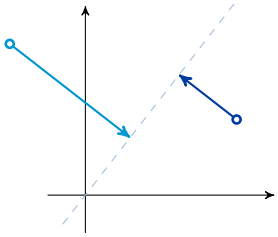
$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Aufgabe 33.14. Geben Sie die Drehmatrix für eine Drehung um 180° an und die Spiegelungsmatrix für eine Spiegelung an der x-Achse. Geben Sie diese Matrizen möglichst ohne Rechnung oder Verwendung trigonometrischer Funktionen an.

Aufgabe 33.15. Das Quadrat in der folgenden Skizze hat den Mittelpunkt im Ursprung des Koordinatensystems und die Seitenlänge 2. Der grau hervorgehobene Winkel beträgt 57°. Geben Sie die kartesischen Koordinaten des Eckpunktes P auf zwei Stellen nach dem Komma an.



Aufgabe 33.16. Geben Sie eine Matrix für die Abbildung an, die Punkte senkrecht auf die Gerade $y = 9x/7$ projiziert. Die Komponenten des Ergebnisses sollen auf zwei Stellen nach dem Komma gerundet sein.

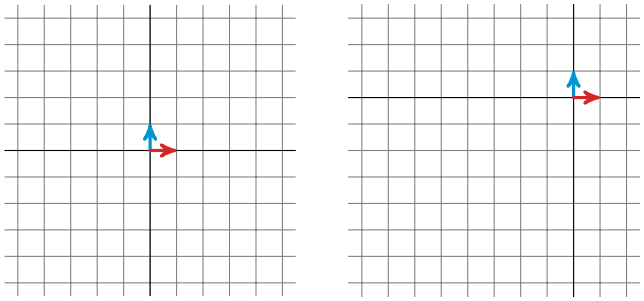


(Hinweis: Setzen Sie die Abbildung aus mehreren Teilen zusammen. Drehen Sie erst so, dass die Projektion sich einfacher als Projektion auf die horizontale Achse hinschreiben lässt, und drehen Sie anschließend wieder zurück. Setzen Sie wie in der Skizze testweise Punkte in Ihre Abbildung ein, um zu überprüfen, ob Ihr Ergebnis plausibel ist.)

Aufgabe 33.17. Geben Sie die Matrix für eine Spiegelung an der Geraden durch den Nullpunkt und den Punkt $(3, 1)$ an. Die Komponenten des Ergebnisses sollen auf zwei Stellen nach dem Komma gerundet sein.

Translation

Eine wichtige Sorte von Funktionen fehlt in der obigen Liste. Es handelt sich um sogenannte *Translationen*, von denen als Beispiel $\mathbf{v} \mapsto \mathbf{v} + (3, 2)$ in der folgenden Skizze gezeigt wird. Man kann sofort sehen, dass es sich *nicht* um eine lineare Abildung handeln kann, weil der Nullpunkt bewegt wird.



Außerdem geht durch Translationen der Zusammenhang zwischen Orts- und Richtungsvektoren verloren. Nennen wir die obige Beispielabbildung f, so gilt mit $\mathbf{p} = (2,3)$, $\mathbf{q} = (3,4)$ und $\mathbf{v} = (1,1)$ zwar $\mathbf{q} = \mathbf{p}+\mathbf{v}$ und wir können $\mathbf{v}$ als Richtungsvektor auffassen, der den Punkt $\mathbf{p}$ nach $\mathbf{q}$ verschiebt, aber es gilt *nicht* $f(\mathbf{q}) = f(\mathbf{p}) + f(\mathbf{v})$ (rechnen Sie nach!), wie es bei einer linearen Abbildung der Fall wäre.

Dass man solche Abbildungen nicht durch eine Matrix darstellen kann, ist für die Anwendungen wohl das größte Problem, weil dadurch eine einheitliche Repräsentation aller relevanten Funktionen verhindert wird. Der nächste Abschnitt zeigt jedoch eine elegante Lösung.

Wir werden an dieser Stelle nicht im Detail auf die Situation im Raum $\mathbb{R}^3$ eingehen. Viele Abbildungen verhalten sich ähnlich, aber insbesondere Drehungen und Spiegelungen sind komplizierter. Sollten Sie beispielsweise für die Computergrafik weitere Informationen benötigen, dann ist das Video *Was Sie schon immer über Drehungen wissen wollten …* wahrscheinlich ein ganz guter Einstieg. Dreidimensionale Drehungen werden zudem in vielen Programmen mithilfe von Quaternionen dargestellt. Das Video Was sind und was sollen die Quaternionen? stellt diese seltsamen „Zahlen“ vor.

34. Homogene Koordinaten

Das im letzten Abschnitt angesprochene Problem, dass Translationen keine linearen Abbildungen sind, lässt sich dadurch aus der Welt schaffen, dass man gleichsam in eine höhere Dimension ausweicht. Formal arbeitet man mit sogenannten *homogenen Koordinaten*, die in der projektiven Geometrie verwendet werden.[24] Die für die Praxis wesentlichen Techniken kann man jedoch ohne die zugehörige Theorie recht leicht verstehen.

Definition

Dem Punkt $(a,b) \in \mathbb{R}^2$ ordnen wir seine **homogenen Koordinaten** $[a,b,1] \in \mathbb{R}^3$ zu.[25] Um den Unterschied hervorzuheben, verwenden wir in diesem Zusammenhang für Vektoren und Matrizen eckige Klammern. Gemeint sind jedoch dieselben Objekte wie vorher.

[24] Im Video *Wie muss man fragen, um "schöne" Antworten zu bekommen?* erfahren Sie mehr über projektive Geometrie.

[25] Das ist eine vereinfachte Definition, die für unsere Zwecke jedoch ausreicht.

Man braucht nun lediglich zwei „Tricks“:

– Wird die lineare Abbildung $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ durch die Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

dargestellt, dann hat die durch

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{34.1}$$

dargestellte lineare Abbildung $f^*\colon \mathbb{R}^3 \to \mathbb{R}^3$ die folgende Eigenschaft: Bildet f den Vektor $\mathbf{v}$ auf den Vektor $\mathbf{w}$ ab, dann bildet f^* die homogenen Koordinaten von $\mathbf{v}$ auf die homogenen Koordinaten von $\mathbf{w}$ ab.

– Ist die Translation $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ durch $f(\mathbf{v}) = \mathbf{v} + (a, b)$ definiert, dann hat die durch

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \tag{34.2}$$

dargestellte lineare Abbildung $f^*\colon \mathbb{R}^3 \to \mathbb{R}^3$ die folgende Eigenschaft: Bildet f den Vektor $\mathbf{v}$ auf den Vektor $\mathbf{w}$ ab, dann bildet f^* die homogenen Koordinaten von $\mathbf{v}$ auf die homogenen Koordinaten von $\mathbf{w}$ ab.

Wie die beiden homogenen Matrizen entstehen, kann man sich leicht dadurch merken, dass die Einheitsmatrix $\mathbf{E}_3$ (graue Ziffern) teilweise überschrieben wird.

Aufgabe 34.1. Überzeugen Sie sich durch Nachrechnen, dass die beiden oben gezeigten „Tricks“ wirklich funktionieren.

Die geometrische Erklärung dafür, was hier passiert: Alle Punkte der Form $(x, y, 1)$ bilden im Raum $\mathbb{R}^3$ eine Ebene E, die parallel zur x-y-Ebene verläuft. Abbildungen vom Typ (34.1) oder (34.2) sind so gebaut, dass sie Punkte aus E auf Punkte aus E abbilden. (In der „dreidimensionalen Welt“ bilden sie Geraden durch den Nullpunkt auf Geraden durch den Nullpunkt ab. In der Ebene E „sieht“ man jeweils nur den Schnittpunkt dieser Geraden mit E.)

Matrizen vom Typ (34.1) übertragen im gewissen Sinne zweidimensionale lineare Abbildungen auf ihr dreidimensionales Pendant: Aus Drehungen um den Nullpunkt werden Drehungen um die z-Achse, aus Spiegelungen an Geraden werden Spiegelungen an Ebenen und so weiter. Matrizen vom Typ (34.2) beschreiben dreidimensionale Scherungen längs der x-y-Ebene. Innerhalb von E „erlebt“ man diese als Translationen.[26]

[26] Ein eindimensionales Wesen, dass auf der Geraden $(0,1) + \mathbb{R}(1,0)$ lebt, würde die Scherung (33.5) ebenfalls als Translation wahrnehmen.

Wenn alle relevanten Abbildungen durch Matrizen repräsentiert werden können, dann können wir wie z. B. in Aufgabe 33.16 mehrere nacheinander ausgeführte Abbildungen zu einer Matrix zusammenfassen. Damit kann man Transformationen, die nicht linear sind, weil sie „am falschen Ort“ stattfinden, durch entsprechende Verschiebungen „linear machen“. Wir schauen uns das am Beispiel einer Drehung um $\pi/6$ um den Punkt $\mathbf{m} = (3,2)$ an. Das ist keine lineare Abbildung, aber man kann sie in die folgenden drei Teile zerlegen:

(i) Translation um $-\mathbf{m}$, so dass $\mathbf{m}$ auf den Ursprung verschoben wird

(ii) die eigentliche Drehung, nun aber mit $\mathbf{0}$ als Mittelpunkt

(iii) Translation um $\mathbf{m}$, um den ersten Schritt wieder rückgängig zu machen

Das Ergebnis sieht so aus:

$$\begin{aligned}&\begin{bmatrix}1&0&3\\0&1&2\\0&0&1\end{bmatrix}\cdot\begin{bmatrix}\cos(\pi/6)&-\sin(\pi/6)&0\\\sin(\pi/6)&\cos(\pi/6)&0\\0&0&1\end{bmatrix}\cdot\begin{bmatrix}1&0&-3\\0&1&-2\\0&0&1\end{bmatrix}\\&=\begin{bmatrix}\sqrt{3}/2&-1/2&4-3\sqrt{3}/2\\1/2&\sqrt{3}/2&1/2-\sqrt{3}\\0&0&1\end{bmatrix}\approx\begin{bmatrix}0.865&-0.500&1.402\\0.500&0.865&-1.232\\0.000&0.000&1.000\end{bmatrix}\end{aligned}\tag{34.3}$$

Aufgabe 34.2. Fällt Ihnen an (34.3) ein gewisses Einsparungspotential auf, wenn Sie das durch die Brille der Informatik betrachten?

Aufgabe 34.3. Sei f die Spiegelung an der y-Achse, g die durch $\mathbf{v} \mapsto \mathbf{v} + (3,2)$ definierte Translation und h die Drehung um den Nullpunkt um 90°. (Damit sind natürlich drei Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$ gemeint.) Geben Sie die homogene 3×3-Matrix an, die die Abbildung $f \circ g \circ h$ repräsentiert.

Aufgabe 34.4. Stellen Sie die Spiegelung an der Geraden $g = \{(2, y) : y \in \mathbb{R}\}$ als Komposition von Translationen und linearen Abbildungen dar und generieren Sie daraus eine 3×3-Matrix, die diese Spiegelung in homogenen Koordinaten realisiert.

Mit homogenen Koordinaten kann man außer Translationen noch weitere Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$, die nicht linear sind, durch 3×3-Matrizen repräsentieren, z. B. die für perspektivische Darstellungen wichtige Zentralprojektion. Und die hier vorgestellten Ideen funktionieren auch dann noch, wenn man im Raum $\mathbb{R}^3$ statt $\mathbb{R}^2$ arbeitet: Man verwendet dann 4×4-Matrizen. In den Kapiteln 32 und 33 von *Konkrete Mathematik (nicht nur) für Informatiker* werden homogene Koordinaten sowie die Anwendung linearer Abbildungen für 3D-Darstellungen in der Computergrafik ausführlicher behandelt.

35. Das Skalarprodukt

In beliebigen Räumen der Form $\mathbb{R}^n$ erhält man keine brauchbare Multiplikation von Vektoren in dem Sinne, dass das Produkt zweier Vektoren wieder ein Vektor ist.

Es gibt jedoch eine anderen Form der Multiplikation, die für die Geometrie sehr hilfreich ist.

Definition

Für Vektoren $\mathbf{x} = (x_1, \ldots, x_n)$ und $\mathbf{y} = (y_1, \ldots, y_n)$ aus $\mathbb{R}^n$ wird ihr **Skalarprodukt** definiert durch $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$. Für $\mathbf{x} \cdot \mathbf{x}$ schreiben wir auch $\mathbf{x}^2$.

Zunächst ein paar Anmerkungen:

- Das Skalarprodukt zweier Vektoren ist ein Skalar und *kein* Vektor. Es handelt sich also *nicht* um eine innere Verknüpfung.
- Die Bezeichnung lässt sich nicht mehr ändern, aber sie ist insofern etwas unglücklich, weil sie so ähnlich wie skalare Multiplikation klingt.
- Für das Skalarprodukt wird je nach Kontext auch die Schreibweise $\langle \mathbf{x}, \mathbf{y} \rangle$ statt $\mathbf{x} \cdot \mathbf{y}$ verwendet – allerdings nicht in diesem Skript.
- Das Zeichen $\cdot$ wird nun sowohl für das Produkt von Skalaren als auch für die skalare Multiplikation als auch für das Skalarprodukt verwendet. Es sollte aber jeweils aus dem Zusammenhang hervorgehen, welches Produkt (Skalar mal Skalar, Skalar mal Vektor, Vektor mal Vektor) gemeint ist.
- Man kann den Begriff *Skalarprodukt* noch allgemeiner definieren. Wir betrachten hier nur das sogenannte *Standardskalarprodukt*.

Aufgabe 35.1. Berechnen Sie das Skalarprodukt der Vektoren $(4, -4, 2)$ und $(9, 1, 5)$. Sie können sich selbst weitere Aufgaben stellen und Ihre Ergebnisse überprüfen, indem Sie in Wolfram Alpha so etwas wie

```
dot product of (4,-4,2) and (9,1,5)
```

eingeben. (Außerdem kennen Sie jetzt das englische Wort für das Skalarprodukt.)

Die folgenden Eigenschaften des Skalarproduktes kann man durch einfaches Nachrechnen beweisen.

Lemma 35.1

Für alle $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ und alle $\alpha \in \mathbb{R}$ gilt

(i) $\mathbf{x} \cdot \mathbf{x} \geq 0$ und $\mathbf{x} \cdot \mathbf{x} = 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$ (*positive Definitheit*)

(ii) $\mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x}$ (*Symmetrie*)

(iii) $(\mathbf{x} + \mathbf{y}) \cdot \mathbf{z} = \mathbf{x} \cdot \mathbf{z} + \mathbf{y} \cdot \mathbf{z}$

(iv) $(\alpha \mathbf{x}) \cdot \mathbf{y} = \alpha \cdot (\mathbf{x} \cdot \mathbf{y})$

Bilinearität

Die Eigenschaften (iii) und (iv) gelten wegen der Symmetrie auch dann, wenn man die Faktoren vertauscht. Beide zusammen nennt man *Bilinearität*, weil sie besagen, dass die beiden Abbildungen $\mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{y}$ und $\mathbf{x} \mapsto \mathbf{y} \cdot \mathbf{x}$ von $\mathbb{R}^n$ nach $\mathbb{R}$ linear sind.

Aufgabe 35.2. Rechnen Sie die Eigenschaften aus Lemma 35.1 mit konkreten Werten durch, um sich zu überzeugen, dass Sie alles richtig verstanden haben.

Satz 35.2

Cauchy-Schwarz-Ungleichung
Für alle $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ gilt $(\mathbf{x} \cdot \mathbf{y})^2 \leq \mathbf{x}^2 \cdot \mathbf{y}^2$ und Gleichheit gilt nur, wenn $\mathbf{x}$ und $\mathbf{y}$ parallel sind.

Beweis. Wir können o. B. d. A. $\mathbf{y} \neq \mathbf{0}$ (und damit $\mathbf{y}^2 \neq 0$) voraussetzen, denn sonst steht ohnehin auf beiden Seiten der Ungleichung 0. Nach Lemma 35.1 gilt für alle $\lambda \in \mathbb{R}$

$$0 \leq (\mathbf{x} - \lambda \mathbf{y})^2 = \mathbf{x}^2 - 2\lambda \mathbf{x} \cdot \mathbf{y} + \lambda^2 \mathbf{y}^2. \tag{35.1}$$

Setzt man speziell $\lambda = (\mathbf{x} \cdot \mathbf{y})/\mathbf{y}^2$ ein, so erhält man

$$0 \leq \mathbf{x}^2 - 2(\mathbf{x} \cdot \mathbf{y})^2/\mathbf{y}^2 + (\mathbf{x} \cdot \mathbf{y})^2/\mathbf{y}^2 = \mathbf{x}^2 - (\mathbf{x} \cdot \mathbf{y})^2/\mathbf{y}^2.$$

Wenn man nun noch mit $\mathbf{y}^2$ multipliziert und anschließend $(\mathbf{x} \cdot \mathbf{y})^2$ addiert, hat man die gewünschte Ungleichung. An (35.1) sieht man wegen der positiven Definitheit zudem, dass sich Gleichheit nur ergeben kann, wenn $\mathbf{x} = \lambda \mathbf{y}$ gilt. ■

Aufgabe 35.3. Für reelle Zahlen x und y gilt natürlich $(x \cdot y)^2 = x^2 \cdot y^2$. Machen Sie sich klar, dass es in der Formulierung von Satz 35.2 aber um andere Produkte geht und dass dort *nicht* auf beiden Seiten der Ungleichung dasselbe steht, obwohl es auf den ersten Blick so aussehen mag.

Aufgabe 35.4. Auch in Satz 35.2 sollten Sie einmal konkrete Werte einsetzen und beide Seiten der Ungleichung ausrechnen, um eine Vorstellung davon zu bekommen, worum es eigentlich geht.

Wir definieren nun einen Begriff, der bereits in Abschnitt 18 kurz vorgestellt wurde.

Definition

Für Vektoren $\mathbf{x} = (x_1, \ldots, x_n)$ aus $\mathbb{R}^n$ wird ihre **Norm** definiert durch

$$\|\mathbf{x}\| = \sqrt{\mathbf{x} \cdot \mathbf{x}} = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Für $n = 2$ ist das der Abstand des Punktes $\mathbf{x}$ vom Nullpunkt bzw. die Länge des Ortsvektors. Das ergibt sich aus dem klassischen Satz des Pythagoras. Für $n = 3$ gilt das ebenfalls, wie die Skizze auf Seite 181 zeigt. Für $n > 3$ können wir die Räume zwar nicht mehr visualisieren, interpretieren diese Zahl aber ebenfalls so.

Aufgabe 35.5. Berechnen Sie die Norm des Vektors $(12, -18, 36)$. Wie Sie sich schon gedacht haben, kann man auch das mit Wolfram Alpha üben:

```
norm of (12,-18,36)
```

Man beachte, dass aus der Definition $\|\mathbf{x}\|^2 = \mathbf{x}^2$ folgt, wobei links ein Produkt zweier reeller Zahlen und rechts ein Skalarprodukt steht. Die Cauchy-Schwarz-Ungleichung kann man damit auch als $|\mathbf{x} \cdot \mathbf{y}| \leq \|\mathbf{x}\| \|\mathbf{y}\|$ formulieren.

Die Norm hat sehr ähnliche Eigenschaften wie der Absolutbetrag. Man vergleiche mit den Lemmata 16.7 und 17.3.

Lemma 35.3

Für alle $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ und alle $\lambda \in \mathbb{R}$ gilt:

(i) $\|\mathbf{x}\| \geq 0$ und $\|\mathbf{x}\| = 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$ (*positive Definitheit*)

(ii) $\|\lambda\mathbf{x}\| = |\lambda| \cdot \|\mathbf{x}\|$ (*absolute Homogenität*)

(iii) $\|\mathbf{x}+\mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$ (*Dreiecksungleichung*)

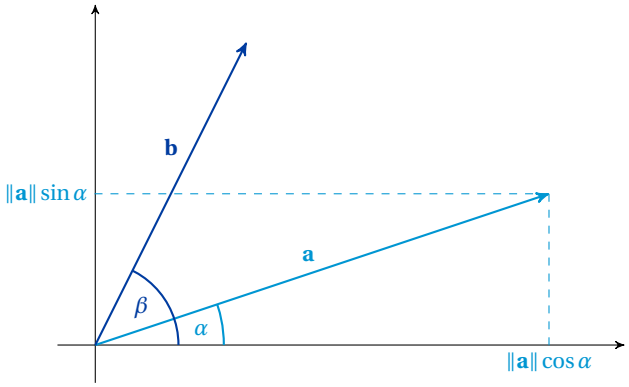
Beweis. Die ersten beiden Punkte kann man durch Einsetzen verifizieren. Für die Dreiecksungleichung erhält man mit Lemma 35.1 und Satz 35.2

$$\begin{aligned}\|\mathbf{x}+\mathbf{y}\|^2 = (\mathbf{x}+\mathbf{y})^2 &= \mathbf{x}^2 + 2\mathbf{x}\cdot\mathbf{y} + \mathbf{y}^2 = \|\mathbf{x}\|^2 + 2\mathbf{x}\cdot\mathbf{y} + \|\mathbf{y}\|^2 \\ &\leq \|\mathbf{x}\|^2 + 2\|\mathbf{x}\|\|\mathbf{y}\| + \|\mathbf{y}\|^2 = (\|\mathbf{x}\| + \|\mathbf{y}\|)^2.\end{aligned}$$

Da Normen nicht negativ sind, kann man auf beiden Seiten die Quadratwurzel nehmen und erhält die gewünschte Ungleichung. ■

Mithilfe die Norm können wir den Abstand zweier Punkte $\mathbf{x}$, $\mathbf{y}$ des Raums $\mathbb{R}^n$ durch $\|\mathbf{x}-\mathbf{y}\|$ berechnen. (Siehe dazu die Skizze in der Lösung von Aufgabe 17.6.) Analog zu den Überlegungen am Anfang von Abschnitt 18 folgt, dass wir damit eine Metrik auf $\mathbb{R}^n$ haben.

Das Skalarprodukt hat allerdings noch eine weitere geometrische Bedeutung. Hat man zwei Vektoren $\mathbf{a}$ und $\mathbf{b}$, die die Winkel α bzw. β mit der positiven horizontalen Achse bilden, so ergibt sich die Situation, die in der folgenden Skizze dargestellt ist.



Für das Skalarprodukt der beiden Vektoren gilt nun nach dem Additionstheorem für den Kosinus

$$\begin{aligned}\mathbf{a}\cdot\mathbf{b} &= \|\mathbf{a}\|(\cos\alpha, \sin\alpha) \cdot \|\mathbf{b}\|(\cos\beta, \sin\beta) \\ &= \|\mathbf{a}\|\|\mathbf{b}\|(\cos\alpha\cos\beta + \sin\alpha\sin\beta) = \|\mathbf{a}\|\|\mathbf{b}\|\cos(\beta-\alpha),\end{aligned} \tag{35.2}$$

wobei $\beta - \alpha$ offensichtlich der Winkel *zwischen* den Vektoren ist. (Und das gilt auch für den Raum $\mathbb{R}^3$.) Das ist eine bemerkenswerte und insbesondere für die Physik wichtige Eigenschaft: Obwohl wir das Skalarprodukt mithilfe von Koordinaten definiert haben, stellt sich heraus, dass es unabhängig von diesen ist und nur von den Längen der Vektoren und ihrer Lage zueinander abhängt.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Wir können auch umgekehrt den Winkel zwischen zwei Vektoren mithilfe von (35.2) ermitteln:[27]

$$\angle(\mathbf{a},\mathbf{b}) = \arccos \frac{\mathbf{a}\cdot\mathbf{b}}{\|\mathbf{a}\|\,\|\mathbf{b}\|} \qquad \angle(\mathbf{a},\mathbf{b})$$

Nach der Cauchy-Schwarz-Ungleichung liegt das Argument für den Arkuskosinus immer im Intervall $[-1,1]$ und der Ausdruck ist damit wohldefiniert (wenn nicht einer der beiden Vektoren der Nullvektor ist). Zu beachten ist allerdings, dass der Arkuskosinus nur Funktionswerte zwischen 0 und π liefert. Geometrisch bedeutet dies, dass $\angle(\mathbf{a},\mathbf{b})$ kein orientierter Winkel ist, sondern dass einfach die kleinere der beiden Alternativen gewählt wird, wenn es zwei gibt.[28]

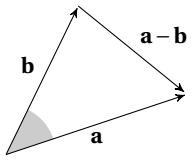
Aufgabe 35.6. Geben Sie den Winkel zwischen $(320,629)$ und $(-40,149)$ in Grad und auf eine Stelle nach dem Komma gerundet an. Sie können Ihr Ergebnis mit der Eingabe

```
vector angle between (320,629) and (-40,149)
```

in Wolfram Alpha überprüfen.

Aufgabe 35.7. Wann stehen zwei Vektoren rechtwinklig aufeinander?

Der Vektorkalkül ermöglicht häufig kurze Beweise von Aussagen, die sich rein geometrisch nur wesentlich umständlicher begründen lassen. Dafür hier nur ein Beispiel.



Kosinusssatz **Satz 35.4**
Für $\mathbf{a},\mathbf{b}\in\mathbb{R}^n\setminus\{\mathbf{0}\}$ gilt $(\mathbf{a}-\mathbf{b})^2 = \mathbf{a}^2+\mathbf{b}^2-2\|\mathbf{a}\|\,\|\mathbf{b}\|\cos\angle(\mathbf{a},\mathbf{b})$.

Beweis. Man berechnet $(\mathbf{a}-\mathbf{b})^2 = \mathbf{a}^2-2\mathbf{a}\cdot\mathbf{b}+\mathbf{b}^2$ und verwendet dann (35.2). ■

Aufgabe 35.8. Was besagt der Kosinussatz für den Fall, dass $\mathbf{a}$ und $\mathbf{b}$ rechtwinklig zueinander stehen?

Aufgabe 35.9. Die $\mathbb{R}^2$-Vektoren $\mathbf{a}$ und $\mathbf{b}$ haben die Längen $\sqrt{10}$ und $\sqrt{15}$. Ferner gilt $\mathbf{a}\cdot\mathbf{b}=0$. Wie lang ist der Vektor $\mathbf{a}+\mathbf{b}$?

Aufgabe 35.10. Die Vektoren $\mathbf{a}$ und $\mathbf{b}$ sind rechtwinklig zueinander, $\mathbf{a}$ hat die Länge $\sqrt{2}$ und $\mathbf{b}$ hat die Länge $\sqrt{3}$. Berechnen Sie das Skalarprodukt $(2\mathbf{a}+2\mathbf{b})\cdot(\mathbf{a}+\mathbf{b})$.

[27] Oder wir könnten ihn unabhängig von der Anschauung für $\mathbb{R}^n$ so definieren.
[28] Weil die Formel symmetrisch in $\mathbf{a}$ und $\mathbf{b}$ ist bzw. weil $\cos(\alpha-\beta)=\cos(\beta-\alpha)$ gilt, kann es auch gar nicht anders sein.

Aufgabe 35.11. Ein Dreieck hat die Eckpunkte $A = (1,1)$, $B = (5,2)$ und $C = (2,4)$. Geben Sie alle Innenwinkel auf zwei Stellen nach dem Komma gerundet an.

Aufgabe 35.12. Ein Dreieck hat die Seitenlängen $r = 19/10$, $s = 23/10$ und $t = 27/10$. Geben Sie mithilfe des Kosinussatzes alle Innenwinkel auf zwei Stellen nach dem Komma gerundet an.

Definition

Eine lineare Abbildung f von $\mathbb{R}^n$ nach $\mathbb{R}^n$ heißt **orthogonal**, wenn für alle $\mathbf{v},\mathbf{w} \in \mathbb{R}^n$ die Beziehung $f(\mathbf{v}) \cdot f(\mathbf{w}) = \mathbf{v} \cdot \mathbf{w}$ gilt. Und eine $n \times n$-Matrix wird **orthogonal** genannt, wenn sie eine orthogonale lineare Abbildung darstellt.

Orthogonale Abbildungen erhalten also das Skalarprodukt. Damit erhalten sie wegen der obigen Überlegungen auch Normen, Abstände und Winkel:

$$\begin{aligned} \|f(\mathbf{v})\| &= \sqrt{f(\mathbf{v}) \cdot f(\mathbf{v})} = \sqrt{\mathbf{v} \cdot \mathbf{v}} = \|\mathbf{v}\| \\ \|f(\mathbf{v}) - f(\mathbf{w})\| &= \|f(\mathbf{v} - \mathbf{w})\| = \|\mathbf{v} - \mathbf{w}\| \\ \angle(f(\mathbf{v}), f(\mathbf{w}) &= \arccos \frac{f(\mathbf{v}) \cdot f(\mathbf{w})}{\|f(\mathbf{v})\| \|f(\mathbf{w})\|} = \arccos \frac{\mathbf{v} \cdot \mathbf{w}}{\|\mathbf{v}\| \|\mathbf{w}\|} = \angle(\mathbf{v},\mathbf{w}) \end{aligned}$$

Definition

Die zu einer $m \times n$-Matrix $\mathbf{A} = (a_{ij})$ **transponierte** $\mathbf{A}^T$ ist die $n \times m$-Matrix (a_{ji}), die man durch Vertauschen der Rollen von Zeilen und Spalten erhält.

Beispielsweise erhält man

$$\mathbf{M}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \quad \text{für} \quad \mathbf{M} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

und natürlich $(\mathbf{A}^T)^T = \mathbf{A}$ für jede Matrix $\mathbf{A}$.

symmetrisch

Aufgabe 35.13. Man nennt eine quadratische Matrix $\mathbf{M}$ *symmetrisch*, wenn $\mathbf{M}^T = \mathbf{M}$ gilt. Die Matrix

$$\mathbf{M} = \begin{pmatrix} a & 2 & b \\ a & b & a-2b \\ 2a & d & c \end{pmatrix}$$

über $\mathbb{R}$ ist symmetrisch. Geben Sie d an.

Die folgende Aussage lässt sich durch simples Hinschreiben nachprüfen, wenn man nicht mit den Indizes durcheinanderkommt.

Lemma 35.5

Sind $\mathbf{A}$ und $\mathbf{B}$ Matrizen, für die das Produkt $\mathbf{A} \cdot \mathbf{B}$ definiert ist, dann ist auch $\mathbf{B}^T \cdot \mathbf{A}^T$ definiert und es gilt $\mathbf{B}^T \cdot \mathbf{A}^T = (\mathbf{A} \cdot \mathbf{B})^T$.

Aufgabe 35.14. Verifizieren Sie (ggf. mithilfe eines Computers wie in Aufgabe 32.6) anhand eines Beispiels, dass Lemma 35.5 korrekt ist.

Identifiziert man wie bisher Vektoren aus dem Raum $\mathbb{R}^n$ mit $n \times 1$-Matrizen, dann entspricht die Berechnung des Skalarproduktes $\mathbf{a} \cdot \mathbf{b}$ der Berechnung des einzigen Eintrags der 1×1-Matrix $\mathbf{a}^T \cdot \mathbf{b}$. Damit erhält man die folgende Aussage:

Lemma 35.6

Eine Matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$ ist genau dann orthogonal, wenn $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}_n$ gilt.

Beweis. Nach Lemma 35.5 sowie dem Absatz vor diesem Lemma ist $\mathbf{A}$ genau dann orthogonal, wenn

$$\mathbf{v}^T \cdot \mathbf{E}_n \cdot \mathbf{w} = \mathbf{v}^T \cdot \mathbf{w} = (\mathbf{A}\mathbf{v})^T \cdot (\mathbf{A}\mathbf{w}) = \mathbf{v}^T \cdot (\mathbf{A}^T \cdot \mathbf{A}) \cdot \mathbf{w}$$

für alle $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ gilt. Sind nun ganz allgemein $\mathbf{B} = (b_{ij})$ und $\mathbf{C} = (c_{ij})$ zwei $n \times n$-Matrizen mit

$$\mathbf{v}^T \cdot \mathbf{B} \cdot \mathbf{w} = \mathbf{v}^T \cdot \mathbf{C} \cdot \mathbf{w}$$

für alle $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, so erhält man speziell mit $\mathbf{v} = \mathbf{e}_i$ und $\mathbf{w} = \mathbf{e}_j$ die Gleichung $b_{ij} = c_{ij}$. Da dass für alle $i, j \in [n]$ gilt, folgt $\mathbf{B} = \mathbf{C}$. ■

Definition

Eine Funktion[29] f von $\mathbb{R}^n$ nach $\mathbb{R}^n$ wird **Isometrie** genannt, wenn sie Abstände nicht ändert, wenn also $\|\mathbf{v} - \mathbf{w}\| = \|f(\mathbf{v}) - f(\mathbf{w})\|$ für alle $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ gilt.

Aufgabe 35.15. Verständnisfrage: Wieso ist jede Isometrie injektiv?

Lemma 35.7

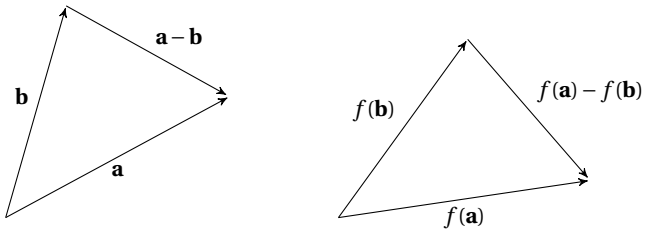
Eine lineare Abbildung von $\mathbb{R}^n$ nach $\mathbb{R}^n$ ist genau dann eine Isometrie, wenn sie orthogonal ist.

Beweis. Dass eine orthogonale lineare Abbildung eine Isometrie ist, ist klar, weil nach den obigen Überlegungen solche Abbildungen unter anderem Abstände erhalten.

Ist umgekehrt die lineare Abbildung $f : \mathbb{R}^n \to \mathbb{R}^n$ eine Isometrie, so gilt zunächst

$$\|f(\mathbf{v})\| = \|f(\mathbf{v}) - \mathbf{0}\| = \|f(\mathbf{v}) - f(\mathbf{0})\| = \|\mathbf{v} - \mathbf{0}\| = \|\mathbf{v}\| \tag{35.3}$$

für alle Vektoren $\mathbf{v}$, d. h., f erhält auch die Norm.



[29] Es wird nicht gefordert, dass f eine lineare Abbildung ist!

Und sind $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$ beliebig, dann bilden die Vektoren $f(\mathbf{a})$, $f(\mathbf{b})$ und $f(\mathbf{a}) - f(\mathbf{b})$ die Seiten eines Dreiecks. Wegen der Erhaltung der Norm und des Abstands hat das von den Vektoren $\mathbf{a}$, $\mathbf{b}$ und $\mathbf{a} - \mathbf{b}$ gebildete Dreieck dieselben Seitenlängen. Daher sind auch alle Winkel gleich, d. h., f erhält auch Winkel. Mit (35.2) folgt, dass f auch das Skalarprodukt erhält. ■

Am Ende des Beweises, als es um die Dreiecke ging, wurde geometrisch argumentiert und das werden wir im Beweis von Korollar 35.8 erneut machen. Man kann das aber im Prinzip auch alles rein vektoriell erledigen – siehe dazu als Beispiel den Kosinussatz oben, der zu drei Seitenlängen eines Dreiecks die Winkel liefern kann.

Aufgabe 35.16. Begründen Sie, warum Translationen immer Isometrien sind.

Die folgende Aussage ist gewissermaßen eine Rechtfertigung dafür, warum es für viele Anwendungen in der Computergrafik ausreicht, sich wie in Abschnitt 34 auf Translationen und einige lineare Abbildungen zu beschränken.

Korollar 35.8

Jede Isometrie von $\mathbb{R}^n$ nach $\mathbb{R}^n$ lässt sich als Komposition einer orthogonalen linearen Abbildung und einer Translation darstellen.

Beweis. Sei $f\colon \mathbb{R}^n \to \mathbb{R}^n$ eine Isometrie, $\tau\colon \mathbb{R}^n \to \mathbb{R}^n$ die durch $\tau(\mathbf{v}) = \mathbf{v} - f(\mathbf{0})$ definierte Translation und $f^* = \tau \circ f$. Offensichtlich (siehe Aufgabe 35.16) ist f^* als Komposition von Isometrien eine Isometrie und es gilt $f^*(\mathbf{0}) = \mathbf{0}$. Wie im Beweis von Lemma 35.7 folgt daraus, dass f^* Norm, Winkel und Skalarprodukt erhält. (Denn ab (35.3) wurde gar nicht mehr verwendet, dass die Abbildung linear ist.)

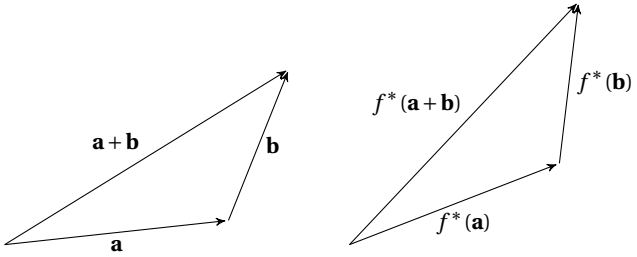
Sind nun $\alpha \in \mathbb{R}$ und $\mathbf{v} \in \mathbb{R}^n$ (mit o. B. d. A. $\alpha\mathbf{v} \neq \mathbf{0}$), so gilt

$$\big(f^*(\mathbf{v}) \cdot f^*(\alpha\mathbf{v})\big)^2 = (\mathbf{v} \cdot \alpha\mathbf{v})^2 = \|\mathbf{v}\|^2 \cdot \|\alpha\mathbf{v}\|^2 = \|f^*(\mathbf{v})\|^2 \cdot \|f^*(\alpha\mathbf{v})\|^2.$$

Nach der Cauchy-Schwarz-Ungleichung sind $f^*(\mathbf{v})$ und $f^*(\alpha\mathbf{v})$ daher parallel, d. h., es gibt ein $\lambda \in \mathbb{R}$ mit $f^*(\alpha\mathbf{v}) = \lambda f^*(\mathbf{v})$. Daraus folgt

$$|\alpha|\|\mathbf{v}\| = \|\alpha\mathbf{v}\| = \|f^*(\alpha\mathbf{v})\| = \|\lambda f^*(\mathbf{v})\| = |\lambda|\|f^*(\mathbf{v})\| = |\lambda|\|\mathbf{v}\|,$$

also $|\lambda| = |\alpha|$. $\lambda = -\alpha$ ist jedoch nicht möglich, weil dann die Winkel zwischen $\mathbf{v}$ und $\alpha\mathbf{v}$ bzw. $f^*(\mathbf{v})$ und $f^*(\alpha\mathbf{v}) = -\alpha f^*(\mathbf{v})$ sich unterscheiden würden. Damit ist $f^*(\alpha\mathbf{v}) = \alpha f^*(\mathbf{v})$ bewiesen.



E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Seien schließlich $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$ und o. B. d. A. $\{\mathbf{a}, \mathbf{b}\}$ linear unabhängig. In der obigen Skizze, die fast wie die im Beweis von Lemma 35.7 aussieht, sieht man links das durch die Vektoraddition $\mathbf{a}+\mathbf{b}$ entstehende Dreieck. Weil Norm und Winkel erhalten bleiben, ist das Dreieck rechts kongruent zum linken. Gleichzeitig ist der Vektor $f^*(\mathbf{a}+\mathbf{b})$ aber offensichtlich auch der, der sich durch Addition von $f^*(\mathbf{a})$ und $f^*(\mathbf{b})$ ergeben muss. Damit erfüllt f^* auch die zweite Bedingung der Linearität.

Insgesamt hat man damit die Zerlegung $f = \tau^{-1} \circ f^*$. ■

Satz 35.9 Die orthogonalen Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$ sind genau die Drehungen und die Spiegelungen.

Beweis. Dass Drehungen und Spiegelungen orthogonal sind, lässt sich leicht mit dem Kriterium aus Lemma 35.6 überprüfen. Und es ist auch geometrisch evident, weil solche Abbildungen offensichtlich Isometrien sind.

Sei nun umgekehrt die Matrix

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

orthogonal. Mit dem Ansatz $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}_n$ sowie der Gleichung[30] $\mathbf{A} \cdot \mathbf{A}^T = \mathbf{E}_n$ erhält man für die einzelnen Komponenten u. a. die vier Gleichungen

$$\begin{aligned} a_{11}^2 + a_{21}^2 &= 1, \\ a_{11}^2 + a_{12}^2 &= 1, \\ a_{21}^2 + a_{22}^2 &= 1 \text{ und} \\ a_{11}a_{21} + a_{12}a_{22} &= 0. \end{aligned}$$

Aus der ersten folgt, dass es einen Winkel α mit $a_{11} = \cos\alpha$ und $a_{21} = \sin\alpha$ gibt. (Siehe Abschnitt 30.) Die zweite und dritte liefern dann $a_{12} = \pm\sin\alpha$ bzw. $a_{22} = \pm\cos\alpha$. Das ergibt vier theoretisch mögliche Kombinationen, von denen jedoch zwei wegen der vierten Gleichung ausscheiden. Die verbleibenden zwei entsprechen genau den Drehungs- bzw. Spiegelungsmatrizen. ■

Im Raum $\mathbb{R}^3$ (und auch in höheren Dimensionen) kann man ebenso vorgehen, wobei man in diesem Fall natürlich mehr rechnen muss.[31] Das sparen wir uns. Es ergibt sich jedenfalls, dass es unabhängig von der Dimension immer zwei Typen von orthogonalen Abbildungen gibt: die Drehungen und die sogenannten *Drehspiegelungen*, die sich als Kombination aus Drehung und Spiegelung darstellen lassen. In der Ebene sind die Drehspiegelungen so simpel, dass sie einfach Spiegelungen sind, in höheren Dimensionen ist es komplizierter. Und auch Drehungen lassen sich in höheren Dimensionen nicht mehr nur einfach durch die Angabe eines Winkels beschreiben. Das müssen Sie bei Bedarf nachschlagen.

Drehspiegelung

[30] Dass diese zweite Gleichung für jede orthogonale Matrix $\mathbf{A}$ gilt, ist nicht völlig trivial und folgt nicht direkt aus Lemma 35.6. Man kann es jedoch z. B. mithilfe von Aufgabe 8.6 zeigen.

[31] Man kann das eleganter machen, dann wird es jedoch auch deutlich abstrakter.

36. Normalenvektoren

In Aufgabe 35.7 hatten wir gesehen, dass zwei Vektoren **a** und **b**, die beide nicht der Nullvektor sind, genau dann rechtwinklig zueinander stehen, wenn $\mathbf{a}\cdot\mathbf{b}=0$ gilt. Man sagt dann auch, dass die beiden Vektoren *orthogonal* sind und schreibt dafür $\mathbf{a}\perp\mathbf{b}$.

orthogonal $\mathbf{a}\perp\mathbf{b}$

Lemma 36.1 Sind die Vektoren $\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^n\setminus\{\mathbf{0}\}$ paarweise orthogonal, dann ist $\{\mathbf{v}_1,\dots,\mathbf{v}_k\}$ eine linear unabhängige Menge mit k Elementen.

Beweis. Dass die Vektoren alle verschieden sind, ist klar, denn sonst gäbe es $i,j\in[k]$ mit $\mathbf{v}_i=\mathbf{v}_j$ und $i\neq j$ und damit $0=\mathbf{v}_i\cdot\mathbf{v}_j=\mathbf{v}_i^2$, woraus $\mathbf{v}_i=\mathbf{0}$ folgen würde.

Wäre $\{\mathbf{v}_1,\dots,\mathbf{v}_k\}$ linear abhängig, dann könnte man o. B. d. A. $\mathbf{v}_1$ als Linearkombination $\sum_{i=2}^{k}\beta_i\mathbf{v}_i$ darstellen. Für alle $j\in\{2,\dots,k\}$ folgt dann jedoch

$$0=\mathbf{v}_j\cdot\mathbf{v}_1=\mathbf{v}_j\cdot\sum_{i=2}^{k}\beta_i\mathbf{v}_i=\beta_j\mathbf{v}_j^2$$

und damit $\beta_j=0$. Das ist offenbar ein Widerspruch. ■

Definition Ein Vektor $\mathbf{v}\in\mathbb{R}^n$ heißt **normiert**, wenn $\|\mathbf{v}\|=1$ gilt. Eine Basis B eines Untervektorraums U von $\mathbb{R}^n$ heißt **Orthogonalbasis** von U, wenn die Vektoren von B paarweise orthogonal sind. Sind zusätzlich alle Vektoren aus B normiert, so spricht man von einer **Orthonormalbasis**.

Die kanonische Basis ist offenbar eine Orthonormalbasis. Es gibt allerdings noch viele weitere Orthonormalbasen. Ein weiteres einfaches Beispiel ist die Basis $\{(1,0),(0,-1)\}$ von $\mathbb{R}^2$.

Aufgabe 36.1. Sei $\alpha\in\mathbb{R}$. Überzeugen Sie sich, dass $\{(\cos\alpha,\sin\alpha),(-\sin\alpha,\cos\alpha)\}$ eine Orthonormalbasis von $\mathbb{R}^2$ ist.

⋆**Aufgabe 36.2**. Der Begriff *orthogonale* Matrix lässt sich damit begründen, dass die Spalten so einer Matrix eine Orthonormalbasis von $\mathbb{R}^n$ bilden. Wieso ist das so?

Aufgabe 36.3. Sei $\mathbf{v}\in\mathbb{R}^n\setminus\{\mathbf{0}\}$. Berechnen Sie die Norm von $(\|\mathbf{v}\|)^{-1}\mathbf{v}$.

Aufgabe 36.4. Normieren Sie den Vektor $\mathbf{v}=(-4,8,1)$.

Lemma 36.2 Zu jedem Untervektorraum U von $\mathbb{R}^n$ gibt es eine Orthonormalbasis.

Beweis. Nach Aufgabe 31.18 hat U eine Basis $\{\mathbf{v}_1,\dots,\mathbf{v}_k\}$ mit k Elementen. Man kann daraus nun rekursiv eine Orthogonalbasis $\{\mathbf{w}_1,\dots,\mathbf{w}_k\}$ konstruieren. Dafür gehen wir davon aus, dass $\{\mathbf{w}_1,\dots,\mathbf{w}_m\}$ für $m<k$ bereits definiert ist und aus m

paarweise orthogonalen Vektoren besteht, die $\langle \mathbf{v}_1, \dots, \mathbf{v}_m \rangle$ aufspannen. Nun macht man den Ansatz

$$\mathbf{w}_{m+1} = \mathbf{v}_{m+1} + \sum_{i=1}^{m} \alpha_i \mathbf{w}_i \quad \text{mit}$$
$$0 \stackrel{!}{=} \mathbf{w}_i \cdot \mathbf{w}_{m+1} = \mathbf{w}_i \mathbf{v}_{m+1} + \alpha_i \mathbf{w}_i^2 \quad \text{für } i \in [m].$$

Die erste Gleichung sorgt dafür, dass $\{\mathbf{w}_1, \dots, \mathbf{w}_{m+1}\}$ den Raum $\langle \mathbf{v}_1, \dots, \mathbf{v}_{m+1} \rangle$ aufspannt, die folgenden garantieren, dass $\mathbf{w}_{m+1}$ orthogonal zu allen bisher konstruierten Vektoren ist. Außerdem liefert jede von ihnen einen der Koeffizienten α_i. Alle zusammen liefern eine Darstellung für $\mathbf{w}_{m+1}$ mit den gewünschten Eigenschaften.

Man beachte, dass nach dieser Konstruktion $\mathbf{w}_1 = \mathbf{v}_1$ gilt. Man kann also ein Element der Orthogonalbasis frei aus denen der ursprünglichen Basis auswählen. Eine Orthonormalbasis erhält man anschließend durch Normieren (Aufgabe 36.3) der Vektoren $\mathbf{w}_1$ bis $\mathbf{w}_k$. ■

Aufgabe 36.5. Mit $\mathbf{v}_1 = (1,2,-3,0)$, $\mathbf{v}_2 = (2,3,1,3)$ und $\mathbf{v}_3 = (4,4,0,0)$ ist $B = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ Basis eines dreidimensionalen Untervektorraums U von $\mathbb{R}^4$. (Ist B wirklich linear unabhängig?) Konstruieren Sie wie im Beweis von Lemma 36.2 eine Orthogonalbasis von U, die $\mathbf{v}_1$ enthält.

Korollar 36.3

Für $n > 0$ hat $\mathbb{R}^n$ zu jedem Vektor $\mathbf{v} \neq 0$ eine Orthogonalbasis, die $\mathbf{v}$ enthält.

Beweis. Wie in der Lösung von Aufgabe 31.18 kann man einen Basis von $\mathbb{R}^n$ konstruieren, indem man mit $\mathbf{v}$ als erstem Element beginnt. Und wie im Beweis von Lemma 36.2 kann man daraus eine Orthogonalbasis machen, die $\mathbf{v}$ enthält. ■

Korollar 36.4

Eine Menge U von Vektoren ist genau dann ein Untervektorraum von $\mathbb{R}^n$ der Dimension $n-1$, wenn man U als

$$\{\mathbf{x} \in \mathbb{R}^n : \mathbf{n} \cdot \mathbf{x} = 0\} \tag{36.1}$$

mit einem Vektor $\mathbf{n} \neq \mathbf{0}$ darstellen kann.

Beweis. Sei zuerst U ein Untervektorraum mit $\dim U = n-1$ und $B = \{\mathbf{b}_1, \dots, \mathbf{b}_{n-1}\}$ eine Orthogonalbasis von U, die nach Lemma 36.2 existiert. Weil U eine echte Teilmenge von $\mathbb{R}^n$ ist, gibt es einen Vektor $\mathbf{v} \in \mathbb{R}^n \setminus U$ und offenbar ist $B \cup \{\mathbf{v}\}$ eine Basis von $\mathbb{R}^n$. Mit demselben Ansatz wie im Beweis von Lemma 36.2 macht man daraus eine Orthonormalbasis $B \cup \{\mathbf{n}\}$ von $\mathbb{R}^n$. Damit ist offensichtlich, dass U die Menge (36.1) ist.

Umgekehrt sei U eine Menge der Form (36.1) mit $\mathbf{n} \neq \mathbf{0}$. Mit $\mathbf{u}_1, \mathbf{u}_2 \in U$ und $\alpha \in \mathbb{R}$ hat man dann

$$\mathbf{n} \cdot (\mathbf{u}_1 + \mathbf{u}_2) = \mathbf{n} \cdot \mathbf{u}_1 + \mathbf{n} \cdot \mathbf{u}_2 = 0 + 0 = 0 \quad \text{und}$$

$$\mathbf{n}\cdot(\alpha\mathbf{u}_1)=\alpha(\mathbf{n}\cdot\mathbf{u}_1)=\alpha\cdot 0=0,$$

woraus nach Lemma 31.2 folgt, dass U ein Untervektorraum ist. Ist nun $\mathbf{v}\in\mathbb{R}^n$ beliebig, so gilt mit $\alpha=(\mathbf{n}\cdot\mathbf{v})(\mathbf{n}^2)^{-1}$ für $\mathbf{u}=\mathbf{v}-\alpha\mathbf{n}$ offenbar $\mathbf{n}\cdot\mathbf{u}=0$ und damit $\mathbf{u}\in U$. Wegen $\mathbf{v}=\mathbf{u}+\alpha\mathbf{n}$ folgt somit, dass $B\cup\{\mathbf{n}\}$ eine Basis von $\mathbb{R}^n$ ist, wenn B eine Basis von U ist. ■

Definition

Ist U ein Untervektorraum von $\mathbb{R}^n$ der Dimension $n-1$ und $\mathbf{a}\in\mathbb{R}^n$, dann nennt man einen affinen Unterraum der Form

$$\mathbf{a}+U=\{\mathbf{a}+\mathbf{u}:\mathbf{u}\in U\}$$

eine **Hyperebene** in $\mathbb{R}^n$.

Die Hyperebenen in $\mathbb{R}^2$ sind also die Geraden, die Hyperebenen in $\mathbb{R}^3$ die Ebenen.

Satz 36.5

Ist $\mathbf{n}\in\mathbb{R}^n\setminus\{\mathbf{0}\}$ und $k\in\mathbb{R}$, dann ist

$$\{\mathbf{x}\in\mathbb{R}^n:\mathbf{n}\cdot\mathbf{x}-k=0\} \tag{36.2}$$

eine Hyperebene in $\mathbb{R}^n$. Umgekehrt gibt es zu jeder Hyperebene $\mathbf{a}+U$ in $\mathbb{R}^n$ einen Vektor $\mathbf{n}\in\mathbb{R}^n\setminus\{\mathbf{0}\}$ und ein $k\in\mathbb{R}$, so dass $\mathbf{a}+U$ die Menge in (36.2) ist. Man kann dabei erreichen, dass $\mathbf{n}$ normiert und k nichtnegativ ist.

Beweis. Sei zuerst $W=\{\mathbf{x}\in\mathbb{R}^n:\mathbf{n}\cdot\mathbf{x}-k=0\}$ gegeben. Für den Vektor $\mathbf{a}=k(\mathbf{n}^2)^{-1}\mathbf{n}$ gilt offenbar $\mathbf{n}\cdot\mathbf{a}=k$. Ferner ist $U=\{\mathbf{x}\in\mathbb{R}^n:\mathbf{n}\cdot\mathbf{x}=0\}$ nach Korollar 36.4 ein Untervektorraum der Dimension $n-1$. Für einen beliebigen Vektor $\mathbf{x}\in\mathbb{R}^n$ sind nun offenbar die Aussagen $\mathbf{x}\in W$, $\mathbf{n}\cdot\mathbf{x}-k=0$, $\mathbf{n}\cdot(\mathbf{x}-\mathbf{a})=0$, $\mathbf{x}-\mathbf{a}\in U$ und $\mathbf{x}\in\mathbf{a}+U$ äquivalent.

Ist umgekehrt eine Hyperebene $\mathbf{a}+U$ gegeben, so wähle man gemäß Korollar 36.4 ein $\mathbf{n}$ mit $U=\{\mathbf{x}\in\mathbb{R}^n:\mathbf{n}\cdot\mathbf{x}=0\}$, und setze $k=\mathbf{n}\cdot\mathbf{a}$. Man erhält nun dieselben Äquivalenzen wie eben. Wenn dies gewünscht ist, kann man $\mathbf{n}$ (vor der Berechnung von k) noch normieren. Und sollte k negativ sein, so ersetze man $\mathbf{n}$ durch $-\mathbf{n}$. ■

Normalenform
Normalenvektor
hessesche Normalenform

Eine Darstellung der Form (36.2) nennt man eine *Normalenform* der Hyperebene und $\mathbf{n}$ den *Normalenvektor*.[32] Ist $\mathbf{n}$ normiert und k nichtnegativ, dann handelt es sich um die sogenannte *hessesche Normalenform*, die nach dem Mathematiker Otto Hesse (und nicht nach dem Bundesland Hessen!) benannt ist.

Aufgabe 36.6. Geben Sie einen Vektor aus $\mathbb{R}^2$ an, der senkrecht auf $(5,2)$ steht.

Aufgabe 36.7. Geben Sie für die Gerade $g=(-3,2)+\mathbb{R}(1,-4)$ die hessesche Normalenform an.

[32] Man beachte, dass das Adjektiv *normal* in diesem Zusammenhang für rechtwinklig steht und nichts mit der Norm zu tun hat.

Definition

Ist (X,d) ein metrischer Raum und sind A und B nichtleere Teilmengen von X, so definiert man den **Abstand** von A und B als

$$d(A,B) = \inf\{d(a,b) : a \in A \wedge b \in B\}.$$

Im Fall $A = \{a\}$ schreibt man auch $d(a,B)$ statt $d(A,B)$ und bezeichnet diesen Wert natürlich als den **Abstand** von a zur Menge B.

Aufgabe 36.8. Verständnisfrage: Wieso existiert das Infimum aus der Definition des Abstands immer?

Das Infimum in der Definition lässt sich nicht durch ein Minimum ersetzen. Betrachtet man beispielsweise die Mengen $A = U_1(\mathbf{0})$ und $B = U_1\big((2,0)\big)$ im Raum $\mathbb{R}^2$, dann gilt zwar $d(A,B) = 0$, aber es gibt keine Punkte $a \in A$ und $b \in B$ mit $d(a,b) = 0$. In der Situation, die das folgende Lemma beschreibt, wird jedoch ein Minimum angenommen.

Lemma 36.6

Ist die Hyperebene $W = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{n}\cdot\mathbf{x} - k = 0\}$ in hessescher Normalenform gegeben, so gilt $d(\mathbf{p},W) = |\mathbf{n}\cdot\mathbf{p} - k|$ für alle $\mathbf{p} \in \mathbb{R}^n$. Zudem gibt es einen Vektor $\mathbf{w} \in W$ mit $d(\mathbf{p},W) = \|\mathbf{p}-\mathbf{w}\|$ und $\mathbf{p}-\mathbf{w}$ steht senkrecht auf dem zu W gehörenden Untervektorraum.

Beweis. Nach Korollar 36.4 und Satz 36.5 sowie den jeweiligen Beweisen gibt es einen Untervektorraum U von $\mathbb{R}^n$ der Dimension $n-1$, so dass W die Form $k\mathbf{n}+U$ hat. (Dabei ist wesentlich, dass $\mathbf{n}$ normiert ist.) Ferner lässt sich $\mathbf{p}$ als $(\mathbf{n}\cdot\mathbf{p})\mathbf{n}+\mathbf{u}_0$ mit $\mathbf{u}_0 \in U$ darstellen und es gilt $\mathbf{n}\cdot\mathbf{u} = 0$ für alle $\mathbf{u} \in U$.

