Lineare Algebra I, WS 2020/21

Ulrich Görtz

Version vom 16. November 2020.

Ulrich Görtz

Universität Duisburg-Essen
Fakultät für Mathematik
45117 Essen

ulrich.goertz@uni-due.de

Ich freue mich über Kommentare und Berichtigungen.

Ich bedanke mich für Bemerkungen/Korrekturen bei Fereshteh Fattahi, Lukas Fußangel, Florian Leptien.

Gesetzt in der Schrift Vollkorn[3] von F. Althausen mit LuaLaTeX, TikZ und anderen TEX-Paketen. Die HTML-Version wird mit plasTeX[4] erzeugt.

[1] https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.de
[2] https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de
[3] http://vollkorn-typeface.com/
[4] https://github.com/plastex/plastex

Inhaltsverzeichnis

KAPITEL 1

Einführung, Motivation

1.1. Bevor es losgeht – Allgemeines zum Mathematikstudium und speziell zum kommenden Wintersemester 2020/21

Herzlich Willkommen zur Vorlesung *Lineare Algebra I* im Wintersemester 2020/21 an der Universität Duisburg-Essen – ich freue mich, dass Sie dabei sind! Gerne hätte ich Sie persönlich im Hörsaal begrüßt, aber dieses Semester findet wegen der Corona-Epidemie unter besonderen Umständen statt, so dass es für den Moment bei einer Begrüßung auf dem Papier und per Video bleiben muss.

Die üblichen Präsenzvorlesungen können nicht stattfinden, sie werden ersetzt durch online bereitgestelltes Material wie dieses Skript, Videos und Aufgaben, die Sie am Rechner bearbeiten können. Andere Bestandteile des Moduls Lineare Algebra bleiben: Insbesondere die Hausaufgaben, die wöchentlich abgegeben werden müssen, und die für Sie gleichermaßen ein wichtiges mathematisches »Training« und die Möglichkeit sind, eine detaillierte Rückmeldung über Ihre Fortschritte zu erhalten. Hoffentlich wird es auch möglich sein, die Übungsgruppen in Präsenz durchzuführen, so dass Sie die Möglichkeit haben, in diesen kleinen Gruppen Ihre Fragen loszuwerden, mathematisch zu arbeiten, und andere Studierende kennenzulernen, mit denen Sie auch außerhalb der Uni-Veranstaltungen studieren können.

Gleich bleiben auch die Lernziele (siehe auch Abschnitt 2.1) des Moduls.

Und auch die wichtigste Tätigkeit, um diese Lernziele zu erreichen, bleibt: Dass Sie selbst über mathematische Probleme nachdenken! Auch wenn er offensichtliche Schwachstellen hat, mag ich den folgenden Vergleich:

Mathematik lernen ist wie schwimmen lernen

(oder ersetzen Sie, wenn Sie möchten, das Schwimmen durch eine andere Sportart oder dadurch, ein Musikinstrument zu lernen …). Um richtig schnell schwimmen zu lernen, ist es hilfreich, darüber Bücher zu lesen und sich Videos von Schwimmstars anzuschauen. Noch wichtiger ist es, Ratschläge von einer Trainer*in zu bekommen, was man falsch macht und worauf man achten muss. Vor allem zählt aber, wie viel Zeit man im Wasser verbringt, und dass man diese Zeit sinnvoll nutzt. Das können Sie auch aufs Klavierspielen übertragen: Natürlich kann es helfen, sich ein Klavierkonzert auf CD anzuhören. Wichtiger ist eine Klavierlehrer∗in , die konkrete Hinweise gibt, und das Lernen strukturiert. Vor allem zählt aber die Zeit, die man selbst am Klavier sitzt und übt. Und so ist es eben auch im Mathematikstudium: Bücher, Skripte, Videos (und Vorlesungen) sind wichtig. Fragen zu diskutieren und Tipps zu bekommen – in der Vorlesung oder vor allem in den Übungsgruppen – ist ebenso wichtig, oder vielleicht noch wichtiger. In erster Linie zählt aber die Zeit, in der Sie sich selbst den Kopf zerbrechen und selbst mathematisch arbeiten. Im Studium wird das auch konkret eingefordert in Form der schon erwähnten Hausaufgaben. Die wöchentlich verteilten Übungszettel werden Ihnen einiges abverlangen. Sie sind das essenzielle Training, und auch das beste Messinstrument für die erzielten Erfolge. Es zeigt sich immer wieder, dass die auf den Übungszetteln erreichte Punktzahl sehr direkt mit dem Erfolg in der Abschlussklausur zusammenhängt.

Zusätzliches Material (Bücher, Skripte, Videos, Aufgaben, …) gibt es im Überfluss. Schauen Sie sich Anhang C an oder geben Sie *Lineare Algebra* in einer Suchmaschine ein. Es kann durchaus nützlich sein, mit einigen dieser Quellen zu arbeiten, *es ersetzt aber nicht, dass Sie sich selbst mit dem Stoff auseinandersetzen und selber Probleme knacken*. Selber Probleme zu lösen ist eine der wichtigsten Fertigkeiten, die in dieser (und allen folgenden) Mathematikvorlesungen erworben werden sollen. Damit Sie darin immer besser werden, müssen Sie das trainieren, und je mehr Sie passiv konsumieren, desto mehr Gelegenheiten verschenken Sie, denselben Stoff »aktiv« zu bearbeiten. Es ist nicht so einfach, hier eine gute Balance zu finden – im Zweifelsfall sollten Sie eher mehr Zeit darauf verbringen »sich selbst den Kopf zu zerbrechen«, als weiteres Material zu suchen.

> ”
>
> But after having finished the classes, I came to an unfortunate conclusion—the videos don't matter too much. Having a video explanation of a concept is nice, but it's rarely superior to the same explanation in text. Text even has the advantages of searchability and nonlinearity, features missing in video. What mattered was having practice problems and projects. […]
>
> I feel the fuss over video has two causes:
> (1) Students associate university subjects with lectures, and don't know how to learn without them.
> (2) Watching videos is fun, doing practice problems is hard.
>
> […] **One reason I'm pessimistic about video is that it gives a false sense of accomplishment.**
>
> Scott H. Young[a]
>
> [a] https://www.scotthyoung.com/blog/2012/11/13/why-lectures/

1.2. Dieses Skript

Das Ziel dieses Skripts ist in erster Linie, den Stoff der Vorlesung zu dokumentieren und so ausführlich darzustellen, dass Sie ihn lernen können. Wie bei mathematischen Texten üblich, stelle ich mir eine »aktive« Leser∗in vor: Nehmen Sie sich Papier und einen Stift zur Hand und betrachten Sie alle Schritte, die Sie nicht verstehen, als kleine Übungsaufgaben, und Rechenschritte, die Ihnen zu schnell gehen, als Rechenaufgaben, die Sie lösen sollten, bevor Sie weiterlesen. Notieren Sie sich die Fragen, die bleiben, damit Sie am nächsten Tag noch einmal darauf zurückkommen können, oder sie im Forum auf der Moodle-Seite oder in Ihrer Übungsgruppe stellen können.

Ich versuche an vielen Stellen implizit vorausgesetztes Wissen explizit machen. Siehe zum Beispiel Anhang B.1. Dies ist ohnehin zu Beginn des Studiums besonders wichtig, und umso mehr in diesem Semester, wo die Möglichkeiten, Fragen zu stellen, eingeschränkt sind. Dadurch sind vielleicht manche Passagen etwas länglich; ich hoffe, dass es Ihnen leicht fallen wird, das zu überspringen, was Ihnen schon bekannt ist.

Darüberhinaus habe ich versucht, Ihnen einige zusätzliche Informationen bereitzustellen, mit denen Sie sich beschäftigen können, wenn Sie Lust haben – zum Beispiel, wenn es Ihrer Motivation dafür dient, sich mit dem eigentlichen Stoff zu beschäftigen, oder einfach zur Abwechslung. Zum Beispiel:

- In Abschnitt 3.3 einige berühmte Beweise, die »jede∗r mal gesehen haben sollte«.

- In Abschnitt 2.3 und an vielen Stellen im Text Hinweise zu Anwendungen der Linearen Algebra.
- In Anhang C einige Literaturhinweise.

Ich hoffe, dass das Skript damit gleichzeitig zu einer »Fundgrube« für Sie wird, um die vielen Verbindungen, die von der Linearen Algebra zu anderen Fragen innerhalb und außerhalb der Mathematik bestehen, zu erkunden. Und ich hoffe, dass diese Ergänzungen Ihrer Motivation dienen, sich mit dem eigentlichen Stoff der Vorlesung zu beschäftigen (wenn Ihre Motivation an dieser Stelle der Unterstützung bedarf), und Sie nicht zu sehr ablenken.

Einige Abschnitte sind mit einem Sternchen (*) markiert. Dies sind Ergänzungen, die nicht zum klausurrelevanten Vorlesungsstoff gehören. Die als *Ergänzung* bezeichneten Einschübe sind ebenfalls optional und nicht klausurrelevant. Gleichwohl können sie natürlich manchmal das Verständnis des klausurrelevanten Stoffs befördern.

Den Kern der Vorlesung bilden die Kapitel 4 bis 11.

> The best teacher, the most successful teacher I had at Breslau, was typical of the point of view of education, was a man in algebra, his name was Rosanes. His name is not known any more. His great success as a teacher was really due to the fact that he didn't teach things very well. He came to the platform. There was a blackboard. In his right hand he had some chalk, in the left hand he had a wet sponge. He turns his back to the audience, and he mumbled something towards the blackboard, and scribbled something in small letters on the blackboard, covering it up with his body. And as he moved along he erased what he had written. And then the student always had to try to snatch a few words. Then there was an enormous task after class, one sat there for another half hour to try to put together the pieces. If one succeeded, one really had learned enormously much.
>
> Interview mit Richard Courant[a]

[a] https://www.aip.org/history-programs/niels-bohr-library/oral-histories/4562

Zur Auflockerung habe ich an einigen Stellen Zitate eingestreut. Ich denke, dass sie alle (mindestens) ein Körnchen Wahrheit enthalten. Aber sie sollten sie nicht zu ernst nehmen.

Neben dem Skript umfasst die Vorlesung die folgenden Teile:

- Auf der Moodle-Seite zur Vorlesung finden Sie alle wichtigen Informationen zur Vorlesung sowie Links zu allen Materialien, die im Rahmen der Vorlesung bereitgestellt werden.
- Lernvideos – ich werde Ihnen wöchentlich Lernvideos zur Verfügung stellen, in denen ein Überblick über die wichtigen Themen der Vorlesungswoche gegeben wird; einige Ergebnisse und Beweise im Detail diskutiert werden; und eine oder mehrere Übungsaufgaben der Vorwoche erklärt werden,
- Fragestunde – einmal wöchentlich findet eine Videokonferenz statt, in der Ihre Fragen behandelt werden können und eventuell weitere Aufgaben besprochen werden können,
- Übungsgruppe – einmal wöchentlich findet (nach jetzigem Stand in Präsenz am Campus Essen) eine Übungsgruppe statt, in der Sie in einer Gruppe von ca. 20 Studierenden Fragen stellen und diskutieren können, und zusammen einfache Aufgaben zum Vorlesungsstoff bearbeiten können,

- Hausaufgaben – jede Woche wird ein Übungsblatt mit Aufgaben herausgegeben, deren Lösungen Sie in der Folgewoche abgeben müssen (gescannt, per Email). Die Übungsleiter∗innen korrigieren die Lösungen und schicken Sie Ihnen zurück. Für die Zulassung zur Klausur benötigen Sie mindestens 50% der in den Hausaufgaben erreichbaren Punkte.

  Sie können und sollten die Aufgaben in einer Gruppe von zwei oder drei Personen abgeben. Die mit dem abgegebenen Übungsblatt erzielten Punkte werden dann jedem Mitglied dieser Gruppe zugeschrieben.

- Online-Aufgaben und Online-Tests – regelmäßig werden Ihnen auf der Moodle-Seite (und per Link im Skript) Online-Aufgaben zur Verfügung gestellt, an denen Sie vor allem Ihre Rechenfertigkeiten üben können. Diese Aufgaben sind freiwillig und fließen nicht in Ihre Punktzahlen ein. Sie können sie auch mehrfach bearbeiten. Meistens werden die Zahlenwerte jeweils neu erzeugt, so dass es nicht so schnell langweilig wird.

  Dreimal im Semester werde ich einen Online-Test auf die Moodle-Seite stellen. Für die Zulassung zur Klausur benötigen Sie mindestens 50% der in den Online-Tests erreichbaren Punkte.

- Eine Online-Version des Skripts finden Sie unter math.ug/la1-ws2021/[1]. Dort können Sie einige Teile »einklappen« (zum Beispiel die Ergänzungen) und dadurch eventuell besser das ausblenden, womit Sie sich nicht beschäftigen möchten. Ganz zufrieden bin ich noch nicht mit der Formatierung; ich hoffe, im Laufe der Zeit noch einige Sachen verbessern zu können. Rückmeldungen sind aber auch jetzt schon willkommen.

Einige dieser Sachen sind (auch) für mich ein Experiment – teilweise, aber nicht nur, der speziellen Situation in diesem Semester geschuldet. Insofern bin ich dankbar für Kommentare, was aus Ihrer Sicht gut, und was weniger gut funktioniert. Ich werde versuchen darauf einzugehen und gegebenenfalls, auch im Licht meiner eigenen Erfahrungen, einige Dinge im Lauf des Semesters ändern. Die Moodle-Seite wird jedenfalls als Fixpunkt bleiben, wo Sie immer die aktuellen Informationen finden können.

1.3. Wie denkt man über ein mathematisches Problem nach? *

… oder umformuliert: Wie löst man ein mathematisches Problem? (In Ihrem Fall heißt das erstmal: Wie löse ich eine Übungsaufgabe? Und in einigen Monaten dann: Wie löse ich eine Klausuraufgabe?)

Dies ist offenbar eine entscheidende Frage, um erfolgreich das Mathematik-Studium zu absolvieren (und auch, um darüberhinaus Mathematik zu erforschen).

Leider kennt niemand eine einfache Antwort darauf. Allerdings sind sich alle einig, dass man diese Fertigkeit trainieren und weiterentwickeln kann. Deshalb werden wir das Problemlösen ausführlich üben.

Einige allgemeingültige Hinweise kann man aber trotzdem geben, hier gemünzt auf die Bearbeitung einer Übungsaufgabe:

- Stellen Sie sicher, dass Sie die Aufgabenstellung verstehen. Vergegenwärtigen Sie sich die Definitionen aller Fachbegriffe, die in dieser Aufgabe vorkommen, oder schlagen Sie sie gegebenenfalls nach. Machen Sie sich klar, was zu tun ist: eine Rechnung, der Beweis einer Gleichheit oder einer Folgerung, das Finden eines Beispiels, …

- Erinnern Sie sich an Ergebnisse, die zu den in der Aufgabe vorkommenden Begriffen in der Vorlesung behandelt wurden. Gibt es eine äquivalente Charakterisierung? Gab es Beispiele?

[1] https://math.ug/la1-ws2021/

- Überlegen Sie sich, ob die Aussage, die Sie zeigen sollen, für Sie plausibel ist. Können Sie Beispiele angeben, in denen sie richtig ist? Oder versuchen Sie, ein Gegenbeispiel zu finden. (Wenn Sie zeigen können, dass das nicht geht, sind Sie auch fertig …)
- Welche Standardverfahren könnte man anwenden, um die Aufgabe zu lösen? Das kann ein Rechenverfahren (Gauß-Algorithmus) oder ein Beweisverfahren (Beweis durch vollständige Induktion, Widerspruchsbeweis, …) sein, das Sie schon kennengelernt haben.

Natürlich wird es viele Aufgaben geben, wo Sie diese Schritte nicht alle durchgehen müssen, weil Sie direkt sehen, was zu tun ist. Und manchmal wird es auch eine Aufgabe geben, die Sie auch mit dieser »Anleitung« noch nicht lösen können.

In diesem Fall: **Stellen Sie Fragen!** Sie sollten versuchen, viele Fragen zu stellen. Nicht nur zu den Übungsaufgaben, die Sie im Moment nicht lösen können, sondern auch zu Schritten im Skript oder den Videos, die Sie nicht verstanden haben, und ganz allgemein zu den Begriffen, die Sie in der Vorlesung kennenlernen.

Wieso, weshalb, warum?

Manchmal ist es nicht so einfach, gute Fragen zu stellen. Arbeiten Sie daran, Ihre Fragen zu konkretisieren (vielleicht, indem Sie sie aufschreiben) und stellen Sie sie – sich selbst, anderen Studierenden, Ihrer Übungsleiter∗in , in der Fragestunde. Nehmen Sie sich Zeit, gute Fragen zu finden. Je mehr Sie sich in Übungs und Fragestunde aktiv beteiligen statt nur zuzuhören, desto mehr werden Sie profitieren. Es lohnt sich, Zeit zur Vorbereitung zu investieren.

Sie werden sehen, dass es einem selbst hilft, etwas zu erklären, das man schon verstanden hat (oder glaubt, verstanden zu haben). Deshalb können Sie grundsätzlich davon ausgehen, dass jede∗r gerne bereit sein wird, sich Ihre Fragen anzuhören und Ihnen zu helfen.

Gute Fragen zu finden ist nicht leicht! Sie zu stellen, kostet vielleicht Überwindung; in der Corona-Zeit kann man nicht direkt in der Vorlesung, und nicht so leicht in der Vorlesungspause/auf dem Flur/im LuDi anderen Studierenden eine Frage stellen. Machen Sie sich bewusst, dass es trotzdem den Aufwand wert ist, Ihre Fragen zu stellen und anderen mit deren Fragen zu helfen.

Versuchen Sie, Ihre Arbeitszeit sinnvoll zu nutzen: Reservieren Sie sich genügend Qualitätszeit, in der Sie ausgeruht und ungestört sind, für das Studium. Dass man die richtige Idee hat, muss man vorbereiten – es bringt nichts, stundenlang auf ein leeres Blatt zu starren, wenn man gar nicht weiß, wo man anfangen soll. Versuchen Sie dann, die oben genannten Schritte durchzuführen (Definitionen und verwandte Sätze nachschauen, Beispiele finden, Fragen formulieren). Wenn nichts hilft, dann gehen Sie zur nächsten Aufgabe.

Wie bearbeite ich ein Übungsblatt[a] von Manfred Lehn (Univ. Mainz).

[a] https://www.agtz.mathematik.uni-mainz.de/wie-bearbeitet-man-ein-uebungsblatt-von-prof-dr-manfred-lehn/

Es gibt viele Bücher zu dem Thema »Wie löse ich ein mathematisches Problem« (oder eine Aufgabe), siehe Anhang C.3 für eine kleine Auswahl.

1.4. Gute wissenschaftliche Praxis

Ein Thema, das mir am Herzen liegt und das ich daher hier ganz an den Anfang stelle, sind die Regeln Guter Wissenschaftlicher Praxis. »Gute wissenschaftliche Praxis« bedeutet, Wissenschaft ehrlich und redlich zu betreiben. Für die Veröffentlichung von wissenschaftlichen Texten bedeutet das insbesondere:

- Keine Ergebnisse als korrekt/vollständig darzustellen, von denen man weiß, das sie das nicht sind,
- keine Daten (oder Ergebnisse) zugrundezulegen, von denen man weiß, dass sie nicht korrekt/stichhaltig sind (oder die man gar selbst verfälscht oder den eigenen Wünschen angepasst hat),
- die Urheberschaft der Ergebnisse vollständig und zutreffend anzugeben.

Gute wissenschaftliche Praxis[a] an der Universität Duisburg-Essen.

[a] `https://www.uni-due.de/de/gute-wissenschaftliche-praxis/`

Zu Recht erhält dieses Thema in Bezug auf Plagiate in Doktorarbeiten in den letzten Jahren auch in der Öffentlichkeit Aufmerksamkeit. Es ist eine wesentliche Bedingung für das Funktionieren von Wissenschaft, dass diese Grundregeln eingehalten werden. Das beginnt »im Kleinen« – auch an Master-Arbeiten und Bachelor-Arbeiten wird der Anspruch gestellt, dass Ergebnisse (und erst recht wörtliche Zitate, die allerdings in mathematischen Texten selten sind), die aus anderen Quellen übernommen werden, entsprechend gekennzeichnet sind.

Gute wissenschaftliche Praxis[a] bei der Deutschen Forschungsgemeinschaft.

[a] `https://www.dfg.de/foerderung/grundlagen_rahmenbedingungen/gwp/`

Dies sollten Sie sich von vorneherein zur Gewohnheit machen. Für Ihre Vorlesungen bedeutet das: Lösungen von Übungsaufgaben werden nicht von Kommiliton∗innen abgeschrieben. Andere Quellen (Bücher, Skripte, Internetseiten), die Sie benutzen, müssen genannt werden.

Verschenken Sie nicht die Gelegenheit, eine Rückmeldung zu Ihren eigenen Bemühungen zu erhalten. Verschwenden Sie nicht die Zeit Ihrer Übungsleiter∗in dadurch, dass diese eine abgeschriebene Lösung korrigieren muss.

1.5. Zu erwartender Arbeitsaufwand

Das Mathematikstudium ist nicht unbedingt ein einfaches Studium – der Arbeitsaufwand ist hoch. Dafür ist es auch ein besonders interessantes und besonders nützliches Studium. Sie werden viel lernen, und zwar interessante Mathematik und gleichzeitig Ihre Kompetenzen erweitern, komplexe Probleme zu analysieren und zu lösen, und diese Lösungen präzise und verständlich anderen Personen darzustellen. Dass Mathematiker∗innen das können, ist aus meiner Sicht der Hauptgrund dafür, dass sie sich um ihre Berufsaussichten keine Sorgen machen müssen: Mathematiker∗innen sind gefragt in vielen verschiedenen Branchen, und das war in den letzten Jahrzehnten durchgängig genauso.

Die Einrichtung von Bachelor- und Master-Studiengängen hat es mit sich gebracht, dass das Studium kleinteiliger organisiert wurde als vorher und dass man versucht, viele Schritte genau zu quantifizieren. Der durchschnittliche Arbeitsaufwand für einen Credit-Punkt wird auf 30 Stunden festgelegt. Die 9 Credit-Punkte, die für die Vorlesung *Lineare Algebra 1* erreicht

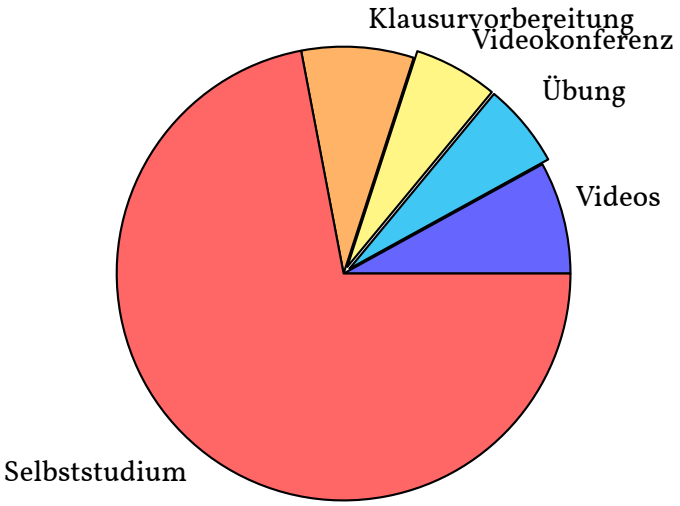
werden, entsprechen also ungefähr einem Arbeitsaufwand von 270 Stunden. Das ist eine ganze Menge!

Das soll nun nicht bedeuten, dass ich dieser Rechnung zustimme. Mindestens ist sie mit Vorsicht zu genießen, schon allein weil der Aufwand individuell sehr verschieden ist (einerseits, wie viel nötig ist; andererseits, zu wie viel die/der Einzelne Lust hat).

Etwas genauer ist es an der Uni Duisburg-Essen so, dass die Credit-Punkte für das *Modul* Grundlagen der Linearen Algebra vergeben werden, das die beiden Vorlesungen Lineare Algebra 1 und 2 umfasst, und das dann 18 CP wert ist. Insofern ist, wenn man überhaupt Arbeitsstunden ausrechnen möchte, ein Teil der oben genannten 270 Stunden in die vorlesungsfreie Zeit zur Nachbereitung zu verlagern, und ein Teil für die Vorbereitung auf die abschließende mündliche Prüfung (die auch die Note bestimmt) einzuplanen.

Jedenfalls: **Das Studium ist ein Vollzeitjob.**

Wie das Diagramm illustriert, das eine grobe Aufteilung der veranschlagten Arbeitszeit zeigt, entfällt nur ein kleiner Teil der veranschlagten Arbeitszeit auf »Veranstaltungen« (in diesem Semester: Video-Fragestunde, Übungsgruppe). Das ist auch unter normalen Umständen nicht viel anders, mit dem Unterschied, dass Sie jetzt keine festen Termine für die Vorlesung selber haben, sondern selbst entscheiden können, wann Sie das Skript/die Videos anschauen (und sich eventuell mehr disziplinieren müssen, das tatsächlich zu tun, als wenn Sie zu einer festen Zeit zur Vorlesung kommen würden).



Was hier unter »Selbststudium« gefasst wird, kann (und sollte) natürlich viele verschiedene Formen annehmen, und soll insbesondere nicht heißen, dass Sie in dieser Zeit durchgehend allein arbeiten müssten. Zum Beispiel fällt mir ein:

- Bearbeitung der Hausaufgaben,
- Bearbeitung von Online-Aufgaben,
- sich mit anderen Studierenden treffen und zusammen arbeiten (Fragen stellen und beantworten),
- auf der Moodle-Seite Fragen stellen und beantworten,
- Vorbereitung auf die Übungsgruppe und die Fragestunde
- das Nacharbeiten des Skripts,
- »selber denken«,
- gegebenenfalls andere Quellen lesen/durcharbeiten, …

Bei einem Problem »festzustecken« ist für die Mathematiker∗in nicht ungewöhnlich. Auch in der Forschung steckt man sozusagen einen großen Teil der Zeit fest. Das bedeutet, dass man sich davon allein nicht zu sehr irritieren lassen sollte. Andererseits bedeutet es, dass man Strategien finden muss, um in diesem Zustand weiterzukommen. Denn das Feststecken einfach hinzunehmen, bringt einen der Lösung natürlich auch nicht näher. Oft lohnt es sich, noch einmal die Definitionen der relevanten Begriffe darüber nachzuschauen und sich an Beispielen zu illustrieren; die Ergebnisse zu wiederholen, die man über diese Begriffe kennt (bzw. kennen sollte), und nachzuvollziehen, wie sie bewiesen wurden; zu überlegen, ob man das Problem lösen könnte, wenn man es ein bisschen verändert…
Ein Link zum Thema zum Blog »Math with bad drawings« von B. Orlin: The state of being stuck[a]

[a] https://mathwithbaddrawings.com/2017/09/20/the-state-of-being-stuck/

Mein Ziel ist es, Ihnen das Lernen so leicht wie möglich zu machen. Ich bin aber für Anregungen, was man verbessern könnte, offen und dankbar. Einen Weg, auf dem dies möglich wäre, ohne dass Sie sich anstrengen müssten, kenne ich leider nicht.

Meine ehrliche Hoffnung ist, dass Sie den hohen Arbeitsaufwand nicht als etwas Negatives sehen, sondern sich darauf einlassen. Die Zeit des Studiums kann und soll eine schöne Zeit des Lebens sein, in der Sie die Möglichkeit haben, viel Zeit mit etwas zu verbringen, das Sie wirklich interessiert. Mathematik zu verstehen und seine eigenen Fortschritte zu sehen, ist sehr befriedigend, und Durchhaltevermögen wird zusätzlich belohnt mit einem Studienabschluss, der Ihnen exzellente Berufsaussichten eröffnet.

KAPITEL 2

Die Vorlesung »Lineare Algebra 1«

2.1. Lernziele

In diesem Abschnitt möchte ich Ihnen kurz die Lernziele dieser Vorlesung vorstellen. Die mathematischen Begriffe, die in 2.1.2 und 2.1.3 genannt werden, kennen Sie jetzt natürlich größtenteils noch nicht; die Listen dort dienen dazu, dass Sie gegebenenfalls später darauf zurückkommen können.

2.1.1. Allgemeines. (Dies ist gewissermaßen das Wichtigste, und vielleicht auch das Schwierigste …)

(1) Mathematische Sprache verstehen,
(2) Definitionen und Aussagen verstehen und präzise wiedergeben,
(3) Beweise nachvollziehen, auf Korrektheit/Vollständigkeit prüfen und reproduzieren,
(4) Beweise selbst finden und verständlich dokumentieren.

Diese Kompetenzen gehen ineinander über. (Zum Verstehen muss man »Details einfüllen«, d.h. Mini-Beweise selbst entwickeln. Je weiter man kommt, desto mehr …)

Auch wenn man nicht forschende Mathematiker∗in werden möchte, muss man im Mathematikstudium beweisen lernen. Denn um den Stoff des Studiums zu meistern, muss sich die Lerngeschwindigkeit im Laufe der Zeit erhöhen, das bedeutet, dass in Vorlesungen späterer Semester Details, die in den Anfängervorlesungen ausführlich begründet werden, nicht weiter erklärt werden: Die Student∗in muss sich selbst überlegen, warum etwas richtig ist, d.h., einen (kleinen oder manchmal auch größeren) Beweis »einfüllen«. Umso mehr gilt das, wenn man seine Bachelor-Arbeit schreibt oder Forschungsartikel lesen möchte, wie bei der Vorbereitung auf ein (Master-)Seminar oder bei der eigenen Masterarbeit.

Diese Fertigkeit (Problemlösen, Strukturen erkennen, …) ist das Wichtigste, was diejenigen aus dem Mathematikstudium mitnehmen, die später nicht an der Uni bleiben (oder in der Schule unterrichten). Und sie ist auch der Hauptgrund, warum Mathematiker*innen keine Sorgen zu haben brauchen, ob sie einen Arbeitsplatz finden.

2.1.2. Begriffe der Linearen Algebra. Sie sollen am Ende der Vorlesung vertraut sein mit den folgenden Themen/Objekten/Begriffen:

(1) Mengen, Abbildungen
(2) Körper
(3) Lineare Gleichungssysteme
(4) Vektorraum, Untervektorraum
(5) linear (un-)abhängig, Erzeugendensystem, Basis, Dimension
(6) lineare Abbildungen, Kern, Bild, Rang, Dimensionsformel für lineare Abbildungen
(7) Zusammenhang lineare Abbildungen und Matrizen, Zeilenrang/Spaltenrang
(8) Gruppen, S_n, $GL_n(K)$, $SL_n(K)$

(9) Determinanten (einer Matrix, eines Endomorphismus), Cramersche Regel
(10) Eigenwerte und Eigenvektoren (Grundbegriffe)

Schauen Sie auch einmal in das Modulhandbuch zu Ihrem Studiengang:
Bachelor Mathematik[a] (Seite 6), Lehramt GyGeBK[b] (Seiten 9ff.)

[a] https://www.uni-due.de/imperia/md/content/mathematik/2016_04_12_modulhandbuch-ba-aktiv.pdf
[b] https://www.uni-due.de/imperia/md/content/didmath/lehre/mhb_ba_gyge_190523.pdf

2.1.3. Rechenmethoden.

(1) Gauß-Algorithmus (zum Beispiel zur Lösung von linearen Gleichungssystemen; Bestimmung von Kern und Bild einer Matrix; Bestimmung von Basen; Berechnung von Determinanten)
(2) Rechnen mit Matrizen (Matrizenprodukt, Determinanten)
(3) Bestimmung von Eigenwerten und Eigenräumen eines Endomorphismus/einer Matrix

Die Rechenmethoden stehen hier bewusst an letzter Stelle (auch wenn wir in der Vorlesung recht bald zu dem zentralen Gauß-Algorithmus kommen werden), weil die anderen Punkte wichtiger sind. Dennoch empfehle ich, auch viel zu rechnen, weil das erstens ausreichend geübt werden muss, damit es fehlerfrei und zügig funktioniert, und zweitens das Verständnis der abstrakten Begriffe profitiert, wenn man sich genügend viele Beispiele rechnerisch erarbeitet hat.

Manchmal wird unterschieden zwischen *Rechenaufgaben* und *Beweisaufgaben*. Der Übergang ist natürlich fließend und auch für eine »Rechenaufgabe« werden Sie oft erstmal ein bisschen nachdenken müssen, um herauszufinden, welche Rechnung überhaupt gefragt ist. Aber in der Tat gibt es verschiedene Kompetenzen, die beide wichtig sind: Einerseits, eine Rechnung korrekt und in angemessener Zeit durchführen zu können; andererseits, eine Aussage begründen (oder gegebenenfalls widerlegen) zu können. In beiden Fällen ist es wichtig, dass Sie Ihre Lösung angemessen dokumentieren können.

Die Rechenkompetenz allein lässt sich gut in den Online-Aufgaben abdecken, außerdem fallen die Rechenaufgaben in der Regel den Studienanfänger∗innen leichter. Deshalb liegt in den Hausaufgaben, die Sie abgeben müssen und die dann per Hand korrigiert werden, und in der Klausur der Schwerpunkt auf den Beweisaufgaben. Dabei geht es nicht darum, geniale Ideen zu entwickeln, sondern einfache Zusammenhänge (wieder) zu erkennen und verstandene Argumente klar dokumentieren zu können.

Online-Aufgaben mit NUMBAS

Zur Vorlesung werden Online-Aufgaben angeboten, die auf dem System NUMBAS[a] basieren, das an der Newcastle University entwickelt wird.
Die Online-Aufgaben werden auf der Moodle-Seite der Vorlesung verlinkt.

[a] https://www.numbas.org.uk/

2.2. Wozu Lineare Algebra?

2.2.1. Wozu man Lineare Algebra braucht (oder gebrauchen kann), lässt sich natürlich leichter jemandem erklären, der schon etwas über Lineare Algebra weiß (und am besten

auch etwas über die Problemstellungen weiß, wo man eine Anwendung finden kann). Trotzdem dazu einige Bemerkungen. Die Lineare Algebra hat sich aus der Theorie der linearen Gleichungssysteme entwickelt, und so ist auch diese Vorlesung aufgebaut. Wir suchen also beispielsweise alle reellen Zahlen x, y, die die beiden Gleichungen

$$3x + y = 7$$
$$x - 2y = \frac{2}{3}$$

erfüllen. Diese Art von Fragestellung kennen Sie aus der Schule und haben wahrscheinlich keine Schwierigkeiten, die Lösungsmenge des Gleichungssystems zu bestimmen. Wir werden aber in Kürze Fragen stellen und Antworten kennenlernen, die über den Schulstoff weit hinausgehen.

> Ich habe bey mir von Jugend auff eine unersättliche Begierde die Wahrheit gewiß zu erkennen und anderen zu dienen gefunden. Daher als ich bey Zeiten vernahm, daß man der Mathematick eine ungezweiffelte Gewißheit zuschreibe, und absonderlich die Algebra als eine richtige Kunst verborgene Wahrheiten zuentdecken rühme; Hingegen aus den so vielfältigen und wiedrigen Meinungen der Gelehrten in anderen Sachen, die zur Mathematick nicht gehören, und aus den steten Aenderung, die darinnen vorgenommen werden, mir auch dazumahl genung begreiflich war, daß es ausser der Mathematick an einer völligen Gewißheit meistentheils fehle; Erweckte bey mir die Begierde zur Warheit eine Liebe zur Mathematick und sonderlich eine Lust zur Algebra, um zusehen, was doch die Ursache sey, warum man in der Mathematick so große Gewissheit habe, und nach was vor Regeln man daselbst dencke, wann man verborgene Wahrheiten zum Vorscheine bringen will, damit ich mich desto sicherer bemühen möchte auch ausser der Mathematick dergleichen Gewißheit zu suchen ...
>
> Aus der Vorrede zu *Mathematisches Lexicon*, C. Wolffen, Leipzig 1716; gefunden in [Jä].

Wenn Sie fragen **»Wozu brauche ich das?«**, dann hoffe ich, dass die erste Antwort ist: Weil es Sie interessiert, eine mathematische Theorie kennenzulernen. Oder genauer: Das Problemgebiet der Linearen Gleichungssysteme strukturell und systematisch kennenzulernen, daran zu sehen, wie Mathematik auf Hochschulniveau betrieben wird, offene Fragen kennenzulernen und eine Grundlage für das gesamte weitere Mathematikstudium zu legen.

> In the broad light of day mathematicians check their equations and their proofs, leaving no stone unturned in their search for rigour. But, at night, under the full moon, they dream, they float among the stars and wonder at the miracle of the heavens. They are inspired. Without dreams there is no art, no mathematics, no life.
>
> Michael Atiyah (NAMS Jan 2010 p.8)
>
> Fundort: https://www.jmilne.org/math/

Ich werde versuchen, dieses Interesse zu erhalten und weiter zu nähren, indem ich im Skript an vielen Stellen optionale Ergänzungen einfüge, die Verbindungen zu anderen Bereichen

der Mathematik und zu konkreten Fragen aufzeigen, die man mit Linearer Algebra lösen kann. In der »Vorlesung« selbst werden wir uns allerdings auf den Kernstoff konzentrieren. Wenn Ihnen das ausreicht, ist es völlig in Ordnung, wenn Sie diese Ergänzungen nicht weiter beachten. Wenn es Ihnen leichter fällt, sich durch den eigentlichen Stoff durchzubeißen, wenn Sie wissen, dass er auch zu etwas gut ist (und sich nicht darauf verlassen möchten, dass ich Ihnen das versichere), dann können Sie auf die Ergänzungen zurückgreifen, die Sie ansprechen.

2.2.2. Bemerkungen zum Lehramtsstudium. Die Vorlesungen Lineare Algebra 1 und 2 sind auch Bestandteil des Lehramtsstudienganges Gymnasium/Gesamtschule/Berufskolleg. Ich möchte einige Bemerkungen dazu machen, warum ich das für sinnvoll halte. Natürlich ist der Vorlesungsstoff überwiegend nicht Unterrichtsstoff. Und auch wenn Sie mit Sicherheit vom fachmathematischen Anteil des Studium für die Tätigkeit an der Schule profitieren, will ich nicht verheimlichen, dass es eines nicht geringen Aufwands bedarf, wenn Sie aus dem Vorlesungsstoff das maximal Mögliche für den Schulunterricht herausholen wollen. Warum sollten Sie trotzdem die regulären Anfängervorlesungen des Bachelor-Studiengangs Mathematik besuchen?

- Am wichtigsten aus meiner Sicht: Es ist für eine Mathematiklehrer∗in essenziell, präzise formulieren zu können (und das ihren Schüler∗innen mitzugeben); und entscheiden zu können, ob eine mathematische Aussage wahr oder falsch ist, und das begründen zu können.

  Das lernt man in der Schule oft nicht ausreichend. Um hier eine hinreichend hohe Sicherheit zu erreichen, muss man diese Fertigkeiten trainieren. Und dann bietet es sich ja an, dieses Training anhand des grundlegenden Stoffs der Mathematik durchzuführen, wie er in den Vorlesungen Lineare Algebra und Analysis behandelt wird.

  Bedenken Sie, dass es ein großer Luxus des Faches Mathematik ist, dass man sich sicher sein kann, dass alles, was man erklärt, auch richtig ist, und man das auch überprüfen kann.

- Lineare Algebra ist Schulstoff (natürlich nicht alles, was in der Vorlesung vorkommt; aber es ist wichtig, dass die Lehrer∗in einen Überblick und einen deutlichen Wissensvorsprung vor den Schüler∗innen hat.)

- Eine der Aufgaben der gymnasialen Oberstufe ist die Vorbereitung auf ein mögliches Studium und eine Mathematiklehrer∗in sollte vermitteln können, wie Mathematik an der Universität betrieben wird.

Es ist nun so, dass der Stoff in der Vorlesung nicht mundgerecht für den Unterricht aufbereitet wird – nicht einmal näherungsweise: Teilweise ist eine erhebliche »Übersetzungsarbeit« zu leisten. Das kann nicht innerhalb dieser Vorlesung geschehen. Schon alleine aus Zeitgründen, aber auch, weil das besser jemand macht, der mehr Kontakt zur Lehrerausbildung hat als eine Professor∗in in der Fachmathematik. Es gibt fachdidaktische Veranstaltungen in Ihrem Studium, die sich dem widmen und Materialien, die Sie dabei unterstützen können.

Übrigens ist diese Diskrepanz ein klassisches Thema, siehe die Bücher Elementarmathematik vom höheren Standpunkt[I] von Felix Klein (erste Auflage um 1908), die historisch und mathematisch interessant sind, die man mit insgesamt über 850 Seiten allerdings nicht mal eben an einem Nachmittag durchliest.

[I] https://gdz.sub.uni-goettingen.de/id/PPN376497785

Weitere Quellen:

B. Schwarz, P. Herrmann, Bezüge zwischen Schulmathematik und Linearer Algebra in der hochschulischen Ausbildung angehender Mathematiklehrkräfte – Ergebnisse einer Dokumentenanalyse[a], Mathematische Semesterberichte **62** (2015), 195–217.

B. Schwarz, P. Herrmann, G. Kaiser, B. Richter, J. Struckmeier, Lineare Algebra in der Lehramtsausbildung – Wenig Bezug zum Mathematikunterricht?[b]

[a] https://link.springer.com/article/10.1007/s00591-015-0147-7
[b] https://www.math.uni-hamburg.de/home/richter/la-lehramtsbezug.pdf

2.2.3. Anwendungen der Linearen Algebra. Eine etwas andere als die oben genannte ist die Frage **»Wozu braucht man das/kann man das gebrauchen?«**. Mit Antworten darauf könnte man speziell in Bezug auf die Lineare Algebra ganze Bücher füllen, und diese Anwendungen können natürlich auch in Ihre persönliche Antwort auf die Frage einfließen, warum Sie lineare Algebra lernen möchten.

Wichtige Gründe, warum die Lineare Algebra an so vielen Stellen nützlich ist, sind, dass man lineare Gleichungssysteme einerseits theoretisch viel besser versteht als Systeme von allgemeineren Gleichungen, und sie andererseits tatsächlich lösen kann, selbst wenn sie einigermaßen groß sind, anders als viele andere Arten/Systeme von Gleichungen (irgendwo gibt es natürlich auch hierbei Grenzen). Außerdem kommen lineare Strukturen praktisch »überall« vor, zumindest näherungsweise.

Ein gutes Beispiel ist die **Analysis.** Es ist die grundlegende Strategie der Differentialrechnung, zu einer (differenzierbaren) Funktion die bestmögliche Annäherung durch eine *lineare* Funktion zu suchen. Die Steigung dieser Geraden ist die Ableitung an der betrachteten Stelle. Während die Theorie der linearen Funktionen $\mathbb{R} \to \mathbb{R}$, also von den reellen Zahlen in sich, so einfach ist, dass man alles Benötigte ad hoc bereitstellen kann, ist es in höheren Dimensionen sinnvoll, diesen Teil der Theorie auf eine systematische Grundlage zu stellen. In der Analysis 2 und Analysis 3 werden die Begriffe des Vektorraums (Definition 6.1) und der linearen Abbildung (Definition 7.1) ein wichtiges Hilfsmittel sein.

Ähnlich ist es in Numerik, Optimierung, Wahrscheinlichkeitstheorie, … In fast allen Bereichen der Mathematik wird Lineare Algebra benutzt. Die Begriffe des Vektorraums und der Gruppe (Definition 9.1, sozusagen die mathematische Art und Weise, über Symmetrie zu sprechen, vergleiche Abschnitt 9.1.1) spielen praktisch überall in der Mathematik eine Rolle. Besonders natürlich in den fortgeschrittenen Vorlesungen der Algebra-Schiene: Algebra, Kommutative Algebra, Algebraische Geometrie, Algebraische Zahlentheorie. Da diese sequentiell aufeinander aufbauen, ist es aber – im Vergleich etwa zur Graphentheorie (siehe Kapitel 14), die nicht viele Vorkenntnisse benötigt – schwieriger, das an dieser Stelle zu illustrieren – Sie müssen sich also noch etwas gedulden, um die Lineare Algebra dort im Einsatz zu sehen.

2.3. Konkrete Fragen, die wir im Laufe der Vorlesungen Lineare Algebra 1/2 werden beantworten können *

Um den vorherigen Abschnitt nicht vollständig im Vagen zu lassen, nenne ich hier einige Fragen/Problemstellungen, die wir mit den im Laufe der Vorlesung entwickelten Methoden beantworten oder mindestens besser verstehen können.

Zum Teil handelt es sich um »Anwendungen« von Methoden der linearen Algebra auf mathematische Probleme, wo diese nicht offensichtlich sind. Zum Teil handelt es sich um

Anwendungen, die außerhalb der Universität wichtig sind. Viele (mindestens ebenso interessante) Anwendungen innerhalb der Mathematik müssen leider außen vor bleiben, weil mehr Mathematik benötigt wird, als uns im Moment zur Verfügung steht, um über diese Probleme überhaupt zu sprechen.

(Für viele der folgenden Fragen/Probleme gibt es mehrere verschiedene Lösungsansätze. Man muss nicht immer Lineare Algebra benutzen – aber oft ist es möglich und nützlich.)

Wenn Ihnen die Formelsprache zu kompliziert ist, dann überspringen Sie die Frage erstmal. Es wird nicht lange dauern, bis Ihnen das keine Probleme mehr bereitet, und dann können Sie noch einmal hierher zurückkommen.

FRAGE 2.1. Die Fibonacci-Folge[2] (siehe auch Wikipedia (Englisch)[3]) ist die Folge natürlicher Zahlen, die gegeben ist durch

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ für alle } n \geq 2.$$

Die ersten Terme der Folge lauten also 0, 1, 1, 2, 3, 5, 8, 13, 21.

> Auf der Webseite mathe-vital.de[a] finden Sie (neben vielen anderen sehenswürdigen Visualisierungen, auch zur linearen Algebra) mehrere Seiten zu den Fibonacci-Zahlen.
> Die Fibonacci-Zahlen und … der Goldene Schnitt I[b], der Goldene Schnitt II[c], die Ananas[d].
>
> [a] https://mathe-vital.de/
> [b] https://mathe-vital.de/Botanik/4-1.html
> [c] https://mathe-vital.de/Botanik/4-3.html
> [d] https://mathe-vital.de/Botanik/4-6.html

Wir werden später die folgenden Fragen leicht mit Linearer Algebra beantworten können:

- Wie kann man möglichst schnell eine einzelne Fibonacci-Zahl F_n für großes n berechnen (zum Beispiel $F_{10\,000\,000\,000}$), ohne alle Fibonacci-Zahlen dazwischen berechnen zu müssen? Siehe Beispiel 5.60.
- Was ist eine geschlossene Formel für die n-te Fibonacci-Zahl F_n, in der die kleineren Fibonacci-Zahlen nicht auftreten? Siehe Ergänzung 6.54, Beispiel 11.9.

Die dabei verwendeten Methoden sind oft auch nützlich, um andere Folgen, die in ähnlicher Weise (durch eine »lineare Rekursionsgleichung«) definiert sind, zu analysieren. (Zum Teil lassen sich diese Fragen natürlich auch auf anderem Wege beantworten. Versuchen Sie es ruhig einmal!) □ Frage 2.1

FRAGE 2.2. Der folgende Satz ist wichtig für das Verfahren des Quadratischen Siebes[4], das ist eines der besten bekannten Verfahren, um sehr große ganze Zahlen in ihre Primfaktoren zu zerlegen. Die Frage, ob/wie man das »schnell« machen kann, ist von hoher Bedeutung für Verschlüsselungsverfahren (beziehungsweise die Frage, ob man sie knacken kann), die an allen möglichen Stellen eingesetzt werden (Online-Banking, …), zum Beispiel das RSA-Verfahren[5].

[2] https://de.wikipedia.org/wiki/Fibonacci-Folge
[3] https://en.wikipedia.org/wiki/Fibonacci_number
[4] https://de.wikipedia.org/wiki/Quadratisches_Sieb
[5] https://de.wikipedia.org/wiki/RSA-Kryptosystem

SATZ 2.3. *Gegeben seien eine natürliche Zahl $n \geq 1$ und n verschiedene Primzahlen $p_1, \ldots, p_n$. Wenn $a_1, \ldots, a_{n+1}$ natürliche Zahlen > 1 sind, in deren Primfaktorzerlegungen nur die Primzahlen $p_1, \ldots, p_n$ vorkommen, dann gibt es eine Möglichkeit, einige der Zahlen a_i so auszuwählen, dass ihr Produkt eine Quadratzahl ist.*

BEISPIEL 2.4. Wir betrachten die Primzahlen 2, 3 und 7 und die vier Zahlen 7, 12, 18, 21. Dann ist $7 \cdot 12 \cdot 21 = 4 \cdot 9 \cdot 49 = (42)^2$ eine Quadratzahl. ◊

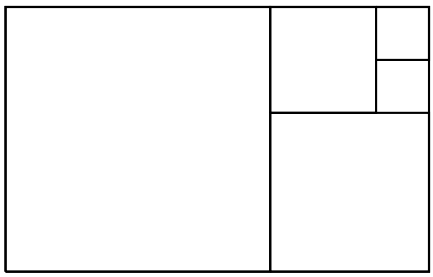
Wir kommen in Ergänzung 6.57 auf diese Frage zurück.

Siehe auch:
R.-H. Schulz, H. Witten, Faktorisieren mit dem quadratischen Sieb[a], LOG IN **172/173** (2011/12), 70–78.

[a] `https://bscw.schule.de/pub/bscw.cgi/d1024028/Schulz_Witten_Quadratisches_Sieb.pdf`

□ Frage 2.2

FRAGE 2.5. Wann kann man ein Rechteck wie in der Abbildung lückenlos durch Quadrate überdecken?



Es gilt der folgende Satz:

SATZ 2.6. *Sei R ein Rechteck mit Seitenlängen $a, b \in \mathbb{R}_{>0}$. Dabei sei $a \in \mathbb{Q}$ und $b \in \mathbb{R} \setminus \mathbb{Q}$. Dann lässt sich R nicht vollständig durch (endlich viele) Quadrate überdecken, die sich nicht überlappen.*

Wir werden das in Kapitel 7 beweisen können, siehe Ergänzung 7.16. □ Frage 2.5

Die nächste »Frage« ist ziemlich lang, aber ein gutes (und inzwischen ziemlich prominentes) Beispiel für eine Anwendung von Methoden der Linearen Algebra, mit denen (fast) jede∗r täglich in Kontakt ist.

FRAGE 2.7 (Googles Page-rank-Algorithmus). Wir wollen das Problem betrachten, eine gute Internet-Suchmaschine zu bauen. Wir stellen uns vor, dass bereits eine Datenbank aller Webseiten, die eine Benutzer∗in finden können soll, existiert. Die Frage, die wir betrachten wollen, ist, wie die Suchmaschine entscheidet, in welcher Reihenfolge die Treffer zu einem Suchbegriff angezeigt werden. Dass Google ziemlich schnell alle damaligen Mitbewerber fast vollständig vom Markt verdrängen konnte, lag wesentlich mit daran, dass bei Google viel verlässlicher die relevanten Treffer weit oben in der Liste der Suchergebnisse angezeigt wurden. Der Ansatz, den wir hier beschreiben, ist die Basis des Google-Algorithmus. (Genauer des Page-rank-Algorithmus, der die Grundlage für die Google-Suche in den ersten Jahren nach der Gründung war. Sicher wurden nicht alle Feinheiten verraten, und inzwischen wurde der Algorithmus weiterentwickelt und/oder durch andere Methoden ersetzt. Das Prinzip, das wir hier kennenlernen, ist aber natürlich nach wie vor von Bedeutung; die Frage, wie man »Wichtigkeit/Relevanz« in einem »Netzwerk« messen kann, stellt sich ja an vielen Stellen.)

Wir stellen uns vor, dass wir die Webseiten in unserer Datenbank durchnummerieren. Für jede Webseite wollen wir eine Zahl berechnen, die misst, wie »wichtig« diese Seite ist. Für die erste Seite in unserer Datenbank bezeichnen wir die zu findende Zahl mit x_1, für die zweite mit x_2 usw., also für die i-te Seite mit x_i. Je höher der Wert x_i ist, desto höher würde die Seite in der Liste der Suchergebnisse angezeigt, wenn sie bei den Treffern dabei ist. (Wenn Sie die Formelsprache hier oder in den nächsten Absätzen stört, dann springen Sie erstmal zu Beispiel 2.8.)

Dabei messen die Zahlen x_i die »Relevanz« einer Seite unabhängig von dem jeweiligen Suchbegriff. Wenn dann eine Suche ausgeführt wird, werden die entsprechenden Webseiten als »Treffer« aus der Datenbank ausgewählt und dann in der Reihenfolge ihrer Relevanz angezeigt.

Die erste wesentliche Überlegung ist, die Relevanz einer Webseite nicht durch eine komplizierte Analyse ihres Inhalts zu messen, sondern mit einer Methode, die sich leicht mit den erhobenen Daten umsetzen lässt. Im ersten Schritt stellen wir fest, dass eine Seite umso relevanter sein dürfte, je mehr andere Seiten auf sie verlinken. Wir könnten also einfach die Anzahl dieser Links für jeden Suchtreffer zählen und die Treffer dementsprechend anordnen. Wenn wir mit L_i die Menge aller Webseiten bezeichnen, die auf die i-te Seite verlinken, so könnten wir diesen Ansatz schreiben als

$$x_i = \#L_i, \quad \text{die Anzahl der Elemente in } L_i.$$

Wir wollen dabei nicht berücksichtigen, wenn eine Seite auf sich selbst verlinkt; es soll also i kein Element von L_i sein.

Es ist aber vernünftig, das Verfahren noch etwas zu verfeinern. Es sollte eine Rolle spielen, ob ein Link auf die betrachtete Seite von einer »wichtigen« oder »unwichtigen« Seite kommt. Wir sollten in der vorherigen Formel nicht für jedes Element j von L_i (wir schreiben dann $j \in L_i$) eine 1 zählen, sondern den Einfluss entsprechend gewichten – und zwar gerade mit der Zahl x_j, die die Relevanz der Seite j angibt. Ein besserer Ansatz wäre also

$$x_i = \sum_{j \in L_i} x_j,$$

das heißt x_i ist die Summe aller Werte x_j, wo die j-te Seite einen Link auf die i-te Seite hat. Wir benutzen hier das Summensymbol $\sum$ (der große griechische Buchstabe Sigma, siehe Beispiel 3.43) als Abkürzung für die Summe aller derjenigen x_j mit $j \in L_i$. Das macht einen komplizierten Eindruck. Denn wir können x_i nicht mehr direkt berechnen, weil wir für die Berechnung der x_j ja möglicherweise x_i schon kennen müssten (wenn $i \in L_j$ ist). Trotzdem ist es nicht so schlimm, wie es aussieht: Wir können die Gesamtheit dieser Gleichungen (für alle i) als ein sehr großes lineares Gleichungssystem in den Unbestimmten x_i auffassen.

Diese Änderung eröffnet noch die folgende Interpretationsmöglichkeit für die Zahlen x_i. Es ist klar, dass das obige Gleichungssystem (wenn es überhaupt eine Lösung hat, für die nicht alle x_i gleich Null sind) keine eindeutige Lösung haben kann; denn wenn wir eine Lösung haben, erhalten wir eine neue Lösung, indem wir jedes x_i mit derselben Zahl multiplizieren. Für die resultierende Sortierung nach Relevanz tut das aber nichts zu Sache (jedenfalls, wenn wir nur mit positiven Zahlen multiplizieren). Wenn wir optimistisch sind, könnten wir versuchen, die Zahlen x_i so zu suchen, dass sie alle zwischen 0 und 1 liegen und dass die Summe aller x_i gleich 1 ist. Damit stellt man sicher, dass die Skala nicht ausufert und man die Werte möglichst konkret festnagelt. So kann man zum Beispiel besser Vergleiche zwischen solchen Berechnungen für verschiedene »Netzwerke« anstellen.

Mit dieser Konvention kann man die Zahl x_i auch als *Wahrscheinlichkeit* interpretieren. Dazu stellen wir uns eine Internet-Surfer*in vor, die auf jeder Seite zufällig irgendeinen der Links auf andere Seiten aufruft. Dann ist x_i die Wahrscheinlichkeit, dass sie sich gerade

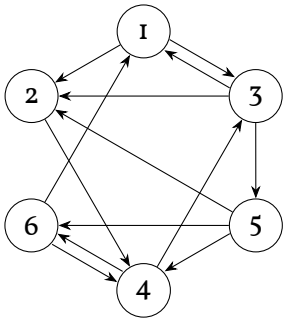
auf der i-ten Seite aufhält. Zum Beispiel würde $x_2 = 0,013 = 1,3\%$ bedeuten, dass die Wahrscheinlichkeit, sich dabei gerade auf der zweiten Seite zu befinden, $1,3\%$ ist.

Eine weitere Verbesserung des Verfahrens ist die folgende. Mit der obigen Formel könnte selbst eine relativ unwichtige Seite die Bewertung vieler anderer Seiten dadurch beeinflussen, dass sie sehr viele Links auf andere Seiten einbaut. Es ist daher vernünftig, ein Stimmgewicht einzuführen, das bewirkt, dass eine Seite ihre Relevanz sozusagen auf alle Seiten aufteilt, auf die sie verlinkt. Wir ersetzen daher die Gleichung oben durch

$$x_i = \sum_{j \in L_i} \frac{1}{n_j} x_j,$$

wobei n_j die Anzahl der ausgehenden Links von Seite j ist. (Weil $j \in L_i$ für alle j, die einen Beitrag zu der Summe liefern, verlinkt Seite j mindestens auf Seite i, also ist $n_j > 0$ und wir können durch diese Zahl teilen.)

Beispiel 2.8. Betrachten wir als Beispiel das in der Abbildung dargestellte Mini-Internet; Links sind dort als Pfeile dargestellt.



Die Daten, die wir brauchen, um das gesuchte Gleichungssystem aufzustellen, sind in der folgenden Tabelle gesammelt:

Seite	Verlinkt von	Anzahl ausgehende Links
1	3, 6	2
2	1, 3, 5	1
3	1, 4	3
4	2, 5, 6	2
5	3	3
6	4, 5	2

Aus diesen Daten stellen wir nach dem obigen Rezept das folgende lineare Gleichungssystem auf. Zum Beispiel erhalten wir folgendermaßen dir erste Gleichung: Auf die erste Seite verlinken die Seiten 3 und 6, also sind nur die Koeffizienten von x_3 und x_6 auf der rechten Seite der Gleichung $\neq 0$. Für den Koeffizienten von x_3 erhalten wir $\frac{1}{3}$, weil die dritte Seite 3 ausgehende Links hat. Die sechste Seite hat 2 ausgehende Links, also ist der Koeffizient von x_6 gleich $\frac{1}{2}$.

$$\begin{array}{lllllllllll}
x_1 &=& & & \frac{1}{3}x_3 & & & & & + & \frac{1}{2}x_6 \\
x_2 &=& \frac{1}{2}x_1 & + & \frac{1}{3}x_3 & & & + & \frac{1}{3}x_5 & & \\
x_3 &=& \frac{1}{2}x_1 & & & + & \frac{1}{2}x_4 & & & & \\
x_4 &=& & x_2 & & & & + & \frac{1}{3}x_5 & + & \frac{1}{2}x_6 \\
x_5 &=& & & \frac{1}{3}x_3 & & & & & & \\
x_6 &=& & & & & \frac{1}{2}x_4 & + & \frac{1}{3}x_5 & &
\end{array}$$

An dieser Stelle können wir schon eine Besonderheit feststellen, die bei der weiteren Betrachtung eine große Rolle spielen wird. Wenn man auf der rechten Seite alle Koeffizienten einer Spalte aufsummiert, dann ist die Summe immer gleich 1. Überzeugen Sie sich, dass das in der Tat eine direkte Konsequenz davon ist, wie wir das Gleichungssystem aufbauen. (Es gibt allerdings die Möglichkeit, dass als »Sonderfall« Spalten auftreten, in denen alle Koeffizienten $= 0$ sind. Wann wäre das der Fall?)

Eine Lösung dieses Gleichungssystems ist gegeben durch $(32, 36, 45, 58, 15, 34)$. Jedenfalls lässt sich leicht nachprüfen, dass diese Zahlen wirklich alle 6 Gleichungen erfüllen. Es ist auch nicht »schwierig«, diese Lösung (zum Beispiel durch Einsetzen und/oder Elimination von Variablen) zu finden. Allerdings macht es sich bei einem Gleichungssystem dieser Größe bezahlt, einen systematischen Ansatz zu wählen, wie wir ihn demnächst kennenlernen werden (den Gauß-Algorithmus, Abschnitt 5.2).

Wir hatten auch gesagt, dass wir als Summe der x_i gerne 1 erhalten möchten. Das ist natürlich mit der obigen Lösung nicht erfüllt. Wir können die Lösung aber skalieren: Wenn wir alle x_i mit derselben Zahl multiplizieren, oder durch dieselbe Zahl teilen, entsteht aus einer Lösung des Gleichungssystems eine neue Lösung. In diesem Fall teilen wir alle Einträge durch die Gesamtsumme 220. Wir erhalten die Lösung $(\frac{32}{220}, \frac{36}{220}, \frac{45}{220}, \frac{58}{220}, \frac{15}{220}, \frac{34}{220})$, wobei wir ausnahmsweise nicht gekürzt haben, weil es so ein bisschen übersichtlicher erscheint. Für diese Lösung ist die Summe aller x_i gleich $\frac{220}{220} = 1$. Außerdem liegen alle x_i zwischen 0 und 1. Man kann auch zeigen: Dies ist die *einzige* Lösung, so dass sich die Einträge zu 1 summieren. Das ist die Lösung des Page-rank-Problems in diesem Fall. Die wichtigste Seite ist Seite 4, mit Abstand am unwichtigsten (aus Sicht des Algorithmus) ist Seite 5. ◊

Auch im allgemeinen Fall handelt es sich hier nach wie vor um ein lineares Gleichungssystem (das wir über den rationalen oder über den reellen Zahlen betrachten können). Dies ist noch nicht ganz das endgültige Gleichungssystem des Page-rank-Algorithmus, aber wir verschieben die Diskussion der weiteren Verbesserungen auf Ergänzung 5.61, wo wir die zur Verfügung stehende Sprache schon etwas erweitert haben.

Quellen zum Page-rank-Algorithmus:

K. Bryan, T. Leise, The 25 000 000 000 eigenvector. The Linear Algebra behind Google[a], SIAM Review, Vol. **48**, No. 3 (2006), 569–581

D. Austin, How Google Finds Your Needle in the Web's Haystack[b] (dort finden Sie auch Verweise auf weitere Literatur zum Page-rank-Algorithmus und allgemeiner zu Suchmaschinen-Algorithmen)

Wikipedia: Deutsch[c], Englisch[d] (dort finden Sie auch eine Diskussion der Defizite des Page-rank-Algorithmus und (wenige) Informationen, wie Google ihn weiterentwickelt und inzwischen großenteils ersetzt hat)

[a] `https://www.rose-hulman.edu/%7Ebryan/googleFinalVersionFixed.pdf`
[b] `http://www.ams.org/publicoutreach/feature-column/fcarc-pagerank`
[c] `https://de.wikipedia.org/wiki/PageRank`
[d] `https://en.wikipedia.org/wiki/PageRank`

Wir wollen es hier dabei belassen, zwei Fragen zu formulieren:

(1) Gibt es eine Lösung für dieses Gleichungssystem, d.h. gibt es Zahlen x_i, die die Gleichungen erfüllen? Ist die Lösung (bis auf Skalieren) eindeutig bestimmt? (Denn wenn es mehrere Lösungen, also mehrere mögliche Rankings der Suchergebnisse gibt, ständen wir vor dem neuen Problem, wie wir uns zwischen diesen entscheiden könnten.)

(2) Wenn es eine eindeutige Lösung gibt, wie kann man sie (angesichts der in der Praxis riesigen Zahl an Gleichungen und Variablen) berechnen?

Wir werden in den Ergänzungen 5.61, 8.17 und 11.15 auf diese Fragen zurückkommen und sehen, dass Frage (1) nach Durchführung der angekündigten Verbesserungen eine positive Antwort hat (Satz 8.19), und es für Teil (2) Methoden gibt, die die spezielle Form dieses Gleichungssystems ausnutzen, siehe Ergänzung 11.15. □ Frage 2.7

FRAGE 2.9. Wie kann man große Datenmengen analysieren, effizient abspeichern und komprimieren? Diese Frage ist recht allgemein gehalten. Wir werden an mehreren Stellen darauf zurückkommen; teilweise erst in der Linearen Algebra 2.

Konkrete Anwendungen sind

- die (verlustfreie oder verlustbehaftete) Kompression von Bilddaten: Wie speichern Sie eine Bilddatei möglichst effizient ab, ohne Information zu verlieren – statt den Farbwert jedes einzelnen Bildpunktes abzuspeichern, möchte man ausnutzen, dass in typischen Bildern benachbarte Bildpunkte oft ähnliche Farbwerte haben. Was hat man für Möglichkeiten, den benötigten Speicherplatz noch deutlich stärker zu reduzieren, wenn man (kleine) Qualitätseinbußen in Kauf nimmt?
- Wie kann man die Qualität einer Datensammlung (beispielsweise wieder einer Bilddatei) verbessern, indem man Fehler (»noise«) sozusagen ausbügelt?

□ Frage 2.9

Wir werden nach und nach mit den Begrifflichkeiten, die zum jeweiligen Zeitpunkt zur Verfügung stehen, weitere Fragen entdecken/sehen, die wir dann erst später beantworten können. Zum Beispiel:

- Es gibt keine Divisionsalgebra, die die reellen Zahlen als Teilkörper enthält und über $\mathbb{R}$ die Vektorraumdimension 3 hat. Siehe Ergänzungen 4.9, 6.59 für die Erläuterung der Frage und 11.14 für die Lösung.

  Mit dieser Frage hat sich R. Hamilton um 1840 beschäftigt, es handelte sich damals um ein aktuelles Forschungsproblem, das ihn 1843 zur »(Er-)findung« der Quaternionen[6] führte. Diese spielen auch in der heutigen Mathematik (und Physik, und zum Beispiel auch in der Computergeometrie) eine Rolle. Es handelt sich dabei um einen Zahlbereich, der die reellen und die komplexen Zahlen enthält, aber auch noch zusätzliche Elemente. Es gelten dort die üblichen Rechenregeln bis auf das Kommutativgesetz der Multiplikation. Siehe Ergänzungen 4.11, 5.64, 8.7.

> ”
>
> Every morning, on my coming down to breakfast, you used to ask me: “Well, Papa, can you multiply triplets?” Whereto I was always obliged to reply, with a sad shake of the head: “No, I can only add and subtract them.”
>
> R. Hamilton in einem Brief an seinen Sohn[a] aus dem Jahr 1865, in dem er auch von seiner Erfindung der Quaternionen berichtet.

[a] https://www.maths.tcd.ie/pub/HistMath/People/Hamilton/Letters/BroomeBridge.html

[6] https://de.wikipedia.org/wiki/Quaternion

Als zwei weitere Beispiele für Gebiete, aus denen die Lineare Algebra nicht wegzudenken ist, seien hier genannt:

- die *Kodierungstheorie*, die sich damit befasst, wie man Informationen so über einen Kommunikationskanal (wie eine Funkverbindung oder ein »Internetkabel«) übertragen kann, dass sich Übertragungsfehler durch den Empfänger feststellen und bestenfalls automatisch korrigieren lassen. Dies ist eine sehr anwendungsnahe Theorie mit großen Überschneidungen mit der Informatik und den Ingenieurwissenschaften. Siehe Kapitel 13,
- die *Graphentheorie*, in der Konfigurationen von Punkten (»Knoten«), die durch Strecken (»Kanten«) miteinander verbunden sind, untersucht werden. Beispiele für *gerichtete* Graphen, in denen jede Kante mit einer Richtung versehen ist, sind die Darstellungen eines Netzwerks im Abschnitt über den Page-rank-Algorithmus (Frage 2.7). Es ist vielleicht ein bisschen überraschend, dass man Methoden der Linearen Algebra (wie zum Beispiel die Theorie der Eigenwerte, deren Anfänge wir zum Ende der Linearen Algebra 1 hin kennenlernen werden und die uns dann auch noch im kommenden Semester beschäftigen wird) auf das Studium von solchen Graphen anwenden kann, sie erweisen sich aber oft als sehr nützlich. Siehe Kapitel 14.
- Die lineare Algebra ist auch eng mit der *analytischen Geometrie* verwoben. Siehe Kapitel 12 für einige Bemerkungen dazu. In der Folgevorlesung Lineare Algebra 2 werden wir dieses Thema noch weiter vertiefen können.
- Der Begriff der *Symmetrie* spielt in vielen Bereichen der Mathematik eine Rolle und Symmetrien werden meist mithilfe des Begriffs der *Gruppe* beschrieben und untersucht, den wir in Kapitel 9 kennenlernen werden.

MathOverflow: Why Linear Algebra is fun! (or?)[a]

[a] https://mathoverflow.net/questions/33911/why-linear-algebra-is-funor

Weitere Beispiele finden Sie in den Büchern [**LM**], [**Ba**], in der Einleitung von [**Fi**] (und den dort gegebenen Literaturverweisen), [**Ma**] (Anwendungen von linearer Algebra auf mathematische Probleme), [**RS**]. Siehe auch Anhang C.

2.4. Alternativer Aufbau der Vorlesung *

Der Aufbau der Vorlesung, den ich gewählt habe, führt theoretische Begriffe erst dann ein, wenn sie benötigt werden und (hoffentlich) durch vorher aufgetretene Fragen motiviert werden können. Es wird trotzdem viele Definitionen geben, die nicht auf der Hand liegen und deren Nutzen nicht von vorneherein klar ist. Ich möchte aber versuchen, soweit es geht, den falschen Eindruck zu vermeiden, dass hier eine Theorie um ihrer selbst willen entwickelt wird, die losgelöst ist von den ursprünglichen Fragestellungen. Eines der Bücher, das einen ähnlichen Zugang wählt, ist das Buch [**Lo**] von Lorenz.

Alternativ kann man eine Darstellung wählen, die für diejenigen, die die Theorie schon kennen, möglichst systematisch ist. Damit kann man an (wenigen) Stellen etwas effizienter arbeiten, muss aber noch öfter Begriffe präsentieren, deren Nutzen sich erst wesentlich später herausstellt. Es gibt auch für diesen Aufbau gute Argumente, und er ist ebenfalls gebräuchlich; siehe zum Beispiel das Buch [**Bo**] von Bosch.

Dann würde man die Themen der Vorlesung zum Beispiel in der folgenden Reihenfolge abarbeiten: Gruppen, Körper, Vektorräume, Basen, Lineare Abbildungen, Matrizen und lineare Gleichungssysteme, Determinanten, Eigenwerte und Eigenvektoren.

(Und wenn man wollte, könnte man den Begriff der Matrix und die »Anwendung« auf die Lösung von linearen Gleichungssystemen vollständig vermeiden, was den Aufbau der Theorie angeht. Das würde dann aber, wie ich denke, doch ein falsches Bild vermitteln.)

2.5. Lineare Gleichungssysteme

Zum Schluss dieses einführenden Kapitels möchte ich wenigstens ein kleines bisschen lineare Algebra besprechen, nämlich die einfachsten Fälle linearer Gleichungssysteme. Dieses Material ist für Sie wahrscheinlich nicht neu (höchstens die systematische Form der Betrachtung). Es soll ein kleiner Ausblick auf das erste große Ziel der Vorlesung sein – die Lösung linearer Gleichungssysteme mit dem Gauß-Algorithmus (5.2). Auch wenn dann im späteren Verlauf die linearen Gleichungssysteme weniger sichtbar sind, bleibt der Gauß-Algorithmus ein wichtiges Mittel für die allermeisten Aufgaben, in denen etwas berechnet werden soll.

Eine *Gleichung* ist ein Ausdruck, in dem zwei Terme gleichgesetzt werden, in denen eine oder mehrere *Unbestimmte* (die wir unten X, Y, X_1, X_2, ... nennen) vorkommen, sowie Zahlen (»Koeffizienten«, unten mit kleinen Buchstaben bezeichnet) aus einem Zahlbereich K (zum Beispiel: die rationale Zahlen oder die reelle Zahlen). Ein *Gleichungssystem* besteht einfach aus mehreren Gleichungen.

Wir suchen die *Lösungsmenge* der Gleichung oder der Gleichungssystems, also alle Möglichkeiten, für alle Unbestimmten Elemente aus K so einzusetzen, dass alle Gleichungen erfüllt sind. Zum Beispiel ist für die Gleichung $x^2 = 2$ die Lösungsmenge die leere Menge, wenn wir die Gleichung über den rationalen Zahlen betrachten, und die Menge $\{\sqrt{2}, -\sqrt{2}\}$, wenn wir die Gleichung über den reellen Zahlen betrachten.

2.5.1. Lineares Gleichungssystem mit 1 Gleichung und 1 Unbestimmten. Wir beginnen ganz einfach und betrachten die Gleichung

$$aX = b$$

für Elemente $a, b \in K$. Die Lösungsmenge $\mathbb{L}$ ist dann eine Teilmenge von K, genauer die Teilmenge $\{x \in K; ax = b\}$.

Fall 1: $a \neq 0$. Dann ist die Lösungsmenge $\mathbb{L} = \{\frac{b}{a}\}$.

Fall 2: $a = 0, b \neq 0$. Dann ist die Lösungsmenge leer: $\mathbb{L} = \emptyset$.

Fall 3: $a = b = 0$. Dann ist jedes x eine Lösung, $\mathbb{L} = K$.

2.5.2. Lineares Gleichungssystem mit 1 Gleichung und n Unbestimmten. Nun betrachen wir eine Gleichung der Form

$$a_1X_1 + a_2X_2 + \cdots + a_nX_n = b,$$

in der mehrere Unbestimmt auftreten (aber keine höheren Potenzen der X_i – es handelt sich um eine *lineare* Gleichung). Die Lösungsmenge ist dann eine Menge von »n-Tupeln«, also Listen der Länge n, von Elementen in K. Wir bezeichnen die Menge aller n-Tupel $(x_1, ..., x_n)$, $x_i \in K$, mit K^n (vergleiche 3.9.1).

Fall 1: Es gibt ein i mit $a_i \neq 0$. Dann erhalten wir alle Lösungen der Gleichung folgendermaßen. Wir wählen beliebige Elemente $x_1, ..., x_{i-1}, x_{i+1}, ..., x_n \in K$ und definieren

$$x_i = \frac{1}{a_i}(b - a_1x_1 + \cdots a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \cdots + a_nx_n).$$

Wir schreiben die Lösungsmenge in der Form

$$\mathbb{L} = \left\{ \left(x_1, \dots, x_{i-1}, \frac{1}{a_i}(b - a_1x_1 + \cdots a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \cdots + a_nx_n), x_{i+1}, \dots, x_n \right); \right.$$
$$\left. x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n \in K \right\}.$$

Fall 2: Alle Koeffizienten a_i sind gleich 0.

Fall 2a: $b = 0$. In diesem Fall lösen alle $x_1, \dots, x_n \in K$ die Gleichung. Wir schreiben die Lösungsmenge als

$$\mathbb{L} = K^n = \{(x_1, \dots, x_n);\ x_1, \dots, x_n \in K\}.$$

Fall 2b: $b \neq 0$. In diesem Fall ist die Gleichung $0 = b$ nicht erfüllt, also ist die Lösungsmenge die leere Menge.

2.5.3. Lineares Gleichungssystem mit 2 Gleichungen und 2 Unbestimmten. Nun betrachten wir ein *System* von zwei Gleichungen und suchen alle Paare (x, y) von Elementen aus K, die beide Gleichungen

$$aX + bY = e$$
$$cX + dY = f$$

gleichzeitig erfüllen. Die Lösungsmenge ist dann eine Teilmenge von K^2, der Menge aller Paare (x, y) von Elementen in K.

Fall 1: $a \neq 0$. Wir ziehen das $\frac{c}{a}$-fache der ersten Gleichung von der zweiten Gleichung ab, multiplizieren danach die zweite Gleichung mit a und erhalten das lineare Gleichungssystem

$$aX + bY = e$$
$$(ad - bc)Y = af - ec.$$

(Machen Sie sich klar, dass sich die Lösungsmenge nicht ändert: Das neue System hat die *gleiche* Lösungsmenge, wie das ursprüngliche System. Vergleiche Lemma 5.12.)

Fall 1a: $a \neq 0, ad - bc \neq 0$. Wir können dann die zweite Gleichung durch $ad - bc$ teilen, dies in die erste Gleichung einsetzen, und die erste Gleichung durch a dividieren. Wir erhalten:

$$X = \frac{e}{a} - \frac{b}{a} \cdot \frac{af - ec}{ad - bc} = \frac{e(ad - bc) - b(af - ec)}{a(ad - bc)} = \frac{ed - bf}{ad - bc}$$
$$Y = \frac{af - ec}{ad - bc}.$$

Fall 1b: $a \neq 0, ad - bc = 0, af - ec = 0$. Dann bekommen wir

$$aX + bY = e$$
$$0 = 0,$$

d.h. die zweite Gleichung fällt weg. Für beliebiges y erhalten wir die Lösung $(\frac{e-by}{a}, y)$. (Vergleiche den Fall einer Gleichung mit 2 Unbestimmten.)

Fall 1c: $a \neq 0, ad - bc = 0, af - ec \neq 0$. Dann ist die zweite Gleichung niemals erfüllt, egal, was wir für X und Y einsetzen – die Lösungsmenge ist leer.

Fall 2: $a = 0, c \neq 0$. Diesen Fall können wir analog zu Fall 1 behandeln. Oder wir können ihn durch Vertauschen der beiden Gleichungen, also durch Umbenennen der Koeffizienten) auf Fall 1 zurückführen. Weil $ad - bc = -(cb - ad)$ gilt, sind die Bedingungen $ad - bc \neq 0$ und $cb - ad = 0$ äquivalent. Wir erhalten also wieder genau dasselbe Kriterium für die eindeutige Lösbarkeit des gegebenen linearen Gleichungssystems. Weil sich bei den Ausdrücken $ed - bf$ und $af - ec$ bei Vertauschen der beiden Zeilen auch gerade das Vorzeichen ändert, gilt in diesem Fall auch wieder die gleiche Formel für die eindeutige Lösung.

Fall 3: $a = c = 0$. In diesem Fall spielt die Wahl von X überhaupt keine Rolle. Die Lösungsmenge des linearen Gleichungssystems ist die Schnittmenge der Lösungsmengen von $bY = e$ und $dY = f$, die jeweils wie oben besprochen (1 Unbestimmte, 1 Gleichung) bestimmt werden können. Im Ergebnis kann die Lösungsmenge leer sein, oder Y ist eindeutig bestimmt (und X ist frei wählbar), oder Y (und X) sind beide frei wählbar.

Wir können unser Ergebnis in der folgenden Form zusammenfassen:

(1) Das lineare Gleichungssystem ist eindeutig lösbar genau dann, wenn $ad - bc \neq 0$. Dann ist
$$\mathbb{L} = \left\{ \left(\frac{ed - bf}{ad - bc}, \frac{af - ec}{ad - bc} \right) \right\}.$$
(2) Wenn $ad - bc = 0$, aber nicht alle Koeffizienten a, b, c, d verschwinden:
   (a) Gilt $af - ec = ed - bf = 0$, so gibt es so viele Lösungen wie die Anzahl der Elemente des Zahlbereichs K (also unendlich viele, wenn K unendlich viele Elemente hat).
   (b) Gilt $af - ec \neq 0$ oder $ed - bf \neq 0$, so gibt es keine Lösungen: die Lösungsmenge ist leer.
(3) Gilt $a = b = c = d = 0$, dann können die folgenden Fälle auftreten:
   (a) Ist $e = f = 0$, so sind alle Paare (x, y) Lösungen des linearen Gleichungssystems.
   (b) Ist $e \neq 0$ oder $f \neq 0$, so ist die Lösungsmenge leer.

Wir sehen auch: Wir wollen zwar auch größere Gleichungssysteme (mehr Unbestimmte, mehr Gleichungen) verstehen, aber nicht in dieser Art und Weise weitermachen. Die Fallunterscheidungen dafür würden viel zu unübersichtlich werden. Wir benötigen einen systematischeren Ansatz, der besser die zugrundeliegende Struktur des Problems ausnutzt und sichtbar macht.

KAPITEL 3

Grundlagen

3.1. Worum geht es eigentlich?

In der Mathematik möchten wir (mathematische) Strukturen verstehen und Erkenntnisse darüber als Aussagen formulieren, an deren Wahrheit kein Zweifel bestehen kann. Etwas konkreter sind die drei wesentlichen Bestandteile des Aufbaus der Mathematik

(1) Definition,

(2) Satz und

(3) Beweis.

In einer *Definition* werden zu verwendende Begriffe erklärt. Der *Satz* formuliert eine Aussage über die definierten Begriffe, und im *Beweis* wird eine vollständige und korrekte Argumentation angegeben, die belegt, dass die Aussage des Satzes wahr sein muss.

Das klingt einerseits ziemlich abstrakt, andererseits ist es nicht sehr präzise. Für den Moment ist mir das wichtigste, dass Sie mitnehmen, dass es uns vorrangig darum gehen wird, »strukturelle Aussagen« zu machen (und weniger darum, konkrete Rechnungen durchzuführen) und die Korrektheit dieser Aussagen zu beweisen. Etwas ausführlicher wird die Frage *Was ist ein Beweis?* im nächsten Abschnitt behandelt, den Sie aber auch erstmal überspringen können.

In der Praxis ist meist ziemlich klar, ob eine Argumentation einen Beweis darstellt oder nicht, und einen Beweis für eine mathematische Aussage zu *finden* ist ein ganz anderes Problem als die formale Frage, was ein Beweis eigentlich ist. Uns interessiert hier nicht so sehr die formale, sondern mehr die »praktische« Seite dieser Medaille (die ja immer noch abstrakt genug ist …).

Man muss kein Genie sein, um Beweise zu verstehen und selbst zu finden. Von selbst kann das aber auch so gut wie niemand. Das wichtigste ist die Übung: Beschäftigen Sie sich viel mit Mathematik, und nehmen Sie sich genügend Zeit, um über Aufgaben nachzudenken und sich mit anderen darüber zu unterhalten.

Siehe auch Anhang C.3.

3.2. Was ist ein Beweis? *

Das heute allgemein anerkannte Grundprinzip der Mathematik ist die sogenannte *axiomatische Methode*:

- ausgehend von einer (kleinen) Liste von Annahmen (»Axiomen«)
- unter Ausnutzung »offensichtlich« korrekter Schlussweisen
- wahre Aussagen zu beweisen.

Die Axiome setzen also sozusagen den Rahmen für die Theorie. Bei der Auswahl der Axiome muss man eine Balance finden, weil man genügend viele/starke Axiome benötigt, um damit

dann auch etwas beweisen zu können, aber andererseits nur solche Axiome verwenden möchte, die »offensichtlich wahr« sind, d.h., die sich in der Anschauung widerspiegeln, die man von der mathematischen Theorie hat, die man aufbauen möchte.

Je nachdem, worüber man mathematisch sprechen möchte, kann man unterschiedliche Axiomensystems benutzen. Drei der bekanntesten Systeme sind

(1) die Peano-Axiome[1], die die Eigenschaften der natürlichen Zahlen formalisieren,

(2) Euklids Axiome der Geometrie[2], die die geometrischen Eigenschaften der Ebene (und des dreidimensionalen Raums) formalisieren. Auch wenn Euklids Ausführungen nicht den heutigen formalen Ansprüchen genügen (eine modernere Variante ist Hilberts Axiomensystem[3]), wird das Prinzip der axiomatischen Methode bei Euklid sehr gut sichtbar.

(3) Die Zermelo-Fraenkelsche Mengenlehre[4] (kurz ZFC), die nach E. Zermelo und A. Fraenkel benannt ist, ist ein Axiomensystem für den Begriff der Menge. Damit lässt sich praktisch die gesamte heutige Mathematik beschreiben. Das C in ZFC steht für die Hinzunahme des *Auswahlaxioms* (englisch *axiom of choice*) zu den anderen Axiomen, siehe Anhang A.1.

ERGÄNZUNG 3.1 (Das Parallelenaxiom). Eines der Axiome der euklidischen Geometrie ist das sogenannte Parallelenaxiom, das besagt, dass zu jeder Gerade und jedem Punkt, der nicht auf dieser Gerade liegt, genau eine Gerade existiert, die durch den Punkt geht und zu der ersten Gerade parallel ist. Das ist sicherlich eine Eigenschaft, die unserer Anschauung entspricht.

Es war lange Zeit nicht bekannt, ob das Parallelenaxiom schon aus den anderen Axiomen folgt (so dass man es nicht als Axiom hätte hinzufügen müssen). Die Entwicklung der nichteuklidischen Geometrie[5] hat aber gezeigt, dass dies nicht der Fall ist: Das Parallelenaxiom ist unabhängig von den anderen Axiomen.

Eine Empfehlung für ein Buch (in Romanform mit mathematischen Einschüben) zu diesem Thema: G. Suri, H. S. Bal, *Eine gewisse Ungewissheit oder Der Zauber der Mathematik*, DuMont 2008. (oder das englische Original: *A certain ambiguity. A Mathematical Novel*, Princeton Univ. Press, 2nd ed., 2010). □ Ergänzung 3.1

Für den formal korrekten Aufbau der Theorie ist es sinnvoll, an dieser Stelle auch zu formalisieren, was man unter einem Beweis, also unter den oben angesprochenen »offensichtlich« korrekten Schlussweisen versteht. Der üblicherweise gewählt Ansatz ist die sogenannte Prädikatenlogik erster Stufe[6].

Literaturverweise (wenn Sie unbedingt mehr wissen müssen):

Ein bisschen mehr sagt Wolfram Pohlers (dessen Forschungsgebiet die mathematische Logik ist) in seinem Skript zur Linearen Algebra[a] (Kapitel 0).

Auch in dem (englischen) Buch [**Hu**] von Hungerford finden Sie etwas mehr Informationen zu diesem Thema.

[a] https://www.uni-muenster.de/imperia/md/content/logik/Skripte/pohlers.lineare_algebra.pdf

[1] https://de.wikipedia.org/wiki/Peano-Axiome
[2] https://de.wikipedia.org/wiki/Euklidische_Geometrie
[3] https://de.wikipedia.org/wiki/Hilberts_Axiomensystem_der_euklidischen_Geometrie
[4] https://de.wikipedia.org/wiki/Zermelo-Fraenkel-Mengenlehre
[5] https://de.wikipedia.org/wiki/Nichteuklidische_Geometrie
[6] https://de.wikipedia.org/wiki/Prädikatenlogik_erster_Stufe

In dieser Vorlesung werden wir aber darauf verzichten, das Axiomensystem auszuformulieren (das oben erwähnte ZFC ist eine Möglichkeit, die für die Vorlesungen Lineare Algebra 1+2 und die meisten (wahrscheinlich: alle) anderen Vorlesungen, die Sie in Ihrem Studium hören werden, ausreicht). Stattdessen werden wir mit einem »naiven« Mengenbegriff arbeiten. Sie müssen sich sozusagen darauf verlassen, dass alle Operationen, die wir mit Mengen ausführen, auch innerhalb von ZFC erlaubt sind (oder sich eigenständig die Mühe machen, das nachzuprüfen; es ist aber nicht unbedingt eine gute Idee, das zu Beginn des Studiums zu tun). Wir werden auch darauf verzichten, die erwähnte Prädikatenlogik ganz formal einzuführen, aber die nötigen Begriffe in Abschnitt 3.6 in der Form bereitstellen, wie wir sie verwenden werden. (Und fast alle anderen Lehrbücher machen es genauso.)

Auch wenn man sich an dieser Stelle mehr Zeit nehmen würde, wären die Beweise im Hauptteil des Textes genauso geschrieben, wie hier. Dieser Formalismus (hat zwar im Gesamtbild seine Berechtigung, aber) hilft nicht beim Verständnis der Linearen Algebra.

Außerdem: Irgendwo muss man anfangen – selbst bei maximaler Formalisierung muss man *auch* auf einer Meta-Ebene arbeiten, die man nicht in gleichem Maße formalisieren kann. Man kann eben vor der allerersten Definition nicht schon definiert haben, was man unter einer *Definition* versteht. Darüberhinaus gibt es auch tiefliegendere Einschränkungen an die vollständige Formalisierung der mathematischen Theorie (Stichwort: Gödelscher Unvollständigkeitssatz[7]). Diese Phänomene werden in der mathematischen Logik genauer untersucht. Dort analysiert man auch die »Beweiskraft« verschiedener formaler Systeme.

Das Grundprinzip, dass alle Aussagen auf die zu Beginn vorausgesetzten Axiome zurückgeführt werden können und dass jede Behauptung mit einer vollständigen und fehlerfreien Argumentation begründet werden muss, ist aber auch in diesem Text fundamental.

3.3. Beweise – einige Klassiker *

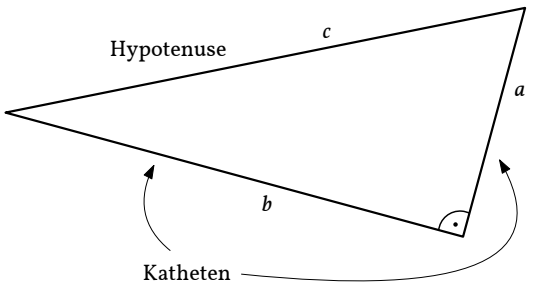
In diesem Abschnitt gehen wir einige "klassische" Beweise durch. Einige der Ergebnisse sind Ihnen sicher bekannt, vielleicht sogar die meisten.

Die Beweise sind alle einfach in dem Sinne, dass sie nur Schulmathematik benötigen. Das heißt aber nicht, dass man leicht darauf kommen kann. Trotzdem ist es eine gute Idee, über die Behauptungen, die unten aufgestellt werden, ein bisschen nachzudenken, bevor man den Beweis liest. Vielleicht finden Sie einen eigenen Beweis? Und wenn nicht, dann ist es oft leichter, einen Beweis zu verstehen (und zu würdigen), wenn man sich vorher schon einmal selbst daran versucht hat. Für Ihre Vorlesung(en) empfehle ich dasselbe!

3.3.1. Der Satz des Pythagoras. Sei Δ ein rechtwinkliges Dreieck. Wie üblich nennen wir die beiden Seiten von Δ, die an dem rechten Winkel anliegen, die *Katheten*, und die Seite, die dem rechten Winkel gegenüberliegt, die *Hypotenuse* des Dreiecks.

Satz 3.2 (Pythagoras). *Sei Δ ein rechtwinkliges Dreieck. Seien a und b die Längen der beiden Katheten, und sei c die Länge der Hypotenuse von Δ. Dann gilt*

$$a^2 + b^2 = c^2.$$

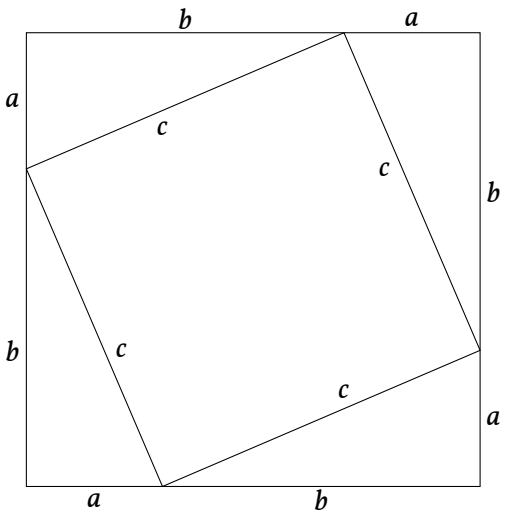


[7] https://de.wikipedia.org/wiki/Gödelscher_Unvollständigkeitssatz

BEMERKUNG 3.3. Auch wenn der Satz traditionell Pythagoras[8] (ca. 550 v. Chr.) zugeschrieben wird, war er mit ziemlicher Sicherheit schon vorher bekannt. ◊

BEWEIS. Es gibt viele Beweise für den Satz des Pythagoras. Der folgende ist wohl einer der einfachsten.

Wir betrachten die nebenstehende Figur, in der das gegebene rechtwinklige Dreieck mit Kathetenlängen a und b viermal vorkommt.



Wir können die Fläche des großen Quadrats auf zweierlei Arten berechnen: Die Seitenlänge des Quadrats ist $a+b$, also ist die Fläche

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Andererseits ist die Fläche die Summe der Teilflächen: viermal die Fläche des Dreiecks, also zweimal die Fläche des Rechtecks mit Kantenlängen a und b; und die Fläche des Quadrats in der Mitte, das Seitenlänge c hat. Damit ergibt sich für die Fläche

$$2ab + c^2.$$

Wir erhalten also

$$a^2 + 2ab + b^2 = 2ab + c^2,$$

und indem wir auf beiden Seiten $2ab$ abziehen, das gewünschte Ergebnis

$$a^2 + b^2 = c^2.$$

Eine Bemerkung zum Schluss: Prüfen Sie noch einmal genau, dass die geometrische Figur wirklich alle Eigenschaften hat, die wir im weiteren Beweis ausgenutzt haben. Ist der Bereich in der Mitte wirklich ein Quadrat, oder könnte es ein Viereck mit vier gleichlangen Seiten (eine *Raute*) sein, das aber kein Quadrat ist?

In [**Ho**] Kapitel 19 wird der Beweis noch ausführlicher aufgedröselt. □

3.3.2. $\sqrt{2}$ ist keine rationale Zahl. Mit $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ bezeichnen wir wie üblich die Menge der ganzen Zahlen und mit $\mathbb{Q}$ die Menge der rationalen Zahlen (also aller Bruchzahlen von ganzen Zahlen).

SATZ 3.4. *Die Menge $\mathbb{Q}$ der rationalen Zahlen enthält kein Element, dessen Quadrat gleich 2 ist.*

Zum Beweis benutzen wir das folgende Lemma. Wir nennen dabei wie üblich eine ganze Zahl $a \in \mathbb{Z}$ gerade, wenn sie durch 2 teilbar ist (also wenn $b \in \mathbb{Z}$ existiert mit $a = 2b$) und andernfalls ungerade.

LEMMA 3.5. (1) *Eine ganze Zahl $a \in \mathbb{Z}$ ist genau dann gerade, wenn ihr Quadrat a^2 gerade ist.*

(2) *Ist a eine ungerade ganze Zahl, so ist $2a$ nicht durch 4 teilbar.*

BEWEIS. Versuchen Sie, bevor Sie den Beweis lesen, erst einmal, einen eigenen Beweis zu finden und aufzuschreiben!

[8] https://de.wikipedia.org/wiki/Pythagoras

zu (1). Ist a gerade, etwa $a = 2b$, dann ist $a^2 = 4b^2$ ebenfalls ein Vielfaches von 2, also gerade. Wenn a ungerade ist, dann ist $a - 1$ gerade, also existiert eine ganze Zahl b mit $a = 2b + 1$.

$$a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$$

und dies ist eine ungerade Zahl, da sie sich um 1 von der geraden Zahl $2(2b^2 + 2b)$ unterscheidet.

zu (2). Da a nach Voraussetzung ungerade ist, können wir wie im vorherigen Teil $a = 2b + 1$ für eine geeignete ganze Zahl b schreiben. Dann ist $2a = 4b + 2$. Wäre diese Zahl durch 4 teilbar, so könnten wir auch $2a = 4c$ für eine ganze Zahl c schreiben, und würden dann erhalten, dass $4c = 4b + 2$, also $2 = 4(c - b)$. Dies ist offenbar nicht möglich. □

Beweis des Satzes. Angenommen, es gäbe eine Bruchzahl, deren Quadrat gleich 2 ist. Wir schreiben diese Zahl als gekürzten Bruch $\frac{a}{b}$, d.h. a und b sind ganze Zahlen, $b \neq 0$, und a und b haben keinen gemeinsamen Teiler > 1. Und es gilt $\left(\frac{a}{b}\right)^2 = 2$, also

$$a^2 = 2b^2.$$

Damit sehen wir zunächst, dass a^2 gerade ist, denn offenbar ist $2b^2$ gerade. Nach dem Lemma (Teil (1)) folgt, dass a eine gerade Zahl ist, wir können also $a = 2c$ für eine ganze Zahl c schreiben. Deshalb ist $a^2 = (2c)^2 = 4c^2$ sogar durch 4 teilbar.

Weil a gerade und der Bruch $\frac{a}{b}$ gekürzt ist, ist andererseits b ungerade. Teil (2) des Lemmas zeigt dann, dass $2b^2$ nicht durch 4 teilbar ist – ein Widerspruch zu der Gleichheit $a^2 = 2b^2$, denn wir haben gezeigt, dass die linke Seite durch 4 teilbar ist, die rechte jedoch nicht. □

Dieser Beweis wird meist, wie wir es auch getan haben, als »Widerspruchsbeweis« aufgeschrieben: Man macht eine Annahme (dass eben doch eine rationale Zahl mit Quadrat gleich 2 existiert) und leitet daraus durch gültige logische Schlüsse eine Aussage ab, die offensichtlich falsch ist. Der einzige Teil dieser Ableitung, der falsch sein könnte, ist die ursprüngliche Annahme. Man hat also bewiesen, dass die Annahme falsch ist. Oft lassen sich Widerspruchsbeweise auch ersetzen durch »direkte« Beweise. Versuchen Sie einmal direkt zu zeigen, dass für jede rationale Zahl x gilt, dass $x^2 \neq 2$.

Häufig wird dieser Satz formuliert als: $\sqrt{2}$ *ist nicht rational*. Um das zu tun, muss man aber erst einmal wissen, dass in einem größeren Zahlbereich – in diesem Fall in den reellen Zahlen $\mathbb{R}$ – eine (positive) Zahl mit Quadrat 2 existiert; diese bezeichnet man dann mit $\sqrt{2}$. Das ist, wie Sie wissen, richtig. Es zu beweisen, ist aber nicht so einfach, schon deshalb, weil man zuerst präzisieren muss, was genau man eigentlich unter den reellen Zahlen versteht. Diese Aufgabe überlassen wir der Analysis-Vorlesung.

Schließlich nutze ich noch die Gelegenheit, auf das Büchlein [**Go**] hinzuweisen, wo (in Kapitel 3) noch genauer hinterfragt wird, ob unser Beweis wirklich vollständig und schlüssig ist. Die anderen Teile des Buchs sind auch empfehlenswert!

3.3.3. Es gibt unendlich viele Primzahlen. Für den nächsten Satz brauchen wir den Begriff der Primzahl: Eine *Primzahl* ist eine ganze Zahl > 1, die keine Teiler außer 1 und sich selbst hat. Zum Beispiel sind $2, 3, 61$ Primzahlen, 57 jedoch nicht, da 57 durch 3 teilbar ist.

(Etwas ausführlicher befassen wir uns in Ergänzung 3.44 mit dem Begriff des Teilers.)

Satz 3.6. *Es gibt unendlich viele Primzahlen.*

Beweis (nach Euklid). Wir zeigen, dass zu jeder endlichen Liste $p_1, \ldots, p_n$ von Primzahlen noch mindestens eine weitere existiert.

Als Vorüberlegung zeigen wir, dass jede ganze Zahl $a > 1$ durch irgendeine Primzahl teilbar ist. In der Tat, ist a selbst eine Primzahl, so ist diese Behauptung richtig, dann a ist durch

sich selbst teilbar. Ist a keine Primzahl, so besitzt a einen Teiler b mit $1 < b < a$. Ist b eine Primzahl, so sind wir fertig, denn b ist ein Teiler von a. Sonst finden wir einen Teiler von b, der noch kleiner ist; und jeder Teiler von b ist auch ein Teiler von a. Dieser Prozess muss irgendwann enden, weil wir in jedem Schritt zu einer kleineren Zahl übergehen. (Siehe auch Beispiel 3.42.)

Nun definieren wir

$$a = p_1 p_2 \cdots p_n + 1,$$

d.h. wir bilden das Produkt aller gegebenen Primzahlen und addieren dann noch 1. Nach der Vorüberlegung ist a teilbar durch eine Primzahl p. Andererseits ist a nicht durch irgendeine der Primzahlen $p_1, \ldots, p_n$ teilbar, denn der Rest bei Division von a durch eine von diesen Zahlen ist 1.

Also ist p eine Primzahl, die von $p_1, p_2, \ldots, p_n$ verschieden ist. □

Probieren Sie das Verfahren im Satz einmal aus, indem Sie mit der Liste 2, 3 von Primzahlen starten und nach und nach eine weitere konstruieren. Sie sehen schon im ersten Schritt, dass nicht alle Primzahlen der Größe nach auftreten, und nach wenigen Schritten, dass die Zahl a, die im Beweis konstruiert wird, nicht unbedingt selbst eine Primzahl ist.

Die Tatsache, dass jede natürliche Zahl > 1 als Produkt von Primzahlen geschrieben werden kann, und dass diese Zerlegung eindeutig ist bis auf die Reihenfolge der Faktoren (*eindeutige Primfaktorzerlegung in* $\mathbb{Z}$) ist übrigens etwas schwieriger zu zeigen. Siehe Satz 3.56.

3.4. Falsche Beweise erkennen *

Fehler passieren immer wieder und es ist wichtig diese zu erkennen: Eigene Fehler (bevor Sie Ihre Lösungen zu den Übungsaufgaben abgeben) und Fehler von anderen – Studierenden, Dozent*innen, in Büchern, Skripten usw. Siehe auch Abschnitt 1.6 in Pinks Skript [**Pi**].

Gleichzeitig kann man aus seinen eigenen Fehlern besonders viel lernen. Das soll zwar kein Aufruf sein, absichtlich Fehler zu machen; aber zu viel Angst sollte man davor auch nicht haben. Und: Wenn Sie in den Hausaufgaben Fehler gemacht haben, sollten Sie sicherstellen, dass Sie genau verstehen, was falsch war und wie es richtig gewesen wäre. Fragen Sie gegebenenfalls bei Ihrer Übungsgruppenleiter*in nach, falls nötig auch mehrfach!

> He was not a very careful person as a mathematician. He made a lot of mistakes. But he made mistakes in a good direction. I tried to imitate him. But I've realized that it's very difficult to make good mistakes.
>
> G. Shimura über Y. Taniyama[a]

[a] `https://en.wikipedia.org/wiki/Yutaka_Taniyama`

Beispiel 3.7. Analysieren Sie den folgenden Beweis:

Behauptung: $1 \leq 0$

Beweis: Sei $a = 1$, $b = 0$. Dann

$1 \leq 0$

$a \leq b \quad | \cdot b$

$ab \leq b^2$

$0 \leq 0$ ✓

◊

> An expert is someone who knows some of the worst mistakes that can be made in his subject, and how to avoid them.
>
> W. Heisenberg, in: *Physics and Beyond*
>
> Gefunden auf http://math.furman.edu/~mwoodard/mqs/data.html

BEISPIEL 3.8. Analysieren Sie die folgende Rechnung.

Aufgabe. Bestimmen Sie die Lösungsmenge des folgenden Gleichungssystems:

$$x + y = 0$$
$$x - y = 3$$

Wie viele Elemente hat die Lösungsmenge?

Lösung. Wir ersetzen die zweite Gleichung durch das Produkt der beiden Gleichungen und wenden die dritte binomische Formel an:

$$x + y = 0$$
$$x^2 - y^2 = 0$$

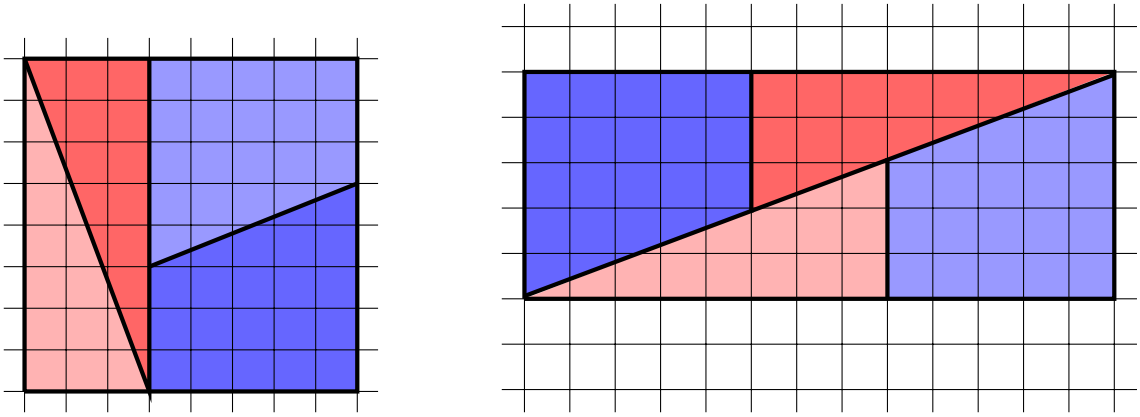
Die erste Gleichung können wir umschreiben als $x = -y$. Wenn das gilt, dann ist die zweite Gleichung automatisch erfüllt. Die Lösungsmenge ist also $\{(x, -x);\ x \in \mathbb{R}\}$. Sie hat unendlich viele Elemente. ◊

BEISPIEL 3.9. Es kommt nicht nur auf das Endergebnis an, sondern auch darauf, ein korrektes Argument verständlich darzulegen. Für die folgende Rechnung gibt es nicht die volle Punktzahl:

$\frac{16}{64} = \frac{1}{4}$ (mit 6 kürzen)

◊

Beispiel 3.10. Betrachten Sie die folgenden Figuren (Schachbrett-Paradoxon[9]):



Wir sehen:

$$64 = 8 \cdot 8 = \text{hellrot} + \text{dunkelrot} + \text{hellblau} + \text{dunkelblau} = 13 \cdot 5 = 65$$

Was geht hier schief? Können Sie sich ähnliche Beispiele ausdenken?

Übrigens: Es ist kein Zufall, dass die Zahlen 3, 5, 8, 13, die als Kantenlängen auftreten, ein Teil der Fibonacci-Folge (siehe Frage 2.1) sind. ◊

Beispiel 3.11. Dieses Beispiel benötigt die komplexen Zahlen, siehe 4.5. Analysieren Sie den folgenden Beweis, dass in den komplexen Zahlen $1 = -1$ gilt.

$$1 = \sqrt{1} = \sqrt{(-1)\cdot(-1)} = \sqrt{-1}\sqrt{-1} = (\sqrt{-1})^2 = -1.$$

◊

Ein subtiler falscher Beweis, dass jedes Dreieck gleichschenklig ist, wurde von Charles Dodgson erfunden (der unter dem Pseudonym Lewis Carroll die Geschichte von Alice im Wunderland geschrieben hat).
Wikipedia (Englisch)[a]

[a] https://en.wikipedia.org/wiki/Mathematical_fallacy#Fallacy_of_the_isosceles_triangle

Auch die »Profis« täuschen sich manchmal selbst und gehen fälschlich davon aus, ein Ergebnis bewiesen zu haben …
E. Burger, F. Morgan, Fermat's Last Theorem, the Four Color Theorem, and Bill Clinton for April Fools' Day[a], Amer. Math. Monthly **104** no. 3 (1997), 246–255.

[a] https://doi.org/10.1080/00029890.1997.11990629

[9] https://de.wikipedia.org/wiki/Schachbrett-Paradoxon

3.5. Offene Fragen *

Manchmal hört man, dass in der Mathematik ja wohl seit langem alles erforscht sei. Dabei ist das Gegenteil der Fall. In der Mathematik und auch in der linearen Algebra gibt es viele noch offene Fragen. Der Stoff der Vorlesungen über Lineare Algebra ist allerdings so grundlegend und so stark »optimiert«, dass uns in der Vorlesung solche offene Fragen kaum begegnen werden.

Besonders in der Zahlentheorie gibt es aber Vermutungen, die ganz leicht zu formulieren sind, die aber seit Jahrzehnten (oder teilweise seit Jahrhunderten) offen sind. Hier zwei Beispiele:

VERMUTUNG 3.12 (Goldbachsche Vermutung[10], 1742). *Jede gerade Zahl, die größer als 2 ist, lässt sich als die Summe von zwei Primzahlen schreiben.*

Es ist bekannt, dass die Vermutung für alle geraden Zahlen bis 4 000 000 000 000 000 000 richtig ist. Man weiß auch, dass jede ungerade Zahl sich als Summe von höchstens 3 Primzahlen schreiben lässt (dies ist die sogenannte *schwache Goldbachsche Vermutung*, die 2013 von Helfgott bewiesen wurde).

Um die nächste Vermutung zu formulieren, brauchen wir eine kleine Vorbereitung. Wir nennen natürliche Zahlen teilerfremd, wenn sie keinen gemeinsamen Teiler > 1 besitzen – zum Beispiel sind 12 und 55 teilerfremd, 15 und 55 jedoch nicht. Das *Radikal* einer natürlichen Zahl n ist das Produkt aller Primzahlen, die n teilen. (Der Unterschied zwischen der Zahl n und ihrem Radikal ist also, dass in n einige Primfaktoren mit einer höheren Potenz auftreten können.) Das Radikal von $1152 = 2^7 \cdot 3^2$ ist $2 \cdot 3 = 6$.

VERMUTUNG 3.13 (abc-Vermutung[11], Oesterlé, Masser, ca. 1985). *Sei $\varepsilon > 0$ eine positive reelle Zahl. Dann gibt es nur endlich viele teilerfremde natürliche Zahlen a, b und c, so dass $a + b = c$ und*

$$c > \mathrm{rad}(abc)^{1+\varepsilon}.$$

Zum Beispiel sind $a = 3, b = 125, c = 128$ teilerfremd und es gilt $a + b = c$. Die Primzahlen, die eine der drei Zahlen teilen, sind 2, 3 und 5, also gilt $\mathrm{rad}(abc) = 2 \cdot 3 \cdot 5 = 30$. Es gilt also $c > \mathrm{rad}(abc)$ (und es ist nicht so schwer zu sehen, dass die obige Aussage falsch würde, wenn man einfach ε durch 0 ersetzt). Man kennt aber kein einziges Beispiel für teilerfremde Zahlen a, b, c mit $a + b = c$ und $c > \mathrm{rad}(abc)^2$.

Die Millennium-Probleme[12] sind sieben Probleme, für deren Lösung das Clay Institute im Jahr 2000 ein Preisgeld von jeweils 1 Million Dollar ausgelobt hat. Von diesen Problemen konnte bisher nur die Poincaré-Vermutung bewiesen werden (G. Perelman, 2002; der Preis wurde ihm 2010 zugesprochen, aber Perelman hat den Preis abgelehnt).

3.6. Grundbegriffe, Notation

In diesem Abschnitt klären wir einige Grundbegriffe, die wir benutzen werden, um über Mathematik zu sprechen.

3.6.1. Aussagen. Eine *Aussage* formuliert Eigenschaften mathematischer Objekte und kann wahr oder falsch sein.

BEISPIEL 3.14. (1) Beispiele für Aussagen sind:

- Die Zahl 5 ist eine Primzahl.

[10] https://de.wikipedia.org/wiki/Goldbachsche_Vermutung
[11] https://de.wikipedia.org/wiki/Abc-Vermutung
[12] https://de.wikipedia.org/wiki/Millennium-Probleme

- Die Zahl 5 ist durch 3 teilbar.

(2) In den folgenden Sätzen kommen zwar auch mathematisch Symbole vor, es handelt sich aber nicht um Aussagen:

- Die Zahl 5 ist grün. (Denn *grün* hat keine mathematische Bedeutung.)
- Die Zahlen 5, 7 größer kleiner. (Kein sprachlich verständlicher Satz.)

◊

Wir können Aussagen miteinander verknüpfen: Seien $A, B, C, \ldots$ mathematische Aussagen.

(1) $A \wedge B$ (A und B) ist genau dann wahr, wenn A und B wahr sind.

(2) $A \vee B$ (A oder B) ist genau dann wahr, wenn A oder B wahr sind. (Es ist auch erlaubt, dass A und B beide wahr sind.)

(3) $\neg A$ (nicht A) ist genau dann wahr, wenn A falsch ist. Man nennt $\neg A$ auch die *Negation* der Aussage A.

(4) $A \Rightarrow B$ bedeutet, dass B aus A folgt, das heißt: wenn A wahr ist, dann ist B wahr. (Für den Fall, dass A falsch ist, wird keine Aussage über B gemacht; in diesem Fall ist die Aussage $A \Rightarrow B$ unabhängig von B wahr!)

Mit anderen Worten: $A \Rightarrow B$ ist genau dann wahr, wenn B wahr oder A falsch ist. (Wir können also das Symbol $\Rightarrow$ als Abkürzung sehen und könnten $A \Rightarrow B$ immer umschreiben als $B \vee \neg A$. Diese »formalistische« Sichtweise des Folgepfeils ist sicher etwas gewöhnungsbedürftig.)

(5) $A \Leftarrow B$ ist gleichbedeutend mit $B \Rightarrow A$.

(6) $A \Leftrightarrow B$ (genau dann A, wenn B) ist wahr wenn A beide wahr oder beide falsch sind.

Damit ist $A \Leftrightarrow B$ gleichbedeutend mit $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Von diesen Zeichen benutzen wir im weiteren Text eigentlich nur $\Rightarrow$ und $\Leftrightarrow$ häufiger, und selbst diese Symbole schreiben wir meist aus.

Um die Äquivalenz von zwei Arten, Aussagen zu verknüpfen, zu überprüfen – zum Beispiel die oben genannte Äquivalenz von $A \Rightarrow B$ und $B \vee \neg A$ – muss man prüfen, dass für alle möglichen Werte von A und B, also für alle Kombinationen von wahr/falsch, beide Verknüpfungen dasselbe Ergebnis liefern. Diese Werte kann man in einer Tabelle (»Wahrheitstafel«) auflisten. Die Zeilen entsprechen den Werten von A (also: in der ersten Zeile ist A in allen Fällen wahr; in der zweiten Zeile ist A in allen Fällen falsch), die Spalten den Werten von B (erste Spalte: B wahr, zweite Spalte: B falsch) und in den Einträgen geben wir das Ergebnis des betrachteten Ausdrucks an. Wir schreiben w für wahr, f für falsch.

A \ B	w	f
w	w	f
f	w	w

Wahrheitstafel für $A \Rightarrow B$.

A \ B	w	f
w	w	f
f	w	w

Wahrheitstafel für $B \vee \neg A$.

Diese Überprüfungen können also ohne weiteres Nachdenken durchgeführt werden (sind aber dafür ziemlich langweilig).

Mit derselben Methode kann man folgendes überprüfen: Wenn $A \Rightarrow B$ und $B \Rightarrow C$ gilt, dann gilt auch $A \Rightarrow C$.

Oft wird es vorkommen, dass wir für eine Liste von mehreren Aussagen zeigen wollen, dass je zwei dieser Aussagen äquivalent sind. Sind zum Beispiel Aussagen (i), (ii), (ii), (iv) gegeben,

deren Äquivalenz gezeigt werden soll, dann genügt es wegen der obigen Bemerkung, statt alle 12 Implikationen zu beweisen, die Implikationen $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$, $(iii) \Rightarrow (iv)$ und $(iv) \Rightarrow (i)$ zu zeigen. (Denn aus $(ii) \Rightarrow (iii)$ und $(iii) \Rightarrow (iv)$ folgt $(ii) \Rightarrow (iv)$, und mit $(iv) \Rightarrow (i)$ erhalten wir $(ii) \Rightarrow (i)$, also insgesamt $(i) \Leftrightarrow (ii)$, usw.) Man nennt diese Vorgehensweise manchmal einen *Ringschluss*.

3.6.2. Quantoren. Der *Allquantor* $\forall$ bedeutet, dass eine Aussage *für alle* Elemente einer Menge gelten soll. Nach dem $\forall$ wird angegeben, auf welche »Variable« er sich bezieht, nach einem Doppelpunkt kommt dann die eigentliche Aussage. Zum Beispiel:

$$\forall n \in \mathbb{Z} : n^2 \geq 0,$$

in Worten: Für jede ganze Zahl $n \in \mathbb{Z}$ ist $n^2 \geq 0$.

Der *Existenzquantor* $\exists$ drückt aus, dass (mindestens) ein Element existiert, so dass die Aussage wahr ist. Zum Beispiel:

$$\exists n \in \mathbb{Z} : (n > 5 \wedge n < 8),$$

in Worten: Es gibt eine ganze Zahl n, die größer als 5 und kleiner als 8 ist.

Es ist wichtig, die *Reihenfolge der Quantoren* zu beachten: Genauso wie $\forall m \in \mathbb{Z} \exists n \in \mathbb{Z} : m = n + 1$ richtig ist, ist $\exists n \in \mathbb{Z} \forall m \in \mathbb{Z} : m = n + 1$ offensichtlich falsch – machen Sie sich das klar.

3.6.3. Beweismethoden. Um Beweisen zu lernen (was wie gesagt ein wichtiges Ziel von Ihnen für diese Vorlesung sein sollte) muss man es an konkreten Aufgaben üben; dazu werden Sie ausgiebig Gelegenheit haben. In diesem Abschnitt soll es aber erst einmal nur darum gehen, einige Begrifflichkeiten zu erklären.

Unter einem *direkten Beweis* für eine zu zeigende Aussage B (die *Behauptung*) versteht kan eine Kette von Folgerungen $A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_n \rightarrow B$, für die bekannt ist, dass A_1 wahr ist. Damit folgt dann auch, dass B wahr ist. Wir haben zum Beispiel für den Satz des Pythagoras (Satz 3.2) einen direkten Beweis gegeben.

Ein *indirekter Beweis* oder *Widerspruchsbeweis*, *Beweis durch Widerspruch* einer Behauptung B besteht aus einer Kette von Folgerungen, die *ausgehend von der Negation von B* eine *falsche* Aussage ableitet. Wenn aber $\neg B \Rightarrow A$ für eine falsche Aussage A gilt, dann muss $\neg B$ falsch, also B wahr sein. Wir haben den Beweis, dass keine rationale Zahl existiert, deren Quadrat 2 ist, als indirekten Beweis geführt (Satz 3.4).

Um die Wahrheit einer Aussage der Form $A \Rightarrow B$ zu beweisen (ohne sich auf die Wahrheit von A und B festzulegen), kann man genausogut die *äquivalente* Aussage $\neg B \Rightarrow \neg A$ beweisen, die sogenannte *Kontraposition* der ursprünglichen Aussage.