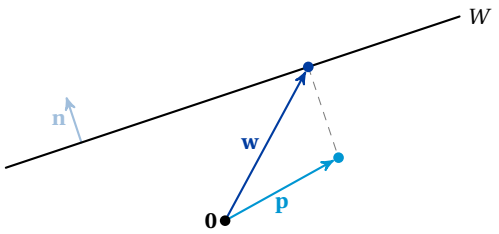
Ist nun $\mathbf{x} = k\mathbf{n}+\mathbf{u}$ mit $\mathbf{u} \in U$ ein beliebiger Punkt von W, so gilt

$$\begin{aligned}\|\mathbf{p}-\mathbf{x}\|^2 &= \|\big((\mathbf{n}\cdot\mathbf{p})\mathbf{n}+\mathbf{u}_0\big) - (k\mathbf{n}+\mathbf{u})\|^2 = \|(\mathbf{n}\cdot\mathbf{p}-k)\mathbf{n} + (\mathbf{u}_0-\mathbf{u})\|^2 \\ &= (\mathbf{n}\cdot\mathbf{p}-k)^2\mathbf{n}^2 + 2\mathbf{n}\cdot(\mathbf{u}_0-\mathbf{u}) + (\mathbf{u}_0-\mathbf{u})^2 = (\mathbf{n}\cdot\mathbf{p}-k)^2 + \|\mathbf{u}_0-\mathbf{u}\|^2\end{aligned}$$

und damit $\|\mathbf{p}-\mathbf{x}\| \geq |\mathbf{n}\cdot\mathbf{p}-k|$. Gleichzeitig sieht man jedoch auch, dass aus der Ungleichung eine Gleichung wird, wenn man den Punkt

$$\mathbf{w} = k\mathbf{n}+\mathbf{u}_0 = k\mathbf{n}+\mathbf{p}-(\mathbf{n}\cdot\mathbf{p})\mathbf{n} = \mathbf{p}+(k-\mathbf{n}\cdot\mathbf{p})\mathbf{n} \tag{36.3}$$

für $\mathbf{x}$ einsetzt. Da $\mathbf{p}-\mathbf{w}$ ein skalares Vielfaches von $\mathbf{n}$ ist, ist schließlich auch klar, dass dieser Vektor senkrecht auf U (also auf allen Vektoren aus U) steht. ■



Eine wesentliche Eigenschaft der hesseschen Normalenform ist also, dass sie eine besonders einfache Form der Abstandsberechnung ermöglicht.[33] Außerdem liefert sie eine weitere Information, die in der Computergrafik hilfreich sein kann. Diese ist für $\mathbb{R}^2$ und $\mathbb{R}^3$ anschaulich klar, für ihre saubere Formulierung nebst Beweis bräuchte man aber noch etwas mehr Mathematik, als wir in diesem Skript zur Verfügung haben:[34]

Eine Hyperebene W teilt den Raum $\mathbb{R}^n$ in zwei Hälften auf, die man als die zwei „Seiten“ von W bezeichnen könnte. Wird W in hessescher Normalenform durch die Gleichung $\mathbf{n}\cdot\mathbf{p}-k=0$ beschrieben und haben $\mathbf{n}\cdot\mathbf{p}_1-k$ und $\mathbf{n}\cdot\mathbf{p}_2-k$ dasselbe Vorzeichen, dann liegen $\mathbf{p}_1$ und $\mathbf{p}_2$ auf derselben Seite von W. Insbesondere liegt $\mathbf{p}$ auf derselben Seite von W wie $\mathbf{0}$, wenn $\mathbf{n}\cdot\mathbf{p}-k$ negativ ist und k nicht verschwindet.

Aufgabe 36.9. Geben Sie den Abstand des Punktes $P=(5,3)$ von der Geraden

$$g=(-3,2)+\mathbb{R}(2,-8)$$

auf zwei Stellen nach dem Komma an.

Aufgabe 36.10. Die Ebene

$$E=\{\mathbf{x}\in\mathbb{R}^3 : 1/\sqrt{21}\cdot(4,-2,1)\cdot\mathbf{x}-5=0\}$$

ist in hessescher Normalenform gegeben. Geben Sie den Abstand des Punktes $(5,0,3)$ von E auf zwei Stellen nach dem Komma an.

Aufgabe 36.11. Geben Sie einen Punkt an, der in der Ebene E aus Aufgabe 36.10 liegt.

Aufgabe 36.12. Geben Sie einen Punkt an, der in der Ebene E aus Aufgabe 36.10 und auf der Geraden $g=\mathbb{R}(1,0,0)$ liegt.

Aufgabe 36.13. Geben Sie einen Vektor aus $\mathbb{R}^3$ an, der senkrecht auf $(5,2,3)$ steht.

Die Aufgaben 36.6 und 36.13 zeigen, dass es sehr leicht ist, einen zu einem vorgegebenem Vektor orthogonalen zu finden. Aber wie findet man in $\mathbb{R}^3$ einen Vektor, der zu *zwei* vorgegebenen Vektoren orthogonal ist?

Achtung: Im Rest des Abschnitts geht es ausschließlich um den Vektorraum $\mathbb{R}^3$, weil die Methoden und Ergebnisse sich nicht ohne Weiteres auf Räume anderer Dimension übertragen lassen!

Definition

Im Vektorraum $\mathbb{R}^3$ ist das **Kreuzprodukt** bzw. **Vektorprodukt** der Vektoren $\mathbf{x}=(x_1,x_2,x_3)$ und $\mathbf{y}=(y_1,y_2,y_3)$ definiert als

$$\mathbf{x}\times\mathbf{y}=(x_2y_3-x_3y_2,x_3y_1-x_1y_3,x_1y_2-x_2y_1).$$

[33] Damit besagt diese Form, dass genau die Punkte zu W gehören, deren Abstand von W verschwindet – was ja auch logisch ist.

[34] Unter anderem eine Verallgemeinerung des Zwischenwertsatzes.

Das Vektorprodukt ist anders als das Skalarprodukt eine innere Verknüpfung. Es ist allerdings *nicht* kommutativ: z. B. gilt (rechnen Sie nach!)

$$(1,0,0) \times (0,1,0) = (0,0,1), \text{ aber } (0,1,0) \times (1,0,0) = (0,0,-1).$$

Aufgabe 36.14. Das Vektorprodukt kann man von Wolfram Alpha berechnen lassen, indem man so etwas wie

```
(1,2,3) x (4,5,6)
```

eingibt.

Aufgabe 36.15. Ist das Vektorprodukt assoziativ?

Durch einfaches Nachrechnen erhält man die folgenden Eigenschaften des Vektorproduktes.

Lemma 36.7

Für alle $\mathbf{x},\mathbf{y},\mathbf{z} \in \mathbb{R}^3$ und alle $\alpha \in \mathbb{R}$ gilt

(i) $(\alpha\mathbf{x}) \times \mathbf{y} = \mathbf{x} \times (\alpha\mathbf{y}) = \alpha(\mathbf{x} \times \mathbf{y})$

(ii) $(\mathbf{x}+\mathbf{y}) \times \mathbf{z} = (\mathbf{x} \times \mathbf{z}) + (\mathbf{y} \times \mathbf{z})$ und $\mathbf{z} \times (\mathbf{x}+\mathbf{y}) = (\mathbf{z} \times \mathbf{x}) + (\mathbf{z} \times \mathbf{y})$

(iii) $\mathbf{x} \times \alpha\mathbf{x} = \mathbf{0}$

(iv) $\mathbf{y} \times \mathbf{x} = -\mathbf{x} \times \mathbf{y}$ (*Antikommutativität*)

Die Eigenschaften (i) und (ii) nennt man wie beim Skalarprodukt *Bilinearität*. Anders als dort müssen sie hier jedoch „doppelt“ erwähnt werden, weil das Vektorprodukt nicht kommutativ ist. Wegen (iii) spricht man von einer *alternierenden* bilinearen Abbildung.

alternierend

Die Verknüpfung × wird bezüglich der Regel „Punkt- vor Strichrechnung“ wie ein Produkt behandelt. Typischerweise werden Klammern wie auf der rechten Seite von (ii) also weggelassen.

Aufgabe 36.16. Setzen Sie in Lemma 36.7 konkrete Werte ein und rechnen Sie nach, um sich zu überzeugen, dass die Aussagen korrekt sind.

Aufgabe 36.17. Zeigen Sie, dass (iv) in Lemma 36.7 aus den ersten drei Eigenschaften folgt, indem Sie $(\mathbf{a}+\mathbf{b}) \times (\mathbf{a}+\mathbf{b})$ berechnen.

⋆**Aufgabe 36.18**. Zeigen Sie, dass in Lemma 36.7 auch die Umkehrung von (iii) gilt, also: Aus $\mathbf{x} \times \mathbf{y} = \mathbf{0}$ folgt, dass $\{\mathbf{x},\mathbf{y}\}$ linear abhängig ist.

Lemma 36.8

Für alle $\mathbf{a},\mathbf{b} \in \mathbb{R}^3$ gilt $(\mathbf{a} \times \mathbf{b}) \cdot \mathbf{a} = 0 = (\mathbf{a} \times \mathbf{b}) \cdot \mathbf{b}$. Ist $\{\mathbf{a},\mathbf{b}\}$ linear unabhängig, so ist $\mathbf{a} \times \mathbf{b}$ also ein Vektor, der senkrecht auf $\mathbf{a}$ und $\mathbf{b}$ steht.

Beweis. Man muss lediglich einsetzen und erhält

$$\left(\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}\right) \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

$$= (a_2b_3 - a_3b_2)a_1 + (a_3b_1 - a_1b_3)a_2 + (a_1b_2 - a_2b_1)a_3$$
$$= a_1a_2b_3 - a_1a_2b_3 - a_1a_3b_2 + a_1a_3b_2 + a_2a_3b_1 - a_2a_3b_1 = 0.$$

Nach Lemma 36.7 und Aufgabe 36.18 ist außerdem klar, dass $\mathbf{a} \times \mathbf{b}$ genau dann *nicht* der Nullvektor ist, wenn $\mathbf{a}$ und $\mathbf{b}$ linear unabhängig sind. ■

Das Vektorprodukt hat noch weitere interessanter Eigenschaften, aber für unsere Zwecke ist Lemma 36.8 ausreichend.

Aufgabe 36.19. Geben Sie den Abstand des Punktes $(2, 0, -4)$ von der Ebene aus Aufgabe 33.5 auf zwei Stellen nach dem Komma an.

Aufgabe 36.20. Sei E die Ebene in $\mathbb{R}^3$, die die drei Punkte $(3, 2, 1)$, $(2, -7, 0)$ und $(5, -2, 5)$ enthält. Geben Sie den Punkt in E an, der den geringsten Abstand zum Punkt $(-4, 0, -1)$ hat.

Resümee

Die lineare Algebra ist eine vergleichsweise neue Entwicklung. In der heutigen Form wird sie erst seit einigen Jahrzehnten unterrichtet, gehört inzwischen aber zum unverzichtbaren Standardstoff der Hochschulmathematik. Das liegt unter anderem auch daran, dass lineare Abbildungen die Ableitungen in der mehrdimensionalen Analysis sind. Das Video *Was ist lineare Algebra?* liefert einen Überblick über die historische Entwicklung und den Stellenwert dieses Gebiets. Themen wie Determinanten oder lineare Gleichungssysteme, die hier aus Zeitgründen leider unter den Tisch fallen mussten, werden ausführlicher in meinem Buch *Konkrete Mathematik (nicht nur) für Informatiker* behandelt.

Die analytische Geometrie basiert auf Ideen von René Descartes[35] aus dem 17. Jahrhundert und hat insbesondere im Bereich der Anwendungen die bis dahin dominierende klassische Geometrie der antiken griechischen Mathematik fast vollständig abgelöst. Welche Auswirkungen die Einführung von Koordinaten auf die Geometrie hatte, wird beispielsweise im Video *Nicht-euklidische Geometrien* oder im Buch *Fünf unlösbare Rätsel der Mathematik* beschrieben.

[35] Zur gleichen Zeit entwickelten andere Mathematiker wie Pierre de Fermat ähnliche Ideen. Aber der einflussreichste dürfte wohl Descartes gewesen sein.

Lösungen zu ausgewählten Aufgaben

Lösung 1.2. Bei drei Aussagen braucht man acht Zeilen und bei vier sind es sechzehn. Allgemein braucht man 2^n Zeilen für n Aussagen.

Lösung 1.3. In der zweiten. Es hat *nicht* geregnet (bei A steht eine Null), aber die Straße ist trotzdem nass (und darum hat B den Wert eins).

Lösung 1.5. Nur die Implikation ist nicht assoziativ. Beispielsweise haben die Aussagen $A \Rightarrow (B \Rightarrow C)$ und $(A \Rightarrow B) \Rightarrow C$ nicht denselben Wahrheitswert, wenn A, B und C alle falsch sind.

Lösung 1.6. Setzt man A für „Der Hahn kräht auf dem Mist“ und B für „Das Wetter ändert sich“, dann handelt es sich um die Aussage $A \Rightarrow B \vee \neg B$. Weil – unabhängig davon, ob B wahr ist – $B \vee \neg B$ *immer* wahr ist, ist das Sprichwort wahr. (Das wussten Sie natürlich schon …)

Lösung 1.8. Die einfachste Antwort ist $\neg A \vee \neg B$ bzw. $\neg A \wedge \neg B$.

Lösung 1.9. Wir können die folgende Tabelle betrachten, die wegen der in der Aufgabenstellung angesprochenen Eigenschaft der reellen Zahlen nur drei (statt acht) Zeilen hat: In den ersten drei Spalten gibt es immer genau eine Eins.

$x < y$	$x = y$	$x > y$	$\neg(x < y)$	$x = y \vee x > y$
1	0	0	0	0
0	1	0	1	1
0	0	1	1	1

Man sieht, dass die beiden letzten Spalten identische Wahrheitswerte haben. $x \geq y$ ist bekanntlich nur eine Abkürzung für $(x = y) \vee (x > y)$.

Lösung 1.11. Zum Beispiel mit $\neg(A \Leftrightarrow B)$ oder $\neg(A \wedge B) \wedge \neg(\neg A \wedge \neg B)$. Es gibt immer viele Möglichkeiten, ein und dieselbe Aussage formal zu repräsentieren. (Sogar immer unendlich viele. Ist Ihnen klar, wieso das so ist?)

Lösung 1.12. Setzen wir A dafür, dass der HSV die Champions League gewinnt, und B dafür, dass ich in die Alster springe. Dann besagen die vier Sätze in dieser Reihenfolge $A \Rightarrow B$, $\neg A \Rightarrow \neg B$, $\neg B \Rightarrow \neg A$ und $A \Rightarrow \neg B$. Wir wissen bereits, dass die

erste und die dritte Aussage äquivalent sind. Mit einer Wahrheitstafel überzeugt man sich, dass die zweite und die vierte Aussage weder untereinander noch zu den anderen beiden äquivalent sind.

Lösung 1.13. Sei A die Aussage, dass auf der Buchstabenseite ein Vokal steht, und B die Aussage, dass auf der Zahlenseite eine gerade Zahl steht. Die zweite Regel ist also einfach $A \Rightarrow B$. Diese Regel wird nur dann verletzt, wenn A wahr ist und B falsch. Darum müssen Sie sich die Karte mit dem Buchstaben U (A ist wahr) und die Karte mit der Zahl 7 (B ist falsch) genauer anschauen. Die anderen beiden Karten müssen Sie nicht umdrehen, denn die Implikation ist unabhängig davon, was auf deren Rückseite gedruckt wurde, immer wahr.

Lösung 1.14. Bezeichnet man die Aussage „Gauß ist schuldig“ zur Abkürzung mit G und die entsprechenden Aussage für Euler und Hilbert mit E und H, so lassen sich die Ergebnisse der bisherigen Ermittlungen wie folgt zusammenfassen: $(H \Rightarrow E) \wedge (G \vee H \Rightarrow \neg E) \wedge (\neg E \vee \neg H \Rightarrow G)$. Mit einer Wahrheitstafel kann man nun nachprüfen, dass diese Formel nur dann wahr wird, wenn G wahr ist und H und E falsch sind. Daher muss Gauß der (einzige) Täter sein.

Lösung 1.15. Belegt man A und B beide mit 0 oder beide mit 1, dann ist die Formel wahr. Also ist sie erfüllbar. Haben A und B jedoch unterschiedliche Wahrheitswerte, dann ist die Formel nicht wahr, also ist es keine Tautologie.

Lösung 1.16. Ja, es handelt sich um eine Tautologie (und damit natürlich „erst recht“ um eine erfüllbare Formel). Ihre Wahrheitstafel hatte hoffentlich acht Zeilen – siehe Aufgabe 1.2.

Lösung 1.17. Mit einer Wahrheitstafel kann man nachprüfen, dass (i) und (iii) zum Erfolg führen, (ii) aber nicht.

Lösung 1.19. Da diese Frage im Abschnitt über Aussagenlogik vorkommt, lösen wir sie natürlich mit Mitteln der Aussagenlogik. Seien A und B die Aussagen, dass Andrew bzw. Bert blau sind. Andrew wird auf die erste Frage mit *ja* antworten, wenn beide blau sind oder wenn er selbst grün ist, wenn also $(A \wedge B) \vee \neg A$ gilt. (Diese Aussage kann man zu $\neg A \vee B$ vereinfachen, obwohl das nicht unbedingt nötig ist.) Die zweite Frage wird er mit *ja* beantworten, wenn beide blau sind oder wenn er grün und Bert blau ist. Das ist also dann der Fall, wenn $(A \wedge B) \vee (\neg A \wedge B)$ gilt. (Man sieht hoffentlich leicht, dass das äquivalent zu B ist, aber auch diese Vereinfachung ist für das Lösen der Aufgabe nicht zwingend notwendig.) Es ergibt sich die folgende Wahrheitstafel:

A	B	$(A \wedge B) \vee \neg A$	$(A \wedge B) \vee (\neg A \wedge B)$
0	0	1	0
0	1	1	1
1	0	0	0
1	1	1	1

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

In der dritten bzw. vierten Spalte steht jeweils genau dann eine Eins, wenn Andrew auf die erste bzw. zweite Frage mit *ja* geantwortet hat. Da die Astronautin nach der ersten Frage noch nicht die Farben weiß, kann Andrews Antwort nicht *nein* gewesen sein, denn daraus hätte sie sofort schließen können, dass Andrew blau und Bert grün ist. Also können wir diesen Fall vergessen. (Darum ist die dritte Zeile ausgegraut.) Da die Astronautin nach der zweiten Antwort die Farben weiß, muss die zweite Antwort *nein* gewesen sein, denn die Antwort *ja* hätte ihr die Farbe von Andrew nicht verraten. Also sind beide grün.

Lösung 1.20. Das war hoffentlich nur eine kleine Fingerübung für Sie. Gemeint war $(x < y) \vee (x = y)$. Siehe auch Aufgabe 1.9.

Wir werden in solchen Ausdrücken in Zukunft häufiger auch die Klammern weglassen und implizit davon ausgehen, dass mathematische Relationszeichen eine höhere Priorität als logische Symbole haben. Das erklärt sich eigentlich von selbst, weil beispielsweise „$x < (y \vee x) = y$“ keinen Sinn ergeben würde, wenn die Individuenvariablen x und y für Zahlen stehen.

Lösung 1.21. Es gibt mehr als eine Möglichkeit, das zu machen. Hier sind zwei Vorschläge:

$$(A_4(n) \wedge \neg A_{100}(n)) \vee A_{400}(n)$$
$$A_4(n) \wedge (A_{400}(n) \vee \neg A_{100}(n))$$

Lösung 1.22. Falls Sie Schwierigkeiten mit dieser Aufgabe haben, hilft vielleicht ein übersichtliches Beispiel, bei dem es statt um unendlich viele Objekte nur um drei geht. Nehmen wir an, Sie haben drei Billardkugeln k_1, k_2 und k_3 und die Aussage $W(x)$ bedeutet, dass die Kugel x weiß ist. Dann gibt es acht mögliche Fälle:

$W(k_1)$	$W(k_2)$	$W(k_3)$
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Der Allquantor steht jetzt natürlich für „alle drei Kugeln“ und der Existenzquantor für „mindestens eine der drei Kugeln“. Die Aussage $\exists x\, W(x)$ ist also offensichtlich in allen Fällen außer dem ersten wahr, weil in allen zugehörigen Zeilen mindestens eine Eins steht. Daher ist die Negation dieser Aussage – also $\neg\exists x\, W(x)$ – *nur* dann wahr, wenn der erste Fall eintritt. Der erste Fall bedeutet jedoch gleichzeitig auch, dass $\neg W(k_1)$, $\neg W(k_2)$ und $\neg W(k_3)$ alle wahr sind, und das heißt $\forall x \neg W(x)$. Das stimmt offensichtlich in keiner der anderen sieben Zeilen.

Lösung 1.23. Diese Aufgabe ist eine Vertiefung von Aufgabe 1.22. Wenn $F(b)$ für „b kann Fußball spielen“ steht und man für b Bremer einsetzen darf, dann ist die

Behauptung, deren Gegenteil Sie formulieren wollen, $\forall b\, F(b)$. Die Aussagen, die zur Wahl stehen, kann man so als Formeln hinschreiben:

(i) $\exists b \neg F(b)$
(ii) $\exists b \neg F(b)$
(iii) $\forall b \neg F(b)$ oder $\neg \exists b\, F(b)$
(iv) $\neg \forall b\, F(b)$

(Beachten Sie, dass sich die ersten beiden Aussagen rein logisch gar nicht unterscheiden.) Nur der dritte Satz ist *nicht* das Gegenteil der Behauptung. Wenn Sie widerlegen wollen, dass *alle* Bremer Fußball spielen können, dann reicht es, *einen* zu finden, der es nicht kann.

(Wenn Sie noch nicht überzeugt sind, dann stellen Sie sich der Einfachheit halber vor, dass Bremen nur drei Einwohner hat, und erstellen Sie eine Tabelle wie in der Lösung zu Aufgabe 1.22.)

Lösung 1.24. Ja, $\exists$ wäre so etwas wie ein „großes $\vee$“.

Lösung 1.25. $\forall x\, W(x)$ wäre die Formel $W(k_1) \wedge W(k_2) \wedge W(k_3)$ und $\exists x\, W(x)$ wäre $W(k_1) \vee W(k_2) \vee W(k_3)$. Wenn es nur endlich viele mögliche Werte gibt, die man für die Individuenvariablen einsetzen kann, ist es also legitim, Aussagen mit Quantoren durch Konjunktionen oder Disjunktionen zu ersetzen. Aber abgesehen von solchen überschaubaren Fällen wäre es trotzdem sehr unpraktisch. Bei Aufgabe 1.23 bräuchte man z. B. mehr als eine halbe Million Junktoren, weil es so viele Bremer gibt …

Lösung 1.26. Aussage (i) ist falsch. Sie besagt, dass es eine natürliche Zahl gibt, die nicht gerade, aber durch 4 teilbar ist. Das geht natürlich nicht. Aussage (ii) ist wahr. Sie besagt, dass es eine natürliche Zahl gibt, die gerade, aber nicht durch 4 teilbar ist. Dafür gibt es unendlich viele Beispiele, etwa 2, 6, oder 10. Aussage (iii) ist wahr. Sie besagt, dass alle natürlichen Zahlen durch 4 teilbar sind, *wenn* alle natürlichen Zahlen gerade sind. Da die erste Aussage schon falsch ist (weil eben *nicht* alle natürlichen Zahlen gerade sind), kann auch die zweite ruhig falsch sein. (Erinnern Sie sich an die Erdkundeklausur und das Eis!)

Aussage (iv) ist falsch. Sie besagt, dass jede gerade natürliche Zahl durch 4 teilbar ist. Gegenbeispiele sind die unter (ii) genannten Zahlen. Aussage (v) ist wahr. Sie besagt, dass jede natürliche Zahl, die durch 4 teilbar ist, auch gerade ist. Aussage (vi) ist falsch. Sie besagt, dass jede natürliche Zahl genau dann gerade ist, wenn sie durch 4 teilbar ist. Wenn das wahr wäre, dann wären sowohl (iv) als auch (v) wahr. Und Aussage (vii) ist auch falsch. Sie besagt, dass jede natürliche Zahl, die nicht durch 4 teilbar ist, auch nicht gerade ist. Man kann hier wieder die Gegenbeispiele aus (ii) verwenden.

Beachten Sie, dass (iii) und (iv) ganz unterschiedliche Aussagen sind, obwohl sie sehr ähnlich aussehen! Für (iii) hätte man auch $\forall n \in \mathbb{N}\, p(n) \Rightarrow \forall m \in \mathbb{N}\, q(m)$ schreiben können. Siehe dazu die Bemerkung zum Einflussbereich der Quantoren auf Seite 19.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 1.27. Wenn t für Töpfe und d für Deckel steht sowie $P(d,t)$ für „d passt auf t“, dann besagt das Sprichwort $\forall t \exists d\, P(d,t)$. $\exists d \forall t\, P(d,t)$ würde hingegen bedeuten, dass es einen „Superdeckel“ gibt, der auf jeden Topf passt.

Lösung 1.28. Die erste Aussage besagt, dass man zu jeder natürlichen Zahl m eine größere finden kann. Das stimmt natürlich, man kann z. B. $n = m+1$ nehmen. Die zweite Aussage ist aber falsch, denn dort wird behauptet, dass es eine Zahl n gibt, die größer als *jede* natürliche Zahl ist. Die dritte und die vierte Aussage sind beide wahr. In beiden Fällen kann man $n = 0$ wählen.

Lösung 1.29. Die erste Aussage besagt, dass jedes der Passwörter mindestens einem Agenten bekannt ist. Die zweite Aussage besagt, dass es mindestens einen Agenten gibt, der alle Passwörter kennt. Um die erste Aussage wahr zu machen, muss man lediglich ein Kreuz in der zweiten Spalte hinzufügen. Damit die zweite Aussage nicht auch wahr wird, darf man dieses Kreuz nicht gerade in der zweiten Zeile machen – denn sonst wäre a_2 der Agent, der alle Passwörter kennt.

Lösung 1.30. Es gibt unzählige Möglichkeiten. Man könnte $x < 42$ und $x > 42$ für $A(x)$ und $B(x)$ nehmen. Es gibt natürliche Zahlen, die kleiner als 42 sind, und es gibt natürliche Zahlen, die größer als 42 sind. Aber es gibt keine Zahl, die gleichzeitig kleiner *und* größer als 42 ist.

Für die erste Aussage hätte man auch $\exists x \in \mathbb{N}\, A(x) \wedge \exists y \in \mathbb{N}\, B(y)$ schreiben können. Siehe dazu die Bemerkung zum Einflussbereich der Quantoren auf Seite 19.

Lösung 1.31. Die Behauptung kann man in der Form $\forall y \in \mathbb{N} \exists x \in \mathbb{Z}\, x^2 = y$ formal hinschreiben. Die Negation davon ist $\exists y \in \mathbb{N} \forall x \in \mathbb{Z}\, x^2 \neq y$. Sie müssen also nur *ein* solches y finden. Sie haben sogar zwei angegeben, nämlich 2 und 3. (Bei dieser Aufgabe ging es noch einmal darum, dass man eine Aussage, die etwas für viele Objekte behauptet, durch ein einziges Gegenbeispiel widerlegen kann.)

Lösung 1.33. A und B waren „n^2 ist ungerade“ und „n ist ungerade“. $\neg B$ ist damit „n ist gerade“ und $\neg A$ ist „n^2 ist gerade“.

Lösung 2.1. Das dürfte wohl kein Problem gewesen sein:

$$A = \{1,2,3,4,5,6,7,8,9\}$$
$$B = \{-4,-3,-2,-1,0,1,2,3,4\}$$

Ihnen war klar, dass die Null keine *positive* Zahl ist, oder?

Lösung 2.2. Das geht zum Beispiel so:

$$Y = \{\, n : n \text{ ist eine ganze Zahl und } 1 \leq n \leq 100 \}$$
$$Z = \{\, m : m \text{ ist eine ungerade ganze Zahl und } m > 1 \}$$

Wenn Sie eine andere Beschreibung gewählt haben, ist das natürlich auch OK. Sie muss allerdings genau genug sein, damit nicht aus Versehen Objekte in die Menge „hineinschlüpfen“ können, die dort nichts zu suchen haben. Hätten Sie etwa nur

$$Y = \{\, n : n \text{ ist eine Zahl und } 1 \leq n \leq 100 \}$$

geschrieben, dann wäre das nicht ausreichend, weil der Begriff „Zahl“ zu vage ist. Wäre $3/2$ in diesem Fall nicht auch ein Element von Y?

Lösung 2.3. Klar: $X = \{x : x = 1 \vee x = \pi \vee x = 42\}$.

Lösung 2.4. In der folgenden Tabelle sind alle Elementbeziehungen markiert.

	$-1/3$	$\sqrt{9}$	1	$\sqrt{8}$	42	$14/2$	π	-12	$3/8$	0	$0.0\overline{1}$
$\mathbb{P}$		$\in$				$\in$					
$\mathbb{N}$		$\in$	$\in$		$\in$	$\in$				$\in$	
$\mathbb{Z}$		$\in$	$\in$		$\in$	$\in$		$\in$		$\in$	
$\mathbb{Q}$	$\in$	$\in$	$\in$		$\in$	$\in$		$\in$	$\in$	$\in$	$\in$
$\mathbb{R}$	$\in$	$\in$	$\in$	$\in$	$\in$	$\in$	$\in$	$\in$	$\in$	$\in$	$\in$

Beachten Sie, dass $\sqrt{9}$ und $14/2$ die natürlichen Zahlen 3 und 7 sind. Ferner ist $0.0\overline{1}$ der Bruch $1/90$. (Das sollte Schulwissen sein, wird jedoch später in Abschnitt 21 noch einmal genauer erklärt.) Allerdings ist $\sqrt{8}$ kein Bruch und π auch nicht. Ersteres erfährt man in der Regel auch schon in der Schule – siehe dazu das Video *Der Satz des Theaitetos* –, während der Beweis der zweiten Aussage etwas mehr Mathematik erfordert. In dem Video *Die Kreiszahl Pi ist irrational* wird das vorgeführt.

Wenn Sie mit dieser Aufgabe Schwierigkeiten hatten, dann schauen Sie sich vielleicht einmal in die Liste der Bücher zum Schulstoff.

Ihnen ist hoffentlich aufgefallen, dass ein $\in$ an einer Position der Tabelle immer impliziert, dass in den Zeilen darunter auch ein $\in$ stehen muss. Das hängt mit den Teilmengenbeziehungen zusammen, die im Skript nach dieser Aufgabe besprochen werden.

Lösung 2.5. In dieser Reihenfolge könnte man als Gegenbeispiele die Zahlen 1, -1, $1/2$ und $\sqrt{2}$ nehmen. Natürlich macht es nichts, wenn Sie andere Gegenbeispiele hatten, solange Ihnen prinzipiell klar ist, worum es geht.

Lösung 2.6. Man könnte z. B. $X = \{1\}$ und $Y = \{2\}$ nehmen. Bei Zahlen ist das nicht so: Wenn x und y zwei reelle Zahlen sind, dann ist immer mindestens eine der beiden Aussagen $x \leq y$ und $y \leq x$ wahr. Siehe auch Aufgabe 1.9.

Lösung 2.7. Würde $\emptyset \subseteq A$ *nicht* wahr sein, dann müsste es ein Element von $\emptyset$ geben, das kein Element von A ist. Das kann aber nicht sein, weil $\emptyset$ gar keine Elemente hat.

Lösung 2.8. Man kann einfach das Beispiel vor dieser Aufgabe fortsetzen und erhält $\{10, 23, 42\} \setminus \{1, 10, 17, 23\} = \{42\}$. Da das nicht dasselbe wie $\{1, 17\}$ ist, kann man bei der Differenz die beiden beteiligten Mengen nicht einfach vertauschen.

Lösung 2.10. Ich würde es so machen:

$$\mathbb{N}^+ = \{n : n \in \mathbb{N} \wedge n > 0\} = \mathbb{N} \setminus \{0\}$$

Lösung 2.11. $A \cap B = A \setminus (A \setminus B)$. Wenn Ihnen nicht klar ist, warum das stimmt, dann zeichnen Sie sich ein Mengendiagramm.

Lösung 2.12. Sie sind identisch. Die Quadrate (bis auf das der Null) werden in der zweiten Menge „doppelt aufgerufen“, aber das ändert ja bekanntlich nichts.

Lösung 2.13. $\mathbb{Q} = \{m/n : m \in \mathbb{Z} \wedge n \in \mathbb{N}^+\}$ wäre eine Möglichkeit. Beachten Sie, dass im Nenner nicht null stehen darf! Dass Brüche mehrfach vorkommen (z. B. 1/2 und 2/4), ist kein Problem. Tatsächlich kommt jeder Bruch unendlich oft vor.

Lösung 2.14. Man kann ahnen, was gemeint ist, aber links vom Doppelpunkt darf zur Vermeidung von Missverständnissen nur *ein* Prototyp stehen, während es sich hier offenbar um zwei (verschiedene) handelt, nämlich um n und $-n$.

Wenn wir demnächst Tupel eingeführt haben, werden Sie sehen, dass man diese falsche Schreibweise auch ganz anders interpretieren könnte. Siehe dazu später auch Aufgabe 5.26.

Lösung 2.15. Analog zu den beiden für Aufgabe 1.21 gezeigten Lösungen könnte man $(A_4 \setminus A_{100}) \cup A_{400}$ oder $A_4 \cap (A_{400} \cup (G \setminus A_{100}))$ nehmen. Natürlich gibt es auch noch weitere legitime Lösungen.

Vergegenwärtigen Sie sich anhand dieser beiden Aufgaben noch einmal den engen Zusammenhang zwischen Mengenverknüpfungen und aussagenlogischen Junktoren!

Lösung 2.16. Sie sind hoffentlich auf diese Ergebnisse gekommen:

$$A = \{0\} \qquad B = \mathbb{N} \qquad C = \mathbb{Q} \qquad D = \mathbb{Q}$$
$$E = \mathbb{Q} \qquad F = \emptyset \qquad G = \mathbb{N} \qquad H = \mathbb{Z}$$

Lösung 2.17. Die Paare sind $A = C = \mathbb{R}$, $B = E = \mathbb{N}$, $D = I = \{0\}$, $F = J = \emptyset$ und $G = H$. Unter anderem muss man dafür wissen, dass $\sqrt{8} = 2\sqrt{2}$ keine rationale Zahl ist (siehe Aufgabe 2.4) und dass 0 und 1 die einzigen Zahlen sind, die ihr eigenes Quadrat sind: $0 \cdot 0 = 0$ und $1 \cdot 1 = 1$.

Lösung 2.18. Die Paare sind $A = G$, $B = F = \mathbb{N}$, $C = D = \mathbb{N}^+$ und $E = H = \emptyset$. A ist die Menge der nichtnegativen rationalen Zahlen.

Lösung 2.19. Wir nennen die drei Mengen, die beschrieben werden sollen, in der Reihenfolge der Aufgabenstellung A, B und C. Es wäre im Prinzip auch OK gewesen, so etwas wie

$$A = \{x : x \text{ ist eine ganze Zahl, deren Quadrat kleiner als } 100 \text{ ist}\}$$

zu schreiben, aber Sie haben sich hoffentlich gedacht, dass die Aufgabe etwas anders gemeint war. Es gibt unendlich viele Möglichkeiten, die Aufgabe zu lösen, und ich mache hier nur ein paar Vorschläge:

$$A = \{z \in \mathbb{Z} : z^2 < 100\} = \{z \in \mathbb{Z} : |z| < 10\}$$
$$B = \{n \in \mathbb{N} : n \leq 300 \wedge 3 \text{ teilt } n\} = \{3n : n \in \mathbb{N} \wedge n \leq 100\}$$
$$C = \left\{\tfrac{2}{n} : n \in \mathbb{N}^+ \wedge \mathrm{ggT}(2, n) = 1\right\} = \left\{\tfrac{2}{2k+1} : k \in \mathbb{N}\right\}$$

Dabei bedeutet $\mathrm{ggT}(2, n) = 1$, dass 1 der größte gemeinsame Teiler von 2 und n ist, dass 2 und n also teilerfremd sind.

Lösung 2.20. Es ergibt sich

$$A = \{n \in \mathbb{N} : n^2 < 400 \wedge 12 \text{ teilt } n^2\} \qquad \text{und}$$
$$B = \{n \in \mathbb{N} : n^2 < 400 \wedge 12 \text{ teilt } n\}.$$

$C = \{0, 1, 2, \ldots, 19\}$ ist die Menge der natürlichen Zahlen, deren Quadrat kleiner als 400 ist. Nur zwei der Elemente von C sind durch 12 teilbar, nämlich 0 und 12. Die Menge der zugehörigen Quadrate ist $\{n^2 : n \in C\} = \{0, 1, 4, 9, \ldots, 361\}$ und in dieser Menge sind 0, 36, 144 und 324 durch 12 teilbar. Daher haben wir

$$A = \{0, 6, 12, 18\} \qquad \text{und} \qquad B = \{0, 12\}.$$

Die beiden Mengen sind nicht gleich.

Diese Aufgabe soll deutlich machen, dass es im Allgemeinen nicht von Vorteil wäre, die von Studierenden oftmals gehassten Formeln durch „normale“ Sprache zu ersetzen. Ich hoffe, Sie stimmen mir zu, dass die beschreibende Mengenschreibweise in diesem Fall wesentlich klarer ist als die Erklärung in der Aufgabenstellung. (Nebenbei gilt das insbesondere auch dann, wenn ein Sachverhalt in einer Sprache formuliert ist, die nicht Ihre Muttersprache ist. Die Formelsprache ist international.)

Lösung 3.1. Das einfachste Beispiel wären $A = \emptyset$ und $B = \{\emptyset\}$. Man könnte aber auch in Anlehnung an (3.1) $A = \{1, 2\}$ und $B = \{1, 2, A\}$ nehmen.

Lösung 3.3. Zunächst gilt $A \setminus \emptyset = A$ und $B \setminus \emptyset = B$. Das sollten Sie sich bereits in Aufgabe 2.9 klargemacht haben. $A \setminus \{\emptyset\}$ entsteht, indem man aus A das Element $\emptyset$ entfernt. Das Ergebnis ist $\{\{\emptyset\}\}$. Beachten Sie die doppelten Klammern! Die resultierende Menge hat ein Element und dieses Element ist selbst wiederum eine Menge. Bei $B \setminus \{\emptyset\}$ soll ebenfalls das Element $\emptyset$ entfernt werden. Da $\emptyset$ aber gar kein Element von B ist, ändert sich nichts: $B \setminus \{\emptyset\} = B$. Ebenso würde $B \setminus \{42\} = B$ gelten.

Diese Aufgabe wurde hauptsächlich deshalb aufgenommen, weil erfahrungsgemäß viele Studierende glauben, dass $\emptyset \in X$ für *jede* Menge X gilt. Das ist falsch! Es gilt $\emptyset \subseteq X$ für jede Menge X (siehe Aufgabe 2.9), aber das ist eine ganz andere Aussage. Wäre die leere Menge ein Element jeder Menge, dann wäre sie auch ein Element von $A \setminus \{\emptyset\}$, obwohl sie gerade entfernt wurde. Ist es nicht logisch, dass das nicht sein kann?

Lösung 3.4. Aussage (vi) ist wahr, siehe dazu Aufgabe 2.9. Alle anderen Aussagen sind falsch. Bei (ii) enthält die Menge links das Element $\{1\}$, die rechte aber nicht. Bei (i), (iii), (iv) und (v) enthält die linke Menge jeweils das Element 1 und die rechte nicht. Bei (vii) enthält die rechte Menge das Element $\emptyset$ und die linke nicht. Bei (viii) enthält umgekehrt die linke Menge das Element $\emptyset$ und die rechte nicht. Und bei (ix) enthält die linke Menge z. B. das Element $\{0, 1\}$ und die rechte nicht.

Lösung 3.5. Dass A die Menge $\{1, 2, 3\}$ ist, ist Ihnen hoffentlich klar. Um diese Aufgabe richtig zu verstehen, muss man sich außerdem daran erinnern, dass $m, n \in A$ eine Abkürzung für $m \in A \wedge n \in A$ ist. Die Variablen m und n durchlaufen unabhängig voneinander die Menge A. Weil A drei Elemente hat, sind damit theoretisch

$3 \cdot 3 = 9$ Produkte möglich. Allerdings ist die Multiplikation kommutativ und in Mengen gibt es keine Dopplungen. Bei $m = 3$ und $n = 2$ kommt beispielsweise dasselbe heraus wie bei $m = 2$ und $n = 3$. Daher ergibt sich $B = \{1, 2, 3, 4, 6, 9\}$. Die Antwort ist somit $|B| = 6$.

Ersetzt man 4 durch größere Zahlen, so kommt erschwerend hinzu, dass sich manche Produkte mit unterschiedlichen Faktoren bilden lassen: Bei $2 \cdot 6$ kommt etwa dasselbe heraus wie bei $3 \cdot 4$. Siehe dazu auch die „Computerlösung“ auf Seite 41.

Lösung 3.6. Sind sie auf diese Fangfrage hereingefallen? Die Menge $\{B\}$ ist ein Singleton. Dabei ist völlig unerheblich, wie B aussieht und ob es sich überhaupt um eine Menge handelt. Die Antwort ist schlicht und einfach $2^1 = 2$. Auch $\mathscr{P}(\{\mathbb{N}\})$ hat nur zwei Elemente, nämlich $\emptyset$ und $\mathbb{N}$.

Die Aufgabe zeigt, dass man in der Mathematik immer sehr genau hinschauen muss, weil in der Regel jedes Symbol von Bedeutung ist. Wäre es um $\mathscr{P}(B)$ gegangen, dann wäre die Antwort $2^{18} = 262\,144$ gewesen, aber $\mathscr{P}(B)$ und $\mathscr{P}(\{B\})$ sind eben zwei ganz unterschiedliche Objekte.

Lösung 3.7. Es stimmt *nie*! Seit Aufgabe 2.7 wissen wir, dass die leere Menge Element jeder Potenzmenge ist. Darum enthält der Durchschnitt zweier Potenzmengen immer die leere Menge und ist deshalb nicht leer. (Wenn Sie diese Antwort verwirrt, dann sollten Sie vielleicht den Abschnitt über Mengen noch einmal studieren.)

Lösung 3.8. Für die erste Aussageform haben wir in Aufgabe 3.4 schon ein Gegenbeispiel gesehen: $A = \mathbb{N}$ und $B = \{0\}$. Für die zweite Aussageform kann man z. B. $A = \{0\}$ und $B = \{1\}$ nehmen. $\mathscr{P}(A \cup B)$ enthält dann $A \cup B$, $\mathscr{P}(A) \cup \mathscr{P}(B)$ aber nicht.

Man beachte übrigens, dass $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$ immer gilt! Machen Sie sich das vielleicht anhand von Beispielen klar.

Lösung 3.9. In gewissem Sinne ist dies auch eine Fangfrage, bei der es um genaues Lesen geht. In der Aufgabe steht nicht, dass es um drei *verschiedene* Zahlen geht! Hat $\{a, b, c\}$ wirklich die Mächtigkeit 3, dann hat X die Mächtigkeit 2. Sind aber alle drei Zahlen identisch, dann hat X die Mächtigkeit 0. Ist auch die Antwort 1 möglich? Ja, wenn z. B. $a = b$ und $a \neq c$ gilt.

Lösung 3.10. Bei dieser Aufgabe geht es natürlich unter anderem auch wieder darum, die Mengenschreibweise zu verstehen. Wir haben:

$A = \emptyset$	$\lvert A\rvert = 0$
$B = \{0, 1, 2, 3, 4, 5, 6\}$	$\lvert B\rvert = 7$
$C = \{7\}$	$\lvert C\rvert = 1$
$D = \{0, 1, 2, 3, 4, 5\}$	$\lvert D\rvert = 6$
$E = \{1, 2, 3, 6, 7, 14, 21, 42\}$	$\lvert E\rvert = 8$
$F = \{0, 1, 2, \ldots, 20\}$	$\lvert F\rvert = 21$

Nach Mächtigkeit sortiert ergibt das A, C, D, B, E, F.

Lösung 3.11. Wenn Sie diese Aufgabe nicht lösen konnten, dann ist das nicht schlimm. Sie sollten es aber zumindest ernsthaft versucht haben. Das gilt ohnehin für alle Aufgaben! Und Ihnen ist dabei hoffentlich klar geworden, wonach überhaupt gefragt wurde.

Teilmengen von A, die mindestens eine Primzahl enthalten, sind zum Beispiel $\{3\}$, $\{2,5,10\}$ oder A selbst. Die Menge *aller* Teilmengen von A ist $\mathscr{P}(A)$. Da A 20 Elemente hat, hat $\mathscr{P}(A)$ nach Satz 3.1 2^{20} Teilmengen, also mehr als eine Million. Die kann man schwerlich alle einzeln durchgehen und auf Primzahlen überprüfen. Was nun? Bis hier sollten Sie ohne Hilfe gekommen sein. Hoffentlich haben Sie einen Zettel vor sich, auf den Sie exemplarisch ein paar der gesuchten Teilmengen gekritzelt haben.

Häufig ist es einfacher, nach dem *Gegenteil* zu fragen, und das ist auch hier so. Eine Teilmenge von A, die *nicht* mindestens eine Primzahl enthält, enthält *keine* Primzahl. Sie ist damit eine Teilmenge von

$$B = \{n \in A : n \notin \mathbb{P}\} = \{0,1,4,6,8,9,10,12,14,15,16,18\}.$$

Wir können die Aufgabe damit so umformulieren, dass wir die Mächtigkeit von $\mathscr{P}(A) \setminus \mathscr{P}(B)$ wissen wollen. Daher ist die Antwort

$$|\mathscr{P}(A)| - |\mathscr{P}(B)| = 2^{|A|} - 2^{|B|} = 2^{20} - 2^{12}.$$

Das sind immer noch mehr als eine Million Mengen und ich habe die Zahl absichtlich nicht hingeschrieben. Um die geht es nämlich nicht. Bei den meisten Aufgaben reicht es, wenn Sie sie so weit lösen können, dass Sie für den letzten Schritt mit dem einfachen Taschenrechner des Departments auskommen würden. Dass Sie $2^{20} - 2^{12}$ eintippen und das Ergebnis abschreiben könnten, glaube ich auch so.

Lösung 3.12. Das kann man wie in Aufgabe 3.11 machen, wie Ihnen hoffentlich aufgefallen ist. $A = \{3,4,5,\ldots,29,30\}$ hat 28 Elemente. Die Menge der Elemente von A, die durch 3 teilbar sind, ist

$$\{3,6,9,12,15,18,21,24,27,30\}$$

und hat die Mächtigkeit 10. Die Menge der Elemente von A, die *nicht* durch 3 teilbar sind, hat daher die Mächtigkeit 18. Die Antwort ist demnach $2^{28} - 2^{18}$.

Lösung 3.13. Beachten Sie, dass diese Aufgabe mit einem Stern gekennzeichnet ist. Es entsteht Ihnen jedoch kein bleibender Schaden, wenn Sie sich damit beschäftigen.

Wir müssen für vier beliebige Objekte a bis d zeigen, dass $(a,b) = (c,d)$ genau dann wahr ist, wenn $a = c$ und $b = d$ gelten. Es handelt sich dabei um eine Äquivalenz, die wir – siehe Aufgabe 1.7 – in zwei Implikationen zerlegen.

Dabei ist der eine Teil ganz einfach (oder auch „trivial“, wie man in der Mathematik gerne sagt). Aus $a = c \wedge b = d$ folgt natürlich, dass $\{\{a\},\{a,b\}\}$ und $\{\{c\},\{c,d\}\}$ dieselbe Menge sind, denn wir dürfen in der zweiten Menge c durch a und d durch b ersetzen.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Die andere Richtung ist etwas aufwendiger. Ich führe den Beweis ausführlich vor, um zu demonstrieren, was man alles beachten muss. Wir gehen davon aus, dass die beiden Mengen $X = \{\{a\},\{a,b\}\}$ und $Y = \{\{c\},\{c,d\}\}$ identisch sind, und wollen zeigen, dass daraus $a = c$ und $b = d$ folgen.

Obwohl es so aussieht, als hätte X zwei Elemente, muss das nicht so sein. Es könnte sein, dass $\{a\} = \{a,b\}$ gilt! Diesen Fall behandeln wir zuerst. Er kann offenbar nur eintreten, wenn $a = b$ gilt. Außerdem hat dann wegen $X = Y$ auch Y nur ein Element und wir können analog $c = d$ schließen. Damit haben wir die Situation $X = \{\{a\}\}$ und $Y = \{\{c\}\}$. Daraus folgt offensichtlich $a = c$ und wegen der vorherigen Überlegungen auch der Rest.

Nun der zweite Fall, nämlich $\{a\} \neq \{a,b\}$. Das impliziert $a \neq b$. Die beiden Elemente von X unterscheiden sich also durch ihre Mächtigkeit. Wegen $X = Y$ muss Y ebenfalls zwei Elemente haben und die müssen dieselben Mächtigkeiten wie die von X haben. Daraus folgt $\{a\} = \{c\}$ und $\{a,b\} = \{c,d\}$. Die erste Gleichung liefert $a = c$. Setzt man in der zweiten nun a für c ein, dann ergibt sich $\{a,b\} = \{a,d\}$ und damit $b = d$.

Falls Sie das für Korinthenkackerei halten: In der mathematischen Praxis schaut man in der Regel nicht unter der Motorhaube nach, wie geordnete Paare intern aufgebaut sind. Solche Fragen sind nur für die Grundlagenmathematik relevant, wenn man sich überzeugen will, dass man so etwas tatsächlich ausschließlich mit Mengen realisieren kann.

Lösung 3.14. Die Dopplungen verschwinden. Beispielsweise ist $2 \cdot 3$ dasselbe wie $3 \cdot 2$. Aber $(2,3)$ ist eben *nicht* dasselbe wie $(3,2)$. Das ist ja gerade der Grund, warum Paare definiert wurden.

Lösung 3.15. $\{0\} \times M$ ist $\{(0,23),(0,42),(0,\pi)\}$. $\emptyset \times M$ ist die leere Menge, denn in dieser Menge befinden sich nach Definition Paare, deren erste Komponente ein Element der leeren Menge ist. Da die leere Menge keine Elemente hat, kann es solche Paare nicht geben.

Etwas anderes hätte auch gar nicht herauskommen dürfen, denn nach Lemma 3.2 hat $\emptyset \times M$ die Mächtigkeit null.

Lösung 3.16. Mit der Frage ist gemeint, ob $A \times B$ immer dasselbe wie $B \times A$ ist. Die Antwort ist *nein* und dafür braucht man nur ein Gegenbeispiel, etwa $A = \{1\}$ und $B = \{2\}$. (Wenn Ihnen das nicht sofort klar ist, dann schreiben Sie $A \times B$ und $B \times A$ auf.) Allgemein gilt $A \times B = B \times A$ dann und *nur* dann, wenn $A = B$ gilt oder eine der beiden Mengen leer ist.

Lösung 3.17. Den ersten Teil kann man natürlich *nicht* realisieren. Nach Lemma 3.2 müsste $|A|$ dann die Mächtigkeit $\sqrt{42}$ haben. Aber die Mächtigkeit einer (endlichen) Menge muss offensichtlich eine (nichtnegative) ganze Zahl sein und $\sqrt{42}$ ist keine ganze Zahl. (Siehe auch Aufgabe 1.31.)

Für den zweiten Teil gibt es viele Möglichkeiten, z. B. $A = \{0,10,20,30,40,50,60\}$ und $B = \{0,1,2,3,4,5\}$.

Lösung 3.18. Offenbar gilt $|A| = 6$ und damit $|B| = 2^6$ nach Satz 3.1. Nach Lemma 3.2 folgt $|C| = 2^6 \cdot 2^6 = 2^{12} = 4096$ und damit auch $|D| = 4096$.

War Ihr Ergebnis vielleicht 4095? Dann haben Sie wahrscheinlich einen typischen Denkfehler begangen, um den es bereits in Aufgabe 3.3 ging. Es gilt zwar (siehe Aufgabe 2.7) $\emptyset \subseteq X$ für jede Menge X, aber das bedeutet *nicht*, dass $\emptyset \in X$ für jede Menge X gilt. Insbesondere gilt in dieser Aufgabe $\emptyset \notin C$ (warum?) und damit $D = C$.

Lösung 3.19. Vielleicht sollten wir erst einmal über die Definition von A_q sprechen und uns klarmachen, dass p und q dort ganz unterschiedliche Rollen spielen. p ist eine Variable, die wie üblich ein „Prototyp“ für die Elemente der Menge ist. Man könnte dafür auch einen anderen Buchstaben wie n oder r verwenden, ohne am Ergebnis etwas zu ändern. q ist hingegen ein *Parameter*, der quasi „von außen“ auf die Menge wirkt. Wir erhalten für unterschiedliche q evtl. *unterschiedliche* Mengen, z. B. $A_2 = \emptyset$, $A_3 = \{2\}$ und $A_4 = A_5 = \{2,3\}$.

Parameter

Nun zur eigentlichen Aufgabe: Damit $|A_q \times A_q| = 100$ gilt, muss A_q nach Lemma 3.2 genau zehn Elemente haben. Und das müssen nach Definition von A_q die ersten zehn Primzahlen sein. Also muss q, weil nach einer Primzahl gefragt wurde, die elfte Primzahl sein: 31.

Lösung 3.20. Eine typische Mathematiker-Frage und darauf gibt es auch eine typische Mathematiker-Antwort: Ja, es gibt 0-Tupel, aber nur eines, nämlich $()$. Das ist wie mit der leeren Menge.

Lösung 3.21. Hier geht es offenbar um eine ähnlich „akademische“ Frage wie bei Aufgabe 3.13. Man kann ein Objekt wie (a_1, a_2, a_3) durch $(a_1, (a_2, a_3))$ definieren. Man baut es sich also aus zwei „verschachtelten“ 2-Tupeln zusammen. Es lässt sich leicht nachweisen – und vielleicht probieren Sie das mal –, dass man damit die gewünschten Eigenschaften erhält.

Man könnte es übrigens auch so machen: $((a_1, a_2), a_3)$. Dadurch erhielte man rein technisch ein *anderes* Objekt. Aber die wesentlichen Eigenschaften der Definition von Seite 45 würde das nicht tangieren. Wie Aufgabe 3.13 ist diese kleine Bastelei für die Grundlagenforschung interessant, aber für die Praxis irrelevant.

Lösung 4.3. Nennen wir die Vereine F, K_1 und K_2. Dann ergibt sich nach dem Inklusions-Exklusions-Prinzip

$$\begin{aligned} |F \cup K_1 \cup K_2| &= |F| + |K_1| + |K_2| - |F \cap K_1| - |F \cap K_2| - |K_1 \cap K_2| + |F \cap K_1 \cap K_2| \\ &= 98 + 76 + 55 - 7 - 5 - 5 + 2 = 214. \end{aligned}$$

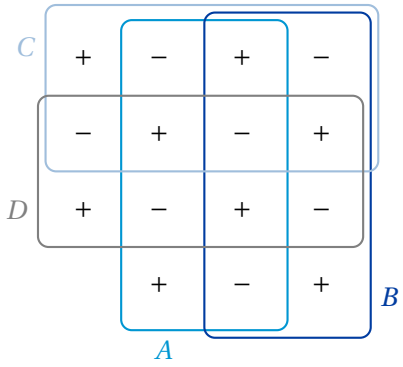
Das Dorf hat also 215 Einwohner. (Hoffentlich haben Sie Albert nicht vergessen …)

Lösung 4.4. So müsste es für $|A \cup B \cup C \cup D|$ aussehen:

$$\begin{aligned} &|A| + |B| + |C| + |D| \\ &- |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| \\ &+ |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| \\ &- |A \cap B \cap C \cap D| \end{aligned}$$

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Grafisch kann man das folgendermaßen darstellen:



Lösung 4.5. Weil $A \cap B$ und $A \cap C$ disjunkt sind, muss $A \cap B \cap C$ leer sein. Wenn Ihnen das nicht klar ist, dann zeichnen Sie sich dazu ein Mengendiagramm! (Hier bietet sich nebenbei die Gelegenheit, darauf hinzuweisen, dass in Aufgaben zur Mathematik selten unnötige Informationen stehen.[36] Wenn Sie nicht alle Aussagen aus dem Aufgabentext verwenden, steckt in Ihrer Lösung wahrscheinlich ein Denkfehler.)

Mit Satz 4.2 haben wir nun

$$\begin{aligned} 70 &= |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 30 + 30 + 30 - 5 - 6 - |B \cap C| + 0 = 79 - |B \cap C| \end{aligned}$$

und das kann man zu $|B \cap C| = 9$ umstellen.

Lösung 4.6. Wir bezeichnen mit A_n die Menge der Zahlen unter 100, die durch n teilbar sind. Wir wollen wissen, wie viele Elemente die Menge $B = A_2 \cup A_3 \cup A_5$ hat. Die Lösung für die Aufgabe ist nämlich dann $100 - |B|$.

Wie viele Elemente enthält eine der Mengen A_n? Für $n = 5$ sind es die Zahlen 0, 5, 10, 15 bis 95, also die Zahlen von $0 \cdot 5$ bis $19 \cdot 5$. Das sind 20, also $100/5$ Zahlen. Für $n = 3$ sind es die Zahlen $0 \cdot 3$ bis $33 \cdot 3$, also 34 Stück. Auf die Zahl 34 kommt man, wenn man 100 durch 3 teilt und dann die nächstgrößere ganze Zahl ermittelt. Man schreibt das mithilfe der sogenannten *oberen Gaußklammer* als $\lceil 100/3 \rceil$. (Sie müssen diese Schreibweise für das Lösen der Aufgabe nicht kennen, aber sie erleichtert das Aufschreiben.) Allgemein hat A_n offenbar $\lceil 100/n \rceil$ Elemente.

Wenn man nun z.B. $A_3 \cap A_5$ betrachtet, so enthält diese Menge alle Zahlen unter 100, die sowohl durch 3 als auch durch 5 teilbar sind. Das sind aber offensichtlich genau die Zahlen, die durch $3 \cdot 5 = 15$ teilbar sind, weil 3 und 5 teilerfremd sind. Mit anderen Worten bedeutet das: $A_3 \cap A_5 = A_{15}$. Ebenso ist $A_2 \cap A_3 \cap A_5 = A_{30}$ und so weiter.

Mit dem Inklusions-Exklusions-Prinzip ergibt sich nun

$$|B| = |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|$$

[36] Auf jeden Fall nicht in diesem Skript und auch nicht in guten Mathebüchern. Für Aufgaben in aktuellen Schulbüchern würde ich allerdings meine Hand nicht ins Feuer legen …

$$
\begin{aligned}
&= |A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}| \\
&= \lceil 100/2 \rceil + \lceil 100/3 \rceil + \lceil 100/5 \rceil \\
&\quad - \lceil 100/6 \rceil - \lceil 100/10 \rceil - \lceil 100/15 \rceil + \lceil 100/30 \rceil \\
&= 50 + 34 + 20 - 17 - 10 - 7 + 4 = 74
\end{aligned}
$$

und die gesuchte Antwort ist $100 - 74 = 26$.