Manchmal ist es für einen Beweis hilfreich, eine *Fallunterscheidung* vorzunehmen, also verschiedene Fälle getrennt zu behandeln. Das kann man machen, wenn man dabei alle Möglichkeiten abdeckt. Manchmal bietet es sich dann an, die Ergebnisse aus bereits abgeschlossenen Fällen in den weiteren Fällen zu benutzen.

Eine weitere wichtige Beweismethode (für Aussagen über natürliche Zahlen) ist die *vollständige Induktion*, der wir einen eigenen Abschnitt (Abschnitt 3.11) widmen werden.

3.6.4. Notationen. Manchmal benutzen wir das Symbol $:=$ um anzuzeigen, dass das Symbol auf der linken Seite (der Seite mit dem Doppelpunkt) neu definiert wird, und gleich dem Ausdruck auf der rechten Seite sein soll.

Für zwei (natürliche, rationale oder allgemein zwei reelle) Zahlen a, b bezeichnen wir mit $\min(a, b)$ die kleinere der beiden, das *Minimum*, und mit $\max(a, b)$ die größere, das *Maximum*. (Sind a und b gleich, so ist $\min(a, b) = \max(a, b) = a = b$.) Analog kann man diese Bezeichnungen für nicht-leere endliche Mengen von Zahlen verwenden. Für unendliche Mengen

Name	Groß	Klein		Name	Groß	Klein	
alpha	A	α		ny	N	ν	
beta	B	β		xi	Ξ	ξ	
gamma	Γ	γ		omikron	O	o	
delta	Δ	δ		pi	Π	π	
epsilon	E	ε		rho	P	ρ	(auch: ϱ)
zeta	Z	ζ		sigma	Σ	σ	(auch: ς)
eta	H	η		tau	T	τ	
theta	Θ	ϑ	(auch: θ)	ypsilon	Y	υ	
iota	I	ι		phi	Φ	φ	(auch: ϕ)
kappa	K	κ		chi	X	χ	
lambda	Λ	λ		psi	Ψ	ψ	
my	M	μ		omega	Ω	ω	

TABELLE 1. Die griechischen Buchstaben

müssen das Minimum und Maximum nicht unbedingt existieren; dann ist also besondere Vorsicht geboten.

3.6.5. Griechische Buchstaben. Gelegentlich benutzen wir *griechische Buchstaben*. Dass das in der Mathematik nicht unüblich ist, wissen Sie schon – denken Sie an die Kreiszahl π. In Ihrem Mathematikstudium wird Ihnen wahrscheinlich jeder griechische Buchstabe irgendwann einmal begegnen, insofern ist es gut investierte Zeit, sie gleich zu Beginn lesen und schreiben zu lernen (Tabelle 1).

3.7. Mengen

Heutzutage wählen die meisten Mathematiker als die formale Grundlage der Mathematik den Begriff der *Menge*. Kompliziertere Objekte drückt man dann in geeigneter Weise als/durch Mengen aus. Zum Beispiel kann man die natürlichen Zahlen als Mengen »kodieren«, indem man die natürliche Zahl n durch eine Menge mit n Elementen »ersetzt«. Unten werden wir sehen, wie man den Begriff der *Funktion* $X \to Y$ in Termen von Mengen ausdrückt.

Es bleibt allerdings zu sagen, was man überhaupt unter einer *Menge* versteht. Formal wäre der richtige Ansatz hier ein geeignetes Axiomensystem zugrundezulegen, das die essenziellen Eigenschaften von Mengen festschreibt und auf dessen Grundlage wir dann arbeiten könnten – zum Beispiel das Axiomensystem ZFC, benannt nach den Mathematikern Ernst Zermelo und Abraham Fraenkel. (Das C steht für das »Auswahlaxiom«, englisch: axiom of choice, siehe Anhang A.1.)

Wir wollen uns diese Arbeit aber hier ersparen und wählen stattdessen einen »naiven Zugang«.

Eine *Menge* ist eine Zusammenfassung mathematischer Objekte. Eine Menge M ist gegeben durch ihre Elemente: Für alle Objekte x gilt entweder $x \in M$ (d.h. x ist ein Element von M; wir sagen, x liege in M) oder $x \notin M$ (d.h. x ist kein Element von M). Zwei Mengen M, M' sind genau dann gleich, wenn sie dieselben Elemente haben, also wenn für alle x gilt:

$$x \in M \quad \text{genau dann, wenn} \quad x \in M'.$$

Literaturverweise: (Meine Empfehlung bleibt aber, sich diese für einen späteren Zeitpunkt aufzuheben.)
Ein bisschen mehr sagt Wolfram Pohlers (dessen Forschungsgebiet die mathematische Logik ist) in seinem Skript zur Linearen Algebra[a] (Kapitel 0).
Auch in dem (englischen) Buch [**Hu**] von Hungerford finden Sie etwas mehr Informationen zu diesem Thema.

[a] https://www.uni-muenster.de/imperia/md/content/logik/Skripte/pohlers.lineare_algebra.pdf

BEISPIEL 3.15. • Die *leere Menge* bezeichnen wir mit $\emptyset$ oder mit $\{\}$. Dies ist die einzige Menge, die kein Element enthält, d.h. für alle x gilt $x \notin \emptyset$. Achtung: »Doppelt gemoppelt« hält in diesem Fall nicht besser: $\{\emptyset\}$ ist *nicht* die leere Menge, sondern eine Menge mit einem Element: $\emptyset \in \{\emptyset\}$.

- Wir können Mengen angeben, indem wir alle ihre Elemente hinschreiben: $\{1, 2, 3, 4, 5\}$. Beachten Sie, dass
$$\{1, 2, 3, 4, 5\} = \{1, 4, 2, 5, 3\} = \{1, 1, 3, 5, 4, 4, 2\},$$
die Reihenfolge der Elemente spielt ebensowenig eine Rolle wie die Frage, ob Elemente mehrfach genannt sind.
- Für die meisten Mengen, die wir betrachten, ist es nicht möglich, alle Elemente direkt hinzuschreiben. Oft werden wir Mengen dadurch angeben, dass wir aus einer Grundmenge alle Elemente auswählen, die eine gewisse Eigenschaft haben. Ist zum Beispiel $\mathbb{N}$ die Menge der natürlichen Zahlen, dann ist
$$\{n \in \mathbb{N};\ \exists m \in \mathbb{N} : n = m^2\}$$
die Menge der Quadratzahlen. Statt des Semikolons findet man auch häufig die Notation mit einem senkrechten Strich |.
- Manchmal kann man alle Elemente einer Menge »aufzählen«, indem man beschreibt, wie sie durch eine Konstruktion aus anderen Elementen entstehen, zum Beispiel können wir die Menge aller Bruchzahlen schreiben als
$$\mathbb{Q} = \left\{ \frac{a}{b};\ a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

◊

BEISPIEL 3.16. Wichtige Beispiele von Mengen sind natürlich die üblichen Zahlbereiche:

- Die Menge der *natürlichen Zahlen* bezeichnen wir mit $\mathbb{N}$:
$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$
Die Frage, ob die Zahl 0 eine natürliche Zahl ist, und dementsprechend ob die mit dem Symbol $\mathbb{N}$ bezeichnete Menge die Zahl 0 enthält, wird in der Literatur nicht einheitlich gehandhabt. In diesem Text schließen wir die 0 mit ein. (Gegebenenfalls schreiben wir $\mathbb{N}_{>0}$ oder $\mathbb{Z}_{>0}$ für die Menge der natürlichen Zahlen ohne 0.)
- Mit $\mathbb{Z}$ bezeichnen wir die Menge der *ganzen Zahlen*:
$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$
Wir erhalten die Menge $\mathbb{Z}$ aus der Menge $\mathbb{N}$ der natürlichen Zahlen, indem wir zu jeder natürlichen Zahl $\neq 0$ ihr Negatives hinzufügen. Ganze Zahlen kann man addieren, subtrahieren und multiplizieren, und es gelten die »üblichen Rechenregeln«.

- Mit $\mathbb{Q}$ bezeichnen wir die Menge der *rationalen Zahlen*, mit anderen Worten die Menge der Bruchzahlen von zwei ganzen Zahlen:

$$\mathbb{Q} = \left\{ \frac{a}{b};\ a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

  Es gelten die üblichen Bruchrechenregeln: Zunächst einmal gilt $\frac{a}{c} = \frac{b}{d}$ genau dann, wenn $ad = bc$ (das beschreibt die Möglichkeit, einen Bruch zu kürzen bzw. zu erweitern). Die Addition und Multiplikation von Brüchen sind definiert als

$$\frac{a}{c} + \frac{b}{d} = \frac{ad + bc}{cd}, \quad \frac{a}{c} \cdot \frac{b}{d} = \frac{ab}{cd}.$$

  Wenn man mit konkreten Zahlen rechnet, sollten die Ergebnisse natürlich in gekürzter Form angegeben werden. Wir betrachten $\mathbb{Z}$ als Teilmenge (siehe Definition 3.18) von $\mathbb{Q}$ und schreiben a statt $\frac{a}{1}$, auch wenn wir a als Element von $\mathbb{Q}$ auffassen. Beachte, dass die Addition und Multiplikation auf $\mathbb{Z}$ und $\mathbb{Q}$ kompatibel sind.

- Die Menge der *reellen Zahlen* hat das Symbol $\mathbb{R}$. Auch wenn das der Rechenbereich ist, der Ihnen (vermutlich) aus der Schule am geläufigsten ist, ist er aus mathematischer Sicht deutlich komplizierter als der Bereich der rationalen Zahlen.

  Man kann jede reelle Zahl durch ihre Dezimalbruchentwicklung beschreiben (die unendlich viele Stellen hinter dem Komma haben kann), aber auch hier gibt es das Problem, dass die Darstellung nicht eindeutig ist (es ist $0,999\cdots = 1$), und es ist nicht ganz trivial, die Rechenoperationen für solche Zahlen »sauber« hinzuschreiben. Weitere Ausführungen zur Konstruktion (bzw. zur Charakterisierung) der reellen Zahlen überlassen wir der Analysis-Vorlesung.

$\Diamond$

ERGÄNZUNG 3.17 (Russells Paradoxon). Dass man die Definition einer Menge als Zusammenfassung mathematischer Objekte nicht ohne jegliche Vorsicht verwenden kann, zeigt das Paradoxon von Bertrand Russell[13]. Wenn wir für jede Menge M und jedes mathematische Objekt x entweder $x \in M$ oder $x \notin M$ haben, können wir auch fragen, ob $M \in M$ oder $M \notin M$ gilt. (Für die Mengen, die wir kennen, gilt sicher $M \notin M$, aber es könnte ja auch Mengen geben, die sich selbst als Element enthalten.)

> Einem wissenschaftlichen Schriftsteller kann kaum etwas Unerwünschteres begegnen, als daß ihm nach Vollendung einer Arbeit eine der Grundlagen seines Baues erschüttert wird. In diese Lage wurde ich durch einen Brief des Herrn Bertrand Russell versetzt, als der Druck dieses Bandes sich seinem Ende näherte.
>
> G. Frege im Nachwort des zweiten Bands seiner Grundgesetze der Arithmetik von 1903, in dem er ein Axiomensystem der Arithmetik aufzubauen versuchte, das auf dem naiven Mengenbegriff basierte

Sei nun X die Menge aller Mengen M, für die gilt $M \notin M$.

Wenn dann $X \in X$ wäre, so folgt $X \notin X$. Wäre $X \notin X$, so folgt $X \in X$. So oder so erhalten wir einen Widerspruch!

[13] https://de.wikipedia.org/wiki/Bertrand_Russell

Solche Paradoxien werden durch die Einführung eines geeigneten Axiomensystems wie ZFC vermieden, da sich die »Menge«, über die Russells Paradox spricht, innerhalb dieses Systems nicht konstruieren lässt.

Buchtipp (in Comicform): A. Doxiadis, C. Papadimitriou, *Logicomix: Eine epische Suche nach Wahrheit*, (der Vollständigkeit halber: …the reader should provide his/her grain of salt[14])

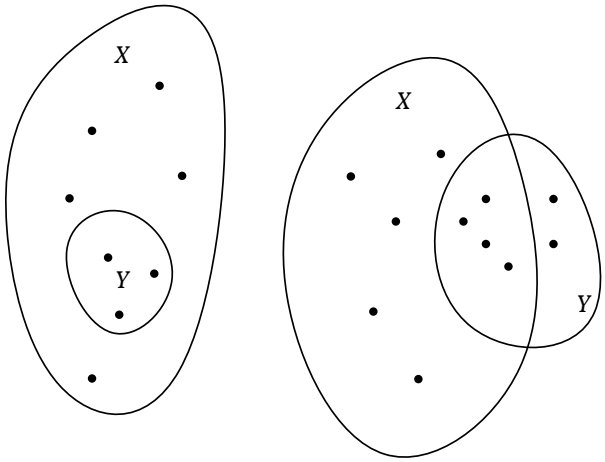
□ Ergänzung 3.17

3.8. Teilmengen, Konstruktionen von Mengen

DEFINITION 3.18. Sei X eine Menge. Wir sagen, eine Menge Y sei eine *Teilmenge* von X und schreiben $Y \subseteq X$, wenn für alle $y \in Y$ gilt: $y \in X$.

Statt des Begriffs *Teilmenge* verwendet man auch den Begriff *Untermenge*, oder sagt einfach, die Menge Y sei *in* X *enthalten* (Wenn die Elemente von X selbst Mengen sind, muss man unter Umständen etwas aufpassen: $Y \subseteq X$ und $Y \in X$ sind zwei sehr unterschiedliche Aussagen.) Wir schreiben $Y \subsetneq X$, wenn $Y \subseteq X$ und $Y \neq X$; in dieser Situation sagt man auch, Y sei eine *echte* Teilmenge von X. ⊣

Wie üblich wird das entsprechende Symbol mit einem Schrägstrich durchgestrichen, um die entsprechende Aussage zu verneinen (wie bei $=$ gleich, $\neq$ ungleich). Also bedeutet $Y \not\subseteq X$, dass Y keine Teilmenge von X ist.



$Y \subseteq X$ $\qquad$ $Y \not\subseteq X$

Statt $Y \subseteq X$ wird oft auch $Y \subset X$ geschrieben, d.h. auch das Symbol $\subset$ schließt in den meisten mathematischen Texten die Gleichheit $Y = X$ als eine Möglichkeit ein. (Die Situation ist also anders als beim Kleiner-/Größer-Zeichen.) In manchen Quellen wird das Zeichen $\subset$ allerdings auch im Sinne von $\subsetneq$ verwendet. Ich bemühe mich, das Symbol $\subset$ dann zu verwenden, wenn die Gleichheit zwar nicht formal ausgeschlossen ist, aber dieser Fall nicht relevant ist bzw. aus dem Kontext klar ist, dass er nicht auftreten kann.

Statt $Y \subseteq X$ kann man auch $X \supseteq Y$ schreiben, und man kann dies auch lesen als »X ist eine *Obermenge* von Y«. Entsprechendes gilt für $\supset$ und $\supsetneq$.

Wir können damit die Gleichheit zweier Mengen M, M' formulieren als

$$M = M' \quad \text{genau dann, wenn} \quad M \subseteq M', M' \subseteq M.$$

Oft zeigt man eine Gleichheit $M = M'$ von Mengen, indem man die beiden Inklusionen $M \subseteq M'$ und $M' \subseteq M$ beweist.

DEFINITION 3.19. Seien X und Y Teilmengen einer Menge M.

(1) Der *Durchschnitt* (oder die *Schnittmenge*) von X und Y ist

$$X \cap Y = \{m \in M;\ m \in X \text{ und } m \in Y\}.$$

[14] https://en.wikipedia.org/wiki/Logicomix#Historical_accuracy

(2) Die *Vereinigung* von X und Y ist

$$X \cup Y = \{m \in M;\ m \in X \text{ oder } m \in Y\}.$$

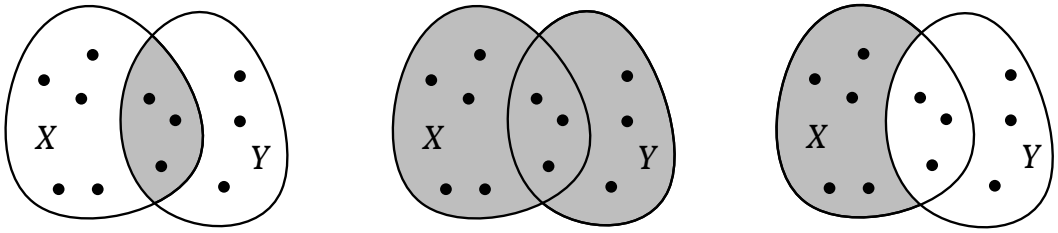
(3) Die *Differenz* von X und Y ist

$$X \setminus Y = \{m \in M;\ m \in X \text{ und } m \notin Y\}.$$

(4) Das *Komplement* von X in M ist

$$X^c = M \setminus X = \{m \in M;\ m \notin X\}.$$

⊣



$X \cap Y$ $X \cup Y$ $X \setminus Y$

Allgemeiner können wir Durchschnitte und Vereinigungen von mehr als zwei Mengen bilden:

DEFINITION 3.20. Seien M und I Mengen, und sei für jedes $i \in I$ eine Teilmenge $M_i \subseteq M$ gegeben.

(1) Der *Durchschnitt* der Teilmengen M_i ist

$$\bigcap_{i \in I} M_i = \{x \in M;\ x \in M_i \text{ für alle } i \in I\}.$$

(2) Die *Vereinigung* der Teilmengen M_i ist

$$\bigcup_{i \in I} M_i = \{x \in M;\ \text{es gibt ein } i \in I \text{ mit } x \in M_i\}.$$

⊣

Wir nennen zwei Teilmengen M_1, M_2 einer Menge M *disjunkt*, wenn $M_1 \cap M_2 = \emptyset$.

3.9. Kartesisches Produkt, Abbildungen

3.9.1. Produkte.

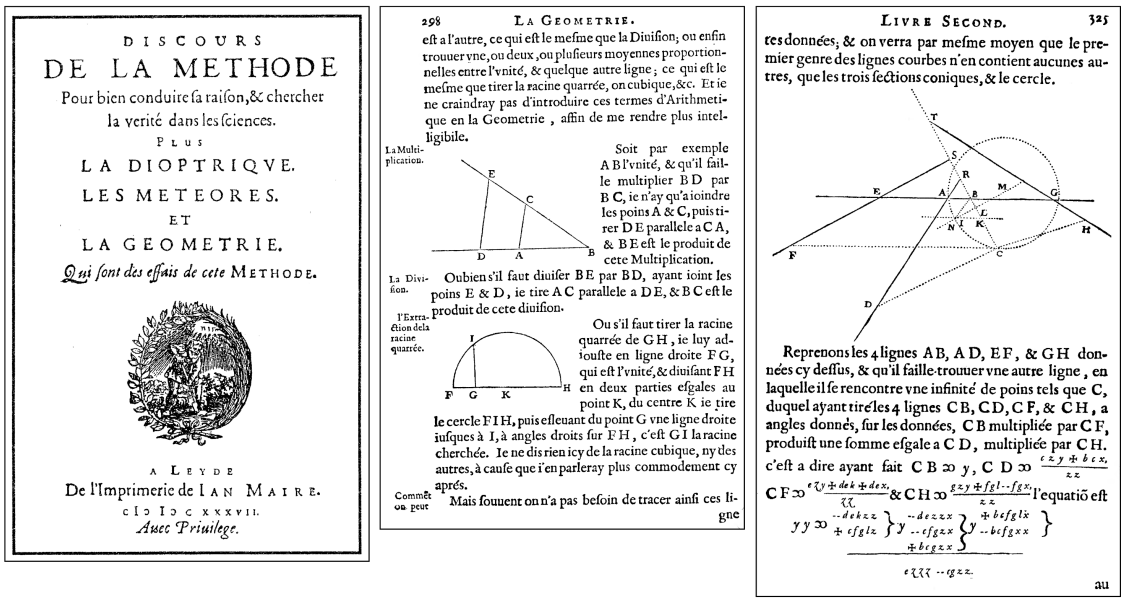
DEFINITION 3.21. (1) Sind X und Y Mengen, so bezeichnen wir mit $X \times Y$ die Menge aller Paare (x, y) mit $x \in X$ und $y \in Y$. Wir nennen $X \times Y$ das *(kartesische) Produkt* der Mengen X und Y.

(2) Analog können wir das Produkt von mehr als zwei Mengen bilden: Sind $X_1, X_2, \ldots, X_n$ Mengen, so ist

$$\prod_{i=1}^{n} X_i = X_1 \times \cdots \times X_n = \{(x_1, \ldots, x_n); \forall i = 1, \ldots n : x_i \in X_i\}$$

die Menge aller »Listen« $(x_1, \ldots, x_n)$ von Elementen der Mengen X_i. Die Elemente des Produkts nennen wir *n-Tupel*.

Im Fall, dass $X_1 = \cdots = X_n = X$ für eine Menge X ist, so schreiben wir X^n statt $X \times X \times \cdots \times X$ für das n-fache Produkt.



DISCOURS
DE LA METHODE
Pour bien conduire ſa raiſon,& chercher
la verité dans les ſciences.
PLUS
LA DIOPTRIQVE.
LES METEORES.
ET
LA GEOMETRIE.
Qui ſont des eſſais de cette METHODE.

A LEYDE
De l'Imprimerie de IAN MAIRE.
CIↃ IↃ C XXXVII.
Avec Priuilege.

298 LA GEOMETRIE.

eſt a l'autre, ce qui eſt le meſme que la Diuiſion; ou enfin trouuer vne, ou deux, ou pluſieurs moyennes proportionnelles entre l'vnité, & quelque autre ligne; ce qui eſt le meſme que tirer la racine quarrée, ou cubique, &c. Et ie ne craindray pas d'introduire ces termes d'Arithmetique en la Geometrie, affin de me rendre plus intelligibile.

La Multiplication.

Soit par exemple A B l'vnité, & qu'il faille multiplier B D par B C, ie n'ay qu'a ioindre les poins A & C, puis tirer D E parallele a C A, & B E eſt le produit de cete Multiplication.

La Diuiſion.

Ou bien s'il faut diuiſer B E par B D, ayant ioint les poins E & D, ie tire A C parallele a D E, & B C eſt le produit de cete diuiſion.

L'Extraction dela racine quarrée.

Ou s'il faut tirer la racine quarrée de G H, ie luy adiouſte en ligne droite F G, qui eſt l'vnité, & diuiſant F H en deux parties eſgales au point K, du centre K ie tire le cercle F I H, puis eſleuant du point G vne ligne droite iuſques à I, à angles droits ſur F H, c'eſt G I la racine cherchée. Ie ne dis rien icy de la racine cubique, ny des autres, à cauſe que i'en parleray plus commodement cy aprés.

Comme on peut

Mais ſouuent on n'a pas beſoin de tracer ainſi ces ligne

LIVRE SECOND. 325

tes données, & on verra par meſme moyen que le premier genre des lignes courbes n'en contient aucunes autres, que les trois ſections coniques, & le cercle.

Reprenons les 4 lignes A B, A D, E F, & G H données cy deſſus, & qu'il faille trouuer vne autre ligne, en laquelle il ſe rencontre vne infinité de poins tels que C, duquel ayant tiré les 4 lignes C B, C D, C F, & C H, a angles donnés, ſur les données, C B multipliée par C F, produiſt une ſomme eſgale a C D, multipliée par C H. c'eſt a dire ayant fait C B ∞ *y*, C D ∞ $\frac{czy+bcx}{zz}$ C F ∞ $\frac{ezy+dek+dex}{zz}$ & C H ∞ $\frac{gzy+fgl\cdots fgx}{zz}$ l'equatiõ eſt

$$yy \infty \frac{\cdots dekzz}{+efglz}\Big\}y \frac{\cdots dezzx}{\cdots efgzx}\Big\}y \frac{+befglx}{\cdots befgxx}\Big\}$$
$$+begzx$$
$$\overline{ezzz \cdots fgzz.}$$

au

Abbildung 1. Drei Seiten aus dem Buch über Geometrie von René Descartes (erschienen 1637). Descartes hat die Verwendung eines Koordinatensystems eingeführt, um die Lage von Punkten anzugeben. Koordinaten eines Punktes in der Ebene bilden ein Paar (x, y) von reellen Zahlen, also ein Element des Produkts $\mathbb{R} \times \mathbb{R}$. Deshalb nennt man das Produkt auch das *kartesische* Produkt. Quelle: Wikimedia[15]

(3) Noch allgemeiner ist für eine Menge I und Mengen X_i für alle $i \in I$ das Produkt

$$\prod_{i \in I} X_i = \{(x_i)_{i \in I};\ \forall i \in I : x_i \in X_i\}$$

definiert. Man nennt I die *Indexmenge* des Produkts.

Für den Spezialfall, dass $I = \emptyset$ die leere Menge ist (und daher gar kein X_i gegeben ist) hat sich die Konvention bewährt, dass das Produkt genau ein Element hat. Man spricht dann vom *leeren Produkt* (aber leer ist die Indexmenge, nicht die Produktmenge selbst).

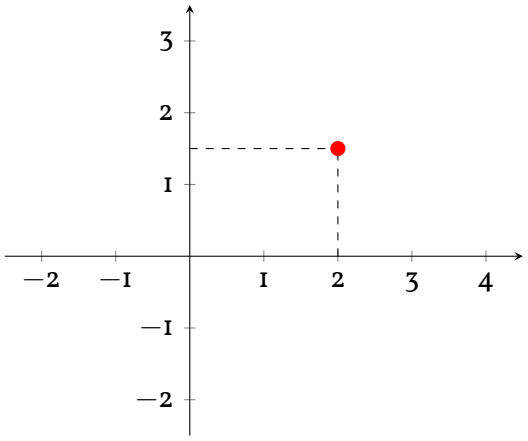
Ist $X_i = X$ für eine Menge X und alle i, so schreiben wir manchmal $X^I = \prod_{i \in I} X$.

⊣

Bei den Elementen des Produkts $X \times Y$ kommt es auf die Reihenfolge an, auch wenn $X = Y$ ist. Zum Beispiel hat $\{1, 2\} \times \{1, 2\}$ die vier verschiedenen Elemente $(1, 1)$, $(1, 2)$, $(2, 1)$, $(2, 2)$. Ein 3-Tupel nennt man meist *Tripel*, ein 4-Tupel manchmal *Quadrupel*, ein 5-Tupel manchmal *Quintupel*.

[15] https://commons.wikimedia.org/w/index.php?title=File%3ADescartes_La_G%C3%A9om%C3%A9trie.djvu

Wie Descartes veranschaulichen wir das Produkt $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ als die Ebene, in der wir die Lage eines Punkts durch seine beiden Koordinaten angeben können. Zum Beispiel hat der rot markierte Punkt in der Abbildung die Koordinaten $(2,\ 1,5)$. Die waagerechte Koordinatenachse, deren Koordinate als erste angegeben wird, heißt üblicherweise die x-Achse, die senkrechte Achse ist die y-Achse. Je nachdem kann man natürlich auch andere Namen verwenden; wird zum Beispiel ein zeitlicher Verlauf dargestellt, verwendet man oft den Parameter t (für lateinisch *tempus*) und stellt diesen auf der waagerechten Achse dar.



3.9.2. Abbildungen. Wir kommen nun zum Begriff der *Abbildung*; neben dem Begriff der Menge der grundlegendste Begriff aus diesem Kapitel.

DEFINITION 3.22. (1) Seien X, Y Mengen. Eine *Abbildung f von X nach Y*, geschrieben $f\colon X \to Y$, ist eine Zuordnung, die jedem Element $x \in X$ genau ein Element $f(x) \in Y$ zuordnet. Man schreibt $x \mapsto f(x)$ und nennt $f(x)$ das *Bild von x unter f* oder den *Wert* der Abbildung f bei x.

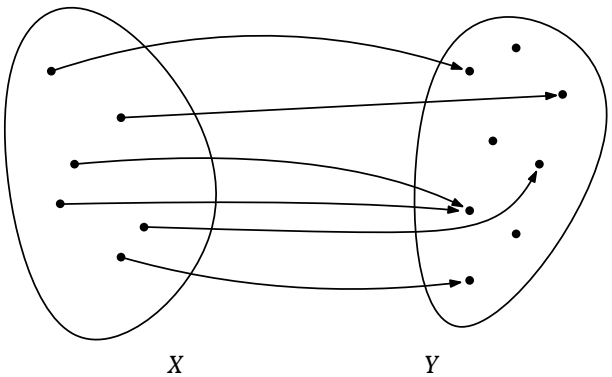
Formaler können wir den Begriff folgendermaßen definieren: Die *Zuordnung* ist gegeben als Teilmenge $F \subset X \times Y$ mit der Eigenschaft, dass zu jedem $x \in X$ genau ein $y \in Y$ existiert mit $(x,y) \in F$. Dieses Element y wird dann als $f(x)$ bezeichnet.

(2) Ist $f\colon X \to Y$ eine Abbildung, so nennen wir X den *Definitionsbereich* und Y den *Wertebereich* (oder manchmal das *Ziel*) der Abbildung f.

⊣

Eine *Funktion* ist nichts anderes als eine Abbildung (und der Funktionswert an einer Stelle ist dann der Wert an dem entsprechenden Element des Definitionsbereichs), allerdings wird der Begriff Funktion vor allem in spezielleren Situationen verwendet, beispielsweise spricht man in der Analysis oft von Funktionen $\mathbb{R} \to \mathbb{R}$. In der Linearen Algebra wird er kaum benutzt.

Auch wenn es von der Wortherkunft etwas miteinander zu tun hat, ist der hier definierte mathematische Begriff der Abbildung natürlich zu trennen vom Begriff einer Abbildung (im Sinne von Zeichnung, Foto, ...) der Alltagssprache.



Schematische Darstellung einer Abbildung. Die Elemente von X und Y sind durch Punkte dargestellt, die Zuordnung durch Pfeile. Die *Abbildungseigenschaft* besteht darin, dass *bei jedem Punkt in X genau ein Pfeil startet, und alle Pfeile in Y enden.*

BEISPIEL 3.23. (1) Beispiele für Funktionen sind

(i) $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2$,

(ii) $g\colon \mathbb{Z} \to \mathbb{Z}, x \mapsto 2x - 3$,

(iii) $g\colon \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$.

Die folgenden »Vorschriften« definieren keine Funktionen:

(i) $f\colon \mathbb{N} \to \mathbb{N}, x \mapsto 2x - 3$ (denn der Wert liegt nicht immer in dem angegebenen Wertebereich),

(ii) $g\colon \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} x & x \geq 0 \\ -x & x \leq 1 \end{cases}$
(denn für x zwischen 0 und 1 ist kein eindeutiger Funktionswert definiert),

(iii) $h\colon \mathbb{Q} \to \mathbb{Q}, x \mapsto \frac{1}{x}$
(denn für $x = 0$ ist kein Funktionswert definiert, weil $\frac{1}{0}$ keine rationale Zahl ist).

(2) Eine Abbildung muss nicht durch eine »Formel« gegeben sein. Zum Beispiel ist $f\colon \{0\} \to \{0, 1\}$ mit

$$f(0) = \begin{cases} 0 & \text{wenn die Goldbachsche Vermutung wahr ist,} \\ 1 & \text{wenn die Goldbachsche Vermutung falsch ist,} \end{cases}$$

eine Abbildung. Allerdings kennt niemand den Wert $f(0)$.

(3) Es gibt ziemlich »erstaunliche« Abbildungen. Zum Beispiel kann man zeigen, dass eine Abbildung $f\colon \mathbb{R} \to \mathbb{R}^2$ existiert, so dass jedes Element von $\mathbb{R}^2$ als Wert $f(x)$ auftritt.

(4) Zu einer Abbildung $X \to Y$ (oder Funktion) können wir den *Funktionsgraph* betrachten, das ist die Teilmenge

$$\{(x, f(x));\ x \in X\}$$

von $X \times Y$ (also gerade die Teilmenge F in Definition 3.22 (1); eine Funktion ist aus dieser Sichtweise dasselbe wie ihr Funktionsgraph). Da wir in der linearen Algebra meist Abbildungen zwischen »höherdimensionalen« Räumen betrachten, ist es meistens nicht möglich, den Funktionsgraph zu zeichnen; daher spielt er für uns eigentlich, anders als in der Analysis, keine Rolle.

◊

Statt vom Wertebereich einer Abbildung f spricht man manchmal auch vom *Bildbereich* von f. Diese Sprechweise ist aber weniger günstig, weil man unter dem *Bild* von f etwas anderes versteht (siehe Definition 3.25).

Die Menge aller Abbildungen von X nach Y bezeichnen wir mit $\mathrm{Abb}(X, Y)$.

Bemerkung 3.24. Überlegen Sie sich, dass wir für Mengen X und Y die Menge $\mathrm{Abb}(X, Y)$ mit dem Produkt $Y^X (= \prod_{x \in X} Y)$ identifizieren können. Wir können also eine Abbildung von X nach Y auch als ein Element des Produkts Y^X auffassen.

Hier zeigt sich, dass die Konvention, dass $Y^\emptyset$ genau ein Element haben soll, sinnvoll ist, denn die Menge $\mathrm{Abb}(\emptyset, Y)$ hat nach unserer Definition für jedes Y genau ein Element. ◊

Ist X eine Menge, so bezeichnen wir mit $\mathrm{id}_X\colon X \to X$ die Abbildung, die jedes $x \in X$ auf sich selbst abbildet: $x \mapsto x$ für alle $x \in X$. Diese Abbildung heißt die *identische Abbildung* oder *Identitätsabbildung* von X (oder manchmal einfach die *Identität* von/auf X).

Definition 3.25. Sei $f\colon X \to Y$ eine Abbildung.

(1) Das *Bild* von f ist
$$\mathrm{Im}(f) = \{y \in Y;\ \text{es existiert } x \in X \text{ mit } f(x) = y\}.$$
(2) Ist $Z \subseteq X$ eine Teilmenge, so nennt man
$$f(Z) = \{f(z);\ z \in Z\}$$
das *Bild von Z unter f*. Es gilt also $\mathrm{Im}(f) = f(X)$.
(3) Ist $Z \subseteq Y$ eine Teilmenge, so heißt
$$f^{-1}(Z) = \{x \in X;\ f(x) \in Z\}$$
das *Urbild von Z unter f*.

⊣

Für jede Abbildung $f\colon X \to Y$ gilt, dass $f^{-1}(Y) = X$, deshalb gibt es für das Urbild des gesamten Wertebereichs kein eigenes Symbol.

Wir nennen eine Abbildung f *konstant*, wenn alle Funktionswerte unter f gleich sind, mit anderen Worten, wenn $\mathrm{Im}(f)$ nur ein einziges Element enthält (oder, in dem Fall, dass der Definitionsbereich von f die leere Menge ist, leer ist).

Definition 3.26. Seien X, Y, Z Mengen und seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen. Wir definieren eine Abbildung $g \circ f\colon X \to Z$ durch
$$(g \circ f)(x) = g(f(x)).$$
(Diese Definition ist sinnvoll, da $f(x) \in Y$, so dass wir die Abbildung g auf dieses Element anwenden können.)

Die Abbildung $g \circ f$ heißt die *Verkettung*, *Verknüpfung* oder manchmal die *Komposition* der Abbildungen f und g. Das Symbol $g \circ f$ liest man auch als *g nach f*. ⊣

Achtung: Wenn man die Abbildungen f und g als Pfeile schreibt:
$$X \xrightarrow{f} Y \xrightarrow{g} Z$$
so steht f links und g rechts, aber die Verkettung der beiden Abbildungen ist $g \circ f$.

Ist $f\colon X \to Y$ eine Abbildung und $U \subseteq X$ eine Teilmenge, so bezeichnen wir mit $f_{|U}$ die Abbildung $U \to Y, x \mapsto f(x)$. Wir behalten also die Zuordnungsvorschrift unverändert bei und verkleinern lediglich den Definitionsbereich. Wir nennen $f_{|U}$ die *Einschränkung* der Abbildung f auf U.

Oftmals möchten wir Objekte »auflisten«, zum Beispiel, indem wir sie durchnummerieren (»Seien x_1, x_2, x_3 reelle Zahlen.«), je nach Situation kann es dabei um endlich viele oder unendlich viele Objekte gehen. Dabei möchten wir erlauben, dass Elemente mehrfach vorkommen (es wäre in dem gerade genannten Beispiel erlaubt, dass $x_1 = x_2$ ist), und ihre Reihenfolge festhalten. Daher ist der Mengenbegriff für diese Zwecke nicht ausreichend. Mithilfe des Abbildungsbegriffs können wir aber eine geeignete Definition machen:

Definition 3.27. Sei X eine Menge. Eine *Familie (oder: ein System) von Elementen aus X (mit Indexmenge I)* ist gegeben durch eine Menge I und für jedes Element $i \in I$ ein Element $x_i \in X$. Formal kann man eine solche Familie als Abbildung $I \to X, i \mapsto x_i$, oder als ein Element des Produkts X^I betrachten bzw. definieren. Wir schreiben eine durch I indizierte Familie oft in der Form $(x_i)_{i \in I}$. ⊣

Der häufigste Fall wird sein, dass $I = \{1, \ldots, n\}$ für eine natürliche Zahl n, oder dass $I = \mathbb{N}$ ist.

3.10. Injektive, surjektive und bijektive Abbildungen

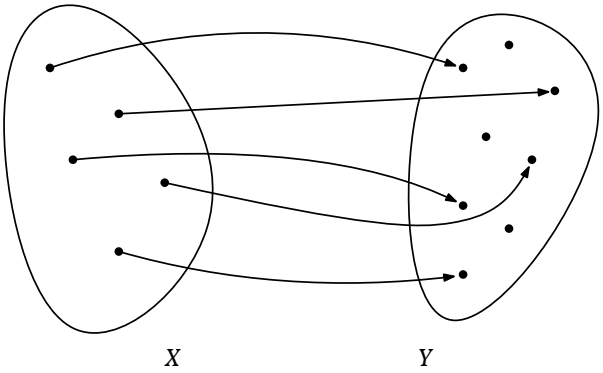
DEFINITION 3.28. Sei $f: X \to Y$ eine Abbildung.

(1) Die Abbildung f heißt *injektiv*, wenn für alle $x, x' \in X$ mit $x \neq x'$ gilt, dass $f(x) \neq f(x')$. Man nennt f in diesem Fall auch eine *Injektion*.

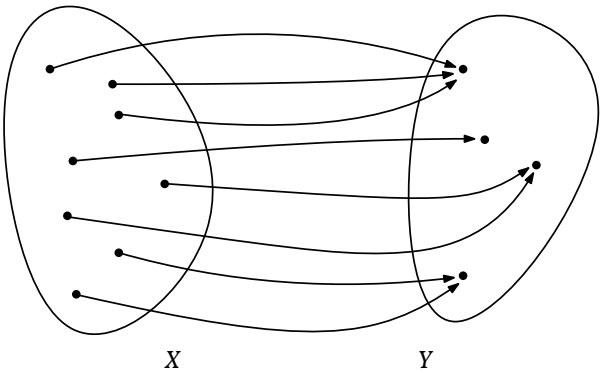
(2) Die Abbildung f heißt *surjektiv*, wenn für alle $y \in Y$ ein $x \in X$ existiert mit $f(x) = y$, mit anderen Worten: wenn $\mathrm{Im}(f) = Y$. Man nennt f in diesem Fall auch eine *Surjektion*.

(3) Die Abbildung f heißt *bijektiv*, wenn sie injektiv und surjektiv ist. Man nennt f in diesem Fall auch eine *Bijektion*.

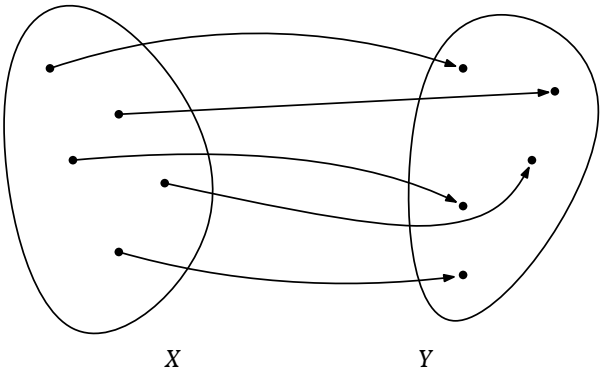
⊣



Injektiv: Jedes Element von Y wird von höchstens einem Pfeil erreicht. Mit anderen Worten: Zwei verschiedene Pfeile dürfen nicht denselben Endpunkt haben.



Surjektiv: Jedes Element von Y wird von mindestens einem Pfeil erreicht.



Bijektiv: Jedes Element von Y wird von genau einem Pfeil erreicht. (Indem man die Richtungen aller Pfeile umdreht, erhält man deswegen eine Abbildung von Y nach X, die *Umkehrabbildung* der ursprünglichen Abbildung, siehe Definition 3.30.)

Eine injektive Abbildung nennt man manchmal auch eine *Einbettung*. Ist $X \subseteq Y$ eine Teilmenge, so ist die *Inklusionsabbildung* (oder kurz: *Inklusion*) $X \to Y$, $x \mapsto x$, eine injektive Abbildung.

BEISPIEL 3.29. Betrachte die folgenden Abbildungen:

(i) $f: \mathbb{R} \to \mathbb{R}, x \mapsto x^2$,

(ii) $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^3$,

(iii) $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto x^2$,

(iv) $f\colon \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$,

(v) $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}, x \mapsto x^2$.

(1) Die folgenden Abbildungen sind injektiv: (ii), (iii), (v). Die anderen Abbildungen aus der Liste sind nicht injektiv.

(2) Die folgenden Abbildungen sind surjektiv: (ii), (iv). Die anderen Abbildungen aus der Liste sind nicht surjektiv.

◊

DEFINITION 3.30. Sei $f\colon X \to Y$ eine Abbildung. Eine Abbildung $g\colon Y \to X$ heißt *Umkehrabbildung* von f, wenn $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ gilt. ⊣

In der Situation ist dann also auch f eine Umkehrabbildung von g. Außerdem sind dann f und g automatisch bijektiv, wie der folgende Satz zeigt:

SATZ 3.31. *Sei $f\colon X \to Y$ eine Abbildung. Es existiert genau denn eine Umkehrabbildung g von f, wenn die Abbildung f bijektiv ist. In diesem Fall ist die Umkehrabbildung von f eindeutig bestimmt.*

BEWEIS. Wenn f eine Umkehrabbildung hat, dann ist f surjektiv (denn für $y \in Y$ gilt $f(g(y)) = y$) und injektiv (denn für $x, x' \in X$ mit $f(x) = f(x')$ gilt $x = g(f(x)) = g(f(x')) = x'$).

Sei nun f bijektiv. Gegeben $y \in Y$, so existiert $x \in X$ mit $f(x) = y$, weil f surjektiv ist. Zudem ist x eindeutig bestimmt, denn f ist injektiv. Wir setzen $g(y) := x$. Damit ist eine Abbildung $g\colon Y \to X$ definiert, und nach Konstruktion gilt $g(f(x)) = x$ für alle $x \in X$. Es ist noch zu zeigen, dass $f \circ g = \mathrm{id}_Y$ ist. Sei dazu $y \in Y$, und sei x das eindeutig bestimmt Element von X mit $f(x) = y$. Dann gilt $f(g(y)) = f(x) = y$.

Alternativ kann man die Umkehrfunktion g von f über ihren Funktionsgraphen angeben; dieser ist

$$\{(f(x), x); x \in X\} \subseteq Y \times X.$$

Wir begründen noch, dass die Umkehrabbildung von f eindeutig bestimmt ist. Wegen der Bedingung $g \circ f = \mathrm{id}_X$ ist g jedenfalls auf allen Elementen der Form $f(x)$ eindeutig bestimmt: Es muss $g(f(x)) = x$ gelten. Weil f surjektiv ist, hat aber jedes Element von Y diese Form. □

Wir bezeichnen die (eindeutig bestimmte) Umkehrabbildung einer bijektiven Abbildung $f\colon X \to Y$ oft mit f^{-1}. In diesem Fall ist für $y \in Y$ also $f^{-1}(y)$ ein Element von X. Man muss hier etwas aufpassen, da man die Bezeichnung $f^{-1}(y)$ (für nicht notwendig bijektive Abbildungen) auch manchmal als Abkürzung für $f^{-1}(\{y\})$ benutzt, und dies ist nach Definition die *Teilmenge*

$$\{x \in X; f(x) \in \{y\}\} = \{x \in X; f(x) = y\}$$

von X. (Ist f bijektiv, so hat diese Teilmenge aber nur ein einziges Element.)

Man zeigt leicht die folgenden Aussagen:

LEMMA 3.32. (1) *Die Verkettung von zwei injektiven Abbildungen ist eine injektive Abbildung.*

(2) *Die Verkettung von zwei surjektiven Abbildungen ist eine surjektive Abbildung.*

(3) *Die Verkettung von zwei bijektiven Abbildungen ist eine bijektive Abbildung.*

LEMMA 3.33. *Seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen. Dann gilt:*

(1) *Ist die Verkettung $g \circ f$ injektiv, dann ist f injektiv.*

(2) *Ist die Verkettung $g \circ f$ surjektiv, dann ist g surjektiv.*

3.11. Vollständige Induktion

3.11.1. Das Grundprinzip der Induktion. In diesem Abschnitt behandeln wir das Prinzip der *vollständigen Induktion*, einer wichtigen Methode, um zu beweisen, dass eine Aussage für alle natürlichen Zahlen gilt. Betrachten Sie als Beispiel die Aussage

$$P(n): \qquad n^3 - n \text{ ist teilbar durch } 3,$$

die für jede natürliche Zahl n sinnvoll ist. Man kann die Aussage in konkreten Fällen überprüfen – zum Beispiel ist $7^3 - 7 = 343 - 7 = 336$ tatsächlich durch 3 teilbar. Aber wie würde man so etwas für *alle* n beweisen?

Das Induktionsprinzip gibt uns eine Methode dafür an die Hand. Formal ausgedrückt wird das in dem folgenden Satz:

Satz 3.34 (Prinzip der vollständigen Induktion). *Sei $P(n)$ eine Eigenschaft, die die natürliche Zahl n haben oder nicht haben kann (oder: sei für jede natürliche Zahl n eine Aussage $P(n)$ gegeben), so dass die folgenden beiden Bedingungen erfüllt sind:*

(a) *$P(0)$ ist wahr, und*

(b) *für jede natürliche Zahl $n \geq 1$ gilt: Wenn $P(n-1)$ wahr ist, dann ist auch $P(n)$ wahr.*

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}$.

Oft wird die Aussage dieses Satzes als eines der Axiome eingesetzt, die für die natürlichen Zahlen angenommen werden. Jedenfalls ist klar, dass für seinen Beweis ein Axiom über die natürlichen Zahlen erforderlich ist, das darüber hinaus geht, dass jede natürliche Zahl $\neq 0$ einen eindeutig bestimmten Nachfolger hat. Wir wollen hier vom *Prinzip des kleinsten Elements* ausgehen, das vielleicht eingängiger ist als das Induktionsprinzip:

Axiom 3.35 (Prinzip des kleinsten Elements). *Jede nicht-leere Teilmenge von $\mathbb{N}$ besitzt ein kleinstes Element.*

Beweis von Satz 3.34. Sei $M = \{n \in \mathbb{N};\ P(n) \text{ ist falsch}\}$. Wir wollen zeigen, dass M die leere Menge ist, denn das bedeutet gerade, dass $P(n)$ für alle n wahr ist. Wenn M nicht leer ist, dann besitzt M nach dem Prinzip vom kleinsten Element ein kleinstes Element n. Weil nach Voraussetzung $P(0)$ wahr ist, kann nicht $n = 0$ sein. Dann ist aber $n - 1 \notin M$, weil n das *kleinste* Element von M ist. Also ist $P(n-1)$ wahr, aber $P(n)$ falsch. Das ist ein Widerspruch zu Teil (b) der Voraussetzung. □

Um mit dem Prinzip der vollständigen Induktion eine Aussage über natürliche Zahlen zu beweisen, muss man also die Eigenschaften (a) und (b) in Satz 3.34 nachweisen. Dabei nennt man Teil (a) den *Induktionsanfang* und Teil (b) den *Induktionsschritt*. In den meisten Beweisen hier im Skript und in der Literatur werden die Wörter Induktionsanfang und Induktionsschritt aber gar nicht mehr hingeschrieben, sondern es wird normalerweise nur darauf hingewiesen, dass ein Induktionsbeweis folgt und dann werden die Fälle $n = 0$ und $n > 0$ betrachtet.

Beispiel 3.36. *Behauptung.* Für alle natürlichen Zahlen n gilt, dass $n^3 - n$ durch 3 teilbar ist.

Beweis durch vollständige Induktion nach n.

Induktionsanfang $n = 0$: In diesem Fall gilt $n^3 - n = 0^3 - 0 = 0$, und $0 = 3 \cdot 0$ ist ein Vielfaches von 3, mit anderen Worten: Durch 3 teilbar.

Induktionsschritt $n > 0$. Wir dürfen nun als Induktionsvoraussetzung annehmen, dass für $n - 1$ die Aussage gilt, das bedeutet, dass $(n-1)^3 - (n-1)$ durch 3 teilbar ist. Wir müssen zeigen, dass $n^3 - n$ ebenso ein Vielfaches von 3 ist.

Wir rechnen[16]

$$(n-1)^3-(n-1)=(n^3-3n^2+3n-1)-(n-1)=n^3-3n^2+2n.$$

Um zu sehen, dass das hilfreich ist, schreiben wir den letzten Ausdruck noch ein bisschen um:

$$(n-1)^3-(n-1)=n^3-3n^2+2n=n^3-n+3(n-n^2).$$

Nun ziehen wir auf beiden Seiten $3(n-n^2)$ ab und erhalten

$$n^3-n=(n-1)^3-(n-1)+3(n-n^2).$$

Nach Induktionsvoraussetzung ist $(n-1)^3-(n-1)$ ein Vielfaches von 3. Offensichtlich ist $3(n-n^2)$ ein Vielfaches von 3. Deswegen ist auch die Summe, und das ist gerade n^3-n ein Vielfaches von 3. □

In diesem Fall ist es nicht allzu schwierig, statt des Induktionsbeweises einen direkten Beweis zu finden, der nur die Eigenschaften natürlicher Zahlen benutzt, die wir als bekannt voraussetzen. Haben Sie eine Idee?

Wie ist es, wenn wir den Exponenten durch eine andere Zahl als 3 ersetzen? Für $k \in \{2,5,7\}$ gilt: n^k-n ist ein Vielfaches von k. Können Sie das beweisen? Für $k=4$ ist diese Aussage nicht richtig. Finden Sie ein Gegenbeispiel? (Siehe Abschnitt 4.2.3.) ◊

Statt im Induktionsschritt zu beweisen, dass für $n>0$ die Aussage $P(n)$ aus $P(n-1)$ folgt, kann man natürlich genau so gut zeigen, dass für $n\geq 0$ die Aussage $P(n+1)$ aus $P(n)$ folgt. (Schreiben Sie den Beweis des vorherigen Beispiels in diesem Stil um. Es ist dann vielleicht besser, zuerst den Ausdruck $(n+1)^3-(n-1)$ umzuformen.)

Wir haben das Induktionsprinzip schon benutzt (ohne es wirklich auszusprechen) im Beweis des Satzes, dass es unendlich viele Primzahlen gibt (Satz 3.6, vergleiche Beispiel 3.42 unten).

3.11.2. Varianten des Induktionsprinzips. Es gibt einige Abwandlungen des Prinzips der vollständigen Induktion:

SATZ 3.37. *Sei $M\subseteq\mathbb{N}$ eine Teilmenge mit den Eigenschaften*

(a) $0\in M$, *und*

(b) *für alle natürlichen Zahlen $n\geq 1$ mit $n-1\in M$ gilt $n\in M$.*

Dann gilt $M=\mathbb{N}$.

BEWEIS. Definiere $P(n)$ als die Aussage $P(n) :\Leftrightarrow n\in M$. Dann gilt $P(0)$, und für alle $n\in\mathbb{N}$ folgt aus $P(n)$, dass $P(n+1)$ gilt. Nach dem Prinzip der vollständigen Induktion ist $P(n)$ für alle $n\in\mathbb{N}$ eine wahre Aussage. Das besagt genau, dass $M=\mathbb{N}$. □

BEMERKUNG 3.38. Statt des Axioms 3.35 könnte man auch einen der beiden Sätze als Axiom hernehmen, und dann die beiden anderen Aussagen daraus ableiten. ◊

Manchmal sind die folgenden Varianten des Induktionsprinzips nützlich:

SATZ 3.39 (»Induktionsanfang bei n_0«). *Sei $n_0\in\mathbb{N}$ eine natürliche Zahl. Sei für alle $n\geq n_0$ die Aussage $P(n)$ gegeben. Es gelte:*

(a) *$P(n_0)$ ist wahr, und*

(b) *für jede natürliche Zahl $n>n_0$ gilt: Wenn $P(n-1)$ wahr ist, dann ist auch $P(n)$ wahr.*

[16] Allgemein gilt $(a+b)^3=a^3+3a^2b+3ab^2+b^3$. Das benutzen wir im ersten Schritt.

Dann ist $P(n)$ wahr für alle natürlichen Zahlen $n \geq n_0$.

BEWEIS. Wir definieren die Aussage $P'(n)$ (für $n \in \mathbb{N}$) als $P(n + n_0)$. Aus dem üblichen Induktionsprinzip folgt dann, dass P' für alle $n \in \mathbb{N}$ wahr ist. Das bedeutet, dass $P(n)$ wahr ist für alle $n \geq n_0$. □

BEISPIEL 3.40. *Behauptung.* Für alle natürlichen Zahlen $n \geq 5$ gilt $2^n > n^2$.

Beweis per Induktion nach n. Induktionsanfang: $n = 5$. Es gilt

$$2^5 = 32 > 25 = 5^2.$$

Induktionsschritt: $n > 5$. Wir müssen zeigen, dass aus der »Induktionsvoraussetzung« $2^{n-1} > (n-1)^2$ folgt, dass $2^n > n^2$. Wir rechnen dazu:

$$2^n = 2 \cdot 2^{n-1} > 2(n-1)^2 = 2n^2 - 4n + 2 = n^2 + (n^2 - 4n + 4) - 2 = n^2 + (n-2)^2 - 2 > n^2 + 3^2 - 2 > n^2,$$

wobei wir die Induktionsvoraussetzung (für das erste $>$) und die Abschätzung $n > 5$ (für das zweite $>$) benutzt haben.

Man beachte, dass die Aussage $2^n > n^2$ für $n \leq 4$ falsch ist. ◊

SATZ 3.41 (»Induktionsvoraussetzung für $0, \ldots, n$«). *Sei $P(n)$ eine Eigenschaft, die die natürliche Zahl n haben oder nicht haben kann (oder: sei $P(n)$ eine Aussage über alle natürlichen Zahlen n) mit den folgenden beiden Eigenschaften:*

(a) *$P(0)$ ist wahr, und*

(b) *für jede natürliche Zahl $n > 1$ gilt: Wenn $P(0), P(1), \ldots, P(n-1)$ alle wahr sind, dann ist auch $P(n)$ wahr.*

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}$.

Machen Sie sich klar, dass die Voraussetzung (b) in diesem Satz schwächer ist als in Satz 3.34, weil man auf mehr Informationen zurückgreifen kann, um $P(n)$ zu zeigen. Der Satz ist also a priori stärker als Satz 3.34. (Man spricht manchmal von *starker* Induktion.) Das heißt: Es ist klar, dass die Aussage von Satz 3.34 aus Satz 3.41 folgen würde, aber wir müssen erst beweisen, dass es auch umgekehrt der Fall ist. Zum Glück ist das nicht schwierig.

BEWEIS. Wir definieren für $n \in \mathbb{N}$ die Aussage $P'(n)$ durch

$$P'(n) :\Longleftrightarrow \quad \forall m \in \{0, \ldots, n\} : P(m).$$

Dann erfüllt P' die Voraussetzungen des üblichen Induktionsprinzips (Satz 3.34) und daher gilt $P'(n)$ für alle n. Damit folgt auch $P(n)$ für alle n, wie gewünscht. □

Manchmal kombiniert man auch die beiden vorherigen Varianten:

BEISPIEL 3.42. *Behauptung.* Jede natürliche Zahl $n \geq 2$ wird von einer Primzahl geteilt. (Vergleiche den Beweis von Satz 3.6)

Begründung. Induktionsanfang: $n = 2$. In diesem Fall ist die Aussage richtig, da 2 eine Primzahl und ein Teiler von sich selbst ist.

Induktionsschritt: $n > 2$. Wir verwenden das Prinzip von Satz 3.41 und dürfen daher annehmen, dass die Aussage für alle natürlichen Zahlen m mit $2 \leq m < n$ richtig ist. Wenn nun n eine Primzahl ist, dann ist die Sache klar. Ansonsten besitzt n eine Zerlegung als Produkt $n = ab$ mit $a, b > 1$. Dann gilt, dass $2 \leq a < n$, also wird a nach Induktionsvoraussetzung von einer Primzahl geteilt. Als Teiler von a ist diese auch ein Teiler von n, und wir sind fertig. ◊

BEISPIEL 3.43. Auch einige Definitionen werden nach dem Induktionsprinzip vorgenommen, zum Beispiel definiert man (für Zahlen $a_0, \dots, a_n$ oder andere »Objekte«, für die eine Addition definiert ist) das Summensymbol $\sum_{i=0}^{n} a_i$, das die Summe der a_i bezeichnen soll. (Σ ist der griechische Großbuchstabe Sigma.) Anschaulich, aber informell möchte man definieren

$$\sum_{i=0}^{n} a_i = a_0 + a_1 + \cdots + a_n,$$

aber die Pünktchen auf der rechten Seite sind kein mathematisches Objekt (wir haben dieses Symbol jedenfalls nicht definiert). Als formale Definition für das Summensymbol setzen wir

$$\sum_{i=0}^{0} a_i = a_0, \qquad \sum_{i=0}^{n} a_i = \sum_{i=0}^{n-1} a_i + a_n \quad (n > 0).$$

Das Induktionsprinzip zeigt, dass dann $\sum_{i=0}^{n} a_i$ für alle natürlichen Zahlen n definiert ist. Analog definiert man $\sum_{i=m}^{n} a_i$, $\sum_{i=-m}^{n} a_i$, usw.

Wenn in dem (Zahl-)Bereich, dessen Addition benutzt wird, das Kommutativgesetz und Assoziativgesetz der Addition gelten (also $a + b = b + a$ und $(a + b) + c = a + (b + c)$ für alle a, b, c), so kommt es auf die Reihenfolge der Summanden nicht an und man kann für jede endliche Menge I und Familie $(a_i)_{i\in I}$ die Summe $\sum_{i\in I} a_i$ definieren. Ist $I = \emptyset$ so spricht man auch von der *leeren* Summe und definiert ihren Wert als 0. Das ist eine sinnvolle Konvention; zum Beispiel gilt dann für jede Indexmenge I, Familie $(a_i)_{i\in I}$ und Teilmenge $J \subseteq I$:

$$\sum_{i\in I} a_i = \sum_{i\in J} a_i + \sum_{i\in I\setminus J} a_i.$$

Analog zum Summenzeichen definiert man das Produktzeichen (Das Symbol Π ist das griechische große Pi.):

$$\prod_{i=0}^{0} a_i = a_0, \qquad \prod_{i=0}^{n} a_i = \left(\prod_{i=0}^{n-1} a_i\right) \cdot a_n \quad (n > 0).$$

Auch hier kann man natürlich weitere Varianten definieren. Das *leere Produkt* $\prod_{i\in\emptyset} a_i$ hat per Konvention den Wert 1. ◊

ERGÄNZUNG 3.44 (Teilbarkeit). Je nachdem, wie viel Lust/Interesse Sie daran haben, zu diesem Zeitpunkt auch »offensichtliche« Eigenschaften der ganzen Zahlen formal zu beweisen, können Sie diese ergänzende Bemerkung lesen oder überspringen.

DEFINITION 3.45. (1) Sei $n \in \mathbb{Z}$ eine ganze Zahl. Wir sagen, eine ganze Zahl $d \in \mathbb{Z}$ sei ein *Teiler* von n (oder d *teile* n), wenn eine ganze Zahl $k \in \mathbb{Z}$ existiert mit $n = dk$. Wir schreiben dann $d \mid n$, gesprochen »d teilt n«.

(2) Eine *Primzahl* ist eine ganze Zahl $p > 1$, deren einzige positive Teiler 1 und p selbst sind.

⊣

Wenn d kein Teiler von n ist, drücken wir das in Symbolen aus als $d \nmid n$. Zum Beispiel gilt für alle $n \in \mathbb{Z}$: $1 \mid n$, $-1 \mid n$, $n \mid n$, $n \mid 0$. Wenn $n \neq 0$ ist, dann gilt $0 \nmid n$.

Einige weitere Eigenschaften der Teilbarkeit sind in dem folgenden Satz gesammelt. Wir schreiben dabei $|a|$ für den *Absolutbetrag* (manchmal sagt man einfach *Betrag*) einer (reellen) Zahl a. Ist $a \geq 0$, so ist $|a| := a$, ist $a < 0$, so setzt man $|a| := -a$. In jedem Fall gilt also $|a| \geq 0$.

SATZ 3.46. *Seien a, b, c ganze Zahlen.*

(1) *Gilt $a \mid b$ und $b \neq 0$, so gilt $|a| \leq |b|$. Gilt $a \mid b$ und $a, b > 0$, so gilt $a \leq b$.*

(2) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*

(3) *Gilt $a \mid b$ und $b \mid a$, so ist $a = b$ oder $a = -b$.*

(4) *Gilt $a \mid b$ und $a \mid c$, so gilt $a \mid (b + c)$ und $a \mid (b - c)$.*

Beweis. Alle diese Aussagen sind leicht zu beweisen. Versuchen Sie es als erstes selbst einmal!

zu (1). Wenn $b = ka$ und $b \neq 0$, so folgt $|k|\,|a| = |ka| = |b|$ und damit $|a| \leq |b|$. Wenn sogar a und b beide positiv sind, dann muss auch k positiv sein, d.h. $k \geq 1$. Daraus folgt $b = ak \geq a$.

zu (2). Gilt $b = ka$ und $c = lb$, so folgt $c = (kl)a$, also $a \mid c$.

zu (3). Gilt $b = ka$ und $a = lb$, so folgt $a = (kl)a$, also $a(kl - 1) = 0$. Weil das Produkt $a(kl - 1)$ Null ist, muss einer der Faktoren Null sein. Ist $a = 0$, so folgt $b = ka = 0$, also $a = b$. Ist $kl = 1$, so muss $k = l = 1$ oder $k = l = -1$ sein, denn k und l sind ganze Zahlen. Daraus folgt die Behauptung.

zu (4). Gilt $b = ka$ und $c = la$, so folgt $b + c = (k + l)a$ und $b - c = (k - l)a$. Das zeigt die Behauptung. □

Satz 3.47 (Division mit Rest). *Seien x und n ganze Zahlen, $n > 0$. Dann existieren eindeutig bestimmte ganze Zahlen q und r mit*

$$x = qn + r, \qquad 0 \leq r < n.$$

Man sagt, die Division mit Rest von x durch n ergebe q, Rest r.

Beweis. Zuerst zeigen wir die Eindeutigkeit: Gilt $x = qn + r = q'n + r'$ mit $0 \leq r, r' < n$, so folgt $(q - q')n + (r - r') = x - x = 0$. Weil $|r - r'| < n$ ist, folgt $|q - q'| \cdot |n| = |r - r'| < n$ und daraus $q - q' = 0$, also $q = q'$ und damit auch $r = r'$.

Es bleibt noch die Existenz der Zahlen q und r zu zeigen. Wir betrachten zunächst den Fall $x \geq 0$ und führen Induktion nach x. Für $x = 0$ setzen wir $q = r = 0$.

Ist $x > 0$, so können wir per Induktionsvoraussetzung annehmen, dass wir $x - 1$ in der Form $q'n + r'$ schreiben können, mit $0 \leq r' < n$. Ist r' sogar kleiner als $n - 1$, so setzen wir $q = q'$, $r = r' + 1$. Dann gilt $n = (n - 1) + 1 = q'n + r' + 1 = qn + r$ und $0 \leq r < n$, wie gewünscht. Sonst ist $r' = n - 1$, und dann können wir $q = q' + 1$ und $r = 0$ setzen.

Ist $x < 0$, so können wir das schon Bewiesene auf $-x$ anwenden und erhalten $-x = q'n + r'$ für Zahlen q', r' mit $0 \leq r' < q$. Ist $r' = 0$, so folgt $x = -q'n$ und wir setzen $q = -q'$, $r = 0$. Ist $r' > 0$, so gilt $x = -q'n - r' = (-q' - 1)n + n - r'$ und wir können $q = -q' - 1$ und $r = n - r' < n$ setzen. □

Es gibt natürlich die Möglichkeit, den Satz auf den Fall $q < 0$ zu verallgemeinern (mit der Bedingung $0 \leq r < |q|$).

Definition 3.48. Seien a, b ganze Zahlen. Eine Zahl $d \in \mathbb{Z}$ heißt ein *gemeinsamer Teiler* von a und b wenn $d \mid a$ und $d \mid b$.

Das größte Element der Menge aller gemeinsamen Teiler von a und b heißt der *größte gemeinsame Teiler* von a und b, geschrieben $\mathrm{ggT}(a, b)$ (sofern nicht $a = b = 0$ gilt).

Sind $a = b = 0$, so ist jede ganze Zahl ein gemeinsamer Teiler von a und b, weswegen wir diesen Fall oben ausschließen. Wir definieren $\mathrm{ggT}(0, 0) = 0$. ⊣

Da für jeden Teiler d einer Zahl $a \neq 0$ gilt, dass $|d| \leq |a|$, haben a und b nur endlich viele gemeinsame Teiler, wenn nicht $a = b = 0$ gilt, und daher hat die Menge der gemeinsamen Teiler tatsächlich ein größtes Element.

BEISPIEL 3.49. Die gemeinsamen Teiler von 24 und 45 sind $-3, -1, 1, 3$, also $\mathrm{ggT}(24, 45) = 3$. ◊

Wir halten noch die folgenden Eigenschaften des größten gemeinsamen Teilers fest:

LEMMA 3.50. *Seien $a, b \in \mathbb{Z}$.*

(1) *Es gilt* $\mathrm{ggT}(a, b) = \mathrm{ggT}(-a, b) = \mathrm{ggT}(a, -b) = \mathrm{ggT}(-a, -b)$.
(2) *Es gilt* $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$.

BEWEIS. zu (1). Dies ist klar, da die Teiler von a mit den Teilern von $-a$ übereinstimmen (und ebenso für b).

zu (2). Wir zeigen, dass die Menge der gemeinsamen Teiler von a und b übereinstimmt mit der Menge der gemeinsamen Teiler von $a - b$ und b. Daraus folgt die Behauptung.

Ist d eine Zahl mit $d \mid a, d \mid b$, so folgt mit Lemma 3.46 (4), dass $d \mid a - b$. Also ist d ein gemeinsamer Teiler von $a - b$ und b.

Ist umgekehrt d eine ganze Zahl mit $d \mid a - b$ und $d \mid b$, so folgt mit demselben Lemma, dass $d \mid (a - b) + b = a$. □

Zum Berechnen des größten gemeinsamen Teilers verwendet man den Euklidischen Algorithmus[17]. □ Ergänzung 3.44

ERGÄNZUNG 3.51 (Die eindeutige Primfaktorzerlegung in $\mathbb{Z}$). In dieser Ergänzung beweisen wir den Satz über die eindeutige Primfaktorzerlegung in den ganzen Zahlen. Der entscheidende Punkt ist die folgende Eigenschaft von Primzahlen:

SATZ 3.52 (Primeigenschaft). *Sei p eine Primzahl. Seien a, b ganze Zahlen, so dass p ein Teiler des Produkts ab ist. Dann ist p ein Teiler von a oder von b (oder von beiden).*

Um den Satz zu beweisen, benutzen wir das folgende Lemma.

LEMMA 3.53. *Sind $a, b \in \mathbb{Z}$, so existieren $x, y \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(a, b) = xa + yb.$$

BEWEIS. Wegen Lemma 3.50 (1) können wir gegebenenfalls a und/oder b durch ihr Negatives ersetzen und daher annehmen, dass $a, b \geq 0$. Ist eine der Zahlen a, b gleich Null, so ist die Aussage von vorneherein klar. Wir können daher sogar voraussetzen, dass $a, b > 0$.

Wir führen nun Induktion nach der Zahl $\max(a, b)$, dem Maximum von a und b. Ist dieses $= 1$, so gilt $a = b = 1$ und $\mathrm{ggT}(a, b) = 1$, und wir nehmen $x = 1, y = 0$.

Sei nun $\max(a, b) > 1$. Ohne Einschränkung sei $a \geq b$ (sonst vertauschen wir einfach a und b.) Gilt $a = b$, so ist $\mathrm{ggT}(a, b) = a$ und wir können wieder $x = 1, y = 0$ setzen. Sonst gilt $a - b, b \geq 1$ und $\max(a - b, b) < \max(a, b)$. Dann erhalten wir

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b) = x'(a - b) + y'b = x'a + (y' - x')b$$

für geeignete ganze Zahlen x', y', wobei wir für die erste Gleichheit Lemma 3.50 und für die zweite die Induktionsvoraussetzung verwenden. Wir setzen also $x := x', y := y' - x'$ und erhalten das gewünschte Ergebnis. □

[17] https://de.wikipedia.org/wiki/Euklidischer_Algorithmus

BEWEIS VON SATZ 3.52. Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$ mit $p \mid ab$. Wenn p nicht a teilt, dann gilt $\mathrm{ggT}(p, a) = 1$ (denn die einzigen positive Teiler von p sind ja nach Definition einer Primzahl 1 und p).

Nach dem Lemma können wir also $x, y \in \mathbb{Z}$ finden mit

$$1 = xp + ya,$$

also

$$b = xpb + yab.$$

Nun werden xpb (offensichtlich) und yab (nach Voraussetzung) von p geteilt, also auch ihre Summe: $p \mid b$. □

BEMERKUNG 3.54. Es ist nicht schwer zu sehen, dass jede ganze Zahl $p > 1$ mit der Eigenschaft, dass $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$ eine Primzahl ist.

In der Tat, wenn p diese Eigenschaft hat und $p = ab$ gilt, dann gilt ja erst recht $p \mid ab$, also $p \mid a$ oder $p \mid b$, und wenn zum Beispiel $p \mid a$ gilt, so folgt $ab = p \leq |a|$, also $b = 1$ oder $b = -1$ und damit $a = p$ oder $a = -p$. ◊

KOROLLAR 3.55. *Sei p eine Primzahl, und seien $a_1, \ldots, a_n$ ganze Zahlen. Wenn p das Produkt $a_1 \cdot \cdots \cdot a_n$ teilt, dann teilt p (mindestens) einen der Faktoren a_i.*

BEWEIS. Dies folgt aus dem Satz über die Primeigenschaft und einer einfachen Induktion. □

SATZ 3.56. *Sei $a \neq 0$ eine ganze Zahl. Dann gibt es $n \geq 0$ und Primzahlen $p_1, \ldots, p_n \in \mathbb{Z}$, so dass*

$$a = \varepsilon \prod_{i=1}^{n} p_i,$$

wobei $\varepsilon = 1$, wenn $a > 0$, und $\varepsilon = -1$, wenn $a < 0$ ist. Dabei sind die Primzahlen p_i bis auf ihre Reihenfolge eindeutig bestimmt.

Für den Fall, dass $a = 1$ oder $a = -1$ ist, verstehen wir die Aussage so, dass a als Produkt von $\varepsilon = 1$ (bzw. $\varepsilon = -1$) und dem »leeren Produkt«, dessen Wert 1 ist, geschrieben wird. Man beachte, dass die p_i in der Aussage des Satzes in der Regel nicht paarweise verschieden sein werden. Insbesondere geht die Eindeutigkeitsaussage darüber hinaus zu behaupten, dass die Menge $\{p_1, \ldots, p_n\}$ der Primzahlen, die im Produkt überhaupt auftreten, eindeutig bestimmt sei; auch die Anzahl der Faktoren, die gleich einer gegebenen Primzahl sind, ist eindeutig bestimmt.

(Aus dem Satz 3.52 über die Primeigenschaft folgt, dass $\{p_1, \ldots, p_n\}$ genau die Menge der Primzahlen ist, die a teilen.)

BEWEIS. Es ist klar, dass es ausreicht, den Fall $a > 0$ zu behandeln, weil sich der andere Fall leicht daraus ableiten lässt.

Existenz der Zerlegung. Wir zeigen die Existenz durch vollständige Induktion nach a. Für $a = 1$ ist nach der obigen Bemerkung über die Interpretation der Aussage in diesem Fall nichts mehr zu zeigen. Sei nun also $a > 1$. Wir haben in Beispiel 3.42 gesehen, dass es eine Primzahl p gibt, die a teilt, etwa $a = pk$. Nach Induktionsvoraussetzung lässt sich k als ein Produkt von Primzahlen schreiben. Indem wir den Faktor p hinzufügen, erhalten wir eine entsprechende Darstellung von a.

Eindeutigkeit der Zerlegung. Wir wenden wiederum Induktion nach a an, wobei der Fall $a = 1$ klar ist. Betrachten wir eine Gleichheit der Form

$$p_1 \cdot \cdots \cdot p_m = a = q_1 \cdot \cdots \cdot q_n$$

für Primzahlen p_i, q_j. Wir müssen zeigen, dass $m = n$ und dass jede Primzahl auf der linken Seite genauso oft vorkommt, wie auf der rechten Seite.

Da $a > 1$ ist, muss $m \geq 1$ (und $n \geq 1$) gelten. Nun gilt $p_m | p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_n$, die Primzahl p_1 teilt also das Produkt $q_1 \cdot \dots \cdot q_n$. Wegen Korollar 3.55 gibt es ein $i \in \{1, \dots, n\}$ mit $p_m \mid q_i$. Weil p_m und q_i Primzahlen sind, muss $p_m = q_i$ gelten. Weil wir uns nur für die Eindeutigkeit der Faktoren *bis auf ihre Reihenfolge* interessieren, können wir die q's so umnummerieren, dass $i = n$ ist; das vereinfacht die Notation ein bisschen.

Es gilt dann also $p_m = q_n$ und daher auch

$$p_1 \cdot \dots \cdot p_{m-1} = q_1 \cdot \dots \cdot q_{n-1}.$$

Auf dieses Produkt können wir die Induktionsvoraussetzung anwenden, das heißt: $m - 1 = n - 1$, und die Familien $p_1, \dots, p_{m-1}$ und $q_1, \dots, q_{n-1}$ unterscheiden sich höchstens durch ihre Reihenfolge. Damit sind wir fertig. □

Vermutlich kennen Sie die Aussage dieses Satzes schon seit langem und halten sie für klar. Jedenfalls wird sie meistens in der Schule irgendwann angegeben. Oftmals wird aber nicht darauf hingewiesen, dass sie keineswegs selbstverständlich ist. Die Existenz einer solchen Zerlegung ist dabei noch recht eingängig, denn man kann ja, wie wir es auch im Beweis tun, jede Zahl immer weiter aufspalten, bis man es nur noch mit Primzahlen als Faktoren zu tun hat. Warum man aber eine Zahl wie 244 609 nur in der einen Weise $244\,609 = 331 \cdot 739$ (oder eben $= 739 \cdot 331$) als Produkt von Primzahlen geschrieben werden kann und es nicht noch andere Möglichkeiten geben könnte, ist nicht offensichtlich.

□ Ergänzung 3.51

3.12. Endliche Mengen

In diesem Abschnitt definieren wir, wann eine Menge *endlich* ist, und wie viele Elemente sie dann hat. Wenn Sie (nicht ganz zu unrecht) denken, dass das ohnehin klar ist, können Sie ihn auch erstmal überspringen, weil die Beweise ein bisschen »technisch« sind. (Und wenn Sie sich irgendwann fragen, wie der Begriff *endlich* formal definiert wird, darauf zurückkommen.)

Oder Sie betrachten diese technischen Beweise als Fingerübungen, um den Umgang mit Injektivität, Surjektivität und Bijektivität von Abbildungen und der Beweismethode der Induktion zu trainieren.

Für jede natürliche Zahl n betrachten wir die Menge $[n] := \{1, \dots, n\}$. (Wenn $n = 0$, dann soll das bedeuten, dass $[0] = \emptyset$ die leere Menge bezeichnet.) Das ist für uns der Prototyp für eine endliche Menge mit n Elementen.

Lemma 3.57. *Seien m, n endliche Zahlen.*

(1) *Wenn es eine injektive Abbildung $[m] \to [n]$ gibt, dann gilt $m \leq n$.*

(2) *Wenn es eine bijektive Abbildung $[m] \to [n]$ gibt, dann gilt $m = n$.*

Beweis. zu (1). Wir führen Induktion nach n. Ist $n = 0$, so ist $[n] = \emptyset$. Ist $M \to \emptyset$ irgendeine Abbildung, so muss auch $M = \emptyset$ gelten. Es folgt $[m] = \emptyset$ und damit $m = 0 = n$ (denn sonst wäre $1 \in [m]$).

Sei nun $n > 0$. Ist $m = 0$, so ist nichts zu zeigen, wir nehmen also auch an, dass $m > 0$. Sei $f\colon [m] \to [n]$ eine injektive Abbildung. Gilt $f([m-1]) \subseteq [n-1]$, so folgt $m - 1 \leq n - 1$ nach Induktionsvoraussetzung, also $m \leq n$. Sonst ist $n \in f([m-1])$ und wegen der Injektivität gibt

es eine eindeutig bestimmte Zahl i mit $1 \leq i < m$ und $f(i) = n$. Andererseits muss (wieder wegen der Injektivität) $f(m) \neq n$ gelten, also $f(m) \in [n-1]$. Wir definieren die Abbildung $g\colon [m-1] \to [n-1]$ wie folgt: $g(i) = f(m)$, $g(j) = f(j)$ für $j \in [m-1] \setminus \{i\}$. Dann ist g eine Injektion $[m-1] \to [n-1]$ und nach Induktionsvoraussetzung folgt $m-1 \leq n-1$, also $m \leq n$.

zu (2). Dies folgt direkt aus Teil (1): Ist f eine Bijektion zwischen $[m]$ und $[n]$, so ist f injektiv, also $m \leq n$ nach Teil (1), und die Umkehrabbildung von f ist eine Injektion $[n] \to [m]$, also gilt auch $n \leq m$. □

Definition 3.58. Eine Menge M heißt *endlich*, wenn eine natürliche Zahl $n \geq 0$ und eine Bijektion $[n] \to M$ existiert. Wir sagen dann, M habe n Elemente und schreiben $\#M = n$. (Oft schreibt man auch $|M|$ statt $\#M$. Diese Zahl heißt auch die *Mächtigkeit* oder *Kardinalität* von M.) ⊣

Statt einer Bijektion $[n] \to M$ könnte man natürlich ebenso gut eine Bijektion $M \to [n]$ betrachten. Durch Übergang zur Umkehrabbildung kann man ja zwischen diesen beiden Standpunkten hin und her gehen.

Wegen des Lemmas kann es für gegebenes M höchstens für eine einzige Zahl n eine Bijektion wie in der Definition geben. Die Zahl n ist also durch M eindeutig bestimmt, so dass die Definition der Mächtigkeit überhaupt sinnvoll ist. Wir sagen, der Begriff der Mächtigkeit sei *wohldefiniert* (siehe Abschnitte 3.13.2, B.1.1).

Ist M eine Menge und M nicht endlich, dann sagen wir, M sei unendlich (und schreiben manchmal $\#M = \infty$). Wichtig ist aber zu beachten, dass es zwischen zwei unendlichen Mengen nicht unbedingt eine Bijektion gibt. Zum Beispiel gibt es keine Bijektion zwischen $\mathbb{Q}$ und $\mathbb{R}$. Siehe Abschnitt 3.14.

Der Mächtigkeitsbegriff hat die Eigenschaften, die man erwartet; allerdings müssen diese, formal betrachtet, natürlich erst einmal bewiesen werden, bevor man sie dann benutzen kann. Zum Beispiel:

Lemma 3.59. *Sei X eine Menge und $x \in X$ ein Element. Dann gilt*

$$\#X = \#(X \setminus \{x\}) + 1.$$

Beweis. Sei etwa n die Mächtigkeit von $X \setminus \{x\}$, es gibt also eine Bijektion $f\colon [n] \to X \setminus \{x\}$. Wir definieren die Abbildung $g\colon [n+1] \to X$ durch $g(i) = f(i)$ für alle $i = 1, \ldots, n$, und setzen $g(n+1) = x$. Dann ist g ebenfalls bijektiv, also $\#X = n + 1 = \#(X \setminus \{x\}) + 1$. □

Den Beweis des folgenden, ähnlichen Lemmas lassen wir als Übungsaufgabe.

Lemma 3.60. *Seien $X, Y \subseteq M$ endliche Teilmengen einer Menge M. Wenn $X \cap Y = \emptyset$, dann gilt $\#(X \cup Y) = \#X + \#Y$.*

Eine andere Aussage, die Sie nicht überraschen wird, aber die eben auch eines Beweises bedarf:

Lemma 3.61. *Seien n eine natürliche Zahl, und $X_1, \ldots, X_n$ nicht-leere Mengen. Dann ist das Produkt $\prod_{i=1}^{n} X_i$ nicht leer.*

Beweis. Für $n = 1$ ist nichts zu zeigen, denn $\prod_{i=1}^{i} X_i = X_1$ ist nach Voraussetzung nicht leer. (Und für $n = 0$ ist die Aussage auch richtig angesichts unserer Konvention, dass das Produkt mit leerer Indexmenge genau ein Element hat.)

Ist $n > 1$, so haben wir nach Definition

$$\left(\prod_{i=1}^{n-1} X_i\right) \times X_n.$$

Nach Induktionsvoraussetzung ist $\left(\prod_{i=1}^{n-1} X_i\right)$ nicht leer; sei x ein Element dieser Menge. Nach Voraussetzung ist X_n nicht leer. Sei $x' \in X_n$. Dann ist $(x, x') \in \left(\prod_{i=1}^{n-1} X_i\right) \times X_n$, also ist auch diese Menge nicht leer. □

KOROLLAR 3.62. *Sei $f\colon X \to Y$ eine surjektive Abbildung von einer Menge X in eine endliche Menge Y. Dann existiert eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$.*

BEWEIS. Nach Lemma 3.61 ist $\prod_{y\in Y} f^{-1}(\{y\}) \neq \emptyset$. Ein Element dieses Produkt gibt uns für jedes $y \in Y$ ein Element in X mit $f(x) = y$. Wir definieren $g(y) := x$.

(Wenn wir $\prod_{y\in Y} f^{-1}(\{y\}) \neq \emptyset$ als Teilmenge von $\prod_{y\in Y} X = \mathrm{Abb}(Y, X)$ betrachten, dann *ist* jedes Element dieser Teilmenge eine Abbildung $Y \to X$ mit der gewünschten Eigenschaft.) □

So einleuchtend die Aussagen von Lemma 3.61 und Korollar 3.62, und so kurz (wenn auch »technisch«) die Beweise sind: Die Beweise, die wir hier gegeben haben, benötigen die Voraussetzung, dass es sich um ein Produkt mit endlicher Indexmenge handelt beziehungsweise dass Y eine endliche Menge ist. Für beliebige Indexmengen und Mengen Y sind diese (zueinander äquivalenten) Aussagen genau der Inhalt des Auswahlaxioms, eines der Axiome der Mengenlehre. Siehe Anhang A.1.

LEMMA 3.63. *Sei $f\colon X \to Y$ eine Abbildung zwischen endlichen Mengen.*

(1) *Wenn f injektiv ist, dann gilt $\#X \leq \#Y$.*

(2) *Wenn f surjektiv ist, dann gilt $\#X \geq \#Y$.*

BEWEIS. Seien m und n die Mächtigkeiten von X und Y. Dann existieren Bijektionen $g\colon [m] \to X$, $h\colon [n] \to Y$. Die Verkettung $h^{-1} \circ f \circ g$ ist dann eine Injektion $[m] \to [n]$, und es folgt $m \leq n$ mit Lemma 3.57.

Für den Beweis von Teil (2) wenden wir Korollar 3.62 an und finden eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Dann ist g notwendigerweise injektiv (Lemma 3.33) und die Behauptung folgt aus Teil (1), angewandt auf g. □

SATZ 3.64. *Seien X, Y endliche Mengen mit $\#X = \#Y$. Sei $f\colon X \to Y$ eine Abbildung. Dann sind äquivalent:*

(i) *Die Abbildung f ist injektiv.*

(ii) *Die Abbildung f ist surjektiv.*

(iii) *Die Abbildung f ist bijektiv.*

BEWEIS. Es ist offenbar ausreichend, die Äquivalenz von (i) und (ii) zu zeigen, denn nach Definition gilt (iii) $\Leftrightarrow$ (i) und (ii).

Sei zunächst f injektiv. Ist f nicht surjektiv, dann existiert $y \in Y \setminus \mathrm{Im}(f)$, also können wir f als Abbildung $X \to Y \setminus \{y\}$ betrachten (die natürlich ebenfalls injektiv ist). Das würde wegen Lemma 3.59 und Lemma 3.63 bedeuten, dass $\#X \leq \#Y - 1$, ein Widerspruch.

Ist andererseits f surjektiv, so gibt es nach Korollar 3.62 eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Lemma 3.33 zeigt, dass g injektiv ist. Aus Teil (1) folgt nun, dass g sogar bijektiv ist. Da $f \circ g$ und g bijektiv sind, ist auch f bijektiv. □

ERGÄNZUNG 3.65 (Hilberts Hotel). Für eine unendliche Menge ist das Lemma nicht richtig. Überlegen Sie sich eine injektive Abbildung $\mathbb{N} \to \mathbb{N}$, die nicht surjektiv ist, und eine surjektive Abbildung $\mathbb{N} \to \mathbb{N}$, die nicht injektiv ist.

Die Existenz von injektiven, aber nicht surjektiven Abbildungen $\mathbb{N} \to \mathbb{N}$ wird in dem Gedankenexperiment des Hotels mit unendlich vielen Zimmern (zu jeder natürlichen Zahl n gibt es das Zimmer Nummer n) illustriert, das D. Hilbert in seiner Vorlesung »Über das Unendliche« 1924 beschrieben hat: Sind alle Zimmer mit Gästen belegt und kommt ein weiterer Gast an, so bittet der Hotelchef einfach jeden Gast, ein Zimmer weiter zu ziehen (von Zimmer n nach Zimmer $n+1$). Dann ist Zimmer 0 frei.

Hilberts Hotel auf Wikipedia[18] und auf Youtube: Video von C. Spannagel[19], Steven Strogatz and Hilbert's Infinite Hotel/WorldScienceFestival[20] (englisch), Video von J. Dekofsky/Ted-ED[21] (englisch).

Siehe Abschnitt 3.14. □ Ergänzung 3.65

3.13. Relationen *

3.13.1. Definition. Die Definitionen aus diesem Abschnitt kann man zunächst überspringen. Thematisch gehören sie aber dennoch ins Grundlagenkapitel und sind daher hier einsortiert. Zum Teil kommen die Begriffe in den Ergänzungen vor, jedenfalls implizit. In der Linearen Algebra 2 werden wir dann noch einmal darauf zurückkommen.

DEFINITION 3.66. Eine *Relation* zwischen zwei Mengen X und Y ist eine Teilmenge $R \subseteq X \times Y$. ⊣

Sofern man von einer Relation zwischen X und Y keine weiteren Eigenschaften kennt, ist der Begriff eher uninteressant (und es gäbe keinen Grund, dafür eine eigene Bezeichnung einzuführen). Der Sinn der Sache ist, Relationen zu betrachten, die durch zusätzliche Eigenschaften besonders ausgezeichnet sind. Dabei gibt es mehrere Arten von Eigenschaften, die es zu betrachten lohnt.

Ein wichtiges Beispiel haben wir bereits gesehen: Eine Abbildung $X \to Y$ ist eine Relation zwischen X und Y mit der Eigenschaft, dass für jedes $x \in X$ genau ein $y \in Y$ existiert, so dass $(x,y) \in R$.

In den folgenden beiden Abschnitten betrachten wir bestimmte Relationen zwischen einer Menge X und sich selbst, also Teilmengen von $X \times X$. Einerseits die *Äquivalenzrelationen*, die dazu dienen, Objekte zusammenzufassen, die zwar nicht unbedingt gleich, aber doch gleichartig sind, was gewisse Eigenschaften angeht. Andererseits *(partielle) Ordnungen*, die beschreiben, wie man Elemente einer Menge vergleichen und anordnen kann.

3.13.2. Äquivalenzrelationen. Sei $R \subseteq X \times X$ eine Relation. Oft wählt man ein Symbol, zum Beispiel $\sim$ und definiert $x \sim y$ als $(x,y) \in R$. Wir sagen dann auch, dass $\sim$ eine Relation auf X sei.

DEFINITION 3.67. Sei $\sim$ eine Relation auf einer Menge X.

(1) Die Relation $\sim$ heißt *reflexiv*, wenn für alle $x \in X$ gilt: $x \sim x$.

[18] https://de.wikipedia.org/wiki/Hilberts_Hotel
[19] https://www.youtube.com/watch?v=XTsaZRKx9UI
[20] https://www.youtube.com/watch?v=wE9fl6tUWhc
[21] https://www.youtube.com/watch?v=Uj3_KqkI9Zo

(2) Die Relation $\sim$ heißt *symmetrisch*, wenn für alle $x, y \in X$ genau dann $x \sim y$ gilt, wenn $y \sim x$ gilt.

(3) Die Relation $\sim$ heißt *transitiv*, wenn für alle $x, y, z \in X$ mit $x \sim y$ und $y \sim z$ gilt, dass $x \sim z$.

(4) Die Relation $\sim$ heißt eine *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist.

⊣

Beispiel 3.68. Ist X eine Menge, so ist Gleichheit $=$ eine Äquivalenzrelation. ◊

Beispiel 3.69. Sei $X \subset \mathbb{Z} \times \mathbb{Z}$ die Menge aller Paare von ganzen Zahlen (a, b) mit $b \neq 0$. Wir definieren für $(a, b), (c, d) \in X$:

$$(a, b) \sim (c, d) \quad \Longleftrightarrow \quad ad = bc$$

Dies ist offenbar eine Relation zwischen X und X. Es ist nicht schwierig nachzuprüfen, dass es sich um eine Äquivalenzrelation handelt. (Sie sollten das zur Übung tun.) Siehe Beispiel 3.72 für die Fortsetzung dieses Beispiels. Wenn Ihnen dieses Beispiel ziemlich künstlich vorkommt, dann ist das in Ordnung, aber Sie sollten gerade dann auch Beispiel 3.72 bis zum Ende lesen. ◊

Sei $\sim$ eine Äquivalenzrelation auf X. Wir sagen dann, $y \in X$ sei *äquivalent* zu x, wenn $x \sim y$ gilt. Für $x \in X$ nennen wir

$$\{y \in X;\ y \sim x\},$$

die Menge aller Elemente, die bezüglich $\sim$ in Relation zu x stehen, die *Äquivalenzklasse* von x. Oft schreibt man $[x]$ für die Äquivalenzklasse von x.

Beispiel 3.70. Sei $X = \mathbb{Z}$ die Menge der ganzen Zahlen. Wir definieren für $x, y \in \mathbb{Z}$:

$$x \sim y \quad \Longleftrightarrow \quad x - y \text{ ist durch 3 teilbar.}$$

Dies ist offenbar eine Relation zwischen $\mathbb{Z}$ und $\mathbb{Z}$. Man prüft leicht nach, dass es sich um eine Äquivalenzrelation handelt. (Sie sollten das zur Übung tun.) Oft schreibt man $x \equiv y \mod 3$ statt $x \sim y$.

In diesem Fall gibt es drei Äquivalenzklassen: Erstens die Teilmenge von $\mathbb{Z}$, die aus allen Zahlen besteht, die durch 3 teilbar sind; zweitens die Teilmenge aller Zahlen, die bei Division durch 3 Rest 1 haben. Und drittens die Teilmenge derjenigen Zahlen, die bei Division durch 3 Rest 2 haben. Die Äquivalenzklassen für diese spezielle Äquivalenzrelation nennt man auch *Restklassen modulo* 3.

Siehe Beispiel 3.73 für die Fortsetzung dieses Beispiels. ◊

Aus Reflexivität, Symmetrie und Transitivität der Äquivalenzrelation folgt, dass je zwei Elemente einer Äquivalenzklasse zueinander äquivalent sind. Außerdem gilt: Ist y in der Äquivalenzklasse von x enthalten und gilt $y \sim z$, so liegt auch z in der Äquivalenzklasse von x; das ist einfach eine Umformulierung der Transitivität.

Lemma 3.71. *Sei $\sim$ eine Äquivalenzrelation auf X. Seien $A, B \subseteq X$ Äquivalenzklassen. Dann gilt entweder $A = B$ oder $A \cap B = \emptyset$.*

Mit anderen Worten: Zwei Äquivalenzklassen sind entweder gleich (die gleiche Teilmenge von X) oder disjunkt.

BEWEIS. Wir zeigen, dass aus $A \cap B \neq \emptyset$ folgt, dass $A = B$. Sei dazu $x \in A \cap B$. Ist dann $y \in A$, so folgt $x \sim y$ (denn $x, y \in A$) und damit $y \in B$ (denn $x \in B$ und B ist eine Äquivalenzklasse). □

Ist $A \subseteq X$ eine Äquivalenzklasse (bezüglich $\sim$) und ist $x \in A$, so nennt man x einen *Repräsentanten* der Äquivalenzklasse. Dann gilt $A = \{y \in X;\, y \sim x\}$.

Wir bezeichnen mit $X/\sim$ die Menge aller Äquivalenzklassen. Dies ist also eine Menge, deren Elemente Teilmengen von X sind. Die Abbildung $X \to X/\sim,\, x \mapsto [x]$, die jedes Element von X auf seine Äquivalenzklasse abbildet, bezeichnet man auch als die *kanonische Projektion*. Per Definition ist diese Abbildung surjektiv, aber in aller Regel nicht injektiv: Denn für $x \sim y$ gilt ja $[x] = [y]$, also haben äquivalente Elemente x und y dasselbe Bild unter dieser Abbildung.

Um eine Abbildung f von der Menge $X/\sim$ in eine Menge Y zu definieren, gibt man $f([x])$ oft an, indem man x verwendet. Weil für $x \sim y$ aber $[x] = [y]$ gilt und deswegen $f([x]) = f([y])$ gelten muss, ist das problematisch. Wenn die »Formel« für $f([x])$ wirklich von x abhängt und für y mit $y \sim x$ ein anderes Ergebnis liefern würde, dann hätten wir gar keine Zuordnung definiert. Siehe Beispiel 3.72 für Beispiele. Wenn die gegebene Vorschrift für alle Elemente der Äquivalenzklasse dasselbe Ergebnis liefert, also unabhängig ist von der Wahl des Repräsentanten der Äquivalenzklasse, dann sagt man, die Vorschrift sei *wohldefiniert*. Oft sagt man auch, die Abbildung sei wohldefiniert.

BEISPIEL 3.72. Wir nehmen wieder die Notation von Beispiel 3.69 auf. Wir hatten eine Äquivalenzrelation $\sim$ auf der Menge aller Paare (a, b) von ganzen Zahlen mit $b \neq 0$ definiert. Wir bezeichnen mit Q die Menge der Äquivalenzklassen, also $Q = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim$. Wir wollen als erstes die im vorherigen Absatz angesprochene Problematik (Stichwort »wohldefiniert«) aufgreifen.

Betrachten wir die Vorschrift $[(a, b)] \mapsto a + b$. Definiert diese eine Abbildung $f\colon Q \to \mathbb{Z}$? Nein, denn die Vorschrift ist nicht wohldefiniert! Es gilt nämlich zum Beispiel $(1, 1) \sim (2, 2)$, also $[(1, 1)] = [(2, 2)]$, aber nicht $1 + 1 = 2 + 2$.

Die Vorschrift $[(a, b)] \mapsto \frac{a}{b}$ ist hingegen wohldefiniert, denn wenn $(a, b) \sim (c, d)$, dann bedeutet das $ad = cb$, also tatsächlich $\frac{a}{b} = \frac{c}{d}$. Wir erhalten so eine Abbildung $i\colon Q \to \mathbb{Q}$.

Die folgende Vorschrift ist ein anderes Beispiel für eine wohldefinierte Zuordnung, und zwar ordnen wir jedem Paar von Elementen in Q ein neues Element in Q zu:

$$M\colon Q \times Q \longrightarrow Q, \quad ([(a, b)], [(c, d)]) \mapsto [(ac, bd)].$$

Wir haben hier die Wohldefiniertheit schon vorweggenommen und so getan, als hätten wir schon eine Abbildung $Q \times Q \to Q$ in der Hand. Wir müssen sie aber natürlich überprüfen. Sei also $[(a, b)] = [(a', b')]$, das bedeutet $ab' = ba'$, und $[(c, d)] = [(c', d')]$, das heißt $cd' = dc'$. Dann gilt tatsächlich $[(ac, bd)] = [(a'c', b', d')]$, denn das heißt ja genau, dass $(ac, bd) \sim (a'c', b', d')$, und wir haben

$$acb'd' = (ab')(cd') = (ba')(dc') = bda'c'.$$

In ähnlicher Weise definieren wir eine Abbildung $A\colon Q \times Q \longrightarrow Q$:

$$A\colon Q \times Q \longrightarrow Q, \quad ([(a, b)], [(c, d)]) \mapsto [(ad + bc, bd)].$$

Wieder muss man überprüfen, dass diese Vorschrift wohldefiniert ist, also dass im Fall $[(a, b)] = [(a', b')]$, das bedeutet $ab' = ba'$, und $[(c, d)] = [(c', d')]$ auch $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$ gilt. Führen Sie diese Rechnung durch.

Um das Beispiel abzuschließen, führen wir noch die Notationen

$$[(a, b)] \cdot [(c, d)] := M([(a, b)], [(c, d)]) \quad \text{und} \quad [(a, b)] + [(c, d)] := A([(a, b)], [(c, d)])$$

ein, wir betrachten also M und A als Multiplikation und Addition auf der Menge Q.

Wir kommen nun noch einmal auf die Abbildung $i\colon Q \to \mathbb{Q}$ zurück. Sie hat die folgenden Eigenschaften:

(1) i ist bijektiv,

(2) $i([(a,b)]+[(c,d)]) = i([(ad+bc,bd)]) = \frac{ad+bc}{bd} = \frac{a}{b}+\frac{c}{d} = i([(a,b)])+i([(c,d)])$

(3) $i([(a,b)]\cdot[(c,d)]) = i([(ac,bd)]) = \frac{ac}{bd} = \frac{a}{b}\cdot\frac{c}{d} = i([(a,b)])\cdot i([(c,d)])$

Zur ersten Aussage: Die Surjektivität ist klar, denn jedes Element von $\mathbb{Q}$ hat die Form $\frac{a}{b}$ für geeignete ganze Zahlen a und $b \neq 0$, und $\frac{a}{b} = i[(a,b)]$. Zur Injektivität: Wenn $i([a,b]) = i([c,d])$, also $\frac{a}{b} = \frac{c}{d}$, dann gilt $ad = bc$. Das bedeutet aber $(a,b) \sim (c,d)$, also $[(a,b)] = [(c,d)]$.

Das bedeutet, dass die Abbildung i eine Identifikation von Q und $\mathbb{Q}$ erlaubt, die mit Addition und Multiplikation verträglich ist. Eine andere Sichtweise ist, dass wir eine Konstruktion der rationalen Zahlen ausgehend von den ganzen Zahlen kennengelernt haben, denn wenn wir $\mathbb{Q}$ noch nicht kennen würden, ist die Menge Q mit den Rechenoperationen, die wir definiert haben, ein vollwertiger Ersatz. ◊

Beispiel 3.73. Wir nehmen wieder die Notation von Beispiel 3.70 auf.

Die Ausführungen hier sind etwas skizzenhaft. Betrachten Sie das Beispiel als erweiterte Übungsaufgabe und/oder melden Sie sich, wenn Sie gerne weitere Details hätten.

Wie üblich bezeichnen wir die Äquivalenzklasse von x mit $[x]$. Wir hatten schon festgestellt, dass $\mathbb{Z}/\sim = \{[0],[1],[2]\}$ gilt. (Die eckigen Klammern haben hier eine andere Bedeutung als in Abschnitt 3.12.)

Eine interessante Beobachtung ist, dass man mit Restklassen modulo 3 (das war unser Name für die Äquivalenzklassen in diesem Beispiel) ähnlich rechnen kann wie ganzen Zahlen: Für alle $x, x', y, y' \in \mathbb{Z}$ mit $x \sim x'$ und $y \sim y'$ gilt

$$x+y \sim x'+y', \qquad xy \sim x'y',$$

also

$$[x+y] = [x'+y'], \qquad [xy] \sim [x'+y'].$$

Ähnlich wie in Beispiel 3.72 (aber sogar noch einfacher) haben wir also eine *wohldefinierte* Addition und Multiplikation auf der Menge der Äquivalenzklassen, die gegeben ist durch

$$[x]+[y] := [x+y], \qquad [x]\cdot[y] := [xy].$$

Wir dürfen also, salopp gesagt, die Rechenzeichen $+$ und $\cdot$ beliebig in die oder aus den eckigen Klammern ziehen.

Ein paar Beispielrechnungen:

$[10] = [1]$ denn 10 hat bei Division durch 3 Rest 1,
$[100] = [1]$ denn 100 hat bei Division durch 3 Rest 1,
oder wir rechnen $[100] = [10\cdot 10] = [10]\cdot[10] = [1]\cdot[1] = [1\cdot 1] = [1]$,
$[10^i] = [1]$ für alle $i \in \mathbb{N}$, mit einem ähnlichen Argument,

und

$$[752] = [7+5+2] = [14] = [2]$$

denn

$$[752] = [7\cdot 100 + 5\cdot 10 + 2] = [7]\cdot[100] + [5]\cdot[10] + [2] = [7]+[5]+[2] = [7+5+2].$$

Die letzte Rechnung lässt sich offensichtlich auf beliebige natürliche Zahlen verallgemeineren und zeigt: Eine natürliche Zahl hat denselben Rest bei Division durch 3 wie ihre Quersumme (die Summe aller ihrer Ziffern).

Insbesondere haben wir das bekannte Kriterium für Teilbarkeit durch 3 bewiesen: Eine natürliche Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Können Sie diese Betrachtungen auf den Fall $n = 9$ übertragen? Was ist zum Beispiel im Fall $n = 7$ anders?

Vergleiche Abschnitt 4.2.1. ◊

Zum Schluss wollen wir noch zwei etwas andere Sichtweisen auf den Begriff der Äquivalenzrelation angeben (was hoffentlich unterstreicht, dass es sich vom Prinzip her um etwas sehr einfaches handelt).

BEMERKUNG 3.74. Ist $f\colon X \to Y$ eine (surjektive) Abbildung, so wird durch

$$x \sim x' \quad \Longleftrightarrow \quad f(x) = f(x')$$

eine Äquivalenzrelation auf X definiert. Umgekehrt hat jede Äquivalenzrelation diese Form, denn man kann für f die kanonische Projektion auf die Menge aller Äquivalenzklassen verwenden. ◊

BEMERKUNG 3.75. Ist $\sim$ eine Äquivalenzrelation, so bilden die Äquivalenzklassen eine Familie von paarweise disjunkten Teilmengen von X, deren Vereinigung ganz X ist.

Ist umgekehrt eine solche Darstellung von $X = \bigcup_{i\in I} X_i$ als Vereinigung von paarweise disjunkten nicht-leeren Teilmengen X_i gegeben, so können wir eine Äquivalenzrelation auf X definieren durch

$$x \sim x' \quad \Longleftrightarrow \quad \text{es gibt } i \text{ mit } x, x' \in X_i.$$

◊

3.13.3. Partielle und totale Ordnungen.

DEFINITION 3.76. Sei X eine Menge und $\preceq$ eine Relation zwischen X und sich selbst.

(1) Die Relation $\preceq$ heißt *antisymmetrisch*, wenn für alle $x, y \in X$ mit $x \preceq y$ und $y \preceq x$ gilt, dass $x = y$.
(2) Die Relation $\preceq$ heißt eine *partielle Ordnung* (oder *Halbordnung* oder manchmal einfach *Ordnung*), wenn sie reflexiv, transitiv und antisymmetrisch ist.

⊣

BEISPIEL 3.77. Sei M eine Menge, und sei $P(M)$ die Potenzmenge von M, also die Menge aller Teilmengen von M. Die Relation $\subseteq$ der Inklusion von Teilmengen ist dann eine partielle Ordnung auf $P(M)$ (und natürlich auch auf allen Teilmengen von $P(M)$). ◊

Ein wichtiger Punkt (und das soll durch das Wort *partiell* betont werden) ist, dass es in der Situation der Definition Elemente x, y geben kann, für die *weder* $x \preceq y$ *noch* $y \preceq x$ gilt. In der Situation des Beispiels ist das in der Tat klar: Sind $A, B \subseteq M$ Teilmengen, dann kann es passieren, dass weder $A \subseteq B$ noch $B \subseteq A$ gilt.

DEFINITION 3.78. Sei X eine Menge und $\preceq$ eine Relation zwischen X und sich selbst.

(1) Die Relation $\preceq$ heißt *total*, wenn für alle $x, y \in X$ gilt, dass $x \preceq y$ oder $y \preceq x$.
(2) Eine Relation $\preceq$ heißt eine *totale Ordnung* (oder *lineare Ordnung*), wenn sie reflexiv, transitiv, antisymmetrisch und total ist.

⊣

Mit anderen Worten: Eine totale Ordnung ist eine partielle Ordnung, bezüglich derer je zwei Elemente stets »vergleichbar« sind, d.h. in Relation stehen (in der einen oder anderen Reihenfolge).

BEISPIEL 3.79. Die übliche $\leq$-Relation ist eine totale Ordnung auf der Menge der reellen Zahlen (und ebenso auf $\mathbb{Q}, \mathbb{Z}, \mathbb{N}$). ◊

DEFINITION 3.80. Sei $\preceq$ eine partielle Ordnung auf X.

(1) Ein Element $x \in X$ heißt *minimales Element* (bezüglich $\preceq$), wenn für alle $y \in X$ mit $y \preceq x$ gilt: $y = x$.
(2) Ein Element $x \in X$ heißt *kleinstes Element* (bezüglich $\preceq$), wenn für alle $y \in X$ gilt: $x \preceq y$.
(3) Ein Element $x \in X$ heißt *maximales Element* (bezüglich $\preceq$), wenn für alle $y \in X$ mit $x \preceq y$ gilt: $y = x$.
(4) Ein Element $x \in X$ heißt *größtes Element* (bezüglich $\preceq$), wenn für alle $y \in X$ gilt: $y \preceq x$.

⊣

Im allgemeinen muss es weder minimale noch maximale Elemente (und erst recht kein kleinstes oder größtes Element) geben; betrachten Sie zum Beispiel die $\leq$-Ordnung auf $\mathbb{Z}$.

Wenn es ein kleinstes Element (bezüglich einer partiellen Ordnung) gibt, dann ist dieses eindeutig bestimmt (und ist ein minimales Element). Wenn es ein eindeutig bestimmtes minimales Element gibt, dann ist dieses das kleinste Element. Entsprechendes gilt für maximale Elemente und das größte Element.

Wenn $\preceq$ eine totale Ordnung ist, dann fallen die Begriffe des minimalen Elements und des kleinsten Elements zusammen; ebenso die Begriffe des maximalen und des größten Elements.

BEISPIEL 3.81. Wir betrachten auf $\mathbb{N}$ die Relation $d \mid n$ der Teilbarkeit. Dies ist eine partielle Ordnung. Für alle $n \in \mathbb{N}$ gilt $1 \mid n$, also ist 1 das kleinste Element in $\mathbb{N}$ bezüglich der Teilbarkeitsordnung. Weil $n \mid 0$ für alle n gilt, ist 0 das größte Element in $\mathbb{N}$ für diese partielle Ordnung!

Für natürliche Zahlen a, b ist $ggT(a, b)$ das größte Element (bezüglich Teilbarkeit) der Menge aller positiven gemeinsamen Teiler von a und b. Mit dieser Beschreibung ist es nicht notwendig, den Fall $a = b = 0$ gesondert zu betrachten.

Um das zu beweisen, müssen wir zeigen, dass jeder gemeinsame Teiler d von a und b auch ein Teiler von $\mathrm{ggT}(a, b)$ ist. Das folgt aus Lemma 3.53, das besagt, dass wir $\mathrm{ggT}(a, b) = xa + yb$ schreiben können (mit ganzen Zahlen x und y).

In der Menge $\{2, 3, 5, 7, 11, \dots\}$ der Primzahlen ist jedes Element gleichzeitig minimal und maximal bezüglich Teilbarkeit. Es gibt weder ein kleinstes noch ein größtes Element. ◊

3.14. Mächtigkeit von Mengen *

Für endliche Mengen haben wir die Mächtigkeit in Abschnitt 3.12 definiert. Wir wollen hier die Erweiterung dieses Begriffs auf den Fall unendlicher Mengen skizzieren. (Für den Moment ohne Beweise.)

In Kapitel 5 in Soergels Skript [**So-AZT**] und in dem (englischen) Buch [**Hu**] (Introduction, Abschnitt 8) von Hungerford finden Sie mehr Informationen zu diesem Thema.

DEFINITION 3.82. Wir nennen zwei Mengen M, M' *gleichmächtig*, wenn eine bijektive Abbildung $M \to M'$ existiert. Wir schreiben dann $\#M = \#M'$ ⊣

Achtung: Zwei unendliche Mengen sind nicht unbedingt gleichmächtig (siehe unten). Aus der unpräzisen Aussage $\#M = \infty$, $\#M' = \infty$ lässt sich also nicht die Gleichheit $\#M = \#M'$ im Sinne dieser Definition folgern.

Wir drücken uns hier darum, genau zu sagen, was für ein Objekt $\#M$ eigentlich ist. (Man nennt diese Ausdrücke Kardinalzahlen[22].) Es soll für uns genügen zu wissen, wie man Kardinalzahlen vergleicht.

DEFINITION 3.83. Eine Menge M heißt *abzählbar* (oder genauer *abzählbar unendlich*), wenn M gleichmächtig ist zur Menge $\mathbb{N}$ der natürlichen Zahlen. Man schreibt dann auch $\#M = \aleph_0$. ⊣

($\aleph$, ausgesprochen Aleph, ist der erste Buchstabe des hebräischen Alphabets.)

Wenn man von einer Menge M sagt, sie sei *höchstens abzählbar*, so meint man, dass M endlich oder abzählbar unendlich sei.

SATZ 3.84. (1) $\mathbb{Q}$ *ist abzählbar.*

(2) $\mathbb{R}$ *ist nicht abzählbar.*

Siehe auch Ergänzung 3.65.

Wir können die Mächtigkeiten von Mengen folgendermaßen anordnen: Sind M, M' Mengen, so schreiben wir $\#M \leq \#M'$, wenn es eine injektive Abbildung $M \to M'$ gibt. Wir schreiben $\#M < \#M'$, wenn $\#M \leq \#M'$ und nicht $\#M = \#M'$ gilt, d.h. wenn es eine Injektion $M \to M'$, aber keine Bijektion zwischen M und M' gibt. Diese Definition für $\leq$ erfüllt die Eigenschaften einer totalen Ordnung: Offenbar folgt aus $\#M \leq \#M'$ und $\#M' \leq \#M''$, dass $\#M \leq \#M''$, weil die Verkettung injektiver Abbildungen wieder injektiv ist. Es ist auch klar, dass $\#M \leq \#M$ für alle M gilt, da die Identität eine injektive Abbildung ist.

Etwas schwieriger sind die folgenden beiden Ergebnisse, die die Antisymmetrie und Totalität zeigen:

THEOREM 3.85 (Satz von Schröder-Bernstein). *Seien M, M' Mengen. Wenn es injektive Abbildungen $M \to M'$ und $M' \to M$ gibt, dann gibt es eine Bijektion $M \to M'$, d.h. M und M' sind gleichmächtig.*

THEOREM 3.86. *Seien M, M' Mengen. Dann gilt genau eine der folgenden drei Aussagen:*

$$\#M < \#M', \quad \#M = \#M', \quad \#M > \#M'.$$

SATZ 3.87. *Sei M eine unendliche Menge. Dann gilt $\#M \geq \#\mathbb{N}$.*

BEISPIEL 3.88. Sei M eine Menge und $P(M)$ ihre Potenzmenge, d.h. die Menge alle Teilmengen von M. Dann gilt $\#M < \#P(M)$.

Es ist klar, dass es eine Injektion $M \to P(M)$ gibt, zum Beispiel die Abbildung $m \mapsto \{m\}$. Wir müssen daher zeigen, dass es keine Surjektion $M \to P(M)$ gibt. Sei $\varphi: M \to P(M)$ eine Abbildung. Wir behaupten, dass $X := \{m \in M;\ m \notin \varphi(m)\}$ nicht im Bild von φ liegt (insbesondere ist φ nicht surjektiv). In der Tat, nehmen wir an, dass $X = \varphi(m)$ für ein $m \in M$. Wenn $m \in X$, dann folgt $m \notin \varphi(m) = X$, ein Widerspruch. Wenn $m \notin X$, dann folgt $m \notin \varphi(m)$, also $m \in X$, auch ein Widerspruch. Weil weder $m \in X$ noch $m \notin X$ richtig sein kann, kann die Teilmenge X von M nicht im Bild von φ liegen. ◊

[22] https://de.wikipedia.org/wiki/Kardinalzahl_(Mathematik)

Beispiel 3.89. Es gilt $\#P(\mathbb{N}) = \#\mathbb{R}$. ◊

Ergänzung 3.90 (Die Kontinuumshypothese). Unter der *Kontinuumshypothese* versteht man die Aussage, dass jede Menge M mit $\#\mathbb{N} \leq \#M \leq \#P(\mathbb{N})$ entweder abzählbar ist (also $\#\mathbb{N} = \#M$ gilt), oder die Mächtigkeit von $P(\mathbb{N})$ hat, also $\#M = \#P(\mathbb{N})(= \#\mathbb{R})$.

Es wurde von K. Gödel und P. Cohen bewiesen, dass die Kontinuumshypothese unabhängig von dem üblichen Axiomensystem ZFC ist – sie lässt sich weder widerlegen (Gödel, 1938), noch beweisen (Cohen, 1960). Man könnte also entweder die Kontinuumshypothese zu den anderen Axiomen hinzunehmen, oder ihre Negation.

Die *verallgemeinerte Kontinuumshypothese* ist die Aussage, dass für jede unendliche Menge M keine Mächtigkeit existiert, die strikt zwischen $\#M$ und $\#P(M)$ liegt. Sie ist ebenfalls unabhängig von ZFC. □ Ergänzung 3.90

KAPITEL 4

Körper

Um Lösungsmengen von Gleichungssystemen sinnvoll zu betrachten, müssen wir sagen, in welchem Bereich wir nach Lösungen suchen. Zum Beispiel ist es bei der Gleichung $x^2 = 2$ wichtig zu sagen, ob Lösungen in $\mathbb{Q}$ oder in $\mathbb{R}$ gesucht sind – im ersten Fall gibt es keine, im zweiten Fall existieren zwei Lösungen.

Um die Theorie nicht für jeden Zahlbereich neu entwickeln zu müssen, legen wir daher zunächst fest, welche Bedingungen wir an die Grundmenge stellen wollen, in der wir nach Lösungen der zu betrachtenden Gleichungssysteme schauen. Diese Bedingungen werden im Begriff des *Körpers* zusammengefasst.

4.1. Körper

4.1.1. Anschaulich gesprochen formalisiert der Begriff des *Körpers*, der in der folgenden Definition erklärt wird, die essenziellen Eigenschaften der Grundrechenarten (Addition $+$, Subtraktion $-$, Multiplikation $\cdot$ und Division $/$), wie sie zum Beispiel für rationale und reelle Zahlen gelten, aber eben auch in anderen »Zahlbereichen«.

Andere Eigenschaften der rationalen und reellen Zahlen (speziell die Eigenschaft der »Anordnung«, also dass man sinnvoll von positiven und negativen Zahlen sprechen kann) und Eigenschaften, in denen sich die Bereiche der rationalen und der reellen Zahlen unterscheiden, werden in der Definition eines Körpers nicht angesprochen.

Ein Körper in diesem Sinne hat nichts mit einem Körper im geometrischen Sinne zu tun. Das englische Wort für Körper im Sinne von Definition 4.1 ist »field«.

Die Definition wird uns erlauben, im folgenden viele Tatsachen mit einem einzigen Beweis für die rationalen Zahlen, für die reellen Zahlen und für alle anderen Körper auch zu beweisen. Dies ist ein Grundprinzip der Mathematik: Versuche zu abstrahieren, welche Eigenschaften eines Objekts für eine gewisse Aussage wirklich erforderlich sind, und »baue« aus diesen essenziellen Eigenschaften eine Definition.

Für eine Menge K verstehen wir unter einer *Verknüpfung* (auf K) eine Abbildung $K \times K \to K$. Eine Verknüpfung erlaubt uns also, zwei Elemente von K herzunehmen (also ein Element von $K \times K$) und daraus ein neues Element von K zu »produzieren«. Typische Beispiele sind die Addition und Multiplikation von (ganzen, rationalen, reellen, …) Zahlen. Diese Beispiele werden in der folgenden Definition abstrahiert.