Falls Sie das nicht komplett selbst lösen konnten, ist das nicht so dramatisch. Wichtig ist, dass Sie verstanden haben, wie das Inklusions-Exklusions-Prinzip verwendet wurde. Überprüfen Sie Ihr Verständnis, indem Sie nun ausrechnen, wie viele natürliche Zahlen es gibt, die kleiner als 1000 und weder durch 2 noch durch 3 noch durch 5 noch durch 7 teilbar sind. (Zur Kontrolle: Die korrekte Antwort ist 228.)

Lösung 4.7. $[0]$ ist die leere Menge, denn es gibt keine natürliche Zahl k mit $1 \leq k \leq 0$. So etwas werden Sie oft in mathematischen Texten finden. Wenn Sie beispielsweise $x_1, \ldots, x_n$ lesen, dann sind damit wahrscheinlich n Variablen (siehe Fußnote 14) gemeint, aber es würde eine Mathematikerin nicht überraschen, dass darin auch der Fall $n = 0$ inbegriffen ist, bei dem es dann eben *keine* Variable gibt.

$[\pi]$ würde zwar vielleicht durchaus Sinn ergeben, aber bei dieser Frage ging es darum, dass $[\pi]$ gar nicht definiert ist. Die Definition gilt nur für natürliche Zahlen n. Denken Sie daran, immer aufmerksam zu lesen!

Lösung 4.8. Nehmen wir das Beispiel $X = \{12, 17\}$ mit $|X| = 2$. P_X ist dann die Menge $\{(a_1, a_2) : \{a_1, a_2\} = \{12, 17\}\}$. Die Aussageform rechts vom Doppelpunkt kann für zwei Belegungen der Individuenvariablen wahr werden: für $a_1 = 12$ und $a_2 = 17$ oder für $a_1 = 17$ und $a_2 = 12$. Das ergibt die beiden Tupel $(12, 17)$ und $(17, 12)$. Und das sind die beiden Elemente von P_X.

Lösung 4.9. Für $X = \emptyset$ wird aus der Aussage*form* in der Definition von P_X die *Aussage* $\{\} = \emptyset$, die immer wahr ist. (Siehe dazu auch die Lösung von Aufgabe 4.7.) Die Menge besteht aus 0-Tupeln, von denen es – siehe Aufgabe 3.20 – nur eines gibt. Also ist $P_\emptyset$ die Menge $\{()\}$.

Lösung 4.11. Man erzeugt alle Permutationen des Tupels, indem man die Indizes – also die Menge $[n]$ – permutiert. Wenn wir es beispielsweise mit dem Tupel $(b_1, b_2, b_3) = (1, 2, 1)$ zu tun haben, dann ist $(3, 1, 2)$ eine Permutation aus P_3 und die zugehörige Permutation des Tupels ist $(b_3, b_1, b_2) = (1, 1, 2)$. Da wir es mit Mengen zu tun haben, werden Dopplungen wie $(b_1, b_3, b_2) = (1, 1, 2)$ automatisch „geschluckt“.

Lösung 4.12. Es geht um ein 5-Tupel, also $n = 5$. Wir haben $b_1 = b_2 = b_3 = 1$ und $b_4 = b_5 = 2$. r ist 2, denn es gibt nur die beiden Komponenten 1 und 2. Wir können $a_1 = 1$ und $a_2 = 2$ setzen. Dann haben wir $k_1 = 3$ und $k_2 = 2$. Wir wir schon wissen, ergibt sich

$$\frac{n!}{k_1!\,k_2!} = \frac{5!}{3!2!} = 10.$$

Lösung 4.13. Es geht um ein 7-Tupel mit den drei unterschiedlichen Komponenten 2, 3 und 7 die mit den Häufigkeiten 4, 2 und 1 auftreten. Die gesuchte Anzahl ist

$$\frac{7!}{4!\,2!\,1!} = 105.$$

Es ist offensichtlich wesentlich einfacher, sich einmal so eine Formel zu überlegen, statt in jedem Einzelfall mühsam alle Permutationen aufzuschreiben und dabei Gefahr zu laufen, einige zu übersehen. Beachten Sie, dass unter den 105 Permutationen natürlich auch das „Original“ $(2,3,2,3,7,2,2)$ mitgezählt wird.

Lösung 4.14. In Satz 4.3 geht es faktisch um die Permutationen von n-Tupeln, bei denen alle Komponenten verschieden sind. Man hat dann $r = n$ und $k_1 = 1$, $k_2 = 1$ und so weiter. Damit ergibt sich als Mächtigkeit schlicht und einfach $n!$, weil der Nenner in Satz 4.4 in diesem Spezialfall die Zahl 1 ist.

Lösung 4.16. $|V_{[8],5}| = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6\,720$.

Lösung 4.17. In gewissem Sinne war dies eine Fangfrage. Die Antwort ist nämlich *nicht* $10 \cdot 9 \cdot 8 = 720$. Das wäre richtig gewesen, wenn es um *alle* 3-Tupel aus drei verschiedenen Dezimalziffern gegangen wäre, weil es zehn Ziffern (0 bis 9) gibt. Weil jedoch führende Nullen wie z. B. bei $(0,4,2)$ keine dreistelligen Zahlen liefern, geht es so nicht. Eine Möglichkeit ist die Überlegung, dass man für die erste Ziffer nicht zehn, sondern nur neun Möglichkeiten hat (weil es keine Null sein darf). Für die zweite hat man dann ebenfalls neun. Die erste kann man nicht mehr wählen, aber dafür ist nun die Null möglich. Und für die dritte Ziffer verbleiben noch acht Möglichkeiten, weil zwei Ziffern bereits „ausgeschieden“ sind. Es ergibt sich $9 \cdot 9 \cdot 8 = 648$. Eine zweite Möglichkeit ist, dass man vom obigen Ergebnis 720 alle „verbotenen“ Tupel abzieht, also alle, die mit Null anfangen. Davon muss es offenbar $9 \cdot 8 = 72$ geben. $720 - 72$ ist ebenfalls 648.

Die „Moral“ dieser Aufgabe ist, dass man immer gut überlegen sollte, was genau man wissen will, bevor man gedankenlos irgendeine Formel anwendet!

Lösung 4.18. Es handelt sich um Lemma 3.3.

Lösung 4.19. Wir haben uns gerade überlegt, dass die Teilmengen von $[n]$ genau den Elementen von $\{0,1\}^n$ entsprechen. Und letztere Menge hat nach Satz 4.6 die Mächtigkeit $|\{0,1\}|^n = 2^n$.

Lösung 4.20. Nach Satz 4.7 berechnet man mit dieser Summe die Anzahl *aller* Teilmengen einer n-elementigen Menge, denn jede Teilmenge einer solchen Menge hat eine Mächtigkeit, die nicht kleiner als 0 und nicht größer als n ist. Also muss 2^n herauskommen.

Lösung 4.21. Die Antwort ist nach Satz 4.7 $\binom{n}{k}$. Dafür muss man sich nur überlegen, dass die in der Aufgabenstellung vorkommenden k-Tupel sortiert sind und erzwungenermaßen lauter verschiedene Komponenten haben. Sie entsprechen also genau den k-elementigen Teilmengen von X.

Lösung 4.22. Bei (v) geht es um Permutationen und es gibt $n!$ mögliche Ergebnisse. (iv) beschreibt Permutationen mit Wiederholungen. Um die Anzahl der Ergebnisse zu berechnen, braucht man genauere Informationen über den Urneninhalt: Welche Zahl befindet sich wie oft in der Urne? Man verwendet dann die Formel aus Satz 4.4. (iii) beschreibt Variationen und die gesuchte Anzahl ist $n!/(n-k)!$. Bei Punkt (ii) ist der Unterschied, dass Zahlen mehrfach gezogen werden können. Das sind also Variationen mit Wiederholungen und damit ergeben sich n^k mögliche Ausgänge. Bei (i) geht es um Kombinationen (denn bei gleichzeitiger Entnahme kann man nichts über eine Reihenfolge aussagen). Die gesuchte Anzahl ist $\binom{n}{k}$. Punkt (vi) beschreibt schließlich Kombinationen mit Wiederholungen. Hier gibt es $\binom{n+k-1}{k}$ mögliche Ausgänge.

Lösung 4.23. Da die Reihenfolge natürlich unerheblich ist und weil es jede Spielkarte nur einmal gibt, geht es um Kombinationen ohne Wiederholungen. Abstrakt gesehen können Sie die Menge der Karten mit der Menge $[52]$ identifizieren. Jedes mögliche Blatt ist dann eine 5-elementige Teilmenge dieser Menge. Also ergeben sich $\binom{52}{5}$ Möglichkeiten. Das sind etwas mehr als zweieinhalb Millionen.

Lösung 4.24. Hier geht es um Variationen mit Wiederholungen, denn es kommt auf die Reihenfolge (die Positionen) an und Farben können mehrfach verwendet werden. In der mathematischen Formulierung lässt sich jeder Farbcode als Quadrupel aus $[6]^4$ notieren, wobei die Zahl in der i-ten Komponente für die Farbe in der i-ten Position steht. Es gibt $6^4 = 1\,296$ Möglichkeiten.

Lösung 4.25. Die Dekanin muss zunächst auswählen, wer die fünf glücklichen Mathematiker sind, die eines der begehrten Büros erhalten. Dann kommt es aber auch noch auf die Reihenfolge an, weil die Büros nicht identisch sind. Das sind Variationen; und zwar *ohne* Wiederholungen, weil sonst einem Prof mehrere Büros zugewiesen würden. Technisch kann man jede mögliche Lösung als ein 5-Tupel aus $V_{[12],5}$ darstellen, wobei die i-te Komponente des Tupels die Person codiert, die das i-te Büro erhält. Die arme Dekanin muss sich daher für eine von $12!/7! = 95\,040$ Möglichkeiten entscheiden.

Lösung 4.26. Da es um die Reihenfolge einer vorgegebenen Sequenz geht, haben wir es mit Permutationen zu tun. Und es sind Permutationen *mit* Wiederholungen, weil einige Buchstaben mehrfach auftreten. Mit den Bezeichnungen von Satz 4.4 hat man $n = 11$, $r = 4$, $k_1 = 1$, $k_2 = 2$ und $k_3 = k_4 = 4$ für ein *M*, zweimal *P* und jeweils viermal *I* und *S*. Es ergibt sich $11!/(2!\,4!^2) = 34\,650$.

Lösung 4.27. Hier geht es um Kombinationen, weil die Reihenfolge der Befüllung der Mulden für die Anzahl keine Rolle spielt. Und es geht um Kombinationen mit Wiederholungen, weil nicht in jede Mulde ein anderer Teig kommt. Abstrakt gesehen ist jede Befüllung ein Tupel der Form $(x_1, x_2, x_3) \in \mathbb{N}^3$, wobei $x_1 + x_2 + x_3 = 12$ gelten muss. (x_1 wäre dann z. B. die Anzahl der Mulden, in die Blaubeermuffinteig kommt.) Es gibt daher $\binom{3+12-1}{12} = \binom{14}{12} = 91$ Möglichkeiten.

Lösung 4.28. Es handelt sich hierbei ebenfalls um Kombinationen mit Wiederholungen. (Es werden fünf von fünf Farben ausgewählt, die aber nicht verschieden sein müssen.) Daher gibt es $\binom{5+5-1}{5} = \binom{9}{5} = 126$ Möglichkeiten.

Lösung 4.29. Da es auf die Reihenfolge ankommt, während die fünf Sehenswürdigkeiten bereits feststehen, geht es um Permutationen. Und es gibt offenbar keine Wiederholungen, denn das würde bedeuten, dass Sehenswürdigkeiten mehrfach besucht würden. Formal kann man jeden Vorschlag als ein 5-Tupel aus P_5 darstellen, bei dem die i-te Komponente angibt, welche der Sehenswürdigkeiten als i-te drankommt. Es gibt daher $5! = 120$ theoretisch mögliche Vorschläge. Da jedes Clubmitglied drei verschiedene Vorschläge abgegeben hat, kann es nicht mehr als 40 Mitglieder geben.

Lösung 4.30. Da es sieben Striche sind und es für jeden Strich zwei Möglichkeiten (breit oder schmal) gibt, handelt es sich um Variationen mit Wiederholungen. Es gibt $2^7 = 128$ Möglichkeiten.

Lösung 4.31. Ein Strichcode kann entweder symmetrisch zum mittleren Strich sein oder nicht. Die symmetrischen Strichcodes sind ihre eigenen Spiegelbilder, die unsymmetrischen Strichcodes haben jeweils ein eindeutig bestimmtes Spiegelbild (das natürlich auch unsymmetrisch ist). Ein symmetrischer Strichcode ist durch die Angabe der ersten vier Striche eindeutig bestimmt, also gibt es $2^4 = 16$ symmetrische Codes. Daher gibt es $128 - 16 = 112$ unsymmetrische Codes, die jeweils paarweise auftreten und daher nur 56 Postleitzahlen abdecken können. Insgesamt kann es in Taka-Tuka-Land also maximal $56 + 16 = 72$ Postleitzahlen geben.

Lösung 4.32. Fangen wir exemplarisch mit dem Fall an, dass Sie den Schokoteig gar nicht verwenden. Dann bleiben 12 Mulden, die Sie mit zwei Teigen befüllen können und das liefert 13 Möglichkeiten: 12-mal Kokos, 11-mal Kokos, 10-mal Kokos und so weiter; die Anzahl der Blaubeermuffins ergibt sich danach von selbst. Wenn Sie allgemein k Mulden mit Schokoteig befüllen, bleiben $13 - k$ Möglichkeiten, die Anzahl der Kokosmuffins (von 0 bis $12 - k$) auszuwählen. Es ergeben sich damit insgesamt

$$\sum_{k=0}^{6} (13 - k) = 13 + 12 + 11 + 10 + 9 + 8 + 7 = 70$$

Möglichkeiten.[37]

An dieser Stelle passt vielleicht die Klärung einer Frage, die oft gestellt wird: Wann wird in der Kombinatorik multipliziert (oder dividiert) und wann wird addiert (oder subtrahiert)? Man kann eine Fragestellung oft in mehrere Fälle aufteilen und für jeden Fall einzeln die Anzahl der möglichen Ausgänge berechnen. Die Ergebnisse werden dann addiert. Dabei muss man allerdings aufpassen, dass sich die behandelten Fälle gegenseitig ausschließen![38] Das ist bei dieser Aufgabe geschehen. (Man muss natürlich darauf achten, dass man keinen Fall vergisst. Im konkreten Beispiel könnte man etwa den Fall übersehen, dass man den Schokoteig gar nicht verwendet.)

[37] Das Summenzeichen kennen Sie aus der Schule noch, oder?

[38] Anderenfalls wird man das Inklusions-Exklusions-Prinzip anwenden müssen.

Bei Aufgabe 4.31 wurde ebenfalls addiert: Die Anzahl der symmetrischen Codes addiert zur Anzahl der unsymmetrischen Codes ergibt die Gesamtzahl aller möglichen Codes.

Manchmal hat man das Glück, dass man es sogar mit sich gegenseitig ausschließenden Fällen zu tun hat, bei denen sich jeweils *dieselbe* Anzahl ergibt. Dann kann man multiplizieren statt addieren. Bei den sechs „Standardformeln“, die in der Tabelle auf Seite 56 zusammengefasst sind, ist das immer der Fall. Wenn man z. B. die Zahlen von 1 bis 6 sortiert, dann kann man von denen jede als erste Zahl nehmen. Das ergibt sechs Fälle, die sich gegenseitig ausschließen. Theoretisch müsste man für jeden Fall die Anzahl der Möglichkeiten ausrechnen und diese Ergebnisse alle addieren. Da man sich aber überlegen kann, dass alle Fälle im Prinzip gleich sind, reicht es, die Anzahl für einen Fall zu ermitteln und das Resultat mit sechs zu multiplizieren.

Lösung 4.33. Wenn man nicht mehr als drei Farben verwenden kann, fallen die Codes weg, bei denen alle vier Farben verschieden sind. Wie viele davon gibt es? Es gibt $\binom{6}{4} = 15$ Möglichkeiten, vier der sechs Farben auszuwählen. Und für jede solche Auswahl gibt es $4! = 24$ Möglichkeiten, die vier Farben anzuordnen. Das sind insgesamt $15 \cdot 24 = 360$ Möglichkeiten. Es verbleiben $1\,296 - 360 = 936$ Farbcodes, bei denen maximal drei Farben verwendet werden.

Lösung 4.34. Bei sechs Kästchen gibt es $2^6 = 64$ verschiedene Möglichkeiten zu antworten. (Das ist nämlich die Anzahl der Teilmengen einer Menge mit sechs Elementen. Siehe dazu auch Aufgabe 4.19.) Drei Möglichkeiten wurden durch die Aufgabenstellung ausgeschlossen, so dass maximal $64 - 3 = 61$ Personen teilgenommen haben können.

Lösung 4.35. Jedes der neun Pixel kann schwarz oder weiß sein; es gibt also insgesamt 2^9 verschiedene Muster. (Man kann das als Variationen mit Wiederholungen interpretieren – es wird neun Mal nacheinander jeweils schwarz oder weiß ausgewählt – oder als Anzahl der Teilmengen einer neun-elementigen Menge.) Man muss aber noch das eine Muster abziehen, bei dem alle Pixel weiß sind, und ebenso die neun Muster, bei denen genau ein Pixel schwarz ist. Und dieselbe Zahl von Mustern (also 10) muss man ein zweites Mal abziehen für die Muster bei denen zu wenige Pixel weiß sind. Somit ergibt sich als Antwort $2^9 - 2 \cdot (1 + 9) = 492$.

Lösung 4.36. Nach einigem Nachdenken sollte klar werden, dass sich hier das Inklusions-Exklusions-Prinzip anbietet, weil sich die genannten Bedingungen nicht gegenseitig ausschließen. Schreiben wir Z_k für die Menge der Zeichenketten, die die k-te Bedingung erfüllen, dann suchen wir die Mächtigkeit der Vereinigung von Z_1, Z_2 und Z_3. $|Z_1|$ ergibt sich mithilfe der Formel für Variationen mit Wiederholungen als $8^3 = 512$, weil der erste Buchstabe feststeht, während man die anderen drei frei wählen kann. Für Z_2 und Z_3 erhält man dieselbe Mächtigkeit. $Z_1 \cap Z_2$ enthält die Zeichenketten, die mit `AB` anfangen, und hat die Mächtigkeit $8^2 = 64$, weil man noch zwei „Freiheitsgrade“ hat. Das gilt sicher auch für die an-

deren Schnitte zweier Mengen. Und analog kommt man darauf, dass $Z_1 \cap Z_2 \cap Z_3$ acht Elemente enhält. Alles zusammen liefert nach Satz 4.2

$$\begin{aligned}
&|Z_1 \cup Z_2 \cup Z_3| \\
&\quad = |Z_1| + |Z_2| + |Z_3| - |Z_1 \cap Z_2| - |Z_1 \cap Z_3| - |Z_2 \cap Z_3| + |Z_1 \cap Z_2 \cap Z_3| \\
&\quad = 512 + 512 + 512 - 64 - 64 - 64 + 8 = 1352.
\end{aligned}$$

In der Mathematik ist es allerdings fast immer so, dass mehr als ein Weg zum Ziel führt. Wie bei der Lösung zu Aufgabe 3.11 kann man auch hier das *Gegenteil* betrachten: Wie konstruiert man eine Zeichenkette, die *keine* der drei Bedingungen erfüllt? Man darf für die erste Stelle kein `A` wählen, hat also noch sieben Möglichkeiten. Das gilt ebenso für die zweite und dritte Stelle. Nur an der vierten Stelle hat man die freie Wahl unter acht Buchstaben. Das ergibt $7 \cdot 7 \cdot 7 \cdot 8 = 2744$ Möglichkeiten. Insgesamt gibt es $8^4 = 4096$ mögliche Zeichenketten der Länge 4, die man aus den vorgegebenen Buchstaben bilden kann. Die Antwort erhält man nun durch $4096 - 2744$ und natürlich kommt dasselbe Ergebnis wie eben heraus.

Lösung 4.37. Alle genannten Varianten lassen sich wie in der Lösung zu Aufgabe 4.36 mit dem Inklusions-Exklusions-Prinzip lösen. Es gibt teilweise auch andere Wege, aber wenn Sie das besagte Prinzip verwenden, haben Sie eine Methode, die in solchen Fällen immer funktioniert.

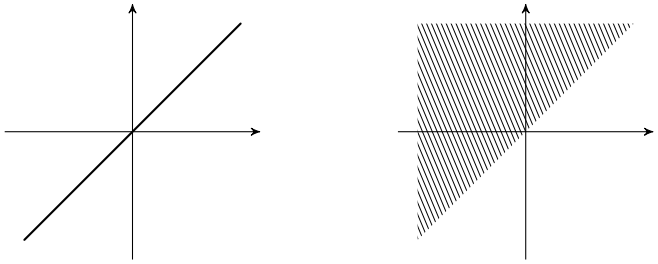
Wie können Sie überprüfen, ob Ihre Antworten richtig sind? Eine Möglichkeit ist ein selbstgeschriebenes kleines Computerprogramm, das jeweils alle erlaubten Zeichenketten erzeugt und diese zählt.[39] Wenn Sie das nicht können oder wollen, dann bietet sich noch ein anderes Verfahren an, das in der Kombinatorik oft hilfreich sein kann: Arbeiten Sie zunächst mit Zahlen, die deutlich kleiner, aber für die Aufgabenstellung noch ausreichend groß sind, um anhand dieser „vereinfachten“ Aufgabe zu überprüfen, ob Ihr Ansatz richtig ist. Im konkreten Fall könnte man nur mit den vier Buchstaben von `A` bis `D` arbeiten. Mit denen kann man nur $4^4 = 256$ Zeichenketten mit vier Zeichen bilden. Die passen alle auf ein Blatt Papier.

Lösung 5.1. Alle vier sind Aussageformen. Und alle vier sind Aussageformen mit *zwei* Individuenvariablen. Ihnen ist hoffentlich klar, dass die Menge $\{y^n : n \in \mathbb{N}\}$ für jedes y eine andere Menge ist, wohingegen der Buchstabe n keine Rolle spielt: $\{y^m : m \in \mathbb{N}\}$ ist *dieselbe* Menge. Alle vier Aussageformen sagen also etwas über x und y aus.

Lösung 5.3. Die Identität auf $\mathbb{R}$ ist die Gerade, die man auch *Hauptdiagonale* nennt. Die Kleiner-Relation ist die Hälfte der Ebene oberhalb der Hauptdiagonale *ohne* die Gerade selbst.

Hauptdiagonale

[39] Das wäre gleichzeitig eine gute Übung im Programmieren!

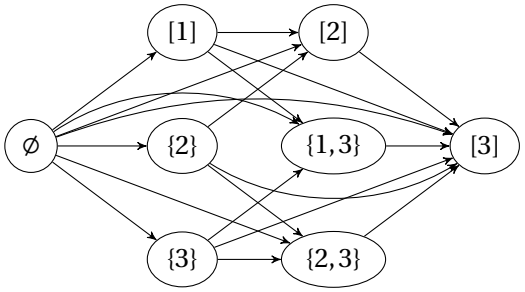


Natürlich sehen wir in beiden Fällen nur einen Ausschnitt, weil sich die Punktmengen in unserer Vorstellung unendlich weit ausdehnen.

Lösung 5.4. Das sollte so aussehen:

	$\emptyset$	$[1]$	$\{2\}$	$\{3\}$	$[2]$	$\{1,3\}$	$\{2,3\}$	$[3]$
1		×			×	×		×
2			×		×		×	×
3				×		×	×	×

Lösung 5.5. Die Hauptarbeit besteht hierbei wohl darin, den Überblick nicht zu verlieren und nichts zu vergessen.



Beachten Sie, dass es keine „Schleifen“ gibt, weil es in der Aufgabe um $\subset$ und nicht um $\subseteq$ ging.

Lösung 5.6. $A^2 = A \times A$ erfüllt trivialerweise alle drei Bedingungen. Diese Relation ist maximal unter den Relationen auf A, weil es kein Paar mehr gibt, das man noch hinzufügen könnte.

Lösung 5.7. Natürlich nicht, weil $(-1,-1)$ beispielsweise kein Element von $\mathrm{id}_{\mathbb{N}}$ ist. Diese Aufgabe sollte insbesondere deutlich machen, dass der Zusatz „auf A“ in der Definition der Reflexivität wichtig ist. $\mathrm{id}_{\mathbb{N}}$ ist reflexiv auf $\mathbb{N}$, aber nicht auf $\mathbb{Z}$ oder auf $\mathbb{R}$. Es ergibt keinen Sinn, einfach zu sagen, dass $\mathrm{id}_{\mathbb{N}}$ reflexiv oder nicht reflexiv sei.

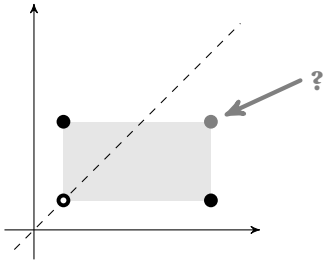
Lösung 5.8. E ist symmetrisch, denn wenn $x^2 + y^2 = 1$ gilt, dann gilt natürlich auch die Gleichung $y^2 + x^2 = 1$, die durch Vertauschen der Variablen entsteht. Geometrisch bedeutet das, dass der Einheitskreis spiegelsymmetrisch zur Hauptdiagonalen ist, denn durch Spiegelung an dieser Geraden wird aus dem Punkt (x, y) der Punkt (y, x).

Man muss hier allerdings aufpassen, dass man nicht den gerade definierten Begriff der Symmetrie einer Relation mit dem Konzept der Symmetrie einer geometrischen Figur verwechselt. Es gibt zwar – wie wir hier gesehen haben – Entsprechungen, aber man muss genau lesen und dem Kontext entnehmen, von *welcher* Symmetrie jeweils die Rede ist.

Lösung 5.9. Nein. Und wir erinnern uns, dass zur Begründung in so einem Fall ein einziges Gegenbeispiel ausreicht. Hier ist eins: $(1,0)$ und $(0,1)$ liegen beide auf dem Einheitskreis, d. h., diese beiden Paare sind Elemente von E. Wäre E transitiv, dann müsste auch $(1,1)$ zu E gehören. Aber der Punkt $(1,1)$ liegt nicht auf dem Kreis, weil 1^2+1^2 nicht 1, sondern 2 ist.

Lösung 5.10. Nein. Beispielsweise haben Hamburg und Niedersachsen sowie Niedersachsen und Bremen eine gemeinsame Grenze, aber nicht Hamburg und Bremen.

Lösung 5.11. Wenn zwei Punkte der Relation gegenüberliegende Ecken eines achsenparallelen Rechtecks bilden, von dem eine weitere Ecke auf der Hauptdiagonalen liegt, dann muss die vierte Ecke ebenfalls zur Relation gehören.



Lösung 5.12. Wir nennen die Relationen von links nach rechts R_1 bis R_3. R_1 ist nicht reflexiv auf $[4]$, die anderen beiden Relationen sind es. Das sieht man sofort, indem man einfach die Hauptdiagonale (die in diesem Fall von links oben nach rechts unten verläuft) anschaut. R_1 ist symmetrisch und transitiv, denn es handelt sich um $[3] \times [3]$, siehe Aufgabe 5.6. R_2 ist auch symmetrisch, R_3 aber nicht. Man erkennt die Symmetrie analog zu Aufgabe 5.8 jeweils daran, dass die Kreuze spiegelsymmetrisch um die Hauptdiagonale verteilt sind. R_2 ist nicht transitiv und das lässt sich mit einem konkreten Gegenbeispiel belegen: Es gilt $1R_24$ und $4R_22$, aber *nicht* $1R_22$.

Die einzige Begründung, die etwas aufwendiger ist, ist die dafür, dass R_3 transitiv ist. So schlimm ist es aber auch nicht. Es liegt daran, dass $(1,4)$ das einzige Paar von R_3 ist, bei dem sich die beiden Komponenten unterscheiden. Gilt aR_3c und cR_3b, so können a, b und c also nicht drei verschiedene Zahlen sein. Wir haben also entweder den Fall aR_3a und aR_3b oder den Fall aR_3b und bR_3b vorliegen. In beiden Fällen ist nichts mehr zu zeigen.

Was man bei dieser Aufgabe übrigens lernt: Eine Relation kann zwei der Eigenschaften haben, ohne dass sie deswegen die dritte haben muss. Die drei Eigenschaften sind, wie man in der Mathematik sagt, *unabhängig* voneinander, d. h. es folgt nicht eine aus der anderen.

Lösung 5.13. Dafür muss man nur x und y vertauschen und erhält

$$R^{-1} = \{(y,x) \in \mathbb{R}^2 : x < y\} = \{(x,y) \in \mathbb{R}^2 : x > y\}.$$

Beachten Sie, dass die Antwort nicht etwa $\{(x,y) \in \mathbb{R}^2 : x \geq y\}$ ist. Das Umkehren der Relation hat nichts mit dem Negieren (wie in Aufgabe 1.9) zu tun.

Lösung 5.14. $R \circ R$ ist die Menge $\{(m,n) \in \mathbb{N}^+ \times \mathbb{N}^+ : 4m \text{ teilt } n\}$. Aus $(m,p) \in R$ und $(p,n) \in R$ folgt, dass es natürliche Zahlen k_1 und k_2 mit $p = k_1 2m$ bzw. $n = k_2 2p$ gibt. Einsetzen liefert $n = k_2 k_1 4m$ und damit muss $4m$ Teiler von n sein. Umgekehrt kann man aus der Tatsache, dass $4m$ Teiler von n ist, folgern, $(2m,n)$ und $(m,2m)$ Elemente von R sind.

Lösung 5.16. Ja, $\sim$ ist eine Äquivalenzrelation auf $\mathbb{N}$. Und das liegt schlicht und einfach daran, dass Q eine Funktion ist. Wir werden im nächsten Abschnitt noch ausführlicher über Funktionen nachdenken, aber für diese Aufgabe reicht das Schulwissen: Ist f eine Funktion mit Definitionsbereich D und $x \in D$, dann ist $f(x)$ ein eindeutig bestimmtes Element des Wertebereichs W von f. Durch $f(x) = f(y)$ wird dann eine Äquivalenzrelation auf D definiert, weil $=$ eine auf W ist. Beispielsweise ist R reflexiv auf D, weil natürlich $f(x) = f(x)$ für alle $x \in D$ gilt. Und so weiter.

Lösung 5.17. Das ist dasselbe Argument wie bei Aufgabe 5.16, denn es geht wieder um eine Funktion; nämlich um die, die jeder Person den Wochentag ihrer Geburt zuordnet.

Lösung 5.18. Ja, es handelt sich um eine Äquivalenzrelation. Die Reflexivität folgt daraus, dass null eine ganze Zahl ist. Die Transitivität erhält man so: Gilt xRy und yRz, dann bedeutet das $x - y \in \mathbb{Z}$ und $y - z \in \mathbb{Z}$. Damit folgt sofort xRz, weil $x - z$ als Summe der ganzen Zahlen $x - y$ und $y - z$ wieder eine ganze Zahl ist. R ist auch symmetrisch, denn $x - y$ ist genau dann eine ganze Zahl, wenn $y - x = -(x - y)$ eine ist.

Geht man von $\mathbb{Z}$ zu $\mathbb{N}$ über, dann bleiben Reflexivität und Transitivität erhalten und die Begründungen sind identisch. Die Symmetrie geht jedoch verloren, weil aus einer positiven natürlichen Zahl $x - y$ durch das Vertauschen die negative Zahl $y - x$ wird.

Lösung 5.19. Es ist empfehlenswert, eine Tabelle wie auf Seite 62 zu erstellen. Man sieht dann, dass R offensichtlich reflexiv auf A ist und dass die Paare $(1,3)$ und $(1,4)$ die Symmetrie „stören“. Da man nach Aufgabenstellung nicht sowohl $(3,1)$ als auch $(4,1)$ hinzufügen kann, um das zu beheben, muss eines der beiden Paare entfernt werden. Mit etwas Herumprobieren erkennt man, dass die Transitivität wegen $2R1$ und $1R3$ auch $2R3$ erzwingen würde. Also muss $(1,3)$ weg. Nimmt man dann $(4,1)$ hinzu, so ist das Resultat, also $(R \setminus \{(1,3)\}) \cup \{(4,1)\}$ eine Äquivalenzrelation. (Und das ist die *einzige* Möglichkeit, durch Entfernen und Hinzufügen von jeweils genau einem Paar eine Äquivalenzrelation zu erreichen.)

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 5.20. Nennen wir die Relationen von links nach rechts R_1 bis R_3, Dann haben wir:

$$\begin{aligned}
[1]_{R_1} &= [2]_{R_1} = [3]_{R_1} = \{1,2,3\}\\
[4]_{R_1} &= \{4\}\\
[4]/R_1 &= \{[1]_{R_1}, [4]_{R_1}\} = \{\{1,2,3\},\{4\}\}\\
[1]_{R_2} &= [2]_{R_2} = \{1,2\}\\
[3]_{R_2} &= [4]_{R_2} = \{3,4\}\\
[4]/R_2 &= \{[1]_{R_2}, [3]_{R_2}\} = \{\{1,2\},\{3,4\}\}\\
[1]_{R_3} &= [3]_{R_3} = \{1,3\}\\
[2]_{R_3} &= [4]_{R_3} = \{2,4\}\\
[4]/R_3 &= \{[1]_{R_3}, [2]_{R_3}\} = \{\{1,3\},\{2,4\}\}
\end{aligned}$$

Lösung 5.21. $A/R = \{\{1,2\},\{3,4\},\{5\},\{6\},\{7\}\}$.

Lösung 5.22. Für $\sim$ aus Aufgabe 5.16 besteht die Faktormenge $\mathbb{N}/\sim$ aus den zehn Äquivalenzklassen $[0]_\sim$ bis $[9]_\sim$. Erwähnenswert ist noch, dass die Klasse $[0]_\sim$ nur ein Element, nämlich die Zahl 0, hat, während alle anderen unendlich viele Elemente haben. In $[3]_\sim$ sind beispielsweise mindestens die Zahlen 3, 30, 300 und immer so weiter enthalten.

Für R aus Aufgabe 5.18 ergeben sich unendlich viele Äquivalenzklassen. Eine davon ist die Klasse $[0]_R$, die der Menge $\mathbb{Z}$ entspricht. Nimmt man allgemein zwei verschiedene Zahlen x und y, die im Intervall $[0,1)$ liegen,[40] dann gilt sicher $[x]_R \neq [y]_R$, denn die Differenz von x und y ist kleiner als 1, aber nicht 0, also keine ganze Zahl. Damit haben wir schon unendlich viele verschiedene Klassen.[41] Gleichzeitig sind das aber auch *alle* Klassen. Jede Zahl x, die *nicht* in $[0,1)$ enthalten ist, liegt in derselben Klasse wie $x' = x - \lfloor x \rfloor$,[42] denn $x - x'$ ist die ganze Zahl $\lfloor x \rfloor$ und x' liegt im Intervall $[0,1)$. Anschaulich ist $[x]_R$ immer die um x „verschobene“ Menge $\mathbb{Z}$, also

$$[x]_R = \{m + x : m \in \mathbb{Z}\} = \{m + x - \lfloor x \rfloor : m \in \mathbb{Z}\}.$$

Zum Beispiel haben wir

$$[1/3]_R = \{\ldots, -8/3, -5/3, -2/3, 1/3, 4/3, 7/3, 10/3, \ldots\}.$$

Lösung 5.23. Jede positive natürliche Zahl n ist in mindestens einer[43] der Mengen von $\mathscr{A}$ enthalten, nämlich in $[n]$. Also haben wir offenbar $\bigcup\mathscr{A} = \mathbb{N}^+$. Die einzige Zahl, die in *allen* Mengen von $\mathscr{A}$ enthalten ist, ist hingegen die Eins, also ergibt sich $\bigcap\mathscr{A} = \{1\}$.

[40] Falls Sie vergessen haben, was Sie in der Schule über Intervalle gelernt haben: Wir wiederholen das später noch.

[41] Falls Sie davon schon einmal gehört haben: Wir haben damit sogar überabzählbar viele Klassen.

[42] Sie haben sich sicher schon gedacht, dass damit die *untere Gaußklammer* – also das Abrunden – gemeint ist. Siehe dazu die Lösung von Aufgabe 4.6.

[43] Sogar in unendlich vielen, aber eine reicht.

Mit $\mathscr{B} = \{[n] : n \in \mathbb{N}\}$ kommt die leere Menge hinzu (siehe Aufgabe 4.7), d. h., wir haben $\mathscr{B} = \mathscr{A} \cup \{\emptyset\}$. Für die Vereinigungsmenge ändert das Hinzufügen der leeren Menge gar nichts, $\bigcup\mathscr{B} = \bigcup\mathscr{A} = \mathbb{N}^+$, aber die Schnittmenge ändert sich, weil es nun *keine* Zahl gibt, die in allen Mengen von $\mathscr{B}$ enthalten ist: $\bigcap\mathscr{B} = \emptyset$.

Lösung 5.24. Hier ergibt sich $\bigcup\mathscr{A} = \mathbb{N}$ und $\bigcap\mathscr{A} = \emptyset$.

Lösung 5.25. Das ist natürlich die leere Menge.

Lösung 5.26. Im ersten Fall wird eine Menge von Paaren definiert und keine Menge von Zahlen. Im zweiten Fall wird eine Menge von Mengen definiert. Man kann die zweite Variante aber reparieren, indem man $\bigcup\{\{n,-n\} : n \in \mathbb{N}\}$ schreibt. Das ist dann tatsächlich die Menge der ganzen Zahlen.

Lösung 5.27. Konnten Sie die Aufgabe lösen? Es ist keine Schande, wenn man so eine Aufgabe nicht lösen kann. Aber wenn Sie etwas lernen wollen, dann ist es dumm, wenn Sie es nicht zumindest probiert haben. Wie viele mathematische Aufgaben ist diese eine, bei der es keinen vorgefertigten Lösungsweg gibt, den man nur nachäffen muss. Häufig hilft nur Nachdenken und – das war ja auch der Tipp – Herumprobieren. Man kommt nicht umhin, einen Stift in die Hand zu nehmen und herumzukritzeln. Was weiß ich? Was fällt mir ein? Stimmt das auch?

Hier kommt man auf diesem Weg schnell zum Ziel. Wegen der ersten Eigenschaft, ist die kleinste Menge, die infrage kommt, $\mathscr{A} = \{\mathbb{R}\}$. Und die tut es auch schon!

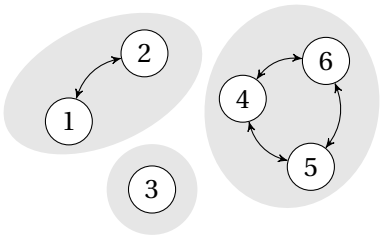
Lösung 5.28. In der Informatik meint man mit einer Partition einen *Teil* eines Laufwerks. Beim *Partitionieren* unterteilt man das gesamte Laufwerk in Partitionen. In der Mathematik würde man die Menge all dieser Partitionen (deren „Vereinigung“ das Laufwerk ergibt) als Partition bezeichnen.

Lösung 5.29. $\mathscr{A}$ ist keine Partition, weil die Elemente von $\mathscr{A}$ nicht paarweise disjunkt sind. Zum Beispiel gehören sowohl $\{0,1,2\}$ als auch $\{2,3,4\}$ zu $\mathscr{A}$, und diese beiden Mengen enthalten beide das Element 2. $\mathscr{B}$ ist keine Partition von $\mathbb{N}$, weil $\bigcup\mathscr{B} = \mathbb{N}^+ \neq \mathbb{N}$ gilt. $\mathscr{C}$ ist keine Partition, weil $\mathscr{C}$ die leere Menge enthält, z. B. für $n = 2$. $\mathscr{D}$ ist offensichtlich eine Partition von $\mathbb{N}$.

Lösung 5.30. Das könnte beispielsweise für die Relation $\mathrm{id}_{[6]} \cup S \cup S^{-1}$ mit

$$S = \{(1,2),(4,5),(4,6),(5,6)\}$$

so aussehen:



Wegen der Reflexivität muss von jedem Knoten ein Pfeil (eine „Schleife“) zum Knoten zurücklaufen. Der Übersichtlichkeit halber wurden die hier gleich weggelassen,

weil sie redundant sind. Wegen der Symmetrie müssen alle Kanten Pfeilspitzen auf beiden Seiten haben; die könnte man ebenfalls weglassen. Und wegen der Transitivität muss es zu jedem „Umweg“ (hier etwa von 4 nach 6 über 5) einen direkten Weg (also im Beispiel eine Kante von 4 nach 6) geben. Es ergeben sich dann wie von selbst disjunkte „Inseln“, die in der Grafik durch die grauen Scheiben dargestellt werden. Das sind die Elemente der Partition.

Lösung 5.31. Für $n = 0, 1, 2, 3$ erhält man die Elemente

$$\{1\}, \quad \{2,3\}, \quad \{4,5,6,7\}, \quad \{8,9,10,11,12,13,14,15\}$$

von $\mathscr{P}$. Kommt Ihnen das bekannt vor? Zwei Zahlen aus $\mathbb{N}^+$ stehen offenbar genau dann in der induzierten Relation zueinander, wenn sie dieselbe Anzahl von Stellen im Binärsystem haben.

Lösung 5.32. Da es nach Satz 5.2 eine eindeutige Zuordnung zwischen den Äquivalenzrelationen auf $[4]$ und den Partitionen von $[4]$ gibt, kann man sich zur Beantwortung der Frage genauso überlegen, wie viele Partitionen von $[4]$ es gibt: Es gibt eine Partition von $[4]$ mit einem Element, nämlich $\{[4]\}$. Betrachtet man die Partitionen von $[4]$ mit zwei Elementen, so kommt man entweder auf solche, bei denen beide Elemente zweielementige Mengen sind,[44] oder auf solche, bei denen eine Menge drei Elemente hat und eine eins.[45] Wenn eine Partition drei Elemente hat, dann muss eins ihrer Elemente zwei Elemente haben, während die anderen beiden Singletons sind.[46] Schließlich gibt es genau eine Partition mit vier Elementen.[47] Insgesamt kommt man also auf 15 Möglichkeiten. Wenn man die Fragestellung verallgemeinert, kommt man übrigens auf die sogenannten *Bellschen Zahlen*.

Lösung 6.1. Es darf nicht von einem Objekt links mehr als ein Pfeil ausgehen.

Lösung 6.2. f_1 ist eine Funktion, denn alle Elemente sind geordnete Paare und f_1 ist rechtseindeutig: Wenn m und n gleich sind, dann sind natürlich auch die Werte $m/3$ und $n/3$ gleich. Der Einheitskreis f_2 ist zwar eine Menge von geordneten Paaren, aber keine Funktion: Zu f_2 gehören z. B. die beiden Elemente $(0,1)$ und $(0,-1)$, also ist f_2 nicht rechtseindeutig. f_3 hat nicht nur geordnete Paare als Elemente, sondern auch die Zahl 3. Daher ist f_3 nicht einmal eine Relation, geschweige denn eine Funktion. f_4 ist eine Funktion. f_5 aber nicht, weil die Rechtseindeutigkeit verletzt ist, denn sowohl $(1,2)$ als auch $(1,3)$ gehören zu f_5. f_6 – die leere Menge – ist eine Funktion. Sie ist erstens eine Menge von Paaren (nämlich von null Paaren) und zweitens ist sie rechtseindeutig, denn eine Relation, die *nicht* rechtseindeutig ist, muss ja mindestens zwei Paare enthalten.

Lösung 6.3. Das sollte hoffentlich kein Problem gewesen sein:

$$\operatorname{dom}(f_1) = \mathbb{N} \qquad \operatorname{rng}(f_1) = \{n/3 : n \in \mathbb{N}\}$$

[44] Davon gibt es offenbar drei: $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$ und $\{\{1,4\},\{2,3\}\}$.

[45] Davon gibt es vier: $\{\{1\},\{2,3,4\}\}$, $\{\{2\},\{1,3,4\}\}$, $\{\{3\},\{1,2,4\}\}$ und $\{\{4\},\{1,2,3\}\}$.

[46] Das ergibt sechs Möglichkeiten: $\{\{1,2\},\{3\},\{4\}\}$, $\{\{1,3\},\{2\},\{4\}\}$, $\{\{1,4\},\{2\},\{3\}\}$, $\{\{2,3\},\{1\},\{4\}\}$, $\{\{2,4\},\{1\},\{3\}\}$ und $\{\{3,4\},\{1\},\{2\}\}$.

[47] Das ist $\{\{1\},\{2\},\{3\},\{4\}\}$.

$$\begin{aligned}
\operatorname{dom}(f_2) = \operatorname{rng}(f_2) &= \{x \in \mathbb{R} : |x| \leq 1\} = [-1,1] \\
\operatorname{dom}(f_4) &= \{1,3,4\} & \operatorname{rng}(f_4) &= \{3,5\} \\
\operatorname{dom}(f_5) &= \{1,4\} & \operatorname{rng}(f_5) &= \{2,3,5\} \\
\operatorname{dom}(f_6) = \operatorname{rng}(f_6) &= \emptyset
\end{aligned}$$

Für f_2 wurde wieder die Schreibweise für Intervalle verwendet – siehe die Lösung zu Aufgabe 5.22. Beachten Sie, dass wir Definitions- und Wertebereich nicht nur für Funktionen, sondern allgemeiner für Relationen definiert hatten. Nur für f_3 ergibt die Angabe dieser beiden Mengen keinen Sinn.

Lösung 6.4. Bei komplizierteren Funktionen ist es häufig nicht so einfach, den Wertebereich genau anzugeben. Die Zielmenge sollte man allerdings möglichst „klein“ wählen, um informativ zu sein. Z. B. ist es besser, in (6.2) $\mathbb{Q}$ statt $\mathbb{R}$ zu schreiben, weil man dann sofort sieht, dass auf jeden Fall keine irrationalen Zahlen ausgegeben werden.

Lösung 6.5. g_1 ist eine Funktion mit Definitions- und Wertebereich $\mathbb{N}$. Ganz allgemein ist die Identität id_A für jede Menge A immer eine Funktion; nämlich einfach die ganz langweilige Funktion, die x auf x abbildet. g_3 ist keine Funktion, denn zu dieser Relation gehören zum Beispiel die Paare $(\{0\},\emptyset)$ und $(\{0\},\{0\})$. Definitions- und Wertebereich von g_3 ist jeweils $\mathscr{P}(\mathbb{N})$. g_4 ist eine Funktion. Sie bildet jede Teilmenge von $\mathbb{N}$ auf ihre Potenzmenge ab. Der Definitionsbereich ist $\mathscr{P}(\mathbb{N})$ und den Wertebereich kann man nicht einfacher als

$$\operatorname{rng}(g_4) = \{\mathscr{P}(A) : A \subseteq \mathbb{N}\}$$

hinschreiben. Siehe dazu auch Aufgabe 6.4; als Zielmenge würde sich eher die Menge $\mathscr{P}(\mathscr{P}(\mathbb{N}))$ eignen. g_5 ist keine Funktion, denn zu dieser Relation gehören zum Beispiel die Paare $(\mathbb{R}\setminus\{0,1\},\mathbb{R}\setminus\{0\})$ und $(\mathbb{R}\setminus\{0,1\},\mathbb{R}\setminus\{1\})$. Ferner haben wir

$$\begin{aligned}
\operatorname{dom}(g_5) &= \{\mathbb{R}\setminus\{a,b\} : a,b \in \mathbb{R}\} \text{ und} \\
\operatorname{rng}(g_5) &= \{\mathbb{R}\setminus\{a\} : a \in \mathbb{R}\}.
\end{aligned}$$

g_6 ist ebenfalls keine Funktion, denn zu dieser Relation gehören zum Beispiel die Paare $(\mathbb{R}\setminus\{0\},\mathbb{R}\setminus\{0,1\})$ und $(\mathbb{R}\setminus\{0\},\mathbb{R}\setminus\{0,2\})$. Offenbar gilt $\operatorname{dom}(g_6) = \operatorname{rng}(g_5)$ und $\operatorname{rng}(g_6) = \operatorname{dom}(g_5)$.

Wir haben zunächst $\operatorname{dom}(g_2) = \operatorname{rng}(g_4)$ und $\operatorname{rng}(g_2) = \operatorname{dom}(g_4)$. Die Begründung dafür, dass g_2 eine Funktion ist, ist allerdings ein bisschen schwieriger (und wurde in der Aufgabenstellung auch nicht verlangt): Jedes Element des Definitionsbereichs von g_2 ist die Potenzmenge einer Menge A von natürlichen Zahlen. Wie kann man A aus dieser Menge von Mengen „rekonstruieren“? A ist die größte der Mengen und alle anderen sind Teilmengen von ihr. Man erhält A dadurch, dass man die Vereinigungsmenge aller Mengen bildet. Mit anderen Worten: g_2 bildet jede Menge $\mathscr{B}$ ihres Definitionsbereichs auf $\bigcup\mathscr{B}$ ab. Damit haben wir eine „Rechenvorschrift“ für g_2.

Lösung 6.6. $f[A]$ ist A, aber $f^{-1}[A]$ ist *nicht* A, sondern $\{-1,0,1\}$, denn es gilt ja auch $f(-1) = 1$. $f^{-1}[\{-1\}]$ ist die leere Menge, denn bekanntlich wird keine reelle Zahl durch f auf -1 abgebildet. $f[\emptyset]$ ist natürlich auch die leere Menge.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 6.7. Wir haben $f[A] = \{(-7)^2-7, 2^2-7, 9^2-7\} = \{-3, 42, 74\}$. Zum Ermitteln von $f^{-1}[A]$ suchen wir die $x \in \mathbb{R}$, für die x^2-7 eine der Zahlen aus A ist. Für $2 \in A$ läuft das z. B. auf das Lösen der Gleichung $x^2-7=2$ hinaus und liefert $x=3$ oder $x=-3$. Insgesamt macht das $f^{-1}[A] = \{-4,-3,0,3,4\}$. $f[f^{-1}[A]]$ ist wieder A. Aber $f^{-1}[f[A]]$ ist $\{-9,-7,-2,2,7,9\}$.

Lösung 6.8. g bildet die *Zahl* 0 auf die Zahl 23 und die *Menge* $\{0\}$ auf die Zahl 42 ab.[48] $\mathrm{dom}(g)$ ist also $\{0,\{0\}\}$ und $\mathrm{rng}(g)$ ist $\{23,42\}$. Ferner haben wir $g(\{0\}) = 42$ und $g[\{0\}] = \{23\}$, eine Zahl und eine *Menge*.

Lösung 6.9. Zum Beispiel $M = \{1\}$. Dann haben wir $f[M] = \{2\}$ und $f^{-1}[f[M]] = \{1,4\}$. (Offenbar muss aber zumindest für jede Funktion $C \subseteq f^{-1}[f[C]]$ gelten.)

Für $N \subseteq \mathrm{rng}(f)$ gilt tatsächlich $f[f^{-1}[N]] = N$ für *jede* Funktion f. Wenn man allerdings in N auch Objekte zulässt, die nicht im Wertebereich liegen, stimmt das nicht mehr. Im Beispiel aus der Aufgabestellung könnte man $N = \{3\}$ nehmen. Dann hätte man $f^{-1}[N] = \emptyset$ und $f[f^{-1}[N]] = \emptyset$.

Lösung 6.10. Das klappt mit $M = \{1\}$ und $N = \{4\}$. Dann gilt

$$f[M \cap N] = f[\emptyset] = \emptyset \quad \text{und} \quad f[M] \cap f[N] = \{2\} \cap \{2\} = \{2\}.$$

Allerdings gilt $f[M \cup N] = f[M] \cup f[N]$ für jede Funktion f und beliebige Mengen $M, N \subseteq \mathrm{dom}(f)$.

Lösung 6.11. Ich meinte das so: Ist f eine beliebige Funktion, dann wird durch

$$R = \{(x,y) \in \mathrm{dom}(f)^2 : f(x) = f(y)\}$$

eine Äquivalenzrelation auf $\mathrm{dom}(f)$ definiert. Die Begründung dafür ist trivial, weil die drei Eigenschaften Reflexivität, Symmetrie und Transitivität jeweils direkt von der Gleichheitsrelation des Wertebereichs „vererbt“ werden. Beispielsweise gilt xRx für alle $x \in \mathrm{dom}(f)$, weil $f(x) = f(x)$ für alle $x \in \mathrm{dom}(f)$ gilt, und Letzteres ist einfach die Reflexivität von $\mathrm{id}_{\mathrm{rng}(f)}$.

Lösung 6.12. Die Äquivalenzklassen sind alle von der Form $f^{-1}[\{y\}]$ für $y \in \mathrm{rng}(f)$.

Lösung 6.13. $R|_X = \{(1,2),(2,6),(3,4)\}$.

Lösung 6.14. Aufgabe 6.6 entnimmt man $\mathrm{dom}(f) = \mathbb{R}$. Und nach Definition gilt $\mathrm{dom}(f|_M) = M$. Aus der Schule ist bekannt, dass $\mathrm{rng}(f)$ die Menge aller nichtnegativen reellen Zahlen ist, also das Intervall $[0,\infty)$. Weil allgemein $f(x) = f(-x)$ gilt, weil also jeder Funktionswert bis auf null „doppelt vorkommt“, gilt $\mathrm{rng}(f|_M) = \mathrm{rng}(f)$.

Lösung 6.15. Ich hatte an Funktionen der Form $x \mapsto mx+b$ gedacht, also an die, die man als Geraden visualisieren kann.

Lösung 6.16. Eine Funktion der Form $x \mapsto mx+b$ ist nur dann injektiv, wenn $m \neq 0$ gilt. Ansonsten hat man es nämlich mit einer *konstanten* Funktion der Form $x \mapsto b$ zu tun, die offensichtlich nicht injektiv ist.

[48] In diesem konkreten Beispiel ist g eine etwas artifizielle Funktion, anhand derer etwas demonstriert werden soll. In der höheren Mathematik können solche „seltsamen“ Konstruktionen aber manchmal durchaus eine Rolle spielen.

Lösung 6.17. Das ist einfach die korrekte Umkehrung der Implikation, um die es im Abschnitt über Aussagenlogik ging.

Lösung 6.18. f ist nicht injektiv, weil z. B. $f(3/2) = 1 = f(1)$ gilt. Für g könnte man das Beispiel $g(\{1\}) = 1 = g(\{2\})$ nehmen und $h(2) = 2 = h(11)$ für h. Natürlich werden Ihre Beispiele anders ausgesehen haben. Die Hauptsache ist, dass Sie das Prinzip verstanden haben.

Lösung 6.19. Das ist natürlich $\operatorname{rng}(f)$, also der Wertebereich von f.

Lösung 6.20. Die Elemente einer Funktion haben allgemein die Form (x, y) und in der Umkehrrelation werden die „umgedrehten" Paare (y, x) gesammelt. In f gilt $(x, y) = (x, 2x+8)$ und $(y, x) = (2x+8, x)$. Wir würden gerne so etwas wie $(y, \dots)$ schreiben, wobei die Punkte für einen Ausdruck stehen, in dem nur noch y vorkommt. Dafür lösen wir $y = 2x+8$ nach x auf. Das ergibt $y-8 = 2x$ bzw. $x = y/2-4$. Die Umkehrfunktion ist also $f^{-1} = \{(y, y/2-4) : y \in \mathbb{R}\}$.

Für g ist die gesuchte Rechenvorschrift $B \mapsto [6] \setminus B = g(B)$, d. h. wir haben $g^{-1} = g$. Falls Sie das nicht sofort sehen, dann machen Sie sich vielleicht mit einem Mengendiagramm klar, dass für $A \subseteq [6]$ immer $g(g(A)) = [6] \setminus ([6] \setminus A) = A$ gilt.

Obwohl es sich um dieselbe Rechenvorschrift wie in (6.3) handelt, ist h injektiv, denn der Definitionsbereich enthält keine negativen Zahlen. Die Rechenvorschrift für h^{-1} ist $m \mapsto \sqrt{m}$, wobei zu beachten ist, dass der Definitionsbereich von h^{-1} die Menge $h[\mathbb{N}] = \{n^2 : n \in \mathbb{N}\} = \{0, 1, 4, 9, 16, \dots\}$ ist – siehe Aufgabe 6.19.

Lösung 6.21. Grundsätzlich ist id_A für jede Menge A injektiv und die Umkehrfunktion ist immer id_A. Aber vielleicht hatten Sie auch eine andere Idee.

Lösung 6.22. f ist nicht injektiv, weil u. a. $f(-1) = 1 = f(1)$ gilt. $f|_A$ ist injektiv.

Lösung 6.23. Dann ist R einfach die Identität auf $\operatorname{dom}(f)$.

Lösung 6.24. Ich hatte an die Arkusfunktionen gedacht. Die trigonometrische Funktionen wie Sinus, Kosinus oder Tangens sind alle *nicht* injektiv. Damit man sie umkehren kann, muss man sie erst einschränken.

Lösung 6.25. Bei f kommt etwa die reelle Zahl π nicht als Funktionswert vor. (Die Funktionswerte von f sind ausschließlich ganze Zahlen.) Bei g kommt der Funktionswert 7 nicht vor. (Und alle größeren natürlichen Zahlen kommen „erst recht" nicht vor.) Und bei h kommt z. B. der Funktionswert 2 nicht vor (weil $\sqrt{2}$ nicht rational ist).

Lösung 6.26. f_1 ist injektiv und die Rechenvorschrift für f_1^{-1} ist $n \mapsto n-1$. f_1 ist aber nicht surjektiv,[49] weil null kein Funktionswert ist. f_2 ist nicht injektiv, weil z. B. 4 und 5 denselben Funktionswert 2 haben. f_2 ist aber surjektiv, denn jede natürlich Zahl m ist Funktionswert des Arguments $2m$. f_3 ist nicht injektiv, weil u. a. wieder 4 und 5 denselben Funktionswert haben. f_3 ist aber nicht surjektiv, weil null als

[49] Ich formuliere hier zur Eingewöhnung gleich mal ungenau, weil in der Aufgabenstellung ja stand, um welche Zielmenge es geht.

Funktionswert nicht vorkommt. f_4 ist natürlich injektiv und surjektiv; siehe auch Aufgabe 6.21.

Diese Aufgabe zeigt „nebenbei“, dass Injektivität und Surjektivität unabhängig voneinander sind. Erinnern Sie sich an Aufgabe 5.12, in der es um eine ähnliche Aussage ging.

Lösung 6.27. Ja. Die Funktion, die A in diesem Fall auf B abbildet, ist $\emptyset$. Siehe Aufgabe 6.2.

Lösung 6.28. Zwei Beispiele wären

$$\{(1,23),(2,42),(3,\pi),(4,0),(5,\sqrt{3})\} \quad \text{und}$$
$$\{(1,42),(2,23),(3,\pi),(4,0),(5,\sqrt{3})\}.$$

Durch die Darstellung ist hoffentlich klar geworden, dass jede solche Funktion eine Permutation der Menge B liefert – denn sie „sortiert“ ja deren fünf Elemente. Deshalb muss es (nach Satz 4.3) $5! = 120$ solche Funktionen geben.

Lösung 6.29. Ja, das tun sie. Das ist der Vorteil der abstrakten Definition über Mengen. Weil Funktionen nichts weiter als (bestimmte) Mengen sind, sind sie gleich, wenn sie als Mengen gleich sind. Und zwei Mengen sind bekanntlich genau dann gleich, wenn sie dieselben Elemente haben. Überträgt man das auf Funktionen und deren Elemente (die Paare sind), dann heißt das, dass zwei Funktionen genau dann gleich sind, wenn sie erstens denselben Definitionsbereich haben und zweitens jedem ihrer Argumente denselben Funktionswert zuordnen. (Und das klingt ja wohl auch nach einer vernünftigen Vorstellung davon, wann zwei Funktionen als gleich bezeichnet werden sollten.)

Lösung 6.30. Jede injektive Funktion $f\colon A \to B$ wählt offenbar ein „erstes“, „zweites“ und „drittes“ Element von B aus, nämlich $f(1)$, $f(2)$ und $f(3)$. Es handelt sich bei solchen Funktionen also um Variationen im Sinne der Kombinatorik. Die Antwort ist somit $5 \cdot 4 \cdot 3 = 60$. (Und die Antwort wäre dieselbe gewesen, wenn es sich bei A z. B. um die Menge $\{23,42,100\}$ gehandelt hätte.)

Lösung 6.31. Man kann sogar zwei angeben, die hoffentlich auch beide sofort einleuchten: Für endliche Mengen A und B gilt $|A| \leq |B|$, wenn eine der beiden folgenden Bedingungen erfüllt ist (und damit beide erfüllt sind):

(i) Es gibt eine injektive Funktion von A nach B.

(ii) Es gibt eine Funktion, die B surjektiv auf A abbildet.

Begründen kann man das damit, dass aus $|A| \leq |B|$ folgt, dass B eine Teilmenge B^* mit $|A| = |B^*|$ haben muss und dass es zwischen A und B^* eine Bijektion gibt.

Wäre in Aufgabe 6.30 die Frage also, wie viele injektive Funktionen von B nach A es gibt, so wäre die Antwort null.

Lösung 6.32. f muss injektiv sein. Nehmen wir uns nämlich irgendein Element x des Definitionsbereichs vor, dann gibt es dazu den Funktionswert $y = f(x)$. Mit $M = \{x\}$ gilt $f[M] = \{y\}$ und nach Aufgabenstellung $f^{-1}[\{y\}] = \{x\}$. Letzeres heißt

aber „übersetzt“, dass es außer x keine andere Eingabe gibt, die die Ausgabe y liefert.

Auch so etwas wie in Aufgabe 6.10 kann bei injektiven Funktionen nicht passieren.

Lösung 6.33. Nein, denn es gilt beispielsweise $2 \cdot 3 = 3 \cdot 2$, d. h. die beiden unterschiedlichen Tupel $(2,3)$ und $(3,2)$ werden auf denselben Funktionswert abgebildet.

Erinnern Sie sich an Aufgabe 3.14. Dort ging es auch um die Multiplikation, die dort A^2 auf B abgebildet hat. Weil die Funktion nicht injektiv ist, hat B weniger Elemente als A^2.

Lösung 6.34. Nein. Eine innere Verknüpfung auf $\mathbb{N}$ ist eine Abbildung von $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$. Aber bei der Subtraktion natürlicher Zahlen voneinander kommen nicht nur natürliche Zahlen heraus: $1 - 2$ ist beispielsweise -1.

Lösung 6.35. Nur f_1 ist nicht injektiv: beispielsweise gilt $f_1(0,0) = 0 = f_1(0,1)$.

Lösung 6.36. Ein Beispiel wäre die Funktion, die (m,n) auf $2^m 3^n$ abbildet. Dass die injektiv ist, folgt aus dem Fundamentalsatz der Arithmetik, der später noch als Satz 12.4 im Skript vorkommt. So eine „Codierung“ von Tupeln nennt man auch Gödelisierung.

Lösung 6.37. Das würde dazu führen, dass der Fall $x = 0$ doppelt auftaucht. Es würde in diesem Fall nichts ändern, weil in beiden Fällen der Funktionswert derselbe wäre, aber man sollte so etwas trotzdem möglichst vermeiden, weil man damit seine Leser verwirren könnte.

Lösung 6.38. Sowohl bei f_1 als auch bei f_2 ist die Definition unglücklich, weil die natürlichen Zahlen von 4 bis 9 jeweils beide Bedingungen erfüllen. Bei f_1 ist das aber nicht so schlimm, weil sich in beiden Fällen für alle sechs Zahlen der Funktionswert null ergibt. f_2 ist jedoch keine Funktion, denn es ist beispielsweise nicht klar, ob dem Argument 7 der Funktionswert 0 oder der Funktionswert 1 zugeordnet werden soll.

Lösung 6.39. Das ist natürlich der Absolutbetrag, der „offiziell“ auf Seite 164 definiert werden wird. Siehe auch Aufgabe 6.22.

Lösung 6.40. $f = \{(1,5),(2,2),(3,3),(4,4),(5,1),(6,6)\}$. $\operatorname{rng}(f)$ ist $[6]$.

Lösung 6.41. Es kommt $\{(1,5),(2,2),(3,3),(5,5)\}$ heraus und das ist nicht dasselbe wie $f \circ g$. Wir wussten bereits, dass die Komposition von Relationen nicht kommutativ ist. Wir haben nun gelernt, dass Sie auch dann nicht kommutativ ist, wenn wir nur rechtseindeutige Relationen komponieren.

Lösung 6.42. Wir haben $(f \circ g)(x) = (2^x)^2 = 2^{2x}$ und $(g \circ f) = 2^{x^2}$. (Das ist Potenzrechnung aus der Mittelstufe.) Wir wissen durch Aufgabe 6.41 bereits, dass die beiden Kompositionen nicht gleich sein müssen, aber das heißt nicht, dass sie auf jeden Fall verschieden sind. Und – Achtung! – dass die beiden Rechenvorschriften, die wir erhalten haben, unterschiedlich *aussehen*, bedeutet auch noch nicht zwangsläufig, dass $f \circ g$ und $g \circ f$ nicht gleich sind. (Vielleicht kennt ja jemand eine geschickte Umformung, die aus der einen Rechenvorschrift die andere macht?)

Daher brauchen wir, siehe Aufgabenstellung, ein konkretes Gegenbeispiel; so etwas wie $(f \circ g)(1) = 4$ und $(g \circ f)(1) = 2$.

Übrigens hätten Sie in diesem Fall auch Pech haben und zufällig den „falschen“ Wert einsetzen können: $(f \circ g)(2) = 16 = (g \circ f)(2)$. Ihnen ist natürlich klar, dass das *nicht* bedeutet, dass die beiden Funktionen identisch sind, oder?

Lösung 6.43. Wir bekommen

$$f \circ g : \begin{cases} \mathbb{N} \to \mathbb{N} \\ x \mapsto x \end{cases} \qquad \text{und} \qquad g \circ f : \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N} \\ (x, y) \mapsto (x, x) \end{cases}$$

heraus. $f \circ g$ ist also einfach $\mathrm{id}_{\mathbb{N}}$.

Lösung 6.44. Ein Beispiel wären die durch $f(x) = x$ und $g(x) = x + 1$ auf $\mathbb{R}$ definierten Funktionen.

Lösung 6.45. Definieren wir $f(n) = \lfloor n/2 \rfloor$ und $g(n) = 2n$, dann ergibt sich $\mathrm{id}_{\mathbb{N}}$ als Komposition $f \circ g$. Man erhält also eine injektive Funktion, obwohl f ersichtlich nicht injektiv ist. Das liegt anschaulich formuliert daran, dass g nicht alle natürlichen Zahlen „trifft“: f hat für jede gerade Zahl und die direkt auf sie folgenden denselben Funktionswert. Aber durch den „Umweg“ über g werden in f nur gerade Zahlen eingesetzt.

Dass man für (ii) kein Beispiel finden kann, kann man sich folgendermaßen klarmachen: Ist g nicht injektiv, so gibt es natürliche Zahlen m und n mit $m \neq n$ und $g(m) = g(n)$. Setzt man nun in f ein, dann hat man $f(g(m)) = f(g(n))$.

Lösung 6.46. Ein sehr simples Beispiel wäre $f = \{(1,0),(2,0)\}$ und $g = \{(0,0),(1,0)\}$. Dann ist $f \circ g$ die leere Menge, also injektiv. Falls Ihnen das zu „banal“ ist, dann fügen Sie sowohl zu f als auch zu g noch das Paar $(3,3)$ hinzu. $f \circ g$ wäre dann $\{(3,3)\}$ und nach wie vor injektiv.

Warum widerspricht das nicht Aufgabe 6.45? Dort wurde in der Aufgabenstellung festgelegt, dass der Wertebereich von g eine Teilmenge des Definitionsbereichs von f sein musste. Hier ist es aber so, dass g die Ausgabe 0 liefert, die man gar nicht als Eingabe in f einsetzen kann.

Lösung 6.47. Mit $f(0,0) = 0 = f(0,1)$ sieht man, dass f nicht injektiv ist. Und mit $(g \circ f)(0,0) = (0,0) = (g \circ f)(0,1)$ sieht man, dass $g \circ f$ ebenfalls nicht injektiv ist.[50] Die anderen beiden Funktionen sind offenbar injektiv.

Lösung 6.48. Mit $f(0,0) = 1 = f(1,0)$ sieht man, dass f nicht injektiv ist. Dieses Gegenbeispiel muss dann auch für $g \circ f$ funktionieren:

$$(g \circ f)(0,0) = (0,2) = (g \circ f)(1,0)$$

g ist offensichtlich injektiv. Die Rechenvorschrift für $f \circ g$ ist

$$(f \circ g)(x) = f(g(x)) = f(x-1, x+1) = x + 2$$

[50] Wie in Aufgabe 6.45 folgt die Nicht-Injektivität von $g \circ f$ aus der von f und man kann dieselben Werte einsetzen, um ein Gegenbeispiel zu bekommen.

und das beschreibt sicherlich auch eine injektive Funktion.

Lösung 6.49. Alle vier sind injektiv. Man kommt evtl. bereits durch das Einsetzen von ein paar Werten und „scharfes Hinsehen“ darauf, dass f und g wohl injektiv sind. Man kann das aber auch ausführlich begründen, wenn man sich daran erinnert (siehe Seite 79), dass Injektivität bedeutet, dass man ein Verfahren angeben kann, das zu jeder Ausgabe eindeutig die Eingabe rekonstruieren kann. Für g erhält man die Eingabe zur Ausgabe (u,v) durch $(v-1,u+1)$. Mit anderen Worten: g ist seine eigene Umkehrfunktion. Für f erhält man die Eingabe zur Ausgabe (u,v) durch $((u+v)/2,(u-v)/2)$. (Das läuft auf das aus der Schule bekannte Lösen eines ganz einfachen linearen Gleichungssystems hinaus: $u=x+y$ und $v=x-y$ werden nach x und y aufgelöst.)

Die Funktionen $f\circ g$ und $g\circ g$ müssen dann als Kompositionen injektiver Funktionen zwangsläufig auch injektiv sein. Der Vollständigkeit halber geben wir noch die Rechenvorschrift von $f\circ g$ an:

$$(f\circ g)(x,y)=f(g(x,y))=f(y-1,x+1)=(x+y,y-x-2).$$

Dass $g\circ g=\mathrm{id}_{\mathbb{Z}\times\mathbb{Z}}$ gilt, wurde im letzten Absatz bereits erklärt.

Lösung 6.50. Man erhält Funktionen von $\mathbb{Z}$ nach $\mathbb{R}$ mit den Rechenvorschriften

$$\begin{aligned}(f+g)(n)&=(2n+4)+(4-2n)=8,\\(f-g)(n)&=(2n+4)-(4-2n)=4n \quad \text{und}\\(fg)(n)&=(2n+4)\cdot(4-2n)=16-4n^2.\end{aligned}$$

Dass die zweite injektiv und die erste nicht injektiv ist, ist wohl klar. Bei der dritten kommt ein Quadrat vor. Das sollte Sie auf eine Idee wie $(fg)(1)=12=(fg)(-1)$ führen. fg ist also ebenfalls nicht injektiv.

Lösung 6.51. fg wäre nun injektiv, denn es fehlen die negativen Zahlen. Wie auf Seite 79 wurde die Funktion quasi durch Restriktion injektiv gemacht.

Lösung 6.52. Nach Satz 6.1 ist f^{-1} eine Funktion. Dass f^{-1} injektiv ist, folgt aus der Rechtseindeutigkeit von f. Dass f^{-1} jedes Element von A „trifft“, liegt daran, dass A der Definitionsbereich von f ist.

Warum ist $g\circ f$ injektiv? Sind $x,y\in A$ mit $x\neq y$, dann gilt $f(x)\neq f(y)$, weil f injektiv ist. Daraus folgt $g(f(x))\neq g(f(y))$, weil g injektiv ist. Und warum bildet $g\circ f$ surjektiv auf C ab? Ist c ein beliebiges Element von C, dann gibt es ein $b\in B$ mit $g(b)=c$, weil g surjektiv auf C abbildet. Und es gibt ein $a\in A$ mit $f(a)=b$, weil f surjektiv auf B abbildet. Das macht zusammen $g(f(a))=c$ und wir haben ein Objekt gefunden, das von $g\circ f$ auf c abgebildet wird.

Lösung 6.53. Das wäre entweder $(1/n:n\in\mathbb{N}^+)$ oder $(1/n)_{n\in\mathbb{N}^+}$.

Lösung 6.54. Es reicht offenbar, wenn wir uns auf den Fall beschränken, dass A eine Menge der Form $[n]$ für $n\in\mathbb{N}$ ist. Aus Lemma 6.6 folgt, dass $B^{[n]}$ dieselbe Mächtigkeit wie B^n hat und die kennen wir gemäß Satz 4.6.

Es gilt also allgemein $|B^A|=|B|^{|A|}$ und das rechtfertigt auch die Schreibweise.

Lösung 6.55. Zunächst einmal hat $[2]^{[n]}$ nach Aufgabe 6.54 die Mächtigkeit 2^n und damit nach Satz 3.1 dieselbe Mächtigkeit wie $\mathscr{P}([n])$. Nach Satz 6.3 muss es also eine Bijektion gemäß der Aufgabenstellung geben.

Man erhält diese Funktion, indem man $A \subseteq [n]$ auf die Funktion

$$\chi_A = \{(k,1) : k \in A\} \cup \{(k,2) : k \in [n] \setminus A\}$$

abbildet. Es gilt also $\chi_A(k) = 1$ genau dann, wenn k ein Element von A ist.

charakteristische Funktion

Eine Funktion der Form χ_A bezeichnet man als *charakteristische Funktion* der Menge A. (Typischerweise sind die Funktionswerte dann jedoch nicht 1 und 2, sondern 1 und 0.)

Lösung 7.1. Das hebe ich mir als Cliffhanger auf. Die folgenden Seiten werden hoffentlich klären, was das „Problem“ ist und warum es keinen Grund gibt, sich zu streiten.

Lösung 7.2. Das Potenzieren ist nicht assoziativ, denn $2^{(3^2)} = 2^9 = 512$ ist nicht dasselbe wie $(2^3)^2 = 8^2 = 64$. $\oplus$ ist auch nicht assoziativ, wie man an $(1 \oplus 2) \oplus 3 = 28$ und $1 \oplus (2 \oplus 3) = 26$ sieht. $\otimes$ ist assoziativ:

$$(x \otimes y) \otimes z = (2xy) \otimes z = 4xyz = 2 \cdot x \cdot (2yz) = x \otimes (2yz) = x \otimes (y \otimes z)$$

Division ist nicht assoziativ, weil beispielsweise $1/(2/3) = 3/2$ und $(1/2)/3 = 1/6$ zwei verschiedene Brüche sind. Dass der Durchschnitt von Mengen assoziativ ist, wissen wir schon seit Aufgabe 2.9. Und die Komposition von Funktionen ist ebenfalls assoziativ:

$$((f \circ g) \circ h)(n) = (f \circ g)(h(n)) = f(g(h(n))) = f((g \circ h)(n)) = (f \circ (g \circ h))(n)$$

Lösung 7.3. Wenn im Format *double* (64 Bit) gerechnet wird, kommen zwei unterschiedliche Werte heraus. Man kann daraus schließen, dass in der Fließkommaarithmetik die Addition *nicht* assoziativ ist – nicht nur in PYTHON. Das gilt auch für die Multiplikation und beides dürfte überraschend sein, wenn man zum ersten Mal damit konfrontiert wird. Ausführliche Informationen dazu in den Kapiteln 12 und 13 von *Konkrete Mathematik (nicht nur) für Informatiker*.

Lösung 7.4. Jede Programmiersprache muss sich entscheiden, wie sie mit arithmetischen Ausdrücken umgeht, wenn keine expliziten Klammern gesetzt wurden. PYTHON macht bei identischen Operatoren wie in dieser Aufgabe das, was die meisten machen: Normalerweise werden die Operatoren wie bei der Division von links nach rechts abgearbeitet. Es gibt allerdings Ausnahmen. Die Potenz wird von rechts nach links ausgewertet.

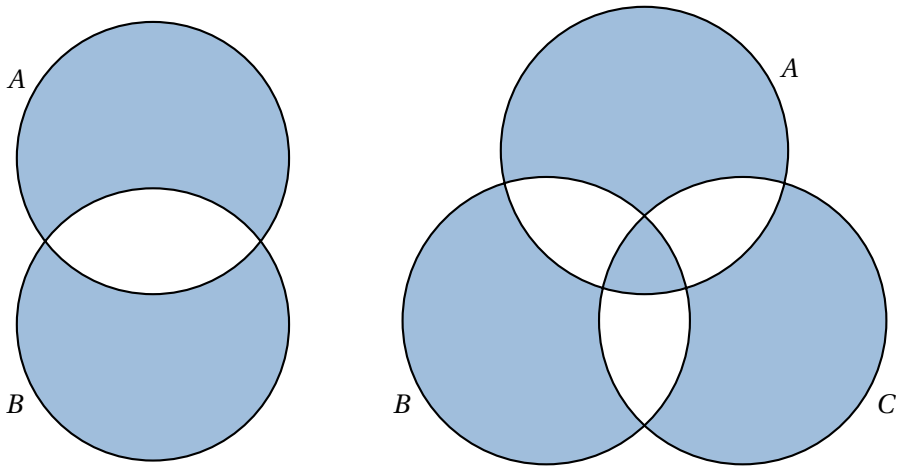
Lösung 7.5. Zunächst ist $\div$ (der sogenannte *Obelus*) ein im deutschen Sprachraum nicht so gebräuchliches Zeichen für Division und vor der Klammer steht implizit ein Multiplikationspunkt (den man oft weglässt). Aus $6 \div 2(1+2)$ wird also $6/2 \cdot (1+2)$. Dann schreibt die Klammer ohne Zweifel vor, dass $1+2$ zuerst berechnet werden muss. Damit sind wir bei $6/2 \cdot 3$ und haben zwei gleichrangige („Punktrechnung“) Operatoren. Wenn wir sie wie üblich als linksassoziativ behandeln, dann

erhalten wir $3 \cdot 3$, also 9. (Bei Rechtsassoziativität würde $6/6 = 1$ herauskommen, aber das widerspricht der gängigen Praxis.)

Unabhängig vom Ergebnis ist das jedoch eine blöde Aufgabe. In einem mathematischen Fachtext würden Sie so etwas nie finden.

Lösung 7.6. Das Potenzieren ist nicht kommutativ, denn $2^3 = 8$ ist nicht dasselbe wie $3^2 = 9$. $\oplus$ ist kommutativ, denn die Multiplikation ist kommutativ und durch Vertauschen von x und y ändert sich nur die Reihenfolge der Faktoren. Auch bei $\otimes$ sieht man (hoffentlich) sofort die Kommutativität. Division ist nicht kommutativ, weil beispielsweise $3/2$ und $2/3$ zwei verschiedene Brüche sind. Dass der Durchschnitt von Mengen kommutativ ist, wissen wir spätestens seit Aufgabe 2.9. Dass die Komposition von Funktionen nicht kommutativ ist, wurde in Aufgabe 6.41 behandelt.

Lösung 7.7. Die symmetrische Differenz für zwei bzw. drei Mengen ist hier dargestellt. Das Nachdenken ist nun allerdings Ihr Job.



Lösung 7.8. Das Potenzieren hat kein neutrales Element. Damit $a^e = a$ für alle a gilt, kommt nur $e = 1$ infrage, aber es gilt nicht immer $1^a = a$. Für $\oplus$ gibt es ebenfalls kein neutrales Element. Wenn man den Ansatz $e \oplus a = a$ nach e auflöst, erhält man einen Ausdruck, in dem a vorkommt. Man braucht aber *ein* Element, das für *alle* a funktioniert. Für $\otimes$ wäre $1/2$ als neutrales Element geeignet. Aber nur dann, wenn $\otimes$ eine Verknüpfung auf $\mathbb{Q}$ wäre! Im Sinne der Aufgabenstellung gibt es *kein* neutrales Element. Für die Division gibt es ebenfalls kein neutrales Element. $a/e = a$ für alle a klappt nur mit $e = 1$, aber $1/a = a$ gilt natürlich nicht immer. Für den Durchschnitt eignet sich als neutrales Element die Menge $\mathbb{N}$, denn es gilt natürlich $M \cap \mathbb{N} = M = \mathbb{N} \cap M$ für alle Teilmengen M von $\mathbb{N}$. Dabei ist aber zu beachten, dass das neutrale Element vom Definitionsbereich der Funktion abhängt. Für die Komposition ist $\mathrm{id}_{\mathbb{N}}$ das neutrale Element. (Siehe auch Satz 6.5.) Auch hier würden wir bei einem anderen Definitionsbereich ein anderes neutrales Element erhalten.

Lösung 7.9. Dann gibt es außer der Eins noch eine weitere Zahl, zu der es ein inverses Element gibt, nämlich -1. Diese Zahl ist auch zu sich selbst invers.

Lösung 7.10. Invers zu $x \in \mathbb{Q}$ ist $\frac{1}{4x}$, wenn x nicht null ist. Für $x = 0$ gibt es kein inverses Element.

Lösung 7.11. Ja, nämlich a. Die Rollen von a und b in der Definition sind offenbar vertauschbar.

Lösung 7.12. Man muss dann immer nur eine der beiden Bedingungen überprüfen. Wenn beispielsweise $e \otimes a$ für alle $a \in M$ gilt, dann gilt wegen der Kommutativität auch automatisch immer $a \otimes e$. (Dass man bei Verknüpfungen, die nicht kommutativ sind, wirklich beide Gleichungen prüfen muss, zeigen die Beispiele in Aufgabe 7.8.)

Lösung 8.1. Alle drei Verknüpfungen sind innere Verknüpfungen, wie man sich leicht überlegt. (Aber Sie haben zumindest darüber nachgedacht, oder?) Keines der Beispiele ist eine Gruppe, das erste und dritte sind jedoch abelsche Monoide:

(i) Die Kommutativität ist offensichtlich. Die Assoziativität sieht man so:

$$(x \otimes y) \otimes z = \sqrt{x^2+y^2} \otimes z = \sqrt{x^2+y^2+z^2}$$
$$x \otimes (y \otimes z) = x \otimes \sqrt{y^2+z^2} = \sqrt{x^2+y^2+z^2}$$

Das neutrale Element ist die Null. Außer der Null hat aber kein Element ein Inverses, denn $x \otimes y$ ist immer positiv, wenn eines der beiden Argumente positiv ist.

(ii) Mit $(3 \otimes 2) \otimes 1 = 7 \otimes 1 = 9$ und $3 \otimes (2 \otimes 1) = 3 \otimes 4 = 11$ sieht man, dass $\otimes$ nicht assoziativ ist. Mit $1 \otimes 2 = 5$ und $2 \otimes 1 = 4$ sieht man, dass $\otimes$ nicht kommutativ ist. Mit dem Ansatz $x = x \otimes e = x + 2e$ folgt, dass als neutrales Element nur 0 infrage käme, aber $0 \otimes y = 2y$ ist im Allgemeinen nicht y. Es gibt somit kein neutrales Element.

(iii) $\otimes$ liefert das Maximum der beiden Argumente. Es ist wohl evident, dass diese Verknüpfung assoziativ und kommutativ und 0 das neutrale Element ist. Eine positive Zahl n kann jedoch kein inverses Element haben, denn $n \otimes m$ ist für alle m immer mindestens so groß wie n.

Lösung 8.2. Die Assoziativität ergibt sich aus der Assoziativität der normalen reellen Addition, die hier absichtlich „umständlich“ aufgeschrieben wird:

$$\begin{aligned}\big((x_1,x_2)\oplus(y_1,y_2)\big)\oplus(z_1,z_2) &= (x_1+y_1,x_2+y_2)\oplus(z_1,z_2)\\ &= \big((x_1+y_1)+z_1,(x_2+y_2)+z_2\big)\\ &= \big(x_1+(y_1+z_1),x_2+(y_2+z_2)\big)\\ &= (x_1,x_2)\oplus(y_1+z_1,y_2+z_2)\\ &= (x_1,x_2)\oplus\big((y_1,y_2)\oplus(z_1,z_2)\big)\end{aligned} \tag{L-1}$$

Das neutrale Element ist $(0,0)$ und invers zu (x_1,x_2) ist $(-x_1,-x_2)$. Die Gruppe ist abelsch. Das liegt an der Kommutativität der reellen Addition und lässt sich auch einfach durch Aufschreiben nachprüfen. (Machen Sie's zur Übung!)

Lösung 8.3. Zunächst einmal haben wir es wirklich mit einer inneren Verknüpfung zu tun, denn für $q_1, q_2 \in M$ gilt $0 \neq |q_1 q_2| = |q_1||q_2| \leq 1 \cdot 1 = 1$ also $q_1 q_2 \in M$.

Dass die Multiplikation assoziativ ist, wissen wir. Und das neutrale Element 1 gehört offenbar zu M. Es handelt sich also um ein Monoid. Um eine Gruppe aber nicht, denn z. B. gehört $1/2$ zu M, aber das inverse Element zu dieser Zahl wäre 2 und diese Zahl gehört nicht zu M.

Lösung 8.4. Die Summe von zwei positiven Zahlen ist zwar wieder eine positive Zahl, aber es gibt für die Addition in dieser Menge kein neutrales Element, denn die Null ist nicht positiv. Bezüglich der Addition erhalten wir also kein Monoid und damit „erst recht“ keine Gruppe, allerdings eine Halbgruppe.

Wenn wir zur Multiplikation übergehen, haben wir es jedoch mit einer Gruppe zu tun, denn das Produkt zweier positiver Zahlen ist positiv und der Kehrwert einer positiven Zahl (das inverse Element) ist ebenfalls positiv. Und die Eins (das neutrale Element) ist auch positiv.

Lösung 8.5. Wir wissen schon (siehe Aufgabe 2.9), dass beide Verknüpfungen assoziativ und kommutativ sind. Das neutrale Element ist im ersten Fall $\emptyset$ und im zweiten $\mathbb{N}$. Wir haben es also auf jeden Fall mit kommutativen Monoiden zu tun. Um Gruppen handelt es sich jedoch nicht. Womit soll man beispielsweise $\{42\}$ vereinigen, damit die leere Menge herauskommt?

Lösung 8.6. Sei $a \in M$ beliebig und b linksinvers zu a. Dazu wähle man ein linksinverses Element c zu b. Dann gilt

$$a \otimes b = e \otimes a \otimes b = c \otimes b \otimes a \otimes b = c \otimes e \otimes b = c \otimes b = e.$$

Im ersten Schritt konnte a durch $e \otimes a$ ersetzt werden, weil e linksneutral ist. Im zweiten Schritt wurde e durch $c \otimes b$ ersetzt, weil c linksinvers zu b ist. Dann wurde $b \otimes a$ durch e ersetzt, weil b linksinvers zu a ist. Und schließlich $e \otimes b$ durch b, weil e linksneutral ist. Auf die Klammerung konnte wegen der Assoziativität durchgehend verzichtet werden. (Und sonst hätte es auch nicht funktioniert.) Gezeigt haben wir damit, dass linksinverse Elemente immer auch *rechtsinvers* sind, dass also $b \otimes a = e$ auch $a \otimes b = e$ impliziert.

rechtsinvers

Damit folgt nun sofort $a \otimes e = a \otimes b \otimes a = e \otimes a = a$: Im ersten Schritt wird e wie oben durch $b \otimes a$ ersetzt, im zweiten $a \otimes b$ durch e, das haben wir gerade hergeleitet. Schließlich wird die Linksneutralität von e ausgenutzt. Insgesamt folgt damit, dass e nicht nur *links*neutral, sondern ein „richtiges“ neutrales Element ist. (Und damit auch *das* neutrale Element, denn jetzt kann man Lemma 7.1 beweisen.)

Lösung 8.7. Nein. Eine der drei Anforderungen an eine Gruppe ist die Existenz eines neutralen Elements. Es muss also mindestens ein Element geben.

Lösung 8.8. Wir nennen das neutrale Element e und greifen uns ein $a \in M$ heraus. Seien b und b' beide invers zu a. Dann gilt

$$b = e \otimes b = (b' \otimes a) \otimes b = b' \otimes (a \otimes b) = b' \otimes e = b', \tag{L-2}$$

also sind b und b' identisch.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 8.9. Von links nach rechts: Weil e das neutrale Element ist, weil b' invers zu a ist, weil $\otimes$ assoziativ ist, weil b invers zu a ist und erneut, weil e das neutrale Element ist.

Lösung 8.10. Zunächst einmal muss man sich klarmachen, dass der Multiplikationspunkt gemäß der Konvention unterschiedliche Dinge bedeutet: in $x_1 \cdot y_1$ „macht“ er im Allgemeinen *nicht* dasselbe wie in $x_n \cdot y_n$, weil einmal die Verknüpfung der Gruppe G_1 und einmal die der Gruppe G_n gemeint ist. Entsprechend ist auch das neutrale Element von G das n-Tupel $(1,\dots,1)$, aber jede der Einsen bedeutet potentiell etwas anderes. Man mag das anfangs verwirrend finden, aber die Alternative – für jede Gruppe ein anderes Symbol wie z. B. $\otimes_i$ – wäre auf die Dauer sehr umständlich. Die Überprüfung der Gruppeneigenschaften läuft nun genau wie in der erwähnten Aufgabe ab. Für die Assoziativität kann man beispielsweise Gleichung (L-1) einfach abschreiben und dabei (x_1, x_2) durch $(x_1,\dots,x_n)$ ersetzen, (y_1, y_2) durch $(y_1,\dots,y_n)$ und so weiter. Die Umformung in der Mitte ist dann erlaubt, weil wir in der i-ten Komponente die Assoziativität der Gruppe G_i verwenden.

Lösung 8.11. Bei dieser Aufgabe geht es eigentlich nur darum, sich durch Hinschreiben zu versichern, dass man die abstrakten Definitionen verstanden hat. Für die Assoziativität greifen wir uns drei Funktion f, g, h von M nach G heraus sowie ein Element m aus M. Dann erhalten wir

$$\big((f\cdot g)\cdot h\big)(m) = (f\cdot g)(m)\cdot h(m) = \big(f(m)\cdot g(m)\big)\cdot h(m) \quad \text{und}$$
$$\big(f\cdot(g\cdot h)\big)(m) = f(m)\cdot(g\cdot h)(m) = f(m)\cdot\big(g(m)\cdot h(m)\big).$$

Dass die beiden Ausdrücke rechts gleich sind, folgt aus der Assoziativität in G. Das neutrale Element von G^M ist die (konstante) Funktion, die jedem $m \in M$ das neutrale Element von G zuordnet.

Wieso ist hier von einer Verallgemeinerung von Aufgabe 8.10 die Rede? Weil man die Funktionen aus G^M als „unendliche Tupel“ betrachten kann. Man kann das sogar noch weiter verallgemeinern, indem die Elemente von M in *unterschiedliche* Gruppen abgebildet werden, aber wir haben noch keine Schreibweise für unendliche Mengenprodukte definiert, also bleibt Ihnen so etwas vorerst erspart.

Lösung 8.12. Nein. Die Assoziativität der Verknüpfung fehlt noch und die kann man leider einer Verknüpfungstabelle nicht so einfach ansehen. Wir müssten das überprüfen, z. B. durch $(aa)a = 1a = a$ und $a(aa) = a1 = a$. (Siehe dazu auch Aufgabe 8.18.) In Aufgabe 8.14 werden wir ein anderes Argument dafür sehen, dass die Verknüpfung assoziativ ist.

Lösung 8.13. Sie muss symmetrisch zur Hauptdiagonalen sein.

Lösung 8.14. Es hätte sein können, dass Ihnen die XOR-Verknüpfung aus der Informatik in den Sinn kommt: Mit 1 für *wahr* und a für *falsch* (oder umgekehrt) wäre die Verknüpfung $(x, y) \mapsto (x \vee y) \wedge \neg(x \wedge y)$.

Man könnte 1 und a aber auch als die ganzen Zahlen 1 und -1 mit der ganz normalen Multiplikation interpretieren.[51] Oder als die Mengen $\emptyset$ und $\{42\}$ mit der symmetrischen Differenz (Aufgabe 7.7) als Verknüpfung.

Eine weitere mögliche Interpretation lernen wir im nächsten Kapitel kennen.

Lösung 8.15. Die Tabelle könnte beispielsweise folgendermaßen entstehen:

$\cdot$	1	a	b
1	1	a	b
a	a		
b	b		

$\cdot$	1	a	b
1	1	a	b
a	a		
b	b	1	

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Zunächst stehen die Zeile und Spalte zum neutralen Element fest. Das ergibt die linke Tabelle. Wegen Korollar 8.3 kann in der zweiten Spalte kein weiteres a mehr vorkommen und in der dritten Zeile kein weiteres b. Also muss dort 1 stehen. Das führt zur mittleren Tabelle. Den Rest kann man ebenfalls mit Korollar 8.3 erledigen. Es ist ein bisschen wie Sudoku …

Welches die inversen Elemente sind, entnimmt man der Tabelle. Und auch, dass die Gruppe abelsch ist. Die Assoziativität ist wieder nicht sofort ersichtlich. Wir glauben das aber an dieser Stelle einfach. Wir werden noch Interpretationen dieser Gruppe sehen, anhand derer die Assoziativität sofort ersichtlich wird. (Nämlich in Aufgabe 13.8.)

Lösung 8.16. Nach Korollar 8.3 muss in jeder Zeile und jeder Spalte der Tabelle jedes Element der Gruppe genau einmal vorkommen. So eine Anordnung nennt man auch lateinisches Quadrat.

lateinisches Quadrat

Lösung 8.17. Wenn a invers zu b ist, dann ist b invers zu a. (Siehe Aufgabe 7.11.) Anders ausgedrückt: wenn $ab = 1$ gilt, dann muss auch $ba = 1$ gelten. Das heißt, dass die Positionen, an denen das neutrale Element in einer Verknüpfungstabelle steht, symmetrisch zur Hauptdiagonalen verteilt sein müssen – und zwar auch dann, wenn die Verknüpfung nicht kommutativ ist.

Lösung 8.18. Wenn Ihr Programm Ausdrücke der Form $(xy)z = x(yz)$ überprüft und für x, y und z alle Werte aus $\{1, a, b\}$ einsetzt, kommt es nach Satz 4.6 auf $3^3 = 27$ Fälle. Man kann sich jedoch dadurch etwas Arbeit sparen, dass man alle Gleichungen, in denen mindestens einmal 1 vorkommt, weglässt, weil die offenbar nicht überprüft werden müssen. Dann verbleiben nur noch $2^3 = 8$ Fälle.

Lösung 8.19. Wir nennen die Abbildungen aus den drei Beispielen f_1 bis f_3. Im ersten Beispiel ist $f_1(a \oplus b)$ immer e und $f_1(a) \otimes f_1(b)$ immer $e \otimes e = e$. Im zweiten Beispiel hat man

$$f_2(a \oplus b) = a \oplus b = a \otimes b = f_2(a) \otimes f_2(b).$$

Und im dritten Beispiel ergibt sich einerseits $f_3(m \oplus n) = f_3(m + n) = 2^{m+n}$ und andererseits $f_3(m) \otimes f_3(n) = 2^m \otimes 2^n = 2^m \cdot 2^n$. Dass das in beiden Fällen dieselbe Zahl ist, wissen Sie sicher noch aus der Schule.

[51] Damit klärt sich dann auch die Frage aus Aufgabe 8.12, ob die Verknüpfung assoziativ ist.

Lösung 8.20. Beispielsweise gilt $f(3 \cdot 1/3) = f(1) = 1$, aber $f(3) \cdot f(1/3) = 3 \cdot 0 = 0$.

Lösung 8.21. Der Wertebereich ist $\mathbb{R}$ und die Verknüpfung muss wegen

$$f\big((x_1, y_1) \oplus (x_2, y_2)\big) = f\big((x_1 + x_2, y_1 + y_2)\big) = x_1 + x_2 = f\big((x_1, y_1)\big) + f\big((x_2, y_2)\big)$$

die normale Addition sein.

Lösung 8.22. Erstens ist $(G, \cdot)$ immer eine Untergruppe von $(G, \cdot)$ und zweitens ist $(\{1\}, \cdot)$ immer eine Untergruppe von $(G, \cdot)$.

Lösung 8.23. Nein, denn $(\mathbb{N}, +)$ ist ja keine Gruppe.

Lösung 8.24. Die Menge der ungeraden ganzen Zahlen kann schon deshalb keine Untergruppe sein, weil das neutrale Element fehlt: die Null ist eine gerade Zahl. Die Menge der geraden Zahlen ist eine Untergruppe, denn die Summe zweier geraden Zahlen ist gerade und das inverse Element einer geraden Zahl ist ebenfalls gerade.

Lösung 8.25. Nein, denn es handelt sich nicht um eine Gruppe. Siehe Aufgabe 8.3.

Lösung 8.26. In Aufgabe 8.4 haben wir eine solche Untergruppe kennengelernt. Eine weitere Möglichkeit wäre $(\mathbb{Q} \setminus \{0\}, \cdot)$. Und eine sehr kleine Untergruppe ist die, die nur aus den Zahlen 1 und -1 besteht.

Lösung 8.27. Es gibt drei, nämlich $\{1, a\}$, $\{1, b\}$ und $\{1, c\}$. Wieso man damit alle „erwischt“ hat, wird demnächst klar werden.

Lösung 8.28. Nach Lemma 8.4 ist 1 ein Element des Kerns K. Ist f injektiv, dann kann K kein weiteres Element enthalten. Das ist schon die eine Richtung der Aussage. Sei nun umgekehrt $\{1\}$ der Kern des Homomorphismus f von G nach H und seien $a, b \in G$ mit $f(a) = f(b)$. Dann gilt

$$1 = f(a)f(a)^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$$

und damit gehört ab^{-1} zum Kern, muss also 1 sein. Multiplikation von $ab^{-1} = 1$ von rechts mit b liefert $a = b$.

Lösung 8.29. Wir schreiben $a \sim b$ für $a^{-1}b$. Wir müssen drei Eigenschaften zeigen:

- Reflexivität: Sei $a \in G$. Dann gilt $a^{-1}a = 1 \in U$ nach Lemma 8.4, also $a \sim a$.
- Symmetrie: Es gelte $a \sim b$, also $a^{-1}b \in U$. Offenbar gilt, ebenfalls nach Lemma 8.4, $b^{-1}a = (a^{-1}b)^{-1} \in U$ und damit $b \sim a$.
- Transitivität: $a \sim b$ und $b \sim c$ bedeutet $a^{-1}b \in U$ und $b^{-1}c \in U$. Das impliziert $a^{-1}c = (a^{-1}b)(b^{-1}c) \in U$, also $a \sim c$, weil U abgeschlossen bezüglich der Gruppenverknüpfung ist.

Lösung 8.30. Ist $[a]_\sim$ die Äquivalenzklasse zu $a \in G$, so gilt $b \in [a]_\sim$ nach Definition genau dann, wenn $a \sim b$, also $a^{-1}b \in U$, gilt. Das ist äquivalent dazu, dass es ein $u \in U$ mit $a^{-1}b = u$ bzw. $b = au$ gibt. Und letzteres ist gleichbedeutend mit $b \in aU$.

Lösung 8.31. Für jede Gruppe G kann man als Isomorphismus von G auf sich selbst natürlich id_G nehmen – eines der trivialen Beispiele, das direkt nach der Definition von Homomorphismen besprochen wurde.

Lösung 8.32. Wir müssen zeigen: Ist G_1 isomorph zu G_2 und G_2 isomorph zu G_3, dann ist G_1 isomorph zu G_3. Sei dazu f_1 ein Isomorphismus von G_1 auf G_2 und f_2 ein Isomorphismus von G_2 auf G_3. Dann ist $f_2 \circ f_1$ zunächst einmal eine Bijektion von G_1 auf G_3. (Siehe Aufgabe 6.52.) Es bleibt zu zeigen, dass diese Komposition auch ein Homomorphismus ist. Das kann man aber einfach durch

$$\begin{aligned}(f_2 \circ f_1)(xy) &= f_2(f_1(xy)) = f_2(f_1(x) \cdot f_1(y)) = f_2(f_1(x)) \cdot f_2(f_1(y)) \\ &= (f_2 \circ f_1)(x) \cdot (f_2 \circ f_1)(y)\end{aligned}$$

nachrechnen.

Lösung 8.33. Nach Lemma 8.4 muss 1 auf 0 abgebildet werden. 1 und a spielen in den jeweiligen Gruppen unterschiedliche Rollen und können einander nicht zugeordnet werden.

Lösung 8.34. Da jeder Automorphismus (nach Lemma 8.4) 1 auf 1 abbilden muss, bleibt nur die Abbildung $\{(1,1),(a,b),(b,a)\}$, die quasi a und b „vertauscht“. Und die tut's auch. Dass das funktioniert, zeigt, dass a und b in dieser Gruppe dieselbe Rolle spielen und man sie mit gruppentheoretischen Mitteln nicht unterscheiden kann.

Lösung 8.35. Im Prinzip kam so eine Abbildung schon in Aufgabe 8.19 vor: Man könnte $x \mapsto 2^x$ nehmen. Aber auch $x \mapsto 3^x$ oder $x \mapsto \mathrm{e}^x$ wären möglich. Es gibt in diesem Fall unendlich viele Isomorphismen zwischen den beiden Gruppen.

Lösung 8.36. Schreiben wir $G = \{1, a, b, c\}$ und $H = \{0, x, y, z\}$. Man könnte alle Bijektionen von G auf H durchprobieren und sich überzeugen, dass keine von denen ein Homomorphismus ist. Das sind jedoch 24 Stück (wieso?) und das wäre ziemlich mühsam. Es geht einfacher: Angenommen, es gäbe einen Isomorphismus f von G auf H. Auf jeden Fall muss $f(1) = 0$ gelten. Für $f(a)$ bleiben damit drei Möglichkeiten: x, y und z. Würde a auf x abgebildet werden, dann hätten wir einerseits $f(a \otimes a) = f(b) \neq 0$, aber andererseits $f(a) \oplus f(a) = x \oplus x = 0$. Das geht also nicht. Probiert man jedoch $f(a) = y$ oder $f(a) = z$, so hat man genau dasselbe Problem. Und das war's schon.

Lösung 9.1. Die Identität auf X.

Lösung 9.2. Das ist die Abbildung von $\mathbb{Z}$ auf $\mathbb{Z}$, die x auf $42 + x$ abbildet.

Lösung 9.3. Da gibt es unendlich viele Möglichkeiten. Ein Beispiel wäre

$$\{(0,42),(42,0)\} \cup \mathrm{id}_{\mathbb{Z}\setminus\{0,42\}}.$$

Ein anderes wäre die Abbildung, die jede gerade Zahl z auf $z+1$ und jede ungerade Zahl z auf $z-1$ abbildet.

Lösung 9.4. Man kann die Elemente direkt der Tabelle aus der Lösung zu Aufgabe 8.15 ablesen. Es sind

$$\begin{aligned}\pi_1 &= \{(1,1),(a,a),(b,b)\}, \\ \pi_a &= \{(1,a),(a,b),(b,1)\} \quad \text{und}\end{aligned}$$

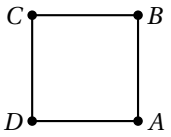
$$\pi_b = \{(1,b),(a,1),(b,a)\}.$$

Man beachte, dass es sechs Permutationen der Menge $\{1,a,b\}$ gibt (siehe Aufgabe 9.7), von denen wir hier nur drei sehen. Wir werden später sehen, dass es nur die *geraden* Permutationen sind.

Lösung 9.5. Die Gruppe besteht aus den vier Drehungen um 0, 90, 180 und 270 Grad. Dabei ist die Drehung um 0 Grad das neutrale Element. Bezeichnet man die Drehung um α Grad als D_α, so ergibt sich die folgende Verknüpfungstabelle:[52]

$\circ$	D_0	D_{90}	D_{180}	D_{270}
D_0	D_0	D_{90}	D_{180}	D_{270}
D_{90}	D_{90}	D_{180}	D_{270}	D_0
D_{180}	D_{180}	D_{270}	D_0	D_{90}
D_{270}	D_{270}	D_0	D_{90}	D_{180}

Bezeichnet man nun die Ecken des Quadrats wie in der folgenden Skizze



und interpretiert man wie üblich Drehungen als Drehungen gegen den Uhrzeigersinn, dann ergeben sich die folgenden Permutationen:

$$\pi_{D_0} = \{(A,A),(B,B),(C,C),(D,D)\}$$
$$\pi_{D_{90}} = \{(A,B),(B,C),(C,D),(D,A)\}$$
$$\pi_{D_{180}} = \{(A,C),(B,D),(C,A),(D,B)\}$$
$$\pi_{D_{270}} = \{(A,D),(B,A),(C,B),(D,C)\}$$

Damit erhält man eine kommutative Untergruppe von $S_{\{A,B,C,D\}}$. Wir werden jedoch noch sehen (Aufgabe 9.12), dass die 24-elementige Gruppe *aller* Permutationen von $\{A,B,C,D\}$ *nicht* kommutativ ist.

Lösung 9.6. Es gibt vier solche Spiegelungen und man erhält insgesamt eine Gruppe mit acht Elementen, die man die *Diedergruppe* D_4 nennt und die nicht mehr abelsch ist. Zur Kontrolle Ihrer Lösung können Sie sich z. B. die entsprechende Wikipedia-Seite anschauen.

Diedergruppe D_4

Lösung 9.7. Nach Satz 4.3 sind es $n!$ Elemente.

Lösung 9.8. Das sieht so aus:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}$$

Lösung 9.9. Man erhält

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad \text{und} \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

[52] Ist Ihnen aufgefallen, dass diese Gruppe isomorph zu einer der beiden aus Aufgabe 8.36 ist?

Sie haben hoffentlich auf die richtige Reihenfolge (erst τ, dann σ) geachtet.

Lösung 9.10. Man muss nur die beiden Zeilen vertauschen.

Lösung 9.11. Zum Beispiel erhält man mit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

die Kompositionen

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \text{und} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

die offensichtlich verschieden sind.

Lösung 9.12. Sei $n > 3$. Für $\rho \in S_3$ setzen wir

$$\rho^* \colon \begin{cases} [n] \to [n] \\ k \mapsto \begin{cases} \rho(k) & k \leq 3 \\ k & k > 3 \end{cases} \end{cases}$$

und erhalten damit eine Permutation, die sich auf $[3]$ wie ρ verhält[53] und ansonsten die Identität ist. Dann bekommt man mit den Bezeichnungen aus Aufgabe 9.11

$$\sigma^*\tau^* = (\sigma\tau)^* \neq (\tau\sigma)^* = \tau^*\sigma^*.$$

Lösung 9.13. Nach Satz 8.2 muss es so eine Permutation geben und dort steht auch, dass man sie (mithilfe von Aufgabe 9.10) durch

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \text{und} \quad \rho = \sigma^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

erhält.

Lösung 9.14. Ja, es handelt sich um (1 3 4 2 5).

Lösung 9.15. $\sigma = (2\,8\,3\,7\,5)$. Sieht Ihre Antwort anders aus? Dann schauen Sie sich Aufgabe 9.16 an.

Lösung 9.16. Nein. Statt (2 8 3 7 5) könnte man z. B. auch (3 7 5 2 8) schreiben.

Lösung 9.17. Auf fünf. Jede der fünf Zahlen kann vorne stehen, aber der Rest folgt dann zwangsläufig.

Lösung 9.18. Ihre Antwort sollte so aussehen:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 6 & 4 & 3 & 1 & 5 \end{pmatrix}$$

[53] Zur Erinnerung: Das heißt $\rho^*|_{[3]} = \rho$.

Lösung 9.19. Die Frage kann man nicht beantworten. Die Zyklenschreibweise ist in dieser Hinsicht mehrdeutig, weil nur die Elemente notiert werden, die durch die Permutation bewegt werden. Der Zyklus aus der Fragestellung könnte Element von S_n für jedes $n \geq 3$ sein.

Lösung 9.20. Gemäß der Definition (mit $m = 1$) handelt es sich um die Identität, die damit auch ein Zyklus ist. Und man könnte sie – für entsprechend großes n – auch als (2) oder (42) schreiben. Wir werden jedoch für die Identität, wenn wir die Zyklenschreibweise verwenden, immer (1) schreiben. In manchen Büchern verwendet man dafür auch (). 0

Lösung 9.21. Man schreibt die Zahlen in der umgekehrten Reihenfolge auf. Für den Zyklus aus Aufgabe 9.15 wäre das z. B. $\sigma^{-1} = (5\ 7\ 3\ 8\ 2)$. Insbesondere sind die inversen Elemente von Zyklen also wieder Zyklen.

Lösung 9.22. Für S_1 bis S_3 ist die Antwort *ja*, weil in diesen drei Fällen *alle* Permutationen Zyklen sind. Ansonsten ist die Antwort aber immer *nein*, weil bereits $(1\ 2)\,(3\ 4)$ kein Zyklus ist.

Lösung 9.23. Die Träger sind $[5]$ und $\{2,3,5,7,8\}$.

Lösung 9.24. Das muss die Identität sein.

Lösung 9.25. So eine Permutation kann es nicht geben. Ist σ eine Permutation und k ein Element ihres Trägers, dann gilt $m = \sigma(k) \neq k$ nach Definition des Trägers. Wäre $\{k\}$ der gesamte Träger, dann hätten wir $m \notin \operatorname{supp}(\sigma)$ und damit $\sigma(m) = m$. Dann wäre σ aber nicht injektiv.

Lösung 9.26. Ist $\{k_1, k_2\}$ der Träger von σ mit $k_1 \neq k_2$, dann muss σ offenbar der Zyklus $(k_1\ k_2)$ sein.

Lösung 9.27. Das würde mit $(1\ 2\ 3)$ und $(1\ 3\ 2)$ klappen. Beachten Sie, dass beide den Träger $\{1,2,3\}$ haben, während der Träger ihres Produkts die leere Menge ist.

Lösung 9.29. Wenn k größer als m ist, dann kann man k als $k = bm + r$ darstellen mit $b, r \in \mathbb{N}$ und $r < m$ darstellen.[54] Dann gilt

$$\sigma^k = \sigma^{bm+r} = \sigma^{bm}\,\sigma^r = \mathrm{id}\,\sigma^r = \sigma^r,$$

d. h., es ist eigentlich nur der Fall $k < m$ interessant. Und für den gilt, dass σ^k in ein Produkt von m/d disjunkten Zyklen zerfällt, wobei d der größte gemeinsame Teiler von k und m ist.

Dazu zwei Beispiele: Ist $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)$, also $m = 10$, dann erhält man $\sigma^6 = (1\ 7\ 3\ 9\ 5)\,(2\ 8\ 4\ 10\ 6)$. Ist $\sigma = (1\ 2\ 3\ 4\ 5)$, also $m = 5$, dann sind σ^2, σ^3 und σ^4 auch Zyklen der Länge 5.

Lösung 9.30. $\sigma = (1\ 8\ 2\ 5)\,(3\ 12\ 10)\,(4\ 7\ 13\ 9\ 6)$.

[54] Das ist die aus der Schule bekannte Division mit Rest, siehe auch Satz 11.2.

Lösung 9.32. Das sieht so aus:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 3 & 8 & 2 & 5 & 7 & 6 & 1 & 11 & 9 & 14 & 10 & 12 & 13 & 15 \end{pmatrix}.$$

Und Sie haben hoffentlich die letzte Spalte mit der Zahl 15 nicht vergessen? Dass die dort stehen muss, geht aus der Aufgabenstellung eindeutig hervor.

Lösung 9.33. In Zweizeilenform ergibt sich

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix},$$

wenn man nicht vergisst, dass man solche Produkte von rechts nach links lesen muss. Zerlegt in Faktoren ist das $\sigma = (1\,5\,4)\,(2\,3)$.

Lösung 9.34. Die Faktoren lassen sich auf 3! verschiedenen Arten anordnen. Für die ersten beiden Faktoren gibt es (siehe Aufgabe 9.17) jeweils vier Arten, sie aufzuschreiben, für den dritten zwei. Das ergibt insgesamt $6 \cdot 4^2 \cdot 2 = 192$ Möglichkeiten.

Lösung 9.35. Man kann die m Zahlen der Trägermenge auf $m!$ Arten geordnet aufschreiben. Nach Aufgabe 9.17 stellen aber jeweils m von diesen Sequenzen denselben Zyklus dar. Damit ergeben sich $m!/m = (m-1)!$ verschiedene Zyklen. Beispielsweise gibt es $3! = 6$ Zyklen mit der Trägermenge $\{1, 7, 23, 42\}$:

$$(1\,7\,23\,42) \quad (1\,7\,42\,23) \quad (1\,23\,7\,42) \quad (1\,23\,42\,7) \quad (1\,42\,7\,23) \quad (1\,42\,23\,7)$$

Lösung 9.36. Wenn Sie die blaue Pille der Mathematik geschluckt haben, dann werden Sie nicken und sagen, dass man sie als Produkt von null Transpositionen darstellen kann. Aber auch ohne diese Sichtweise ist es möglich, denn $(1\,2)\,(1\,2)$ ist ebenfalls die Identität.

Lösung 9.37. $\sigma = (1\,8)\,(8\,2)\,(2\,5)\,(3\,12)\,(12\,10)\,(4\,7)\,(7\,13)\,(13\,9)\,(9\,6)$. Man fängt am besten mit der Darstellung als Produkt von Zyklen an und geht dann wie im Beweis von Lemma 9.5 vor.

Lösung 9.38. Die Lösung von Aufgabe 9.36 liefert die Antwort auf dem Silbertablett. Zu jeder Darstellung kann man „gefahrlos“ $(1\,2)\,(1\,2)$ hinzufügen – und das, sooft man will.

Lösung 9.39. Indem man einfach den Weg für alle Elemente von $[4]$ von rechts nach links verfolgt, kommt man auf die Zweizeilenform

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$

aus der man dann den Zyklus $(1\,2\,4\,3)$ ablesen kann, der wiederum wie im Beweis von Lemma 9.5 zu $(1\,2)\,(2\,4)\,(4\,3)$ wird. Mit etwas Übung kann man sich die Zwischenschritte aber auch sparen.

Lösung 9.40. Wegen Lemma 9.5 reicht es, jede Transposition als Produkt von Nachbartranspositionen darzustellen. Und eine Transposition der Form $(k\ m)$ mit $k < m$ sieht als Produkt von Nachbartranspositionen so aus:

$$(k\ m) = (k\ k+1)\,(k+1\ k+2)\cdots(m-1\ m)\,(m-2\ m-1)\cdots(k\ k+1).$$

Hier noch ein konkretes Beispiel zum Nachrechnen:

$$(2\,7) = (2\,3)\,(3\,4)\,(4\,5)\,(5\,6)\,(6\,7)\,(5\,6)\,(4\,5)\,(3\,4)\,(2\,3).$$

Lösung 9.41. Dafür reicht schon so ein einfaches Beispiel wie $(1\,2\,3)$ in S_3. Weil $[3]$ nur drei Elemente hat, kann es gar nicht zwei paarweise disjunkte Transpositionen geben. Aber mit einer einzigen Transposition, kann man keine Permutationen darstellen, deren Träger ganz $[3]$ ist.

Lösung 9.43. Dem Beweis von Lemma 9.5 entnimmt man, dass man σ als Produkt von fünf Transpositionen schreiben kann. Nach Korollar 9.7 handelt es sich um eine ungerade Permutation. (Vergleichen Sie zur Kontrolle die Anzahl der Fehlstände von σ.)

Lösung 9.44. Eine zu sortierende Liste ist eine Permutation σ der sortierten Liste. Jeder Sortieralgorithmus muss auf die eine oder andere Art σ^{-1} durchführen. Weil Bubblesort das durch eine Abfolge von Transpositionen erledigt, steht vor Beginn des Verfahrens bereits fest, ob eine gerade oder eine ungerade Zahl von Vertauschungen durchgeführt werden muss. Siehe auch Aufgabe 9.40.

Lösung 9.45. Wie wir bereits seit Aufgabe 9.36 wissen, ist jede Transposition zu sich selbst invers, also ist die Antwort

$$\sigma^{-1} = \tau_m^{-1}\tau_{m-1}^{-1}\cdots\tau_2^{-1}\tau_1^{-1} = \tau_m\tau_{m-1}\cdots\tau_2\tau_1.$$

Lösung 9.46. Sind σ und τ Permutationen, die sich als Produkte von m bzw. k Transpositionen darstellen lassen, dann kann man $\sigma\tau^{-1}$ nach Aufgabe 9.45 durch ein Produkt von $m+k$ Transpositionen darstellen. Wenn m und k beide gerade sind, dann ist auch $m+k$ gerade. Mit Korollar 9.7 und Lemma 8.5 folgt, dass es sich bei der Menge der geraden Permutationen um eine Untergruppe handelt.