DEFINITION 4.1. Ein *Körper* ist ein Tripel $(K, +, \cdot)$ bestehend aus einer Menge K und Verknüpfungen

$$+\colon K \times K \to K, \quad \cdot\colon K \times K \to K,$$

so dass gilt:

(1) Die Verknüpfung $+$ ist assoziativ, kommutativ, hat ein eindeutig bestimmtes neutrales Element 0 und es existieren (eindeutig bestimmte) inverse Elemente, genauer:

   (a) Es gilt das *Assoziativgesetz*, d.h. für alle $a, b, c \in K$ gilt

$$(a + b) + c = a + (b + c).$$

(b) Es gilt das *Kommutativgesetz*, d.h. für alle $a, b \in K$ gilt

$$a + b = b + a.$$

(c) Es gibt ein eindeutig bestimmtes *neutrales Element* bezüglich der Addition, d.h. ein eindeutig bestimmtes Element $0 \in K$, so dass

$$0 + a = a + 0 = a \quad \text{für alle } a \in K.$$

(d) Jedes Element $a \in K$ besitzt ein *inverses Element* bezüglich der Addition, d.h. es existiert $b \in K$ mit

$$a + b = 0 = b + a,$$

wobei 0 das im vorherigen Punkt geforderte neutrale Element bezeichnet. (Wir sehen unten, dass dann zu jedem $a \in K$ *genau ein* inverses Element existiert, d.h. b ist durch a eindeutig bestimmt. Wir bezeichnen das Inverse von a bezüglich der Addition mit $-a$; es gilt dann also $a + (-a) = 0 = (-a) + a$.)

(2) Die Verknüpfung $\cdot$ ist assoziativ, kommutativ, hat ein eindeutig bestimmtes neutrales Element 1, das von 0 verschieden ist, und für alle $x \in K \setminus \{0\}$ existiert ein inverses Element, genauer:

(a) Es gilt das *Assoziativgesetz*, d.h. für alle $a, b, c \in K$ gilt

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(b) Es gilt das *Kommutativgesetz*, d.h. für alle $a, b \in K$ gilt

$$a \cdot b = b \cdot a.$$

(c) Es gibt ein eindeutig bestimmtes *neutrales Element* bezüglich der Multiplikation, d.h. ein Element $1 \in K$, so dass

$$1 \cdot a = a \cdot 1 = a \quad \text{für alle } a \in K.$$

(d) Jedes Element $a \in K \setminus \{0\}$ besitzt ein *inverses Element* bezüglich der Multiplikation, d.h. es existiert $b \in K$ mit

$$a \cdot b = 1 = b \cdot a,$$

wobei 1 das im vorherigen Punkt geforderte neutrale Element bezeichnet. (Wir sehen unten, dass dann zu jedem $a \in K \setminus \{0\}$ *genau ein* inverses Element existiert, d.h. b ist durch a eindeutig bestimmt. Wir bezeichnen das Inverse von a bezüglich der Multiplikation mit a^{-1}; es gilt dann also $a \cdot a^{-1} = 1 = a^{-1} \cdot a$. Beachte, dass dieser Punkt auf das neutrale Element der Addition Bezug nimmt. Das Element 0 besitzt kein multiplikatives Inverses.)

(e) Es gilt $0 \neq 1$.

(3) Es gilt das *Distributivgesetz*:

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \text{für alle } a, b, c \in K.$$

⊣

Üblicherweise sagt man, K sei ein Körper und erwähnt die Verknüpfungen $+, \cdot$ nicht explizit. Wenn es unbedingt nötig ist, die Addition/Multiplikation auf verschiedenen Körpern in der Notation zu unterscheiden, schreibt man $+_K, \cdot_K$ (und gegebenenfalls 0_K statt 0, 1_K statt 1). In Termen mit Elementen aus K wird der Multiplikationspunkt $\cdot$ üblicherweise weggelassen, d.h. ab steht für $a \cdot b$. Wir verwenden die übliche Konvention *Punkt- vor Strichrechnung*, um nicht zu viele Klammern schreiben zu müssen. Das Distributivgesetz schreiben wir also auch in der Form $(a + b)c = ac + bc$.

Für $a, b \in K$ schreiben wir $a - b := a + (-b)$. Damit haben wir für jeden Körper auch eine Subtraktion $-: K \times K \to K$ definiert. Auch die Bruchschreibweise $\frac{a}{b} := ab^{-1} (= b^{-1}a)$ (für $a, b \in K$, $b \neq 0$) verwendet man manchmal für allgemeine Körper. Wir schreiben $K^\times = K \setminus \{0\}$, die sogenannte *multiplikative Gruppe* von K. Diese Bezeichnung wird erst später klar werden (Bemerkung 9.4 (2)), wenn wir den Begriff der *Gruppe* definieren; sie hängt damit zusammen, dass das Produkt von Elementen auf $K^\times$ wieder in $K^\times$ liegt (siehe Abschnitt 4.1.3) und dass jedes Element von $K^\times$ ein Inverses bezüglich der Multiplikation hat. Die Elemente von $K^\times$ heißen auch die *Einheiten* des Körpers K.

Für $n \in \mathbb{N}$ und $a \in K$ schreiben wir $a^n = a \cdot \cdots \cdot a$ (n Faktoren) und nennen dieses Element von K die n-te Potenz von a. Eine formale(re) Definition wäre zu sagen, dass $a^0 := 1$ und $a^n = a^{n-1} \cdot a$ für alle $n > 1$. Ist $a \neq 0$, so kann man auch $a^{-n} = (a^{-1})^n$ definieren.

4.1.2. Beispiele für Körper.

Beispiel 4.2. (1) Der Körper $\mathbb{Q}$ der *rationalen Zahlen*:

$$\mathbb{Q} = \left\{ \frac{a}{b};\ a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

Die Addition und Multiplikation sind durch die üblichen Bruchrechenregeln gegeben:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Das neutrale Element bezüglich der Addition ist $0 = \frac{0}{1}$, das neutrale Element bezüglich der Multiplikation ist $1 = \frac{1}{1}$. Das Inverse von $\frac{a}{b}$ bezüglich der Addition ist $\frac{-a}{b}$, das Inverse bezüglich der Multiplikation ist (für $a \neq 0$) $\frac{b}{a}$.

(2) Die Menge $\mathbb{R}$ der reellen Zahlen bildet bezüglich der »üblichen« Addition und Multiplikation einen Körper. (Auch wenn Sie die reellen Zahlen aus der Schule kennen und sie dort wohl häufiger verwendet wurden als der Körper der rationalen Zahlen, sollten Sie sich klarmachen, dass es wesentlich schwieriger ist, die reellen Zahlen und die Verknüpfungen $+$ und $\cdot$ darauf präzise zu definieren.) Siehe zum Beispiel [**He**] I.2. Eine axiomatische Charakterisierung finden Sie in praktisch allen Lehrbüchern der Analysis. Wie man die reellen Zahlen konstruieren kann, wird meistens nicht erklärt. Eine Möglichkeit bilden die Dedekindschen Schnitte[1]. Eine andere ist, die reellen Zahlen als Äquivalenzklassen von Cauchy-Folgen von rationalen Zahlen[2] zu betrachten; diese Sichtweise geht auf Cantor zurück. Die Algebra-Vorlesung wird dazu die nötigen Hilfsmittel bereitstellen.

◊

Beispiel 4.3. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist (mit der üblichen Addition und Multiplikation) *kein* Körper, denn es gibt zwar ein neutrales Element für die Multiplikation – die ganze Zahl 1 – aber zum Beispiel hat 2 kein multiplikatives Inverses: Es gibt keine ganze Zahl a mit $2a = 1$. (In der Tat sind 1 und -1 die einzigen Elemente, die ein multiplikatives Inverses haben, und zwar jeweils sich selbst.) Was die Bedingungen an die Addition (und die Distributivität) angeht, sind alle Bedingungen erfüllt.

Die Menge der natürlichen Zahlen ist ebenfalls kein Körper. In diesem Fall gibt es für Elemente $\neq 0$ nicht einmal ein additives Inverses. ◊

[1] https://de.wikipedia.org/wiki/Dedekindscher_Schnitt
[2] https://en.wikipedia.org/wiki/Construction_of_the_real_numbers#Construction_from_Cauchy_sequences

Literatur zu den oben genannten (und anderen) Zahlbereichen:

T. Körner, *Where do Numbers Come From?*, Cambridge Univ. Press, 2020.

J. Kramer, A. von Pippich, *Von den natürlichen Zahlen zu den Quaternionen*, Springer 2013, https://doi.org/10.1007/978-3-658-02055-2, oder die erweiterte englische Übersetzung *From Natural Numbers to Quaternions*, https://doi.org/10.1007/978-3-319-69429-0.

Oder der Klassiker
H. D. Ebbinghaus et al., *Zahlen*, Springer 1992.

DEFINITION 4.4. Seien $K \subseteq L$ Körper, deren zugrundeliegende Mengen ineinander enthalten sind. Wenn $x +_K y = x +_L y$ und $x \cdot_K y = x \cdot_L y$ für alle $x, y \in K$ gilt, dann heißt K ein *Teilkörper* von L, und L ein *Erweiterungskörper* von K. ⊣

Zum Beispiel ist $\mathbb{R}$ ein Erweiterungskörper von $\mathbb{Q}$.

BEISPIEL 4.5 (Die komplexen Zahlen). Sei $\mathbb{C}$ die Menge aller Paare (a, b) von reellen Zahlen. Eine komplexe Zahl können wir also auch als einen Punkt in der reellen Ebene $\mathbb{R}^2$ auffassen, wenn wir die beiden Einträge des Paars (a, b) als Koordinaten verstehen. Man spricht daher auch von der *komplexen Zahlenebene*.

Wir definieren eine Addition

$$(a, b) + (c, d) := (a + c, b + d),$$

und eine Multiplikation

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

Es ist dann nicht schwer zu überprüfen, dass $\mathbb{C}$ mit diesen Verknüpfungen ein Körper ist. Dass die Kommutativgesetze für $+$ und $\cdot$ gelten, kann man unmittelbar nachprüfen. Die Gültigkeit der Assoziativgesetze und des Distributivgesetzes kann man auch direkt nachrechnen; weil es etwas lästig ist, lassen wir die Rechnung hier aus. Wir werden aber später eine Möglichkeit kennenlernen, die Gültigkeit dieser Gesetze ohne weiteren Rechenaufwand zu beweisen, siehe Beispiel 5.42.

Es ist direkt ersichtlich, dass $0_{\mathbb{C}} = (0, 0)$ neutrales Element bezüglich der Addition und dass $1_{\mathbb{C}} = (1, 0)$ neutrales Element bezüglich der Multiplikation ist.

Das Negative (d.h. das additive Inverse) von (a, b) ist $(-a, -b)$. Am schwierigsten ist es vielleicht zu sehen, wie das multiplikative Inverse von (a, b) gegeben ist (sofern nicht $a = b = 0$ gilt). Wenn man die Formel

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

einmal hat, ist es aber leicht nachzurechnen, dass das Produkt dieser beiden Element tatsächlich gleich $1_{\mathbb{C}}$ ist. Man beachte, dass $a^2 + b^2 \neq 0$, weil a und b reelle Zahlen sind, die nicht beide verschwinden.

Dieser Körper heißt der *Körper der komplexen Zahlen*. Er enthält die reellen Zahlen als »Teilkörper«, das bedeutet: $\mathbb{R} \to \mathbb{C}$, $a \mapsto (a, 0)$, ist eine injektive Abbildung, die mit Addition und Multiplikation in $\mathbb{R}$ bzw. $\mathbb{C}$ verträglich ist, d.h. es gilt

$$(a + b, 0) = (a, 0) + (b, 0), \quad (ab, 0) = (a, 0)(b, 0).$$

Mittels dieser Injektion identifizieren wir üblicherweise $\mathbb{R}$ mit seinem Bild in $\mathbb{C}$ und schreiben einfach a statt $(a, 0)$. Hier benutzen wir den Begriff Teilkörper in einer Situation, die

ein kleines bisschen allgemeiner ist als Definition 4.4, weil $\mathbb{R}$ streng genommen keine Teilmenge von $\mathbb{C}$ ist, sondern wir nur eine injektive Abbildung $\mathbb{R} \to \mathbb{C}$ fixieren; diese kleine Ungenauigkeit wollen wir uns an dieser Stelle erlauben.

Das Element $(0,1)$, das oft mit i bezeichnet wird, hat die Eigenschaft

$$(0,1)^2 = (0,1) \cdot (0,1) = (-1,0) = -1,$$

sein Quadrat ist -1. In $\mathbb{C}$ besitzt die quadratische Gleichung $x^2 + 1 = 0$ (anders als in $\mathbb{R}$) also eine Lösung, genauer die beiden Lösungen i und $-i$. Es ist nicht sehr schwer zu zeigen, dass alle quadratischen Gleichungen mit Koeffizienten in $\mathbb{C}$ auch eine Lösung in $\mathbb{C}$ besitzen. Es gilt sogar der *Fundamentalsatz der Algebra*: Jedes nicht-konstante Polynom mit Koeffizienten in $\mathbb{C}$ besitzt eine Nullstelle in $\mathbb{C}$.

Es gilt $(a,b) = a + ib$, und meist schreibt man komplexe Zahlen in dieser Form. Man nennt dann a den *Realteil* und b den *Imaginärteil* der komplexen Zahl $a + ib$.

Wir kratzen hier, in der linearen Algebra, nur an der Oberfläche der komplexen Zahlen. Sie spielen sowohl in der Analysis, speziell in der sogenannten *Funktionentheorie*, der Theorie komplex-differenzierbarer Funktionen, eine herausragende Rolle, sind aber beispielsweise auch in der Algebra und der algebraischen Geometrie sehr wichtig.

Ausführliches Video[a] über die »Basics« der komplexen Zahlen von G. Sanderson/3Blue1Brown (auf Englisch).

[a] `https://www.youtube.com/watch?v=5PcpBw5Hbwo`

Für die Praxis ist es für Sie erstmal am wichtigsten, dass Sie wissen, wie Sie mit komplexen Zahlen rechnen. Und das ist ganz einfach: Man benutzt das Distributivgesetz, das Rechnen mit reellen Zahlen, und die Tatsache, dass $i^2 = -1$. Dann braucht man sich die Definitionen von Addition und Multiplikation in der obigen Form gar nicht zu merken. Zum Beispiel:

$$(3 + 2i)(-1 - 2i) = -3 - 6i - 2i + 4i^2 = -7 - 8i,$$

und um einen Bruch von komplexen Zahlen zu vereinfachen, erweitert man so, dass man im Nenner die dritte binomische Formel anwenden kann:

$$\frac{1+i}{2-2i} = \frac{(1+i)(2+2i)}{(2-2i)(2+2i)} = \frac{2+2i+2i+2i^2}{4-4i^2} = \frac{4i}{8} = \frac{1}{2}i.$$

Probieren Sie es selbst aus![a]

[a] `https://math.ug/applets/komplexe-zahlen.html`

◊

Beispiel 4.6. (1) Da jeder Körper ein Nullelement und ein Einselement besitzt und diese nach Definition verschieden sein müssen, hat jeder Körper mindestens zwei Elemente. Es ist nicht schwer zu sehen, dass es genau einen Körper mit zwei Elementen gibt. Dieser wird mit $\mathbb{F}_2$ bezeichnet.

Als Menge ist $\mathbb{F}_2 = \{0,1\}$ (Achtung! Diese sind das Nullelement und das Einselement des Körpers $\mathbb{F}_2$, nicht (zum Beispiel) das Nullelement und das Einselement des Körpers $\mathbb{Q}$. Während es nicht so wichtig ist, die 0 und 1 von $\mathbb{Q}$ bzw. $\mathbb{R}$ zu unterscheiden – da es für die Addition und Multiplikation rationaler Zahlen unerheblich ist, ob wir sie als rationale oder als reelle Zahlen auffassen, ist diese Unterscheidung hier essenziell. Es kann ja zum Beispiel im Körper $\mathbb{F}_2$ nicht $1 + 1 = 2$ gelten, da 2 gar kein Element dieses Körpers ist!)

Um zu sehen, dass es tatsächlich die Möglichkeit gibt, auf $\mathbb{F}_2 = \{0, 1\}$ eine Addition und Multiplikation zu definieren, so dass die Körperaxiome erfüllt sind, überlegt man sich zunächst, dass nur die folgende Möglichkeit in Frage kommt:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Die Tabellen sind dabei folgendermaßen zu lesen: Die Summe $a + b$ von Elementen $a, b \in \mathbb{F}_2$ steht in der linken Tabelle in der Zeile zum Element a und der Spalte zum Element b. Zum Beispiel ist $1 + 0 = 1$, $1 + 1 = 0$. Entsprechend sind in der rechten Tabelle alle Produkte von zwei Elementen eingetragen. Es ist dann (etwas langweilig, aber) nicht schwer, die Körperaxiome nachzuprüfen.

Der Körper $\mathbb{F}_2$ ist kein Teilkörper von $\mathbb{Q}$, denn (selbst wenn man die Menge $\mathbb{F}_2 = \{0, 1\}$ als Teilmenge von $\mathbb{Q}$ auffassen könnte): in $\mathbb{F}_2$ gilt $1 + 1 = 0$, aber in $\mathbb{Q}$ ist das nicht richtig.

Zwar ist die ganze Zahl 2 kein Element von $\mathbb{F}_2$, es ist aber eine nützliche Sichtweise, in jedem Körper K neben 0 und 1 auch Elemente $2_K, 3_3, \ldots$ zu definieren, und zwar als $2_K := 1 + 1$, $3_K = 1 + 1 + 1$, usw. (Und meist schreibt man dann wieder einfach 2, 3, usw. statt 2_K, 3_K. Wenn man Missverständnisse befürchtet, kann man 2_K, 3_K schreiben, oder schreibt speziell im Fall von $\mathbb{F}_2$ auch $\overline{2}$, $\overline{3}$, …, oder manchmal $[2]$, $[3]$, dots für diese Elemente.) In diesem Sinne gilt dann im Körper $\mathbb{F}_2$ die Gleichheit $2 = 0$. Siehe Abschnitt 4.2.2.)

(2) In ähnlicher Weise kann man einen Körper mit genau 3 Elementen konstruieren, für die wir hier die Bezeichnungen 0, 1, 2 wählen wollen, und dieser wird mit $\mathbb{F}_3$bezeichnet.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Im Körper $\mathbb{F}_3$ gilt also $(3 :=) 1 + 1 + 1 = 0$ und $2 = -1$.

Wie im Fall von $\mathbb{F}_2$ kann man auch hier die Körperaxiome direkt nachprüfen, allerdings ist es noch aufwändiger. Siehe Abschnitt 4.2.1 für eine bessere und gleichzeitig allgemeinere Lösung.

(3) Es gibt keinen Körper mit genau 6 Elementen.

Für den Fall von 6 Elementen kann man das mit ein bisschen Mühe direkt einsehen, indem man nachprüft, dass es keine Möglichkeit gibt, eine Additions- und eine Multiplikationstabelle wie oben für eine sechselementige Menge aufzustellen, die mit den Körperaxiomen verträglich ist.

Allgemeiner können Sie in der Algebra-Vorlesung lernen, dass die Anzahl der Elemente eines Körpers entweder unendlich oder die Potenz einer Primzahl ist (siehe auch Ergänzung 6.51), und dass es zu jeder Primzahlpotenz q genau einen Körper mit q Elementen gibt.

(4) Die Verknüpfung $(a, b) \mapsto a - b$ auf den rationalen Zahlen erfüllt weder das Assoziativgesetz noch das Kommutativgesetz (geben Sie dafür Beispiele!). Finden Sie weitere Verknüpfungen, die einige der Forderungen aus der Definition eines Körpers nicht erfüllen.

$\Diamond$

Das nächste Lemma zeigt, dass es ausreichen würde, in den Körperaxiomen die Existenz neutraler Elemente für Addition und Multiplikation zu fordern, da diese automatisch eindeutig bestimmt wären. Da die Axiome über die Existenz von Inversen aber auf die neutralen

Elemente Bezug nehmen müssen, haben wir die Eindeutigkeit in unsere Definition aufgenommen. Außerdem sehen wir, dass die inversen Elemente jeweils eindeutig bestimmt sind.

LEMMA 4.7. (1) *In der Situation von Definition 4.1 sind die neutralen Elemente der Addition und der Multiplikation in K notwendigerweise eindeutig bestimmt, auch wenn dies nicht gefordert würde.*

(2) *Für jedes $a \in K$ ist das additive inverse Element eindeutig bestimmt. Für jedes $a \in K^\times$ ist das multiplikative Inverse eindeutig bestimmt.*

BEWEIS. zu (1). Seien e, e' Elemente von K, die beide die Eigenschaft eines neutralen Elements der Addition haben. Wir zeigen, dass dann $e = e'$ gelten muss; das beweist die behauptete Eindeutigkeit. In der Tat gilt

$$e = e + e' = e',$$

wobei wir bei der ersten Gleichheit benutzen, dass e' ein neutrales Element bezüglich $+$ ist, und bei der zweiten Gleichheit die entsprechende Eigenschaft für e ausnutzen.

Analog können wir für die Multiplikation argumentieren. Haben $e, e' \in K$ beide die Eigenschaft eines neutralen Elements bezüglich der Multiplikation, so folgt

$$e = e \cdot e' = e'.$$

zu (2). Sei nun $a \in K$ und seien $b, b' \in K$ inverse Elemente von a bezüglich der Addition, d.h. es gelte $a + b = b + a = 0$, $a + b' = 0$. Wir erhalten dann

$$b = b + 0 = b + (a + b') = (b + a) + b' = 0 + b' = b'.$$

Die Rechnung zur Eindeutigkeit der multiplikativen Inversen verläuft analog. □

4.1.3. Rechenregeln. Sei K ein Körper, und seien $a, b, c, \ldots$ Elemente von K.

Kürzungsregeln. Aus $a + c = b + c$ folgt $a = b$, denn wir können auf beiden Seiten $-c$ addieren und erhalten $a = a + (c - c) = (a + c) - c = (b + c) - c = b$.

Ist $c \neq 0$, so folgt aus $ac = bc$ mit einem analogen Argument, dass $a = b$, da c ein multiplikatives Inverses besitzt.

Multiplikation mit 0. Es gilt $0 \cdot a = 0$. In der Tat gilt $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, und die Behauptung folgt, indem wir auf beiden Seiten $0 \cdot a$ abziehen (mit anderen Worten: das Negative des Elements $0 \cdot a$ addieren).

Weitere Rechenregeln Es gilt $-(-a) = a$. Warum?

Es gilt $(-1) \cdot a = -a$. In der Tat, $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$, und das bedeutet, dass $(-1) \cdot a$ die charakterisierende Eigenschaft des Negativen von a erfüllt.

Insbesondere folgt $(-1) \cdot (-1) = -(-1) = 1$, und daher auch $(-a) \cdot (-b) = ab$ für alle a, b.

BEMERKUNG 4.8. Beachten Sie, dass wir in einem allgemeinen Körper keinen Begriff von positiven und negativen Elementen haben. Nicht nur haben wir diese Begriffe nicht in unsere Definition aufgenommen – es gibt Körper, in denen sie sich nicht sinnvoll (also mit den erwarteten Eigenschaften) definieren lassen. Im Körper der komplexen Zahlen gibt es ein Element i mit $i \cdot i = -1$. (Auch in $\mathbb{F}_2$ gibt es ein Element mit dieser Eigenschaft.) Aus den üblichen Eigenschaften der Begriffe *positiv* und *negativ* würde aber folgen, dass Quadratzahlen immer positiv (oder Null) sind, und dass -1 negativ ist. Das lässt sich nicht mit der Gleichheit $i^2 = -1$ in Einklang bringen. ◊

Nullteilerfreiheit. Gilt $ab = 0$, so folgt $a = 0$ oder $b = 0$. Denn wenn $a \neq 0$ ist, dann können wir die beiden Seiten der Gleichung $ab = 0$ mit a^{-1} multiplizieren und erhalten $b = 0$. (Oder äquivalent umformuliert: Sind $a, b \in K^\times$, so ist $ab \neq 0$, also $ab \in K^\times$.)

Summen und Produkte mit mehr als zwei Elementen. Die Assoziativgesetze zeigen auch, dass man auch in Summen und Produkten von mehr als drei Elementen die Klammern nach Belieben setzen kann, ohne das Ergebnis zu verändern, zum Beispiel:

$$(a + b) + (c + (d + e)) = a + (b + ((c + d) + e)).$$

Daher können und werden wir es uns üblicherweise erlauben, die Klammern in solchen Ausdrücken wegzulassen. (Wenn mehrere Rechenoperationen in einem Ausdruck vorkommen, soll wie gesagt *Punkt- vor Strichrechnung* gelten, d.h. $\cdot$ und $/$ haben Priorität vor $+$ und $-$. Operatoren aus der gleichen Klasse (also $+, -$ einerseits und $\cdot, /$ andererseits) verarbeiten wir von links nach rechts.

Wir können in beliebigen Körpern die Summennotation $\sum_{i=1}^{n} a_i$ und die Produktnotation $\prod_{i=1}^{n} a_i$ anwenden, und wegen des Kommutativgesetzes sogar Summen (und analog Produkte) der Form $\sum_{i \in I} a_i$ für endliche Mengen I und Familien $(a_i)_{i \in I}$ betrachten.

Ergänzung 4.9 (Schiefkörper).

Definition 4.10. Ein *Schiefkörper* ist eine Menge D zusammen mit Verknüpfungen $+: D \times D \to D, \cdot: D \times D \to D$, für die alle Körperaxiome bis auf möglicherweise die Kommutativität der Multiplikation erfüllt sind. ⊣

Wie beim Begriff des Erweiterungskörpers kann man auch hier die Situation betrachten, dass ein Körper K und ein Schiefkörper D gegeben sind, so dass $K \subset D$ eine Teilmenge ist und dass die Addition und Multiplikation auf D für Elemente von K dieselben Ergebnisse liefert wie Addition und Multiplikation auf D. Gilt zusätzlich noch $xy = yx$ für alle $x \in K$ und $y \in D$, dann nennt man D eine (assoziative) *Divisionsalgebra* über K. (In der Regel fordert man auch noch, dass D als K-Vektorraum von endlicher Dimension ist. Der Dimensionsbegriff wird uns aber erst später zur Verfügung stehen.)

Es ist ein interessantes Problem zu verstehen, welche Divisionsalgebren es über einem gegebenen Körper gibt. Ein Beispiel werden wir in der folgenden Ergänzung 4.11 kennenlernen.

Siehe auch Ergänzungen 6.59, 11.14. □ Ergänzung 4.9

Ergänzung 4.11 (Die Hamiltonschen Quaternionen). Wir definieren auf $\mathbb{H} := \mathbb{R}^4 = \{(a, b, c, d);\ a, b, c, d \in \mathbb{R}\}$ eine Addition durch

$$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d').$$

Die Multiplikation definieren wir durch

$$(a, b, c, d) \cdot (a', b', c', d') =$$
$$(aa' - bb' - cc' - dd', ab' + ba' + cd' - dc', ac' - bd' + ca' + db', ad' + bc' - cb' + da').$$

Man kann zeigen, dass $\mathbb{H}$ mit diesen Operationen einen Schiefkörper bildet. Das neutrale Element der Addition ist $0 = (0, 0, 0, 0)$, das neutrale Element der Multiplikation ist $1 = (1, 0, 0, 0)$. Dass die Addition alle geforderten Eigenschaften hat, ist klar.

Wenn wir $\mathbb{R}$ mittels der Einbettung $\mathbb{R} \to \mathbb{H}, a \mapsto (a, 0, 0, 0)$, mit der Teilmenge $\{(a, 0, 0, 0);\ a \in \mathbb{R}\}$ identifizieren, dann ist $\mathbb{H}$ sogar eine Divisionsalgebra über $\mathbb{R}$, genannt die Algebra der Hamiltonschen Quaternionen.

Wir können sogar mit $a + bi \mapsto (a, b, 0, 0)$ die komplexen Zahlen $\mathbb{C}$ als Teilkörper in $\mathbb{H}$ einbetten. Dann wird $i \in \mathbb{C}$ auf das Element $(0, 1, 0, 0) \in \mathbb{H}$ abgebildet, das man wieder mit i

bezeichnet. Außerdem setzt man oft $j := (0,0,1,0)$ und $k := (0,0,0,1)$. Die oben angegebene Multiplikation ist die eindeutig bestimmte Verknüpfung, die $\mathbb{H}$ zu einem Schiefkörper macht, so dass $(a,0,0,0)(a',b',c',d') = (aa',ab',ac',ad')$, und dass

$$i^2 = j^2 = k^2 = ijk = -1$$

gilt. So einfach das auch aussieht – Hamilton hat jahrelang darüber nachgedacht, wie man eine Divisionsalgebra über $\mathbb{R}$ konstruieren könnte, bis ihm die Idee für die hier angegebene Multiplikation kam. Siehe Ergänzung 4.9.

Wir sehen, dass nicht $xy = yx$ für alle $x \in \mathbb{C}$ und $y \in \mathbb{H}$ gilt, zum Beispiel ist

$$ij = 1 = -ji.$$

Es ist nicht sehr angenehm, die Schiefkörperaxiome anhand der hier gegebenen Formeln zu überprüfen, und es gibt bessere Methoden, wie wir in Kürze sehen werden (Ergänzung 5.64).

Siehe auch Ergänzung 8.7. □ Ergänzung 4.11

> One of the big misapprehensions about mathematics that we perpetrate in our classrooms is that the teacher always seems to know the answer to any problem that is discussed. This gives students the idea that there is a book somewhere with all the right answers to all of the interesting questions, and that teachers know those answers. And if one could get hold of the book, one would have everything settled. That's so unlike the true nature of mathematics.
>
> L. Henkin
> in: Steen, Albers (eds.), *Teaching Teachers, Teaching Students*, Birkhäuser, 1981.
>
> Gefunden auf http://math.furman.edu/~mwoodard/mqs/data.html

4.2. Endliche Körper

4.2.1. Rechnen mit Restklassen. Sei $n \geq 1$ eine natürliche Zahl. Wir betrachten die Menge

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

mit n Elementen, die wir mit den Symbolen $\overline{a}$ für a in den natürlichen Zahlen von 0 bis $n-1$ bezeichnen. (Die Wahl der Bezeichnung – $\mathbb{Z}/n$ – wird im zweiten Semester noch klarer werden. Andere übliche Bezeichnungen sind $\mathbb{Z}/(n)$ und $\mathbb{Z}/n\mathbb{Z}$.)

Wir nennen die Elemente von $\mathbb{Z}/n$ auch *Restklassen* (*modulo n*).

Wir definieren die folgenden Verknüpfungen:

$$a + b := \overline{r}, \text{ wobei } r \text{ der Rest von } a + b \text{ bei Division durch } n \text{ ist,}$$
$$a \cdot b := \overline{r}, \text{ wobei } r \text{ der Rest von } a \cdot b \text{ bei Division durch } n \text{ ist.}$$

Wie üblich lassen wir den Multiplikationspunkt $\cdot$ manchmal weg. Es ist klar, dass sowohl für $+$ als auch für $\cdot$ das Kommutativgesetz gilt.

BEISPIEL 4.12. (1) Für $n = 12$ erhalten wir zum Beispiel

$$\overline{9} + \overline{6} = \overline{3}.$$

(Wie beim »Rechnen« auf der Uhr: 6 Stunden nach 9 Uhr ist es 3 Uhr, denn ab 12 beginnt die Zählung wieder bei 1.)

(2) Es gilt für $n = 17$:

$$\overline{3} \cdot \overline{6} = \overline{1} \quad \text{in } \mathbb{Z}/17 \ .$$

(3) Für alle n, und alle $a \in \mathbb{Z}/n$ gilt $\overline{0} + a = a$, also ist $\overline{0}$ ein neutrales Element für $+$. Es gilt $\overline{0} \cdot a = \overline{0}$. Ferner gilt $\overline{1} \cdot a = a$, also ist $\overline{1}$ ein neutrales Element für $\cdot$.

(4) Sei $n = 2$. Dann ist $\overline{1} + \overline{1} = \overline{0}$, und wir sehen, dass die Operationen $+$ und $\cdot$ auf $\mathbb{Z}/2$ gerade die Addition und Multiplikation liefern, die wir auf $\mathbb{F}_2$ definiert haben.

(5) Sei $n = 3$. In diesem Fall kann man $\mathbb{Z}/3$ mit den Operationen $+$ und $\cdot$ mit dem Körper $(\mathbb{F}_3, +, \cdot)$ identifizieren.

$\Diamond$

Wir bezeichnen mit $\pi\colon \mathbb{Z} \to \mathbb{Z}/n$ die Abbildung, die $x \in \mathbb{Z}$ abbildet auf $\overline{r}$, wobei r der Rest von x bei Division durch n ist. Diese Abbildung nennt man manchmal die *kanonische Projektion*. Offenbar handelt es sich um eine surjektive Abbildung. Natürlich ist π nicht injektiv; es gilt genau dann $\pi(a) = \pi(b)$, wenn a und b denselben Rest bei Division durch n haben, oder äquivalent ausgedrückt: wenn $a - b$ durch n teilbar ist. Insbesondere gilt $\pi(a) = 0$ genau dann, wenn a ein Vielfaches von n ist.

Sehr nützlich ist, dass die Abbildung π mit den Additionen und Multiplikationen auf beiden Seiten verträglich ist, und zwar im folgenden Sinne:

Erstens können wir die Definition der Addition und Multiplikation auf $\mathbb{Z}/n$ auch schreiben als

$$a + b = \pi(a + b), \quad a \cdot b = \pi(ab), \quad a, b \in \mathbb{Z}/n \ . \tag{1}$$

Zweitens gilt:

LEMMA 4.13. *Seien $x, x' \in \mathbb{Z}$. Dann gilt*

$$\pi(x + x') = \pi(x) + \pi(x'), \quad \pi(xx') = \pi(x) \cdot \pi(x').$$

BEWEIS. Wir schreiben die Division durch n mit Rest aus als

$$x = qn + r, \quad x' = q'n + r', \quad 0 \le r, r' < n.$$

Es gilt also $\pi(x) = r, \pi(x') = r'$.

Es ist eine offensichtliche Eigenschaft der Division mit Rest durch n, dass sich der Rest nicht ändert, wenn wir den Dividenden (die Zahl, die durch n geteilt wird) um ein Vielfaches von n abändern.

Also gilt

$$\pi(x) + \pi(x') = \pi(r + r') = \pi(x + x'),$$

wobei die erste Gleichheit aus (1) folgt, und die zweite, weil sich x und r, beziehungsweise x' und r' nur um Vielfache von n unterscheiden.

Weil $xx' = (qq'n + qr' + q'r)n + rr'$ sich ebenfalls um ein Vielfaches von n von rr' unterscheidet, können wir für $\cdot$ ganz analog rechnen:

$$\pi(x) \cdot \pi(x') = \pi(rr') = \pi(xx').$$

$\square$

Dieses Lemma erlaubt es uns, ohne weiteren Aufwand zu zeigen, dass die Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}/n$ assoziativ und kommutativ sind und dass das Distributivgesetz gilt. Seien nämlich $x, y, z \in \mathbb{Z}/n$, und seien $\dot{x}, \dot{y}, \dot{z} \in \mathbb{Z}$ mit $\pi(\dot{x}) = x$, $\pi(\dot{y}) = y$, $\pi(\dot{z}) = z$ (wir könnten x, y, z als Elemente von $\mathbb{Z}$ auffassen und $\dot{x} = x$ usw. wählen, aber es ist für das Weitere egal; wichtig ist nur, dass so eine Wahl überhaupt möglich ist, d.h. dass π surjektiv ist).

Dann gilt zum Beispiel

$$\begin{aligned}(x+y)+z &= (\pi(\dot{x})+\pi(\dot{y}))+\pi(\dot{z}) = \pi(\dot{x}+\dot{y})+\pi(\dot{z}) = \pi((\dot{x}+\dot{y})+\dot{z}) \\ &= \pi(\dot{x}+(\dot{y}+\dot{z})) = \pi(\dot{x})+\pi(\dot{y}+\dot{z}) = x+(\pi(\dot{y})+\pi(\dot{z})) = x+(y+z).\end{aligned}$$

Diese Gleichungskette ist zwar lang, aber die einzelnen Schritte sind ganz formal. Wir benutzen mehrfach das Lemma, und in der Mitte dann das Assoziativgesetz für die Addition in $\mathbb{Z}$. Wenn wir alle $+$-Zeichen in dieser Rechnung durch $\cdot$ ersetzen, dann ergibt sich ein Beweis des Assoziativgesetzes der Multiplikation. Die beiden Kommutativgesetze und das Distributivgesetz können nach exakt dem gleichen Schema bewiesen werden.

Wir haben oben schon festgestellt, dass $\overline{0} \in \mathbb{Z}/n$ ein neutrales Element bezüglich $+$ und $\overline{1} \in \mathbb{Z}/n$ ein neutrales Element bezüglich $\cdot$ ist. Für $a \in \mathbb{Z}$ ist $\pi(-a)$ ein additives Inverses von $\pi(a)$, denn

$$\pi(a)+\pi(-a) = \pi(a+(-a)) = \overline{0}.$$

Das einzige Axiom, das aus der Liste der Körperaxiome noch fehlt, ist die Existenz von multiplikativen Inversen. Hier zeigt sich eine interessante Situation:

- Anders als in $\mathbb{Z}$ haben manchmal auch Elemente $\neq \overline{1}$ (und $\neq -\overline{1}$) ein multiplikatives Inverses. Wir hatten beispielsweise oben schon festgehalten, dass in $\mathbb{Z}/17$ gilt, dass $\overline{3}\cdot\overline{6} = \overline{1}$. Wir haben auch schon gesehen, dass $\mathbb{Z}/2$ der Körper $\mathbb{F}_2$ und $\mathbb{Z}/3$ der Körper $\mathbb{F}_3$ ist.
- Im allgemeinen ist $\mathbb{Z}/n$ kein Körper; zum Beispiel gilt in $\mathbb{Z}/6$: $\overline{2} \neq \overline{0}$, $\overline{3} \neq \overline{0}$, aber $\overline{2}\cdot\overline{3} = \overline{0}$. Diese Beobachtung können wir leicht verallgemeinern: Wenn $n = ab$ mit $0 < a, b < n$ gilt, dann gilt $\overline{a}\overline{b} = \overline{0}$ in $\mathbb{Z}/n$, obwohl $\overline{a} \neq \overline{0}$ und $\overline{b} \neq \overline{0}$ ist. Also ist $\mathbb{Z}/n$ kein Körper.

Der zweite Punkt zeigt uns, dass $\mathbb{Z}/n$ höchstens dann ein Körper sein kann, wenn n eine Primzahl (vergleiche Ergänzung 3.44) ist. Wir wollen nun zeigen, dass wir für eine Primzahl p tatsächlich einen Körper $\mathbb{Z}/p$ konstruiert haben.

Dafür benutzen wir die *Primeigenschaft*: Ist p eine Primzahl und ist p ein Teiler des Produkts ab von zwei ganzen Zahlen a, b, so ist p ein Teiler von a oder von b (wie immer ist auch erlaubt, dass p beide Zahlen a und b teilt). Siehe Satz 3.52 in Ergänzung 3.51 für einen Beweis. Wir wollen uns, für den Fall, dass Sie diese Ergänzung ausgelassen haben, auf die Bemerkung beschränken, dass diese Eigenschaft aus der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ folgt. Denn die (eindeutige!) Primfaktorzerlegung des Produktes ab erhalten wir, indem wir die Primfaktorzerlegungen von a und von b zusammenfügen (miteinander multiplizieren), und wenn p als Faktor in dem Produkt auftritt, muss es folglich auch in einem der Faktoren dabei sein.

SATZ 4.14. *Sei p eine Primzahl. Dann ist $\mathbb{Z}/p$ ein Körper.*

BEWEIS. Nach dem bereits Gesagten ist nur noch zu zeigen, dass jedes Element $a \in (\mathbb{Z}/p) \setminus \{\overline{0}\}$ ein multiplikatives Inverses besitzt. Sicher genügt es dafür, zu beweisen, dass die Abbildung

$$m_a\colon \mathbb{Z}/p \to \mathbb{Z}/p\,, \quad x \mapsto a\cdot x,$$

surjektiv ist, denn $m_a(x) = \overline{1}$ besagt ja gerade $a \cdot x = \overline{1}$; dann ist x das gesuchte Inverse.

Weil $\mathbb{Z}/p$ eine endliche Menge ist, ist es äquivalent zu zeigen, dass m_a injektiv ist (Satz 3.64).

Das bedeutet, wir müssen zeigen, dass für $x \neq y \in \mathbb{Z}/p$ stets $ax \neq ay$, oder mit anderen Worten $a(x-y) \neq \overline{0}$ gilt. Wir schreiben $a = \pi(\dot{a}), x = \pi(\dot{x}), y = \pi(\dot{y})$ für geeignete ganze Zahlen $\dot{a}, \dot{x}, \dot{y}$. Dann können wir umformulieren: Dass $a \neq \overline{0}$ ist, ist gleichbedeutend damit, dass $p \nmid \dot{a}$, ebenso bedeutet $x \neq y$, dass $p \nmid \dot{x} - \dot{y}$. Wegen der oben bemerkten Primeigenschaft erhalten wir daraus, dass p kein Teiler des Produkts $\dot{a}(\dot{x} - \dot{y})$ ist. Folglich ist $a(x-y) = \pi(\dot{a})(\pi(\dot{x}) - \pi(\dot{y})) = \pi(\dot{a}(\dot{x} - \dot{y})) \neq \overline{0}$, wie gewünscht. □

ERGÄNZUNG 4.15. Wir geben noch einen alternativen Beweis dafür, dass $\mathbb{Z}/p$ für Primzahlen p ein Körper ist. Dieser beruht auf Lemma 3.53 aus Ergänzung 3.51. (Wir haben dieses Lemma benutzt, um die Eindeutigkeit der Primfaktorzerlegung zu beweisen; insofern hängt auch der erste Beweis für die Körpereigenschaft von $\mathbb{Z}/p$ bei unserem Aufbau der Dinge von Lemma 3.53 ab. Man kann aber die Primeigenschaft, und damit die Eindeutigkeit der Primfaktorzerlegung auch (etwas) anders beweisen.)

SATZ 4.16. *Sei $n > 1$ eine natürliche Zahl, und sei $a \in \mathbb{Z}$. Genau dann besitzt $\pi(a)$ ein multiplikatives Inverses in $\mathbb{Z}/n$, wenn* $\operatorname{ggT}(a, n) = 1$.

BEWEIS. Sei $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, n) = 1$. Nach Lemma 3.53 existieren dann $x, y \in \mathbb{Z}$ mit

$$1 = xa + yn.$$

Das bedeutet aber

$$\pi(x) \cdot a = \pi(xa) = \pi(1 - yp) = \pi(1) + \pi(-yp) = \pi(1) = \overline{1},$$

also ist $\pi(x)$ das gesuchte Inverse von a.

Hat andererseits $\pi(a)$ ein multiplikatives Inverses, so können wir dieses in der Form $\pi(b)$ für $b \in \mathbb{Z}$ schreiben. Dass das Produkt $\pi(a)\pi(b) = \overline{1}$ ist (in $\mathbb{Z}/n$), bedeutet genau, dass $1 - ab$ von n geteilt wird. Ist also d ein gemeinsamer Teiler von a und n, so muss d auch 1 teilen, also $d \in \{-1, 1\}$. □

KOROLLAR 4.17. *Sei p eine Primzahl. Dann ist $\mathbb{Z}/p$ ein Körper.*

BEWEIS. Sei $a \in \mathbb{Z}/p$, $a \neq \overline{0}$. Wir schreiben $a = \pi(\dot{a})$ für eine ganze Zahl $\dot{a}$. Weil $a \neq \overline{0}$, wird $\dot{a}$ nicht von p geteilt, und weil p eine Primzahl ist, folgt $\operatorname{ggT}(\dot{a}, p) = 1$. Daher können wir den vorherigen Satz anwenden. □

(Wir erhalten so auch einen (etwas) anderen Beweis von Satz 3.52: Der Satz sagt, dass wenn immer die Primzahl p ein Produkt ab teilt, p einen der Faktoren teilt. In der Tat, $p \mid ab$ bedeutet $\pi(a)\pi(b) = \pi(ab) = \overline{0}$, und da $\mathbb{Z}/p$ ein Körper ist, gilt dann $\pi(a) = \overline{0}$ oder $\pi(b) = \overline{0}$. Das bedeutet gerade $p \mid a$ oder $p \mid b$.) □ Ergänzung 4.15

Für eine Primzahl p schreiben wir statt $\mathbb{Z}/p$ oft auch $\mathbb{F}_p$, um zu betonen, dass es sich hierbei um einen Körper handelt.

(Wenn Sie Lust haben, ist jetzt ein guter Zeitpunkt, sich den Sternchen-Abschnitt 3.13.2 über Äquivalenzrelationen anzuschauen, und dort speziell das Beispiel über $\mathbb{Z}/3$.)

Zum Schluss noch einige gebräuchliche Schreibweisen: Oft schreibt man $\overline{a}$ statt $\pi(a)$ für beliebige ganze Zahlen a. Für $0 \leq a < n - 1$ fällt das mit der oben verwendeten Schreibweise zusammen. Manchmal schreibt man auch $[a]$ statt $\overline{a}$.

Wenn keine Missverständnisse zu befürchten sind (oder die Autor*in entscheidet, der Leser*in zuzumuten, das selbst (gedanklich) »aufzuräumen«), dann kann man auch einfach a statt $\overline{a}$ schreiben.

Eine andere übliche Schreibweise ist es, statt $\pi(x) = \pi(y)$ (für $x, y \in \mathbb{Z}$ und ein fixiertes n)

$$x \equiv y \mod n$$

zu schreiben (gesprochen »x ist *kongruent zu y modulo n*«). Wie oben erläutert ist das äquivalent dazu zu sagen, dass $x - y$ von n geteilt wird.

Die Schreibweise, statt $\bar{a}$ einfach a zu schreiben, kann man im Rahmen der folgenden allgemeinen Konvention sehen: Sei K ein beliebiger Körper. Für eine natürliche Zahl n schreiben wir n_K, oder einfach n, wenn klar ist, dass wir n als Element von K betrachten möchten, für das Element

$$n_K := 1 + \cdots + 1 \quad (n \text{ Summanden})$$

von K. Zum Beispiel gilt (für die übliche Einbettung der Menge der natürlichen Zahlen in den Körper $\mathbb{Q}$) $n_{\mathbb{Q}} = n$ für alle natürlichen Zahlen n. Andererseits gilt $2_{\mathbb{F}_2} = 0_{\mathbb{F}_2}$ und allgemeiner $n_{\mathbb{F}_2} = 0_{\mathbb{F}_2}$ für alle geraden, und $n_{\mathbb{F}_2} = 1_{\mathbb{F}_2}$ für alle ungeraden natürlichen Zahlen n. Man sagt auch, in $\mathbb{F}_2$ gelte $2 = 0$, $3 = 1$, etc.

Man erweitert diese Definition auf alle ganzen Zahlen, indem man $(-n)_K := -n_K$ für natürliche Zahlen n setzt. Dann ist n_K für alle ganzen Zahlen n definiert. Hier ist $-n_K$ das Negative in K des Elements n_K.

4.2.2. Die Charakteristik eines Körpers *. In diesem Abschnitt untersuchen wir das Phänomen, dass in manchen Körpern der Ausdruck $1 + \cdots + 1$ gleich 0 ist, etwas genauer. Zum Beispiel gilt in $\mathbb{F}_2$, dass $1 + 1 = 0$, und in $\mathbb{F}_p$, dass $1 + \cdots 1 = 0$ (mit p Summanden auf der linken Seite).

Wir verwenden weiter die am Ende des vorherigen Abschnitts eingeführte Schreibweise n_K für $n \in \mathbb{Z}$. Wie gesagt, werden wir später dazu übergehen, einfach n statt n_K zu schreiben, aber für den Moment bleiben wir bei dem Index $-_K$ zur besseren Unterscheidung.

Wir können also von der Abbildung $\varphi\colon \mathbb{Z} \to K$, $n \mapsto n_K$ sprechen. Es folgt leicht aus der Definition von n_K, dass $\varphi(m + n) = \varphi(m) + \varphi(n)$ gilt, wobei auf der linken Seite $+$ die Addition in $\mathbb{Z}$, und auf der rechten Seite $+$ die Addition in K bezeichnet. (Überlegen Sie sich, dass das auch hinkommt, wenn m und/oder n negativ sind.) Darüberhinaus gilt auch $\varphi(mn) = \varphi(m)\varphi(n)$, wobei wieder links in $\mathbb{Z}$ und rechts in K multipliziert wird. Das zeigt man zuerst für nicht-negative m und n, indem man m und n als Summen von m bzw. n Summanden 1 schreibt und das Distributivgesetz ausnutzt. Aus $\varphi(-m) = -\varphi(m)$ kann man das Ergebnis dann in der allgemeinen Form herleiten.

Definition 4.18. Sei K ein Körper. Wenn es eine natürliche Zahl $n \geq 1$ gibt, so dass $n_K = 0$, also

$$1 + \cdots + 1 = 0$$

in K gilt (mit n Summanden auf der linken Seite), so nennen wir die kleinste solche Zahl $n \geq 1$ die *Charakteristik* von K.

Gibt es kein solches n, so sagen wir, K habe die Charakteristik 0. ⊣

Da in jedem Körper per Definition die Elemente 0 und 1 verschieden sind, kann ein Körper nicht die Charakteristik 1 haben. Es gilt sogar die folgende viel stärkere Einschränkung:

Satz 4.19. *Sei K ein Körper der Charakteristik $p \neq 0$. Dann ist p eine Primzahl.*

Beweis. Sei K ein Körper mit Charakteristik $p \neq 0$. Wir haben bereits bemerkt, dass $p > 1$ gelten muss. Angenommen, p ließe sich als Produkt zweier Zahlen $m, n > 1$ zerlegen. Wir könnten dann p_K (oder mit der oben eingeführten Notation $\varphi(p)$ schreiben als

$$p_K = \varphi(p) = \varphi(mn) = \varphi(m)\varphi(n) = m_K n_K,$$

was bedeutet, dass $m_K = 0$ oder $n_K = 0$ gelten muss. Das steht im Widerspruch zur Minimalität von p in der Definition der Charakteristik. □

BEISPIEL 4.20. Die Charakteristik von $\mathbb{Q}$ ist 0, ebenso die Charakteristik von jedem Erweiterungskörper von $\mathbb{Q}$, insbesondere also von $\mathbb{R}$ und $\mathbb{C}$.

Ist p eine Primzahl, so ist die Charakteristik von $\mathbb{F}_p$ gleich p. In der Tat folgt aus der Definition von $\mathbb{F}_p$ als Menge von Restklassen modulo p, dass $p_{\mathbb{F}_p} = 0$, aber $n_{\mathbb{F}_p} \neq 0$ für alle $n = 1, \ldots, p-1$.

Es gibt für jede Primzahl p noch weitere Körper der Charakteristik, sowohl endliche mit mehr als p Elementen, als auch unendliche. Da in einem Körper K der Charakteristik 0 die Elemente n_K, $n \in \mathbb{Z}$, alle verschieden sind, gibt es aber keine endlichen Körper der Charakteristik 0. ◊

4.2.3. Der Kleine Fermatsche Satz *. Wir kommen noch einmal auf die endlichen Körper zurück und beginnen mit der folgenden simplen Beobachtung:

$$\begin{aligned} 2^7 - 2 &= 128 - 2 = 126 = 7 \cdot 18, \\ 3^7 - 3 &= 2\,187 - 3 = 2\,184 = 7 \cdot 312, \\ 4^{13} - 4 &= 67\,108\,860 = 13 \cdot 5\,162\,220. \end{aligned}$$

In allen Beispielen ist der Ausdruck $a^n - a$ durch n teilbar. (Siehe auch Beispiel 3.36.) Das funktioniert aber nicht immer:

$$2^9 - 2 = 512 - 2 = 510$$

ist nicht durch 9 teilbar.

Der strukturelle Unterschied zwischen diesen Beispielen ist, dass im ersten Fall der Exponent immer eine Primzahl war. In der Tat gilt:

SATZ 4.21 (Kleiner Fermatscher Satz). *Sei p eine Primzahl und $a \in \mathbb{Z}$ irgendeine ganze Zahl. Dann ist $a^p - a$ durch p teilbar.*

BEWEIS. Wenn wir $K = \mathbb{F}_p$ schreiben, dann können wir die Aussage umformulieren als

$$(a^p - a)_K = 0.$$

Es gilt aber $(a^p - a)_K = (a_K)^p - a_K$, also genügt es zu zeigen, dass für alle Elemente $x \in \mathbb{F}_p$ gilt: $x^p = x$.

Für $x = 0$ ist das klar. Sei also nun $x \neq 0$. Betrachte die Multiplikation mit x als Abbildung $\xi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times : y \mapsto xy$. Diese Abbildung ist injektiv, weil $x \neq 0$ und $\mathbb{F}_p$ ein Körper ist. Weil $\mathbb{F}_p^\times$ nur endlich viele Elemente hat, ist sie automatisch sogar bijektiv.

Das bedeutet, dass das Produkt aller Bilder $\xi(y), y \in \mathbb{F}_p^\times$, unter der Abbildung ξ mit dem Produkt aller $y \in \mathbb{F}_p^\times$ übereinstimmt, denn die Faktoren sind ja bis auf die Reihenfolge genau dieselben:

$$x^{p-1} \cdot (1 \cdot \cdots \cdot (p-1)) = (x \cdot 1) \cdot (x \cdot 2) \cdot \cdots \cdot (x(p-1)) = 1 \cdot \cdots \cdot (p-1).$$

Die rechte Seite ist wieder in $\mathbb{F}_p^\times$, also $\neq 0$, und wir können durch sie teilen. Wir erhalten damit

$$x^{p-1} = 1,$$

also $x^p = x$, wie gewünscht. □

BEMERKUNG 4.22. Eine kleine Verfeinerung dieses Satzes ist ein wichtiger Bestandteil des RSA-Verfahrens[3], eines der wichtigsten Public-Key-Verfahren, also Verschlüsselungsverfahren, bei denen Absender und Empfänger verschlüsselt kommunizieren können, ohne vorher einen geheimen Schlüssel auszutauschen. Stattdessen kann der Empfänger den Schlüssel, den der Absender zum Verschlüsseln benutzt, öffentlich machen (public key), ohne dass Außenstehende die Möglichkeit hätten, den öffentlichen Schlüssel zum Entschlüsseln zu verwenden.

Ausgangsbasis für alle solchen Public-Key-Verfahren ist eine mathematische Operation, die vergleichsweise schnell berechenbar und eindeutig umkehrbar ist, für die aber die Berechnung der Umkehroperation einen wesentlich höheren Rechenaufwand erfordert. Im Falle des RSA-Verfahrens benutzt man, dass es leicht ist, große Primzahlen zu finden und das Produkt zweier solcher Primzahlen zu berechnen, dass aber kein Verfahren bekannt ist, um in annehmbarer Zeit die Zerlegung eines solchen Produkts in seine Primfaktoren zu bestimmen. Konkret würde man zum Beispiel mit zwei Primzahlen beginnen, die jeweils etwa 1 000 Stellen haben. Mittelfristig könnte die Entwicklung leistungsstarker Quantencomputer allerdings eine Möglichkeit darstellen, auch Produkte dieser Größenordnung in ihre Primfaktoren zu zerlegen, so dass das Verfahren dann als geknackt gelten müsste (siehe Shor-Algorithmus[4]). ◊

BEMERKUNG 4.23. Der Kleine Fermatsche Satz ist eine Möglichkeit zu testen, ob eine (große) Zahl n eine Primzahl ist. Man nimmt eine Zahl a und rechnet aus, ob $a^n - a$ durch n teilbar ist. Diese Rechnung lässt sich *wesentlich* schneller durchführen, als die Zahl n in ihre Primfaktoren zu zerlegen. Wenn $a^n - a$ nicht durch n teilbar ist, dann kann n keine Primzahl sein. Wenn für mehrere Zahlen a die Zahl $a^n - a$ durch n teilbar ist, dann ist die Wahrscheinlichkeit hoch, dass n eine Primzahl ist.

In der Praxis benutzt man etwas ausgefeiltere Tests, die aber oft letztlich auf dem Kleinen Fermatschen Satz beruhen, zum Beispiel den Miller-Rabin-Test[5]. Diese Tests sind in der Regel probabilistischer Natur, d.h. sie liefern mit einer verschwindend geringen Wahrscheinlichkeit ein falsches Ergebnis. Das nimmt man in der Praxis dann in Kauf.

Um eine große Primzahl (sagen wir mit mehreren hundert Stellen) zu finden, wie sie zum Beispiel für manche Verschlüsselungsverfahren benötigt wird, probiert man dann einfach so lange zufällig gewählte große Zahlen durch, bis man eine findet, die den zugrunde gelegten Primzahltest besteht. ◊

4.3. Polynomfunktionen

4.3.1. Summe und Produkt von Abbildungen in einen Körper. Sei K ein Körper. Wir bezeichnen mit $\mathrm{Abb}(X, K)$ die Menge aller Abbildungen $X \to K$. Indem wir die Addition und Multiplikation auf K benutzen, können wir die Summe und das Produkt von zwei Abbildungen $f, g \in \mathrm{Abb}(X, K)$ definieren:

$$f + g \colon X \to K, \quad x \mapsto f(x) + g(x),$$

und

$$f \cdot g \colon X \to K, \quad x \mapsto f(x)g(x).$$

Wir erhalten so eine Addition $+$ und eine Multiplikation $\cdot$ auf $\mathrm{Abb}(X, K)$.

Zwar ist $\mathrm{Abb}(X, K)$ kein Körper (es sei denn, X hat genau ein Element), aber das soll uns an dieser Stelle nicht stören.

[3] https://de.wikipedia.org/wiki/RSA-Kryptosystem
[4] https://de.wikipedia.org/wiki/Shor-Algorithmus
[5] https://de.wikipedia.org/wiki/Miller-Rabin-Test

4.3.2. Polynomfunktionen auf einem Körper.

Sei K weiter ein Körper.

DEFINITION 4.24. Eine Abbildung $f\colon K \to K$ heißt *Polynomfunktion*, wenn eine natürliche Zahl $n \geq 0$ und Elemente $a_i \in K$, $i = 0, \ldots, n$, existieren, so dass für alle $x \in K$ gilt:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i.$$

⊣

Die Elemente a_i nennt man die *Koeffizienten* von f. (Aber siehe Bemerkung 4.29: Ist K endlich, so sind die Koeffizienten einer solchen Darstellung nicht eindeutig durch die Abbildung f bestimmt!) Der Koeffizient a_0 heißt der *Absolutterm* oder das *absolute Glied*. Dies ist gleichzeitig der Wert von f an der Stelle 0: $f(0) = a_0$.

Es ist oft nützlich, den Fall, dass f die konstante Funktion mit Wert 0 ist, separat zu behandeln. Wenn wir diesen Fall ausschließen, brauchen wir nur noch Polynomfunktionen zu betrachten, bei denen mindestens ein Koeffizient $\neq 0$ ist. Dann können wir auch direkt annehmen, dass der Koeffizient mit dem höchsten Index nicht verschwindet, weil wir die Terme mit verschwindenden Koeffizienten weglassen können.

Ist $f\colon K \to K$ eine Abbildung, dann nennen wir die Elemente a von K mit $f(a) = 0$ die *Nullstellen* der Funktion f. Eine einfache aber wichtige Beobachtung ist die folgende: Ist f das Produkt von Polynomfunktionen $g, h\colon K \to K$ (im Sinne von Abschnitt 4.3.1, das heißt also einfach, dass $f(x) = g(x)h(x)$ für alle $x \in K$ gilt), dann ist f wieder eine Polynomfunktion, und für $a \in K$ gilt $f(a) = 0$ genau dann, wenn $g(a) = 0$ oder $h(a) = 0$ ist.