Ferner wird durch $\sigma \mapsto (1\ 2)\circ\sigma$ eine Funktion definiert, die nach Korollar 8.3 injektiv ist und die offenbar alle geraden Permutationen auf ungerade abbildet und alle ungeraden auf gerade. Deshalb muss es genauso viele gerade wie ungerade Permutationen geben.

Lösung 9.47. Wenn man die Ecken zyklisch mit den Zahlen 1 bis 4 bezeichnet, dann sind die Drehungen um 0, 90, 180 und 270 Grad als Permutationen dieser Ecken die Elemente (1), $(1\,2\,3\,4)$, $(1\,3)\,(4\,2)$ und $(1\,4\,3\,2)$ von S_4. Die Spiegelungen an den Diagonalen sind $(1\,3)$ und $(2\,4)$, die anderen beiden Spiegelungen sind $(1\,4)\,(2\,3)$ und $(1\,2)\,(3\,4)$.

Die beiden Drehungen um 0 und 180 Grad bilden also zusammen mit den beiden letztgenannten Spiegelungen eine Untergruppe, die nur aus geraden Permutationen besteht.

Lösung 10.1. Man muss nur eine der beiden Gleichungen überprüfen. (Siehe auch Aufgabe 7.12.)

unär

Lösung 10.2. In Sprachen mit C-ähnlicher Syntax hat das Minuszeichen meistens zwei Bedeutungen: als *unärer* (einstelliger) Operator in Ausdrücken wie `a=-b` und als zweistelliger Operator in Ausdrücken wie `a=0-b`. Die erste Bedeutung ist also für die Berechnung des inversen Elements gedacht, die zweite für die abgeleitete Operation der Subtraktion. Der dritten möglichen Interpretation des Minuszeichens (als Teil der Zahl) „entledigt“ man sich dadurch, dass man einen Ausdruck wie `-42` nicht als Literal interpretiert, sondern als Anwendung des unären Operators auf das Literal `42`.

In Sprachen mit Lisp-Syntax wird noch deutlicher, dass es eigentlich drei Interpretation gibt. Dort gibt es den zweistelligen Operator, den man `(- 44 2)` schreibt, den unären Operator in der Form `(- 42)` und die *Zahl* `-42`, bei der das Minuszeichen Teil der Objektsyntax ist.

Lösung 10.3. Die dritte Aussage folgt mit $(-a)\cdot(-b) = a\cdot\big(-(-b)\big) = a\cdot b$. Dabei gilt die erste Gleichheit wegen der zweiten Aussage des Lemmas und die zweite nach Aufgabe 7.11. Die siebte Aussage ergibt sich aus

$$\begin{aligned} a-(b-c) &= a+\big(-(b-c)\big) = a+c-b = a+c+(-b) = a+(-b)+c \\ &= (a-b)+c = a-b+c. \end{aligned}$$

Die zweite Gleichheit folgt aus der sechsten Aussage des Lemmas. Die anderen Identitäten sind Konventionen, die Linksassoziativität der „Strichrechnung“ und die Kommutativität der Addition.

Lösung 10.4. Weil die Addition kommutativ ist, die Subtraktion aber nicht. $b-a$ dürfen Sie nicht einfach zu $a-b$ umformen. Wenn Sie aber das Minuszeichen „mitnehmen“, dann dürfen Sie aus $b+(-a)$ durch Vertauschen $(-a)+b$ machen. Und Sie müssen sich z. B. auch nicht zwei binomische Formeln merken, sondern nur eine. Die für $(a-b)^2$ erhalten Sie aus der für $(a+b)^2$, wenn Sie $(-b)$ für b substituieren.

Lösung 10.5. Ja. Nach Aufgabe 8.24 wissen wir bereits, dass wir es mit einer Untergruppe bzgl. der Addition zu tun haben. Nach Lemma 10.3 brauchen wir nur noch, dass das Produkt von geraden Zahlen gerade ist, und das sollte wohl bekannt sein. (Ansonsten werden Fragen zur Teilbarkeit im nächsten Kapitel noch einmal aufgefrischt.)

Man beachte jedoch, dass $\mathbb{Z}$ unitär ist, während die Eins kein Element von $2\mathbb{Z}$ ist. Wenn man nur mit unitären Ringen arbeiten will, dann muss man die Definition des Begriffs *Unterring* entsprechend anpassen und auch Lemma 10.3 ändert sich dadurch.

Lösung 10.6. Der Beweis ist nicht schwer. Nach den Lemmata 8.5 und 10.3 muss man lediglich zeigen, dass Differenzen und Produkte von Polynomen wieder Polynome sind. Für Polynome aus $\mathbb{R}[x]$ kennen Sie das aus der Schule und für beliebige

Ringe ändert sich im Prinzip nichts. Nur die abstrakte Schreibweise erfordert evtl. etwas Denkarbeit.

Seien p und q die durch

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \quad \text{und}$$
$$q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k$$

definierten Polynome. Dann ergibt sich

$$(p-q)(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m \quad \text{und}$$
$$(p \cdot q)(x) = d_0 + d_1 x + d_2 x^2 + \ldots d_{k+n} x^{k+n}$$

mit $m = \max\{k, n\}$,

$$c_i = \begin{cases} a_i - b_i & i \le k \wedge i \le n \\ a_i & k < i \le n \\ -b_i & n < i \le k \end{cases}$$

und

$$d_i = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_{i-1} b_1 + a_i b_0.$$

Entscheidend ist, dass alle c_i und d_i natürlich wieder Elemente von R und $p - q$ und $p \cdot q$ deshalb wieder Polynome über R sind. (Man muss lediglich beachten, dass $p - q$ nicht notwendig ein Polynom vom Grad m ist, weil c_m verschwindet, wenn $n = k$ und $a_n = b_k$ gilt. Ebenso können auch c_{m-1} und weitere Koeffizienten verschwinden.)

Lösung 10.7. Zwei. Er muss die Null als neutrales Element der Addition enthalten und die Eins als neutrales Element der Multiplikation. Da die Eins nach Definition in $R \setminus \{0\}$ liegt, kann nicht $0 = 1$ gelten. Dass es einen Körper mit nur zwei Elementen tatsächlich gibt, werden wir demnächst sehen.

Lösung 10.8. Nein, z. B. ist das Paar $(1, 0)$ in diesem Ring nicht die Null, hat aber offenbar kein inverses Element bzgl. der Multiplikation. (Zur Erinnerung: $(1, 1)$ ist die Eins in diesem unitären Ring.)

Lösung 10.9. Dass $(\mathbb{C}, +)$ eine abelsche Gruppe ist, wissen wir bereits. Dass die Multiplikation eine innere Verknüpfung ist, ist offensichtlich. Wir müssen zunächst Assoziativität und Kommutativität der Multiplikationüberprüfen. Das geschieht durch einfaches Einsetzen in die Definition:

$$\begin{aligned} \big((a,b)\cdot(c,d)\big)\cdot(e,f) &= (ac-bd, ad+bc)\cdot(e,f) \\ &= \big((ac-bd)e-(ad+bc)f, (ac-bd)f+(ad+bc)e\big) \\ &= (ace-bde-adf-bcf, acf-bdf+ade+bce) \\ (a,b)\cdot\big((c,d)\cdot(e,f)\big) &= (a,b)\cdot(ce-df, cf+de) \\ &= \big(a(ce-df)-b(cf+de), a(cf+de)+b(ce-df)\big) \end{aligned}$$

$$= (ace - adf - bcf - bde, acf + ade + bce - bdf)$$
$$(a,b)\cdot(c,d) = (ac - bd, ad + bc)$$
$$(c,d)\cdot(a,b) = (ca - db, da + cb)$$

Und auch die Distributivität ist unproblematisch:[55]

$$\begin{aligned}(a,b)\cdot\big((c,d)+(e,f)\big) &= (a,b)\cdot(c+e,d+f)\\ &= \big(a(c+e)-b(d+f), a(d+f)+b(c+e)\big)\\ &= (ac+ae-bd-bf, ad+af+bc+be)\\ (a,b)\cdot(c,d)+(a,b)\cdot(e,f) &= (ac-bd, ad+bc)+(ae-bf, af+be)\\ &= (ac-bd+ae-bf, ad+bc+af+be)\end{aligned}$$

Man rechnet ebenfalls leicht nach, dass $(1,0)$ das neutrale Element der Multiplikation ist. Lediglich beim Kehrwert muss man etwas nachdenken. Ist (a,b) ein Element von $\mathbb{C}\setminus\{(0,0)\}$, dann ist sein Kehrwert $\big(a/(a^2+b^2), -b/(a^2+b^2)\big)$. Überzeugen Sie sich, dass das tatsächlich stimmt!

Lösung 10.10. Nein, z. B. hat das Polynom x kein inverses Element bzgl. der Multiplikation. Die Eins ist das (konstante) Polynom $x^0 = 1$ vom Grad 0, aber wenn man x mit einem anderen Polynom multipliziert, das nicht gerade die Null ist, dann hat das Produkt immer mindestens den Grad 1.

Lösung 10.11. Die ersten beiden Aussagen (zwei der sogenannten *binomischen Formeln*) gelten in jedem Körper (sogar in jedem Ring) und folgen aus der Distributivität: man muss einfach ausmultiplizieren. Allerdings kann man für $ab+ab$ im Allgemeinen nicht $2ab$ schreiben, weil es ein Objekt namens „2“ vielleicht gar nicht gibt. (Und es gibt tatsächlich Körper, in denen $ab+ab$ verschwindet, z. B. den Restklassenkörper $\mathbb{Z}_2$, den wir bald kennenlernen.) Zur „fehlenden“ zweiten binomischen Formel siehe Aufgabe 10.4.

Die dritte Aussage ergibt in beliebigen Körpern keinen Sinn, weil dort nicht klar ist, was das Zeichen $\geq$ bedeuten soll. Solche Körper lernen wir im nächsten Kapitel kennen und im Vorgriff sei bereits erwähnt, dass die dritte Aussage auch im Körper der komplexen Zahlen nicht sinnvoll ist.

Lösung 11.1. Das Minimum ist $42\cdot 0 = 0$. Alle anderen Elemente der Menge sind größer als diese Zahl. Ein Maximum existiert natürlich nicht, weil zu jedem Element $42n$ der Menge das noch größere Element $42(n+1)$ existiert.

Lösung 11.2. Wenn es so eine Folge gäbe, dann wäre $A = \{a_n : n \in \mathbb{N}\}$ eine nichtleere Teilmenge von $\mathbb{N}$ ohne Minimum. Denn das Minimum von A müsste ja eine der Zahlen a_n sein, aber nach Aufgabenstellung wäre a_{n+1} noch kleiner und ebenfalls ein Element von A.

Lösung 11.3. Wenn man eine endliche Menge von reellen Zahlen hat, dann kann man Schritt für Schritt ein Element der Menge entfernen und dieses zum provisorischen Kandidaten für das Minimum deklarieren. Wenn das nächste entfernte

[55] Man beachte, dass man wegen der Kommutativität der Multiplikation nur eine der beiden Bedingungen für die Distributivität überprüfen muss.

Element kleiner ist, wird es zum neuen Kandidaten, ansonsten bleibt es beim alten Kandidaten. Da die Anzahl der verbleibenden Elemente abnimmt, bilden die Mächtigkeiten der „Restmengen“ eine Folge von immer kleiner werdenden natürlichen Zahlen, die nach Aufgabe 11.2 irgendwann abbricht. Der letzte Kandidat ist das Minimum. (Und für Maxima macht man das natürlich analog.)

Aufgaben wie diese zeigen nebenbei, dass solche scheinbar „esoterischen“ mathematischen Themen durchaus Relevanz für die Praxis der Informatik haben. Man muss dort nämlich häufig begründen, warum ein Algorithmus funktioniert. Dazu gehört auch der Nachweis, dass das Verfahren *terminiert*, also irgendwann aufhört. Ein Beispiel für so einen Nachweis haben Sie gerade gesehen, denn im Prinzip wurde ein „Programm“ beschrieben, dass das Minimum einer Menge ermittelt.

Lösung 11.4. Weil die Mächtigkeiten der Restmengen dann keine natürlichen Zahlen sind.

Lösung 11.5. Im Beweis von Satz 9.4 wurde argumentiert, dass die Reste immer kleiner werden und dass das irgendwann aufhören muss. Wenn Ihnen das beim aufmerksamen Lesen nicht aufgefallen ist, dann zeigt das, dass diese Aussage über natürliche Zahlen recht „natürlich“ zu sein scheint.

Lösung 11.7. Wenn Sie mit dem besagten Modell z. B. 424 242 mod 17 berechnen wollen, dann tippen Sie erst die Zahl 424 242 ein, dann die Taste $\boxed{a\ b/c}$, dann die Zahl 17 und anschließend das Gleichheitszeichen. Ihnen ist hoffentlich klar, wie das angezeigte Ergebnis zu interpretieren ist.

Bei größeren Zahlen wie 42 424 242 klappt das allerdings evtl. nicht mehr. Da bleibt Ihnen bei primitiven Rechnern nichts anderes übrig, als erst zu dividieren und dann das Produkt aus dem Divisor und dem ganzzahligen Anteil des Quotienten vom Dividenden abzuziehen. Im konkreten Fall also erst 42 424 242 $\boxed{\div}$ 17 und dann 42 424 242 $\boxed{-}$ 2 495 543 $\boxed{\times}$ 17. (Der Taschenrechner beherrscht zum Glück die Regel "Punkt- vor Strichrechnung".)

Lösung 11.8. Weil der Ausdruck a mod m nicht definiert ist, wenn m null ist. In diesem Sinne ist auch die Division keine innere Verknüpfung auf $\mathbb{R}$ (allerdings eine auf $\mathbb{R} \setminus \{0\}$).

Lösung 11.9. Für $m > 0$ ergibt sich k durch $\lfloor a/m \rfloor$. Wenn man eine Formel haben will, die auch für negative Werte von m funktioniert, muss man den etwas komplizierteren Ausdruck $k = \operatorname{sgn}(m) \cdot \lfloor a/|m| \rfloor$ verwenden. Dabei ist sgn die Vorzeichenfunktion, die wir offiziell auf Seite 165 einführen und die man für $m \neq 0$ auch durch $m/|m|$ ersetzen kann.

Lösung 11.10. Nein. Die Aufzählung 1, -1, a und $-a$ der trivialen Teiler könnte einen zu dieser Aussage verleiten. Aber die Zahlen 1 und -1 bilden eine Ausnahme, weil in diesen beiden Fällen $\{1, -1\} = \{a, -a\}$ gilt, es also nur zwei (triviale) Teiler gibt.

Lösung 11.11. Hier geht es natürlich darum, sich die Definition genau anzuschauen. Kann man eine entsprechende Zahl k finden? Die Antwort auf die erste Frage

ist *ja*, denn man kann $k = 0$ wählen. *Jede* Zahl ist also Teiler der Null. Die Antwort auf die zweite Frage ist jedoch *nein*, denn für jede Zahl k gilt $k \cdot 0 = 0$, da kommt also nie 7 heraus. Null teilt nur sich selbst und keine andere Zahl.

Lösung 11.12. Weil wir das Dezimalsystem verwenden, kann man eine durch 10 teilbare Zahl daran erkennen, ob die letzte Ziffer eine Null ist. Weil 2 und 5 Teiler von 10 sind, erkennt man Teilbarkeit durch 2 bzw. 5 daran, ob die letzte Ziffer durch 2 bzw. 5 teilbar ist. Weil 4 ein Teiler von 100 ist, erkennt man Teilbarkeit durch 4 daran, ob die letzten beiden Ziffern eine durch 4 teilbare Zahl darstellen: 7324 ist z. B. durch 4 teilbar, weil 24 durch 4 teilbar ist. Ebenso ist eine Zahl genau dann durch 8 teilbar, wenn die letzten drei Ziffern eine durch 8 teilbare Zahl darstellen.

Eine Zahl ist genau dann durch 3 bzw. 9 teilbar, wenn ihre (iterierte) Quersumme (siehe Aufgabe 5.16) durch 3 bzw. 9 teilbar ist. Warum das so ist, werden wir später klären. Eine Zahl ist durch 6 teilbar, wenn sie durch 2 und durch 3 teilbar ist. Auch für die Zahlen 7 und 11 gibt es Teilbarkeitsregeln. Die sind aber etwas komplizierter und werden ebenfalls erst später besprochen.

Siehe dazu auch das Vorkurs-Video "Teilbarkeit, Teilen mit Rest".

Lösung 11.13. Man nennt eine Zahl *gerade*, wenn sie durch 2 teilbar ist. Dazu gehören also Zahlen wie 2, 42 oder -18. Man nennt eine Zahl *ungerade*, wenn sie *nicht* gerade ist. Die Menge der geraden Zahlen ist also $\{2n : n \in \mathbb{Z}\}$ und die Menge der ungeraden Zahlen ist $\{2n+1 : n \in \mathbb{Z}\}$, weil bei Division durch 2 außer 0 und 1 kein anderer Rest auftreten kann.

Die Frage steht insbesondere deshalb an dieser Stelle, weil immer mal wieder gefragt wird, ob die Null eine gerade Zahl sei. Ja, ist sie. Siehe auch Aufgabe 11.11.

Lösung 11.14. Da kommt auch in allen drei Fällen 5 heraus. Das Vorzeichen spielt keine Rolle, weil der größte gemeinsame Teiler auf jeden Fall mindestens 1 ist, wenn nicht beide Zahlen null sind.

Lösung 11.15. In beiden Fällen ist das Ergebnis 42. Allgemein folgt aus der Definition sofort $\operatorname{ggT}(a,a) = \operatorname{ggT}(0,a) = |a|$. (Erinnern Sie sich an Aufgabe 11.11.)

Lösung 11.18. Nein. Wenn $d = xa + yb$ gilt, dann kann man zur rechten Seite „gefahrlos“ $ba - ab = 0$ addieren. Das ergibt $d = (x+b)a + (y-a)b$. Und das kann man auch mehrfach oder alternativ mit vertauschten Rollen $(ab - ba)$ machen. Es gibt also unendlich viele Möglichkeiten.

Im konkreten Beispiel hat $25 = -5a + 9b$ funktioniert, aber

$$25 = (-5+225)a + (9-400)b = 220a - 391b$$

tut es z. B. auch. Rechnen Sie nach!

Lösung 11.19. Man muss dafür im Wesentlichen nur einen Schritt modifizieren:

(i) Setze `A` und `B` auf die Werte a und b.

(ii) Gilt `A` $\cdot$ `B` $= 0$, dann ist das Ergebnis das Maximum von `A` und `B` und der Algorithmus ist beendet.

(iii) Ist `A` > `B`, dann ersetze `A` durch `A` mod `B`, anderenfalls `B` durch `B` mod `A`.

(iv) Fahre fort mit Schritt (ii).

Die entscheidende Änderung ist, dass statt der Differenz der Rest berechnet wird. Damit bei dieser Rechnung nicht versehentlich durch null dividiert wird, sieht der Test in Schritt (ii) nun etwas anders aus. (`A`·`B` ist null, wenn mindestens einer der beiden Faktoren null ist.)

Ob diese Version schneller als das Original ist, wenn man sie auf einem Computer implementiert, ist übrigens gar nicht so leicht zu beantworten. Erstens kann je nach Prozessor die Division (also mod) zeitaufwendiger als die Subtraktion sein und zweitens spart man nicht in jedem Fall Schleifendurchläufe. Probieren Sie es z. B. mal mit 1008 und 623 und Sie werden sehen, dass man mit der Subtraktionsvariante nicht mehr Arbeit hat als mit der neuen.

Lösung 11.20. Wenn k ein gemeinsamer Teiler von a und b ist, dann teilt er nach Lemma 11.4 auch $xa+yb$, also 1. Da 1 aber nur die Teiler 1 und -1 hat, kommen als gemeinsame Teiler von a und b nur 1 und -1 infrage.

Lösung 11.21. Wenn man die Gleichung etwas umstellt, dann sieht sie so aus:

$$x!y! - x! - y! = 2 \tag{L-3}$$

Wenn $x \le y$ gilt, dann sind alle drei Terme auf der linken Seite von (L-3) durch $x!$ teilbar, also ist die ganze linke Seite durch $x!$ teilbar und damit muss auch 2 durch $x!$ teilbar sein. Das geht aber nur, wenn $x! = 1$ oder $x! = 2$ gilt. Setzt man diese beiden Werte in (L-3) ein, so erhält man $y! - 1 - y! = 2$ (also $-1 = 2$) für $x! = 1$ und $2y! - 2 - y! = 2$ (also $y! = 4$) für $x! = 2$. Beides ist nicht möglich.

Wenn hingegen *nicht* $x \le y$ gilt, so gilt $y < x$ und man kann genau wie eben argumentieren, wenn man die Rollen von x und y vertauscht. Es gibt also keine ganzen Zahlen, die die Gleichung erfüllen.

Lösung 11.22. Eine ausführliche Lösung gibt es in dem Video *Die Superzahl*.

Lösung 12.1. Ich hatte an $\mathbb{N} \setminus (\mathbb{P} \cup \{0,1\})$ gedacht.

Lösung 12.2. Wenn p Teiler von a_n ist, dann gilt die Aussage. Ist p jedoch *nicht* Teiler von a_n, dann sind p und a_n nach der Bemerkung vor dem Korollar teilerfremd. Nach Lemma 11.8 (mit $a = p$, $b = p_n$ und $c = a_1 \cdots a_{n-1}$) folgt $p | a_1 \cdots a_{n-1}$. Nun können wir dieselbe Argumentation mit a_{n-1} statt a_n wiederholen und nach und nach die Faktoren entfernen, die teilerfremd zu p sind. Irgendwann finden wir ein Vielfaches von p, spätestens dann, wenn wir bei a_1 angelangt sind.

Lösung 12.3. Wenn man geduldig weitermacht (oder einen Computer die Arbeit machen lässt), kommt man auf $1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30031 = 59 \cdot 509$.

Lösung 12.4. Jedem Gegenbeispiel der Form (12.1) ordnen wir die Zahl $m+n$ zu. Wenn es Gegenbeispiele gäbe, dann erhielte man damit eine nichtleere Menge von natürlichen Zahlen, die ein kleinstes Element haben muss.

Lösung 12.7. Sinnvollerweise probieren Sie der Reihe nach zuerst die kleinsten Primzahlen durch. Teilweise kann man das (siehe Aufgabe 11.12) schon direkt sehen. Da 32 892 eine gerade Zahl ist, teilen Sie also durch 2 und erhalten 16 446. Dabei ist zu beachten, dass ein Primfaktor mehrfach vorkommen kann: Im konkreten Fall können wir erneut durch 2 dividieren und erhalten 8 223. Diese Zahl ist durch 3 teilbar und wir erhalten 2 741. Das ist eine Primzahl und die Antwort wäre $32\,892 = 2^2 \cdot 3 \cdot 2\,741$ gewesen.

Lösung 12.8. Eine Zahl p ist nach Definition prim, wenn Sie sich durch keine positive Zahl (außer 1) teilen lässt, die kleiner als p ist. Wir müssen aber nicht *alle* Zahlen durchprobieren, die zwischen 1 und p liegen. Erstens müssen wir wegen der Transitivität der Teilbarkeitsrelation nur durch Primzahlen teilen. Zweitens, und das ist der eigentliche „Shortcut“, müssen wir nicht durch Zahlen teilen, die größer als $\sqrt{p}$ sind! Warum? Wenn p keine Primzahl ist, dann gibt es Zahlen q_1 und q_2, die beide kleiner als p sind und für die $q_1 q_2 = p$ gilt. Wären die beide größer als $\sqrt{p}$, dann wäre ihr Produkt größer als $\sqrt{p} \cdot \sqrt{p} = p$. Das kann nicht sein, also ist mindestens eine der beiden Zahlen höchstens so groß wie $\sqrt{p}$ und das gilt „erst recht“ für die Primteiler dieser Zahl.

Im konkreten Fall können Sie also Ihren Taschenrechner $\sqrt{2741} \approx 52.3546$ berechnen lassen und wissen, dass Sie nur durch die 15 Primzahlen von 2 bis 47 teilen müssen. Die nächste Primzahl, 53, ist bereits zu groß.

Lösung 12.9. Nennen wir die zwei Zahlen a und b und ihren größten gemeinsamen Teiler d. Ist p eine beliebige Primzahl, die in den Primfaktorzerlegungen der beiden Zahlen in den Potenzen p^k bzw. p^n vorkommt, dann ist p^m mit $m = \min\{k, n\}$ offenbar ein Teiler von a und von b und damit nach Korollar 11.6 ein Teiler von d. Andererseits kann p^{m+1} sicher *kein* Teiler von d sein, denn sonst wäre es auch ein Teiler von a und b (und dann wäre p^{k+1} ein Teiler von a oder p^{n+1} ein Teiler von b). Damit ergibt sich die Primfaktorzerlegung von d: Sie besteht aus allen Primzahlen, die Teiler sowohl von a als auch von b sind, und die zugehörige Potenz ist jeweils das Minimum der entsprechenden Potenzen für a und b.

Konkretes Beispiel: 1008 ist $2^4 \cdot 3^2 \cdot 7$ und 1080 ist $2^3 \cdot 3^3 \cdot 5$. Die Primzahlen, die in beiden Zerlegungen vorkommen, sind 2 und 3. Die kleinste Potenz für 2 ist 3, die kleinste für 3 ist 2. Daher muss nach den Überlegungen aus dem letzten Absatz $2^3 \cdot 3^2 = 72$ der größte gemeinsame Teiler von 1008 und 1080 sein. Und das stimmt natürlich.

Lösung 12.11. Wenn man ein paar Fälle durchgerechnet und sich ggf. auch noch die zugehörigen Primfaktorzerlegungen angeschaut hat, sollte man darauf kommen, dass immer

$$ab = \mathrm{ggT}(a,b)\,\mathrm{kgV}(a,b)$$

gilt. Das kleinste gemeinsame Vielfache erhält man aus den Primfaktorzerlegungen von a und b, indem man quasi das Vorgehen aus Aufgabe 12.9 „umkehrt“: Man braucht von allen Paaren von Primzahlpotenzen jeweils die mit dem höheren Exponenten.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Fortetzung des konkreten Beispiels aus der erwähnten Aufgabe: kgV(1008, 1080) ist $15120 = 2^4 \cdot 3^3 \cdot 5 \cdot 7$. Und $72 \cdot 15120$ ist dasselbe wie $1008 \cdot 1080$.

Lösung 13.1. Bei Division durch $n = 6$ gibt es die sechs möglichen Reste 0 bis 5. Die Faktormenge ist also

$$\mathbb{Z}/6\mathbb{Z} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}.$$

$[0]_6$ ist die Menge aller ganzen Zahlen, die durch 6 teilbar sind. Dazu gehören neben null z. B. 6, 12 und 600, aber auch negative Zahlen wie -6 oder -66. Es gilt also $[0]_6 = [6]_6$ und $[0]_6 = [12]_6$ und so weiter. $[1]_6$ enthält alle Zahlen, die bei Division durch 6 den Rest 1 haben. Das sind außer der Eins u. a. 7, 13, 61 und negative Zahlen wie -5 oder -59. Alle sechs Äquivalenzklassen enthalten unendlich viele ganze Zahlen.

Lösung 13.2. Wenn Sie sich nur einfach diesen Lösungshinweis anschauen, ohne selbst nachgedacht zu haben, dann kann ich Ihnen auch nicht helfen. So werden Sie's jedenfalls nicht lernen …

$[3]_7$ ist die Menge $\{7n+3 : n \in \mathbb{Z}\} = \{\ldots, -18, -11, -4, 3, 10, 17, 24, \ldots\}$. $\mathbb{Z}/7\mathbb{Z}$ ist die Menge, deren Elemente die sieben Mengen $[0]_7$ bis $[6]_7$ sind. Der Zusammenhang ist, dass $\mathbb{Z}/7\mathbb{Z}$ die Faktormenge zu einer bestimmten Äquivalenzrelation (Kongruenz modulo 7) ist und $[3]_7$ eine der Äquivalenzklassen, aus denen diese Faktormenge besteht.

Wenn man $[3]_7$ und $[7]_3$ als Mengen betrachtet, dann haben sie gemeinsame Elemente, z. B. die Zahl 10. Damit beschäftigen wir uns später. Wie ich am Anfang des Abschnitts sagte, werden wir jedoch meistens nur mit einem festen n arbeiten, also wird für uns z. B. $[7]_3$ keine Rolle spielen, solange wir uns nur mit $\mathbb{Z}/7\mathbb{Z}$ beschäftigen.[56]

$[424242]_{11} = [424341]_{11}$ ist eine andere Formulierung dafür, dass 424242 und 424341 kongruent modulo 11 sind. Dass das stimmt, kann man entweder dadurch bestätigen, dass man beide Zahlen durch 11 teilt und feststellt, dass man denselben Rest (in diesem Fall 5) erhält, oder dadurch, dass man die beiden Zahlen subtrahiert und feststellt, dass ihre Differenz (in diesem Fall 99) durch 11 teilbar ist. Die erste Methode ist das Vorgehen direkt nach der Definition der Kongruenz, die zweite basiert auf Lemma 13.1.

Lösung 13.3. a/b ist im Allgemeinen keine ganze Zahl und der Ausdruck $[a/b]_n$ wäre dann gar nicht definiert. Erinnern Sie sich an das, was im letzten Kapitel über die „vier Grundrechenarten" gesagt wurde.

Lösung 13.4. Die Ergebnisse für die Beispiele aus Aufgabenstellung sind

$$[8]_{11} + [5]_{11} = [13]_{11} = [2]_{11},$$
$$[4]_{12} - [7]_{12} = [-3]_{12} = [9]_{12},$$

[56] Es gibt subtile Zusammenhänge zwischen verschiedenen Restklassenringen, aber so weit werden wir nicht in die Zahlentheorie vordringen.

$$[4]_{12} + [-7]_{12} = [-3]_{12} = [9]_{12} \text{ und}$$
$$[10]_{15} \cdot [6]_{15} = [60]_{15} = [0]_{15}.$$

Sie sollten vielleicht vorsichtshalber noch weitere Beispiele durchrechnen. Wie Sie Ihre Ergebnisse überprüfen können, sollten Sie auf den letzten Seiten gelernt haben.

Lösung 13.5. Gar nichts. Jedenfalls haben wir so einen Ausdruck nicht definiert. Die Definition gilt nur für die Addition, Subtraktion und Multiplikation von Restklassen zum *selben n*.

Lösung 13.6. Brüche können auf viele verschiedene Arten dargestellt werden. Die Rechenregeln für Brüche müssen so definiert sein, dass unabhängig von der Darstellung immer dasselbe herauskommt. Beispielsweise ist das Produkt zweier Brüche bekanntlich ein Bruch, dessen Zähler das Produkt der Zähler der Faktoren und dessen Nenner das Produkt der Nenner der Faktoren ist. Also gilt $\frac{3}{4} \cdot \frac{5}{7} = \frac{15}{28}$. Aber statt $\frac{3}{4}$ kann man auch $\frac{9}{12}$ schreiben und statt $\frac{5}{7}$ auch $\frac{10}{14}$. Multipliziert man die beiden, dann erhält man $\frac{90}{168}$. Kürzen zeigt, dass dies tatsächlich nur eine andere Darstellung von $\frac{15}{28}$ ist. Aber haben Sie sich bisher schon einmal Gedanken darüber gemacht, dass und warum das klappt?

Lösung 13.7. Beispielsweise gilt die Kommutativität der Addition in $\mathbb{Z}/n\mathbb{Z}$ wegen

$$[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n,$$

wobei die beiden äußeren Gleichheitszeichen nur die Anwendung der Definition sind, während die Gleichheit in der Mitte gilt, weil die Addition von ganzen Zahlen kommutativ ist.

Lösung 13.8. Der Isomorphismus ist $\{(1,[0]_3),(a,[1]_3),(b,[2]_3)\}$. Man muss nun nur noch nachrechnen, dass es sich wirklich um einen handelt. Damit ist dann auch die offene Frage geklärt, ob die in Aufgabe 8.15 durch eine Tabelle eingeführte Verknüpfung assoziativ ist.

Lösung 13.9. Die linke. Der Isomorphismus ist $\{(1,[0]_4),(a,[1]_4),(b,[2]_4),(c,[3]_4)\}$.

Lösung 13.10. In $\mathbb{Z}/11\mathbb{Z}$ ergibt sich $10+9=8$, $3-8=6$ und $6\cdot 6=3$. In $\mathbb{Z}/12\mathbb{Z}$ erhalten wir $10+9=7$, $3-8=7$ und $6\cdot 6=0$.

Lösung 13.11. Die beiden Antworten sind 6 und 13.

Lösung 13.12. Für den Datentyp `int` wurden 32 Bit verwendet und deshalb wird modulo 2^{32} gerechnet. Rechnen Sie es nach!

Der arithmetische Überlauf, der hier beschrieben wird, tritt in PYTHON oder COMMON LISP übrigens nicht ein, weil dort mit Langzahlarithmetik gerechnet wird.

Lösung 13.13. In 13! kommen die Faktoren 2, 5, und 10 vor, also kann man 13! durch 100 teilen. Darum muss als Ergebnis eine Zahl herauskommen, die in der Dezimaldarstellung am Ende zwei Nullen hat.

Lösung 13.14. Alle Zahlen der Form $10^k - 1$ für natürliche Zahlen k sind offenbar durch 9 (und damit auch durch 3) teilbar. Es ergibt sich

$$\begin{aligned}[7164]_9 &= [7\cdot 10^3 + 1\cdot 10^2 + 6\cdot 10^1 + 4\cdot 10^0]_9\\ &= [7]_9\cdot[10^3]_9 + [1]_9\cdot[10^2]_9 + [6]_9\cdot[10^1]_9 + [4]_9\cdot[10^0]_9\\ &= [7]_9\cdot[1]_9 + [1]_9\cdot[1]_9 + [6]_9\cdot[1]_9 + [4]_9\cdot[1]_9\\ &= [7]_9 + [1]_9 + [6]_9 + [4]_9 = [7+1+6+4]_9\end{aligned}$$

und damit haben 7164 und die Quersumme von 7164 denselben Rest bei Division durch 9. Ersetzt man 9 durch 3, sieht die Rechnung genauso aus.

Lösung 13.15. Wenn man sich die geraden und die ungeraden Potenzen von zehn separat anschaut, so ergibt sich modulo 11 ein einfaches Muster, weil die Gleichung $10^2 = 100 = 9\cdot 11 + 1$ gilt:

$$\begin{aligned}[10^2]_{11} &= [1]_{11}\\ [10^{2n}]_{11} &= [(10^2)^n]_{11} = \left([10^2]_{11}\right)^n = \left([1]_{11}\right)^n = [1]_{11}\\ [10^{2n+1}]_{11} &= \left([10^2]_{11}\right)^n\cdot[10]_{11} = [1]_{11}\cdot[10]_{11} = [10]_{11} = [-1]_{11}\end{aligned}$$

Lösung 13.16. Nennen wir die Zahl, die wir untersuchen wollen, m. Durch das Abtrennen der letzten Ziffer zerlegen wir diese Zahl in der Form $m = 10a + b$ und berechnen dann $a - 2b$. Ist nun $a - 2b$ durch 7 teilbar, so findet man eine Zahl k mit $a - 2b = 7k$. Multiplikation mit 10 liefert $10a - 20b = 70k$ bzw. (nach Addition von $21b$ auf beiden Seiten) die Darstellung $m = 10a + b = 70k + 21b$. Rechts steht jetzt eine Linearkombination der Zahlen 70 und 21, die beide durch 7 teilbar sind. Also ist die linke Seite, m, nach Lemma 11.4 auch durch 7 teilbar.

Ist umgekehrt m durch 7 teilbar, so findet man ein k mit $7k = m = 10a + b$ bzw. $b = 7k - 10a$. Damit folgt $a - 2b = a - 2\cdot(7k - 10a) = 21a - 14k$ und wir haben $a - 2b$ als Linearkombination zweier Vielfacher von 7 dargestellt.

Lösung 13.17. Die Kommutativität ist gleichbedeutend damit, dass die beiden Tabellen symmetrisch zur Hauptdiagonalen sind. In der Zeile und Spalte zur Null in der linken Tabelle werden einfach die Werte aus der Zeile darüber bzw. der Spalte links daneben wiederholt, weil die Null das neutrale Element der Addition ist. Analog gilt das für die Zeile und Spalte zur Eins in der rechten Tabelle. Zusätzlich sieht man rechts noch, dass nach Lemma 10.1 in jedem Ring die Multiplikation mit null natürlich immer das Ergebnis null liefert. Die erste Zeile und Spalte der Multiplikationstabelle können wir uns in Zukunft auch sparen.

Lösung 13.18. Man könnte eine Zeile hinzufügen:

−	0	5	4	3	2	1
+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Das ist so zu lesen, dass beispielsweise Addition von 2 dasselbe wie Subtraktion von 4 ist, denn es gilt ja $[2]_6 = [-4]_6$. Die Werte in der neuen Zeile ergaben sich dadurch, dass man die Werte direkt darunter von 6 subtrahiert.

Lösung 13.19. Will man z. B. $x + 4 = 1$ lösen, dann sucht man in der Spalte mit der Überschrift 4 nach der Zahl 1. Weil man die in der Zeile zur 3 findet, ist $x = 3$ die Lösung. Das wird immer klappen, weil die Additionstabelle bekanntlich ein lateinisches Quadrat ist – siehe Aufgabe 8.16.

Lösung 13.21. Das erste Ergebnis ist 142. Im zweiten Fall kommt 8 heraus. Bei so kleinen Zahlen wie 13 geht es evtl. schneller, wenn man einfach die möglichen Fälle im Kopf durchprobiert. Es kommen ja nur die elf Zahlen von 2 bis 12 infrage.

Lösung 13.23. Nach der Konvention für Körper ist $4/5$ lediglich eine Abkürzung für $4 \cdot 1/5$ und damit nach Aufgabe 13.21 für $4 \cdot 8$, also für 6.

Lösung 13.24. Modulo 13 erhalten wir $4^2 = 3$ und $4^3 = 3 \cdot 4 = -1$. Damit folgt

$$4^{100} = 4^{99} \cdot 4 = \left(4^3\right)^{33} \cdot 4 = (-1)^{33} \cdot 4 = -4 = 9.$$

Dabei haben wir ausgenutzt, dass in jedem Ring $(-1)^k = 1$ für gerade Exponenten k und $(-1)^k = -1$ für ungerade k gilt. Das folgt nach Punkt (iii) von Lemma 10.2.

Lösung 13.25. Gemäß unserer Konvention sind Exponenten wie 100 keine Elemente von $\mathbb{Z}_{13}$ sondern natürliche Zahlen, die angeben, wie oft multipliziert wird. 100-mal multiplizieren ist nicht dasselbe wie 9-mal multiplizieren.

Lösung 13.26. Zunächst einmal kann man $a = 1$ für jedes n als Beispiel nehmen. Aber so ein Beispiel würde man sicher als trivial bezeichnen. Durch Probieren erhält man interessantere Beispiele wie $a = 8$ und $n = 9$.

Lösung 13.27. Die Gleichung $a^{p-1} = 1$ kann man auch als $a \cdot a^{p-2} = 1$ hinschreiben und erkennt, dass a^{p-2} der Kehrwert von a ist.

Daraus folgt übrigens auch, dass die Umkehrung des kleinen Satzes von Fermat gilt: Wenn in einem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ für *alle* Elemente a außer 0 die Gleichung $a^{n-1} = 1$ gilt, dann handelt es sich um einen Körper (und n ist eine Primzahl). Man vergleiche diese Aussage mit Aufgabe 13.26.

Lösung 14.1. Wir brauchen zunächst eine Lösung x_1 der ersten Kongruenz, die ein Vielfaches von $5 \cdot 7 = 35$ ist. Wir suchen also eine Zahl k_1 mit $[35k_1]_3 = [1]_3$. Da wir hier modulo 3 rechnen, können wir 35 durch 2 ersetzen und stattdessen $[2k_1]_3 = [1]_3$ lösen. Im allgemeinen Fall (z. B. in einem Programm) würden wir wie im Absatz hinter Satz 13.4 diese Gleichung mit dem erweiterten euklidischen Algorithmus lösen. Im konkreten Fall bietet sich jedoch simples Probieren an, weil für k_1 nur die Zahlen 0, 1 und 2 infrage kommen. $k_1 = 2$ tut es[57] und liefert uns $x_1 = 35 \cdot 2 = 70$. (In diesem Schritt rechnen wir nicht mehr modulo 3 und müssen mit 35 statt mit 2 multiplizieren.)

[57] Beachten Sie, dass der Beweis des chinesischen Restsatzes eine Garantie dafür liefert, dass sich unter diesen drei Kandidaten eine Lösung befindet.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Für die beiden anderen Kongruenzen sind die jeweiligen Ansätze $[21k_2]_5 = [2]_5$ und $[15k_3]_7 = [4]_7$ bzw. vereinfacht $[k_2]_5 = [2]_5$ sowie $[k_3]_7 = [4]_7$. Damit erhalten wir $k_2 = 2$, $k_3 = 4$, $x_2 = 21 \cdot 2 = 42$ und $x_3 = 15 \cdot 4 = 60$ und schließlich die Lösung $x = 70 + 42 + 60 = 172$.

Lösung 14.3. Aus dem Beweis kann man folgern, dass sich aus einer Lösung eine andere ergibt, wenn man das Produkt $m_1 \cdots m_n$ addiert oder subtrahiert. In Aufgabe 14.1 ist beispielsweise $172 - 3 \cdot 5 \cdot 7 = 67$ auch eine Lösung und 277 und -38 sind es auch. Es gibt also offensichtlich immer unendlich viele Lösungen und damit gibt es zum Beispiel auch eine eindeutig bestimmte kleinste Lösung, die nichtnegativ ist.

Lösung 14.4. Es ist einfach, ein unlösbares Kongruenzsystem anzugeben, wenn die Moduln identisch sind:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 3 \end{aligned}$$

Aber das wäre geschummelt. Hier ist ein Beispiel mit verschiedenen Moduln:

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 2 \pmod 6 \end{aligned}$$

Jedes x, das die erste Kongruenz löst, ist offenbar ungerade. Jedes x, das die zweite Kongruenz löst, ist gerade. Daher kann kein x beide Kongruenzen lösen.

Lösung 14.5. Gilt $[x]_{15} = [y]_{15}$, so ist $x - y$ nach Lemma 13.1 ein Vielfaches von 15 und damit auch ein Vielfaches von 3 und 5. Nach demselben Lemma folgt daher $[x]_3 = [y]_3$ und $[x]_5 = [y]_5$. Das ist die Wohldefiniertheit.

Der zweite Punkt folgt aus der Definition des Rechnens mit Restklassen (■) sowie aus der Definition der Verknüpfungen in direkten Produkten (□):

$$\begin{aligned} f([x]_{15} + [y]_{15}) &\overset{■}{=} f([x+y]_{15}) = ([x+y]_3, [x+y]_5) \overset{■}{=} ([x]_3 + [y]_3, [x]_5 + [y]_5) \\ &\overset{□}{=} ([x]_3, [x]_5) + ([y]_3, [y]_5) = f([x]_{15}) + f([y]_{15}) \end{aligned}$$

Für die Multiplikation sieht die Begründung genauso aus.

Gilt $f([x]_{15}) = ([x]_3, [x]_5) = ([y]_3, [y]_5) = f([y]_{15})$, also $[x]_3 = [y]_3$ und $[x]_5 = [y]_5$, so ist nach Lemma 13.1 $x - y$ durch 3 und 5 teilbar. Also ist $x - y$ durch 15 teilbar und damit folgt mit demselben Lemma $[x]_{15} = [y]_{15}$. Also ist f injektiv.

Ist schließlich $([a]_3, [b]_5)$ ein beliebiges Element von $\mathbb{Z}_3 \times \mathbb{Z}_5$, so gibt es nach dem chinesischen Restsatz eine Zahl $x \in \mathbb{N}$ mit $x \equiv a \pmod 3$ und $x \equiv b \pmod 5$. Für diese Zahl gilt natürlich $f([x]_{15}) = ([a]_3, [b]_5)$. f ist somit auch surjektiv.

Beachten Sie, dass bei dieser Lösung lediglich verwendet wurde, dass 3 und 5 teilerfremd sind. Die Aussage gilt also beispielsweise auch, wenn wir $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}_3$ und $\mathbb{Z}_5$ durch $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ ersetzen.

Lösung 15.1. Wir nennen die Relationen von links nach rechts R_1 bis R_3. Alle drei Relationen sind offensichtlich reflexiv auf $[4]$, wie man an der Hauptdiagonale der Tabelle unschwer erkennen kann. Dass R_2 und R_3 transitiv sind, ist trivial. R_1 ist hingegen nicht transitiv, weil zwar $1R_13$ und $3R_12$ gilt, aber nicht $1R_12$. R_2 ist offensichtlich total. R_1 ist auch total, man muss das aber etwas mühsamer durch Inspektion der Tabelle nachprüfen. R_3 ist nicht total, denn es gilt z. B. weder $1R_32$ noch $2R_31$. R_1 und R_3 sind antisymmetrisch. In R_3 gibt es gar kein Paar $(a,b) \in R_3$ mit $a \neq b$. R_1 ist so gebaut, dass für $a,b \in [4]$ mit $a \neq b$ immer nur entweder (a,b) oder (b,a) in der Relation enthalten ist. R_2 ist nicht antisymmetrisch, denn wir haben beispielsweise $(1,2) \in R_2$ und $(2,1) \in R_2$, aber natürlich $1 \neq 2$.

Vergleichen Sie die Ergebnisse mit denen von Aufgabe 5.12.

Lösung 15.2. Zum Glück haben Sie damals im ersten Semester Aufgabe 2.9 bearbeitet. Daher gibt es nun fast nichts mehr zu tun, weil sie nach den Punkten (i), (iii) und (iv) jener Aufgabe bereits wissen, dass $\subseteq$ reflexiv, transitiv und antisymmetrisch ist. Wir haben es also tatsächlich mit einer Halbordnung zu tun. Allerdings im Allgemeinen nicht mit einer linearen Ordnung, denn für $A = \{0,1\}$ gilt z. B. weder $\{0\} \subseteq \{1\}$, noch $\{1\} \subseteq \{0\}$. Eine lineare Ordnung erhalten wir nur für den Extremfall, dass $|A| \leq 1$ gilt.

Lösung 15.3. Nach Lemma 11.3 ist T transitiv und natürlich ist T auch reflexiv auf $\mathbb{N}^+$, weil jede Zahl sich selbst teilt. Und wenn m ein Teiler von n ist, dann gilt sicher $m \leq n$. Teilt dann umgekehrt n auch noch m, dann kann nur $m = n$ gelten. Das ist die Antisymmetrie. Damit haben wir eine Halbordnung. Aber eine lineare Ordnung ist es nicht, weil beispielsweise 3 kein Teiler von 5 und 5 kein Teiler von 3 ist.

Lösung 15.4. Transitivität und Reflexivität haben wir in diesem Fall auch, aber es fehlt die Antisymmetrie: 42 und -42 teilen sich beispielsweise gegenseitig, sind aber deswegen noch nicht gleich.

Lösung 15.5. Man könnte es z. B. so machen:

	1	2	3
1			×
2	×		
3	×		

Nennen wir diese Relation R, dann haben wir $2R1$, aber nicht $1R2$, also ist R nicht symmetrisch. Andererseits haben wir $3R1$ und $1R3$, obwohl $1 \neq 3$ gilt, also ist R auch nicht antisymmetrisch.

Lösung 15.6. Die naheliegende Antwort ist die Relation $\subset$. Falls Sie das Zeichen zwischendurch vergessen haben, weil es in diesem Skript nicht oft vorkommt, dann erinnern Sie sich vielleicht, dass es einen Index mathematischer Symbole zum Nachschlagen gibt.

Lösung 15.7. Das kann man ganz einfach mit der folgenden Relation R erledigen:

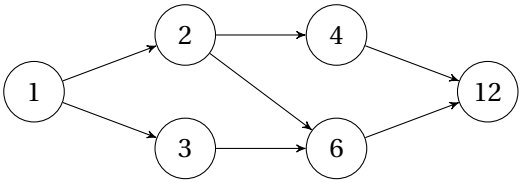
	1	2
1	×	
2		

Wegen $1R1$ ist die Relation nicht irreflexiv auf $[2]$. Aber reflexiv ist sie dort auch nicht, denn $2R2$ gilt nicht.

Lösung 15.8. Würde aRa für ein $a \in A$ gelten, dann wäre das ein direkter Widerspruch zur Asymmetrie (und zwar mit $b = a$). Auch die Antisymmetrie ist trivial, denn die Voraussetzung $aRb \wedge bRa$ derselben kann bei asymmetrischen Relationen gar nicht eintreten.

Die Antwort auf die letzte Frage ist nein. Siehe dazu das Beispiel in der Lösung von Aufgabe 15.5.

Lösung 15.9. Das sollte so aussehen:



Lösung 15.10. Die noch fehlenden Punkte:

(i) Aus $a \prec b$ folgt $a \preceq b$ und damit $a + c \preceq b + c$ nach **GK1**. $a + c = b + c$ kann aber nicht gelten, denn sonst könnte man auf beiden Seiten c subtrahieren und $a = b$ folgern.

(ii) Mit **GK2** folgt aus den Voraussetzungen zunächst $0 \preceq ab$. Wegen Lemma 10.4 ist $0 = ab$ jedoch in diesem Fall nicht möglich.

(vi) Das folgt aus (v) mit $1 \cdot 1 = 1$ und wegen $1 \neq 0$ (siehe Aufgabe 10.7).

(vii) Das folgt aus (i), indem man auf beiden Seiten $-a$ bzw. a addiert.

(viii) Mit (vii) hat man zunächst $0 \prec b - a$, mit (ii) dann $0 \prec (b-a)c = bc - ac$ und erneut mit (vii) $ac \prec bc$.

(ix) Man kann wie in (viii) argumentieren, aber nach (iii) c durch $-c$ ersetzen und die Rechengesetze aus Lemma 10.2 anwenden.

(x) Das folgt direkt aus (viii).

(xi) Das folgt ebenfalls direkt aus (viii).

(xii) Die Richtung „von rechts nach links“ folgt aus (ii) sowie (iii) zusammen mit $(-a)(-b) = ab$ nach Lemma 10.2. Gilt hingegen weder $0 \prec a \wedge 0 \prec b$ noch $a \prec 0 \wedge b \prec 0$, dann ist entweder a oder b null und damit ab auch null, oder wir haben o. B. d. A. $0 \prec a$ und $b \prec 0$ und damit $0 \prec -b$, also $0 \prec -ab$ nach Lemma 10.2 und (ii), also $ab \prec 0$ nach (iii), in beiden Fällen jedenfalls *nicht* $0 \prec ab$.

(xiii) Aus $1/a \prec 0$ würde mit (ix) $1 = a \cdot (1/a) \prec 0 \cdot (1/a) = 0$ im Widerspruch zu (vi) folgen.

(xiv) Das folgt aus (x) und (xiii).

(xv) Das folgt aus (viii), indem man $a \prec b$ auf beiden Seiten mit $1/(ab)$ multipliziert.

Lösung 15.11. Dass $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ gilt, ist klar. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ folgt, weil man in der Definition $b = 0$ wählen kann und so alle rationalen Zahlen erhält. Wählt man $a = 0$ und $b = 1$, dann erhält man $\sqrt{2}$. Und weil diese Zahl nicht rational ist (siehe Aufgabe 2.4), ist $\mathbb{Q}$ sogar eine echte Teilmenge von $\mathbb{Q}(\sqrt{2})$.

Weil wir innerhalb der reellen Zahlen bleiben und glauben, dass $\mathbb{R}$ ein angeordneter Körper ist (dazu später mehr), fallen uns die meisten Eigenschaften, die wir überprüfen müssen, in den Schoß – z. B. Kommutativität, Assoziativität, Distributivität, **GK1** und **GK2**. Dass 0 und 1 Elemente von $\mathbb{Q}(\sqrt{2})$ sind, sollte klar sein. Wir müssen nur noch (mit Lemma 8.5) zeigen, dass $\mathbb{Q}(\sqrt{2})$ abgeschlossen bzgl. Subtraktion und $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ abgeschlossen bzgl. Division ist. Dass die Differenz zweier Elemente von $\mathbb{Q}(\sqrt{2})$ wieder ein Element von $\mathbb{Q}(\sqrt{2})$ ist trivial. (Rechnen Sie es nach!) Bei der Division kann man das leicht überprüfen, wenn man die richtige Idee hat:

$$\begin{aligned}\frac{a+b\sqrt{2}}{c+d\sqrt{2}} &= \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \cdot \frac{c-d\sqrt{2}}{c-d\sqrt{2}} = \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2} \\ &= \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2} \cdot \sqrt{2}\end{aligned}$$

Die Zahlen am Ende sind offensichtlich wieder rational. Dabei muss man nur darauf achten, dass $c - d\sqrt{2}$ nicht null sein darf. Das ergibt aber durch Umformung $c/d = \sqrt{2}$, wenn d nicht null ist, und ist daher unmöglich (denn sonst wäre $\sqrt{2}$ rational). Wenn d hingegen verschwindet, dann muss auch c verschwinden und $c + d\sqrt{2}$ ist null: wir hätten gar nicht erst dividieren dürfen.

Es fehlt nur noch der Beweis dafür, dass das Beispiel nicht trivial und $\mathbb{Q}(\sqrt{2})$ nicht ganz $\mathbb{R}$ ist. Dafür zeigen wir, dass $\sqrt{3}$ kein Element von $\mathbb{Q}(\sqrt{2})$ ist: Sonst hätten wir $a+b\sqrt{2} = \sqrt{3}$ und durch Quadrieren beider Seiten ergäbe sich $a^2+2ab\sqrt{2}+2b^2 = 3$ bzw. nach Umformen $\sqrt{2} = (3-a^2-2b^2)/(2ab)$. Dann stünde jedoch rechts eine rationale Zahl und wir hätten einen Widerspruch.

Lösung 15.12. Sie haben sich natürlich erinnert, dass auf Seite 125 bereits ein solches Beispiel zu finden ist.

Lösung 15.13. Zum Beispiel $B = \{\{1,2\},\{3,4\}\}$. Es gibt viele Möglichkeiten.

Lösung 15.14. Wenn m_1 und m_2 Maximum der Menge A sind, dann gilt $m_1 \preceq m_2$, weil m_1 Element von A und m_2 Maximum von A. Vertauscht man die Rollen, dann erhält man $m_2 \preceq m_1$. Wegen der Antisymmetrie folgt $m_1 = m_2$.

Lösung 15.15. $\{B_1, B_2, B_3\}$ hat als obere Schranke auf jeden Fall $B_1 \cup B_2 \cup B_3$. Beachten Sie aber, dass das nicht mehr notwendig funktioniert, wenn die beteiligten Mengen nicht alle endlich sind, beispielsweise mit $B_1 = \{0\}$, $B_2 = \{1\}$ und $B_3 = \mathbb{N} \setminus \{0,1\}$. Da haben Sie auch gleich eine nach oben unbeschränkte Menge.

Lösung 15.16. In beiden Fällen ist das die Zahl 2.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 15.17. Das gilt für $\{2,3\}$ und für $\{1,2,3\}$. Beide haben 4 und 5 als obere Schranken, aber die Menge $\{4,5\}$ hat kein Minimum.

Lösung 16.1. Die meisten Aussagen über Suprema oder Maxima haben ein entsprechendes Pendant, das man erhält, indem man stattdessen die „entgegengesetzten" Begriffe (Infimum statt Supremum, $>$ statt $<$ und so weiter) verwendet. In der Regel beweist man das wie hier durch einen Vorzeichenwechsel.

Ist M so eine Menge und u eine untere Schranke, dann ist $-u$ eine obere Schranke von $M' = \{-m : m \in M\}$. M' muss also ein Supremum s haben und $-s$ ist dann das gesuchte Infimum von M.

Lösung 16.2. Sind a und b rationale Zahlen mit $ab = 2$, dann sind a und b verschieden, weil 2 nicht das Quadrat einer rationalen Zahl ist. O. B. d. A. gelte $0 < a < b$. Für die Zahl $c = (a+b)/2$ gilt $a < c < b$ und weil ihr Produkt mit $d = 4/(a+b)$ ebenfalls 2 ist, muss d auch zwischen a und b liegen. (Aus $d \leq a$ folgt $cd < ba = 2$ und aus $b \leq d$ folgt $cd > ab = 2$.)

Angenommen, die rationale Zahl q ist das Supremum von C. Ist q das Maximum von C, dann gilt $q^2 < 2$. Mit $r = 2/q$ gilt dann $rq = 2$ und damit $r > q$. Nach unserer Vorüberlegung gibt es rationale Zahlen q_1 und r_1 mit $q < q_1 < r_1 < r$ und $q_1 r_1 = 2$ und damit $q_1^2 < 2$ bzw. $q_1 \in C$. Dann war q aber nicht das Maximum. Es mus also $q^2 > 2$ gelten. Wie eben findet man dann aber mit $r = 2/q$ rationale Zahlen q_2 und r_2 mit $r < r_2 < q_2 < q$. Weil daraus $q_2^2 > 2$ folgt, ist q_2 eine obere Schranke von C. Das widerspricht der Tatsache, dass q das Supremum von C, also die *kleinste* obere Schranke von C, sein soll.

Lösung 16.3. Für die erste „Regel" kann man $x = y = 2/3$ nehmen, für die zweite $x = y = 3/2$. Aber es gibt selbstverständlich unendlich viele Gegenbeispiele.

Lösung 16.4. Für $x \geq 0$ gilt $|x| = x$. Dass dann $|x| < \varepsilon$ aus $-\varepsilon < x < \varepsilon$ folgt, ist klar. Gilt umgekehrt $|x| < \varepsilon$, dann ergibt sich daraus $-\varepsilon < x < \varepsilon$, weil natürlich $-\varepsilon < 0$ gilt.

Für $x < 0$ gilt $|x| = -x$. $|x| < \varepsilon$ bedeutet dann $-x < \varepsilon$ und damit $-\varepsilon < x$. $x < \varepsilon$ ist wegen $\varepsilon > 0$ klar. Gilt umgekehrt $-\varepsilon < x < \varepsilon$, dann ergibt Multiplikation mit -1 die Ungleichung $\varepsilon > -x > -\varepsilon$ und damit insbesondere $\varepsilon > |x|$.

Lösung 16.5. Für $x \geq 0$ gilt $-|x| = -x \leq x = |x|$. Und für den Fall $x < 0$ hat man $-|x| = x \leq -x = |x|$. Dass im ersten Fall $-x \leq x$ und im zweiten $x \leq -x$ gilt, beweist man mit der „Allzweckwaffe" Lemma 15.3.

Lösung 16.6. Wie wäre es mit $x = 1$ und $y = -1$?

Lösung 16.7. Wäre $q + r$ rational, dann müsste $(q + r) - q$ als Differenz zweier rationaler Zahlen ebenfalls rational sein. Das ist aber r. Für das Produkt argumentiert man analog mit $r = (qr)/q$.

Nebenbei sei angemerkt, dass auch $-r$ irrational sein muss. Das liegt daran, dass $\mathbb{Q}$ ein Körper ist: Wäre $-r$ rational, so wäre r als additiv inverses Element von $-r$ ebenfalls rational. Ebenso ist $1/r$ irrational, wenn $r \neq 0$ gilt.

Lösung 16.8. Man kann z. B. $\sqrt{2}$ und $-\sqrt{2}$ nehmen. Die Summe ist 0 und das Produkt -2.

Lösung 16.9. I ist nach Definition ein Intervall, wenn die Aussage

$$\forall r_1, r_2 \in I \, \forall x \in \mathbb{R} \, (r_1 < x < r_2 \Rightarrow x \in I)$$

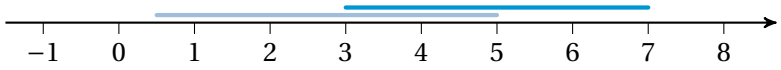
wahr ist. Für unechte Intervalle ist der linke Teil der Implikation aber immer falsch, weil diese Menge gar keine zwei Elemente r_1 und r_2 mit der Eigenschaft $r_1 < r_2$ enthalten. Daher ist, wie wir bereits im allerersten Abschnitt gelernt haben, die Aussage immer wahr.

Lösung 16.10. Die leere Menge kann man beispielsweise als $[1,0]$ oder als $[42,42)$ schreiben. Singletons bekommen die Form $[x,x]$.

Lösung 16.11. Hoffentlich haben Sie nicht gedacht, dass diese Menge fünf Elemente hat. In Lemma 16.12 steht ja auch explizit, dass alle echten Intervalle unendlich viele Elemente haben. Ich habe diese Aufgabe nur aufgenommen, weil es eine offenbar unausrottbare Fehlinterpration gibt, nach der manche Studierende eine Menge wie $[1,5]$ als die Menge der *ganzen* Zahlen zwischen 1 und 5 interpretieren. Das ist aber schlicht und einfach falsch und widerspricht der Definition, in der explizit steht, dass $[1,5]$ die Menge aller *reellen* Zahlen zwischen 1 und 5 ist!

Nebenbei bemerkt hat die Intervallschreibweise nichts mit der Notation $[n]$ zu tun, die in Abschnitt 4 eingeführt wurde. Bei Intervallen stehen zwischen den Klammern immer *zwei* Zahlen, die durch ein Komma getrennt sind.

Lösung 16.12. Grundsätzlich kann es für solche Fragen hilfreich sein, sich die beteiligten Intervalle als Abschnitte der Zahlengeraden zu skizzieren, z. B. so:



Der Durchschnitt ist dann sofort erkennbar. Lediglich bei den Intervallgrenzen muss man explizit prüfen, ob sie in der Schnittmenge liegen oder nicht. Die Ergebnisse in diesem Fall sind in dieser Reihenfolge $(3,5)$, $[3,5]$, $(3,7]$, $[3,3] = \{3\}$ und $[3,3) = \emptyset$.

Lösung 16.13. Die Vereinigung von $A = [1/3,42)$ und $[42,43)$ ist das Intervall $[1/3,43)$. Die Vereinigung von A und $(42,43)$ ist kein Intervall, weil die Zahl 42 „fehlt“ und damit für eine Lücke sorgt.

Lösung 16.14. Nein. $[0,3] \setminus [1,2]$ ist beispielsweise kein Intervall. Und diese Menge lässt sich auch nicht „kürzer“ schreiben, lediglich anders, etwa als $[0,1) \cup (2,3]$.

Lösung 16.15. Die Paare sind $A = (-2,2) = H$, $B = \mathbb{R} = G$, $C = E$, $D = \emptyset = I$ und $F = J$.

Lösung 16.16. $[40,42] \setminus [40,41)$ ist das Intervall $[41,42]$. $[40,41] \setminus \mathbb{N}$ ist das Intervall $(40,41)$. $[40,42] \setminus [40,42)$ ist das Intervall $\{42\}$, das aber kein *echtes* Intervall ist. $[40,41] \setminus \mathbb{Q}$ ist kein Intervall, denn diese Menge hat unendlich viele „Lücken“. (Nach Lemma 16.10 befinden sich zwischen 40 und 41 unendlich viele rationale Zahlen,

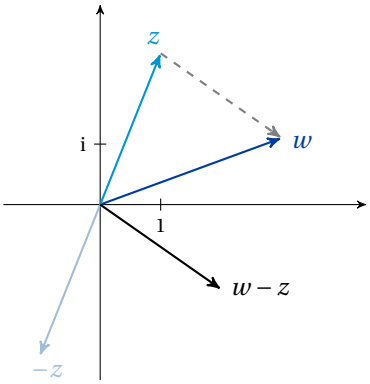
die alle entfernt wurden.) $[40,41] \cap [41,43]$ ist das Intervall $\{41\}$, das ebenfalls kein *echtes* Intervall ist. $(40,42) \setminus \mathbb{N}$ ist die Menge $(40,41) \cup (41,42)$ mit der „Lücke“ 41.

Lösung 17.1. Kam Ihnen das bekannt vor? Das haben Sie (hoffentlich) schon einmal in Aufgabe 10.9 gemacht …

Lösung 17.2. $\mathrm{Re}(z) = 3$ und $\mathrm{Im}(z) = -4$. Eigentlich dürfte das kein Problem sein. Die Aufgabe soll lediglich auf zwei typische Fehler hinweisen. Erstens ist der Imaginärteil *nicht* 4. (Das Vorzeichen wird ab und zu mal vergessen.) Und zweitens ist der Imaginärteil *nicht* $-4\mathrm{i}$. Das i gehört nicht dazu.

Lösung 17.5. Hat z die Koordinaten (a,b), so hat die Zahl $-z$ die Koordinaten $(-a,-b)$. Den Ort von $-z$ erhält man also durch Punktspiegelung von z am Ursprung.

Lösung 17.6. Die Skizze geht mithilfe von Aufgabe 17.5 aus der für die Addition hervor, wenn man sich daran erinnert, dass $w - z$ für $w + (-z)$ steht.



Beachten Sie, dass wegen $w = z + (w - z)$ der (verschobene) $w - z$-Pfeil von der Spitze von z auf die von w zeigt. (In der Skizze ist das der gestrichelte graue Pfeil.)

Lösung 17.7. $|\mathrm{i}| = \sqrt{0^2 + 1^2} = 1$.

Lösung 17.8. $|-z| = |-a-b\mathrm{i}| = \sqrt{(-a)^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$. Angesichts von Aufgabe 17.5 ist geometrisch auch klar, warum in beiden Fällen dasselbe herauskommen muss.

Lösung 17.9. Für reelle Zahlen kommt in beiden Fällen dasselbe heraus. (Wenn dem nicht so wäre, wäre die Definition auch sehr unglücklich.) Setzt man eine reelle Zahl a in die neue (komplexe) Definition ein, dann erhält man

$$|a| = |a + 0\mathrm{i}| = \sqrt{a^2 + 0^2} = \sqrt{a^2}$$

und das ist der reelle Betrag.[58] Auch für reelle Zahlen ist der Betrag also der Abstand von der Null.

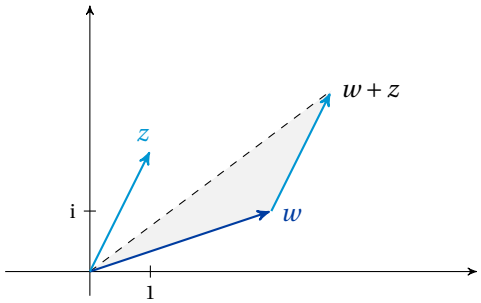
[58] Achtung: Ein häufig anzutreffender Denkfehler ist, dass $\sqrt{a^2}$ dasselbe wie a ist. Dass das falsch ist, kann man sehen, wenn man für a eine negative Zahl einsetzt.

Lösung 17.10. Wenn man das Rechnen nicht verlernt hat, ist das Routine:

$$\begin{aligned}
|wz| &= |(a+b\mathrm{i})(c+d\mathrm{i})| = |(ac-bd)+(ad+bc)\mathrm{i}| \\
&= \sqrt{(ac-bd)^2+(ad+bc)^2} \\
&= \sqrt{a^2c^2-2acbd+b^2d^2+a^2d^2+2adbc+b^2c^2} \\
&= \sqrt{a^2c^2+b^2d^2+a^2d^2+b^2c^2} \\
|w|\cdot|z| &= |a+b\mathrm{i}|\cdot|c+d\mathrm{i}| = \sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2} \\
&= \sqrt{(a^2+b^2)\cdot(c^2+d^2)} = \sqrt{a^2c^2+b^2c^2+a^2d^2+b^2d^2}
\end{aligned}$$

Aufgefallen sein sollte Ihnen, dass in beiden Fällen dasselbe herauskommt.

Lösung 17.11. Ihre Skizze sollte in etwa so aussehen:



In der Dreiecksungleichung geht es um das grau eingefärbte Dreieck und die geometrisch evidente Aussage, dass der direkte Weg (die gestrichelte Linie) von 0 zum Ziel $w+z$ kürzer ist als der „Umweg“ über w (entlang der blauen Pfeile).

Lösung 17.12. Hat z die Koordinaten (a,b), so hat die Zahl $\overline{z}$ die Koordinaten $(a,-b)$. Den Ort von $\overline{z}$ erhält man also durch Achsenspiegelung von z an der reellen (horizontalen) Achse.

Lösung 17.13. Das ist nun wirklich einfach.

$$\begin{aligned}
\overline{w+z} &= \overline{(a+c)+(b+d)\mathrm{i}} = (a+c)-(b+d)\mathrm{i} = a-b\mathrm{i}+c-d\mathrm{i} \\
&= \overline{a+b\mathrm{i}}+\overline{c+d\mathrm{i}} = \overline{w}+\overline{z} \\
\overline{w\cdot z} &= \overline{(ac-bd)+(ad+bc)\mathrm{i}} = (ac-bd)-(ad+bc)\mathrm{i} = (a-b\mathrm{i})\cdot(c-d\mathrm{i}) \\
&= \overline{a+b\mathrm{i}}\cdot\overline{c+d\mathrm{i}} = \overline{w}\cdot\overline{z}
\end{aligned}$$

In beiden Fällen kommt also jeweils dasselbe heraus. Zumindest bei der Addition ist das geometrisch evident, weil es offenbar egal ist, ob wir erst spiegeln und dann (geometrisch) addieren oder umgekehrt. Wie die Multiplikation geometrisch zu interpretieren ist, müssen wir uns noch erarbeiten.

Lösung 17.14. Ist $z=a+b\mathrm{i}$, so erhält man

$$\begin{aligned}
z+\overline{z} &= (a+b\mathrm{i})+(a-b\mathrm{i}) = 2a = 2\,\mathrm{Re}(z) \quad \text{und} \\
z-\overline{z} &= (a+b\mathrm{i})-(a-b\mathrm{i}) = 2b\mathrm{i} = 2\mathrm{i}\,\mathrm{Im}(z).
\end{aligned}$$

Lösung 17.15. Weil der Realteil von z negativ und der Imaginärteil positiv ist, muss das Argument zwischen 90 und 180 Grad liegen. (Machen Sie sich eine Skizze, wenn Ihnen das nicht klar ist!) Das Argument von z^2 ist doppelt so groß und liegt daher zwischen 180 und 360 Grad (bzw. „offiziell“ zwischen -180 und 0 Grad, aber das ist für die geometrische Lage natürlich irrelevant). Deshalb liegt z^2 unterhalb der reellen Achse und kann *nicht* in der oberen Hälfte liegen.

Lösung 17.16. Das läuft analog zur letzten Aufgabe. Das Argument von z liegt im Bereich von 0 bis -90 Grad. (Skizze!) Das Argument von z^3 liegt daher zwischen 0 und -270 Grad und damit *nicht* im oberen rechten Quadranten.

Lösung 17.17. Wir beginnen mit $c^2 - d^2 = 3$ und $2cd = 4$. Das liefert $d = 2/c$ und Einsetzen in die erste Gleichung führt zu $c^2 - 4/c^2 = 3$ bzw. $c^4 - 3c^2 - 4 = 0$. Mit $x = c^2$ wird daraus $x^2 - 3x - 4 = 0$ mit den Lösungen 4 und -1. Wir verwerfen die negative Lösung und setzen $x_1 = 4$. Das liefert $c_1 = 2$ und $c_2 = -2$ und dazu $d_1 = 1$ und $d_2 = -1$, was schließlich zu den Lösungen $w_1 = 2 + \mathrm{i}$ und $w_2 = -w_1$ führt. (Machen Sie eine Probe, indem Sie $2 + \mathrm{i}$ quadrieren!)

Lösung 17.19. Um auf $d = b/(2c)$ zu kommen, muss man durch c teilen. Das geht aber nur, wenn c nicht null ist. Außerdem stimmt die Bemerkung in Fußnote 22 nur, wenn $|a|$ *kleiner* als $|z|$ ist, was wiederum nur der Fall ist, wenn $b \neq 0$ gilt.

Man muss also erst den Fall $b = 0$ separat behandeln. Dann ist z die reelle Zahl a und das lässt sich leicht abhandeln: Ist a positiv, dann sind die Lösungen $\sqrt{a}$ und $-\sqrt{a}$. Ist a negativ, dann sind die Lösungen $\mathrm{i}\sqrt{a}$ und $-\mathrm{i}\sqrt{a}$.

Nun kann man $b \neq 0$ voraussetzen und den Fall $c = 0$ verwerfen. w_1 wäre dann nämlich die Zahl $d\mathrm{i}$ mit dem Quadrat $-d^2$.

Lösung 17.20. Division durch 2 ergibt $w^2 + (1 + \mathrm{i})w + (6 + 18\mathrm{i}) = 0$. Mit den Bezeichnungen aus dem Beweis von Satz 17.7 haben wir $p = 1 + \mathrm{i}$ und $q = 6 + 18\mathrm{i}$. $p^2/4 - q$ ist $-6 - 35\mathrm{i}/2$. Eine „Wurzel“ dieser Zahl ist $5/2 - 7\mathrm{i}/2$. Kombiniert mit $-p/2 = -1/2 - \mathrm{i}/2$ ergeben sich die zwei Lösungen $2 - 4\mathrm{i}$ und $-3 + 3\mathrm{i}$. (Machen Sie eine Probe!)

Lösung 18.1. $w - z$ ist die Summe von $w - v$ und $v - z$. Die beiden Differenzen rechts spielen also die Rolle von w und z in Lemma 17.3.

Lösung 18.2. Das sollte für Sie hoffentlich nur eine Fingerübung im Einsetzen von Werten in eine Formel sein.

$$\begin{aligned} d\big((x_1, y_1), (x_2, y_2)\big) &= |x_1 - x_2| + |y_1 - y_2| \\ &\leq \big(|x_1 - x_3| + |x_3 - x_2|\big) + \big(|y_1 - y_3| + |y_3 - y_2|\big) \\ &= \big(|x_1 - x_3| + |y_1 - y_3|\big) + \big(|x_3 - x_2| + |y_3 - y_2|\big) \\ &= d\big((x_1, y_1), (x_3, y_3)\big) + d\big((x_3, y_3), (x_2, y_2)\big) \end{aligned}$$

Die Ungleichung in der zweiten Zeile gilt, weil dort (zweimal) die Dreiecksungleichung für Differenzen von reellen Zahlen (Korollar 16.8) angewandt wurde.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 18.3. Für drei Punkte, von denen keine zwei auf einer gemeinsamen Geraden durch 0 liegen, sieht es so aus:

$$d(z,w) = |z| + |w| \leq |z| + |v| + |v| + |w| = d(z,v) + d(v,w)$$

Anschaulich heißt das: Will man von Brest nach Marseille fahren, aber zwischendurch die Großeltern in Rouen besuchen, dann kommen *zwei* Fahrten zwischen Paris und Rouen gegenüber der „direkten“ Verbindung hinzu.

Liegen alle drei Punkte auf einer Geraden durch „Paris“, dann ergibt sich die Dreiecksungleichung für den euklidischen Abstand. Liegen z und w auf einer gemeinsamen Ursprungsgeraden, aber v nicht, dann hat man

$$d(z,w) = |z-w| \leq |z| + |w| \leq |z| + |v| + |v| + |w| = d(z,v) + d(v,w).$$

Und liegen o. B. d. A. w und v auf so einer Geraden, z aber nicht, dann ergibt sich

$$d(z,w) = |z| + |w| \leq |z| + |v| + |w-v| = d(z,v) + d(v,w),$$

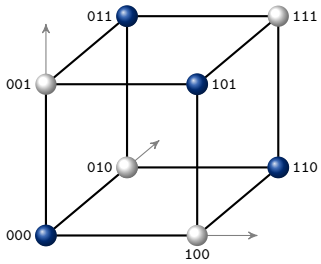
wobei die Ungleichung in der Mitte aus $w = v + (w-v)$ folgt.

Lösung 18.4. Bei der Fallunterscheidung würde es nun um Geraden durch p und nicht durch 0 gehen. Die Formel für Punkte, die nicht gemeinsam auf so einer Geraden liegen, ergäbe sich als $d(z,w) = |z-p| + |p-w|$. Anschaulich ist klar, dass das immer noch eine Metrik sein muss, weil man das Koordinatensystem ja einfach so verschieben kann, dass p der neue Ursprung ist. Für den allgemeinen Fall, dass keine zwei Punkte gemeinsam auf einer der relevanten Geraden liegen, sieht die Überprüfung von **M3** so aus:

$$\begin{aligned} d(z,w) &= |z-p| + |p-w| \leq |z-p| + |p-v| + |v-p| + |p-w| \\ &= d(z,v) + d(v,w). \end{aligned}$$

Die restliche Rechnerei erspare ich mir und Ihnen.

Lösung 18.5. Eine Möglichkeit wäre $\{000, 011, 101, 110\}$, wobei die Tupel hier ohne Klammern und Kommata geschrieben wurden.



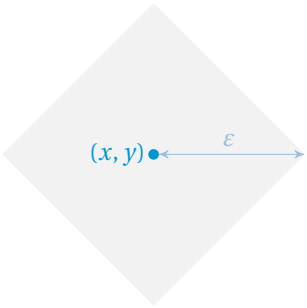
In der Skizze wären das die blauen Punkte (und man hätte stattdessen auch die weißen nehmen können). Den Hamming-Abstand kann man hier schön grafisch interpretieren als die Anzahl der Kanten, die man passieren muss, um von einem Punkt zum anderen zu kommen.

Lösung 18.6. Wenn man $\{0,1\}^2$ als Teilmenge von $\mathbb{R}^2$ betrachtet, dann stimmen Hamming-Abstand und Manhattan-Metrik auf dieser Menge überein. Das gilt auch für $\{0,1\}^n$ und $\mathbb{R}^n$, wenn man die Manhattan-Metrik sinngemäß auf höhere Dimensionen verallgemeinert.

Lösung 18.8. Die Menge $U_\varepsilon(x)$ ist in $\mathbb{R}$ das Intervall $(x-\varepsilon, x+\varepsilon)$. Geometrisch erhält man es, wenn man die entsprechende Kreisscheibe in $\mathbb{C}$ mit der reellen Achse schneidet.

Lösung 18.9. (a,b) ist $U_\varepsilon(x)$, wenn man $x = (a+b)/2$ und $\varepsilon = (b-a)/2$ setzt.

Lösung 18.10. Die Menge $U_\varepsilon\big((x,y)\big)$ ist in der Manhattan-Metrik ein Quadrat mit Mittelpunkt (x,y), dessen Diagonalen achsenparallel verlaufen und die Länge 2ε haben.



Lösung 18.11. In $U_2(\texttt{AC})$ liegen nach Definition alle Wörter, deren Levenshtein-Distanz von `AC` kleiner als 2 ist. Da diese Distanz immer eine ganze Zahl ist, geht es um die Wörter, deren Abstand von `AC` 0 oder 1 ist. Den Abstand 0 kann wegen der positiven Definitheit nur `AC` haben. Den Abstand 1 kann man nach Definition der Metrik nur durch *eine* Operation erreichen. Durch Entfernen eines Buchstabens kann man offenbar `A` oder `C` enthalten. Durch Ersetzen eines Buchstabens kann man aus `AC` die Wörter `BC`, `CC`, `AA` oder `AB` machen. Und durch Hinzufügen eines Buchstabens erhält man Wörter wie `AAC` mit drei Buchstaben. Insgesamt ergibt sich $U_2(\texttt{AC}) = \{\texttt{A}, \texttt{C}, \texttt{AA}, \texttt{AB}, \texttt{AC}, \texttt{BC}, \texttt{CC}, \texttt{AAC}, \texttt{ABC}, \texttt{ACA}, \texttt{ACB}, \texttt{ACC}, \texttt{BAC}, \texttt{CAC}\}$.

Lösung 18.12. Intervalle der Form (a,∞) oder $(-\infty,a)$ mit $a \in \mathbb{R}$ sind offen. Und Vereinigungen von Intervallen sind auch offen.

Lösung 18.13. Nach Aufgabe 18.9 und Lemma 18.2 ist I offen in $\mathbb{R}$. Aber das war nicht die Frage! Als Teilmenge von $\mathbb{C}$ ist I *nicht* offen, denn für jedes noch so kleine $\delta > 0$ ist die echt komplexe Zahl $(1+\delta\mathrm{i})/2$ ein Element von $U_\delta(1/2)$, aber keines von $I \subseteq \mathbb{R}$.

Lösung 18.14. In diesem Fall sind *alle* Teilmengen von X offen, denn für alle $x \in X$ gilt offenbar $U_{1/2}(x) = \{x\}$. Ist $A \subseteq X$ und $y \in A$, so folgt mit $\delta = 1/2$ also sofort $U_\delta(y) \subseteq A$.

Lösung 18.16. Der Rand von $[a,\infty)$ und (a,∞) besteht jeweils nur aus der Zahl a. Der Rand von $(-\infty,b]$ und $(-\infty,b)$ besteht jeweils nur aus der Zahl b. (a,∞) und $(-\infty,b)$ sind offen und das Innere der jeweiligen Pendants mit eckigen Klammern.

$[a,\infty)$ und $(-\infty,b]$ sind abgeschlossen und der Abschluss der jeweiligen Pendants mit runden Klammern. Kein echtes Intervall hat isolierte Punkte.

Lösung 18.17. Diese Frage haben Sie in Aufgabe 18.12 eigentlich schon beantwortet, aber manchmal schadet Wiederholung ja nicht. Zum Beispiel könnte man $(0,1) \cup (2,3)$ nehmen – siehe Lemma 18.3. Ganz allgemein gilt sogar, dass jede in $\mathbb{R}$ offene Menge sich als Vereinigung von (evtl. unendlich vielen) Intervallen darstellen lässt.

Lösung 18.18. A° ist die Menge der inneren Punkte von A und nach Definition sind innere Punkte von A Elemente von A. Damit ist der erste Teil bereits erledigt. Für den zweiten Teil muss man zeigen, dass jedes Element a von A Berührungspunkt von A ist. Das ist aber auch nach Definition sofort klar, denn eine offene Menge B, die a enthält, kann nicht disjunkt zu A sein, weil natürlich $a \in A \cap B$ gilt.

Lösung 18.19. Ist x ein Berührungspunkt von A und *nicht* Element von A, dann liegt x in $X \setminus A$ und ist damit auch Berührungspunkt von $X \setminus A$, also nach Definition Randpunkt.

Lösung 18.20. Zum Beispiel das Intervall $[0,1)$.

Lösung 18.21. Ja, das besagt Lemma 16.11.

Lösung 18.22. Einerseits gilt $U_r(x) \subseteq \overline{U_r(x)}$, andererseits $\overline{U_r(x)} \subseteq U_{r+1}(x)$.

Lösung 18.23. Ist A eine Teilmenge von $U_r(x)$, dann ist A nach oben und unten durch $x+r$ bzw. $x-r$ beschränkt. Ist umgekehrt A nach oben durch b und nach unten durch a beschränkt, dann ist A eine Teilmenge von $U_r(0)$, wenn wir $r = 1 + \max\{a,b\}$ setzen.

Lösung 18.24. Ist eine Menge X mit der diskreten Topologie versehen und x irgendein Element von X, dann gilt $X = U_2(x)$, also ist jede Teilmenge von X beschränkt. Aber auch in der Menge $\{0,1\}^n$ mit dem Hamming-Abstand sind alle Mengen beschränkt, denn der Abstand zweier Elemente kann höchstens n sein.

Lösung 19.1. Die erste Aussage ist wahr, denn „nur“ eine Milliarde natürliche Zahlen sind nicht größer als 999 999 999. Die zweite Aussage ist falsch. Zwar sind unendlich viele Zahlen gerade, aber es gibt auch unendlich viele Ausnahmen, nämlich die ungeraden Zahlen. Ebenso ist die dritte Aussage falsch, weil es nach dem Satz des Euklid unendlich viele Zahlen gibt, die nicht zusammengesetzt sind. Die vierte Aussage ist wahr, denn die ersten hundert Folgenglieder sind null und damit nicht positiv, aber danach kommen nur noch positive Zahlen.

Lösung 19.2. Die Frage kommt an dieser Stelle, weil nach meiner Erfahrung Studierende sie häufig mit *nein* beantworten. Aber das ist falsch. Selbstverständlich konvergiert (42) gegen 42. Wie üblich muss man sich dafür die Definition nur genau anschauen. Für jedes noch so kleine ε liegt 42 natürlich in $U_\varepsilon(42)$, also liegen nicht nur *fast* alle, sondern sogar *alle* Folgenglieder in dieser Umgebung. Grundsätzlich geht in jedem metrischen Raum eine konstante Folge der Form (a) gegen a.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 19.3. Die Folge konvergiert weder gegen 1 noch gegen -1. Eine Begründung dafür liefert das nun folgende Lemma 19.2.

Lösung 19.4. Bei der Frage geht es um Eigenschaften von metrischen Räumen. Wären die beiden Mengen nicht disjunkt, dann gäbe es ein $x \in U_{\varepsilon/2}(a) \cap U_{\varepsilon/2}(b)$. Es würde also $d(x,a) < \varepsilon/2$ und $d(x,b) < \varepsilon/2$ gelten. Mit der Dreiecksungleichung folgt der Widerspruch $d(a,b) \leq d(a,x) + d(x,b) < \varepsilon/2 + \varepsilon/2 = \varepsilon$.

Lösung 19.5. Wenn eine Folge den Grenzwert a hat, dann müssen fast alle Folgenglieder in $U_{1/2}(a)$ liegen. Diese Umgebung ist jedoch das Singleton $\{a\}$, d. h., fast alle Folgenglieder *sind* a. Mit anderen Worten sind in metrischen Räumen genau die Folgen konvergent, die ab einem bestimmten Punkt konstant sind.

Lösung 19.6. Die Folge aus Aufgabe 19.3 könnte man nehmen.

Lösung 19.7. Das folgt direkt aus der Aussage des Lemmas über Produkte, wenn man für (b_n) die konstante Folge (λ) nimmt.

Lösung 19.8. Anderenfalls gälte $|b_n| \leq |b|/2$ und mit der Dreiecksungleichung käme man dann auf den Widerspruch

$$|b| = |b - b_n + b_n| \leq |b - b_n| + |b_n| < |b|/2 + |b|/2 = |b|.$$

Lösung 19.9. Die erste Folge ist eine Nullfolge. Die zweite Folge geht gegen $-1/2$ (man beachte das Vorzeichen). Das macht man mit demselben „Trick“ wie eben, wobei hier mit $1/n^2$ erweitert wird. Und durch Erweitern mit $1/n^3$ ergibt sich bei der dritten Folge der Grenzwert 0. Sie erkennen für Folgen dieser Art hoffentlich ein allgemeines Verfahren, bei dem man immer mit dem Kehrwert der höchsten Potenz von n erweitert, wenn in Zähler und Nenner Polynome in n stehen. Mit etwas Übung sieht man den Grenzwert, ohne dass man die Berechnung explizit durchführen muss.

Lösung 19.10. Mit dem besagten „Trick“ (Erweitern mit n^{-3}) erhält man den Grenzwert $6/a$. Damit daraus 42 wird, muss $a = 1/7$ gelten.

Lösung 19.11. Wie für $\big((-1/n)^n\big)$ zeigt man mit dem Majorantenkriterium, dass es sich um eine Nullfolge handelt. Die Folge (i^n) hat die ersten vier Glieder 1, i, -1 und $-\mathrm{i}$ und wiederholt diese Werte von da an zyklisch. Die Folgenglieder $\big((\mathrm{i}/n)^n\big)$ kommen also der Null immer näher, drehen sich dabei aber im Kreis.

Lösung 19.12. Man könnte z. B. $a_n = 0$ und $b_n = 1/n$ nehmen.

Lösung 19.13. Das folgt aus dem Lemma für (b_n), wenn man für (a_n) die konstante Folge (0) nimmt.

Lösung 19.14. Sonst hätten wir $x = 0$ und damit $M = \{0\}$. Das kann man dadurch widerlegen, dass man mindestens ein positives Element von M findet. Zum Beispiel so: Nach Korollar 16.3 gibt es ein $k \in \mathbb{N}^+$ mit $1/k < y$. Weil „erst recht“ $1/k^n < y$ gilt, folgt $1/k \in M$.

Lösung 19.15. Geht man über zu $\mathbb{Z}/4\mathbb{Z}$, dann wird aus $5^n + 3$ der Ausdruck $1^n + 3$ und das ist offenbar $1 + 3 = 0$.

leere Summe

Lösung 19.16. Im Induktionsanfang ($n=0$) haben wir es mit der leeren Summe zu tun.[59] Wir müssen also $0 = 0\cdot(0+1)/2$ „beweisen“ und das ist offensichtlich trivial. Für den Induktionsschritt berechnen wir

$$1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{n(n+1)}{2}+\frac{2(n+1)}{2}$$
$$= \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$$

und sind damit bereits fertig. Wichtig für das Verständnis ist, dass die erste Gleichheit aus der Induktionsvoraussetzung folgt, denn dort haben wir die Summenformel für die ersten n der insgesamt $n+1$ Summanden angewandt. Alle weiteren Umformungen sind simple Schulmathematik.

Lösung 19.17. Dort wird gesagt, dass aus $x_1 > x_2 > 0$ wegen Lemma 15.3 $x_1^n > x_2^n$ folgt. Eigentlich folgt aber nur $x_1^2 > x_2^2$. Wenn man korrekt vorgeht, dann geht es um die Aussageform $P(n)$, die

$$\forall\, x_1, x_2 \in \mathbb{R}\,(x_1 > x_2 > 0 \Rightarrow x_1^{n+1} > x_2^{n+1})$$

besagt. $P(0)$ ist dann trivial und den Induktionsschritt beweist man mit dem erwähnten Lemma.

Und auch später müsste man noch einmal die vollständige Induktion anwenden. Am Ende des Beweises wird nämlich $\lim_{k\to\infty} a_k^n = \left(\lim_{k\to\infty} a_k\right)^n$ ausgenutzt. Das folgt zwar aus den Rechenregeln für Grenzwerte, aber direkt nur für $n=2$.

Lösung 19.18. Wäre die Aussage nicht wahr, dann gäbe es wieder eine *kleinste* Zahl $n \in \mathbb{N}$, für die $P(n)$ *nicht* gilt. Weil es sich um die kleinste Zahl dieser Art handelt, gilt dann jedoch $P(m)$ für alle m, die kleiner als n sind. Und damit folgt mit (19.1) sofort der Widerspruch, dass auch $P(n)$ gelten muss.

In Satz 19.8 wird verlangt, dass die Wahrheit von $P(n+1)$ aus der von $P(n)$ folgen muss. In der Formulierung dieser Aussage darf man hingegen für den Nachweis der Wahrheit von $P(n+1)$ die Wahrheit aller Aussagen „davor“ voraussetzen. Man könnte (19.1) auch als $(P(0)\wedge P(1)\wedge\cdots\wedge P(n-1)) \Rightarrow P(n)$ schreiben.

Lösung 19.19. Wenn wir $P(n)$ für $2^n > n^2$ schreiben, dann gilt $P(n)$ offenbar *nicht* für *alle* $n\in\mathbb{N}$, denn $P(2)$, $P(3)$ und $P(4)$ sind falsch. In diesem Fall wählen wir also $k=5$. Der Induktionsanfang $P(5)$ ist die Aussage $32 = 2^5 > 5^2 = 25$, die offenbar wahr ist. Im Induktionsschluss haben wir nun

$$2^{n+1} = 2\cdot 2^n \overset{\text{IV}}{>} 2\cdot n^2 = n^2+n^2 \overset{\star}{\geq} n^2+(2n+1) = (n+1)^2. \tag{L-4}$$

Dabei steht „IV“ für das Anwenden der Induktionsvoraussetzung. Wichtig ist allerdings auch, dass die mit dem Stern markierte Abschätzung nur unter der Bedingung $n\geq 3$ funktioniert, denn dann haben wir $n^2 \geq 3n = 2n+n \geq 2n+1$. Wir hätten zwar auch $n=0$ beginnen können, weil $P(0)$ eine wahre Aussage ist, aber der Schluss (L-4) wäre dann nicht mehr für alle n korrekt gewesen.

[59] Falls Ihnen dieses Konzept neu vorkommt und Sie sich nicht erinnern, dass in diesem Skript bereits zweimal das leere Produkt vorkam, dann schauen Sie vielleicht mal im Index nach.

Lösung 19.20. Wir beginnen die Induktion mit $n = 1$, was nach Aufgabe 19.19 legitim ist. An der Stelle im Induktionsschritt, an der wir $\{k_1, k_2\}$ betrachten, setzen wir jedoch voraus, dass die Aussage für $n = 2$ bereits bewiesen ist.

Lösung 19.21. Es handelt sich um diese Aussageform:

$$P(n): \qquad \forall x \in [-1,\infty)\ (1+x)^n \geq 1 + nx.$$

Wichtig ist, dass $P(n)$ etwas über n aussagt, aber *nicht* über x, weil die Variable x durch den Quantor gebunden ist. (Siehe Fußnote 15 auf Seite 19.)

Lösung 19.22. Wie wäre es mit $(1 + 1/n)$? Es gibt natürlich viele Beispiele.

Lösung 19.23. In diesem Fall hat man $a_n = 3^{-n}$.

Lösung 19.24. Wir wollen zeigen, dass $a_n = a'_n$ für alle $n \in \mathbb{N}$ gilt. Das ist unsere Aussageform $P(n)$. Wegen $a_0 = x = a'_0$ gilt $P(0)$. Für den Induktionsschritt nehmen wir nun an, dass $P(n)$ gilt, also $a_n = a'_n$. Dann folgt $a_{n+1} = f(a_n) = f(a'_n) = a'_{n+1}$, also $P(n+1)$.

Lösung 19.25. Nacheinander ergibt sich dies:

$$\begin{aligned} a_2 &= a_0 + a_1 = 0 + 1 = 1 & a_3 &= a_1 + a_2 = 1 + 1 = 2 \\ a_4 &= a_2 + a_3 = 1 + 2 = 3 & a_5 &= a_3 + a_4 = 2 + 3 = 5 \\ a_6 &= a_4 + a_5 = 3 + 5 = 8 & a_7 &= a_5 + a_6 = 5 + 8 = 13 \end{aligned}$$

Lösung 19.26. Wir erhalten nacheinander:

$$\begin{aligned} p_0 &= 2 & 1 + p_0 &= 3 \\ p_1 &= 3 & 1 + p_0 p_1 &= 7 \\ p_2 &= 7 & 1 + p_0 p_1 p_2 &= 43 \\ p_3 &= 43 & 1 + p_0 p_1 p_2 p_3 &= 1807 \end{aligned}$$

1807 hat die Primteiler 13 und 139 und damit folgt $p_4 = 13$.

Lösung 19.27. Im ersten Fall wäre das $F(a) = a/3$ mit $x = 1$. Für die andere Folge ist eine solche Definition gar nicht möglich, denn mit

$$a_1 = h(a_0) = h(1) = h(a_1) = a_2$$

würden wir eine konstante Folge erhalten. Hier muss man Satz 19.12 mit $F(\emptyset) = 1$ und $F(g) = (1 + \max \mathrm{dom}(g)) \cdot \max \mathrm{rng}(g)$ für $g \neq \emptyset$ verwenden.

Lösung 19.28. Für die Fibonacci-Folge setzt man $F(\emptyset) = 0$, $F(\{(0,0)\}) = 1$ und $F(g) = g(n) + g(n+1)$ für alle g mit $\mathrm{dom}(g) = [n+2]_0$. Für die andere Folge definiert man F durch $F(\emptyset) = 2$ und $F(g)$ als kleinsten Primteiler von $g(0) \cdot g(1) \cdot \dots \cdot g(n)$ für alle g mit $\mathrm{dom}(g) = [n+1]_0$.

Lösung 19.29. Es ergibt sich $b_2 = (1+3) \bmod 5 = 4$, $b_3 = 2$, $b_4 = 1$ und $b_5 = 3$. An dieser Stelle ist ohne Rechnen klar, dass sich die Werte periodisch wiederholen müssen, weil $(b_4, b_5) = (b_0, b_1)$ gilt und der nächste Folgenwert nur von den beiden vorherigen abhängt. Weil die „Schrittweite“ offenbar 4 ist, muss $b_{13} = b_9 = b_5 = 3$ gelten.

Lösung 19.30. Es kommt immer zu periodischen Wiederholungen. Ab b_2 kommen nur noch Folgenwerte aus der Menge $\{0,1,2,3,4\}$ vor. Für die Paare (b_2,b_3), (b_3,b_4), (b_4,b_5) und so weiter gibt es nach Satz 4.6 daher nur 25 verschiedene Möglichkeiten. Irgendwann tritt also ein Paar auf, das schon einmal vorkam.

Lösung 19.31. Man muss sich nur klarmachen, dass so etwas wie $\sqrt[m]{a}$ nur eine andere Schreibweise für $a^{1/m}$ ist. Das sollte man ohnehin immer im Kopf behalten, weil sich dadurch Wurzelterme oft vereinfachen lassen.

Lösung 19.32. Zum Beispiel $a=-2$: $\sqrt{(-2)^2}=\sqrt{4}=2\neq -2$. Das ist kein Widerspruch, weil die Aussagen in Lemma 19.14 nur für nichtnegative Zahlen a und b gelten.

Lösung 19.33. Hier muss man ein bisschen umformen und dann wieder mit dem Kehrwert des am schnellsten wachsenden Terms erweitern. Es ergibt sich:

$$\frac{4^{n+1}+2^n}{4^n+2^{2n}}=\frac{4^{n+1}+2^n}{2\cdot 4^n}\cdot\frac{4^{-n}}{4^{-n}}=\frac{4+(1/2)^n}{2}\xrightarrow{n\to\infty}\frac{4+0}{2}=2$$

Lösung 19.34. Man muss lediglich eine einfache Umformung erkennen, um auf eine Folge zu kommen, deren Grenzwert wir gerade hergeleitet haben:

$$\sqrt[n]{2^{n+1}}=\sqrt[n]{2^n\cdot 2}=\sqrt[n]{2^n}\cdot\sqrt[n]{2}=2\cdot\sqrt[n]{2}\to 2\cdot 1=2$$

Lösung 19.36. Zum Beispiel $\big((-1)^n/n\big)$.

Offensichtlich gilt die Umkehrung von Lemma 19.17 jedoch, wenn (a_n) eine reelle Nullfolge ist, die nie das Vorzeichen wechselt: Dann ist $(1/a_n)$ bestimmt divergent.

Lösung 20.1. In den meisten Fällen kann man Lemma 20.2 anwenden. Die Folge $(2^{n+42}/3^n)$ ist die Nullfolge $\big(2^{42}\cdot(2/3)^n\big)$ und daher ist die erste Aussage wahr und die zweite nicht. $\big(2^n/(n^2 2^n)\big)$ ist die Nullfolge $(1/n^2)$ und daher ist die dritte Aussage falsch. $\big(n^2 2^n/3^n\big)$ ist die Folge $\big(n^2/(3/2)^n\big)$, die nach Lemma 19.11 eine Nullfolge ist, also ist die vierte Aussage wahr. $\big(2^n/(2^n)^2\big)$ ist die Nullfolge $(1/2^n)$ und daher ist die fünfte Aussage falsch. Dass die letzte Aussage richtig ist, folgt schließlich mit $\log n\in\mathcal{O}(n)$ und Punkt (iii) von Satz 20.1.

Lösung 21.1. a_k ist in diesem Fall k^2. Es müsste daher so aussehen:

$$\begin{aligned}\sum_{k=3}^{5}k^2&=5^2+\sum_{k=3}^{4}k^2=5^2+4^2+\sum_{k=3}^{3}k^2\\&=5^2+4^2+3^2+\sum_{k=3}^{2}k^2=5^2+4^2+3^2+0=50\end{aligned}$$

Lösung 21.2. Das sollte so aussehen:

$$s_1=\sum_{k=1}^{101}4k \qquad s_2=\sum_{i=3}^{1000}(3i+1)$$

$$s_3=\sum_{n=1}^{11}n^{-2}=\sum_{n=1}^{11}\frac{1}{n^2} \qquad s_4=\sum_{j=1}^{42}(-1)^{j+1}j$$

$$s_5 = \sum_{k=2}^{33} n a_{3k}$$

Beachten Sie, dass bei solchen Summen die „Schrittweite“ immer 1 ist. Um z. B. in s_1 Schritte der Weite 4 zu erreichen, werden die Summanden entsprechend multipliziert. Bei s_2 wird außerdem der konstante Term 1 addiert, um das „Verschieben“ der Summe zu erreichen. Bei s_4 sorgt die Potenz von -1 für den Vorzeichenwechsel. Es wurden absichtlich unterschiedliche Namen für die Laufvariablen verwendet, um klarzumachen, dass diese Namen keine Rolle spielen. (Sofern sie nicht in den Summanden auftauchen. Bei s_5 sollte die Laufvariable also *nicht* n heißen.)

Lösung 21.4. $1 \cdot 1 + 1 \cdot 1$ ist nicht dasselbe wie $(1+1)\cdot(1+1)$. Man kann als Gegenbeispiel also $a_k = b_k = 1$, $m = 1$ und $n = 2$ nehmen.

Lösung 21.5. Bei der ersten Summe kann man zunächst den Faktor 3 ausklammern und erkennt dann eine arithmetische Summe, die „zu spät anfängt“ und daher in zwei Teile zerlegt werden muss. Bei der zweiten Summe handelt es sich im Wesentlichen um eine geometrische Summe mit $q = 1/2$.

$$\sum_{n=5}^{20} 3n = 3\sum_{n=5}^{20} n = 3\Big(\sum_{n=1}^{20} n - \sum_{n=1}^{4} n\Big) = 3\Big(\frac{20\cdot 21}{2} - \frac{4\cdot 5}{2}\Big) = 600$$

$$\sum_{n=3}^{8} \frac{1}{2^n} = \sum_{n=0}^{8} \Big(\frac{1}{2}\Big)^n - \sum_{n=0}^{2} \Big(\frac{1}{2}\Big)^n = \frac{\left(\frac{1}{2}\right)^9 - 1}{\frac{1}{2} - 1} - \frac{\left(\frac{1}{2}\right)^3 - 1}{\frac{1}{2} - 1} = 2\Big(\Big(\frac{1}{8} - 1\Big) - \Big(\frac{1}{512} - 1\Big)\Big)$$
$$= \frac{1}{4} - \frac{1}{256} = \frac{63}{256}$$

Lösung 21.6. Die „Schrittweite“ ist hier offenbar 10 statt 1, also klammert man 10 aus und bekommt

$$40 + 50 + 60 + \cdots + 230 = 10(4 + 5 + 6 + \cdots + 23) = 10\sum_{k=4}^{23} k = 10\Big(\sum_{k=1}^{23} k - \sum_{k=1}^{3} k\Big)$$
$$= 10\Big(\frac{23\cdot 24}{2} - \frac{3\cdot 4}{2}\Big) = 2700.$$

Lösung 21.7. Hier kann man im Prinzip wie in Aufgabe 21.6 vorgehen (die Schrittweite ist offenbar 3), muss aber beachten, dass die Summanden keine Vielfachen von 3 sind und deshalb „verschoben“ werden müssen:

$$7 + 10 + 13 + 16 + \cdots + 1000 = (1+6) + (1+9) + (1+12) + \cdots + (1+999)$$
$$= \sum_{k=2}^{333} (1+3k) = \Big(\sum_{k=2}^{333} 1\Big) + 3\sum_{k=2}^{333} k$$
$$= 332\cdot 1 + 3\cdot\Big(\frac{333\cdot 334}{2} - 1\Big) = 167\,162$$

Lösung 21.8. Mit $\sum_{k=1}^{n} k^2 = n^3/3 + n^2/2 + n/6$ ergibt sich

$$\sum_{n=1}^{8} n^2 = \frac{1}{3}\cdot 8^3 + \frac{1}{2}\cdot 8^2 + \frac{1}{6}\cdot 8 = \frac{512 + 96 + 4}{3} = 204.$$

Für die zweite Summe erhält man 9450. Hier ist natürlich zu beachten, dass die Summe erst bei 3^2 und nicht bei 1^2 beginnt.

Lösung 21.9. Zum Glück kürzt sich fast alles weg:

$$\prod_{k=3}^{8} \frac{k}{k+1} = \frac{3}{4} \cdot \frac{4}{5} \cdot \frac{5}{6} \cdot \frac{6}{7} \cdot \frac{7}{8} \cdot \frac{8}{9} = \frac{3}{9} = \frac{1}{3}$$

Lösung 21.10. Die richtige Antwort lautet $\prod_{k=m}^{n} \lambda a_k = \lambda^{n-m+1} \prod_{k=m}^{n} a_k$ und *nicht* $\prod_{k=m}^{n} \lambda a_k = \lambda \prod_{k=m}^{n} a_k$. Wenn Ihnen das nicht klar ist, dann schreiben Sie sich für kleine Werte wie $m = 1$ und $n = 4$ explizit hin, wofür die Ausdrücke stehen.

Lösung 21.11. Haben Sie's gesehen? Es ist der Binomialkoeffizient:

$$\prod_{i=1}^{k} \frac{n-i+1}{i} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k} = \binom{n}{k}$$

Lösung 21.12. Als Reihe hat das Beispiel die Form $\sum_{k=0}^{\infty} (-1)^k$ und die Folge der Partialsummen ist $1, 0, 1, 0, 1, 0, \ldots$. Da diese Folge nicht konvergiert, gibt es keinen Reihenwert.

Lösung 21.13. Man könnte beispielsweise $a_n = 0$ für gerade n und $a_n = n$ für ungerade n definieren. Dann wäre 0 der einzige Häufungspunkt, die Folge jedoch unbeschränkt und damit nicht konvergent.

Lösung 21.14. Man kann z. B. die Folge

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \ldots$$

nehmen. Dann ist *jedes* Element des Intervalls $I = (0,1)$ ein Häufungspunkt der Folge. Das liegt daran, dass offenbar alle Brüche zwischen 0 und 1 als Folgenglieder vorkommen. Ist $x \in I$ und $\varepsilon > 0$ vorgegeben, so gibt es, da $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt, unendlich viele rationale Zahlen in $U_\varepsilon(x)$. Ist ε o. B. d. A. klein genug, liegen diese alle in I und kommen daher als Folgenglieder vor.

Übrigens sind 0 und 1 ebenfalls Häufungspunkte der Folge. Man müsste aber etwas umständlicher formulieren, um das auch noch zu begründen.

Lösung 21.15. Dass (a_n) auch eine Cauchy-Folge ist, folgt aus

$$|a_m - a_n| \leq |(a_m - a_n) + \mathrm{i}(b_m - b_n)| = |(a_m + \mathrm{i}b_m) - (a_n + \mathrm{i}b_n)|.$$

Ebenso zeigt man, dass (b_n) eine Cauchy-Folge ist.

Ist nun $\varepsilon > 0$ vorgegeben, so gibt es $n_1, n_2 \in \mathbb{N}$ mit $|a_n - a| < \varepsilon/2$ für $n \geq n_1$ und $|b_n - b| < \varepsilon/2$ für $n \geq n_2$. Für $n \geq \max\{n_1, n_2\}$ gilt dann

$$|(a_n + \mathrm{i}b_n) - (a + \mathrm{i}b)| = |(a_n - a) + \mathrm{i}(b_n - b)| \leq |a_n - a| + |b_n - b| < \varepsilon.$$

Lösung 21.16. Mit $q = 1/3$ erhalten wir $\sum_{n=0}^{\infty} 3^{-n} = (1 - 1/3)^{-1} = 3/2$. Und mit $\sum_{n=0}^{1} 3^{-n} = 1 + 1/3 = 4/3$ ergibt sich als gesuchter Reihenwert $3/2 - 4/3 = 1/6$.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 21.18. Zum Beispiel so:

$$\sum_{n=3}^{\infty} \frac{3}{n+n^2} = 3\Big(\sum_{n=1}^{\infty} \frac{1}{n+n^2} - \sum_{n=1}^{2} \frac{1}{n+n^2}\Big) = 3\Big(1-\frac{1}{2}-\frac{1}{6}\Big) = 1$$

$$\sum_{n=2}^{\infty} \frac{5}{2^n} = 5\Big(\sum_{n=0}^{\infty} \frac{1}{2^n} - \sum_{n=0}^{1} \frac{1}{2^n}\Big) = 5\Big(2-1-\frac{1}{2}\Big) = \frac{5}{2}$$

$$\sum_{n=0}^{\infty} \frac{2\cdot 4^n + 3^{n+1}}{6^n} = 2\sum_{n=0}^{\infty} \big(\frac{2}{3}\big)^n + 3\sum_{n=0}^{\infty} \big(\frac{1}{2}\big)^n = 2\Big(1-\frac{2}{3}\Big)^{-1} + 3\Big(1-\frac{1}{2}\Big)^{-1} = 12$$

Lösung 21.19. In gewissem Sinne sind die „meisten“ Funktionen weder monoton steigend noch fallend. Man könnte die Folge aus Aufgabe 19.3 als Beispiel nehmen. Oder eine Parabel wie $x \mapsto x^2$. Oder die Sinusfunktion.

Lösung 21.20. Sie sind injektiv. Ist $f\colon A \to \mathbb{R}$ beispielsweise streng monoton steigend und sind $x, y \in A$ verschieden, so gilt $a < b$ oder $b < a$ und damit $f(a) < f(b)$ oder $f(b) < f(a)$, auf jeden Fall also $f(a) \neq f(b)$.

Lösung 21.21. Es gibt keine streng monoton fallende Folge natürlicher Zahlen.

Lösung 21.22. Wäre auch nur ein Folgenglied a_{n_0} negativ, so wären ab n_0 alle Folgenglieder höchstens so groß wie a_{n_0}, weil die Folge monoton fällt. Dann wäre nach Lemma 19.6 aber auch der Grenzwert höchstens so groß wie a_{n_0} und damit negativ und nicht null.

Lösung 21.23. Weil dann fast alle Folgenglieder unterhalb von $q = (b+1)/2$ liegen müssen. (q liegt genau in der Mitte zwischen b und 1. Man hätte auch irgendeine andere Zahl aus dem Intervall $(b,1)$ nehmen können.)

Lösung 21.24. Das gilt z. B. für das „Standardbeispiel“ der harmonischen Reihe. $\sqrt[n]{1/n}$ ist für $n > 1$ immer kleiner als 1.

Man könnte auch so etwas wie die Reihe $\sum_{n=1}^{\infty}(1/2 - 1/n)$ nehmen, die nach dem Nullfolgenkriterium nicht konvergiert.

Lösung 21.25. Die n-te Wurzel des n-ten Reihenglieds ist $1/2 - 1/n$ und dieser Wert ist nie größer als $1/2$. Daher konvergiert die Reihe.

Lösung 21.26. Der Quotient zweier aufeinanderfolgender Reihenglieder ist

$$\frac{(3+(n+1)^2)7^{-(n+1)}}{(3+n^2)7^{-n}} = \frac{1}{7}\cdot\frac{3+(n+1)^2}{3+n^2} = \frac{1}{7}\cdot\frac{n^2+2n+4}{n^2+3}.$$

Für $n \to \infty$ geht dieser Ausdruck gegen $1/7$ und da diese Zahl kleiner als 1 ist, konvergiert die Reihe.

Lösung 21.27. Für $k \geq 2$ gilt

$$k^{-2} = \frac{1}{k^2} \leq \frac{1}{k(k-1)}.$$

Damit ist $\sum_{k=2}^{\infty}(k^2-k)^{-1}$ eine Majorante für $\sum_{k=2}^{\infty} k^{-2}$ und das ist dieselbe Reihe wie $\sum_{k=1}^{\infty}(k^2+k)^{-1}$, die nach Lemma 21.10 konvergiert.

Lösung 21.29. Das Ergebnis ist 42/55. Siehe auch Aufgabe 21.32.

Lösung 21.33. $10^{100}/7$ ist $10^{100} \cdot 1/7$ und $1/7$ hat die periodische Dezimaldarstellung $0.\overline{142857}$. Die Periodenlänge ist 6, also haben $10^6/7$, $10^{12}/7$ und so weiter dieselben Nachkommastellen wie $1/7$. Insbesondere hat $10^{96}/7$ diese Nachkommastellen, weil 96 durch 6 teilbar ist. $10^{100}/7$ ist gegenüber dieser Zahl um vier Stellen verschoben, also sind die ersten drei Nachkommastellen dieser Zahl 5, 7 und 1.

Lösung 21.34. Der entscheidende Schritt zur Lösung von Aufgabe 21.33 war die Verschiebung um vier Stellen, die sich durch $100 \bmod 6 = 4$ ergab. Jetzt brauchen wir $5^{1000} \bmod 6$. Dafür können wir dieselbe Technik wie in Aufgabe 13.24 anwenden: $5^2 \bmod 6$ ist 1, also muss $5^{1000} \bmod 6$ ebenfalls 1 sein. Es ergibt sich somit eine Verschiebung um eine Stelle und daher ist die dritte Nachkommastelle 8.

Lösung 21.35. Die Antworten für π sind 3.142, 3.1416 und 3.1415927. Bei 3/80 kommt 0.037 oder 0.038 heraus. Sowohl bei kaufmännischem als auch bei mathematischem Runden würde man sich für 0.038 entscheiden müssen.

Lösung 21.36. Die Frage stellt sich offenbar nur, wenn vor einer Fünf gerundet wird, auf die nur noch Nullen folgen. Bei irrationalen Zahlen wie $\sqrt{2}$ kann dieser Fall nicht eintreten.

Lösung 21.37. Beispielsweise 0.0996. Gerundet ist das 0.100.

Lösung 21.39. Ein besonders einfaches Beispiel ist $x = y = 1$ mit $\tilde{x} = \tilde{y} = 1.1$. Die absoluten Fehler sind in beiden Fällen 0.1, die relativen Fehler liegen jeweils bei 10 %. Die „falsche“ Summe 1.2 weicht um 0.2 von der richtigen ab, das „falsche“ Produkt 1.21 ist 21 % größer als das richtige.

Lösung 22.1. Es bietet sich $n \mapsto n+1$ an. Wenn Sie eine andere Idee hatten, ist das aber auch OK – falls es sich wirklich um eine Bijektion handelt.

Lösung 22.2. Man könnte zum Beispiel

$$n \mapsto \begin{cases} n/2 & n \text{ gerade} \\ -(n+1)/2 & n \text{ ungerade} \end{cases}$$

nehmen. Es gibt aber auch hier viele andere Möglichkeiten.

Lösung 22.3. Als injektive Abbildung von A nach B kann man natürlichen einfach $f = \mathrm{id}_A$ nehmen. Als injektive Abbildung von B nach A eignet sich z. B. ein „Zusammendrücken“ des Intervalls wie $x \mapsto g(x) = x/2 + 1/4$. Da diese Funktion streng monoton ist, ist sie injektiv, und ihr Wertebereich ist offenbar das Intervall $[1/4, 3/4]$, also eine Teilmenge von $(0,1)$.

Lösung 22.4. Eine Möglichkeit wäre die folgende:

$$: \begin{cases} B \to A \\ \qquad x \mapsto \begin{cases} 2^{-1} & x = 0 \\ (n+2)^{-1} & x = 1/n \text{ für ein } n \in \mathbb{N}^+ \\ x & \text{sonst} \end{cases} \end{cases}$$

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 22.5. f^{-1} ist offenbar identisch mit f. Und indem man die Gleichung $y = x/2+1/4$ nach x auflöst, erhält man $g^{-1}(y) = 2y-1/2$. (Siehe z. B. Aufgabe 6.20.)

Sowohl f als auch g bilden $1/2$ auf $1/2$ ab. $1/2$ liegt also auf einer Schleife – einer Kette ohne Anfang – und damit nicht auf einer B-Kette. Nach (22.1) haben wir $h(1/2) = f(1/2) = 1/2$.

Für $3/8$ haben wir $g(1/4) = 3/8$, $f(1/4) = 1/4$ und $g(0) = 1/4$. Aber $0 \in B$ gehört nicht zum Wertebereich von f. Also liegt $3/8$ auf einer B-Kette. (22.1) liefert somit $h(3/8) = g^{-1}(3/8) = 1/4$.

Für $5/16$ schließlich haben wir $g(1/8) = 5/16$ und $f(1/8) = 1/8$. Aber $1/8 \in A$ gehört nicht zum Wertebereich von g. $5/16$ liegt damit ebenfalls nicht auf einer B-Kette und es folgt $h(5/16) = f(5/16) = 5/16$.