SATZ 4.25. *Sei $f\colon K \to K$ eine Polynomfunktion. Gilt*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i.$$

(siehe Definition 4.24) und sind nicht alle $a_i = 0$, dann gibt es höchstens n verschiedene Nullstellen von f in K.

Zumindest in Spezialfällen ist Ihnen der Satz bekannt; zum Beispiel kann eine quadratische Gleichung nicht mehr als zwei Lösungen haben. In diesem Semester werden die Polynomfunktionen keine zentrale Rolle spielen, sondern nur gelegentlich als Beispielmaterial dienen. Das wird sich in der Linearen Algebra 2 ändern und wir werden dann noch einmal systematischer auf diesen Begriff zurückkommen. Daher können Sie, wenn Sie möchten, den Beweis des Satzes erstmal überspringen.

BEWEIS. Ähnlich wie wir die Division mit Rest für ganze Zahlen haben, können wir auch Polynomfunktionen (für die wir eine Darstellung wie in der Definition gewählt haben) mit Rest durcheinander dividieren. Wir nennen das Polynomdivision.

LEMMA 4.26 (Polynomdivision). *Seien f, g Polynomfunktionen mit $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ und es gelte $a_n \neq 0$, $b_m \neq 0$ und $0 < m \leq n$. Dann existieren eine Polynomfunktion q mit $q(x) = \sum_{i=0}^{n-m} c_i x^i$ und eine Polynomfunktion r mit $r(x) = \sum_{i=0}^{l} d_i x^i$, so dass*

$$f = qg + r, \qquad \text{und } l < m.$$

(Die erste Bedingung ist im Sinne von Abschnitt 4.3.1; sie bedeutet einfach, dass $f(x) = q(x)g(x) + r(x)$ für alle $x \in K$. Es wird nicht behauptet, dass $c_{n-m} \neq 0$ sein muss.)

BEWEIS DES LEMMAS. Wir führen Induktion nach n. Ist $n < m$, so können wir einfach $r(x) := f(x) = \sum_{i=0}^{n} a_i x^i$ und $q = 0$ setzen.

Ist $n \geq m$, so sei $q_1(x) = \frac{a_n}{b_m} x^{n-m}$ und $f_1 = f - q_1 g$, also gilt für alle $x \in K$:

$$f_1(x) = f(x) - q_1(x)g(x) = \sum_{i=0}^{n} a_i x^i - \frac{a_n}{b_m} x^{n-m} \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{n-1} \left(a_i - \frac{a_n b_{i-n+m}}{b_m} \right) x^i,$$

wobei wir für $j < 0$ den Wert von b_j als 0 ansehen wollen. Wir können daher auf diese Darstellung von f_1 die Induktionsvoraussetzung anwenden und $f_1 = q_2 g + r$ schreiben, wobei die höchste Potenz von x, die in r auftritt, kleiner als m ist. Wir erhalten dann

$$f = f_1 + q_1 g = (q_1 + q_2)g + r,$$

und setzen $q := q_1 + q_2$, um die gewünschte Darstellung von f zu erhalten. □

Nun zum Beweis des Satzes. Wir führen Induktion nach n. Ist $n = 0$, also $f = a_0$, so hat f gar keine Nullstellen, weil nach Voraussetzung nicht alle a_i (und das ist hier nur a_0) Null sein dürfen.

Sei nun $n > 0$. Wir können annehmen, dass $a_n \neq 0$ ist, denn sonst könnten wir den Term $a_n x^n$ einfach weglassen und ein noch besseres Ergebnis beweisen. Sei a eine Nullstelle von f. (Sollte f gar keine Nullstellen haben, ist die Aussage sowieso klar.) Wir wenden das Lemma über die Polynomdivision an auf das gegebene f und $g(x) = x - a$. Das bedeutet $m = 1$, also können wir f schreiben als $f = qg + r$ mit $r(x) = d_0$ (denn die Zahl l im Lemma muss < 1 sein).

Wir haben also $f(x) = q(x)(x-a) + d_0$ für alle $x \in K$. Wenn wir $x = a$ setzen, dann bekommen wir

$$0 = f(a) = q(a)(a - a) + d_0 = d_0,$$

also gilt $d_0 = 0$ und damit $f(x) = q(x)(x - a)$. Nun gibt uns das Lemma auch, dass $q(x) = \sum_{i=0}^{n-1} c_i x^i$. Nach Induktionsvoraussetzung hat q höchstens $n - 1$ Nullstellen in K. Ist b irgendeine Nullstelle von f, so gilt $q(b)(b - a) = f(b) = 0$, also ist $b = a$ oder $q(b) = 0$. Insgesamt folgt die Behauptung. □

Natürlich kann f wie im Satz auch weniger als n Nullstellen haben, betrachten Sie zum Beispiel die Funktion $f\colon \mathbb{R} \to \mathbb{R}, f(x) = x^2 + 1$, oder allgemein die Funktion $f\colon K \to K$, $f(x) = x^n$, die 0 als einzige Nullstelle hat.

BEISPIEL 4.27. Sei $K = \mathbb{Q}$ und $f(x) = x^3 - 3x^2 + 3x - 2$. Wir sehen, dass f bei $x = 2$ eine Nullstelle hat. (Man kann zeigen, dass die Nullstellen in $\mathbb{Q}$ eines Polynoms mit Koeffizienten in $\mathbb{Z}$ und höchstem Koeffizient 1 alle in $\mathbb{Z}$ liegen und den Absolutterm teilen; in diesem Fall kommen also nur die Teiler von -2, d.h. $-2, -1, 1, 2$, als Nullstellen *in* $\mathbb{Q}$ in Frage. Natürlich kann es weitere Nullstellen in $\mathbb{R} \setminus \mathbb{Q}$, oder auch in $\mathbb{C} \setminus \mathbb{Q}$, geben. Auch in diesem Beispiel gibt es nur eine rationale Nullstelle und zwei reelle Nullstellen, die nicht in $\mathbb{Q}$ liegen.)

Wir führen die Polynomdivision von f durch $x - 2$ durch:

$$\begin{array}{rrrr|l}
(x^3 & -3x^2 & +3x & -2) & : \quad (x-2) \quad = \quad x^2 - x + 1 \\
-x^3 & +2x^2 & & & \\
\hline
 & -x^2 & +3x & -2 & \\
 & +x^2 & -2x & & \\
\hline
 & & x & -2 & \\
 & & -x & +2 & \\
\hline
 & & & 0 &
\end{array}$$

(Das Vorgehen ist hier nicht so leicht zu illustrieren; versuchen Sie, die obige Rechnung schrittweise wie eine schriftliche Division zu lesen. Mit den unteren Zeilen ergeben sich nach und nach die Summanden des Ergebnisses.)

Wie im Beweis des Satzes bleibt in diesem Fall kein Rest. Die weiteren Nullstellen von f können wir nun ausrechnen, indem wir die quadratische Gleichung $x^2 - x + 1 = 0$ lösen. ◊

KOROLLAR 4.28. *Sei K ein unendlicher Körper. Sei f eine Polynomfunktion auf K, die nicht konstant 0 ist. Dann sind die Zahlen n und a_i in der Darstellung $f(x) = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$ eindeutig bestimmt.*

BEWEIS. Sind $f(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n'} a'_i x^i$ Darstellungen von f, so ist die Differenz

$$\sum_i (a_i - a'_i) x^i$$

eine Polynomfunktion, die an jedem Element von K verschwindet, also unendlich viele Nullstellen hat. Ihre Koeffizienten müssen also sämtlich verschwinden. □

Ist K ein unendlicher Körper, so nennen wir die Zahl n aus Korollar **??** den Grad der Polynomfunktion. (Der Nullfunktion weisen wir formal den Grad $-\infty$ zu.)

BEMERKUNG 4.29. Ist K ein endlicher Körper, so kann eine Polynomfunktion f konstant $= 0$ sein, also $f(x) = 0$ für alle $x \in K$, und dennoch eine Darstellung $f(x) = \sum_{i=0}^{n} a_i x^i$ haben, in der nicht alle a_i verschwinden. Die Aussage von Korollar 4.28 ist in diesem Fall falsch. Zum Beispiel ist für $K = \mathbb{F}_p$ die Polynomfunktion $f(x) = x^p - x$ die Nullfunktion; dies ist gerade die Aussage des Kleinen Fermatschen Satzes (Satz 4.21). Wir kommen in der Linearen Algebra 2 auf diesen Punkt noch einmal zurück. ◊

KAPITEL 5

Lineare Gleichungssysteme und Matrizen

5.1. Lineare Gleichungssysteme

5.1.1. Definitionen. Wir halten im gesamten Abschnitt einen Körper K fest. Im Kontext der linearen Gleichungssysteme ist es nützlich, Elemente von K^n, also n-Tupel von Elementen von K, nicht wie üblich als Tupel $(x_1, ..., x_n)$ zu schreiben, sondern in einer Spalte:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Das von vorneherein so zu tun, erspart uns eine spätere Umstellung der Notation (und damit mögliche Verwirrung beim späteren Zurückblättern). Die Begründung für diese Konvention liegt im Formalismus des Matrizenprodukts, das wir in Abschnitt 5.3 kennenlernen werden.

Da diese *Spaltenvektoren* allerdings im Text sehr viel Platz wegnehmen, wollen wir stattdessen die Notation $(x_1, ..., x_n)^t$ verwenden, wo das kleine t (» transponiert«) bedeuten soll, dass wir uns dieses Tupel als Spalte denken.

(Eine pragmatische Lösung wäre, einfach das ^{t} zu ignorieren, bis Sie zu Bemerkung 5.36 im Abschnitt 5.3 kommen.)

Definition 5.1. Sei K ein Körper, seien m, n natürliche Zahlen. Ein *lineares Gleichungssystem (LGS)* von m Gleichungen in n Unbestimmten $X_1, ..., X_n$ über K ist gegeben durch m Gleichungen

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n &= b_2 \\ \vdots \qquad\qquad & \qquad \vdots \\ a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n &= b_m \end{aligned}$$

mit $a_{ij} \in K$ für alle $i = 1, ..., m, j = 1, ..., n, b_i \in K, i = 1, ..., m$.

Ein lineares Gleichungssystem heißt *homogenes* lineares Gleichungssystem, falls $b_i = 0$ für alle $i = 1, ..., m$. Sonst heißt das lineare Gleichungssystem *inhomogen*.

Wir schreiben kurz, das obige lineare Gleichungssystem sei gegeben durch die Elemente (a_{ij}, b_i) von K.

Die Elemente a_{ij} von K heißen auch die *Koeffizienten* des linearen Gleichungssystems. Genauer ist a_{ij} der Koeffizient von X_j in der i-ten Gleichung des Gleichungssystems. Ein Element $(x_1, ..., x_n)^t$ von K^n heißt *Lösungsvektor* des linearen Gleichungssystems, wenn nach Einsetzen von x_i für X_i (für alle i) alle m Gleichungen erfüllt sind.

Die *Lösungsmenge* $\mathbb{L}$ des linearen Gleichungssystems ist die Menge aller Lösungsvektoren, also die Menge aller n-Tupel $(x_1, ..., x_n)^t \in K^n$, so dass für alle $i = 1, ..., m$ gilt:

$$a_{i1}x_1 + a_{i2}x_2 \cdots + a_{1n}x_i = b_i.$$

Sei ein lineares Gleichungssystem M gegeben durch (a_{ij}, b_i). Das lineare Gleichungssystem M_0, das gegeben ist durch $(a_{ij}, 0)$, d.h. die Koeffizienten a_{ij} werden beibehalten, aber alle b_i werden durch 0 ersetzt, heißt das *zu M gehörige homogene lineare Gleichungssystem*.

Das Wort »linear« bezieht sich hier darauf, dass die Unbestimmten alle nur in der ersten Potenz auftreten (keine Quadrate oder höheren Potenzen und keine Produkte von Unbestimmten). Geometrisch gesehen ist die Lösungsmenge einer Gleichung der Form $aX_1 + bX_2 = c$ über den reellen Zahlen eine Gerade in $\mathbb{R}^2$, und auch in allgemeineren Fällen sind, wie sich zeigen wird, die Lösungsmengen linearer Gleichungssysteme »lineare Objekte«.

Wir nennen ein lineares Gleichungssystem *lösbar*, wenn die Lösungsmenge nicht leer ist, d.h. wenn es überhaupt einen Lösungsvektor gibt. Sonst heißt das System *unlösbar*. Gibt es genau einen Lösungsvektor, d.h. hat die Lösungsmenge genau ein Element, dann sprechen wir von einem *eindeutig lösbaren* System.

Jedes homogene lineare Gleichungssystem ist lösbar, denn $(0, \ldots, 0)^t$ ist ein Lösungsvektor. Diese Lösung wird auch die *triviale Lösung* genannt. Umgekehrt gilt: Wenn ein lineares Gleichungssystem $(0, \ldots, 0)^t$ als Lösungsvektor hat, dann muss es ein homogenes Gleichungssystem sein.

BEISPIEL 5.2. Sei $K = \mathbb{R}$. Wir betrachten als Beispiel das folgende Gleichungssystem:

$$\begin{aligned} 2X_1 - 2X_2 &= 3 \\ X_1 + 2X_2 &= 3 \end{aligned}$$

Addieren wir die beiden Gleichungen, so sehen wir, dass $3X_1 = 6$, also $X_1 = 2$ gelten muss. Durch Einsetzen in die zweite Gleichung bekommen wir dann $X_2 = \frac{1}{2}$, und man sieht direkt, dass dies tatsächlich eine Lösung des Gleichungssystems ist: Die Lösungsmenge ist

$$\left\{ \left(2, \frac{1}{2}\right)^t \right\}.$$

Vergleiche auch Abschnitt 2.5.

Wenn wir $\mathbb{R}^2$ als die Zahlenebene sehen, dann können wir jede Teilmenge als eine Menge von Punkten in dieser Ebene betrachten. Zum Beispiel ist die Menge

$$\{(x_1, x_2);\ 2x_1 - 2x_2 = 3\}$$

eine Gerade in $\mathbb{R}^2$, siehe die Abbildung.

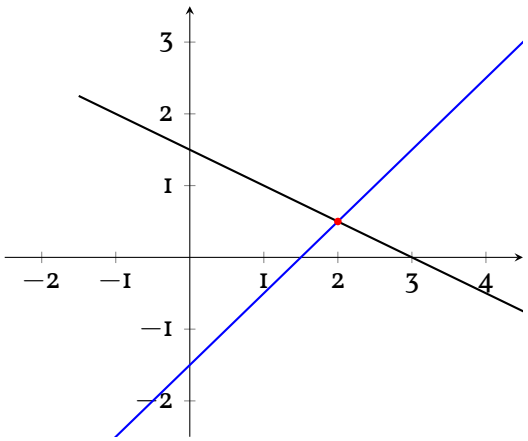
In ähnlicher Weise ist

$$\{(x_1, x_2);\ x_1 + 2x_2 = 3\}$$

eine Gerade. Und die Lösungsmenge des obigen Gleichungssystems ist einfach die Schnittmenge dieser beiden Geraden.
Das ist auch allgemeiner richtig, dann für alle $a_1, a_2, b \in \mathbb{R}$ ist

$$\{(x_1, x_2);\ a_1x_1 + a_2x_2 = b\}$$

eine Gerade – es sei denn es ist $a_1 = a_2 = 0$; dann ist diese Menge entweder gleich $\mathbb{R}^2$ (wenn $b = 0$) oder leer (wenn $b \neq 0$).



Da zwei Geraden in $\mathbb{R}^2$ entweder gleich sind oder sich in höchstens einem Punkt schneiden, sehen wir, dass es kein lineares Gleichungssystem mit 2 Gleichungen und 2 Unbestimmten

über $\mathbb{R}$ gibt, das mehr als eine, aber nur endlich viele Lösungen hat. (Wie ist es mit mehr Gleichungen/Unbestimmten? Über anderen Körpern? – Später wird es uns leicht fallen, diese Fragen zu beantworten, zum Teil können Sie es vielleicht jetzt schon?) ◊

In ähnlicher Weise wie im vorherigen Beispiel können wie die Lösungsmengen von linearen Gleichungssystemen in $\mathbb{R}^3$ als Durchschnitte von Ebenen betrachten (und, wenn Ihre Anschauung das mitmacht, kann man die Situation auch für mehr als 3 Unbestimmte ähnlich sehen.)

5.1.2. Addition und Skalarmultiplikation auf K^n. Um die Struktur der Lösungsmengen besser zu verstehen, ist es hilfreich, auch auf der Menge K^n Rechenoperationen einzuführen, und zwar eine Addition und eine »Skalarmultiplikation« (also Multiplikation mit Elementen des Körpers K, die auch als *Skalare* bezeichnet werden).

DEFINITION 5.3. Für $(x_1, ..., x_n)^t, (y_1, ..., y_n)^t \in K^n$ definieren wir die Summe

$$(x_1, ..., x_n)^t + (y_1, ..., y_n)^t := (x_1 + y_1, ..., x_n + y_n)^t,$$

und für $a \in K$ das *Produkt* von a mit $(x_1, ..., x_n)^t$ durch

$$a \cdot (x_1, ..., x_n)^t := (ax_1, ..., ax_n)^t.$$

⊣

BEISPIEL 5.4. (1) Ist $K = \mathbb{C}$, so ist zum Beispiel

$$i\begin{pmatrix} 1 \\ 1+i \end{pmatrix} + \begin{pmatrix} i \\ 1-i \end{pmatrix} = \begin{pmatrix} 2i \\ 0 \end{pmatrix}.$$

(2) Ist $K = \mathbb{F}_7$, dann ist zum Beispiel

$$2\begin{pmatrix} 5 \\ 2 \end{pmatrix} + \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

◊

Wir nennen die Elemente von K^n auch *Vektoren*. Da die Addition separat in den einzelnen Komponenten erfolgt, ist klar, dass das Assoziativgesetz und das Kommutativgesetz gelten, und dass der sogenannte *Nullvektor* $(0, ...0)^t$ ein neutrales Element für die Addition ist (und zwar das einzige). Wir bezeichnen den Nullvektor meist einfach mit 0 (und damit bleibt der Leser∗in die Aufgabe überlassen festzustellen, welches Objekt mit dem Symbol 0 eigentlich gerade gemeint ist). Ist $x = (x_1, ..., x_n)^t \in K^n$, so ist $-x := (-x_1, ..., -x_n) = (-1) \cdot x$ das inverse Element von x bezüglich der Addition. Natürlich stellt sich nicht die Frage, ob es sich bei K^n für $n > 1$ um einen Körper handelt, weil wir keine Multiplikation $K^n \times K^n \to K^n$ definiert haben. Immerhin ist klar, dass eine Art Assoziativgesetz gilt, das heißt $a(bx) = (ab)x$ für $a, b \in K, x \in K^n$.

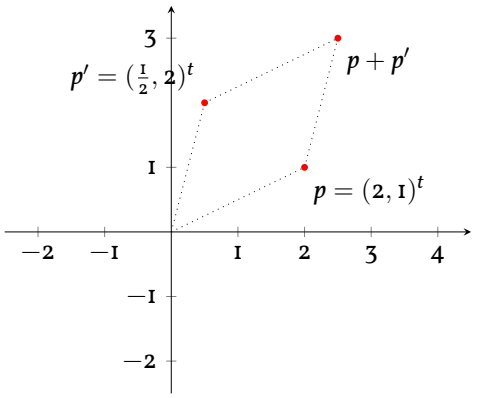
BEMERKUNG 5.5. Die Addition und Skalarmultiplikation in $\mathbb{R}^2$ können wir geometrisch veranschaulichen, vergleiche die Abbildungen: Für $p, p' \in \mathbb{R}^2$ sind $0, p, p'$ und $p + p'$ die vier Eckpunkte eines Parallelogramms.

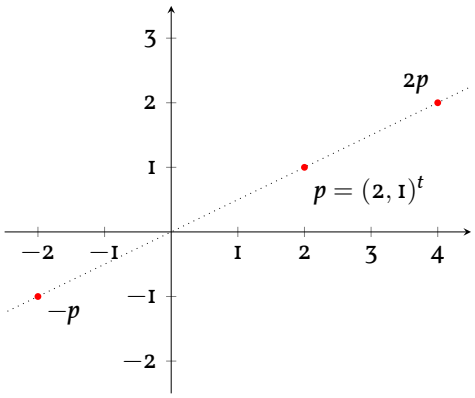
Für $p \in \mathbb{R}^2 \setminus \{0\}$ liegen alle Punkte $ap, a \in \mathbb{R}$ auf der Geraden durch den Ursprung $(0, 0)^t$ und p.

Selber ausprobieren[a].

[a] https://math.ug/applets/R2.html

Die Definition der Addition und Skalarmultiplikation sind also der erste Schritt, »mit Punkten zu rechnen«, und damit der Beginn der analytischen Geometrie (siehe Kapitel 12).





Im Prinzip gelten dieselben Beschreibungen in $\mathbb{R}^3$ und allgemein in $\mathbb{R}^n$, allerdings ist es dann weniger leicht, dies an Abbildungen zu illustrieren. ◊

5.1.3. Matrizen. Es ist praktisch, die Koeffizienten eines linearen Gleichungssystems zu »organisieren«, ohne dass wir immer alle Unbestimmten mit ausschreiben müssen (wie wir di Unbestimmten nennen, spielt ja ohnehin keine Rolle). Dafür führen wir den Begriff der Matrix ein. Im Moment ist das eine reine Organisationshilfe für uns, später werden wir allerdings viele, teilweise auch tiefliegendere, Anwendungen sehen, wo Matrizen sehr nützlich sind.

DEFINITION 5.6 (Matrix). Seien m, n natürliche Zahlen. Unter einer *Matrix* der Größe $m \times n$ mit Einträgen in K (man spricht auch von einer $(m \times n)$-Matrix über K) verstehen wir eine Familie $(a_{ij})_{i=1,\dots,m, j=1,\dots,n}$ von Elementen von K. Die Elemente a_{ij} heißen die *Einträge* oder *Koeffizienten* der Matrix. Eine Matrix stellen wir uns immer in der Form

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

vor, d.h. wir schreiben die Koeffizenten in einem rechteckigen Schema auf, in dem der erste Index die Zeile und der zweite Index die Spalte angibt. In der linken oberen Ecke steht der Eintrag a_{11}, rechts daneben $a_{12}, \dots$, und in der i-ten Zeile und j-ten Spalte steht a_{ij}.

Die Menge aller $(m \times n)$-Matrizen über K bezeichnen wir mit $M_{m\times n}(K)$. Die Menge aller $(n \times n)$-Matrizen bezeichnen wir manchmal mit $M_n(K)$ statt mit $M_{n\times n}(K)$; wir sprechen auch von *quadratischen* Matrizen. ⊣

Formal betrachtet können wir eine Matrix als eine Abbildung $M\colon \{1, \dots, m\} \times \{1, \dots, n\} \to K$ definieren, dann ist a_{ij} in der obigen Definition der Wert $M(i, j)$. Rein formal können wir dann auch die Fälle erlauben, in denen $m = 0$, oder $n = 0$ oder $m = n = 0$ ist. Mit der Konvention $\{1, \dots, m\} = \emptyset$, falls $m = 0$ (und entsprechend für n) ist eine Matrix dann eine Abbildung $\emptyset \to K$, also gibt es in diesen Fällen genau eine Matrix (die »leere« Matrix der Größe $0 \times n$, $m \times 0$ oder 0×0). Die *Nullmatrix* (der Größe $m \times n$) ist die Matrix $0 \in M_{m\times n}(K)$, deren Einträge alle gleich Null sind. Es gibt also für jede Wahl von m und n eine Nullmatrix, und diese sind natürlich alle verschieden, da sie verschiedene Größen haben. Trotzdem schreibt man meist einfach 0 dafür, oder $0_{m\times n}$, wenn man die Größe mitangeben möchte. Wir können Elemente von K^n auch als Matrizen mit einer einzigen Spalte und n Zeilen betrachten: $K^n = M_{n\times 1}(K)$.

Gegeben ein lineares Gleichungssystem

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n &= b_2 \\ \vdots \qquad\qquad & \qquad \vdots \\ a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n &= b_m \end{aligned}$$

mit $a_{ij} \in K$ für alle $i = 1, \ldots, m, j = 1, \ldots, n, b_i \in K, i = 1, \ldots, m$, so bezeichnen wir die Matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{1m} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

als die *Koeffizientenmatrix* des linearen Gleichungssystems, und die Matrix

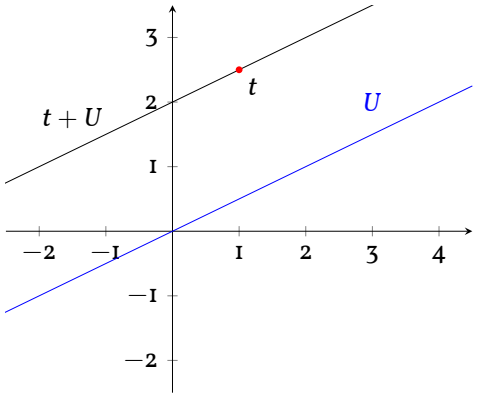
$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{1m} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

als die *erweiterte Koeffizientenmatrix* des linearen Gleichungssystems. (Der senkrechte Strich vor der letzten Spalte ist nur eine Erinnerung, dass diese Spalte von der rechten Seite der Gleichungen eines linearen Gleichungssystems herkommt, und hat, was die Matrix betrifft, keine mathematische Bedeutung.)

Wir führen für $t \in K^n$ und eine Teilmenge $U \subseteq K^n$ die folgende Schreibweise ein:

$$t + U := \{t + u;\ u \in U\}.$$

Beispiel 5.7. Ein Beispiel in $\mathbb{R}^2$, wo U die Gerade durch den Ursprung mit Steigung $\frac{1}{2}$ und t der Punkt $(1, \frac{5}{2})^t$ ist. ◊



Damit können wir formulieren, wie die Lösungsmenge eines linearen Gleichungssystems und die Lösungsmenge des zugehörigen homogenen linearen Gleichungssystems zusammenhängen.

Satz 5.8. *Seien K ein Körper, $A \in M_{m\times n}(K)$ und $b \in K^m$. Sei $\mathbb{L}$ die Lösungsmenge des linearen Gleichungssystems mit erweiterter Koeffizientenmatrix $(A \mid b)$, sei $\mathbb{L}_0$ die Lösungsmenge des zugehörigen homogenen linearen Gleichungssystems mit Koeffizientenmatrix A. Ist $t \in \mathbb{L}$, so gilt*

$$\mathbb{L} = t + \mathbb{L}_0.$$

Beweis. Dass x in $t + \mathbb{L}_0$ ist, ist äquivalent dazu, dass $x - t \in \mathbb{L}_0$ ist. Deshalb ist die behauptete Gleichheit von Mengen äquivalent zu der Behauptung

$$x \in \mathbb{L} \quad \Leftrightarrow \quad x - t \in \mathbb{L}_0$$

für alle $x = (x_1, \ldots, x_n)^t \in K^n$. Nun bedeutet $x \in \mathbb{L}$ gerade, dass für alle $i = 1, \ldots, m$ gilt:

$$\sum_{j=1}^{n} a_{ij}x_j = b_j,$$

und $x - t \in \mathbb{L}_0$ heißt, dass für alle i

$$\sum_{j=1}^{n} a_{ij}(x_j - t_j) = 0,$$

wobei wir mit t_j die Einträge des Vektors t bezeichnen. Nun ist nach Voraussetzung $t \in \mathbb{L}$, und deshalb gilt

$$\sum_{j=1}^{n} a_{ij}(x_j - t_j) = \sum_{j=1}^{n} a_{ij}x_j - \sum_{j=1}^{n} a_{ij}t_j = \sum_{j=1}^{n} a_{ij}x_j - b_j.$$

Die behauptete Äquivalenz ist damit klar. □

Es ist klar, dass die Lösungsmenge eines (inhomogenen) linearen Gleichungssystems leer sein kann. Dann existiert gar kein t wie im Satz, und der Satz liefert über diesen Fall keine Informationen.

Zum Schluss noch eine Sprechweise: Die Einträge a_{ii} einer quadratischen Matrix $A = (a_{ij})_{i,j}$ heißen die *Diagonaleinträge*. Die »Felder« mit Indizes $(1,1), (2,2), \ldots$ nennt man auch die (Haupt-)Diagonale einer Matrix. Die $(n \times n)$-Matrix, deren Diagonaleinträge alle gleich 1, und deren andere Einträge alle gleich 0 sind, heißt die Einheitsmatrix (der Größe n) und wird mit E_n bezeichnet.

$$E_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

5.2. Der Gauß-Algorithmus

5.2.1. Elementare Zeilenumformungen. Die Standardmethode, um die Lösungsmenge eines linearen Gleichungssystems zu bestimmen, ist der *Gauß-Algorithmus*. Das Ziel des Algorithmus ist es, ein gegebenes lineares Gleichungssystem durch Äquivalenzumformungen auf ein lineares Gleichungssystem möglichst einfacher Gestalt zu bringen, das dieselbe Lösungsmenge hat wie das ursprüngliche lineare Gleichungssystem.

Beispiel 5.9. Um das Ziel zu illustrieren, hier zwei Beispiele.

(1) Am einfachsten ist der Fall, dass die Koeffizientenmatrix des Gleichungssystems die Einheitsmatrix E_n ist (Einsen auf der Diagonale, Nullen überall sonst). Die Lösungsmenge des Gleichungssystems mit erweiterter Koeffizientenmatrix $(E_n \mid b)$ ist $\{b\}$.

(2) Eine ganz so einfache Form wie in Teil (1) werden wir nicht immer erreichen können (jedenfalls kann das ja nur für eindeutig lösbare Gleichungssysteme die richtige Lösungsmenge geben).

Betrachten wir als weiteres Beispiel das Gleichungssystem mit erweiterter Koeffizientenmatrix (mit Elementen a und b_i im fixierten Körper K)

$$\left(\begin{array}{ccc|c} 1 & a & 0 & b_1 \\ 0 & 0 & 1 & b_2 \\ 0 & 0 & 0 & b_3 \end{array}\right).$$

In diesem Fall ist es immer noch einfach, die Lösungsmenge abzulesen. Ist $b_3 \neq 0$, so ist die Lösungsmenge leer.

Sei nun $b_3 = 0$. Die dritte Zeile besteht dann sämtlich aus Nullen und ist als Gleichung gesehen die Gleichung $0 = 0$, die immer erfüllt ist. Die zweite Zeile besagt dann als Gleichung ausgeschrieben, dass $x_3 = b_2$. Die erste Zeile beschreibt die Gleichung $x_1 + ax_2 = b_1$, also $x_1 = b_1 - ax_2$. Das bedeutet, dass wir für jede Wahl von x_2 in K den

Lösungsvektor $(b_1 - ax_2, x_2, b_2)^t$ erhalten, und alle Lösungsvektoren entstehen auf diese Art und Weise. Die Lösungsmenge ist

$$\{(b_1 - ax_2, x_2, b_2)^t;\ x_2 \in K\}.$$

Auch in diesem Fall braucht man also nicht weiter zu rechnen, sondern kann die Lösungsmenge aus der erweiterten Koeffizientenmatrix direkt ablesen. Das streben wir auch im allgemeinen Fall an.

◊

Wir beginnen nun damit, die Umformungen zu beschreiben, die wir erlauben werden, um das gegebene lineare Gleichungssystem zu verändern. Danach überlegen wir uns, dass diese Umformungen die Lösungsmenge nicht verändern.

DEFINITION 5.10 (Elementare Zeilenumformungen eines LGS). Gegeben ein lineares Gleichungssystem, so nennen wir die folgenden Umformungen *elementare Zeilenumformungen vom Typ I, II bzw. III:*

(I) Addition eines Vielfachen (mit $a \in K$) einer Gleichung zu einer anderen Gleichung.

(II) Vertauschung zweier Gleichungen.

(III) Multiplikation einer Gleichung mit einem Skalar $a \in K^\times$.

⊣

In (I) kann man natürlich statt von der Addition des a-fachen auch von der Subtraktion des $(-a)$-fachen sprechen.

BEISPIEL 5.11. Betrachten Sie das folgende lineare Gleichungssystem über $\mathbb{Q}$:

$$\begin{aligned} X - Y &= 3 \\ -2X + 3Y &= 0 \end{aligned}$$

Wir führen eine Zeilenumformung vom Typ I durch und zwar addieren wir das 2-fache der ersten Zeile zur zweiten Zeile. Wir erhalten das Gleichungssystem

$$\begin{aligned} X - Y &= 3 \\ Y &= 6. \end{aligned}$$

◊

Analog haben wir den Begriff der elementaren Zeilenumformungen vom Typ I, II, III von Matrizen:

(I) Addition eines Vielfachen (mit $a \in K$) einer Zeile zu einer anderen Zeile.

(II) Vertauschung zweier Zeilen.

(III) Multiplikation einer Zeile mit einem Skalar $a \in K^\times$ (d.h. jeder Eintrag der Zeile wird mit a multipliziert).

Das bedeutet, dass eine elementare Zeilenumformung eines linearen Gleichungssystem genau der gleichen elementaren Zeilenumformung der erweiterten Koeffizientenmatrix entspricht.

(Entsprechend kann man auch von elementaren Spaltenumformungen von Matrizen sprechen. Das wird aber für uns erst später in der Vorlesung eine Rolle spielen.)

Wir benutzen für diese Zeilenumformungen die folgende Notation:

- Addition das a-fachen von Zeile j zu Zeile $i \neq j$: $Z_i \rightsquigarrow Z_i + aZ_j$,
- Vertauschen der Zeilen i und j: $Z_i \leftrightsquigarrow Z_j$,
- Multiplizieren von Zeile i mit $a \in K, a \neq 0$: $Z_i \rightsquigarrow aZ_i$.

Wenn ein lineares Gleichungssystem (oder analog eine Matrix) aus einer anderen Matrix durch eine elementare Zeilenumformung entsteht, dann kann man das ursprüngliche lineare Gleichungssystem (bzw. die ursprüngliche Matrix) durch eine elementare Zeilenumformung wieder zurückerhalten. Wir sagen deshalb, dass elementare Zeilenumformungen *umkehrbar* sind. In der Tat, entsteht A' aus A durch Addition des a-fachen von Zeile j zu Zeile i, so entsteht A aus A' durch Addition des $(-a)$-fachen von Zeile j zu Zeile i. Entsteht A' aus A durch Vertauschen der Zeilen i und j, so entsteht auch A aus A' durch Vertauschen dieser Zeilen. Entsteht schließlich A' aus A durch Multiplikation der i-ten Zeile mit $a \neq 0$, so entsteht A aus A' durch Multiplikation der i-ten Zeile mit a^{-1}. (Hier ist es wichtig, dass wir für Typ (III) nur Elemente $\neq 0$ in K als Faktoren erlauben.)

LEMMA 5.12. *Zwei lineare Gleichungssysteme, die durch elementare Zeilenumformungen auseinander hervorgehen, haben dieselbe Lösungsmenge.*

BEWEIS. Sei $(A \mid b)$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems, und gehe das lineare Gleichungssystem mit erweiterter Koeffizientenmatrix $(A' \mid b')$ daraus durch eine elementare Zeilenumformung hervor. Wegen der Umkehrbarkeit der Operationen genügt es zu zeigen, dass jede Lösung von $(A \mid b)$ auch eine Lösung von $(A' \mid b')$ ist. Das ist offensichtlich für Umformungen vom Typ (II) und (III). Für Zeilenumformungen vom Typ (I), etwa $Z_i \rightsquigarrow Z_i + aZ_j$, haben wir für ein Element $x = (x_1, \ldots, x_n)^t$ der Lösungsmenge des ursprünglichen Gleichungssystems die Ausgangssituation

$$\sum_{k=1}^{n} a_{ik}x_k = b_i, \quad \sum_{k=1}^{n} a_{jk}x_k = b_j,$$

und sehen, dass

$$\sum_{k=1}^{n}(a_{ik} + aa_{jk})x_k = \sum_{k=1}^{n} a_{ik}x_k + a\sum_{k=1}^{n} a_{jk}x_k = b_i + ab_j,$$

das bedeutet, dass x auch die neu erhaltene Gleichung erfüllt. (Wie man an der Rechnung sieht und wie auch direkt einsichtig ist, ist es natürlich wichtig, die Zeilenumformungen immer auch in der ganz rechten Spalte der erweiterten Koeffizientenmatrix anzuwenden.) □

5.2.2. Die Zeilenstufenform. Wir beschreiben als nächstes die spezielle Form von Matrizen, die wir mit dem Gauß-Algorithmus erreichen wollen. (Danach werden wir uns überlegen, dass man jede Matrix durch eine Folge von elementaren Zeilenumformungen auf diese Form bringen kann; das ist der eigentliche Gauß-Algorithmus.)

DEFINITION 5.13. Sei A eine Matrix mit m Zeilen und n Spalten.

(1) Wir sagen, die Matrix A habe *Zeilenstufenform*, wenn die folgenden Bedingungen erfüllt sind:
   (a) In jeder Zeile ist der erste Eintrag, der von Null verschieden ist, gleich 1. Diese erste Eins (von links gesehen), bezeichnen wir als die *führende Eins* der entsprechenden Zeile.
   (b) Alle Einträge in der Spalte einer führenden Eins, die unter der führenden Eins liegen, sind gleich Null.

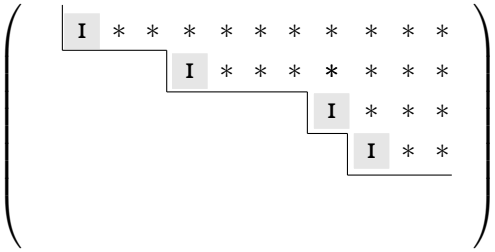
(c) Die führende Eins einer Zeile liegt rechts von der führenden Eins der darüberliegenden Zeile.

(Es ist in Teil (a) erlaubt, dass eine Zeile nur aus Nullen besteht. Wegen Teil (c) müssen dann aber auch alle darunterliegenden Zeilen sämtlich aus Nullen bestehen. »Gleiche Höhe« ist in Bedingung (c) nicht ausreichend, die führende Eins einer Zeile darf nicht in derselben Spalte sein wie die der darüberliegenden Zeile.)

(2) Wir sagen, die Matrix A habe *reduzierte Zeilenstufenform*, wenn sie Zeilenstufenform hat und zusätzlich *alle* Einträge in einer Spalte einer führenden Eins, abgesehen von der führenden Eins selbst, gleich Null sind (also auch die Einträge *über* der führenden Eins).

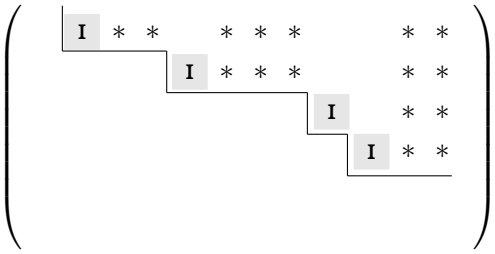
⊣

Beispiel 5.14. Schematisch dargestellt bedeutet Zeilenstufenform, dass die Matrix die folgende Gestalt hat:



Hier sind die »Stufen« eingezeichnet. Die führenden Einsen sind grau hinterlegt. An den mit Sternchen $*$ markierten Stellen dürfen beliebige Elemente von K stehen (selbstverständlich auch 0 und 1). Im leeren Bereich unten links stehen nur Nullen.

In der reduzierten Zeilenstufenform wird zusätzlich gefordert, dass über den *führenden Einsen* nur Nullen stehen:



Über anderen, »nicht-führenden« Einsen (an den Sternchen-Stellen) müssen natürlich nicht unbedingt Nullen stehen. ◊

Theorem 5.15 (Gauß-Algorithmus). *Seien K ein Körper und m, n natürliche Zahlen. Jede Matrix $A \in M_{m\times n}(K)$ kann durch wiederholte Anwendung elementarer Zeilenumformungen in eine Matrix in reduzierter Zeilenstufenform überführt werden.*

Beweis. Wir erklären zuerst, wie sich eine Matrix A in Zeilenstufenform überführen lässt. Dazu führen wir Induktion nach Anzahl der Zeilen. Der Induktionsanfang (wahlweise für 0 Zeilen oder eine Zeile) ist klar.

Bringe nun eine der Zeilen, die mit einer minimalen Anzahl von Nullen beginnen, durch eine Zeilenvertauschung in die erste Zeile. Sei a der erste von Null verschiedene Eintrag der neuen ersten Zeile; er liege in Spalte j. Multipliziere die erste Zeile mit a^{-1}, so dass also der erste von Null verschiedene Eintrag der neuen ersten Zeile gleich 1 ist:

$$\begin{pmatrix} 1 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix}$$

Durch dieses Vorgehen sind alle Einträge in Spalten mit Index $< j$ gleich Null. Gibt es in den Zeilen $2, 3, \ldots$ in der j-ten Spalte Einträge $\neq 0$, so ziehe nun geeignete Vielfache der ersten Zeile von diesen Zeilen ab, um eine Matrix zu erhalten, in denen die 1 in der ersten Zeile der einzige Eintrag in Spalte j ist, der von Null verschieden ist. Bezeichne die Matrix, die wir so erhalten, mit A':

$$\begin{pmatrix} 1 & * & * & * & * & * \\ & * & * & * & * & * \\ & * & * & * & * & * \\ & * & * & * & * & * \end{pmatrix}$$

Nach Induktionsvoraussetzung wissen wir bereits, dass wir die Matrix, die durch die Zeilen $2, 3, \ldots, m$ von A' gegeben ist, durch elementare Zeilenumformungen in Zeilenstufenform bringen können. Wenn wir dieselben Umformungen auf die Matrix A' anwenden (und die erste Zeile von A' unverändert lassen), erhalten wir eine Matrix in Zeilenstufenform.

Es bleibt nun nur noch zu zeigen, dass sich eine Matrix in Zeilenstufenform durch elementare Zeilenumformungen in reduzierte Zeilenstufenform überführen lässt. Das können wir aber offensichtlich erreichen, indem wir jeweils geeignete Vielfache der Zeilen mit führenden Einsen von den Zeilen darüber abziehen. □

Beispiel 5.16. Beispiele für die Durchführung des Gauß-Algorithmus.

(1) Sei $K = \mathbb{Q}$ und

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix}.$$

Wir bringen A mit dem Gauß-Algorithmus zunächst auf Zeilenstufenform.

$$\begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix} \xrightarrow{Z_1 \leftrightsquigarrow Z_2} \begin{pmatrix} 3 & 4 & 5 \\ 0 & 1 & 2 \\ 6 & 7 & 8 \end{pmatrix} \xrightarrow{Z_1 \rightsquigarrow \frac{1}{3}Z_1} \begin{pmatrix} 1 & \frac{4}{3} & \frac{5}{3} \\ 0 & 1 & 2 \\ 6 & 7 & 8 \end{pmatrix} \xrightarrow{Z_3 \rightsquigarrow Z_3 - 6Z_1}$$

$$\begin{pmatrix} 1 & \frac{4}{3} & \frac{5}{3} \\ 0 & 1 & 2 \\ 0 & -1 & -2 \end{pmatrix} \xrightarrow{Z_3 \rightsquigarrow Z_3 + Z_2} \begin{pmatrix} 1 & \frac{4}{3} & \frac{5}{3} \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Schließlich können wir noch die reduzierte Zeilenstufenform herstellen:

$$\begin{pmatrix} 1 & \frac{4}{3} & \frac{5}{3} \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{Z_1 \rightsquigarrow Z_1 - \frac{4}{3}Z_2} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

(2) Sei $K = \mathbb{C}$, sei $z \in \mathbb{C}$ eine fixierte Zahl und sei

$$A = \begin{pmatrix} a & i \\ i & 1 \end{pmatrix}.$$

Wir wenden auf die Matrix A den Gauß-Algorithmus an. Da wir nicht wissen, ob $a \neq 0$ ist, beginnen wir damit, die Zeilen zu vertauschen.

$$\begin{pmatrix} a & i \\ i & 1 \end{pmatrix} \xrightarrow{Z_1 \leftrightsquigarrow Z_2} \begin{pmatrix} i & 1 \\ a & i \end{pmatrix} \xrightarrow{Z_1 \rightsquigarrow -iZ_1} \begin{pmatrix} 1 & -i \\ a & i \end{pmatrix} \xrightarrow{Z_2 \rightsquigarrow Z_2 - aZ_1} \begin{pmatrix} 1 & -i \\ 0 & (a+1)i \end{pmatrix}.$$

An dieser Stelle müssen wir eine Fallunterscheidung machen. Ist $a = -1$, so hat A die reduzierte Zeilenstufenform

$$\begin{pmatrix} 1 & -i \\ 0 & 0 \end{pmatrix}.$$

Ist $a \neq -1$, so können wir die zweite Zeile durch $(a+1)i$ teilen und das i-fache der neuen zweiten Zeile zur ersten Zeile addieren. In diesem Fall hat A als reduzierte Zeilenstufenform die Einheitsmatrix E_2.

◊

Wir sehen im ersten Beispiel, dass eine Matrix in aller Regel keine eindeutig bestimmte Zeilenstufenform hat (die Matrix, die wir durch die ersten Umformungen erhalten hatten, hat ja Zeilenstufenform, genau wie die Matrix in reduzierter Zeilenstufenform, die beiden Matrizen unterscheiden sich aber). Der folgende Satz sagt aber, dass die »Form«, d.h. die Anzahl und Position der Stufen bzw. der führenden Einsen für alle Matrizen in Zeilenstufenform, die man aus einer Matrix A durch elementare Zeilenumformungen erhalten kann, die gleiche ist. Und es gibt sogar nur eine einzige Matrix in reduzierter Zeilenstufenform, die man aus einer Matrix A so erhalten kann.

SATZ 5.17. *Sei $A \in M_{m\times n}(K)$ eine Matrix.*

(1) *Alle Matrizen in Zeilenstufenform, die man aus A durch elementare Zeilenumformungen erhalten kann, haben dieselbe Anzahl an führenden Einsen und haben die führenden Einsen in denselben Spalten.*

(2) *Es gibt genau eine Matrix in reduzierter Zeilenstufenform, die aus A durch elementare Zeilenumformungen hervorgeht. Wir nennen diese auch die* reduzierte Zeilenstufenform von A.

BEWEIS. Wir betrachten A als die Koeffizientenmatrix eines homogenen linearen Gleichungssystems. Da wir bereits wissen (Lemma 5.12), dass elementare Zeilenumformungen die Lösungsmenge nicht ändern, genügt es zu zeigen, dass die Anzahl und Position der führenden Einsen in einer Matrix in Zeilenstufenform durch die Lösungsmenge des zugehörigen homogenen Gleichungssystems eindeutig bestimmt ist. Und entsprechend für Teil (2), dass eine Matrix in reduzierter Zeilenstufenform durch die Lösungsmenge des zugehörigen homogenen linearen Gleichungssystems eindeutig bestimmt ist.

zu (1). Sei $\mathbb{L}$ die Lösungsmenge des durch A gegebenen homogenen linearen Gleichungssystems. Sei A' eine Matrix in Zeilenstufenform, die aus A durch elementare Zeilenumformungen entsteht.

Wir zeigen durch Induktion nach der Anzahl der Spalten von A, dass wir die Anzahl und Positionen der führenden Einsen in A' an $\mathbb{L}$ ablesen können. Wenn A nur eine Spalte hat, dann ist A' die Nullmatrix (wenn A selbst die Nullmatrix ist, also genau dann, wenn $\mathbb{L} = K$) oder die Matrix $(1, 0, ..., 0)^t$ (in allen anderen Fällen, also genau dann, wenn $\mathbb{L} = \{0\}$). In diesem Fall ist die Zeilenstufenform eindeutig bestimmt.

Nun sei die Anzahl n der Spalten > 1. Wir können die Induktionsvoraussetzung anwenden: Für jede Matrix in Zeilenstufenform sind auch die ersten $n-1$ Spalten in Zeilenstufenform, und elementare Zeilenumformungen verändern jede Spalte für sich, unabhängig von den anderen Spalten. Wir erhalten die Lösungsmenge des durch die ersten $n-1$ Spalten gegebenen homogenen Gleichungssystems als

$$\{(x_1, ..., x_{n-1})^t;\ (x_1, ..., x_{n-1}, 0)^t \in \mathbb{L}\} \subseteq K^{n-1},$$

diese ist also durch $\mathbb{L}$ eindeutig bestimmt. Es folgt per Induktion, dass die Anzahl und Lage der führenden Einsen in den ersten $n-1$ Spalten durch $\mathbb{L}$ eindeutig bestimmt ist.

Schließlich enthält die letzte Spalte genau dann eine führende 1, wenn der n-te Eintrag in allen Elementen der Lösungsmenge $= 0$ ist.

zu (2). Den Beweis von Teil (2) erläutern wir hier nur an einem Beispiel, das das Prinzip erklärt. Damit könnten Sie den Beweis auch an dieser Stelle schon in der allgemeinen Situation ausarbeiten. Wir verschieben das im Skript auf etwas später, weil es mit dem Produkt von Matrizen einfacher (und durchsichtiger) möglich sein wird, siehe Satz 5.59. Betrachten wir als Beispiel die Matrix

$$\begin{pmatrix} 1 & 0 & a & b & c \\ 0 & 1 & d & e & f \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

in reduzierter Zeilenstufenform. Wir wissen aus Teil (1) bereits, dass die Anzahl und Lage der Stufen bzw. der führenden Einsen durch die Lösungsmenge $\mathbb{L}$ des homogenen Gleichungssystems dazu eindeutig bestimmt sind. Es geht nun noch darum, die Koeffizienten $a, \dots, f$ durch $\mathbb{L}$ auszudrücken. Dafür können wir sagen, dass das einzige Element von $\mathbb{L}$ von der Form $(*, *, 1, 0, 0)^t$ (wobei die Sternchen wie üblich beliebige Elemente aus dem Grundkörper bezeichnen) der Vektor $(-a, -d, 1, 0, 0)^t$ ist. Genauso ist $(-b, -e, 0, 1, 0)^t$ der einzige Vektor in $\mathbb{L}$, dessen letzte drei Einträge $0, 1, 0$ sind, und $(-c, -f, 0, 0, 1)^t$ der einzige Vektor in $\mathbb{L}$, dessen letzte drei Einträge $0, 0, 1$ sind. Wir können also alle Einträge der Matrix in $\mathbb{L}$ »wiederfinden«. □

SATZ 5.18 (Lösungsmenge eines LGS in (reduzierter) Zeilenstufenform). *Sei $(A \mid b)$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems mit m Gleichungen und n Unbestimmten. Wir setzen voraus, dass die Matrix A Zeilenstufenform hat.*

(1) *Wenn es ein i gibt, so dass die i-te Zeile von A eine Nullzeile, aber die i-te Zeile von $(A \mid b)$ keine Nullzeile ist, dann ist die Lösungsmenge leer. Hat sogar $(A \mid b)$ Zeilenstufenform, dann können wir die Bedingung formulieren als: die letzte Spalte von $(A \mid b)$ enthält eine führende Eins.*

(2) *Nun gelte, dass in den Matrizen A und $(A \mid b)$ genau dieselben Zeilen Nullzeilen sind. Dann ist die Lösungsmenge nicht leer. Wir benennen die Spalten von A, die eine führende Eins enthalten, mit $1 \le j_1 < \cdots < j_r \le n$. Dann besteht die Lösungsmenge aus den folgenden Elementen von K^n: Jede Wahl von Elementen $x_j \in K, j \notin \{j_1, \dots, j_r\}$ lässt sich durch die Vorschrift*

$$x_{j_i} = b_i - \sum_{j > j_i} a_{ij} x_j, \qquad i = 1, \dots, r$$

zu einem Lösungsvektor ergänzen, und auf diese Art und Weise erhält man alle Lösungsvektoren.

(Wenn A sogar reduzierte Zeilenstufenform hat, dann treten auf den rechten Seiten dieser Gleichungen nur x_j mit $j \notin \{j_1, \dots, j_r\}$ auf (die anderen a_{ij} sind Null). Sonst muss man die x_{j_i} beginnend mit x_{j_r} bestimmen und sich dann Schritt für Schritt zu x_{j_1} vorarbeiten.)

BEWEIS. zu (1). Wenn die angegebene Bedingung erfüllt ist, dann hat die i-te Gleichung die Form $0 = b_i$ mit $b_i \neq 0$ und ist daher nicht erfüllbar.

zu (2). Bei der oben angegebenen Darstellung für x_{j_i} $(i = 1, \dots, r)$ handelt es sich einfach um eine äquivalente Formulierung der i-ten Gleichung des Systems, $i = 1, \dots, r$. Die Zeilen nach der r-ten Zeile sind Nullzeilen, die als Gleichung einfach $0 = 0$ aussagen – das ist immer erfüllt.

Daher beschreibt der Satz genau die Bedingungen, die ein Lösungsvektor erfüllen muss. □

Schauen Sie sich auch die folgenden Beispiele an, die das etwas konkreter machen.

BEISPIEL 5.19. (1) Sei $K = \mathbb{Q}$ und

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix}.$$

Wir haben in Beispiel 5.16 (1) gesehen, dass A die Zeilenstufenform

$$\begin{pmatrix} 1 & \frac{4}{3} & \frac{5}{3} \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

hat. Daran können wir die Lösungsmenge des durch A gegebenen homogenen Gleichungssystems ablesen als

$$\mathbb{L} = \left\{ \begin{pmatrix} z \\ -2z \\ z \end{pmatrix} ; z \in \mathbb{Q} \right\},$$

denn $-\frac{4}{3} \cdot (-2z) - \frac{5}{3}z = z$. Statt diese Rechnung an dieser Stelle zu machen, kann man auch die Matrix auf die reduzierte Zeilenstufenform

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

bringen und dann die Lösungsmenge noch direkter ablesen. Das Ergebnis ist natürlich dasselbe.

(2) Sei K irgendein Körper und seien $a, b, c, d, e \in K$. Wir betrachten die erweiterte Koeffizientenmatrix

$$\left(\begin{array}{cccc|c} 1 & a & 0 & b & c \\ 0 & 0 & 1 & d & e \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

in reduzierter Zeilenstufenform. Die Lösungsmenge des zugehörigen linearen Gleichungssystems ist

$$\mathbb{L} = \left\{ \begin{pmatrix} c - ax - bx' \\ x \\ e - dx' \\ x' \end{pmatrix} ; x, x' \in K \right\}$$

Eine etwas andere Art, die Elemente der Lösungsmenge zu notieren, ist die folgende:

$$\mathbb{L} = \left\{ \begin{pmatrix} c \\ 0 \\ e \\ 0 \end{pmatrix} + x \begin{pmatrix} -a \\ 1 \\ 0 \\ 0 \end{pmatrix} + x' \begin{pmatrix} -b \\ 0 \\ -d \\ 1 \end{pmatrix} ; x, x' \in K \right\}$$

Damit sehen wir auch direkt die Darstellung von $\mathbb{L}$ in der Form $t + \mathbb{L}_0$, wobei $\mathbb{L}_0$ die Lösungsmenge des zugehörigen homogenen Systems ist:

$$\mathbb{L} = \begin{pmatrix} c \\ 0 \\ e \\ 0 \end{pmatrix} + \left\{ x \begin{pmatrix} -a \\ 1 \\ 0 \\ 0 \end{pmatrix} + x' \begin{pmatrix} -b \\ 0 \\ -d \\ 1 \end{pmatrix} ; x, x' \in K \right\}$$

◊

Bemerkung 5.20. Sei $(A \mid b)$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems. Wenn man in A Spalten vertauscht, entspricht das in Termen des Gleichungssystems einfach einem Umsortieren der Unbestimmten. Da alle Zeilenumformungen separat auf jede einzelne Spalte wirken, ist es zulässig, zunächst eine Spaltenvertauschung von A vorzunehmen, dann den Gauß-Algorithmus anzuwenden, und dann in der so erhaltenen Matrix die umgekehrte Spaltenumformung durchzuführen, und am Ergebnis die Lösungsmenge abzulesen. Allerdings muss man dabei besonders gut aufpassen, dass keine Flüchtigkeitsfehler passieren (zum Beispiel vergisst man leicht, am Ende wieder zurückzutauschen). Die letzte

Spalte von $(A \mid b)$ spielt selbstverständlich eine Sonderrolle und darf nicht mitvertauscht werden.

Bei den Gleichungssystemen, die Sie »per Hand« lösen müssen, sollte es nicht erforderlich sein, Spalten zu vertauschen. In der Praxis, bei der Berechnung der Lösungsmengen von Gleichungssystemen mit »vielen« Gleichungen und Unbestimmten mit einem Computerprogramm, wo auch Rundungsfehler ein Problem darstellen können, kann das aber sinnvoll sein (so wie es dann auch wichtiger ist, die Zeilenumformungen geschickt zu wählen). ◊

Wir fassen unsere Ergebnisse noch einmal zusammen:

SATZ 5.21. *Sei $(A \mid b)$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems. Sei $(A' \mid b')$ eine Matrix in Zeilenstufenform, die aus $(A \mid b)$ durch elementare Zeilenumformungen entsteht.*

(1) *Es sind äquivalent:*
   (i) *Das durch $(A \mid b)$ gegebene lineare Gleichungssystem besitzt eine Lösung.*
   (ii) *Die Matrizen A' und $(A'|b')$ haben gleich viele Stufen.*

(2) *Es sind äquivalent:*
   (i) *Das durch $(A \mid b)$ gegebene lineare Gleichungssystem besitzt eine eindeutige Lösung.*
   (ii) *Die Matrix A' hat in jeder Spalte eine Stufe, und für jede Nullzeile in A' ist der entsprechende Eintrag in b' ebenfalls gleich 0.*

(3) *Sei nun in der obigen Situation A eine* quadratische *Matrix. Dann sind äquivalent:*
   (i) *Das durch $(A \mid b)$ gegebene lineare Gleichungssystem besitzt eine eindeutige Lösung.*
   (ii) *Für die Matrix $A' = (a'_{ij})_{i,j}$ gilt $a_{ii} = 1$ für alle i, d.h. die Diagonaleinträge sind alle $= 1$, und $a_{ij} = 0$ für alle $i > j$, d.h. die »Einträge unterhalb der Diagonale« sind alle gleich Null.*

   Insbesondere ist diese Eigenschaft unabhängig von b.

   Hat in dieser Situation A' sogar reduzierte Zeilenstufenform, dann beschreibt $(A \mid b)$ ein eindeutig lösbares lineares Gleichungssystem genau dann, wenn A' die Einheitsmatrix ist.

BEWEIS. Vorbemerkung: Wenn $(A' \mid b')$ durch elementare Zeilenumformungen aus $(A \mid b)$ entsteht und (reduzierte) Zeilenstufenform hat, so entsteht auch A' durch elementare Zeilenumformungen (nämlich durch genau dieselben Umformungen) aus A und hat (reduzierte) Zeilenstufenform.

zu (1). Das ist eine Umformulierung von Satz 5.18 (1).

zu (2). Dass das Gleichungssystem eindeutig lösbar ist, ist gleichbedeutend damit, dass es eine Lösung gibt, aber dass wir keine Elemente in K wie in Satz 5.18 (2) wählen können, denn sonst gäbe es mindestens zwei Lösungen. Das heißt genau, dass in jeder Spalte eine Stufe ist.

zu (3). Dies folgt aus Teil (2) mit der Bemerkung, dass eine quadratische Matrix in Zeilenstufenform genau dann in jeder Spalte eine Stufe hat, wenn es sich um eine Matrix mit der beschriebenen Form handelt. (Wir sprechen von einer »oberen Dreiecksmatrix« mit Einsen auf der Diagonale, siehe Abschnitt 5.3.2.)