Lösung 23.1. Ja, denn $\emptyset$ ist eine bijektive Abbildung von $\emptyset$ auf $[0]$. Falls Ihnen das nicht klar ist, schauen Sie sich noch einmal die Aufgaben 4.7 und 6.2 an.

Lösung 23.2. Offenbar stehen in der k-ten Diagonale k Brüche p/q, für die jeweils $p+q = k+1$ gilt. Zählt man wie in der Skizze ab, so kommen innerhalb einer Diagonale die Brüche mit kleinem Nenner zuerst. *Vor* den Brüchen in der k-ten Diagonale kommen $1+2+\cdots+(k-1)$ andere Brüche an die Reihe. Nach der gaußschen Summenformel sind das $k(k-1)/2$. Insgesamt wird dem (gekürzten) Bruch p/q damit die Zahl

$$(p+q-1)(p+q-2)/2 + q = (p^2+q^2+2pq-3p-q+2)/2$$

zugeordnet.

Lösung 23.3. Als Teilmenge von $\mathbb{N}$ ist $\mathbb{P}$ nach Lemma 23.2 abzählbar. Nach dem Satz von Euklid ist $\mathbb{P}$ unendlich.

Lösung 23.4. Bildet man das Polynom $x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ auf das Tupel $(a_0, \ldots, a_n)$ ab, so erhält man offenbar eine Bijektion von $\mathbb{Q}[x]$ auf $\bigcup_{n\in\mathbb{N}^+} \mathbb{Q}^n$. Nach Korollar 23.7 ist der Wertebereich dieser Bijektion abzählbar.

Lösung 23.5. Weil A abzählbar ist, gibt es eine Injektion f von A nach $\mathbb{N}$. Jeder endlichen Teilmenge B von A kann dadurch eindeutig ein n-Tupel zugeordnet werden; nämlich das Tupel $(a_1, \ldots, a_n)$, für das $\{a_1, \ldots, a_n\} = B$ und $f(a_i) < f(a_{i+1})$ für alle $i < n$ gilt. Nach Korollar 23.7 ist $\mathscr{P}_{<\infty}(A)$ daher abzählbar.

Lösung 24.1. Nach Korollar 23.4 ist $\mathbb{Q}$ abzählbar. Wäre $\mathbb{R} \setminus \mathbb{Q}$ ebenfalls abzählbar, so wäre $\mathbb{R}$ als Vereinigung dieser beiden Mengen nach Satz 23.6 abzählbar. Das widerspricht jedoch Korollar 24.3.

Lösung 24.2. Bildet man die reelle Zahl r auf die Funktion $x \mapsto r$ ab, so erhält man für jede Zahl eine andere Polynomfunktion aus $\mathbb{R}[x]$. Damit gilt $\mathbb{R} \eqsim \mathbb{R}[x]$. Nach Korollar 24.3 und Lemma 24.2 ist $\mathbb{R}[x]$ daher überabzählbar.

Lösung 24.3. A ist abzählbar, weil durch $m \mapsto m^2$ eine injektive Funktion von A nach $\mathbb{N}$ definiert wird. Für festes $k \in \mathbb{N}^+$ ist $B_k = \{\sqrt[k]{n} : n \in \mathbb{N}^+\}$ abzählbar, weil durch $m \mapsto m^k$ eine injektive Funktion von B_k nach $\mathbb{N}$ definiert wird. Daher ist

$B = \bigcup_{k\in\mathbb{N}^+} B_k$ nach Satz 23.6 ebenfalls abzählbar. C ist eine Teilmenge von $\mathbb{Z}$ und daher abzählbar. D ist überabzählbar, weil bereits die Teilmenge $\mathbb{R}\times\{0\}$ von D offenbar dieselbe Mächtigkeit wie $\mathbb{R}$ hat. E ist überabzählbar, weil bereits die Teilmenge $[1,2)$ von E als echtes Intervall überabzählbar ist. Für jedes $n\in\mathbb{N}$ ist $\mathscr{P}([n])$ endlich (Satz 3.1), also ist F nach Satz 23.6 abzählbar. G ist die leere Menge (siehe Aufgabe 3.15) und daher endlich und insbesondere abzählbar.

Lösung 24.4. Beachten Sie, dass A eine Menge von Zahlen ist, während es sich bei B um eine Menge von Mengen handelt!

A ist *nicht* abzählbar, weil es sich um eine Obermenge der überabzählbaren Menge $[0,1)$ handelt. B ist hingegen abzählbar, denn man kann B offenbar als $\{[0,1)\}\cup C$ mit $C = \{\,[0,1)\cup\{q\} : q\in\mathbb{Q}\setminus[0,1)\,\}$ darstellen. Mit $q\mapsto[0,1)\cup\{q\}$ erhält man eine Injektion von $\mathbb{Q}\setminus[0,1)$ nach C. $\mathbb{Q}\setminus[0,1)$ ist als Teilmenge von $\mathbb{Q}$ abzählbar, damit also auch C, und dann natürlich auch die Menge B, die nur ein Element mehr als C enthält.

Lösung 24.5. Man bildet $A\subseteq\mathbb{N}$ auf die *charakteristische Funktion*

$$\chi_A = \{(k,1) : k\in A\}\cup\{(k,0) : k\in\mathbb{N}\setminus A\}$$

ab. Siehe auch Aufgabe 6.55.

Lösung 25.1. Nein. Als Gegenbeispiel kann man die konstante Funktion $f(x) = c$ nehmen.

Lösung 25.3. Sei $f\colon I\to\mathbb{R}$ stetig und I ein Intervall. Um zu zeigen, dass die Menge $f[I] = \operatorname{rng}(f)$ ein Intervall ist, greifen wir uns zwei Werte r_1, r_2 mit $r_1 < r_2$ aus $f[I]$ und eine Zahl $r\in(r_1,r_2)$ heraus und müssen begründen, warum r ein Element von $f[I]$ ist.

Nach Definition gibt es $x_1, x_2\in I$ mit $f(x_1) = r_1$ und $f(x_2) = r_2$. Weil I ein Intervall ist, liegen alle Werte zwischen x_1 und x_2 ebenfalls in I. Man kann mit $a = \min\{x_1,x_2\}$ und $b = \max\{x_1,x_2\}$ sowie $d = r$ nun Satz 25.3 anwenden.

Lösung 25.5. Der Abstand von a_0 und b_0 ist 4 und durch das fortgesetzte Halbieren ist der Abstand von a_k und b_k somit $2^{-k}\cdot 4 = 2^{2-k}$. Nach dem 15. Schritt ist der Abstand 2^{-13}. (Man hätte natürlich auch einfach $b_{15} - a_{15}$ berechnen können, aber so hat man eine allgemeine Formel.) Die Mitte des Intervalls ist vom richtigen Ergebnis also maximal 2^{-14} entfernt. Das ist ungefähr $6.1\cdot 10^{-5}$ und damit weniger als $5\cdot 10^{-4}$, aber mehr als $5\cdot 10^{-5}$. Man darf also maximal drei Nachkommastellen angeben: -1.167.

Lösung 25.6. Die korrekte Antwort ist 1.40 – und nicht etwa 1.4!

Lösung 25.7. Eine Lösung in PYTHON könnte so aussehen:

```
def zero(f,a,b,n):
    eps = 10**-n
    m = (a+b)/2
    while abs(a-m) > eps:
```

```
        if f(m) == 0:
            return round(m,n)
        if f(a)*f(m) < 0:
            b = m
        else:
            a = m
        m = (a+b)/2
    return round(m,n)

zero(lambda x: x**5-x+1,-2,2,3)
```

Lösung 25.8. Laut Aufgabenstellung kennen wir diese Werte:

x	$1/5$	$1/4$	$1/3$	$1/2$	1
$f(x)$	-32	16	-8	4	-2

Das ist allerdings schon mehr Information als nötig. Eigentlich brauchen wir nur das hier:

x	$1/5$	$1/4$	$1/3$	$1/2$	1
$f(x)$	$-$	$+$	$-$	$+$	$-$

Dabei steht $-$ für $f(x) < 0$ und $+$ für $f(x) > 0$. Da f nach Voraussetzung stetig ist, muss es zwischen $+$ und $-$ bzw. zwischen $-$ und $+$ jeweils mindestens eine Nullstelle geben. Da es vier solche Vorzeichen gibt, muss f mindestens vier Nullstellen haben.

Lösung 26.1. Sei $f(x) = a$ und $g(x) = x$. Dann ergibt sich

$$f'(x_0) = \lim_{x\to x_0} \frac{f(x) - f(x_0)}{x - x_0} = \lim_{x\to x_0} \frac{a - a}{x - x_0} = 0 \quad \text{und}$$
$$g'(x_0) = \lim_{x\to x_0} \frac{g(x) - g(x_0)}{x - x_0} = \lim_{x\to x_0} \frac{x - x_0}{x - x_0} = 1.$$

Lösung 26.2. Man erhält $2x_0$, und zwar so:

$$\lim_{x\to x_0} \frac{x^2 - x_0^2}{x - x_0} = \lim_{x\to x_0} \frac{(x - x_0)(x + x_0)}{x - x_0} = \lim_{x\to x_0} (x + x_0) = 2x_0$$

Lösung 26.3. Die Steigung der Tangente (also der Wert L aus Lemma 26.2) ist (nach Aufgabe 26.2) $2x_0 = -2$. Der Funktionswert $f(x_0)$ ist $(-1)^2 = 1$. Damit erhält man die Gerade $x \mapsto 1 + (-2)(x - (-1)) = -2x - 1$ und man kann durch Einsetzen verifizieren, dass diese Gerade durch den Punkt $(-1, 1)$ geht.

Lösung 26.4. Da 1 die Ableitung von $x \mapsto x$ ist, ergibt sich $1 \cdot x_0 + x_0 \cdot 1 = 2x_0$. Natürlich muss dasselbe herauskommen, was wir schon einmal berechnet hatten.

Lösung 26.5. Dass die Aussage für den trivialen Fall $n = 0$ gilt, hatten wir uns schon überlegt. Mit der Leibnizregel und der Induktionsvoraussetzung für die Ableitung von $x \mapsto x^n$ erhalten wir nun für die Ableitung von $x \mapsto x^{n+1} = x \cdot x^n$

$$1 \cdot x_0^n + (n x_0^{n-1}) \cdot x_0 = x_0^n + n x_0^n = (n + 1) x_0^n.$$

Lösung 26.6. Die Ableitung ist $9x_0^2 - 10x_0 + 8$.

Lösung 26.7. So geht es los:

$$\begin{aligned} f(x) &= 3x^3 - 5x^2 + 8x - 2 \\ f^{(1)}(x) = f'(x) &= 9x^2 - 10x + 8 \\ f^{(2)}(x) = f''(x) &= 18x - 10 \\ f^{(3)}(x) &= 18 \\ f^{(4)}(x) &= 0 \end{aligned}$$

Alle weiteren Ableitungen sind ebenfalls die konstante Nullfunktion.

Lösung 26.8. Mit der Leibnizregel erhält man

$$\begin{aligned} f'(x) &= (2x)(x^3 - x) + (x^2 + 3)(3x^2 - 1) = 2x^4 - 2x^2 + 3x^4 + 9x^2 - x^2 - 3 \\ &= 5x^4 + 6x^2 - 3. \end{aligned}$$

Die alternative Berechnung liefert

$$\begin{aligned} f(x) &= (x^2 + 3)(x^3 - x) = x^5 + 3x^3 - x^3 - 3x = x^5 + 2x^3 - 3x \quad \text{und} \\ f'(x) &= 5x^4 + 6x^2 - 3. \end{aligned}$$

Natürlich muss in beiden Fällen dasselbe herauskommen!

Lösung 26.9. x^{-3} ist der Kehrwert von x^3 und die Ableitung von x^3 ist (nach Aufgabe 26.5) $3x^2$. Damit ergibt sich

$$f'(x) = \frac{-3x^2}{(x^3)^2} = -3x^{-4}.$$

Lösung 26.10. Man muss das nur noch für negative Zahlen beweisen. Sei also $n \in \mathbb{N}^+$. Wir wissen schon, dass nx^{n-1} die Ableitung von x^n ist. Für $f(x) = x^{-n}$ gilt dann

$$f'(x) = \frac{-nx^{n-1}}{(x^n)^2} = \frac{-nx^{n-1}}{x^{2n}} = -nx^{n-1-2n} = -nx^{-n-1}.$$

Lösung 26.12. Die Ableitung des Zählers ist $2x + 2$, die des Nenner $6x$. Damit ergibt sich insgesamt

$$f'(x) = \frac{(2x+2)(3x^2-2) - (x^2+2x+2)6x}{(3x^2-2)^2} = -\frac{6x^2 + 16x + 4}{9x^4 - 12x^2 + 4}.$$

Lösung 26.14. Wir haben hier $h = f \circ g$ mit $g(x) = 3x^2 - 5x + 2$ und $f(x) = x^4$. Die „äußere“ Ableitung ist $f'(x) = 4x^3$, die „innere“ $g'(x) = 6x - 5$. Damit ergibt sich

$$h'(x) = 4(3x^2 - 5x + 2)^3(6x - 5) = (3x^2 - 5x + 2)^3(24x - 20).$$

Lösung 26.15. Die Ableitung ist gemäß (26.5)

$$(f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))} = \frac{1}{f'(\sqrt[n]{y})} = \frac{1}{n(\sqrt[n]{y})^{n-1}} = \frac{1}{n\sqrt[n]{y^{n-1}}}.$$

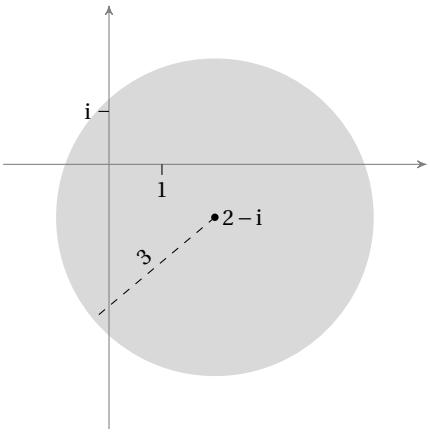
Welchen der letzten beiden Terme man einfacher bzw. „schöner“ findet, ist Geschmackssache.

Lösung 26.16. $f^{-1}(x)$ hat dann die Form $x^{1/n}$ und aus der Ableitung wird

$$(f^{-1})'(y) = \frac{1}{n} \cdot y^{-(n-1)/n} = \frac{1}{n} \cdot y^{\frac{1}{n}-1}.$$

Lösung 27.1. Der Entwicklungspunkt ist -3. Der Abstand zwischen 1 und -3 ist größer als der Konvergenzradius 2, also konvergiert die Reihe für $z = 1$ nicht. Das gilt „erst recht“ für $z = 2$. Für $z = -4$ konvergiert die Reihe, weil der Abstand zu -3 kleiner als 2 ist. Für $z = -1$ kann man auf der Basis der Informationen aus der Aufgabenstellung keine definitive Aussage machen, weil der entsprechende Abstand exakt 2 ist. Das gilt ebenso für $z = -3 + 2\mathrm{i}$.

Lösung 27.2. Der Entwicklungspunkt ist $2 - \mathrm{i}$. Daher sollte es so aussehen:



Die Reihe wird also beispielsweise konvergieren, wenn man $z = \mathrm{i}$ setzt, weil i im Inneren des Kreises liegt. Und sie wird *nicht* konvergieren, wenn man $z = 5$ setzt. Der Abstand von 5 zum Entwicklungspunkt ist (ein bisschen) größer als 3.

Lösung 27.3. Man kann auf zwei Arten zum Ergebnis kommen. Die eine ist, dass man die einzelnen Reihenglieder differenziert, wie man es auch im besagten Satz macht. Nach der Kettenregel hat $a_n(z - z_0)^n$ die Ableitung $na_n(z - z_0)^{n-1}$, weil die „innere“ Ableitung einfach 1 ist. Die zweite Variante ist, dass man (27.1) als $f(z - z_0)$ betrachtet, wobei $f(z) = \sum_{n=0}^{\infty} a_n z^n$ gilt. Man würde dann (wieder mit der Kettenregel) als Ableitung $f'(z - z_0)$ erhalten. In beiden Fällen ist das Ergebnis jedenfalls $\sum_{n=0}^{\infty} na_n(z - z_0)^{n-1}$ mit demselben Entwicklungspunkt und demselben Konvergenzradius.

Lösung 28.1. $\exp(0)$ ist 1, weil in diesem Fall alle Reihenglieder bis auf das erste verschwinden. Für e erhält man

$$\mathrm{e} = \exp(1) \approx 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} = 65/24 \approx 2.70833.$$

Wenn man wie hier nach k Summanden abbricht, dann gilt für den fehlenden Teil der Reihensumme

$$\sum_{n=k}^{\infty} \frac{1}{n!} = \frac{1}{k!} \sum_{n=k}^{\infty} \frac{k!}{n!} = \frac{1}{k!} \sum_{n=k}^{\infty} \frac{1}{(k+1)(k+2)\cdots n}$$
$$\leq \frac{1}{k!} \sum_{n=0}^{\infty} \frac{1}{(k+1)^n} = \frac{1}{k!} \cdot \frac{1}{1-1/(k+1)} = \frac{1}{k!} \cdot \frac{k+1}{k}.$$

Im konkreten Fall $k = 5$ ist der Fehler also höchstens $1/100$ und daher wäre 2.7 eine sichere Rundung. (Der tatsächliche Wert von e auf zehn Stellen nach dem Komma gerundet ist 2.718281828. Da diese Zahl irrational ist, kann man immer nur Näherungswerte angeben.)

Lösung 28.2. Für das Quotientenkriterium betrachten wir für festes $z \in \mathbb{C}$ den Quotienten zweier aufeinanderfolgender Reihenglieder und erhalten

$$\frac{z^{n+1}}{(n+1)!} \Big/ \frac{z^n}{n!} = \frac{z^{n+1}}{(n+1)!} \cdot \frac{n!}{z^n} = \frac{z}{n+1}. \tag{L-5}$$

Die Folge $(z/(n+1))_{n\in\mathbb{N}}$ ist bis auf den konstanten Faktor z im Prinzip die harmonische Folge, die gegen null konvergiert. Also sind fast alle Terme der Form (L-5) z. B. kleiner als $1/2$.

Lösung 28.3. In beiden Fällen muss man die Kettenregel verwenden. Im ersten Fall erhält man $2x\exp(x^2)$. Im zweiten Fall werden die Rollen von „äußerer“ und „innerer“ Funktion vertauscht und man erhält $2\exp(x)^2$.

Lösung 28.4. Beispiele wären $2\exp(x)$ oder $\exp(x+42)$. Generell ist jede Funktion der Form $x \mapsto a\exp(x+b)$ mit Konstanten a und b ihre eigene Ableitung.

Lösung 28.6. Für den Induktionsanfang muss man verifizieren, dass (28.3) korrekt ist, wenn man $n = 0$ einsetzt. Das ist offenbar der Fall:

$$(a+b)^0 = 1 = \binom{0}{0} a^0 b^{0-0} = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$$

Der Induktionsschluss sieht dann so aus:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n}{n} a^{n+1} b^0 + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + \binom{n}{0} a^0 b^{n+1} \\
&= \binom{n+1}{n+1} a^{n+1} b^0 + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + \binom{n+1}{0} a^0 b^{n+1}
\end{aligned}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

Bei der ersten Gleichheit wurde die Induktionsvoraussetzung angewendet, weiter unten dann Eigenschaften des Binomialkoeffizienten, die aus der Schule bekannt sein sollten. Zur Wiederholung eignen sich z. B. die Videos *Binomialkoeffizienten* und *Das Pascalsche Dreieck*.

Lösung 28.7. Nach dem binomischen Lehrsatz gilt

$$(x+1)^{19} = \sum_{k=0}^{19} \binom{19}{k} x^k 1^{19-k} = \sum_{k=0}^{19} \binom{19}{k} x^k$$

und damit ist die Antwort $\binom{19}{13} = 27\,132$.

Lösung 28.8. Nach Lemma 10.4 muss einer der beiden Faktoren verschwinden, damit sich null ergibt. Da nach Lemma 28.6 der zweite Faktor aber niemals verschwindet, kann nur null herauskommen, wenn $2x-6=0$ gilt. Die einzig mögliche Lösung ist also $x=3$.

Lösung 28.9. Für $x \geq 0$ gilt offenbar $\exp(x) \geq 1+x$. (Dafür muss man nur die ersten beiden Reihenglieder summieren.) Damit gilt „erst recht“ $\exp(x) > x$ für jedes $x > 1$ und nach Satz 28.7 $\exp(-x) = 1/\exp(x) < 1/x$. Weil exp nach Lemma 28.2 und Korollar 26.3 stetig ist, gehören nach dem Zwischenwertsatz alle Elemente von $[1/x, x]$ zum Wertebereich. Weil x beliebig war, ist die Behauptung damit bewiesen, denn es gilt $\bigcup\{[1/x, x] : x \in (1,\infty)\} = (0,\infty)$.

Lösung 28.10. Zunächst sei an Aufgabe 21.20 erinnert. Dort wurde begründet, dass f überhaupt eine Umkehrfunktion hat. Wäre f^{-1} *nicht* streng monoton steigend, dann gäbe es x und y aus dem Wertebereich von f mit $x < y$ und $f^{-1}(x) \geq f^{-1}(y)$. Auf diese Werte kann man aber f anwenden und wegen der strengen Monotonie von f folgt

$$x = f(f^{-1}(x)) \geq f(f^{-1}(y)) = y,$$

was offenbar ein Widerspruch ist.

Lösung 28.11. Wieder ein Fall für die Kettenregel. Es ergeben sich $2x/(x^2+1)$ und $(2\ln x)/x$.

Lösung 28.12. Man kann den Beweis von Lemma 28.9 einfach kopieren:

$$\exp(\ln x_1 - \ln x_2) = \exp(\ln x_1)\exp(-\ln x_2) = \exp(\ln x_1)/\exp(\ln x_2) = x_1/x_2.$$

Man beachte, dass damit insbesondere auch $\ln(1/x) = -\ln x$ gilt.

Lösung 28.13. Man muss wirklich nur einsetzen. Daher werden hier exemplarisch nur (i) und (v) vorgerechnet.

$$a^r \cdot a^s = \exp(r\ln a)\exp(s\ln a) = \exp(r\ln a + s\ln a) = \exp\big((r+s)\ln a\big) = a^{r+s}$$
$$(a^r)^s = \exp(r\ln a)^s = \exp\big(s\ln\exp(r\ln a)\big) = \exp(sr\ln a) = a^{sr}$$

 CC BY-NC-ND 3.0 DE

Lösung 28.14. Für $a > 1$ gilt $\ln a > 0$. Aus $x_1 < x_2$ folgt dann $x_1 \ln a < x_2 \ln a$ und damit hat man

$$a^{x_1} = \exp(x_1 \ln a) < \exp(x_2 \ln a) = a^{x_2},$$

weil die Exponentialfunktion nach Lemma 28.6 auf $\mathbb{R}$ streng monoton steigt. Für $0 < a < 1$ folgt die Behauptung analog mit $\ln a < 0$.

Lösung 28.15. Nach Definition geht es um die Funktion $x \mapsto \exp(r \ln x)$. Mit der Kettenregel und Lemma 28.8 erhält man als Ableitung

$$r/x \cdot \exp(r \ln x) = r/x \cdot x^r = r x^{r-1}.$$

Lemma 26.9 gilt also auch dann noch, wenn man q durch eine beliebige reelle Zahl r ersetzt.

Lösung 28.16. Nach Definition geht es um die Funktion $x \mapsto \exp(x \ln a)$ und da muss man mal wieder die Kettenregel anwenden. Als Ableitung ergibt sich

$$\ln a \exp(x \ln a) = (\ln a) a^x.$$

Lösung 28.17. Ihnen ist hoffentlich klar, dass $2^6 = 64$ und $10^5 = 100\,000$ gilt. Daher sind die Antworten 6 und 5.

Lösung 28.18. Man wendet Lemma 28.11 an und braucht sogar nur eine der beiden Funktionen. Entweder $\log_{10} 42 / \log_{10} 7$ oder $\ln 42 / \ln 7$.

Lösung 28.19. Es ergibt sich $a = 1/\sqrt{500}$, $b = \sqrt{5} \cdot \sqrt{500} = \sqrt{2500} = 50$ und schließlich $c = \log_{10} 20b = \log_{10} 1000 = 3$.

Lösung 28.20. Nach Definition gilt $x = c^b$. Nach den bekannten Rechenregeln aus Lemma 28.10 folgt $x^{-2/b} = (c^b)^{-2/b} = c^{-2} = 1/c^2$. Welchen der beiden letzten Ausdrücke man als einfacher oder schöner ansieht, ist Geschmackssache.

Lösung 28.21. Wendet man auf beide Seiten $\log_a$ an, so erhält man mit Lemma 28.11

$$x = \log_a(5/a^2) = \log_a 5 - \log_a a^2 = (\log_a 5) - 2.$$

Alternativ kann man auch erst die Gleichung mit a^2 multiplizieren und dann den Logarithmus anwenden. Das führt über $a^{x+2} = 5$ zu $x + 2 = \log_a 5$, also natürlich zum selben Ergebnis.

Lösung 28.22. Nach dem Lemma 28.11 gilt $\log_a x = \ln x / \ln a$. Nach Lemma 28.8 ist die Ableitung daher $1/(x \ln a)$.

Lösung 29.1. Das sind $2x \cos(x^2 + 1)$ und $\cos x / \sin x$. Die zweite Funktion wird auch als Kotangens bezeichnet.

Lösung 29.2. Nach der Quotientenregel erhält man (in Kurzschreibweise)

$$\tan' = \frac{\sin' \cos - \sin \cos'}{\cos^2} = \frac{\cos^2 + \sin^2}{\cos^2}.$$

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Das kann man auf zwei Arten vereinfachen: entweder durch Kürzen zu $1+\tan^2$ oder mit dem später bewiesenen Satz des Pythagoras zu $1/\cos^2$. Welche Form man bevorzugt, ist Geschmackssache.

Lösung 29.3. Nach dem besagten Lemma hat man

$$\cos(7\pi/6) = \cos(\pi+\pi/6) = \cos(\pi-\pi/6) = \cos(5\pi/6) \quad \text{und}$$
$$\cos(5\pi/6) = \cos(\pi/2+\pi/3) = -\cos(\pi/2-\pi/3) = -\cos(\pi/6).$$

Das Ergebnis ist übrigens $-\sqrt{3}/2$.

Lösung 29.4. Nach Lemma 29.12 ist das

$$\sin(5\pi/9) = \sin(\pi/18+\pi/2) = \cos(\pi/18).$$

Lösung 29.5. Simple Rechnerei:

$$\begin{aligned}
\cos(z+2\pi) &= \cos z\cos 2\pi - \sin 2\pi \sin z = 1\cdot\cos z - 0\cdot\sin z = \cos z\\
\sin(z+2\pi) &= \sin z\cos 2\pi + \sin 2\pi\cos z = 1\cdot\sin z + 0\cdot\cos z = \sin z\\
\cos(z+\pi/2) &= \cos z\cos(\pi/2) - \sin z\sin(\pi/2) = 0\cdot\cos z - 1\cdot\sin z\\
&= -\sin z\\
\sin(z+\pi/2) &= \sin z\cos(\pi/2) + \sin(\pi/2)\cos z = 0\cdot\sin z + 1\cdot\cos z\\
&= \cos z\\
-\cos(\pi/2-z) &= -\cos z\cos(\pi/2) - \sin z\sin(\pi/2) = -0\cdot\cos z - 1\cdot\sin z\\
&= -\sin z = \cos(z+\pi/2)\\
\cos(\pi+z) &= \cos z\cos\pi - \sin z\sin\pi = -1\cdot\cos z - 0\cdot\sin z = -\cos z\\
\cos(\pi-z) &= \cos z\cos\pi + \sin z\sin\pi = -1\cdot\cos z + 0\cdot\sin z = -\cos z
\end{aligned}$$

Lösung 29.6. Das war so gemeint:

$$\cos 2z = \cos(z+z) = \cos^2 z - \sin^2 z = 2\cos^2 z - \cos^2 z - \sin^2 z = 2\cos^2 z - 1$$

Man kann das auch nach $\cos z$ auflösen und erhält dann $\cos t = 1/2\cdot\sqrt{2+2\cos 2t}$. Letzteres stimmt allerdings wegen der Wurzel nur für $t\in\mathbb{R}$ und $\cos t\geq 0$, nach dem Beweis von Satz 29.8 also unter anderem für $t\in[0,\pi/2]$.

Lösung 29.7. Der „Witz“ an der Formel ist, dass man für das Argument t das Wissen über das doppelt so große Argument $2t$ verwenden und sich so nach und nach zu immer kleineren Argumenten vorarbeiten kann.

$$\cos\left(\frac{\pi}{4}\right) = \frac{1}{2}\cdot\sqrt{2+2\cos\left(\tfrac{\pi}{2}\right)} = \frac{1}{\sqrt{2}}$$
$$\cos\left(\frac{\pi}{8}\right) = \frac{1}{2}\cdot\sqrt{2+2\cos\left(\tfrac{\pi}{4}\right)} = \frac{\sqrt{2+\sqrt{2}}}{2}$$

Man könnte nun also fortfahren und den Kosinus für Argumente wie $\pi/16$ berechnen. Aber auch für andere Zahlen erhält man auf diesem Weg Ergebnisse. In dem Video *Wie hat man früher Sinus und Kosinus berechnet?* wird das Verfahren beschrieben.

Lösung 29.8. Wir wissen aus dem Beweis von Satz 29.8, dass der Kosinus von 0 bis $\pi/2$ streng monoton von 1 auf 0 fällt. Wegen $\cos 0 = 1$ und $\cos 1 - 1 < 0$ folgt aus dem Zwischenwertsatz, dass es mindestens eine Lösung gibt. Wegen der strengen Monotonie der beiden Funktionen folgt die Eindeutigkeit. Mit dem Bisektionsverfahren erhält man 0.74.

Lösung 29.9. Wäre f ungerade, so könnte man die Tabelle aus der Lösung von Aufgabe 25.8 erweitern:

x	-1	$-1/2$	$-1/3$	$-1/4$	$-1/5$	$1/5$	$1/4$	$1/3$	$1/2$	1
$f(x)$	$+$	$-$	$+$	$-$	$+$	$-$	$+$	$-$	$+$	$-$

Damit hat man neun Vorzeichenwechsel und deshalb muss f mindestens neun Nullstellen haben. (Und was käme heraus, wenn f gerade wäre?)

Lösung 30.1. Nach Korollar 29.7 gilt $\cos^2 z = 1 - \sin^2 z$ für alle $z \in \mathbb{C}$. Damit folgt $\cos x = \sqrt{1 - \sin^2 x}$ für $x \in \mathbb{R}$, *wenn* $\cos x$ nicht negativ ist. Das ist insbesondere für $x \in [-\pi/2, \pi/2]$ der Fall. Es folgt

$$\arcsin'(x) = \frac{1}{\cos \arcsin x} = \frac{1}{\sqrt{1 - \sin^2 \arcsin x}} = \frac{1}{\sqrt{1 - x^2}}.$$

Analog erhält man

$$\arccos'(x) = \frac{1}{-\sin \arccos x} = -\frac{1}{\sqrt{1 - \cos^2 \arccos x}} = -\frac{1}{\sqrt{1 - x^2}}.$$

Auch in diesem Fall ist die Wurzel nur deshalb korrekt, weil „zufällig“ der Sinus auf dem Intervall $[0, \pi]$ nicht negativ wird.

Lösung 30.2. Dass der Kosinus auf $[0, \pi/2]$ injektiv ist, folgt aus dem Beweis von Satz 29.8. Die Injektivität auf $[0, \pi]$ folgt dann mit Lemma 29.13. Die Aussage für den Sinus folgt schließlich mit Lemma 29.12.

Lösung 30.3. Der Arkussinus liefert nur Werte zwischen $-\pi/2$ und $\pi/2$, so dass die „naive“ Formel $t = \arcsin(y/r)$ nur für komplexe Zahlen rechts von der imaginären Achse richtig wäre. Nutzt man die Zusammenhänge $\sin(\pi/2 + x) = \sin(\pi/2 - x)$ und $\sin(-\pi/2 + x) = \sin(-\pi/2 - x)$ aus,[60] dann erhält man

$$t = \begin{cases} \arcsin(y/r) & x \geq 0 \\ \pi - \arcsin(y/r) & x < 0 \wedge y \geq 0 \\ -\pi - \arcsin(y/r) & x < 0 \wedge y < 0 \end{cases},$$

wobei diese Formel sogar noch etwas komplizierter als die für arccos ist, weil man nach der Definition des Arguments dafür sorgen muss, dass t zwischen $-\pi$ und π liegt.

[60] Diese Gleichungen besagen, dass der Sinus gerade wäre, wenn die vertikale Achse durch $x = \pi/2$ bzw. $x = -\pi/2$ verliefe. Und das stimmt ja auch wegen der Phasenverschiebung.

Lösung 30.4. Das ist wieder ein Job für die Umkehrregel:

$$\arctan'(x) = \frac{1}{1+\tan^2 \arctan x} = \frac{1}{1+x^2}.$$

Es ist in gewissem Sinne erstaunlich, dass eine Umkehrfunktion einer über eine Reihe definierten Funktion eine so einfache Ableitung hat, die sich mithilfe der Grundrechenarten darstellen lässt.

Lösung 30.5. Der Absolutbetrag von z ist $|z| = \sqrt{5^2+3^2}$. Für das Argument kann man den Imaginärteil 3 durch den Realteil -5 dividieren und auf den Quotienten den Arkustangens anwenden. Man muss aber beachten, dass $\arctan(-3/5)$ das Argument von $5-3\mathrm{i}$ statt von z wäre; richtig ist in diesem Fall $\arctan(-3/5)+\pi$. (Wie so oft hilft eine kleine Skizze. Wenn Sie sehen, in welchem Quadranten z liegt, dann wird klar, dass der Winkel $\arctan(-3/5)$, also ungefähr $-31°$, nicht richtig sein kann.)

Mit dem Taschenrechner erhalten wir (gerundet) den Betrag 5.831 und das Argument 2.601. Die gesuchte Polardarstellung ist somit $z \approx 5.831\,\mathrm{e}^{2.601\,\mathrm{i}}$.

Für die Polardarstellung von z^3 erinnern wir uns daran (siehe Seite 176), wie man die Multiplikation komplexer Zahlen geometrisch interpretieren kann. Damit folgt sofort $|z^3| = |z|^3 = \sqrt{34^3} \approx 198.252$. Analog ergibt sich das Argument von z^3 durch Verdreifachen des Argumentes von z. Allerdings liegt das (gerundete) Ergebnis 7.804 dieser Multiplikation außerhalb des Intervalls $(-\pi,\pi]$ und wir sollten daher noch $2\pi = 360°$ subtrahieren: $\arg(z^3) \approx 1.520$. (Man hätte natürlich auch erst z^3 berechnen und dann wie im ersten Teil weitermachen können. Aber so ist der Rechenaufwand wohl geringer.)

Lösung 30.6. Die Ableitungsfunktion kann man mit der Leibnizregel oder mit der Kettenregel berechnen. In beiden Fällen ergibt sich $f'(x) = 2\sin x \cos x$. Mit einem Taschenrechner ergibt sich gerundet $f'(6/5) \approx 0.68$. Man hat nun ein Steigungsdreieck (siehe Skizze auf Seite 252) mit der waagerechten Kathete 1 und der senkrechten Kathete $f'(6/5)$. Mit dem Arkustangens kommt man so auf den Steigungswinkel $\varphi = \arctan(f'(6/5)) \approx 0.59$.

Hier kann man übrigens beobachten, dass man nicht zu früh runden sollte. Setzt man im letzten Schritt für $f'(6/5)$ den gerundeten Wert 0.68 ein, so erhält man – gerundet auf zwei Stellen nach dem Komma – $\arctan(0.68) \approx 0.60$.

Lösung 31.1. Bei dieser Aufgabe geht es hauptsächlich darum, sich erstens die Bedeutung der Definition vor Augen zu führen und sich zweitens klarzumachen, dass es sehr einfach ist, diese Eigenschaften nachzuprüfen. (Und genauso einfach ist es für Räume der Form K^n.) Aus didaktischen Gründen wird das hier noch einmal Schritt für Schritt vorgeführt, aber Sie haben es hoffentlich selbst schon aufgeschrieben. Die Rolle von $\mathbf{u}$ und $\mathbf{v}$ spielen die Paare (u_1,u_2) und (v_1,v_2). Alle Buchstaben in der folgenden Rechnung stehen für beliebige reelle Zahlen.

$$\begin{aligned}\alpha \odot \big((u_1,u_2) \oplus (v_1,v_2)\big) &= \alpha \odot (u_1+v_1, u_2+v_2) = \big(\alpha\cdot(u_1+v_1), \alpha(u_2+v_2)\big)\\ &= (\alpha u_1 + \alpha v_1, \alpha u_2 + \alpha v_2) = (\alpha u_1, \alpha u_2) \oplus (\alpha v_1, \alpha v_2)\end{aligned}$$

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

$$
\begin{aligned}
&= \big(\alpha \odot (u_1, u_2)\big) \oplus \big(\alpha \odot (v_1, v_2)\big) \\
(\alpha+\beta) \odot (v_1, v_2) &= \big((\alpha+\beta)\cdot v_1, (\alpha+\beta)\cdot v_2\big) = (\alpha v_1 + \beta v_1, \alpha v_2 + \beta v_2) \\
&= (\alpha v_1, \alpha v_2) \oplus (\beta v_1, \beta v_2) \\
&= \big(\alpha \odot (v_1, v_2)\big) \oplus \big(\beta \odot (v_1, v_2)\big) \\
(\alpha\cdot\beta) \odot (v_1, v_2) &= \big((\alpha\cdot\beta)\cdot v_1, (\alpha\cdot\beta)\cdot v_2\big) = \big(\alpha\cdot(\beta\cdot v_1), \alpha\cdot(\beta\cdot v_2)\big) \\
&= \alpha \odot (\beta\cdot v_1, \beta\cdot v_2) = \alpha \odot \big(\beta \odot (v_1, v_2)\big) \\
1 \odot (v_1, v_2) &= (1\cdot v_1, 1\cdot v_2) = (v_1, v_2)
\end{aligned}
$$

Lösung 31.2. Das sollte hoffentlich keine Schwierigkeiten bereiten.

$$
\begin{aligned}
(4,3) \oplus (2,4) &= (4+2, 3+4) = (1,2) \\
3 \odot (2,4) &= (3\cdot 2, 3\cdot 4) = (1,2)
\end{aligned}
$$

Lösung 31.3. Nach Definition muss für jedes $\alpha \in K$ der Ausdruck $\alpha \odot \mathbf{0}$ ein Vektor sein. Weil es nur einen Vektor gibt, bleibt nur die Möglichkeit $\alpha \odot \mathbf{0} = \mathbf{0}$. Das ist schon alles.

Lösung 31.6. Gilt $a = b = 0$, dann ist $\{(\lambda a, \lambda b) : \lambda \in \mathbb{R}\}$ zwar ein Untervektorraum von $\mathbb{R}^2$, aber keine Gerade, sondern der triviale Untervektorraum $\{(0,0)\}$.

Lösung 31.7. Es handelt sich um die Menge $\{(\alpha, \beta, 0) : \alpha, \beta \in \mathbb{R}\}$. Man erhält jeden Vektor der Form $(\alpha, \beta, 0)$ als Linearkombination $\alpha \cdot (1,0,0) + \beta/2 \cdot (0,2,0)$.

Lösung 31.8. Es handelt sich um die Menge $\{(\alpha, 0) : \alpha, \in \mathbb{R}\}$. Einer der beiden aufspannenden Vektoren ist quasi überflüssig.

Lösung 31.9. Die Menge $\mathbb{R}[x]$ aller Polynomfunktionen über $\mathbb{R}$.

Lösung 31.10. Nein, ist es nicht. Nach der Definition müssten eigentlich auch Summen mit weniger als k Summanden berücksichtigt werden. Das ist aber nicht wirklich nötig, weil man in solchen Summen vor die „fehlenden“ Vektoren den Skalar 0 setzen kann. Ist konkret $K = \mathbb{R}$ und $k = 3$, so kann man z. B. $\alpha_1 \mathbf{w}_1 + \alpha_3 \mathbf{w}_3$ als $\alpha_1 \mathbf{w}_1 + 0\,\mathbf{w}_2 + \alpha_3 \mathbf{w}_3$ schreiben.

Lösung 31.11. Es ist der Nullvektor, denn es gilt natürlich immer $1 \cdot \mathbf{0} = \mathbf{0}$.

Lösung 31.12. Wie wäre es mit diesen beiden?

$$
\begin{aligned}
(6,6,0) &= 6\cdot(1,0,0) + 3\cdot(0,2,0) \\
(6,6,0) &= 6\cdot(1,0,0) + 3\cdot(0,2,0) + 0\cdot(0,0,3)
\end{aligned}
$$

Falls Sie das als Schummelei empfinden: Es ging um die präzise Formulierung. Die zweite Linearkombination ist nicht reduziert, aber das war nicht gefragt.

Lösung 31.13. Hier sind gleich drei Beispiele:

$$
\begin{aligned}
(6,6) &= 6\cdot(1,1) \\
(6,6) &= 3\cdot(2,0) + 2\cdot(0,3) \\
(6,6) &= 3\cdot(1,1) + 3/2\cdot(2,0) + 1\cdot(0,3)
\end{aligned}
\tag{L-6}
$$

Offenbar gibt es unendlich viele Möglichkeiten.

Ihre Antwort hätte übrigens auch so aussehen können:

$$\begin{aligned}(6,6) &= 3\cdot(2,0)+2\cdot(0,3)\\ (6,6) &= 2\cdot(0,3)+3\cdot(2,0)\end{aligned} \tag{L-7}$$

Das entsprach zwar nicht dem Sinn der Aufgabe, aber durch die Formulierung wurde es auch nicht ausgeschlossen.

Lösung 31.14. Aus

$$(0,0,0) = \alpha\cdot(1,0,0)+\beta\cdot(0,2,0)+\gamma\cdot(0,0,3) = (\alpha,2\beta,3\gamma)$$

folgt offenbar sofort $\alpha=\beta=\gamma=0$. Daher ist X linear unabhängig. Sind umgekehrt α, β und γ beliebig, so gilt

$$(\alpha,\beta,\gamma) = \alpha\cdot(1,0,0)+\beta/2\cdot(0,2,0)+\gamma/3\cdot(0,0,3)$$

und damit ist klar, dass X den Raum $\mathbb{R}^3$ aufspannt.

Lösung 31.15. Weil B' echte Obermenge ist, gibt es einen Vektor $\mathbf{w}\in B'\setminus B$. Weil B den Raum V aufspannt, gibt es $\mathbf{v}_i\in B$ und $\alpha_i\in K\setminus\{0\}$ mit $\mathbf{w}=\sum_{i=1}^n\alpha_i\mathbf{v}_i$. Damit folgt dann die Darstellung $1\cdot\mathbf{w}-\sum_{i=1}^n\alpha_i\mathbf{v}_i$ des Nullvektors als reduzierte Linearkombination.

Lösung 31.16. Weil B' echte Teilmenge ist, gibt es einen Vektor $\mathbf{w}\in B\setminus B'$. Würde B' den ganzen Raum aufspannen, dann gäbe es Vektoren $\mathbf{v}_i\in B'$ und Skalare $\alpha_i\in K\setminus\{0\}$ mit $\mathbf{w}=\sum_{i=1}^n\alpha_i\mathbf{v}_i$. Man hätte wieder die Darstellung $1\cdot\mathbf{w}-\sum_{i=1}^n\alpha_i\mathbf{v}_i$ des Nullvektors als reduzierte Linearkombination im Widerspruch dazu, dass B linear unabhängig ist.

Lösung 31.17. Die Basis dieses Vektorraums ist die leere Menge – siehe Fußnote 8 auf Seite 289. Daher ist die Dimension 0.

Lösung 31.18. Nach Satz 31.6 kann keine Teilmenge von U mit mehr als n Elementen linear unabhängig sein. Es gibt also eine Teilmenge $C=\{\mathbf{c}_1,\ldots,\mathbf{c}_k\}$ von U mit $k\le n$ Elementen, die linear unabhängig ist und die Eigenschaft hat, dass $C\cup\{\mathbf{u}\}$ für jedes $\mathbf{u}\in U\setminus C$ linear abhängig ist.

Für jedes $\mathbf{u}\in U\setminus C$ gibt es demnach eine Darstellung

$$\mathbf{0} = \alpha\mathbf{u}+\sum_{i=1}^{k}\alpha_i\mathbf{c}_i,$$

so dass nicht alle Skalare verschwinden. Insbesondere kann α nicht null sein, denn sonst wäre C linear abhängig. Damit kann man nach $\mathbf{u}$ auflösen und erhält eine Darstellung von $\mathbf{u}$ als Linearkombination über C. Also ist C eine Basis von U.

Man kann so eine Menge C rekursiv erzeugen, indem man mit der leeren Menge beginnt und so lange Elemente hinzufügt, bis das nicht mehr möglich ist. Nach spätestens n Schritten muss das passieren. Alternativ kann man statt mit der leeren Menge auch mit einer linear unabhängigen Teilmenge von U anfangen. Diese Aussage wird auch *Basisergänzungssatz* genannt.

Basisergänzungssatz

Lösung 31.19. Dass es nur einen Untervektorraum der Dimension 0 gibt, ist klar, weil es nur eine Basis der Mächtigkeit null gibt. Ist U ein Untervektorraum von V, der eine Basis $C = \{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$ mit n Elementen hat, so ist nach Satz 31.6 $C \cup \{\mathbf{v}\}$ für jeden Vektor $\mathbf{v} \in V \setminus C$ linear abhängig. Wie in der Lösung von Aufgabe 31.18 folgt daraus $\mathbf{v} \in \langle C \rangle$.

Lösung 31.20. Hat der Raum die Dimension 7, so gibt es eine Basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_7\}$ mit 7 Elementen. $\langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \rangle$ ist dann ein Beispiel (eines von vielen!) für einen Untervektorraum der Dimension 3.

Lösung 31.21. In der Definition wird gefordert, dass Definitions- und Zielmenge einer linearen Abbildung Vektorräume über *demselben* Körper sind. Alles andere würde auch keinen Sinn ergeben, weil der Skalar α in der Definition in beiden Vektorräumen verwendet wird.

Lösung 31.22. Dass die Komposition eine Funktion von V_1 nach V_3 ist, ist klar. Wir müssen lediglich zeigen, dass $f_2 \circ f_1$ linear ist. Das ist zum Glück ganz einfach. Für $\mathbf{v} \in V_1$ und $\alpha \in K$ gilt $f_1(\alpha \mathbf{v}) = \alpha f_1(\mathbf{v})$, weil f_1 linear ist, und $f_2(\alpha f_1(\mathbf{v})) = \alpha f_2(f_1(\mathbf{v}))$, weil f_2 linear ist. Beides zusammen ergibt $(f_2 \circ f_1)(\alpha \mathbf{v}) = \alpha (f_2 \circ f_1)(\mathbf{v})$. Die zweite Bedingung für die Linearität weist man analog nach.

Lösung 31.23. $f\big((3,2)\big) = 3f(\mathbf{e}_1) + 2f(\mathbf{e}_2) = 3 \cdot (2,1) + 2 \cdot (2,-4) = (10,-5)$.

Lösung 31.24. $f\big((3,2)\big) = 3f(\mathbf{e}_1) + f(2\mathbf{e}_2) = 3 \cdot (2,1) + (2,-4) = (8,-1)$.

Lösung 31.25. Sie wollen α und β mit $(3,1) = \alpha \cdot (2,1) + \beta \cdot (0,2)$ finden. Das ergibt das lineare Gleichungssystem, das aus den Gleichungen $3 = 2\alpha$ und $1 = \alpha + 2\beta$ besteht. Die erste Gleichung liefert $\alpha = 3/2$ und die zweite $\beta = (1-\alpha)/2 = -1/4$. Es folgt $f\big((3,1)\big) = 3/2 \cdot f\big((2,1)\big) - 1/4 f\big((0,2)\big) = 3/2 \cdot (3,2) - 1/4 \cdot (1,-5) = 17/4 \cdot (1,1)$.

Lösung 31.26. $f\big((3,-2,8)\big)$ ist die Funktion $x \mapsto 3 - 2x + 8x^2$ und der Wertebereich von f ist die Menge aller Polynomfunktionen über $\mathbb{R}$, deren Grad nicht größer als 2 ist.

Lösung 32.1. Die Ergebnisse sind

$$\mathbf{A} + \mathbf{B} = \begin{pmatrix} 5+4 & 2+1 & 0+4 \\ 3+4 & 1+6 & 4+5 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{und}$$

$$5 \cdot \mathbf{A} = \begin{pmatrix} 5 \cdot 5 & 5 \cdot 2 & 5 \cdot 0 \\ 5 \cdot 3 & 5 \cdot 1 & 5 \cdot 4 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 0 \\ 1 & 5 & 6 \end{pmatrix}.$$

Lösung 32.2. Beispielsweise könnte man die $m \times n$-Matrix $(a_{i,j})$ auf den Vektor aus K^{mn} abbilden, dessen k-te Komponente $a_{1+\lfloor (k-1)/n \rfloor, 1+(k-1) \bmod n}$ ist. (Das sieht komplizierter aus, als es ist. Probieren Sie es anhand eines konkreten Beispiels aus.)

Lösung 32.3. $\mathbf{A} \cdot \mathbf{C}$ und $\mathbf{B} \cdot \mathbf{B}$ sind 3×3-Matrizen, $\mathbf{B} \cdot \mathbf{A}$ ist eine 3×5-Matrix, $\mathbf{C} \cdot \mathbf{A}$ eine 5×5-Matrix und $\mathbf{C} \cdot \mathbf{B}$ eine 5×3-Matrix. Die anderen Produkte kann man alle nicht bilden.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 32.4. Das Produkt sieht so aus:

$$\begin{pmatrix} 3 & 7 & 0 \\ -1 & -2 & 9 \\ -1 & 4 & 3 \\ 8 & 0 & -6 \end{pmatrix} \cdot \begin{pmatrix} 5 & 2 & -4 \\ -1 & 3 & 7 \\ 0 & -2 & 2 \end{pmatrix} = \begin{pmatrix} 8 & 27 & 37 \\ -3 & -26 & 8 \\ -9 & 4 & 38 \\ 40 & 28 & -44 \end{pmatrix}$$

Lösung 32.5. Die Produkte sind:

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix} \qquad \mathbf{B} \cdot \mathbf{A} = \begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix}$$

Lösung 32.8. Das ist

$$\begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix},$$

wobei Sie hoffentlich auf den Faktor 2 vor $\mathbf{e}_2$ geachtet haben.

Lösung 32.9. Am einfachsten ist es wohl, wenn man die Merkregel von Seite 302 verwendet und die Basisvektoren einsetzt. Für $\mathbf{e}_1 = (1,0)$ erhält man $g(\mathbf{e}_1) = (0,1,1)$ und $f\big((0,1,1)\big) = (-2,2)$ und hat damit bereits die erste Spalte der gesuchten Matrix. Analog berechnet man $f(g(\mathbf{e}_2)) = (3,1)$. Damit ist

$$\begin{pmatrix} -2 & 3 \\ 2 & 1 \end{pmatrix}$$

die Matrix, die $f \circ g$ darstellt.

Lösung 32.10. $f(\mathbf{e}_2)$ ist einfach die zweite Spalte der Matrix, also $(3,4,1)$. Den anderen Wert erhält man durch Matrixmultiplikation:

$$f\big((2,1)\big) = \begin{pmatrix} 1 & 3 \\ 0 & 4 \\ 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 4 \end{pmatrix}$$

Lösung 32.11. Das ist natürlich die Einheitsmatrix $\mathbf{E}_n$ und das passt dann auch zu den Lemmata 32.2 und 32.3.

Lösung 32.12. Durch Einsetzen der Basisvektoren erhält man

$$\begin{pmatrix} 3 & -2 & 0 \\ 1 & 2 & 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

als Matrizen für f und g. Multipliziert man diese beiden, so ergibt sich die Matrix aus der Lösung von Aufgabe 32.9. Man muss natürlich darauf achten (siehe Aufgabe 32.5), dass die Faktoren die richtigen Reihenfolge haben. (Sonst würde auch der Typ des Ergebnisses gar nicht stimmen. Es muss sich ja eine 2×2-Matrix ergeben, weil $f \circ g$ eine Funktion von $\mathbb{R}^2$ nach $\mathbb{R}^2$ ist.)

Lösung 33.1. Sind $\mathbf{p}$ und $\mathbf{q}$ Ortsvektoren und ist $\mathbf{v}$ ein Richtungsvektor, so ist $\mathbf{p}-\mathbf{v}$ einfach die Verschiebung des Punktes $\mathbf{p}$ in Richtung von $-\mathbf{v}$. $\mathbf{q}-\mathbf{p}$ kann man als den Richtungsvektor interpretieren, der $\mathbf{p}$ auf $\mathbf{q}$ verschiebt.

Lösung 33.2. Für den ersten Punkt muss es ein $\lambda \in \mathbb{R}$ mit $(0,5) = (1,2) + \lambda(-2,6)$ geben. Das führt auf die beiden Gleichungen $0 = 1-2\lambda$ und $5 = 2+6\lambda$. Aus der ersten folgt $\lambda = 1/2$ und dieser Wert löst auch die zweite. Daher liegt $(0,5)$ auf der Geraden. Für den zweiten Punkt erhält man $5 = 1-2\lambda$ und $0 = 2+6\lambda$. Die erste Gleichung liefert $\lambda = -2$, aber das ist keine Lösung für die zweite Gleichung. Der Punkt $(5,0)$ liegt somit *nicht* auf der Geraden. (Nebenbei bemerkt kann bei solchen Aufgaben eine grobe Skizze recht hilfreich sein.)

Lösung 33.3. Die Geraden sind nicht parallel, denn aus $(-2,6) = \nu(-5,2)$ würde in der ersten Komponente $\nu = 2/5$, in der zweiten jedoch $\nu = 3$ folgen. Daher muss es nach Lemma 33.2 genau einen Schnittpunkt geben. Mit dem Ansatz

$$(1,2) + \lambda(-2,6) = (2,3) + \mu(-5,2)$$

erhält man ein lineares Gleichungssystem für λ und μ, das sich mit Schulwissen lösen lässt: $\lambda = 7/26$, $\mu = 4/13$. Einsetzen liefert den Schnittpunkt $(6/13, 47/13)$.

Lösung 33.4. Wie im Beweis des besagten Lemmas kann man beispielsweise

$$g = \mathbf{p}_1 + \mathbb{R}(\mathbf{p}_2 - \mathbf{p}_1) = (1,-3,2) + \mathbb{R}(4,7,6)$$

nehmen. Es gibt natürlich unendlich viele richtige Antworten.

Lösung 33.5. Das wäre $(1,-3,2) + \mathbb{R}(4,7,6) + \mathbb{R}(6,2,-2)$.

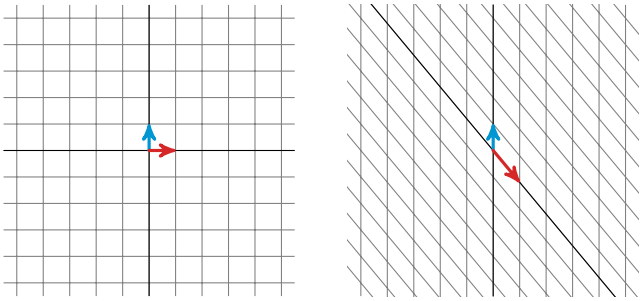
Lösung 33.6. Nach Definition müssen die beiden Richtungsvektoren der Ebene linear unabhängig sein. Hat man drei Punkte, die auf einer gemeinsamen Geraden liegen, so kann man das nicht hinbekommen, und es ist wohl auch anschaulich klar, dass drei solche Punkte nicht eindeutig eine Ebene festlegen. Eine mögliche Antwort auf die Frage wären die Punkte $\mathbf{p}_i = (i,0,0)$ für $i = 1,2,3$.

Lösung 33.7. Ist eine Gerade durch $\mathbf{q}_1$ und $\mathbf{q}_2$ parallel zu einer durch $\mathbf{p}_1$ und $\mathbf{p}_2$, so gibt es nach Definition ein $\lambda \in K$ mit $\lambda(\mathbf{p}_2 - \mathbf{p}_1) = \mathbf{q}_2 - \mathbf{q}_1$. Ist nun f die lineare Abbildung, so folgt nach Anwendung von f auf beide Seiten der Gleichung und Ausnutzung der Linearität $\lambda(f(\mathbf{p}_2) - f(\mathbf{p}_1)) = f(\mathbf{q}_2) - f(\mathbf{q}_1)$. Die Gerade durch $f(\mathbf{q}_1)$ und $f(\mathbf{q}_2)$ ist somit parallel zu der durch $f(\mathbf{p}_1)$ und $f(\mathbf{p}_2)$

Lösung 33.8. $\begin{pmatrix} 3.7 & 0 \\ 0 & 3.7 \end{pmatrix}$

Lösung 33.10. $\mathbf{M}$ muss die $n \times n$-Diagonalmatrix sein, in deren Hauptdiagonale überall λ steht, also $\mathbf{M} = \lambda \mathbf{E}_n$.

Lösung 33.11. In diesem Fall wird längs der vertikalen Achse geschert. Und nach „unten“, weil -1.2 negativ ist.



Lösung 33.12. Bezeichnet man mit $\mathbf{D}_\alpha$ die Matrix für die Drehung um den Winkel α, dann sollte Ihre Rechnung so ausgesehen haben:

$$\begin{aligned}\mathbf{D}_\alpha \cdot \mathbf{D}_\beta &= \begin{pmatrix}\cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha\end{pmatrix} \cdot \begin{pmatrix}\cos\beta & -\sin\beta \\ \sin\beta & \cos\beta\end{pmatrix} \\ &= \begin{pmatrix}\cos\alpha\cos\beta - \sin\alpha\sin\beta & -\sin\alpha\cos\beta - \sin\beta\cos\alpha \\ \sin\alpha\cos\beta + \sin\beta\cos\alpha & \cos\alpha\cos\beta - \sin\alpha\sin\beta\end{pmatrix} \\ &= \begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix} = \mathbf{D}_{\alpha+\beta}\end{aligned}$$

Lösung 33.13. Grundsätzlich sollten Sie sich bei solchen Fragen zuerst eine Skizze machen und wie in den entsprechenden Abbildungen im Skript die Bilder der Basisvektoren einzeichnen, die man direkt der Matrix entnehmen kann. Man sieht dann hoffentlich sofort: Die erste Matrix beschreibt eine Drehung um 90°. Die zweite ist die Spiegelungsmatrix für den Winkel 45°, d. h., es wird an der Hauptdiagonalen gespiegelt. Das kann man nun zur Sicherheit noch überprüfen, indem man die entsprechenden Matrizen ausrechnet.