Die Bemerkung am Ende ergibt sich daraus, dass die einzige quadratische Matrix in reduzierter Zeilenstufenform, die in jeder Spalte eine Stufe hat, die Einheitsmatrix ist. □

Teil (2) zeigt, dass ein lineares Gleichungssystem mit erweiterter Koeffizientenmatrix $(A \mid b)$, $A \in M_{m\times n}(K)$ mit $m < n$ (mehr Unbestimmte als Gleichungen, man spricht auch von einem *unterbestimmten* linearen Gleichungssystem) nicht eindeutig lösbar sein kann. Dass in Teil (3) des Satzes die reduzierte Zeilenstufenform von A die Einheitsmatrix ist, ist eine Bedingung, die nicht von b abhängt. Wir können noch ein bisschen mehr zeigen:

KOROLLAR 5.22. *Sei $A \in M_n(K)$ eine* quadratische *Matrix. Dann sind äquivalent:*

(i) *Für alle $b \in K^n$ ist das durch $(A \mid b)$ gegebene Gleichungssystem eindeutig lösbar.*

(ii) *Für alle $b \in K^n$ ist das durch $(A \mid b)$ gegebene Gleichungssystem lösbar.*

(iii) *Es existiert $b \in K^n$, so dass das Gleichungssystem, das durch $(A \mid b)$ gegeben ist, eindeutig lösbar ist.*

(iv) *Die reduzierte Zeilenstufenform von A ist E_n.*

BEWEIS. Es ist offensichtlich, dass (i) $\Rightarrow$ (ii) gilt, und aus dem vorherigen Satz folgt (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i). Es genügt daher, nun noch die Implikation (ii) $\Rightarrow$ (iii) zu zeigen. Wir zeigen, dass aus (ii) die Aussage (iii) für $b = 0$ folgt. Wenn das durch A gegebene homogene lineare Gleichungssystem mehrere Lösungen hat, dann hat die reduzierte Zeilenstufenform A' von A eine Nullzeile. Es ist dann klar, dass $b' \in K^n$ existiert, so dass das Gleichungssystem zu $(A' \mid b')$ nicht lösbar ist – wir müssen nur einen Eintrag von b' in einer Zeile, die in A' eine Nullzeile ist, auf einen Wert $\neq 0$ festsetzen.

Da A' aus A durch elementare Zeilenumformungen entsteht, können wir auch A aus A' durch elementare Zeilenumformungen erhalten. Wenden wir diese Zeilenumformungen auf die erweiterte Matrix $(A' \mid b')$ an, so erhalten wir eine Matrix $(A \mid b)$ mit $b \in K^n$, deren Gleichungssystem dieselbe Lösungsmenge hat wie das System $(A' \mid b')$, also die leere Menge. Das zeigt, dass (ii) falsch ist, wenn (iii) nicht gilt, oder mit anderen Worten (ii) $\Rightarrow$ (iii). □

5.2.3. Teilräume von K^n. Um die Struktur der Lösungsmenge eines linearen Gleichungssystems noch besser beschreiben zu können (und um später die Frage zu beantworten, welche Teilmengen von K^n als Lösungsmenge eines linearen Gleichungssystemes auftreten können), machen wir die folgende Definition:

DEFINITION 5.23. Eine Teilmenge $U \subseteq K^n$ heißt *Teilraum* von K^n, wenn die folgenden Bedingungen erfüllt sind:

(a) $0 \in U$,

(b) für alle $u, v \in U$ gilt $u + v \in U$, und

(c) für alle $a \in K$, $u \in U$ gilt $au \in U$.

⊣

BEISPIEL 5.24. (1) Die Teilmengen $\{0\}$ und K^n sind Teilräume von K^n. Den Teilraum $\{0\}$ nennt man auch den *Nullraum*; manchmal bezeichnet man den Nullraum auch mit 0 (ohne Mengenklammern).

(2) Die einzigen Teilräume von $K^1 = K$ sind 0 und K. (Warum?)

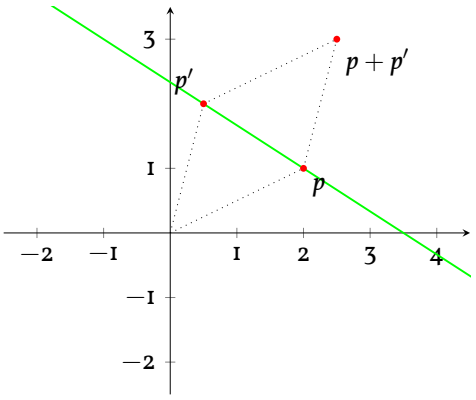
(3) Ist $x \in K^n$, so ist die Menge $\{ax;\ a \in K\}$ ein Teilraum von K^n. (Warum?)

(4) Jede Gerade in $\mathbb{R}^2$, die den Ursprung enthält, ist ein Teilraum (von der Form von Teil (3) dieses Beispiels). Wir werden sehen: Die Teilräume von $\mathbb{R}^2$ sind $\{0\}$, $\mathbb{R}^2$ und die Geraden in $\mathbb{R}^2$, die den Ursprung $(0,0)^t$ enthalten. Können Sie zeigen, dass es keine anderen gibt?

(5) Die leere Menge $\emptyset$ ist kein Teilraum. Die Teilmenge $\{(x,y);\ y = x^2\}$ ist kein Teilraum von $\mathbb{R}^2$, denn sie enthält $(1,1)^t$ und $(-1,1)^t$, aber nicht die Summe $(1,1)^t + (-1,1)^t = (0,2)^t$.

◊

Beispiel 5.25. Die grüne Gerade im Bild rechts erfüllt keine der Bedingungen (a), (b), (c): Zum Beispiel ist (b) verletzt, weil sie p und p' enthält, aber nicht die Summe $p + p'$. Finden Sie ein Beispiel, das zeigt, dass (c) ebenfalls nicht erfüllt ist. ♢



Die (für den Moment) wichtigsten Beispiele für Teilräume liefert uns das folgende Lemma.

Lemma 5.26. *Sei $U \subseteq K^n$ die Lösungsmenge eines homogenen linearen Gleichungssystems. Dann ist U ein Teilraum von K.*

Beweis. Zunächst liegt sicher der Nullvektor in der Lösungsmenge jedes homogenen linearen Gleichungssystems: $0 \in U$. Sind $v = (v_j)_j, w = (w_j)_j \in U$, erfüllen also $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_n)$ alle Gleichungen des gegebenen homogenen linearen Gleichungssystems, so gilt das auch für die Summe $(v_1 + w_1, \ldots, v_n + w_n)$. In der Tat, betrachten wir eine Gleichung der Form

$$a_1 X_1 + \cdots + a_n X_n = 0,$$

so sehen wir

$$\begin{aligned} a_1(v_1 + w_1) + \cdots + a_n(v_n + w_n) &= a_1 v_1 + a_1 w_1 + \cdots + a_n v_n + a_n w_n \\ &= a_1 v_1 + \cdots + a_n v_n + a_1 w_1 + \cdots + a_n w_n \\ &= 0 + 0 = 0. \end{aligned}$$

Ähnlich, aber noch einfacher, ist es zu zeigen, dass für jede Lösung v eines homogenen linearen Gleichungssystems und jedes Element $a \in K$ auch av eine Lösung ist. Damit sind alle Eigenschaften gezeigt, die wir überprüfen müssen, um zu beweisen, dass U ein Teilraum von K^n ist. □

Frage 5.27. Wir wollen diesen Abschnitt damit beenden, zwei Fragen zu formulieren, die sich an dieser Stelle stellen, die wir aber erst mit etwas mehr Theorie werden befriedigend beantworten können.

(1) Ist jeder Teilraum von K^n die Lösungsmenge eines homogenen linearen Gleichungssystems? (Das ist in der Tat der Fall, siehe Satz 8.9.)

(2) In Korollar 5.22 haben wir gesehen, dass für eine quadratische Matrix A die Eigenschaft, dass das Gleichungssystem $(A|0)$ eindeutig lösbar ist, dazu äquivalent ist, dass alle Gleichungssysteme $(A|b)$ lösbar sind.

    Können wir diese Beziehung zwischen der *Eindeutigkeit* der Lösung und der *Existenz* von Lösungen verallgemeinern? Kann man zum Beispiel »quantifizieren«, wie viele Lösungen ein lineares Gleichungssystem $(A \mid 0)$ hat, auch wenn es nicht eindeutig lösbar ist, und das in Beziehung dazu setzen, für »wie viele« b das Gleichungssystem $(A \mid b)$ lösbar ist?

    Weil wir (wenn K unendlich viele Elemente hat) darüber sprechen, dass unendlich viele Lösungen existieren, ist nicht klar, was man unter »quantifizieren« verstehen soll. Wir werden diese Frage in einer sehr schönen (und nützlichen) Art und Weise beantworten; siehe Abschnitt 8.2.

□ Frage 5.27

5.3. Das Matrizenprodukt

5.3.1. Rechnen mit Matrizen. In diesem Abschnitt wollen wir Matrizen noch einmal losgelöst vom Begriff des linearen Gleichungssystems studieren und insbesondere Rechenoperationen auf der Menge der Matrizen definieren, die sich in vielen Situationen als sehr nützlich erweisen (auch für die Behandlung von linearen Gleichungssystemen). Wir wiederholen hier zur Erinnerung noch einmal die Definition 5.6.

DEFINITION 5.28. Seien m, n natürliche Zahlen. Unter einer *Matrix* der Größe $m \times n$ mit Einträgen in K (man spricht auch von einer $(m \times n)$-Matrix über K) verstehen wir eine Familie $(a_{ij})_{i=1,\dots,m,\, j=1,\dots,n}$ von Elementen von K. Die Elemente a_{ij} heißen die *Einträge* oder *Koeffizienten* der Matrix. Eine Matrix stellen wir uns immer in der Form

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

vor, d.h. wir schreiben die Koeffizenten in einem rechteckigen Schema auf, in dem der erste Index die Zeile und der zweite Index die Spalte angibt.

Die Menge aller $(m \times n)$-Matrizen über K bezeichnen wir mit $M_{m\times n}(K)$. Ist $m = n$, so schreiben wir manchmal $M_n(K)$ statt $M_{m\times n}(K)$. ⊣

Die *Nullmatrix* (der Größe $m \times n$) ist die Matrix $0 \in M_{m\times n}(K)$, deren Einträge alle gleich Null sind.

Als Spezialfall können wir die Elemente des K^n, die wir wie gehabt als Spaltenvektoren betrachten wollen, als Matrizen mit n Zeilen und einer Spalte auffassen, das heißt $K^n = M_{n\times 1}(K)$.

Auch mit Matrizen kann man rechnen. Um zum Beispiel zwei Matrizen (der selben Größe) zu addieren, addieren wir einfach auf jeder Position separat die Einträge. Wie man sinnvolles Produkt von zwei Matrizen definiert, ist nicht ganz so offensichtlich. Wir fassen die wichtigen Rechenoperationen in der folgenden Definition zusammen:

DEFINITION 5.29. Seien K ein Körper und l, m, n natürliche Zahlen. Die Einträge der Matrizen A und B bezeichnen wir mit a_{ij} beziehungsweise b_{ij}.

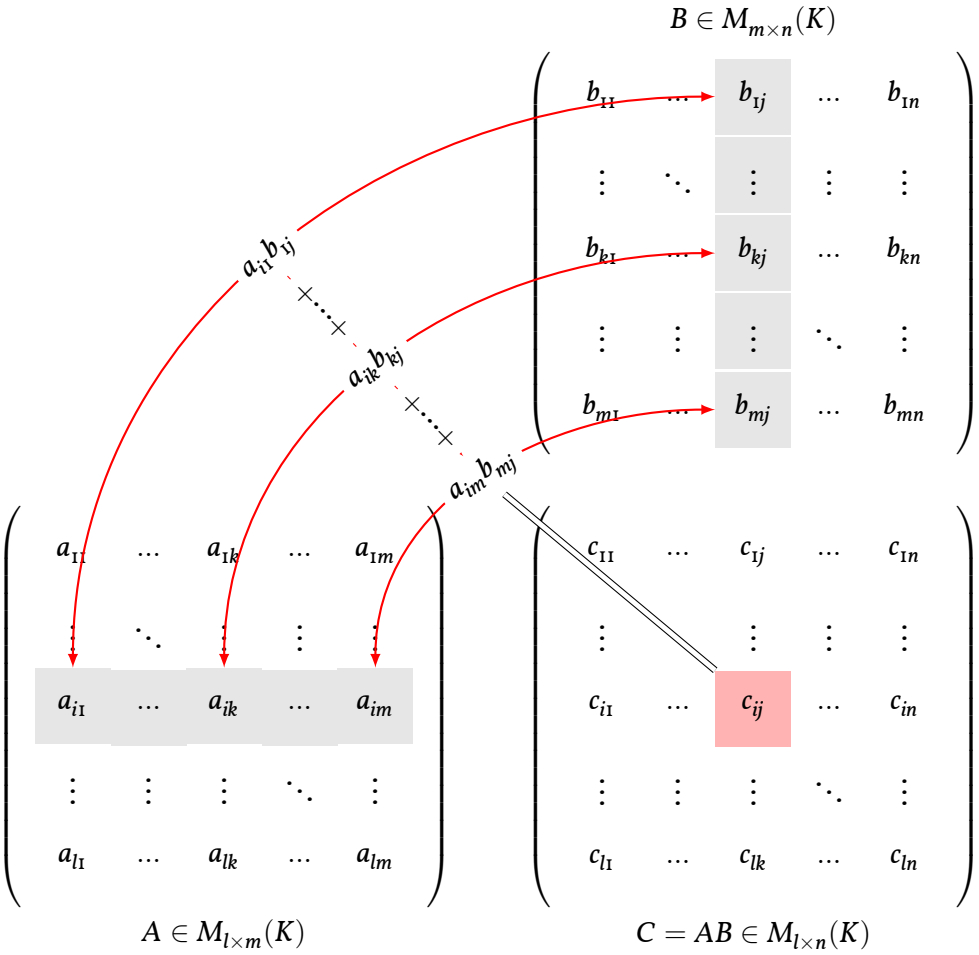
(1) (Summe von Matrizen) Für Matrizen $A, B \in M_{m\times n}(K)$ derselben Größe definieren wir
$$A + B = (a_{ij} + b_{ij})_{i=1,\dots,m,\, j=1,\dots,n} \in M_{m\times n}(K).$$

(2) (Produkt eines Skalars und einer Matrix) Für eine Matrix $A \in M_{m\times n}(K)$ und ein Element $a \in K$ definieren wir
$$aA = Aa = (aa_{ij})_{ij} \in M_{m\times n}(K).$$

(3) (Produkt zweier Matrizen) Sind $A \in M_{l\times m}(K)$ und $B \in M_{m\times n}(K)$ Matrizen, so definieren wir das *Produkt*
$$A \cdot B = \left(\sum_{j=1}^{m} a_{ij} b_{jk} \right)_{i=1,\dots,l,\, k=1,\dots,n} \in M_{l\times n}(K).$$
Den Multiplikationspunkt lässt man dabei oft aus: $AB = A \cdot B$.

⊣

BEISPIEL 5.30. Es ist für die Berechnung des Matrizenprodukts manchmal hilfreich, die zu multiplizierenden Matrizen A und B so anzuordnen, wie in der Abbildung gezeigt, d.h. dass B nach oben verschoben wird, und das Ergebnis dann rechts von A und unter B zu stehen kommt. Um die Zelle c_{ij} von $C = AB$ auszurechnen, benutzt man die i-te Zeile von A und die j-te Spalte von B. Diese haben beide m Einträge. Man multipliziert die ersten Einträge, die zweiten Einträge, ..., und summiert alle diese Produkte auf.



(Illustration angepasst von texample.net[1], Autor: Alain Matthes.) ◊

Angesichts der Identifikation $K^n = M_{n\times 1}(K)$ können wir auch Elemente von K^n mit Matrizen multiplizieren (wenn die Größen zusammenpassen). Für quadratische Matrizen $A \in M_n(K)$ können wir dann auch die Potenzen A^n von A für $n \in \mathbb{N}$ definieren: $A^0 = E_n$, $A^1 = A$, $A^2 = AA$, und so weiter: $A^n = A^{n-1}A$ für $n > 0$.

SATZ 5.31. *(Eigenschaften der Rechenoperationen mit Matrizen) Seien $l, m, n \in \mathbb{N}$.*

(1) *Die Addition von Matrizen definiert eine Verknüpfung*

$$+ : M_{m\times n}(K) \times M_{m\times n}(K) \to M_{m\times n}(K),$$

die die folgenden Eigenschaften hat:

(a) *Assoziativität:* $(A + B) + C = A + (B + C)$,

(b) *Kommutativität:* $A + B = B + A$,

(c) *die Nullmatrix 0 ist neutrales Element:* $0 + A = A = A + 0$,

[1] https://texample.net/tikz/examples/matrix-multiplication/

(d) *das additive Inverse der Matrix* $(a_{ij})_{i,j}$ *ist die Matrix* $-A := (-a_{ij})_{i,j} (= (-1) \cdot A)$.

(2) *Die Multiplikation von Matrizen definiert eine assoziative Verknüpfung* $M_{l\times m}(K) \times M_{m\times n}(K) \to M_{l\times n}(K)$.

(3) *Die Addition und das Produkt von Matrizen verhalten sich distributiv, d.h. es gilt*

$$(A + B)C = AC + BC, \quad A(B + C) = AB + AC,$$

wenn immer man die entsprechenden Summen und Produkte bilden kann.

BEWEIS. Die Eigenschaften der Addition sind klar, da die Addition eintragweise erfolgt. Seien nun A, B, C Matrizen mit Einträgen a_{ij}, b_{ij}, c_{ij}, so dass die Produkte AB, und BC existieren. Die Assoziativität des Produkts ergibt sich aus der Gleichungskette

$$\sum_k \left(\sum_j a_{ij} b_{jk} \right) c_{kl} = \sum_k \sum_j a_{ij} b_{jk} c_{kl} = \sum_j \sum_k a_{ij} b_{jk} c_{kl} = \sum_j a_{ij} \left(\sum_k b_{jk} c_{kl} \right),$$

in der links der Eintrag von $(AB)C$ in der i-ten Zeile und l-ten Spalte, und rechts der entsprechende Eintrag von $A(BC)$ steht. (Die Intervalle, über die die Indizes in den Summen laufen, bestimmen sich aus der Größe von B und sind hier ausgelassen.) Die äußeren Gleichheiten benutzen dabei das Distributivgesetz in K, die mittlere das Kommutativgesetz: Wir summieren die Ausdrücke $a_{ij}b_{jk}c_{kl}$ für alle j und k auf, und es spielt keine Rolle, wie wir sie anordnen.

Die Rechnung für das Distributivgesetz ist einfach und wir lassen sie hier aus. □

Die Einheitsmatrix (der richtigen Größe) ist ein neutrales Element bezüglich der Multiplikation: $E_m A = A$ und $AE_n = A$ für alle $A \in M_{m\times n}(K)$.

BEISPIEL 5.32. Wie das folgende Beispiel zeigt, ist das Produkt von Matrizen *nicht kommutativ*:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

◊

Die Multiplikation eines Skalars mit einer Matrix ist auch assoziativ und kommutativ: $a(AB) = (aA)B = A(aB)$, wie man unmittelbar nachprüft.

ERGÄNZUNG 5.33 (Der Strassen-Algorithmus). Interessanterweise lässt sich ein Produkt von zwei $(n \times n)$-Matrizen mit weniger als den a priori erforderlichen n^3 Multiplikationen berechnen. Die bekannteste Methode ist der Strassen-Algorithmus[2]. Für das Produkt von zwei (2×2)-Matrizen kommt er mit 7 Multiplikationen (statt 8 für die direkte Rechnung) aus; allerdings werden mehr Additionen als in der direkten Rechnung durchgeführt. Weil Computer für eine Multiplikation mehr Zeit benötigen als für eine Addition, wird der Algorithmus in der Praxis verwendet, aber er bringt einen signifikanten Vorteil erst für Matrizen mit mehreren Hundert Zeilen und Spalten. □ Ergänzung 5.33

BEISPIEL 5.34. Eine weitere Eigenschaft des Matrizenprodukts, die einen Unterschied zur Multiplikation in einem Körper bedeutet, ist, dass das Produkt von zwei Matrizen $\neq 0$ die Nullmatrix sein kann:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

◊

[2] https://en.wikipedia.org/wiki/Strassen_algorithm

Auch wenn die Berechnung des Matrizenprodukts nicht schwierig ist, gibt es darüber weitreichende strukturelle Aussagen, für deren Beweis wir erst im Laufe der Vorlesung die notwendigen Methoden entwickeln werden. Ein Beispiel für so eine Aussage ist der folgende

SATZ 5.35. *Seien K ein Körper, $n \geq 1, A \in M_{n\times n}(K)$. Wenn eine natürliche Zahl N existiert mit $A^N = 0$, dann gilt $A^n = 0$.*

Siehe Satz 6.50 für einen Beweis. In der Linearen Algebra 2 werden wir diese Aussage noch weiter verallgemeinern und besser verstehen können (der hier angegebene Satz ist ein Spezialfall des »Satzes von Cayley-Hamilton«).

BEMERKUNG 5.36. Sei $(A \mid b)$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems. Für $x \in K^n = M_{n\times 1}(K)$ ist dann das Matrizenprodukt Ax eine $(m \times 1)$-Matrix, also ein Element von K^m, und zwar mit dem Eintrag

$$\sum_{j=1}^{n} a_{ij}x_j$$

in der i-ten Zeile; das ist genau die linke Seite der i-ten Gleichung des betrachteten Gleichungssystems. Das bedeutet: $x \in K^n$ ist ein Lösungsvektor des linearen Gleichungssystems genau dann, wenn $Ax = b$. Die Lösungsmenge des linearen Gleichungssystems $(A \mid b)$ ist also

$$\{x \in K^n;\ Ax = b\}.$$

$\Diamond$

BEMERKUNG 5.37. Wir können elementare Zeilenumformungen als Multiplikation mit einer geeigneten Matrix von links ausdrücken. Sei A eine Matrix.

Typ (I). Sei A' die Matrix, die aus A durch Addition des a-fachen der j-ten Zeile zur i-ten Zeile entsteht. Dann gilt

$$A' = E_{ij}(a)A,$$

wobei wir für $i \neq j$ und $a \in K$ definieren:

$$E_{ij}(a) := \begin{pmatrix} 1 & & & & \\ & \ddots & & a & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

wobei der Eintrag a in der i-ten Zeile und j-ten Spalte ist, auf der Diagonale Einsen stehen und alle anderen Einträge Null sind. (Ist $i > j$ so befindet sich der Eintrag a, anders als in der Abbildung, unterhalb der Diagonalen.)

Typ (II). Sei A' die Matrix, die aus A durch Vertauschen der i-ten und j-ten Zeile entsteht. Dann gilt

$$A' = P_{ij}A,$$

wobei wir für $i \neq j$ definieren:

$$P_{ij} := \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

Hier befinden sich die beiden Einsen außerhalb der Diagonale in Zeile i und Spalte j, und in Zeile j und Zeile i. Auf der Diagonale stehen in den Zeilen i und j Nullen, sonst überall 1.

Typ (III). Sei A' die Matrix, die aus A durch Multiplikation der i-ten Zeile mit $a \in K^\times$ entsteht. Dann gilt

$$A' = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} A,$$

wobei sich der Eintrag a auf der Diagonalen an Position i befindet, alle anderen Einträge aus der Diagonalen sind 1, alle Einträge außerhalb der Diagonalen sind 0. Wir werden für diese »Diagonalmatrix« später die Notation $\mathrm{diag}(1, \ldots, 1, a, 1, \ldots 1)$ benutzen, siehe Abschnitt 5.3.2.
◊

Wir können nun auch die Schreibweise $-^t$, die wir für Zeilenvektoren schon eingeführt hatten, auf beliebige Matrizen ausdehnen:

Definition 5.38. Sei $A = (a_{ij})_{i,j} \in M_{m\times n}(K)$ eine Matrix Die *transponierte Matrix* A^t von A ist die Matrix

$$A^t = (a_{ji})_{i=1,\ldots,n,\ j=1,\ldots m} \in M_{n\times m}.$$

⊣

Beim Übergang zur transponierten Matrix spiegeln wir also sozusagen an der Diagonalen. Die Anzahl der Zeilen in A^t ist die Anzahl der Spalten von A, und umgekehrt.

Beispiel 5.39. (1)

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

(2)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}^t = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}^t = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

◊

Lemma 5.40. (1) *Sei A eine Matrix. Dann gilt $A^{tt} := (A^t)^t = A$.*

(2) *Seien A, B Matrizen, deren Produkt AB existiert. Dann existiert das Produkt B^tA^t und es gilt*

$$(AB)^t = B^tA^t.$$

Beweis. Teil (1) ist klar. Zu Teil (2). Die Existenz der Produkte heißt *in beiden Fällen*, dass B so viele Zeilen wie A Spalten hat. Der Eintrag von $(AB)^t$ in der j-ten Zeile und i-ten Spalte ist der Eintrag von AB in Zeile i und Spalte j, also

$$\sum_k a_{ik}b_{kj},$$

wobei wir $A = (a_{ik})_{i,k}$ und $B = (b_{k,j})_{k,j}$ geschrieben haben. Aber das ist nichts anderes als

$$\sum_k b_{kj} a_{ik},$$

was der Eintrag von $B^t A^t$ in Zeile j und Spalte i ist. □

5.3.2. Spezielle Matrizen. Wir führen noch einige Sprechweise über Matrizen mit speziellen Eigenschaften ein.

Sei $A = (a_{ij})_{i,j}$ eine quadratische Matrix der Größe $n \times n$. Wir nennen A eine *obere Dreiecksmatrix*, wenn $a_{ij} = 0$ für alle i, j mit $i > j$. (An den links mit $*$ markierten Einträgen kann irgendein Element von K stehen, die unmarkierten Einträge müssen $= 0$ sein.)

$$\begin{pmatrix} * & * & \cdots & * \\ & * & \cdots & * \\ & & \ddots & \vdots \\ & & & * \end{pmatrix}$$

Analog kann man von *unteren Dreiecksmatrizen* sprechen (also wenn $a_{ij} = 0$ für alle i, j mit $i < j$).

$$\begin{pmatrix} * & & & \\ & * & & \\ & & \ddots & \\ & & & * \end{pmatrix}$$

Eine *Diagonalmatrix* ist eine quadratische Matrix $A = (a_{ij})_{i,j}$ mit $a_{ij} = 0$ für alle $i \neq j$.
Mit $\operatorname{diag}(c_1, \ldots, c_n)$ bezeichnen wir die Diagonalmatrix der Größe n mit den Diagonaleinträgen $c_1, c_2, \ldots, c_n$.
Dann gilt $aA = \operatorname{diag}(a, \ldots, a)A = A \operatorname{diag}(a, \ldots, a)$ für $a \in K$ und $A \in M_{m \times n}$, wobei in der diag-Ausdruck auf der linken Seite von A dann m Einträge, der auf der rechten Seite n Einträge haben muss.

Die $(n \times n)$-Matrix

$$E_n := \operatorname{diag}(1, \ldots, 1) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

heißt die *Einheitsmatrix* (der Größe n über dem Körper K). (Die Einträge, die gleich Null sind, sind hier weggelassen.)

Wir können Matrizen aus kleineren Matrizen (passender Größen) zusammensetzen; wir sprechen dann von der Notation als *Blockmatrizen*. Sind zum Beispiel $A \in M_{m_1 \times n_1}(K)$, $B \in M_{m_1 \times n_2}(K)$, $C \in M_{m_2 \times n_1}(K)$, $D \in M_{m_2 \times n_2}(K)$, so erhalten wir durch Zusammensetzen die $(m_1 + m_2) \times (n_1 + n_2)$-Matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$.

Das ist verträglich mit der Multiplikation von Matrizen:

LEMMA 5.41. *Für* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *und* $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ *mit* $A \in M_{l_1 \times m_1}(K)$, $B \in M_{l_1 \times m_2}(K)$, $C \in M_{l_2 \times m_1}(K)$, $D \in M_{l_2 \times m_2}(K)$, $A' \in M_{m_1 \times n_1}(K)$, $B' \in M_{m_1 \times n_2}(K)$, $C' \in M_{m_2 \times n_1}(K)$, $D' \in M_{m_2 \times n_2}(K)$ *gilt*

$$MM' = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} = \begin{pmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{pmatrix} \in M_{(l_1 + l_2) \times (n_1 + n_2)}(K).$$

BEWEIS. Das lässt sich unmittelbar anhand der Definition des Matrixprodukts nachrechnen. □

Weil das Matrizenprodukt (der kleineren Matrizen) nicht kommutativ ist, darf man natürlich in der Situation des Lemmas in den Produkten in den einzelnen Blockeinträgen von MM' die Faktoren nicht vertauschen. Ähnlich funktioniert das mit Blockmatrizen, deren Zeilen und/oder Spalten mehr als zwei Blöcke enthalten.

BEMERKUNG 5.42. Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen (siehe Beispiel 4.5). Die Elemente von $\mathbb{C}$ schreiben wir als $a + bi$ mit $a, b \in \mathbb{R}$.

Wir haben eine Bijektion

$$\iota\colon \mathbb{C} \to \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ;\ a, b \in \mathbb{R} \right\}$$

Dabei entsprechen die Addition und Multiplikation auf der linken Seite genau der Addition und Multiplikation von Matrizen auf der rechten Seite, das heißt für alle $z_1, z_2 \in \mathbb{C}$ gilt:

$$\iota(z_1 + z_2) = \iota(z_1) + \iota(z_2), \qquad \iota(z_1 z_2) = \iota(z_1)\iota(z_2).$$

Dies rechnet man unmittelbar anhand der Definitionen von Addition und Multiplikation auf den beiden Seiten nach. Zum Beispiel für die Multiplikation (der schwierigere Fall), mit $z_\lambda = a_\lambda + b_\lambda i, \lambda = 1, 2$:

$$\iota(z_1 z_2) = \begin{pmatrix} a_1 a_2 - b_1 b_2 & -(a_1 b_2 + a_2 b_1) \\ a_1 b_2 + a_2 b_1 & a_1 a_2 - b_1 b_2 \end{pmatrix}$$

und

$$\iota(z_1)\iota(z_2) = \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 & -a_1 b_2 - b_1 a_2 \\ b_1 a_2 + a_1 b_2 & -b_1 b_2 + a_1 a_2 \end{pmatrix}.$$

Es spielt dabei keine Rolle, ob wir schon wissen, dass $\mathbb{C}$ mit diesen Verknüpfungen ein Körper ist. Wir sehen auch, dass für zwei Matrizen von der oben betrachten Form (d.h., die im Bild von ι liegen), auch die Summe und das Produkt diese Form haben.

Wir können die Bijektion ι (und die Gültigkeit der Assoziativgesetze und des Distributivgesetzes in $M_2(\mathbb{R})$) benutzen, um zu beweisen, dass die Assoziativgesetze für $+$ und $\cdot$ und das Distributivgesetz in $\mathbb{C}$ gelten. Dazu bezeichnen wir mit ι^{-1} die Umkehrabbildung.

Nun folgt zum Beispiel das Assoziativgesetz der Multiplikation:

$$\begin{aligned}(z_1 z_2) z_3 &= \iota^{-1}(\iota((z_1 z_2) z_3)) = \iota^{-1}(\iota(z_1 z_2)\iota(z_3)) = \iota^{-1}((\iota(z_1)\iota(z_2))\iota(z_3)) \\ &= \iota^{-1}(\iota(z_1)(\iota(z_2)\iota(z_3))) = \iota^{-1}(\iota(z_1)\iota(z_2 z_3)) = \iota^{-1}(\iota(z_1(z_2 z_3))) = z_1(z_2 z_3).\end{aligned}$$

(Vergleichen Sie das mit der Methode, wie wir in Abschnitt 4.2.1 das Assoziativgesetz in $\mathbb{Z}$ und die kanonische Projektion $\mathbb{Z} \to \mathbb{Z}/n$ benutzt haben, um das Assoziativgesetz in $\mathbb{Z}/n$ zu beweisen.)

Für das Assoziativgesetz der Addition und das Distributivgesetz kann man genau dieselbe Methode anwenden, um diese auf die entsprechenden Aussagen in $M_2(\mathbb{R})$ zurückzuführen. ◊

5.3.3. Bild und Kern einer Matrix. Wir wollen in diesem Abschnitt beschreiben, wie wir einer Matrix $A \in M_{m\times n}(K)$ eine Abbildung $f_A\colon K^n \to K^m, x \mapsto Ax$, zuordnen können, und erklären, wie wir damit einige Aussagen über lineare Gleichungssysteme noch einmal umformulieren können. Diese neue Sichtweise ist ein wichtiger Spezialfall der Theorie der linearen Abbildungen, die wir in den Kapiteln 7 und 8 entwickeln werden. Diese beiden Kapitel stellen einen sehr wichtigen Teil der Vorlesung dar, so dass es die Zeit wert ist, uns an dieser Stelle schon ein bisschen darauf vorzubereiten.

Das Grundprinzip ist sehr einfach:

DEFINITION 5.43. Seien K ein Körper und $A \in M_{m\times n}(K)$ eine Matrix über K. Wir nennen die Abbildung

$$f_A\colon K^n \to K^m, \quad x \mapsto Ax,$$

die *durch A definierte Abbildung*. ⊣

Zwei wichtige Begriffe über Abbildungen der Form f_A sind das Bild (wie für jede Abbildung) und der Kern:

DEFINITION 5.44. Sei $A \in M_{m\times n}(K)$. Das *Bild von A*, in Zeichen $\operatorname{Im} A$, ist das Bild der Abbildung $f_A\colon K^n \to K^m$, d.h.

$$\operatorname{Im} A = \{y \in K^m;\ \text{es existiert } x \in K^n,\ \text{so dass } Ax = y\}.$$

⊣

DEFINITION 5.45. Sei $A \in M_{m\times n}(K)$. Der *Kern von A*, in Zeichen $\operatorname{Ker} A$, ist das Urbild des Elements $0 \in K^m$ unter der Abbildung f_A, d.h.

$$\operatorname{Ker} A = \{x \in K^n;\ Ax = 0\}$$

⊣

Wir können die neuen Sprechweisen benutzen, um in prägnanter Form über lineare Gleichungssysteme zu sprechen (und später, um die Theorie der linearen Gleichungssystem in natürlicher Weise in den allgemeinen Kontext einzuordnen):

SATZ 5.46. *Sei $A \in M_{m\times n}(K)$ eine Matrix.*

(1) *Der Teilraum* $\operatorname{Ker}(A)$ *ist die Lösungsmenge des homogenen linearen Gleichungssystems mit Koeffizientenmatrix A.*
(2) *Der Teilraum* $\operatorname{Im}(A)$ *ist die Menge aller $b \in K^m$, so dass das lineare Gleichungssystem mit erweiterter Koeffizientenmatrix $(A \mid b)$ eine Lösung besitzt.*

BEWEIS. Beide Teile sind direkte Übersetzungen der Definitionen $f_A(x) = Ax$, des Kerns und Bildes und der Tatsache, dass die Lösungsmenge des linearen Gleichungssystems mit erweiterter Koeffizientenmatrix $(A \mid b)$ die Menge $\{x \in K^n;\ Ax = b\}$ ist. □

Ein weiteres Indiz dafür, dass die Abbildungen der Form f_A gut zu den Strukturen passen, auf die wir beim Studium linearer Gleichungssysteme gestoßen sind, ist das folgende Lemma:

LEMMA 5.47. *Sei $A \in M_{m\times n}(K)$ eine Matrix. Dann gilt:*

(1) $\operatorname{Ker}(A)$ *ist ein Teilraum von K^n,*
(2) $\operatorname{Im}(A)$ *ist ein Teilraum von K^m.*

BEWEIS. zu (1). Das folgt mit dem vorherigen Satz aus Lemma 5.26. Natürlich lässt sich die Aussage auch leicht direkt nachrechnen.

zu (2). Wegen $f_A(0) = 0$ ist $0 \in \operatorname{Im}(f_A)$. Sind $v, w \in \operatorname{Im}(f_A)$, etwa $v = f_A(v')$, $w = f_A(w')$, so gilt

$$v + w = f_A(v') + f_A(w') = Av' + Aw' = A(v' + w') = f_A(v' + w') \in \operatorname{Im}(f_A).$$

Für $v = f_A(v')$ und $a \in K$ gilt $av = aAv' = A(av') = f_A(av') \in \operatorname{Im}(f_A)$. Damit haben wir alle Teilraumbedingungen überprüft. □

Wir können jetzt Frage 5.27 (2) als die Frage formulieren, ob wir beschreiben können, »wie groß« die Teilräume $\operatorname{Ker}(f_A)$ und $\operatorname{Im}(f_A)$ sind, und einen Zusammenhang dazwischen herstellen können.

Die Verknüpfung von Abbildungen der Form f_A ist gerade durch das Matrizenprodukt gegeben. Das liefert eine weitere Rechtfertigung für die Definition des Matrizenprodukts, so wie wir sie gegeben haben.

SATZ 5.48. *Seien $A \in M_{l\times m}(K)$, $B \in M_{m\times n}$. Dann gilt*

$$f_A \circ f_B = f_{AB}.$$

BEWEIS. Dies folgt aus der Assoziativität des Matrizenprodukts, wie die folgende Rechnung zeigt:

$$(f_A \circ f_B)(x) = f_A(f_B(x)) = A(Bx) = (AB)x = f_{AB}(x)$$

für alle $x \in K^n$. □

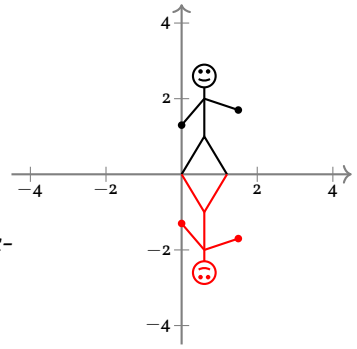
BEISPIEL 5.49. Sei $K = \mathbb{R}$. In diesem Fall kann man die Abbildungen f_A geometrisch interpretieren. Im Fall $n = 2$ (und mit gewissen Grenzen im Fall $n = 3$) kann man das auch graphisch gut veranschaulichen. In den Abbildungen unten ist jeweils die rote Figur das Bild der schwarzen Figur unter der betrachteten Abbildung.

(1)

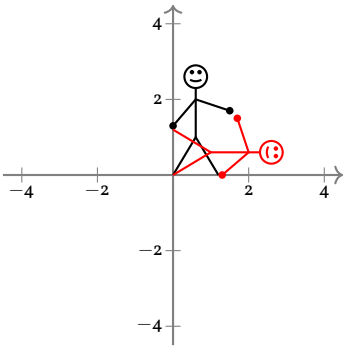
Sei $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Dann gilt

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}$$

und diese Abbildung ist einfach die *Spiegelung an der x-Achse*.



(2)

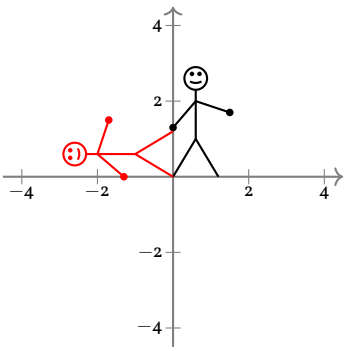


Sei $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Dann gilt

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$$

und diese Abbildung ist die *Spiegelung an der Diagonalen*. Jede Spiegelung an einer Ursprungsgeraden in $\mathbb{R}^2$ kann in der Form f_A dargestellt werden. Können Sie für eine gegebene Gerade $g = \{(x,y)^t \in \mathbb{R}^2;\ ax + by = 0\}$, $a, b \in \mathbb{R}$, die Matrix A ausrechnen, für die f_A die Spiegelung an g ist?

(3)



Sei $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Dann gilt

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix}$$

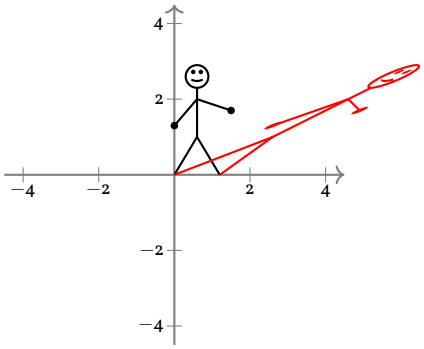
und diese Abbildung ist die *Drehung um 90° gegen den Uhrzeigersinn*.
Können Sie auch die Drehung um 180° und um 270° gegen den Uhrzeigersinn in der Form f_A für geeignete Matrizen A darstellen? Wir werden später sehen, dass sich alle Drehungen um den Ursprung in der Form f_A darstellen lassen, siehe Beispiel 8.6.

(4)

Sei $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Dann gilt

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y + 2x \end{pmatrix}$$

und diese Abbildung nennt man eine *Scherung*.

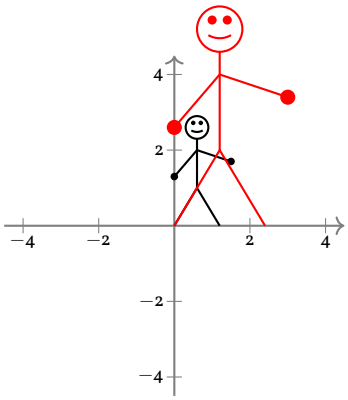


(5)

Sei $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. Dann gilt

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 2y \end{pmatrix}.$$

Diese Abbildung nennt man eine *Streckung* (um den Faktor 2).
Wie würden Sie die Abbildung f_A beschreiben, wenn $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ mit $a < 0$ ist? Was macht f_A, wenn A eine Diagonalmatrix mit verschiedenen Werten auf der Diagonale ist? Was passiert, wenn eine Null auf der Diagonale steht?



◊

Auf dieser Webseite[a] können Sie das ausprobieren.

[a] https://math.ug/applets/lineare-abbildungen-1.html

Wir werden die Abbildungen der Form f_A in den Kapiteln 7 und 8 genauer untersuchen und dann unter anderem charakterisieren können, welche Abbildungen $K^n \to K^m$ in dieser Art beschrieben werden können.

5.3.4. Invertierbare Matrizen. Wir haben schon besprochen, dass elementare Zeilenumformungen sich als Multiplikation mit einer Matrix von links beschreiben lassen, und dass sie umkehrbar sind. Wenn S die Matrix zu einer elementaren Zeilenumformung von A ist, dann gibt es eine Matrix S', die ebenfalls eine elementare Zeilenumformung beschreibt, so dass $S'SA = A$. Das führt uns auf die folgende Definition:

DEFINITION 5.50. Eine quadratische Matrix $A \in M_{n\times n}(K)$ heißt *invertierbar*, wenn eine Matrix $B \in M_{n\times n}(K)$ existiert mit

$$AB = BA = E_n.$$

⊣

LEMMA 5.51. *Sei $A \in M_{n\times n}(K)$ eine invertierbare Matrix. Dann gibt es* genau eine *Matrix $B \in M_{n\times n}(K)$ mit $AB = BA = E_n$. Wir bezeichnen sie mit A^{-1} und nennen sie die zu A inverse Matrix. Es ist dann auch B invertierbar, und $B^{-1} = A$.*

BEWEIS. Seien B und B' gegeben mit $AB = B'A = E_n$. (Wir brauchen also jeweils nur die eine Hälfte der definierenden Eigenschaft, allerdings einmal die Rechts- und einmal die Linksversion.) Dann gilt

$$B = E_n B = (B'A)B = B'(AB) = B'E_n = B'.$$

Der zweite Teil der Behauptung ist dann klar. □

Wenn die Matrix A invertierbar ist, dann können wir aus dem Ergebnis $C = AB$ einer Matrizenmultiplikation die Matrix B zurückgewinnen: $B = A^{-1}C$.

LEMMA 5.52. *Seien $A, B \in M_n(K)$ invertierbar. Dann ist auch das Produkt AB invertierbar und es gilt*

$$(AB)^{-1} = B^{-1}A^{-1}.$$

BEWEIS. Es gilt $(AB)(B^{-1}A^{-1}) = E_n = (B^{-1}A^{-1})(AB)$. □

BEISPIEL 5.53. Wir benutzen die Notation von Bemerkung 5.37. Sei K ein Körper, $n \in \mathbb{N}$, $1 \leq i, j \leq n, i \neq j, a \in K$.

(1) Es gilt $E_{ij}(a)^{-1} = E_{ij}(-a)$.

(2) Es gilt $P_{ij}^{-1} = P_{ij}$.

(3) Eine Diagonalmatrix $\operatorname{diag}(a_1, \ldots, a_n)$ mit $a_i \in K$ ist genau dann invertierbar, wenn $a_i \neq 0$ für alle $i = 1, \ldots, n$ gilt. In diesem Fall ist

$$\operatorname{diag}(a_1, \ldots, a_n)^{-1} = \operatorname{diag}(a_1^{-1}, \ldots, a_n^{-1})$$

Insbesondere ist für $a \neq 0$: $\operatorname{diag}(1, \ldots, 1, a, 1, \ldots, 1)^{-1} = \operatorname{diag}(1, \ldots, 1, a^{-1}, 1, \ldots, 1)$.

Wir sehen erneut, dass elementare Zeilenumformungen die Lösungsmenge des zugehörigen homogenen linearen Gleichungssystems nicht ändern, denn für jede invertierbare Matrix S ist $Ax = 0$ äquivalent zu $SAx = 0$. ◊

SATZ 5.54. *Seien K ein Körper, $n \in \mathbb{N}$ und $A \in M_n(K)$. Dann sind äquivalent:*

(i) *Die Matrix A ist invertierbar.*

(ii) *Die reduzierte Zeilenstufenform von A ist E_n.*

Erinnern Sie sich, dass wir in Korollar 5.22 die Eigenschaft von A, reduzierte Zeilenstufenform E_n zu haben, in Termen von linearen Gleichungssystemen umgeschrieben haben. Dies werden wir im Beweis des Satzes benutzen.

BEWEIS. Wenn A invertierbar ist, dann ist $Ax = 0$ äquivalent zu $x = A^{-1}0 = 0$, das homogene lineare Gleichungssystem zu A ist daher eindeutig lösbar. Aus Korollar 5.22 folgt, dass A reduzierte Zeilenstufenform E_n hat.

Nun habe A reduzierte Zeilenstufenform E_n. Dann gibt es elementare Zeilenumformungen, die A in die Einheitsmatrix umformen. Wir können diese als Multiplikation mit Matrizen $S_1, S_2, \ldots, S_l$ ausdrücken:

$$S_l S_{l-1} \cdots S_1 A = E_n.$$

Wir haben in Beispiel 5.53 gesehen, dass alle S_i invertierbar sind. Also können wir mit ihren Inversen von links multiplizieren und erhalten

$$A = S_1^{-1} S_2^{-1} \cdots S_l^{-1} E_n.$$

Die rechte Seite ist invertierbar und genauer erhalten wir

$$A^{-1} = S_l \cdots S_1.$$

□

Wenn wir am Schluss das Beweises $A^{-1} = S_l \cdots S_1 E_n$ schreiben, dann liefert uns dies direkt einen Algorithmus, um A^{-1} zu berechnen: Wenn wir A durch elementare Zeilenumformungen, die durch die Matrizen $S_1, \ldots, S_l$ beschrieben werden, auf die Einheitsmatrix bringen können, dann bringen *genau dieselben* Zeilenumformungen die Einheitsmatrix auf die Matrix A^{-1}.

BEISPIEL 5.55. Um das Verfahren zum bestimmen des Inversen einer Matrix $A \in M_n(K)$ in der Praxis durchzuführen, schreibt man A und E_n nebeneinander in eine $(n \times 2n)$-Matrix. Etwas übersichtlicher wird es, wenn man in der Mitte einen senkrechten Strich mitführt. Dann bringt man mit elementaren Zeilenumformungen die Matrix A auf reduzierte Zeilenstufenform und führt die Umformungen immer für die gesamte Matrix durch. Ist das Ergebnis der reduzierten Zeilenstufenform von A die Einheitsmatrix, dann ist A invertierbar, und die rechte Hälfte der so erhaltenen Matrix ist A^{-1}. Erhält man eine andere Matrix als E_n als reduzierte Zeilenstufenform von A, so ist die Matrix A nicht invertierbar.

Ein konkretes Beispiel: Sei $K = \mathbb{Q}$, $n = 3$ und

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 3 & 1 & 0 \end{pmatrix}.$$

Wir bringen nun in der Matrix

$$(A \mid E_3) = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

die linke Hälfte durch elementare Zeilenumformungen auf reduzierte Zeilenstufenform:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{Z_2 \rightsquigarrow Z_2 - 2Z_1,\ Z_3 \rightsquigarrow Z_3 - 3Z_1}$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & -2 & 1 & 0 \\ 0 & -2 & 0 & -3 & 0 & 1 \end{array}\right) \xrightarrow{Z_3 \rightsquigarrow Z_3 - Z_2,\ Z_2 \rightsquigarrow -\frac{1}{2} Z_2}$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -\frac{1}{2} & 1 & -\frac{1}{2} & 0 \\ 0 & 0 & -1 & -1 & -1 & 1 \end{array}\right) \xrightarrow{Z_3 \rightsquigarrow -Z_3,\ Z_2 \rightsquigarrow Z_2 + \frac{1}{2} Z_3,\ Z_1 \rightsquigarrow Z_1 - Z_2}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 & \frac{3}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & 1 & 1 & -1 \end{array}\right)$$

Wir erhalten

$$A^{-1} = \begin{pmatrix} -\frac{1}{2} & 0 & \frac{1}{2} \\ \frac{3}{2} & 0 & -\frac{1}{2} \\ 1 & 1 & -1 \end{pmatrix}.$$

Es bietet sich bei dieser Rechnung an, die Probe durchzuführen: Das Produkt AA^{-1} muss die Einheitsmatrix ergeben. ◊

BEISPIEL 5.56. Seien K ein Körper und $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine 2×2-Matrix.

Wir setzen $\delta(A) = ad - bc$. Wir haben in Abschnitt 2.5 gesehen, dass das homogene lineare Gleichungssystem zu A genau dann eindeutig lösbar ist, wenn $\delta(A) \neq 0$ gilt. Aus Satz 5.54 und Korollar 5.22 folgt damit, dass

$$A \text{ ist invertierbar} \iff \delta(A) \neq 0.$$

In diesem Fall gilt

$$A^{-1} = \frac{1}{\delta(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Um das zu sehen, muss man nur nachrechnen, dass $AA^{-1} = E_2$ gilt, und das ist eine leichte Rechnung.

Den Ausdruck $\delta(A)$ nennt man auch die *Determinante* der Matrix A (und später schreiben wir $\det(A)$ statt $\delta(A)$). Siehe Kapitel 10 für eine systematische Diskussion und die Verallgemeinerung auf quadratische Matrizen beliebiger Größe. ◊

LEMMA 5.57. *Sei $A \in M_{n\times n}(K)$ eine invertierbare Matrix. Dann ist auch die transponierte Matrix A^t invertierbar, und es gilt*

$$(A^t)^{-1} = (A^{-1})^t.$$

BEWEIS. Wir haben $A^t(A^{-1})^t = (A^{-1}A)^t = E_n^t = E_n$ nach Lemma 5.40, analog $(A^{-1})^t A^t = E_n$, und zusammen das zeigt die Behauptung. □

Das folgende Korollar ist tiefliegender als es erscheinen mag. Wir werden auf diese Aussage später wieder zurückkommen (und einen anderen Beweis geben), siehe Korollar 7.23.

KOROLLAR 5.58. *Sei $A \in M_{n\times n}(K)$ eine Matrix.*

(1) *Wenn eine Matrix $B \in M_{n\times n}(K)$ existiert mit $AB = E_n$, dann ist A invertierbar und $A^{-1} = B$.*
(2) *Wenn eine Matrix $B \in M_{n\times n}(K)$ existiert mit $BA = E_n$, dann ist A invertierbar und $A^{-1} = B$.*

BEWEIS. zu (1). Es genügt zu zeigen, dass A invertierbar ist; es ist dann klar, dass $B = A^{-1}$ gelten muss. Für die Invertierbarkeit genügt es wegen Satz 5.54 und Korollar 5.22 zu zeigen, dass das lineare Gleichungssystem $Ax = b$ für alle $b \in K^n$ lösbar ist. Das folgt aber unmittelbar aus der Voraussetzung, denn wir setzen einfach $x = Bb$ und erhalten $Ax = A(Bb) = E_n b = b$.

zu (2). Für diesen Teil können wir wieder Satz 5.54 und Korollar 5.22 anwenden und zeigen diesmal, dass das homogene lineare Gleichungssystem $Ax = 0$ eindeutig lösbar ist. In der Tat, ist $x \in K^n$ mit $Ax = 0$, so folgt $x = E_n x = BAx = 0$.

Alternativ kann man Teil (2) aus Teil (1) (oder auch umgekehrt) durch den Übergang zu den transponierten Matrizen erhalten. □

Wir können nun auch noch einmal auf die Eindeutigkeit der reduzierten Zeilenstufenform zurückkommen:

SATZ 5.59. *Die reduzierte Zeilenstufenform einer Matrix $A \in M_{m\times n}(K)$ ist eindeutig bestimmt, also unabhängig von der Wahl der elementaren Zeilenumformungen.*

BEWEIS. Seien A' und A'' Matrizen in reduzierter Zeilenstufenform, die beide aus A durch elementare Zeilenumformungen erhalten werden können. Dann gibt es invertierbare Matrizen S' und S'' mit $A' = S'A$ und $A'' = S''A$, also

$$A' = S'(S'')^{-1}A''.$$

Wir bezeichnen mit B die Matrix, die aus den Spalten von A' besteht, die eine führende Eins enthalten. Alle anderen Spalten lassen wir weg. Ist r die Anzahl der führenden Einsen in A', so ist $B \in M_{n\times r}(K)$. Wir wissen bereits, dass sich in A' und A'' die Spalten mit führenden Einsen an denselben Positionen befinden. Deshalb erhalten wir genau dasselbe Ergebnis, wenn wir B in der gleichen Art und Weise aus A'' statt aus A' konstruieren, und es folgt

$$B = S'(S'')^{-1}B.$$

Die Matrix B hat eine sehr einfache Form, es handelt sich um eine Blockmatrix, die aus der Einheitsmatrix E_r und der Nullmatrix der Größe $(n-r)\times r$ zusammengesetzt ist: $B = \begin{pmatrix} E_r \\ 0 \end{pmatrix}$ (und die Zeilen unterhalb der r-ten Zeilen sind auch in A' und A'' Nullzeilen).

Die Gleichheit $B = S'(S'')^{-1}B$ übersetzt sich damit in

$$S'(S'')^{-1} = \begin{pmatrix} E_r & * \\ 0 & * \end{pmatrix},$$

wobei das obere Sternchen eine Matrix in $M_{r\times(n-r)}(K)$ und das untere eine in $M_{(n-r)\times(n-r)}(K)$ bezeichnen, über die wir nichts Genaueres zu sagen brauchen.

Weil die Zeilen unterhalb der r-ten Zeile in A' und A'' sowieso Nullzeilen sind, genügt es zu zeigen, dass die ersten r Zeilen übereinstimmen. Wir schreiben (nur für diesen Beweis) $M_{\leq r}$ für die Matrix, die aus den ersten r Zeilen der Matrix M besteht. Dann haben wir

$$(A')_{\leq r} = (S'(S'')^{-1}A'')_{\leq r} = (S'(S'')^{-1})_{\leq r}A'' = \begin{pmatrix} E_r & * \end{pmatrix}\begin{pmatrix} (A'')_{\leq r} \\ 0 \end{pmatrix} = (A'')_{\leq r},$$

wobei wir ausgiebig von der Schreibweise als Blockmatrizen Gebrauch gemacht haben (Abschnitt 5.3.2 und Lemma 5.41). □

5.3.5. Ergänzungen *

Beispiel 5.60. Wir betrachten die Folge $(F_n)_{n\geq 0}$ der Fibonacci Zahlen, die definiert ist durch

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2},\ n \geq 2.$$

Wir können die rekursive Definition durch die folgenden Matrixgleichungen formulieren:

$$\begin{pmatrix} F_1 \\ F_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} F_{n-1} \\ F_{n-2} \end{pmatrix}.$$

Setzen wir

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

so erhalten wir dadurch

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A^n\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Dies kann man ausnutzen, um »schnell« eine Fibonacci-Zahl F_n für großes n zu berechnen, ohne alle vorherigen Fibonacci-Zahlen berechnen zu müssen. Denn die Potenz A^n kann man in wesentlich weniger als n Schritten ausrechnen: Wir schreiben $n = \sum_{i=0}^{r} a_i \cdot 2^i$ mit $a_i \in \{0,1\}$, $a_r \neq 0$ (dies ist die Binärdarstellung der Zahl n). Zuerst berechnet man A^2, dann $A^4 = A^2\cdot A^2$, und alle weiteren Potenzen A^{2^i} für $i \leq r$. Dies erfordert nur r Matrixmultiplikationen. Dann berechnen wir A^{n-1} als Produkt derjenigen Matrizen A^{2^i}, für die $a_i = 1$ ist.

Ist zum Beispiel $n = 16781841 = 2^{24} + 2^{12} + 2^9 + 2^4 + 2^0$, so brauchen wir mit diesem Rezept für die Berechnung von F_n nur 28 Produkte von (2×2)-Matrizen auszurechnen. Das wäre notfalls noch per Hand machbar (im Gegensatz zu n Additionen, die bei einer Geschwindigkeit von einer Addition pro Sekunde fast 200 Tage dauern würden – wenn Sie rund um die Uhr addieren).

Die Darstellung mithilfe der Matrix A kann man auch benutzen, um Identitäten zwischen verschiedenen Gliedern der Fibonacci-Folge herzuleiten. Dazu bemerken wir zunächst, dass für $n \geq 1$

$$A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix},$$

wie man unmittelbar per Induktion nachprüft. Damit folgt zum Beispiel für $m, n \geq 1$ aus der Gleichheit $A^{m+n} = A^m A^n$, dass

$$\begin{pmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{pmatrix} = A^m A^n = \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix} \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Nehmen wir nun auf beiden Seiten den Eintrag in der zweiten Zeile und ersten Spalte, so erhalten wir die Formel

$$F_{m+n} = F_m F_{n+1} + F_{m-1} F_n.$$

Durch Spezialisierung erhält man viele verschiedene Identitäten zwischen den Fibonacci-Zahlen, zum Beispiel für $m = n$: $F_{2n} = (F_{n+1} + F_{n-1})F_n$. ◊

ERGÄNZUNG 5.61 (Der Page-rank-Algorithmus, Fortsetzung). Dies ist die Fortsetzung der Diskussion aus Frage 2.7. Wir bezeichnen wie dort mit x_i, $i = 1, \ldots, N$, die Zahlen die wir suchen, um die »Relevanz« von Webseiten zu beschreiben, mit L_i die Menge aller Seiten, die einen Link auf Seite i enthalten, und mit n_j die Zahl der von Seite j ausgehenden Links. Wir arbeiten über dem Körper $K = \mathbb{R}$.