Lösung 33.14. In beiden Fällen kann man sich sofort (ggf. mithilfe einer Skizze) überlegen, auf welche Vektoren die beiden kanonischen Einheitsvektoren abgebildet werden müssen. Das müssen die Spalten der jeweiligen Matrix sein. Das Ergebnis sieht also so aus:

$$\begin{pmatrix}-1 & 0 \\ 0 & -1\end{pmatrix} \qquad \begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}$$

Lösung 33.15. Da der Mittelpunkt des Quadrates der Koordinatenursprung ist, haben wir es offenbar mit einer Drehung des Quadrates zu tun, das die Ecken $(\pm 1, \pm 1)$ hat. *Vor* der Drehung wäre der Winkel der Linie vom Ursprung zur oberen rechten Ecke zur horizontalen Achse 45° gewesen. Es wurde somit um $57 - 45 = 12$ Grad gedreht. Die gesuchten Koordinaten erhält man, in dem man den Punkt $(1, -1)$ mit der Drehmatrix für 12° multipliziert. Alternativ kann man auch direkt argumentieren, dass der Punkt P die Polarkoordinaten $\sqrt{2}$ und $-45+12$ Grad haben muss. (Warum?) Es ergibt sich jedenfalls gerundet $(1.19, -0.77)$.

(Beachten Sie, dass man die ungefähre Lage von P der Skizze entnehmen kann. Sollten Sie beispielsweise eine negative x-Koordinate herausbekommen haben, dann sollte schon deswegen klar sein, dass Sie einen Fehler gemacht haben müssen.)

Lösung 33.16. Sei $\mathbf{D}_\alpha$ wie in der Lösung von Aufgabe 33.12 die entsprechende Drehmatrix. Der Winkel, den die Gerade, auf die projiziert werden soll, mit der x-Achse bildet, ist $\alpha = \arctan(9/7)$. Dreht man um $-\alpha$, so wird die Gerade also auf die horizontale Achse gedreht, und die Projektion wird dann durch die Matrix (33.6) dargestellt. Insgesamt erhält man die gesuchte Matrix damit durch

$$\mathbf{D}_\alpha \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \mathbf{D}_{-\alpha} = \frac{1}{130} \cdot \begin{pmatrix} 49 & 63 \\ 63 & 81 \end{pmatrix} \approx \begin{pmatrix} 0.38 & 0.48 \\ 0.48 & 0.62 \end{pmatrix}.$$

(Die Matrix in der Mitte erhält man, wenn man exakt rechnet, z. B. mit einem Computeralgebrasystem. Es reicht jedoch, wenn Sie mit einem Taschenrechner den gerundeten Wert ermitteln.)

Lösung 33.17. Der Winkel der Geraden aus der Aufgabenstellung mit der horizontalen Achse ist $\alpha = \arctan(1/3)$. Die Matrix für die Spiegelung ist daher

$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} = \frac{1}{5} \cdot \begin{pmatrix} 4 & 3 \\ 3 & -4 \end{pmatrix} \approx \begin{pmatrix} 0.80 & 0.60 \\ 0.60 & -0.80 \end{pmatrix}.$$

Beachten Sie, dass man in diesem Fall das Ergebnis exakt als Bruch angeben kann und dass eine Nachkommastelle ausreichen würde. Da in der Aufgabenstellung jedoch von zwei Stellen die Rede war, sollten die Nullen dort auch stehen.

Lösung 34.1. Ihre Rechnung sollte im Wesentlichen so ausgesehen haben:

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x+a \\ y+b \\ 1 \end{bmatrix}$$

Wenn man die dritte Komponente des Ergebnisses (die offensichtlich immer die Zahl 1 ist) ignoriert, kommt genau das heraus, was man erwarten würde.

Lösung 34.2. Die Antwort wird bereits durch die Verwendung des Grautons angedeutet: Solange wir nur die beiden Typen (34.1) und (34.2) einsetzen, werden Produkte von solchen Matrizen immer dieselbe letzte Zeile haben. Daher kann man diese auch weglassen. Und genau das machen manche Softwarebibliotheken auch.

Lösung 34.3. Die Matrizen für f und h kann man ohne großes Nachdenken hinschreiben (siehe Aufgabe 33.14) und in (34.1) einsetzen. Ebenso sollte die Matrix für g nach dem Muster (34.2) hoffentlich ein Kinderspiel sein. Insgesamt erhält man also

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -3 \\ 1 & 0 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

Lösung 34.4. g ist offenbar eine Parallele zur y-Achse und die Matrix für die Spiegelung an der y-Achse kann man wie in Aufgabe 33.14 ohne Rechnen angeben. Analog zum vorgerechneten Beispiel verschieben wir erst um $(-2,0)$, um g mit der y-Achse in Deckung zu bringen. Dann wird gespiegelt und anschließend wird die Translation zurückgenommen. Die Matrix sieht also folgendermaßen aus:

$$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Lösung 35.7. Weil der Kosinus von $\pi/2$ den Wert null hat, ist das genau dann der Fall, wenn das Skalarprodukt der beiden Vektoren null ist. Damit hat man ein sehr einfaches Kriterium, das ohne trigonometrische Funktionen auskommt. (Wir gehen natürlich davon aus, dass der Nullvektor nicht beteiligt ist, weil es sonst wie bereits erwähnt wenig Sinn ergeben würde, von Winkeln zu sprechen.)

Lösung 35.8. Der dritte Summand verschwindet (siehe Aufgabe 35.7) und man erhält die vektorielle Version des Satzes des Pythagoras: $(\mathbf{a}-\mathbf{b})^2 = \mathbf{a}^2 + \mathbf{b}^2$.

Lösung 35.9. Man kann es einfach ausrechnen: Mit

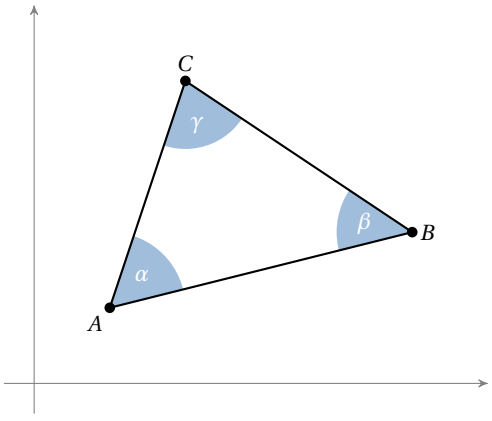
$$\|\mathbf{a}+\mathbf{b}\|^2 = (\mathbf{a}+\mathbf{b})^2 = \mathbf{a}^2 + 2\mathbf{a}\cdot\mathbf{b} + \mathbf{b}^2 = \mathbf{a}^2 + \mathbf{b}^2 = \|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 = 10 + 15 = 25$$

folgt $\|\mathbf{a}+\mathbf{b}\| = 5$. Aber eine Skizze hätte auch gereicht. Weil $\mathbf{a}$ und $\mathbf{b}$ nach Aufgabenstellung senkrecht aufeinander stehen, geht es hier mal wieder um den Satz des Pythagoras.

Lösung 35.10. Mit den Rechenregeln für das Skalarprodukt erhält man

$$(2\mathbf{a}+2\mathbf{b})\cdot(\mathbf{a}+\mathbf{b}) = 2\mathbf{a}^2 + 2\mathbf{b}\cdot\mathbf{a} + 2\mathbf{a}\cdot\mathbf{b} + 2\mathbf{b}^2 = 2\|\mathbf{a}\|^2 + 2\|\mathbf{b}\|^2 = 4 + 6 = 10.$$

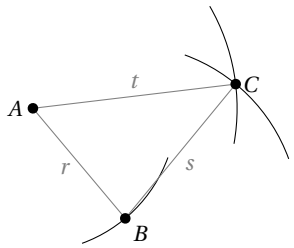
Lösung 35.11. Wie üblich ist eine Skizze hilfreich. Dort vergeben wir auch gleich Namen für die Winkel. Die Ortsvektoren bezeichnen wir mit denselben Buchstaben wie die Punkte, also z. B. $\mathbf{a}$ für A.



Das Dreieck sieht annähernd gleichseitig aus, also sollten sich drei Winkel in der Nähe von $\pi/3 \approx 1$ ergeben. (Auf jeden Fall muss die Summe der Winkel π sein.)

Die eigentliche Berechnung erfolgt wie in Aufgabe 35.6. Beispielsweise ist α der Winkel zwischen $\mathbf{b}-\mathbf{a}$ und $\mathbf{c}-\mathbf{a}$. Zur Kontrolle meine Ergebnisse: $\alpha \approx 1.00$, $\beta \approx 0.83$, $\gamma \approx 1.30$.

Lösung 35.12. So ein Dreieck kann man mit einem Zirkel konstruieren (obwohl man das natürlich für die Lösung der Aufgabe nicht machen muss). Wir vergeben die Bezeichnungen wie in der Skizze und benennen die Ortsvektoren und Winkel zu den Eckpunkten wie in der Lösung zu Aufgabe 35.11.



Für den bei A liegenden Winkel α ergibt sich mit dem Kosinussatz

$$\begin{aligned} s^2 &= r^2 + t^2 - 2rt\cos\alpha, \\ 2rt\cos\alpha &= r^2 + t^2 - s^2, \\ \cos\alpha &= (r^2 + t^2 - s^2)/2rt = 187/342 \quad \text{und schließlich} \\ \alpha &= \arccos(187/342) \approx 0.99. \end{aligned}$$

Analog erhält man

$$\begin{aligned} \beta &= \arccos(7/38) \approx 1.39 \quad \text{und} \\ \gamma &= \arccos(13/18) \approx 0.76. \end{aligned}$$

Lösung 35.13. Aus der Symmetrie

$$\begin{pmatrix} a & 2 & b \\ a & b & a-2b \\ 2a & d & c \end{pmatrix} = \mathbf{M} = \mathbf{M}^T = \begin{pmatrix} a & a & 2a \\ 2 & b & d \\ b & a-2b & c \end{pmatrix}$$

folgt zunächst $a = 2$, dann $b = 2a = 4$ und damit $d = a - 2b = -6$.

Lösung 35.15. Sind $\mathbf{x}$ und $\mathbf{y}$ verschieden, so ist ihr Abstand nicht null. Die Isometrie ändert diesen Abstand nicht, also ist auch der Abstand der Bilder von $\mathbf{x}$ und $\mathbf{y}$ nicht null. Und das impliziert, dass sie verschieden sind.

Lösung 35.16. Anschaulich ist das natürlich ohnehin klar. Aber auch formal ist das einfach zu begründen. Ist $\mathbf{a} \in \mathbb{R}^n$ und $\tau\colon \mathbb{R}^n \to \mathbb{R}^n$ durch $\tau(\mathbf{v}) = \mathbf{v} + \mathbf{a}$ definiert, dann gilt natürlich

$$\|\tau(\mathbf{v}) - \tau(\mathbf{w})\| = \|(\mathbf{v}+\mathbf{a}) - (\mathbf{w}+\mathbf{a})\| = \|\mathbf{v}-\mathbf{w}\|$$

für alle Vektoren $\mathbf{v}$ und $\mathbf{w}$.

Lösung 36.1. Dass die beiden Vektoren orthogonal sind, sieht man sofort, wenn man ihr Skalarprodukt berechnet. Dass sie beide normiert sind, folgt aus Korollar 29.7.

Lösung 36.2. Eine Erklärung liefert die Merkregel, dass die Spalten die Bilder der Basisvektoren sind. Weil die kanonische Basis eine Orthonormalbasis ist und eine orthogonale Abbildung Winkel und Normen nicht ändert, müssen auch die Spalten eine Orthonormalbasis bilden. Eine zweite Erklärung steckt in Lemma 35.6: Das Produkt $\mathbf{A}^T \cdot \mathbf{A}$ berechnet alle möglichen Skalarprodukte der Spalten von $\mathbf{A}$ miteinander. Die Einsen in $\mathbf{E}_n$ besagen, dass die Spalten normiert sind, und die Nullen besagen, dass die Spalten paarweise senkrecht zueinander stehen.

Lösung 36.3. Die Norm ist $\|(\|\mathbf{v}\|)^{-1}\mathbf{v}\| = |(\|\mathbf{v}\|)^{-1}|\|\mathbf{v}\| = (\|\mathbf{v}\|)^{-1}\|\mathbf{v}\| = 1$. Es gibt also offenbar zu jedem Vektor außer dem Nullvektor einen normierten Vektor, der in dieselbe Richtung zeigt. Den hier gezeigten Prozess der Berechnung eines solchen Vektors nennt man das *Normieren* von $\mathbf{v}$.

Normieren

Lösung 36.4. Wie in Aufgabe 36.3 berechnen wir zunächst $\|\mathbf{v}\| = 9$. Der normierte Vektor ist also $(\|\mathbf{v}\|)^{-1}\mathbf{v} = 1/9 \cdot (-4, 8, 1)$.

Lösung 36.5. Wir überzeugen uns zunächst, dass B linear unabhängig ist, indem wir die Linearkombination

$$\alpha \cdot \begin{pmatrix} 1 \\ 2 \\ -3 \\ 0 \end{pmatrix} + \beta \cdot \begin{pmatrix} 2 \\ 3 \\ 1 \\ 3 \end{pmatrix} + \gamma \cdot \begin{pmatrix} 4 \\ 4 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

betrachten. In der vierten Komponente folgt $\beta = 0$. Setzt man das in die Gleichung der dritten Komponente ein, so erhält man $\alpha = 0$. Damit folgt dann aus einer der ersten beiden Gleichungen auch $\gamma = 0$.

Wir beginnen nun mit $\mathbf{w}_1 = \mathbf{v}_1$. Mit $\mathbf{w}_2 = \mathbf{v}_2 + \alpha_1 \mathbf{w}_1$ sowie

$$0 = \mathbf{w}_1 \cdot \mathbf{w}_2 = \mathbf{w}_1 \cdot \mathbf{v}_2 + \alpha_1 \mathbf{w}_1^2 = 5 + \alpha_1 \cdot 14$$

erhalten wir $\alpha_1 = -5/14$ und damit $\mathbf{w}_2 = 1/14 \cdot (23, 32, 29, 42)$. Und mit

$$\begin{aligned} \mathbf{w}_3 &= \mathbf{v}_3 + \beta_1 \mathbf{w}_1 + \beta_2 \mathbf{w}_2, \\ 0 &= \mathbf{w}_1 \cdot \mathbf{w}_3 = \mathbf{w}_1 \cdot \mathbf{v}_3 + \beta_1 \mathbf{w}_1^2 = 12 + \beta_1 \cdot 14 \quad \text{sowie} \\ 0 &= \mathbf{w}_2 \cdot \mathbf{w}_3 = \mathbf{w}_2 \cdot \mathbf{v}_3 + \beta_2 \mathbf{w}_2^2 = 110/7 + \beta_2 \cdot 297/14 \end{aligned}$$

ergibt sich $\beta_1 = -6/7$, $\beta_2 = -20/27$ und schließlich

$$\mathbf{w}_3 = 1/27 \cdot (52, 16, 28, -60).$$

$\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$ ist eine Orthogonalbasis von U. (Das ist nicht die einzige mögliche Lösung, aber es ist die, die man erhält, wenn man wie in dem besagten Beweis vorgeht.)

Lösung 36.6. Mit etwas Nachdenken sollte man auf den einfachen „Trick“ kommen, dass man einen zu (x,y) senkrechten Vektor erhält, indem man die Komponenten vertauscht und bei einer von beiden das Vorzeichen ändert: $(y,-x)$ oder $(-y,x)$ erfüllen beide die Bedingung. Im konkreten Fall wären das $(2,-5)$ bzw. $(-2,5)$.

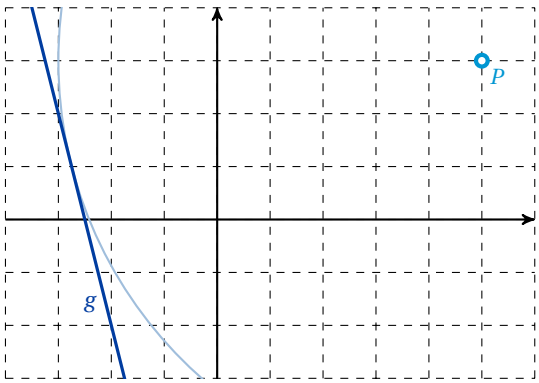
Lösung 36.7. Hier spielt $\mathbb{R}(1,-4)$ die Rolle des Untervektorraums U und wir brauchen einen Normalenvektor. Das ist in diesem Fall einfach, denn wir können wie in Aufgabe 36.6 einfach $\mathbf{n} = (4,1)$ nehmen. Durch Normieren erhalten wir $\mathbf{n}_0 = 1/\sqrt{17}\cdot(4,1)$. Wie im Beweis von Satz 36.5 berechnen wir nun $\mathbf{n}_0\cdot(-3,2)$ und erhalten $-10/\sqrt{17}$. Wegen des falschen Vorzeichens müssen wir noch mit -1 multiplizieren und erhalten schließlich

$$g = \{\mathbf{x}\in\mathbb{R}^2 : -1/\sqrt{17}\cdot(4,1)\cdot\mathbf{x} - 10/\sqrt{17} = 0\}. \tag{L-8}$$

Lösung 36.8. Weil Abstände nicht negativ sein können, ist die Menge, um deren Infimum es geht, nach unten beschränkt. Außerdem ist sie nicht leer, weil A und B nicht leer sind. Nach Aufgabe 16.1 existiert das Infimum.

Lösung 36.9. Der erste Schritt bei so einer Aufgabe sollte die Darstellung der Hyperebene in hessescher Normalenform sein. Zum Glück haben wir das für diese Gerade in Aufgabe 36.7 bereits gemacht und (L-8) erhalten.[61] Wir müssen nun nur noch $(5,3)$ für $\mathbf{x}$ einsetzen und erhalten

$$|-1/\sqrt{17}\cdot(4,1)\cdot(5,3) - 10/\sqrt{17}| = |-33/\sqrt{17}| \approx 8.00.$$



Wie üblich ist es sinnvoll, eine Zeichnung zu machen. In der obigen Skizze ist zusätzlich ein Kreis mit dem Radius 8 um P eingezeichnet.

Lösung 36.10. Prinzipiell ändert sich beim Übergang in eine andere Dimension nichts, wenn man bereits eine hessesche Normalenform hat. Die Rechnung ist in diesem Fall

$$|1/\sqrt{21}\cdot(4,-2,1)\cdot(5,0,3) - 5| = |23/\sqrt{21} - 5| \approx 0.02.$$

Lösung 36.11. Der einfachste Weg dürfte sein, so wie im Beweis von Satz 36.5 vorzugehen und den Punkt $5/\sqrt{21}\cdot(4,-2,1)$ zu wählen. Aber es gibt natürlich unendlich viele korrekte Antworten.

[61] Dass der Richtungsvektor nun $(2,-8)$ statt $(1,-4)$ ist, spielt offenbar keine Rolle.

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Lösung 36.12. Die Punkte auf g haben offenbar die Form $(x,0,0)$ mit $x \in \mathbb{R}$. Setzt man so einen Punkt in die Gleichung von E ein, so erhält man

$$1/\sqrt{21} \cdot (4,-2,1) \cdot (x,0,0) - 5 = 4x/\sqrt{21} - 5 = 0.$$

Diese Gleichung wird durch $x = 5/4 \cdot \sqrt{21}$ gelöst. Also ist $(5/4 \cdot \sqrt{21},0,0)$ der gesuchte Schnittpunkt von g und E.

Lösung 36.13. Man kann wie in Aufgabe 36.6 vorgehen und eine Komponente einfach ignorieren. $(-5,2,0)$ wäre eine mögliche Lösung.

Lösung 36.15. Nein, ist es nicht. Sie haben hoffentlich einfach mal ein Beispiel durchgerechnet und das gleich gesehen. Wenn Sie nicht gerade zufällig ein „falsches“ Beispiel gewählt haben, sind Sie auf so etwas gekommen:

$$\big((1,0,0) \times (0,1,0)\big) \times (0,1,0) = (-1,0,0)$$
$$(1,0,0) \times \big((0,1,0)) \times (0,1,0)\big) = (0,0,0).$$

Lösung 36.17. Es ergibt sich

$$\mathbf{0} \overset{\text{(iii)}}{=} (\mathbf{a}+\mathbf{b}) \times (\mathbf{a}+\mathbf{b}) \overset{\text{(ii)}}{=} \mathbf{a}\times\mathbf{a} + \mathbf{b}\times\mathbf{a} + \mathbf{a}\times\mathbf{b} + \mathbf{b}\times\mathbf{b} \overset{\text{(iii)}}{=} \mathbf{b}\times\mathbf{a} + \mathbf{a}\times\mathbf{b}$$

und deshalb sind $\mathbf{b} \times a$ und $\mathbf{a} \times \mathbf{b}$ bezüglich der Vektoraddition invers zueinander.

Lösung 36.18. $\mathbf{x} \times \mathbf{y} = \mathbf{0}$ führt nach Definition zu den Gleichungen

$$x_2 y_3 = x_3 y_2, \quad x_3 y_1 = x_1 y_3 \quad \text{und} \quad x_1 y_2 = x_2 y_1.$$

Das kann man umformen zu

$$y_3 = \frac{y_2}{x_2} \cdot x_3, \quad y_1 = \frac{y_3}{x_3} \cdot x_1 = \frac{y_2}{x_2} \cdot x_1 \quad \text{und} \quad y_2 = \frac{y_1}{x_1} \cdot x_1 = \frac{y_2}{x_2} \cdot x_1$$

und erhält dadurch $\mathbf{y} = y_2/x_2 \cdot \mathbf{x}$.

Das gilt allerdings nur unter der Bedingung $0 \notin \{x_1, x_2, x_3\}$. Zusätzlich muss man noch diverse Fälle untersuchen, bei denen ein oder mehrere der x_i verschwinden. Das spare ich mir hier aber, weil es analog funktioniert.

Lösung 36.19. Der Abstand kann wie in Aufgabe 36.10 berechnet werden, wenn wir eine hessesche Normalenform der Ebene haben. Aus der Lösung von Aufgabe 33.5 übernehmen wir zunächst die Punktrichtungsform $(1,-3,2) + \mathbb{R}(4,7,6) + \mathbb{R}(6,2,-2)$. Ein Normalenvektor muss senkrecht auf beiden Richtungsvektoren stehen und kann mit dem Vektorprodukt ermittelt werden:

$$\mathbf{n} = (4,7,6) \times (6,2,-2) = (-26,44,-34)$$

Durch Normieren bekommen wir

$$\mathbf{n}_0 = (\|\mathbf{n}\|)^{-1}\mathbf{n} = (2\sqrt{942})^{-1}(-26,44,-34).$$

Und Multiplikation mit dem auf der Ebene liegenden Punkt $(1,-3,2)$ liefert

$$\mathbf{n}_0 \cdot (1,-3,2) = -113/\sqrt{942}.$$

Damit ergibt sich als hessesche Normalenform der Ebene

$$E = \{\mathbf{x} \in \mathbb{R}^3 : 1/\sqrt{942} \cdot (13,-22,17) \cdot \mathbf{x} - 113/\sqrt{942} = 0\}.$$

Den gesuchten Abstand d erhält man nun durch Einsetzen:

$$d = \Big|\big((13,-22,17) \cdot (2,0,-4) - 113\big)/\sqrt{942}\Big| = 155/\sqrt{942} \approx 5.05.$$

Lösung 36.20. Zuerst wird die Ebene wie in Aufgabe 33.5 in Punktrichtungsform gebracht, dann wie in Aufgabe 36.19 in hessesche Normalenform. Den gesuchten Punkt $\mathbf{w}$ erhält man durch die Darstellung in (36.3).

$$\begin{aligned}
E &= (3,2,1) + \mathbb{R}(1,9,1) + \mathbb{R}(2,-4,4) \\
&= \left\{\mathbf{x} \in \mathbb{R}^3 : \frac{1}{6\sqrt{58}} \cdot (40,-2,-22) \cdot \mathbf{x} - \frac{94}{6\sqrt{58}}\right\} \\
\mathbf{w} &= (-4,0,1) + \frac{1}{6\sqrt{58}} \cdot \big(94 - (40,-2,-22) \cdot (-4,0,1)\big)\Big(\frac{1}{6\sqrt{58}} \cdot (40,-2,-22)\Big) \\
&= (-4,0,1) + \frac{23}{87} \cdot (20,-1,-11) = \frac{1}{87} \cdot (112,-23,-166)
\end{aligned}$$

Damit ist die Aufgabe gelöst. Man kann allerdings noch diverse Proben machen. Zunächst kann man ähnlich wie in Aufgabe 33.2 prüfen, ob $\mathbf{w}$ wirklich auf E liegt. Das ist tatsächlich der Fall:

$$\mathbf{w} = (3,2,1) - \frac{15}{29}(1,9,1) - \frac{52}{87}(2,-4,4)$$

Außerdem kann man den Abstand $\|\mathbf{w} - (-4,0,1)\| = 23 \cdot \sqrt{2/29}$ mit dem durch die hessesche Normalenform gelieferten Wert (farblich hervorgehoben) vergleichen.

Literatur

In der folgenden Liste sind diverse Bücher aufgeführt, die alle Mathematik speziell für Studierende der Informatik behandeln. Es ist sicher eine gute Idee, sich ein paar dieser Bücher einmal anzuschauen. Vielleicht verstehen Sie die Erklärungen dort besser als in diesem Skript, vielleicht finden Sie weitere Aufgaben oder vielleicht werden Themen, die hier zu kurz kommen, dort ausführlicher behandelt. Die Links führen jeweils zu den Seiten der Verlage und die Bücher sind danach ausgewählt, dass man Sie als e-Books aus dem Netz der HAW Hamburg (und wohl auch aus den Netzen vieler anderer deutscher Hochschulen) kostenlos herunterladen kann.

- Folkmar Bornemann: Konkrete Analysis für Studierende der Informatik, Springer, 2008.
- Steffen Goebbels / Jochen Rethmann: Mathematik für Informatiker, Springer Vieweg, 2014.
- Peter Hartmann: Mathematik für Informatiker, Springer Vieweg, 2019.
- Stasys Jukna: Crashkurs Mathematik für Informatiker, Teubner, 2008.
- Bernd Kreußler / Gerhard Pfister: Mathematik für Informatiker, Springer, 2009.
- Christoph Meinel / Martin Mundhenk: Mathematische Grundlagen der Informatik, Springer Vieweg, 2015.
- Matthias Schubert: Mathematik für Informatiker, Vieweg + Teubner, 2012.
- Gerald Teschl / Susanne Teschl: Mathematik für Informatiker Band 1 und Band 2, Springer Vieweg, 2013/2014.
- Edmund Weitz: Konkrete Mathematik (nicht nur) für Informatiker, Springer Spektrum, 2021.
- Kurt-Ulrich Witt: Mathematische Grundlagen für die Informatik, Springer Vieweg, 2013.

Und im Anschluss noch eine ähnliche Liste. Hier geht es in erster Linie um den Schulstoff, der im Skript vorausgesetzt wird und mit dem viele Studierende erfahrungsgemäß Probleme haben. Wenn Sie Ihre Defizite rechtzeitig (und *nicht* erst kurz vor den Prüfungen!) identifizieren und an ihnen arbeiten wollen, dann kön-

nen die folgenden Bücher dabei sicher helfen. Sie sind nach denselben Kriterien wie oben ausgesucht worden.

- Albrecht Beutelspacher: Mathe-Basics zum Studienbeginn, Springer Spektrum, 2016.
- Erhard Cramer, Johanna Nešlehová: Vorkurs Mathematik, Springer Spektrum, 2015.
- Klaus Dürrschnabel et al.: So viel Mathe muss sein!, Springer Spektrum, 2023.
- Arnfried Kemnitz: Mathematik zum Studienbeginn, Springer Spektrum, 2014.
- Marcel Klinger: Vorkurs Mathematik für Nebenfachstudierende, Springer Spektrum, 2015.
- Michael Knorrenschild: Vorkurs Mathematik, Carl Hanser, 2021.
- Werner Poguntke: Keine Angst vor Mathe, Vieweg + Teubner, 2010.
- Sabrina Proß, Thorsten Imkamp: Brückenkurs Mathematik für den Studieneinstieg, Springer Spektrum, 2018.
- Joachim Siegert: Mathematik trainieren - Brüche, Funktionen und Co., Springer Spektrum, 2018.
- Jürgen Tietze: Terme, Gleichungen, Ungleichungen, Springer Spektrum, 2015.
- Jan van de Craats, Rob Bosch: Grundwissen Mathematik, Springer, 2010.
- Guido Walz, Frank Zeilfelder, Thomas Rießinger: Brückenkurs Mathematik, Springer Spektrum, 2019.

In diesem Zusammenhang empfehle ich auch meine 34-teilige Videoserie zum Vorkurs Mathematik aus dem Wintersemester 2019.

Index

Abbildung, *siehe* Funktion
ABEL, NIELS HENRIK, 98
abelsche
    Gruppe, 98
    Halbgruppe, 98
abelsches Monoid, 98
abgeschlossen, 103, 186
abhängig
    linear, 291
Ableitung, 252, 255
    Ableitung
        n-te, 255
    zweite, 255
Ableitungsfunktion, 255
Abschluss, 186
absolut konvergieren, 218
Absolutbetrag, 79, 164, 173, 360
absolute Homogenität, 318
absoluter Fehler, 230
Abstand, 327
abzählbar, 238
    unendlich, 238
abzählende Kombinatorik, 46
Additionstheoreme, 273
ADENAUER, KONRAD, 8
affiner Unterraum, 304
Affinkombination, 306
allgemeine alternierende
        harmonische Reihe, 220
allgemeine harmonische Reihe, 220
Allquantor, 18
alternierend, 329
alternierende Gruppe, 117
alternierende harmonische
        Reihe, 218
ALU, 94
Analysis, 191
analytisch, 260
angeordneter Körper, 157
Antikommutativität, 329
Antinomien, *siehe* Widersprüche der
        naiven Mengenlehre
antisymmetrisch, 153
Äquivalenz, 13
Äquivalenzklasse, 66
Äquivalenzrelation, 65
    induzierte, 69
ARCHIMEDES VON SYRAKUS, 162
Archimedisches Axiom, 162
Argument, 75, 176
ARISTOTELES, 23
arithmetische Summenformel, *siehe*
        gaußsche Summenformel
Arkuskosinus, 279
Arkussinus, 279
Arkustangens, 281
ARMSTRONG, NEIL, 8
Assoziativität, 14, 94
asymmetrisch, 155
`atan2`, 282
äußere Verknüpfung, 286
aufgespannt, 289
aufzählende Mengenschreibweise, 27
Auslassungspunkte, 26

E. Weitz: Mathematik [5. Dezember 2025, 14:43]. CC BY-NC-ND 3.0 DE

Aussage, 8
Aussageform, 17
Aussagenlogik, 7
Aussagenvariable, 12
Auswahlaxiom, 237, 292
Automorphismus, 107
axiomatische Mengenlehre, 35

babylonisches Wurzelziehen, 162
BACHMANN, PAUL, 205
bag, 56
ball, 183
Basis, 292
    geordnete, 301
    kanonische, 292
Basisergänzungssatz, 419
Basler Problem, 220
bedingt konvergieren, 218
Bedingung
    hinreichende, 11
    notwendige, 11
Belegung, 13
Bellsche Zahlen, 355
BERNOULLI, JAKOB, 199
Bernoullische Ungleichung, 199
Berührungspunkt, 186
beschränkt, 159, 189
    nach oben, 159
    nach unten, 159
beschränkte Folge, 193
beschreibende Mengenschreibweise, 27
bestimmte Divergenz, 204
Betrag, *siehe* Absolutbetrag
Beweis, 7
    direkter, 22
    durch Widerspruch, 23
    indirekter, 22
BÉZOUT, ÉTIENNE, 131
Bijektion, 81
bijektiv, 81
Bild, 75, 76
Bildmenge, 74
Bilinearität, 316, 329
Binomialkoeffizient, 53
Binomischer Lehrsatz, 263
Bisektion, 248
Bogenmaß, *siehe* Radiant
BOLZANO, BERNARD, 90
BOOLE, GEORGE, 23, 24
BOURBAKI, NICOLAS, 80
Bubblesort, 117
BÜRGI, JOST, 283

CANTOR, GEORG, 34, 240
CAUCHY, AUGUSTIN-LOUIS, 213, 283, 317
Cauchy-Folge, 213
Cauchy-Kriterium, 214
Cauchy-Produkt, 263
Cauchy-Schwarz-Ungleichung, 317
charakteristische Funktion, 363, 408
codomain, 75
coset, 105

Datenbanken, 70
DE FERMAT, PIERRE, *siehe* Fermat, Pierre de
DE MORGAN, AUGUSTUS, *siehe* Morgan, Augustus De
de-morgansche Regeln, 14
definit
    positiv, 180, 316, 318
Definition, 40
Definitionsbereich, 74
DESCARTES, RENÉ, 43, 330
Destrukturierung, 91
Dezimaldarstellung, 225
Diagonalargument, 241
Diagonalmatrix, 311
dicht, 165, 189
Diedergruppe, 371
Differentialquotient, 252
Differenz
    symmetrische, 95
Differenz, mengentheoretische, 29
differenzierbar, 252
    zweimal, 255
Dimension, 293
Dimensionssatz, *siehe* Kern-Bild-Formel
direkter Beweis, 22

direktes Produkt, 100, 118
DIRICHLET, PETER GUSTAV LEJEUNE, 90
Dirichlet-Funktion, 247
disjunkt, 46, 110
Disjunktion, 12
diskrete Metrik, 185
Distributivität, 117
divergent, 193
divergieren, bestimmt, 204
Division mit Rest, 126
domain, 74
Drehspiegelung, 323
Drehung, 309, *siehe* Rotation
Dreiecksungleichung, 164, 173, 180, 318
Durchschnitt, 29

Ebene, 304
echt komplex, 170
echte Teilmenge, 28
echter Teiler, 128
echtes Intervall, 166
eineindeutig, 81
Einheit, imaginäre, 170
Einheitskreis, 62, 183
Einheitsmatrix, 301
Einheitsvektor, 292
Einmaleins, 94
Einschränkung, 77
EINSTEIN, ALBERT, 6
Eintrag, 298
Eisenbahnmetrik, 182
Element, 26, 298
  größtes, 159
  inverses, 97
  kleinstes, 159
  neutrales, 96
Elementzeichen, 26
endlich, 237
Entwicklungspunkt, 260
ε-Kugel, 183
ε-Umgebung, 183
erfüllbar, 16
erzeugt, 289
es gibt, 19
EUKLID VON ALEXANDRIA, 23, 70, 129, 150, 181
euklidischer
  Abstand, 181
  Algorithmus, 129
EULER, LEONHARD, 16, 90, 220, 261, 272, 275, 283
eulersche
  Formel, 272
  Identität, 275
  Zahl, 261
Existenzquantor, 19
exklusives Oder, 10
Exponentialfunktion, 261, 268

Faktormenge, 66
Fakultät, 49
FALK, SIGURD, 300
Falksches Schema, 300
fallende Faktorielle, 52
Fallunterscheidung, 83
falsch, 8
Familie, 89
fast alle, 192
FAULHABER, JOHANNES, 210
Faulhabersche Formel, 210
Fehler
  absoluter, 230
  relativer, 230
Fehlstand, 115
FERMAT, PIERRE DE, 7, 147, 330
FIBONACCI, *siehe* Pisa, Leonardo da
Fibonacci-Folge, 201
Folge, 89
  beschränkte, 193
  geometrische, 199
  harmonische, 192
  komplexe, 191
  reelle, 191
Folgenglied, 191
FPU, 94
französische Eisenbahnmetrik, 182
FREGE, GOTTLOB, 23
freie Individuenvariable, 19
Fundamentalfolge, 213
Funktion, 74

analytische, 260
charakteristische, 363, 408
gerade, 272
glatte, 255
mehrstellige, 82
periodische, 276
rationale, 247
ungerade, 272
zweistellige, 82
Funktionalgleichung, 264
Funktionswert, 75
für alle, 18

GALOIS, ÉVARISTE, 123
ganze Zahlen, 27
ganzrationale Funktion, *siehe* Polynomfunktion
GAUSS, CARL FRIEDRICH, 16, 151, 164, 198
Gaußklammer
obere, 164
untere, 164
gaußsche
Summenformel, 198, 209
Zahlenebene, 172
gebundene Individuenvariable, 19
gehen, 191
GENTZEN, GERHARD, 19
geometrische
Folge, 199
Reihe, 215
Summenformel, 209
geordnete Basis, 301
geordneter Körper, 157
geordnetes Paar, 42
Gerade, 304
gerade
Funktion, 272
Permutationen, 115
Zahlen, 128
glatt, 255
gleichmächtig, 233
Glied einer Folge, 191
GÖDEL, KURT, 16
Gödelisierung, 238, 360
Grad, 121, 278
Grenzwert, 193
Großer Fermatscher Satz, 7
groß-Oh, 205
größter gemeinsamer Teiler, 129
größtes Element, 159
Gruppe, 98
abelsche, 98
alternierende, 117
kommutative, 98
symmetrische, 109
triviale, 99
Gruppenhomomorphismus, 102
Gruppenisomorphismus, 106

Halbgruppe, 98
abelsche, 98
kommutative, 98
Halbordnung, 153
HALMOS, PAUL, 96
HAMMING, RICHARD WESLEY, 182
Hamming-Abstand, 182
harmonische
Folge, 192
Reihe, 214
Reihe, alternierende, 218
HASSE, HELMUT, 156
Hasse-Diagramm, 156
Häufungspunkt, 212
Hauptdiagonale, 301, 349, 351
Hauptzweige, 279
HESSE, OTTO, 326
hessesche Normalenform, 326
HILBERT, DAVID, 16
hinreichende Bedingung, 11
homogene Koordinaten, 313
Homogenität, absolute, 318
Homomorphismus, 102
Hyperebene, 326

Identität, 62
iff, 13
im Allgemeinen nicht|hyperpage, 86
imaginäre Einheit, 170
Imaginärteil, 170
Implikation, 10, 12

Indikatorfunktion, *siehe* charakteristische Funktion
indirekter Beweis, 22
Individuenvariable, 17
  freie, 19
  gebundene, 19
Induktion, vollständige, 197
Induktionsanfang, 197
Induktionsschluss, *siehe* Induktionsschritt
Induktionsschritt, 197
Induktionsvoraussetzung, 197
induziert, 69
Infixnotation, 93
Injektion, 238
injektiv, 78
Inklusions-Exklusions-Prinzip, 46
innere Verknüpfung, 83
innerer Punkt, 186
Inneres, 186
Intervall, 166
  echtes, 166
  unechtes, 166
inverses Element, 97
Inversion, 115
irrational, 162
irreflexiv, 154
isolierte Punkt, 186
Isometrie, 321
isomorph, 106, 294
Isomorphismus, 106, 294

JONES, WILLIAM, 275
Junktor, 12

k-permutations, 52
kanonische
  Basis, 292
  Primfaktorzerlegung, 137
kartesische Darstellung, 278
kartesisches
  Koordinatensystem, 44
  Produkt, 43
Kategorientheorie, 35
kaufmännisches Runden, 228
Kehrwert, 145
Kehrwertregel, 255
Kern, 105, 296
Kern-Bild-Formel, 296
Klassifikationssatz, 298
Kleiner-Relation, 62
kleines Einmaleins, 94
kleinstes
  Element, 159
  gemeinsames Vielfaches, 137
Kodierungstheorie, 151
Koeffizient, 121, 258
kollinear, 304
Kombinationen, 53
  mit Wiederholungen, 54
Kombinatorik, 37, 56
  abzählende, 46
kommutative
  Gruppe, 98
  Halbgruppe, 98
kommutativer Ring, 117
kommutatives Monoid, 98
Kommutativität, 13, 95
kommutieren, 111
komplexe
  Folge, 191
  Zahlen, 169
Komponente, 42, 45, 298
Komposition, 64
kongruent modulo, 138
Kongruenz, 148
Kongruenzsystem, 148
konjugiert komplex, 174
Konjunktion, 12
konstant, 357
Konvention, 40
konvergent, 193
Konvergenzradius, 259
konvergieren, 191
  absolut, 218
  bedingt, 218
Koordinatensystem, kartesisches, 44
Korollar, 40
Körper, 121
  geordneter, 157
  vollständig angeordneter, 161
Kosinus, 272

Kosinussatz, 319
Kreiszahl, 275
Kreuzprodukt, 328
Kryptographie, 125, 148
Kugel, *siehe auch* ε-Kugel

LAGRANGE, JOSEPH-LOUIS, 123
LAMBERT, JOHANN HEINRICH, 275
LANDAU, EDMUND, 205
lateinisches Quadrat, 368
Laufvariable, 208
leer, 41
leere
  Menge, 29
  Summe, 400
leeres Produkt, 60, 137
LEIBNIZ, GOTTFRIED WILHELM, 56, 90, 123, 283
Leibniz-Kriterium, 217
Leibnizregel, 254
LEJEUNE DIRICHLET, PETER GUSTAV, *siehe* Dirichlet, Peter Gustav Lejeune
Lemma, 40
  von Bézout, 131
Levenshtein-Distanz, 182
LEWENSTEIN, WLADIMIR, 182
Limes, 193
linear
  abhängig, 291
  unabhängig, 291
lineare Ordnung, 153
Linearkombination, 129, 289
linksassoziativ, 95
linkseindeutig, 78
linksinvers, 99
Linksnebenklasse, 105
linksneutral, 96
Logarithmentafel, 283
Logarithmus, 266
  zur Basis a, 268

Mächtigkeit, 39, 233
Majorante, 219
Majorantenkriterium
  für Folgen, 195
  für Reihen, 219
Manhattan-Metrik, 181
maplet, 75
mathematisches Runden, 228
Matrix, 298
  transponierte, 320
Maximum, 126, 159
mehrstellige Funktion, 82
Memoisation, 205
Menge, 25
  leere, 29
Mengendiagramm, 30
Mengenklammern, 26
Mengenlehre, 34
Mengenprodukt, 43
Mengenschreibweise
  aufzählende, 27
  beschreibende, 27
mengentheoretische Differenz, 29
MERTENS, FRANZ, 263
Metrik, 180
  diskrete, 185
metrischer Raum, 180
Minimum, 125, 159
Monoid, 98
  abelsches, 98
  kommutatives, 98
monoton
  fallend, 217
  steigend, 217
MORGAN, AUGUSTUS DE, 14
Multimenge, 56
Multinomialkoeffizient, 51
Multiplikativität, 164, 173, 180

n-stellige Relation, 61
Nachbartransposition, 114
Nachkommastelle, 226
naive Mengenlehre, 35
NAPIER, JOHN, 283
natürliche Zahlen, 27
natürlicher Logarithmus, 266
$n\mathrm{C}r$, 54
Nebenklasse, 105
Negation, 12
negativ, 157

neutrales Element, 96
NEWTON, ISAAC, 6, 231, 283
NOETHER, EMMY, 123
Norm, 181, 317
Normalenform, 326
Normalenvektor, 326
Normieren, 427
normiert, 324
notwendige Bedingung, 11
$n\mathrm{P}r$, 52
NSA, 151
Nullfolge, 193
Nullfolgenkriterium, 214
nullteilerfrei, 122
Nullvektor, 286

o. B. d. A., 158
Obelus, 363
obere Schranke, 159
Obermenge, 28
oder, 9, *siehe auch* Disjunktion
Off-by-one-Error, 52
offen, 185
offene
    ε-Kugel, 183
    ε-Umgebung, 183
Operatorüberladung, 141
Ordnung, 105, 205
    lineare, 153
ORESME, NIKOLAUS VON, 214
orthogonal, 320, 324
Orthogonalbasis, 324
Orthonormalbasis, 324
Ortsvektor, 303

Paar, geordnetes, 42
paarweise, 58
parallel, 304
Parameter, 342
Parameterdarstellung, 304
Parameterform, 304
Parität, 115
Partialsumme, 211
Partition, 68
    induzierte, 69
PASCAL, BLAISE, 56
PEANO, GIUSEPPE, 19, 26
periodische Funktion, 276
Permutationen, 48, 107
    gerade, 115
    mit Wiederholungen, 50
    ungerade, 115
Permutationsgruppe, 108
Pfeildiagramm, 73
PISA, LEONARDO DA, 201
POINCARÉ, HENRI, 141
Polardarstellung, 278
Polynom, 121
Polynomfunktion, 121
positiv, 157
    definit, 180, 316, 318
Potenzmenge, 38
Potenzreihe, 258, 260
Prädikatenlogik, 17
prim, 133
Primfaktor, 134
Primfaktorzerlegung, 137
Primteiler, 134
Primzahlen, 27, 133
Produkt
    direktes, 100, 118
    leeres, *siehe* leeres Produkt
Produktregel, 254
Projektion, 311
Proposition, 40
Punkt
    innerer, 186
    isolierter, 186
Punkt- vor Strichrechnung, 14, 95
Punktrichtungsform, 304
PYTHAGORAS VON SAMOS, 173, 273

Quadrat, 108
Quadrat,lateinisches, 368
Quadratwurzel, 197
Quadrupel, 45
Quantor, 18
Quersumme, 66
    alternierende, 143
Quintupel, 45
Quotientenkriterium, 219
Quotientenmenge, 66

Radiant, 278
Rand, 186
Randpunkt, 186
range, 74
Rangsatz, *siehe* Kern-Bild-Formel
rationale
  Funktionen, 247
  Zahlen, 27
Realteil, 170
Rechenschieber, 283
rechtsassoziativ, 95
rechtseindeutig, 74
rechtsinvers, 366
rechtsneutral, 96
reduziert, 289
reelle
  Folge, 191
  Zahlen, 27
reflexiv, 63
Reihe, 211
  allgemeine alternierende harmonische, 220
  allgemeine harmonische, 220
  alternierende harmonische, 218
  geometrische, 215
  harmonische, 214
Reihenglied, 211
rein imaginär, 170
Rekursion, 200
Relation, 61
relationale Datenbanken, 70
relativen Fehler, 230
Rest, 127
Restklasse, 138
Restklassenkörper, 145
Restklassenring, 138
Restriktion, 77
Richtungsvektor, 303
RIEMANN, BERNHARD, 219, 220
Riemannsche Vermutung, 220
Riemannscher Umordnungssatz, 219
Ring, 117
  kommutativer, 117
  unitärer, 117
Rotation, 108
Runden, 228
  kaufmännisches, 228
  mathematisches, 228

Satz, 39
  des Pythagoras, 173, 273
  des Euklid, 23, 135
  vom Minimum und Maximum, 250
  von Bolzano-Weierstraß, 212
  von Cantor, 242
  von Cantor-Bernstein, 234
  von Cayley, 108
  von Mertens, 263
Scherung, 309
Schnittmenge, 67
Schranke
  obere, 159
  untere, 159
SCHWARZ, HERMANN AMANDUS, 317
set, 28
signifikante Stellen, 229
Signum, 115
Signumfunktion, 165
Singleton, 38
Sinus, 272
Skalar, 286
skalare Multiplikation, 286
Skalarprodukt, 316
Skalierung, 308
Spiegelung, 310
Standardskalarprodukt, 316
Stellenwertsystem, 221
stetig, 246
Stichprobe, 52, 53
Strecke, 306
streng monoton
  fallend, 217
  steigend, 217
strenge Totalordnung, 154
Summe, 211
  leere, *siehe* leere Summe
Summenformel
  arithmetische, 209
  gaußsche, 198, 209
  geometrische, 209
Summenschreibweise, 208

SUN ZI, 148
support, 110
Supremum, 160
surjektiv, 79
symmetrisch, 63, 180, 316, 320
symmetrische
    Differenz, 95
    Gruppe, 109

TAKAKAZU, SEKI, 123
Tangens, 272, 280
Tangente, 251
Taschenrechner, 52, 54, 278, 340
Tautologie, 16
Teiler, 128
    echter, 128
    größter gemeinsamer, 129
    trivialer, 128
Teilfolge, 250
Teilkörper, 287
Teilmenge, 28
    echte, 28
Theorem, 40
total, 153
Totalordnung, 153
    strenge, 154
Träger, 110
transitiv, 63
Translation, 312
transponierte Matrix, 320
Transposition, 114
Trichotomie, 154
Tripel, 45
triviale
    Gruppe, 99
    Untergruppen, 103
trivialer
    Teiler, 128
    Vektorraum, 287
    Zyklus, 111
Tupel, 45
Typ, 298

überabzählbar, 241
Umgebung, 184
Umkehrfunktion, 78
Umkehrrelation, 64
Umordnungssatz, Riemannscher, 219
unabhängig
    linear, 291
unär, 376
und, 9, *siehe auch* Konjunktion
unechtes Intervall, 166
unendlich, 237
ungerade
    Funktion, 272
    Permutationen, 115
    Zahlen, 128
unitärer Ring, 117
univalent, 74
untere Schranke, 159
Untergruppe, 103
Unterring, 120
Untervektorraum, 288
Urbild, 76

Variationen, 52
    mit Wiederholungen, 52
Vektor, 286
    normierter, 324
Vektorprodukt, 328
Vektorraum, 286
    trivialer, 287
Vektorraumhomomorphismus, 294
Vektorraumisomorphismus, 294
Vereinigung, 29
Vereinigungsmenge, 67
Verknüpfung, 82
    äußere, 286
    innere, 83
Verknüpfungstabelle, 101
verschwinden, 129
Vielfaches, 128
    kleinstes gemeinsames, 137
vollständig, 214
    angeordnet, 161
Vollständige Induktion, 197
VON ORESME, NIKOLAUS, *siehe* Oresme, Nikolaus von
Vorzeichenfunktion, 165

wahr, 8
Wahrheitstafel, 13
Wahrheitswert, 8
WEIERSTRASS, KARL, 90, 231, 283
wenn, dann, *siehe* Implikation
Wert, 211
Wertebereich, 74
Widersprüche der naiven Mengenlehre, 35
Winkel zwischen Vektoren, 319
wissenschaftliches Runden, 228
wohldefiniert, 141
Wohlordnung, 125
Wurzel, 197
Wurzelfunktion, 79
Wurzelkriterium, 219

Zahlen
- echt komplexe, 170
- ganze, 27
- gerade, 128
- irrationale, 162
- komplexe, 169
- natürliche, 27
- rationale, 27
- reelle, 27
- rein imaginäre, 170
- ungerade, 128
- zusammengesetzte, 133

Zahlengerade, 44, 162
Zahlentheorie, 125
ZAPPA, FRANK, 7
Zeta-Funktion, 220
Zielmenge, 75
Ziffernblatt, 143
zusammengesetzte Zahlen, 133
zweistellige
- Funktion, 82
- Relation, *siehe* Relation

Zweizeilenform, 109
Zwischenwertsatz, 247
Zyklus, 110
- trivialer, 111

Mathematische Symbole

Es ergibt wenig Sinn, mathematische Symbole alphabetisch zu sortieren. Daher werden sie in der folgenden Liste einfach in der Reihenfolge aufgeführt, in der sie definiert bzw. eingeführt wurden.

$\wedge$, 12
$\vee$, 12
$\neg$, 12
$\Rightarrow$, 12
1, 12
0, 12
$\Leftrightarrow$, 13
$\forall$, 18
$\exists$, 19
$\{1, \pi, 42\}$, 26
$\in$, 26
$\notin$, 26
$\{1, 2, 3, \ldots, 100\}$, 26
$\{x : A(x)\}$, 27
$\mathbb{N}$, 27
$\mathbb{Z}$, 27
$\mathbb{Q}$, 27
$\mathbb{R}$, 27
$\mathbb{P}$, 27
$\subseteq$, 28
$\supseteq$, 28
$\subset$, 28
$\not\subseteq$, 28
$\emptyset$, 29
$\cup$, 29
$\cap$, 29
$\setminus$, 29
$\mathbb{N}^+$, 31
$\{x \in M : A(x)\}$, 32
$\{t(x_1, \ldots, x_n) : A(x_1, \ldots, x_n)\}$, 32
$\mathscr{P}(A)$, 38
$|A|$, 39
2^A, 39
(a, b), 42
$A \times B$, 43
A^2, 43
$(a_1, \ldots, a_n)$, 45
A^n, 45
$[n]$, 48
P_X, 48
P_n, 49
p_n, 49
$n!$, 49
$P_{(b_1,\ldots,b_n)}$, 50
$\binom{n}{k_1,\ldots,k_r}$, 51
$V_{X,k}$, 51
$n^{\underline{k}}$, 52
$(n)_k$, 52
$\mathscr{P}_k(X)$, 53
$\mathscr{P}_{<k}(X)$, 53
$\mathscr{P}_{\leq k}(X)$, 53
$\binom{n}{k}$, 53
$\binom{X}{k}$, 54
$C_{n,k}$, 54

$\{|1,1,3,3,3,4|\}$, 55
$\{1,1,3,3,3,4\}_b$, 55
id_A, 62
Δ_A, 62
R^{-1}, 64
$R \circ S$, 64
$[a]_R$, 66
A/R, 66
$\bigcup \mathscr{A}$, 67
$\bigcup_{M \in \mathscr{A}} M$, 67
$\bigcap \mathscr{A}$, 67
$\bigcap_{M \in \mathscr{A}} M$, 67
$\bigcup_{n \in \mathbb{N}^+} [n]$, 68
D_f, 74
W_f, 74
$f\colon A \to B$, 75
$f(x)$, 75
$x \mapsto f(x)$, 75
$f[C]$, 76
$f^{-1}[D]$, 76
$f(C)$, 77
$f^{-1}(D)$, 77
$f|_C$, 77
$f \restriction C$, 77
$f + g$, 87
$f - g$, 87
$f \cdot g$, 87
f/g, 87
$(f(i) : i \in I)$, 89
$(f(i))_{i \in I}$, 89
B^A, 89
${}^A B$, 89
$\oplus$, 93
$\otimes$, 93
$A \triangle B$, 95
$\mathbb{R}^+$, 99
a^{-1}, 100
$1/a$, 100
a^2, 100
$-a$, 100
aU, 105
S_X, 107
S_n, 109
$(k_1\ k_2\ \ldots\ k_m)$, 110
(1), 110
$\mathrm{supp}(\sigma)$, 110
$\mathrm{sgn}(\sigma)$, 115
$2\mathbb{Z}$, 121
$R[x]$, 121
b/a, 122
$\frac{b}{a}$, 122
$b : a$, 122
$\min A$, 125
$\max A$, 126
$\min_{n \in \mathbb{N}} a_n$, 126
$a \bmod m$, 127
$a \mid b$, 128
$a \nmid b$, 128
$\mathrm{ggT}(a,b)$, 129
(a,b), 129
$\mathrm{kgV}(a,b)$, 137
$[a]_n$, 138
$\mathbb{Z}/n\mathbb{Z}$, 138
$\pm$, 139
$\mathbb{Z}_p$, 145
$a \equiv b \pmod{m}$, 148
$\preceq$, 156
$\prec$, 156
$\succeq$, 156
$\succ$, 156
$\mathbb{Q}(\sqrt{2})$, 159
$\min B$, 159
$\max B$, 159
$\sup M$, 160
$\inf M$, 160
$\lceil x \rceil$, 164
$\lfloor x \rfloor$, 164
$|x|$, 164
$\mathrm{sgn}(x)$, 165
$[a,b]$, $[a,b)$, etc., 167
$\mathbb{R}_{\geq 0}$ etc., 168
$\mathbb{C}$, 169
i, 170
$\mathrm{Re}(z)$, 170
$\mathrm{Im}(z)$, 170
$|z|$, 173
$\overline{z}$, 174
$\arg(z)$, 176
$U_\varepsilon(x)$, 183
∂A, 186
A°, 186
$\overline{A}$, 186

(a_n), 191
$\lim_{n\to\infty} a_n$, 193
$a_n \overset{n\to\infty}{\longrightarrow} a$, 193
$a_n \to a$, 193
$\sqrt[n]{y}$, 197
$\sqrt{y}$, 197
$[n]_0$, 200
x^r, 202
$\mathcal{O}(f)$, 205
$\sum_{k=m}^{n} a_k$, 208
$\prod_{k=m}^{n} a_k$, 210
$\sum_{k=m}^{\infty} a_k$, 211
$\approx$, 229
$A \nsim B$, 233
$A \simeq B$, 234
A^1, 239
A^0, 239
$\mathscr{P}_{<\infty}(A)$, 240
$\frac{df}{dx}(x_0)$, 252
$f'(x_0)$, 252
$f''(x_0)$, 255
$\frac{d^2f}{dx^2}(x_0)$, 255
$\exp(z)$, 261
e, 261
e^z, 265
ln, 266
log, 266
a^z, 267
$\log_a$, 268
$\cos z$, 272
$\sin z$, 272
$\tan x$, 272
$\sin^2 z$, 273
π, 275
arcsin, 279
arccos, 279
$\tan z$, 280
arctan, 281
$\langle X \rangle$, 289
$\mathbf{e}_i$, 292
$\dim V$, 293
$\ker f$, 296
$A^{m\times n}$, 299
$(a_{i,j})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$, 299
$(a_{i,j})$, 299
$\mathbf{A}\cdot\mathbf{B}$, 299
$\mathbf{E}_n$, 301
$\mathbb{1}_n$, 301
$\mathbf{p} + K\mathbf{v}$, 304
$\mathbf{p} + K\mathbf{v} + K\mathbf{w}$, 304
$[a, b, 1]$, 313
$\mathbf{x}\cdot\mathbf{y}$, 316
$\mathbf{x}^2$, 316
$\angle(\mathbf{a}, \mathbf{b})$, 319
$\mathbf{A}^T$, 320
$\mathbf{a} \perp \mathbf{b}$, 324
$d(A, B)$, 327
$d(a, B)$, 327
$\mathbf{x} \times \mathbf{y}$, 328
χ_A, 363
D_4, 371
(), 373