Der aktuelle Diskussionsstand ist, dass die x_i das lineare Gleichungssystem

$$x_i = \sum_{j \in L_i} \frac{1}{n_j} x_j, \qquad i = 1, \ldots, N,$$

erfüllen sollen.

Wir suchen eine Lösung, in der $0 \leq x_i < 1$ für alle i und $\sum x_i = 1$ gilt, und zwar sollte es *genau eine* Lösung mit dieser Eigenschaft geben. Durch die Zusatzeigenschaften können wir die x_i auch als Wahrscheinlichkeit deuten, dass jemand, der im Internet surft und immer zufällig irgendeinem Link folgt, sich gerade auf der Seite i befindet.

Sei H die Matrix mit Einträgen

$$H_{ij} = \begin{cases} \frac{1}{n_j} & j \in L_i, \\ 0 & \text{sonst.} \end{cases}$$

Dann können wir das obige lineare Gleichungssystem schreiben als $(H - E_N)x = 0$, wobei $x = (x_i)_i \in K^N$.

Es gibt noch zwei »offensichtliche« Probleme mit diesem Ansatz:

- Es lassen sich leicht Beispiele finden, in denen dieses homogene lineare Gleichungssystem keine nicht-triviale Lösung hat, und zwar dann, wenn es Seiten gibt, die gar keine Links enthalten. Zum Beispiel ein »Internet« mit drei Seiten und den Links $1 \to 2$, $2 \to 1$, $2 \to 3$. In diesem Fall würde der Ansatz scheitern.

  Wir wollen dieses Problem so lösen, dass wir in jeder Nullspalte der Matrix H alle Einträge durch $\frac{1}{N}$ ersetzen. Mit der Interpretation als Wahrscheinlichkeiten können wir uns das so vorstellen, dass die Surfer∗in von einer Seite, die keine Links enthält, zufällig irgendeine Seite im Netz auswählt, und allen Seiten dieselbe Wahrscheinlichkeit zugewiesen wird.

  Wenn wir H so abändern:

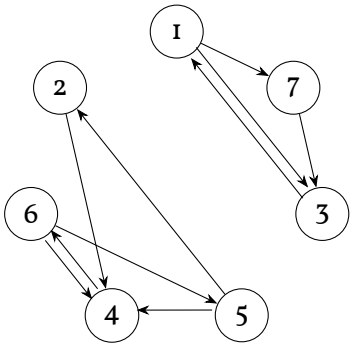
$$H_{ij} = \begin{cases} \frac{1}{n_j} & j \in L_i, \\ \frac{1}{N} & \text{wenn kein } i' \text{ existiert mit } j \in L_{i'}, \\ 0 & \text{sonst,} \end{cases}$$

  dann hat die Matrix H die Eigenschaft, dass alle Spaltensummen in H gleich 1 sind, d.h. $\sum_{i=1}^{N} H_{ij} = 1$ für alle j.

  In den Spalten, die vorher Nullspalten waren, ist das klar, weil nun dort alle N Einträge den Wert $\frac{1}{N}$ haben. In den anderen Spalten ist die Spaltensumme $\sum \frac{1}{n_j}$, wobei über alle

i mit $j \in L_i$ summiert wird, also über alle Seiten i, auf die die Seite j verlinkt, und nach Definition gibt es genau n_j solche Seiten.

- Stellen Sie sich vor, dass das »Netz« von Webseiten, das wir betrachten, verschiedene Komponenten hat, zwischen denen man nicht durch Links hin- und hergelangen kann:



In diesem Fall ist es klar, dass die gegebenen Daten keinen vernünftigen Anhaltspunkt liefern, um die Relevanz von Seiten, die in verschiedenen solchen Komponenten liegen, zu vergleichen. Das Internet hat sehr viele Komponenten, so dass man dieses Problem nicht einfach ignorieren kann.

Der Trick, mit dem wir uns (bzw. Google sich) behelfen, ist dass wir die Matrix H ersetzen durch die Matrix

$$G := dH + (1-d)A,$$

wobei A die Matrix ist, deren Einträge alle gleich $\frac{1}{N}$ sind, und wobei d eine Zahl ist, die zwischen 0 und 1 liegt. Je näher d bei 1 liegt, desto geringer ist der Unterschied zwischen G und H. Interessanterweise ist es für die Qualität des Algorithmus aber sogar hilfreich, d nicht zu nahe bei 1 zu wählen. Google hat ursprünglich den Wert $d = 0,85$ benutzt.

Das passt auch gut zur Interpretation der x_i als Aufenthaltswahrscheinlichkeiten: Es bedeutet, dass die Surfer∗in mit Wahrscheinlichkeit $1-d$ (also im Beispiel 15%) nicht einem Link auf der Seite folgt, sondern auf irgendeine zufällige Seite im Netz springt.

Wir haben damit die endgültige mathematische Formulierung des Page-Rank-Algorithmus erhalten: Wir möchten das lineare Gleichungssystem $(G - E_N)x = 0$ lösen. In der Matrix G (der »Google-Matrix«) sind alle Einträge positiv, und die Spaltensummen sind alle gleich 1. Während das nützliche Eigenschaften der Matrix G sind, ist andererseits diese Matrix *extrem groß*, so groß, dass es aussichtslos ist, einfach den Gauß-Algorithmus auszuführen.

Wir werden später sehen, dass die Lösungsmenge des homogenen linearen Gleichungssystems $(G - E_N)x = 0$ aus den Vielfachen eines einzigen Vektors $x \neq 0$ besteht. Bis auf Skalieren gibt es also eine *eindeutig bestimmte Lösung*. Genauer werden wir den folgenden Satz beweisen (vergleiche Beispiel 2.8):

SATZ 5.62. *Es gibt genau eine Lösung $x \in \mathbb{R}^N$ des linearen Gleichungssystems $(G - E_N)x = 0$ mit der Eigenschaft $\sum_{i=1}^{N} x_i = 1$, und für diese Lösung gilt $0 \leq x_i \leq 1$ für alle i.*

(Ist $x' \in K^N$ ein Element, das auch $(G - E_N)x' = 0$ erfüllt, so existiert $\lambda \in \mathbb{R}$ mit $x' = \lambda x$.)

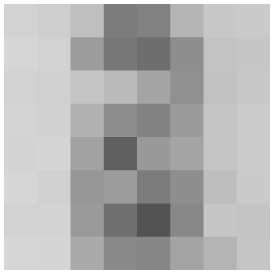
Den Beweis geben wir wie gesagt später, siehe Satz 8.19. Immerhin können wir an dieser Stelle schon Folgendes sehen: Wären die Zeilensummen von G alle $= 1$ (statt der Spaltensummen), so wäre klar, dass das homogene lineare Gleichungssystem mit Koeffizientenmatrix $G - E_N$ eine nicht-triviale Lösung hat (warum?). (Und die Eindeutigkeit ist auch nicht extrem schwierig, wie wir später sehen werden.) Mit ein bisschen mehr Theorie wird es uns leicht fallen, zwischen diesen beiden Bedingungen (Spaltensummen bzw. Zeilensummen) eine Verbindung herzustellen. □ Ergänzung 5.61

Abbildung 1. Das Originalfoto

Ergänzung 5.63 (Bildkompression). In dieser Ergänzung besprechen wir eine Methode der Bildkompression mit dem sogenannten Haar-Wavelet. Wir beschränken uns darauf, die Grundidee zu erklären. In der Praxis kann man das Verfahren noch weiter verbessern. Es gibt auch andere sehr gute Kompressionsverfahren, die auf linearer Algebra beruhen, zum Beispiel auf der Singulärwertzerlegung, die wir in der Linearen Algebra 2 kennenlernen werden.

Um das Prinzip zu erläutern und zu illustrieren, beschränken wir uns auf ein Schwarz-Weiß-Bild. Man kann aber genau dieselbe Überlegung auf Farbbilder anwenden, indem man das Bild in mehrere Farben aufspaltet, beispielsweise in Rot, Grün und Blau (RGB), und dann die drei Farben separat behandelt.

Wir betrachten ein Bild (Abbildung 1) mit 512×512 Punkten (»Pixeln«), die jeweils einen Grauwert haben, der durch eine natürliche Zahl zwischen 0 und 255 gegeben ist. Dabei ist 0 gleich schwarz, und 255 ist gleich weiß. Um die Bildinformation in dieser vollständigen Form abzuspeichern, müssen also ca. 260 000 dieser Grauwerte abgespeichert werden, jeder Wert benötigt ein »Byte« an Speicherplatz. Insgesamt brauchen wir also ca. 260 Kilobyte für dieses Bild, wenn keine Kompression angewandt wird. (Nehmen Sie statt dieses kleinen Beispiels ein Bild mit beispielsweise 8MP und 3 Farben, so bräuchte man 24 Megabyte, um das Bild abzuspeichern.)



Die Grundidee aller Kompressionsverfahren ist es, auszunutzen, dass es in einem typischem Bild viele Bereiche gibt, die mehr oder weniger einfarbig sind, d.h. benachbarte Punkte haben sehr ähnliche Farbwerte bzw. in unserem Fall Grauwerte.
Für das hier vorgestellte Verfahren teilen wir das Bild in Blöcke von 8×8 Pixeln auf und behandeln jeden Block einzeln. Ein vergrößerter 8×8-Block aus dem Originalbild ist hier dargestellt.

Wir nehmen nun einen dieser Blöcke her und beginnen damit, die erste Zeile des Blocks folgendermaßen umzuformen: Wir fassen die 8 Werte als 4 Paare auf, d.h. die ersten beiden Einträge bilden das erste Paar, der dritte und vierte Eintrag das zweite Paar, usw. Für jedes dieser Paare (a, b) bilden wir den Durchschnitt $\frac{a+b}{2}$ und den Wert $\frac{a-b}{2}$. Aus diesen Werten

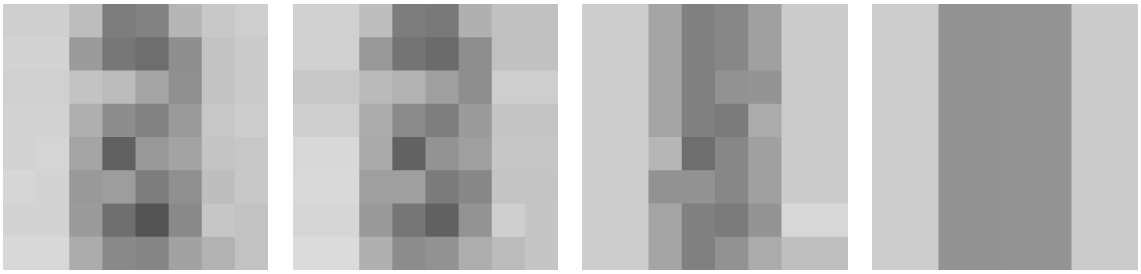


ABBILDUNG 2. Das Ergebnis, das aus dem vorher gezeigten Block von 8×8 Pixeln wird, wenn alle Werte < 1, bzw. < 4, bzw. < 10, bzw. < 18 auf Null gesetzt werden.

kann man a und b zurückgewinnen als

$$a = \frac{a+b}{2} + \frac{a-b}{2}, \quad b = \frac{a+b}{2} - \frac{a-b}{2},$$

aber diese Ersetzung hat für uns den Vorteil, dass tendenziell oft $\frac{a-b}{2}$ eine kleine Zahl sein wird (sogar gleich Null, wenn $a = b$), weil typischerweise a und b nahe beieinander liegen. Wir schreiben das Ergebnis wieder als eine Zeile mit 8 Einträgen, wobei wir zuerst die 4 Durchschnittswerte aufschreiben, und dann die 4 Terme der zweiten Form.

Mit anderen Worten: Wir ersetzen die Zeile $v = (v_1, \ldots, v_8)$ durch

$$\left(\frac{v_1+v_2}{2}, \frac{v_3+v_4}{2}, \frac{v_5+v_6}{2}, \frac{v_7+v_8}{2}, \frac{v_1-v_2}{2}, \frac{v_3-v_4}{2}, \frac{v_5-v_6}{2}, \frac{v_7-v_8}{2} \right)$$

Das können wir auch als ein Matrizenprodukt ausdrücken: Wir ersetzen den Zeilenvektor v durch das Produkt vH_1, wobei

$$H_1 = \begin{pmatrix} 0,5 & & & 0,5 & & & & \\ 0,5 & & & -0,5 & & & & \\ & 0,5 & & & 0,5 & & & \\ & 0,5 & & & -0,5 & & & \\ & & 0,5 & & & 0,5 & & \\ & & 0,5 & & & -0,5 & & \\ & & & 0,5 & & & 0,5 & \\ & & & 0,5 & & & -0,5 & \end{pmatrix}$$

Im zweiten Schritt wenden wir dasselbe Verfahren noch einmal auf die ersten 4 Einträge der neuen Zeile an: Wir teilen diese in zwei Paare auf, und schreiben dann an die ersten beiden Stellen die Durchschnittswerte des ersten und zweiten Paares, und an die dritte und vierte Stelle die Hälfte der Differenzen. Auch dies können wir als Produkt mit einer Matrix ausdrücken, und zwar mit

$$H_2 = \begin{pmatrix} 0,5 & & 0,5 & & & & & \\ 0,5 & & -0,5 & & & & & \\ & 0,5 & & 0,5 & & & & \\ & 0,5 & & -0,5 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}$$

Zum Schluss machen wir das ganze noch einmal für die ersten beiden Einträge der neuen Zeile, das heißt wir multiplizieren mit

$$H_3 = \begin{pmatrix} 0,5 & 0,5 & & & & & & \\ 0,5 & -0,5 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}$$

Insgesamt ersetzen wir also v durch $vH_1H_2H_3$. Setzen wir $H := H_1H_2H_3$, so wird v durch vH ersetzt. Für die anderen Zeilen machen wir dasselbe, das bedeutet, dass wir den Block A, aufgefasst als (8×8)-Matrix, ersetzen durch AH. Wie oben erwähnt, lässt sich diese Operation auch wieder umkehren (bis jetzt haben wir also keine Information verloren): die Umkehrung erhält man durch Multiplikation mit der inversen Matrix H^{-1}.

Zum Schluss führen wir dasselbe Verfahren für alle Spalten des neu erhaltenen Blocks durch. Das bedeutet, dass wir AH ersetzen durch H^tAH, wobei H^t die zu H transponierte Matrix bezeichnet. In derselben Weise formt man nun alle (8×8)-Blöcke der Bilddatei um.

Bis zum jetzigen Zeitpunkt haben wir die vorhandene Information nur in eine andere Form gebracht und können die Ausgangsdaten vollständig rekonstruieren. Trotzdem ergibt sich in der Regel auch dadurch schon die Möglichkeit, die Daten platzsparender abzuspeichern, weil die neue 512×512-Matrix in der Regel viele Nulleinträge haben wird. Dann kann man »sich merken«, dass gewisse Bereiche gleich Null sind, statt jeden Eintrag einzeln zu speichern.

Seine volle Kraft entfaltet das Verfahren allerdings, wenn man in H^tAH alle Einträge auf Null setzt, deren Absolutbetrag kleiner ist als ein vorgegebener Wert, beispielweise alle Einträge, die betragsmäßig kleiner sind als 1. Dadurch erhält man normalerweise einen deutlich größeren Anteil an Nullen, so dass die Matrix wesentlich platzsparender abgespeichert werden kann, siehe die Abbildungen 2, 3. Trotzdem kann man, wenn man es nicht übertreibt, das ursprüngliche Bild ohne großen Qualitätsverlust zurückgewinnen, wenn man dasselbe Verfahren zur Rücktransformation anwendet.

Es ist zwar nicht zwingend, dieses Verfahren mithilfe des Matrizenprodukts zu beschreiben, und die ganze Sache ist auch mathematisch nicht sehr tiefliegend. Sie ist aber in der Praxis nützlich, lässt sich wie schon angedeutet auch noch weiter verbessern, und die Formulierung mit dem Matrizenprodukt ist einerseits eine klare und einfache Beschreibung, und ermöglicht es andererseits, auf die Theorie des Matrizenprodukts zurückzugreifen, und für die praktische Implementierung Programmbibliotheken zu benutzen, in denen schnelle Matrizenoperationen zur Verfügung gestellt werden.

Quelle: [**VK**]. □ Ergänzung 5.63

ERGÄNZUNG 5.64 (Quaternionen, Fortsetzung). Wir können nun auch noch einmal auf die Hamiltonschen Quaternionen zurückkommen (siehe Ergänzung 4.11) und erklären, wie man recht einfach zeigen kann, dass $\mathbb{H}$ ein Schiefkörper ist. Wir betrachten die injektive (warum?) Abbildung

$$\iota\colon \mathbb{H} \to M_2(\mathbb{C}), \qquad (a,b,c,d) \mapsto \begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix}.$$

Es ist leicht nachzurechnen, dass ι verträglich ist mit der Addition und Multiplikation in $\mathbb{H}$ und in $M_2(\mathbb{C})$:

$$\iota(x+y) = \iota(x) + \iota(y), \quad \iota(xy) = \iota(x)\iota(y).$$

ABBILDUNG 3. Von links oben nach rechts unten die »komprimierten« Fotos, wo alle Werte < 1, bzw. < 4, bzw. < 10, bzw. < 18 auf 0 gesetzt wurden. Damit wurden ca. 68%, bzw. 86%, bzw. 93%, bzw. 96% der Einträge in der beschreibenden Matrix zu Null.

Im dritten und vierten Bild sieht man bereits die deutlich niedrigere Qualität, an mehreren Stellen zeigen sich »Kompressionsartefakte«. Allerdings wurde die Datenmenge in diesen Fällen auch sehr stark verkleinert. Natürlich müsste man nun, wenn man die Qualität dieses Kompressionsverfahrens bewerten wollte, Vergleiche mit anderen Verfahren durchführen, insbesondere mit dem »naiven« Ansatz, die Datenmenge dadurch zu verkleinern, dass man das Bild auf eine kleinere Auflösung herunterrechnet. Das würde hier ein bisschen zu weit führen, aber ich stelle gerne den Python-Code zur Verfügung, wenn Sie diese Frage aufgreifen und selbst experimentieren möchten.

Daraus folgen (ganz ähnlich wie in Beispiel 5.42) das Assoziativgesetz der Multiplikation und das Distributivgesetz.

Es bleibt noch zu zeigen, dass jedes Element in $\mathbb{H} \setminus \{0\}$ ein multiplikatives Inverses besitzt. Dazu genügt es zu zeigen, dass jede Matrix $\neq 0$, die im Bild von ι liegt, invertierbar ist und

dass die inverse Matrix ebenfalls im Bild von ι liegt. Dazu benutzen wir Beispiel 5.56 und die dort eingeführte *Determinante* einer (2×2)-Matrix. Es gilt

$$\delta(\iota((a,b,c,d))) = \delta\left(\begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix}\right) = a^2+b^2+c^2+d^2,$$

und dies ist eine nicht-negative reelle Zahl, die genau dann $= 0$ ist, wenn $(a,b,c,d) = 0$ ist.

Ist der Wert von δ nicht Null, so gilt

$$\begin{aligned}\begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix}^{-1} &= (a^2+b^2+c^2+d^2)^{-1}\begin{pmatrix} a-bi & c+di \\ -c+di & a+bi \end{pmatrix} \\ &= (a^2+b^2+c^2+d^2)^{-1}\iota(a,-b,-c,-d).\end{aligned}$$

Es ist auch leicht, das Inverse von $(a,b,c,d) \neq 0$ direkt anzugeben:

$$(a,b,c,d)^{-1} = \left(\frac{1}{a^2+b^2+c^2+d^2}, \frac{-b}{a^2+b^2+c^2+d^2}, \frac{-c}{a^2+b^2+c^2+d^2}, \frac{-d}{a^2+b^2+c^2+d^2}\right).$$

Damit haben wir vollständig bewiesen, dass $\mathbb{H}$ ein Schiefkörper ist. □ Ergänzung 5.64

KAPITEL 6

Vektorräume

Ähnlich wie der Begriff des Körpers die essenziellen Anforderungen an einen »Zahlbereich«, in dem die üblichen Rechenregeln für die Grundrechenarten gelten, zusammenfasst, macht dies der Begriff des Vektorraums, den wir in diesem Kapitel definieren, für die Eigenschaften von K^n und seiner Teilräume – insbesondere also für die Lösungsmengen homogener linearer Gleichungssysteme – und der Rechenoperationen der Addition und der Multiplikation mit Elementen (»Skalaren«) aus K.

6.1. Vektorräume

DEFINITION 6.1. Sei K ein Körper. Ein *(K-)Vektorraum* oder *Vektorraum über K* ist eine Menge V zusammen mit Verknüpfungen $+\colon V \times V \to V$ (Addition) und $\cdot\colon K \times V \to V$ (Skalarmultiplikation), so dass gilt:

(1) (a) Die Verknüpfung $+$ auf V ist *assoziativ*, d. h. für alle $u, v, w \in V$ gilt $(u + v) + w = u + (v + w)$.
   (b) Die Verknüpfung $+$ auf V besitzt ein eindeutig bestimmtes neutrales Element 0. (Dieses Element nennt man den *Nullvektor* von V.)
   (c) Jedes Element $v \in V$ besitzt ein inverses Element bezüglich $+$, d.h. es existiert $w \in V$ mit $v + w = 0 = w + v$.
   (d) Die Verknüpfung $+$ auf V ist kommutativ: Für alle $v, w \in V$ gilt $v + w = w + v$.

(2) (a) Für alle $a, b \in K, v \in V$ gilt: $a \cdot (b \cdot v) = (ab) \cdot v$.
   (b) Für alle $v \in V$ gilt $1 \cdot v = v$.
   (c) (Distributivgesetz 1) Für alle $a, b \in K, v \in V$ gilt: $(a + b) \cdot v = a \cdot v + b \cdot v$.
   (d) (Distributivgesetz 2) Für alle $a \in K, v, w \in V$ gilt: $a \cdot (v + w) = a \cdot v + a \cdot w$.

⊣

Man nennt K auch den *Grundkörper* des Vektorraums V. Die Skalarmultiplikation ist also keine Verknüpfung, die aus zwei Elementen von V ein weiteres produziert. Stattdessen verknüpft man ein »Skalar«, d.h ein Element des Grundkörpers K, mit einem Element von V. Wie bei der Multiplikation von Elementen eines Körpers lassen wir bei der Skalarmultiplikation den Punkt $\cdot$ üblicherweise aus.

Wie im Fall eines Körpers (vergleiche Lemma 4.7) ist das additive Inverse eines Elements v eindeutig bestimmt. Wir bezeichnen es mit $-v$ und nennen dieses Element auch das *Negative* von v. Wir setzen $v - w := v + (-w)$ und können somit auch davon sprechen, Elemente von V zu subtrahieren.

BEISPIEL 6.2. Sei K ein Körper. In allen folgenden Fällen ist es leicht nachzurechnen, dass die Bedingungen der Vektorraumdefinition (die »Vektorraumaxiome«) erfüllt sind. (In den meisten Fällen haben wir das schon gemacht oder implizit ausgenutzt, ohne den Begriff Vektorraum zu benutzen.)

(1) Ist $n \in \mathbb{N}$, so ist K^n mit der im vorherigen Kapitel definierten Addition und Skalarmultiplikation ein K-Vektorraum. Dies ist das prototypische Beispiel eines Vektorraums und man nennt K^n den *Standardvektorraum*.

(2) Der *Nullvektorraum* (oder auch *Nullraum*) ist der K-Vektorraum, der nur ein einziges Element hat. Dies muss dann der Nullvektor des Vektorraums sein. Wir schreiben manchmal 0 für den Nullraum $\{0\}$. Eine andere Bezeichnung für denselben Vektorraum ist K^0. (Ganz streng genommen könnten wir von unterschiedlichen Nullvektorräumen sprechen, je nachdem, wie wir das eine Element nennen. Da aber dieses Element wegen der Vektorraumaxiome immer die Rolle des Nullvektors in diesem Vektorraum haben muss, handelt es sich doch praktisch gesehen immer um denselben Raum. Wir werden das im folgenden Kapitel präzisieren, siehe Bemerkung 7.12.)

(3) Der Raum der $(m \times n)$-Matrizen $M_{m\times n}(K)$ ist mit der Addition von Matrizen und der Skalarmultiplikation (Definition 5.29) ein Vektorraum über K.

(4) Sei $U \subseteq K^n$ ein Teilraum im Sinne von Definition 5.23. Dann sind die Einschränkungen der Addition und Skalarmultiplikation auf K^n Abbildungen $+\colon U \times U \to U$ und $\cdot\colon K \times U \to U$, mittels derer U zu einem Vektorraum über K wird.

(5) Sei M eine Menge. Die Menge $\mathrm{Abb}(M, K)$ aller Abbildungen $M \to K$ ist ein Vektorraum, wenn wir die Addition und Skalarmultiplikation für $f, g\colon M \to K$, $a \in K$ definieren durch

$$(f+g)\colon M \to K,\ m \mapsto f(m)+g(m), \qquad (af)\colon M \to K,\ m \mapsto af(m).$$

(6) Die Menge der Polynomfunktionen $K \to K$ ist ein K-Vektorraum, wenn die Addition und Skalarmultiplikation wie im vorherigen Punkt definiert werden.

(7) Wir können das Beispiel $\mathrm{Abb}(M, K)$ noch verallgemeinern: Sei W ein K-Vektorraum und sei X irgendeine Menge. Dann ist die Menge $\mathrm{Abb}(X, W)$ mit den folgenden Verknüpfungen ein K-Vektorraum:

$$f+g := (X \to W,\ x \mapsto f(x)+g(x)),$$
$$a \cdot f := (X \to W, x \mapsto af(x),$$

wobei $f, g \in \mathrm{Abb}(X, W)$, $a \in K$. Alle Vektorraumaxiome sind leicht nachzuprüfen; es lässt sich alles auf die entsprechenden Bedingungen in W zurückführen. Der Nullvektor in diesem Vektorraum ist die konstante Abbildung mit Wert $0 \in W$.

(8) Sei L ein Erweiterungskörper von K (siehe 4.4). Dann können wir die Multiplikation $L \times L \to L$ einschränken zu einer Abbildung $K \times L \to L$. Mit dieser Abbildung als Skalarmultiplikation und der Körperaddition wird L zu einem K-Vektorraum. Zum Beispiel können wir in dieser Weise $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum betrachten: Die Addition ist die gewöhnliche Addition reeller Zahlen, und für $a \in \mathbb{Q}$, $v \in \mathbb{R}$ ist die Skalarmultiplikation durch die Bildung des Produkts von $a \in \mathbb{Q} \subset \mathbb{R}$ und $v \in \mathbb{R}$ als reelle Zahlen gegeben.

Analog ist $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum.

So simpel diese Feststellung ist, so nützlich ist sie doch, später in der Algebra-Vorlesung, aber zum Beispiel auch in Ergänzung 6.51 und Ergänzung 7.16.

◊

ERGÄNZUNG 6.3. Da die Summe und das Produkt von stetigen Funktionen $\mathbb{R} \to \mathbb{R}$ wieder stetig ist, sieht man, dass die Menge aller stetigen Funktionen $\mathbb{R} \to \mathbb{R}$ (mit der Addition und Skalarmultiplikation für Abbildungen wie vorher) ein $\mathbb{R}$-Vektorraum ist. Entsprechendes gilt für die Menge aller differenzierbaren Funktionen, und auch wenn man den Definitionsbereich durch eine geeignete Teilmenge von $\mathbb{R}$ ersetzt, beispielsweise durch ein offenes Intervall. □ Ergänzung 6.3

BEMERKUNG 6.4 (Was ist ein Vektor). Man kann sich fragen, ob es nicht natürlicher wäre, die Definition eines Vektorraums dadurch zu ersetzen, dass man erst einmal definiert, was ein *Vektor* ist.

Es ist aber unmöglich, die gewünschten Eigenschaften von Vektoren in dieser Weise zu abstrahieren, weil sie eben nur im Zusammenspiel mit anderen Vektoren fassbar sind (der Addition von Vektoren und der Multiplikation mit Elementen des Grundkörpers). Deshalb stellt man in der linearen Algebra die Definition eines Vektorraums an den Beginn und definiert dann:

DEFINITION 6.5. Die Elemente eines Vektorraums heißen *Vektoren*. ⊣

Die (etwas formalistische) Antwort auf die Frage *Was ist ein Vektor?* ist also: *Ein Vektor ist ein Element eines Vektorraums.*

> In mathematics you don't understand things. You just get used to them.
>
> John von Neumann,
> Antwort auf die Bemerkung eines Physikers, der gesagt hatte
> »I don't understand the method of characteristics.«
>
> wiedergegeben in: G. Zukav, *The Dancing Wu Li Masters: An Overview of the New Physics*, Rider, London, 1990.

Man muss vielleicht schon etwas (mathematisch) abgebrüht sein, um sich mit dieser Definition anzufreunden, sie entspricht aber der Zielsetzung, jede Definition so anzulegen, dass sie möglichst vielseitig einsetzbar ist – in diesem Fall heißt das: über die geometrische Anschauung hinaus.

Aber wie stellt man die Verbindung zu der Anschauung her, dass ein Vektor als ein Pfeil interpretiert werden kann (der eine Länge und eine Richtung hat)? Selbst wenn wir uns auf den Vektorraum $\mathbb{R}^2$, also die reelle Zahlenebene, oder den $\mathbb{R}^3$, den wir anschaulich mit dem uns umgebenden Raum identifizieren können, einschränken – die Elemente sehen wir ja als Punkte in der Ebene beziehungsweise im Raum, und nicht als Pfeile.

Was der Pfeil gut beschreibt, ist die *Operation*, v zu einem anderem Element zu addieren. Wenn wir den Startpunkt des Pfeils vom Ursprung nach v an den Punkt x legen, ist der Endpunkt des Pfeils bei $x+v$. In diesem Sinn ist dieser Pfeil eine Beschreibung der Abbildung $t_v\colon V \to V$, $x \mapsto x + v$.

Die Abbildung $V \to \mathrm{Abb}(V, V)$, $v \mapsto t_v$ ist eine injektive Abbildung. Das bedeutet, dass der Vektor durch die Abbildung t_v eindeutig bestimmt ist. Man kann den Vektor v aus dem Pfeil »zurückgewinnen« – das ist ja klar, weil v gerade der Endpunkt des Pfeils ist, wenn wir ihn am Ursprung beginnen lassen.

Der Begriff des *affinen Raums unter einem Vektorraum* macht die Unterscheidung zwischen den Rollen der Elemente von V als »Punkte« bzw. als »Pfeile« noch deutlicher. Wir werden ihn in der Vorlesung aber allenfalls streifen. Siehe Kapitel 12. ◊

LEMMA 6.6 (Rechenregeln). *Seien K ein Körper und V ein K-Vektorraum. Für alle $a \in K$, $v \in V$ gilt:*

(1) $a \cdot v = 0$ *genau dann, wenn* $a = 0$ *oder* $v = 0$.

(2) $-(av) = (-a)v = a(-v)$, *und* $(-1) \cdot v = -v$.

(3) $a \sum v_i = \sum av_i$, $(\sum a_i)v = \sum a_i v$, $\sum a_i v_i + \sum b_i v_i = \sum (a_i + b_i)v_i$ *(alle Summen seien endliche Summen).*

BEWEIS. zu (1). Sei zuerst $a = 0$ und $v \in V$ beliebig. Dann gilt wegen der Distributivität und wegen $0 + 0 = 0$:

$$0v = (0 + 0)v = 0v + 0v,$$

und wenn wir auf beiden Seiten $-(0v)$ addieren (also das Inverse von $0v$ addieren), erhalten wir

$$0 = 0v.$$

Sei nun $v = 0$ und $a \in K$ beliebig. Dann gilt

$$a0 = a(0 + 0) = a0 + a0,$$

und wir folgern ähnlich wie vorher, dass $a0 = 0$.

Seien nun $a \in K^\times$, $v \in V \setminus \{0\}$. Um den Beweis von Teil (1) abzuschließen, müssen wir noch zeigen, dass $av \neq 0$. Wir wissen, dass

$$a^{-1}(av) = (a^{-1}a)v = 1 \cdot v = v \neq 0,$$

und deshalb muss $av \neq 0$ gelten (denn sonst wäre nach dem schon Gezeigten $a^{-1}(av) = a^{-1}0 = 0$).

zu (2). Wir zeigen zunächst $-(av) = (-a)v$, mit anderen Worten, dass $(-a)v$ das Negative von av ist. In der Tat gilt

$$av + (-a)v = (a - a)v = 0v = 0.$$

Die zweite Behauptung ergibt sich ganz ähnlich:

$$av + a(-v) = a(v - v) = a0 = 0.$$

Die letzte Behauptung folgt, wenn wir $a = 1$ setzen: $(-1) \cdot v = 1 \cdot (-v) = -v$.

zu (3). Diese Aussagen folgen mit vollständiger Induktion aus den Distributivgesetzen. □

DEFINITION 6.7. Seien K ein Körper und V ein K-Vektorraum. Eine nichtleere Teilmenge $U \subseteq V$ heißt *Untervektorraum (oder Teilraum) von* V, wenn U abgeschlossen unter Addition und Skalarmultiplikation ist, das bedeutet: Sind $u, u' \in U$, so gilt auch $u + u' \in U$. Ist $u \in U$ und $a \in K$, so ist $au \in U$. ⊣

Wenn $U \subseteq V$ ein Untervektorraum ist, dann existiert ein Element $u \in U$, und aus den Untervektorraumeigenschaften folgt $0 = u + (-1) \cdot u \in U$: die Menge U enthält den Nullvektor $0 \in V$. Man könnte also in der Definition die Bedingung, dass U nicht leer ist, von vorneherein durch die Bedingung $0 \in U$ ersetzen.

Weil $-u = (-1) \cdot u$, impliziert die Abgeschlossenheit unter der Skalarmultiplikation, dass U zu jedem Element auch sein additives Inverses enthält. Deswegen ist U mit den Einschränkungen der Verknüpfungen von V selbst ein K-Vektorraum.

BEISPIEL 6.8. (1) In jedem Vektorraum V sind $\{0\}$ (oft geschrieben als 0, und bezeichnet als der *triviale Untervektorraum*) und V Teilräume.

(2) Für $V = K^n$ stimmt der hier definierte Begriff des Untervektorraums mit dem des Teilraums aus Definition 5.23 überein. Insbesondere erhalten wir so eine Vielzahl von Beispielen von Untervektorräumen: Jede Lösungsmenge eines homogenen Gleichungssystems mit n Unbestimmten ist ein Untervektorraum von K^n.

(3) Sind $U_1, U_2 \subseteq V$ Untervektorräume, so ist $U_1 \cap U_2$ ein Untervektorraum von V. Allgemeiner gilt: Ist I irgendeine Menge und sind U_i, $i \in I$, Untervektorräume von V, so ist der Durchschnitt $\bigcap_{i\in I} U_i$ ein Untervektorraum von V.

◊

FRAGE 6.9. Sei K ein Körper. Was sind die Untervektorräume von K^2? Es ist nicht schwer zu sehen, dass neben 0 und K^2 auch alle Teilmengen der Form $\{ax; a \in K\}$ für ein festes Element $x \in K^2$ die Untervektorraumeigenschaften erfüllen. Es ist richtig, aber nicht offensichtlich, dass damit alle Untervektorräume von K^2 gefunden sind.

Versuchen Sie einmal, das zu zeigen! Spätestens am Ende dieses Kapitels, wenn wir den Begriff der Dimension behandelt haben, wird Ihnen der Beweis leicht fallen. □ Frage 6.9

Eine weitere Methode, um aus gegebenen Untervektorräumen einen weiteren zu konstruieren, ist die *Summe von Untervektorräumen*:

DEFINITION 6.10. Sei V ein K-Vektorraum. Sind $U, W \subseteq V$ Untervektorräume von V, so ist

$$U + W := \{u + w;\ u \in U, w \in W\}$$

ein Untervektorraum von V, den wir die *Summe* der Untervektorräume U und W nennen. ⊣

LEMMA 6.11. *Sei V ein K-Vektorraum. Sind $U, W \subseteq V$ Untervektorräume von V, so ist $U + W$ der kleinste Untervektorraum von V, der U und W enthält.*

Das bedeutet: $U + W$ ist ein Untervektorraum von V und wenn $V' \subseteq V$ irgendein Untervektorraum mit $U \subseteq V'$ und $W \subseteq V'$ ist, dann gilt $U + W \subseteq V'$.

BEWEIS. Es ist leicht nachzuprüfen, dass $U + V$ ein Untervektorraum von V ist.

Sei nun $V' \subseteq V$ ein Untervektorraum von V, der U und W enthält. Dann gilt für alle $u \in U$ und $w \in W$, dass $u \in V'$ und $w \in V'$, also $u + w \in V'$ (denn V' ist ein Untervektorraum). Also gilt $U + W \subseteq V'$. □

Zusammen mit der obigen Bemerkung, dass der Durchschnitt von Untervektorräumen wieder ein Untervektorraum ist, ergibt sich damit die Beschreibung von $U + W$ als dem Durchschnitt aller Untervektorräume V' von V, die U und W enthalten.

DEFINITION 6.12. Sei V ein K-Vektorraum.

(1) Sind $U, W \subseteq V$ Untervektorräume mit $U \cap W = 0$, so schreiben wir statt $U + W$ auch $U \oplus W$ und sagen, U und W bilden (innerhalb V) eine *direkte Summe*.

(2) Sei $U \subseteq V$ ein Untervektorraum von V. Wir nennen einen Untervektorraum W einen *Komplementärraum* von U (oder ein *Komplement* von U), wenn $U \oplus W = V$, mit anderen Worten: $U + W = V$ und $U \cap W = 0$.

⊣

Während die Summe von Untervektorräumen ein Verfahren ist, zu zwei beliebigen Untervektorräumen einen weiteren zu *konstruieren*, drückt das Symbol $\oplus$ an dieser Stelle eine *Eigenschaft* des Paars U, W von Untervektorräumen aus (nämlich, dass sie trivialen Durchschnitt haben). Siehe auch Abschnitt 6.6.

Wir werden unten sehen (Korollar 6.44), dass jeder Untervektorraum in einem Vektorraum einen Komplementärraum besitzt. In aller Regel ist dieser *nicht eindeutig* bestimmt, sondern es gibt viele (üblicherweise unendlich viele) verschiedene Komplementärräume zu einem gegebenen U.

BEISPIEL 6.13. Sei $K = \mathbb{R}$ und $V = \mathbb{R}^2$. Ist $U \subseteq V$ eine Gerade durch den Ursprung, so ist U ein Untervektorraum, wie wir bereits gesehen haben. Jede Ursprungsgerade $W \subseteq V$, die von U verschieden ist, ist dann ein Komplementärraum von V. Es ist klar, dass $U \cap W = 0$, da U und W verschieden sein sollen. Es ist dann nicht schwer zu sehen (aber auch nicht ganz offensichtlich), dass $U + W = V$ gilt. Machen Sie sich das geometrisch klar! ◊

BEISPIEL 6.14. Sei $K = \mathbb{Q}$, $n \geq 1$. Seien

$$U = \left\{ (x_1, \ldots, x_n) \in K^n;\ \sum_{i=1}^{n} x_i = 0 \right\},$$
$$W = \{(a, \ldots, a) \in K^n;\ a \in K\}.$$

Dann sind U und W Untervektorräume von K^n und es gilt $U \oplus W = K^n$.

Wie ist es, wenn K ein anderer Körper ist? ◊

LEMMA 6.15. *Sei V ein K-Vektorraum, und seien U, W Untervektorräume von V. Dann sind äquivalent:*

(i) *Es gilt $U \oplus W = V$.*

(ii) *Jedes Element $v \in V$ lässt sich als Summe $v = u + w$ mit $u \in U$ und $w \in W$ schreiben und u und w sind dabei eindeutig bestimmt.*

BEWEIS. (i) $\Rightarrow$ (ii). Weil $U + W = V$ gilt, ist klar, dass sich jedes Element $v \in V$ als Summe $v = u + w$ mit $u \in U$ und $w \in W$ schreiben lässt. Gilt $v = u + w = u' + w'$ mit $u, u' \in U$, $w, w' \in W$, so folgt $u - u' = w - w'$, und dieses Element liegt in U (als Differenz zweier Elemente in U), und auch in W. Weil $U \cap W = 0$, folgt $u - u' = 0$ und $w - w' = 0$, also $u = u'$, $w = w'$. Das beweist die Eindeutigkeit der Darstellung.

(ii) $\Rightarrow$ (i). Es ist klar, dass $U + W = V$ gilt. Sei nun $v \in U \cap W$. Wäre $v \neq 0$, so erhielten wir die beiden *verschiedenen* Darstellungen $v = 0 + v = v + 0$ im Widerspruch zu (ii). Also muss $U \cap W = 0$ gelten. □

6.2. Erzeugendensysteme

DEFINITION 6.16. Unter einer *Linearkombination* von Vektoren $v_1, \ldots, v_n$ eines K-Vektorraums V verstehen wir einen Vektor der Form

$$a_1 v_1 + \cdots + a_n v_n, \quad a_i \in K.$$

Wir können diese Sprechweise auch auf eine möglicherweise unendliche Familie $(v_i)_{i \in I}$ von Vektoren ausdehnen. Eine Linearkombination ist dann eine Summe der Form

$$\sum_{i \in I} a_i v_i, \quad a_i \in K, \quad \text{nur endlich viele } a_i \neq 0.$$

Eine Summe mit unendlich vielen Summanden können wir in einem Vektorraum nicht bilden, aber da alle bis auf endlich viele a_i verschwinden, handelt es sich hier nur um eine endliche Summe. (In speziellen Konstellationen kann man natürlich auch dem Summensymbol mit unendlich vielen Summanden $\neq 0$ einen Sinn geben, wie einer konvergenten Reihe in der Analysis. In der linearen Algebra kommen derartige Grenzwertbildungen aber nicht vor.) ⊣

Wir sagen, ein Vektor v lasse sich als Linearkombination der Familie $v_1, \dots, v_n$ darstellen, wenn $a_1, \dots, a_n \in K$ existieren mit $v = a_1 v_1 + \cdots + a_n v_n$. Analog kann man davon sprechen, ob ein Vektor sich als Linearkombination einer (möglicherweise unendlichen) Familie $(v_i)_{i \in I}$ darstellen lässt.

Der Nullvektor lässt sich als Linearkombination jeder Familie $(v_i)_{i \in I}$ darstellen, indem man alle Koeffizienten $= 0$ wählt. (Mit der sinnvollen Konvention, dass die Summe über eine leere Indexmenge gleich Null sein soll, gilt das selbst für den Fall $I = \emptyset$.)

Beispiel 6.17. Der Vektor $(2, 4, 5)^t \in \mathbb{R}^3$ lässt sich nicht als Linearkombination der Vektoren $(1, 0, -1)^t$ und $(1, 1, 0)^t$ schreiben. (Warum nicht?)

Er lässt sich aber als Linearkombination von $(1, 0, 1)$ und $(0, 8, 6)$ schreiben. (Warum?) ◊

Definition 6.18. Seien K ein Körper und V ein K-Vektorraum. Eine Familie $B = (b_i)_{i \in I}$ von Elementen von V heißt *Basis* von V, falls jedes Element $v \in V$ in eindeutiger Weise (also für genau eine Wahl von Koeffizienten) als Linearkombination von Elementen aus B dargestellt werden kann. ⊣

Beispiel 6.19. Sei $n \geq 1$. Die Familie

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

ist eine Basis von K^n und wird als die *Standardbasis von K^n* bezeichnet.

Es ist klar, dass $e_1, \dots, e_n$ tatsächlich eine Basis von K^n bilden, denn ist $v = (x_i)_i \in K^n$ gegeben, so gilt $v = x_1 e_1 + \cdots x_n e_n$, und die x_i sind die einzigen Koeffizienten, für die die zugehörige Linearkombination den Vektor v liefert. ◊

Beispiel 6.20. Sei K ein Körper, $V \neq 0$ ein K-Vektorraum und $v \in V$ irgendein Element $\neq 0$. Dann ist $U = \{av;\ a \in K\}$ ein Untervektorraum von V und jedes Element $\neq 0$ von U bildet eine Basis von U.

Wenn K mehr als zwei Elemente hat, dann hat U also mehrere verschiedene Basen. ◊

Wie das Beispiel zeigt, ist eine Basis eines Teilraums fast nie eindeutig bestimmt.

Sei K ein Körper. Wir haben gesehen, dass die Lösungsmenge eines homogenen linearen Gleichungssystems in n Unbestimmten ein Teilraum von K^n ist. Ist das Gleichungssystem durch eine Matrix A in reduzierter Zeilenstufenform gegeben, so liefert die Methode, die wir kennengelernt haben, um die Lösungsmenge abzulesen, auch eine Basis dieses Vektorraums:

Satz 6.21. *Sei $A \in M_{m \times n}(K)$ die Koeffizientenmatrix eines homogenen linearen Gleichungssystems. Wir nehmen an, dass A reduzierte Zeilenstufenform hat. Seien r die Anzahl der Spalten von A, die eine führende Eins enthalten, und seien $j'_1 < \cdots < j'_{n-r}$ die Indizes der anderen Spalten.*

Sei für $\lambda = 1, \dots, n - r$ der Vektor $b_\lambda = (b_{\lambda j})_j \in K^n$ der eindeutig bestimmte Lösungsvektor mit

$$b_{\lambda j} = \begin{cases} 1 & j = j'_\lambda \\ 0 & j \in \{j'_1, j'_2, \dots, j'_{n-r}\} \setminus \{j'_\lambda\} \end{cases}$$

(die Werte $b_{\lambda j}$ für $j \notin \{j'_1, \dots, j'_{n-r}\}$ ergeben sich dann eindeutig aus der Bedingung, dass b_λ ein Lösungsvektor des gegebenen Gleichungssystems ist, siehe Satz 5.18).

Dann bilden die Vektoren $b_1, \dots, b_{n-r}$ eine Basis der Lösungsmenge des Gleichungssystems $Ax = 0$.

BEWEIS. Das folgt unmittelbar aus der Beschreibung der Lösungsmenge in Satz 5.18, vergleiche auch Beispiel 5.19. □

Mit anderen Worten: Die Vektoren, mit denen wir nach der üblichen Methode die Lösungsmenge eines homogenen linearen Gleichungssystems aufschreiben (vergleiche das Ende von Beispiel 5.19 (2)) bilden eine Basis dieses Teilraums von K^n.

BEMERKUNG 6.22. Machen Sie sich an einem Beispiel klar, dass es zwar nach Satz 5.17 zu gegebener Lösungsmenge nur eine Matrix in reduzierter Zeilenstufenfrom gibt, die diese Lösungsmenge ergibt, und wir demnach aus dem vorherigen Satz eine Basis der Lösungsmenge erhalten, ohne weitere Wahlen zu treffen, dass aber die Lösungsmenge meistens noch viele andere Basen hat (die eben nicht auf diese Art und Weise entstehen). ◊

BEMERKUNG 6.23. Wir können aus unseren Ergebnissen über lineare Gleichungssysteme auch ein Kriterium dafür ableiten, wann eine Familie $v_1, \ldots, v_n \in K^n$ eine Basis bilden. Dass es so ist, heißt genau, dass die Gleichung

$$X_1 v_1 + X_2 v_2 + \cdots + X_n v_n = b$$

für jedes $b \in K^n$ eine eindeutige Lösung $(x_i)_i \in K^n$ hat. Wenn wir die v_i als Spalten in eine Matrix A schreiben, so bedeutet das genau, dass für alle $b \in K^n$ das lineare Gleichungssystem $(A \mid b)$ eindeutig lösbar ist. Wir haben gesehen, dass das dazu äquivalent ist, dass die Matrix A invertierbar ist.

Es ist auch nicht schwierig, die Theorie der linearen Gleichungssysteme zu benutzen, um zu zeigen, dass eine Basis von K^n immer aus genau n Elementen bestehen muss. Weil wir dieses Ergebnis aber auch in Kürze aus der allgemeinen Theorie erhalten, verzichten wir hier auf eine genauere Analyse. Siehe auch Ergänzung 6.46. ◊

DEFINITION 6.24. Sei V ein Vektorraum.

(1) Seien $v_1, \ldots, v_n \in V$. Der *von $v_1, \ldots, v_n$ aufgespannte Untervektorraum* ist die Teilmenge aller derjenigen Vektoren von V, die sich als Linearkombination der v_i darstellen lassen. Er wird mit $\langle v_1, \ldots, v_n \rangle$ bezeichnet:

$$\langle v_1, \ldots, v_n \rangle = \left\{ \sum_{i=1}^{n} a_i v_i;\ a_i \in K \right\}.$$

(2) Ist allgemeiner $M \subseteq V$ irgendeine (möglicherweise unendliche) Teilmenge, so ist der *von M aufgespannte Untervektorraum* von V die Teilmenge aller derjenigen Elemente aus V, die sich als Linearkombination von Elementen aus M darstellen lassen. Er wird mit $\langle M \rangle$ bezeichnet:

$$\langle M \rangle = \left\{ \sum_{i=1}^{n} a_i v_i;\ n \geq 1, a_i \in K, v_i \in M \right\}.$$

Man spricht auch vom *von $v_1, \ldots, v_n$ (bzw. von M) erzeugten Untervektorraum*, von der *linearen Hülle* oder vom *Spann* der Vektoren $v_1, \ldots, v_n$ bzw. der Menge M. ⊣

Wie in der Definition angedeutet, ist $\langle v_1, \ldots, v_n \rangle$ und allgemeiner $\langle M \rangle$ ein Untervektorraum von V. Das prüft man leicht anhand der Definition nach.

SATZ 6.25 (Charakterisierung der linearen Hülle). *Seien K ein Körper, V ein K-Vektorraum und $M \subseteq V$ eine Teilmenge. Dann gilt:*

(1) *$\langle M \rangle$ ist der Durchschnitt aller Untervektorräume, die M enthalten.*

(2) *$\langle M\rangle$ ist der kleinste Untervektorraum von V, der M enthält, das bedeutet: $\langle M\rangle$ ist ein Untervektorraum, und ist $U \subseteq V$ irgendein Untervektorraum mit $M \subseteq U$, so gilt $\langle M\rangle \subseteq U$.*

BEWEIS. Zu (1). Sei U der Durchschnitt aller Untervektorräume, die M enthalten. Dies ist ein Untervektorraum von V (Beispiel 6.8). Er enthält M und damit auch alle Linearkombination von Elementen aus M, d.h. $\langle M\rangle \subseteq U$. Andererseits ist $\langle M\rangle$ ein Untervektorraum, der M enthält, also gilt auch $U \subseteq \langle M\rangle$.

Zu (2). Das folgt direkt aus Teil (1), denn der Durchschnitt aller Untervektorräume, die M enthalten, ist natürlich in jedem solchen Untervektorräume enthalten. □

BEISPIEL 6.26. Wir betrachten den $\mathbb{R}$-Vektorraum $V = \mathbb{R}^3$, den wir anschaulich mit dem uns umgebenden Raum identifizieren. Ist $v \in V$, $v \neq 0$, so ist $\langle v\rangle$ die eindeutig bestimmte Gerade durch den Ursprung, die v enthält. Ist $v' \in V$ ein Vektor, der nicht auf der Gerade $\langle v\rangle$ liegt, so ist $\langle v, v'\rangle$ die eindeutig bestimmte Ebene, die den Ursprung, v und v' enthält. ◊

BEISPIEL 6.27. Sei K ein Körper, $n \geq 1$. Sei

$$U = \left\{ (x_1, \ldots, x_n) \in K^n;\ \sum_{i=1}^{n} x_i = 0 \right\},$$

dies ist ein Untervektorraum von K^n. (Vergleiche Beispiel 6.14.) Dann gilt

$$U = \left\langle \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \right\rangle$$

und diese Elemente bilden sogar eine Basis von U. ◊

Um den Begriff der Basis besser zu verstehen, ist es nützlich, die zwei Aspekte der Definition – die Existenz einer Darstellung als Linearkombination einerseits, und die Eindeutigkeit andererseits – separat zu untersuchen. Der Begriff des Erzeugendensystems, den wir nun definieren, isoliert den Aspekt der Existenz solcher Darstellungen. Im nächsten Abschnitt behandeln wir dann mit dem Begriff der linearen Unabhängigkeit den Aspekt der Eindeutigkeit der Darstellung.

DEFINITION 6.28. Seien K ein Körper und V ein K-Vektorraum. Eine Teilmenge M von V heißt *Erzeugendensystem* von V, falls $\langle M\rangle = V$, d.h. wenn zu jedem $v \in V$ eine Zahl $N \geq 0$ und Elemente $m_1, \ldots, m_N \in M$ und $a_1, \ldots, a_N \in K$ existieren, so dass $x = \sum_{i=1}^{N} a_i m_i$. ⊣

DEFINITION 6.29. Ein K-Vektorraum V heißt *endlich erzeugt*, wenn ein Erzeugendensystem von V existiert, das nur endlich viele Elemente hat. ⊣

Die Vektorräume K^m, $m \in \mathbb{N}$ sind endlich erzeugt, denn es gibt ein Erzeugendensystem (sogar eine Basis) mit m Elementen. Seien $v_1, \ldots, v_n \in K^m$ und sei $A \in M_{m\times n}(K)$ die Matrix mit den Spalten $v_1, \ldots, v_n$. Dass $v_1, \ldots v_n$ ein Erzeugendensystem von K^m bilden, bedeutet genau, dass für alle $b \in K^m$ das lineare Gleichungssystem $(A \mid b)$ lösbar ist.

Die Begriffe *Erzeugendensystem* und *endlich erzeugt* können wir auch auf Untervektorräume eines Vektorraums anwenden (denn jeder Untervektorraum ist ja selbst auch ein K-Vektorraum).

BEISPIEL 6.30 (Beispiel eines nicht endlich erzeugten Vektorraums). Sei K ein Körper und sei V der Vektorraum aller Folgen $(a_i)_{i\in\mathbb{N}}$ mit $a_i \in K$, also $V = \prod_{i\in\mathbb{N}} K$, mit der komponentenweisen Addition und Skalarmultiplikation. Es ist leicht zu überprüfen, dass es sich tatsächlich um einen K-Vektorraum handelt. (Wir können diesen Vektorraum auch als den Vektorraum $\mathrm{Abb}(\mathbb{N}, K)$ aus Beispiel 6.2 betrachten. Vergleiche auch Abschnitt 6.6.)

Die Teilmenge $U \subset V$, die aus allen Folgen mit nur endlich vielen Einträgen $\neq 0$ besteht, ist ein Untervektorraum. Auch das lässt sich leicht nachrechnen.

Der Vektorraum U ist nicht endlich erzeugt. Denn sind $u_1, \ldots, u_n \in U$, so haben nach Definition von U alle u_i nur endlich viele von 0 verschiedene Einträge. Sei $N \in \mathbb{N}$ der höchste Index, bei dem in irgendeinem der u_i ein Eintrag $\neq 0$ steht. Der Vektor, der an der Stelle $N+1$ eine 1 und sonst überall Nullen hat, ist ein Element von U, das nicht in $\langle u_1, \ldots, u_n\rangle$ liegt.

Es ist richtig, aber weniger offensichtlich, dass auch der Vektorraum V nicht endlich erzeugt ist. Siehe Satz 6.43. ◊

BEISPIEL 6.31. Sei K ein unendlicher Körper. Der K-Vektorraum U aller Polynomfunktionen $K \to K$ (Abschnitt 4.3 und Beispiel 6.2) ist nicht endlich erzeugt. Denn für jede Polynomfunktion $f\colon K \to K$, die nicht die Nullfunktion ist, ist die Darstellung $f(x) = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$ eindeutig bestimmt. Die Zahl n bezeichnet man dann als den Grad von f. Sind $f_1, \ldots, f_r$ Polynomfunktionen vom Grad $\leq n$, so hat auch jede Linearkombination der f_i Grad $\leq n$. Da Polynomfunktionen von beliebig großem Grad existieren, folgt aus dieser Überlegung, dass U nicht endlich erzeugt ist.

(Betrachtet man die Koeffizienten $a_0, \ldots, a_n$ als eine unendliche Folge von Elementen in K, deren weitere Glieder alle $= 0$ sind, so kann man dieses Beispiel mit dem vorherigen identifizieren.)

Ist K endlich, so gibt es nur endlich viele Polynomfunktionen $K \to K$, und insbesondere ist der Vektorraum aller dieser Polynomfunktionen eine endliche Menge und erst recht endlich erzeugt. ◊

6.3. Lineare Unabhängigkeit

Gegeben eine Familie $(v_i)_{i\in I}$ von Vektoren in einem Vektorraum V, dann bezeichnen wir $\sum_{i\in I} 0v_i$ (also die Linearkombination, in der alle Koeffizienten gleich Null sind) als die *triviale Linearkombination* der gegebenen Familie von Vektoren. Ihr Wert ist der Nullvektor. Diese Linearkombination ist natürlich völlig uninteressant, und sie hat nur deshalb einen eigenen Namen, damit man sie – zum Beispiel in der folgenden Definition – von der Betrachtung ausschließen kann.

DEFINITION 6.32. V ein K-Vektorraum. Eine Familie $(v_i)_{i\in I}$ von Vektoren $v_i \in V$ heißt *linear unabhängig* (l.u.), falls für jede endliche Teilmenge $J \subseteq I$ gilt: Sind $a_i \in K$, $i \in J$ mit

$$\sum_{i\in J} a_i v_i = 0,$$

so gilt für alle $i \in J$: $a_i = 0$.

Eine Familie von Vektoren aus V, die nicht linear unabhängig ist, heißt *linear abhängig* (l.a.). ⊣

In ähnlicher Weise definiert man die Begriffe *linear unabhängig* und *linear abhängig* für Teilmengen eines Vektorraums. Man beachte, dass in einer Familie von Vektoren derselbe Vektor mehrfach auftreten kann, jedoch nicht in einer Menge. Ist etwa $v \in V$, $v \neq 0$, so ist die

Menge $\{v, v, \ldots, v\}$ linear unabhängig, weil sie gleich der Menge $\{v\}$ ist. Die Familie $(v_i)_{i=1,\ldots,n}$ mit $v_i := v$ ist jedoch für $n > 1$ linear abhängig.

Elemente $v_1, \ldots, v_n \in K^m$ sind genau dann linear unabhängig, wenn das homogene lineare Gleichungssystem $Ax = 0$, in dem A die Matrix mit den Spalten $v_1, \ldots, v_n$ ist, nur die triviale Lösung besitzt, oder anders ausgedrückt: eindeutig lösbar ist.

BEISPIEL 6.33. (1) Ist V ein Vektorraum, so ist jede Basis von V linear unabhängig, denn dann lässt sich jedes Element in eindeutiger Weise als Linearkombination schreiben, insbesondere der Nullvektor.

Zum Beispiel ist die Familie $e_1, \ldots, e_n$ der Standardbasisvektoren in K^n linear unabhängig.

(2) Die leere Menge von Vektoren ist aus trivialen Gründen linear unabhängig.

(3) Jede Familie, in der der Nullvektor vorkommt, ist linear abhängig.

$\Diamond$

LEMMA 6.34. *Seien K ein Körper, V ein K-Vektorraum, $v_1, \ldots, v_n \in V$, $n \geq 1$. Dann sind äquivalent:*

(i) *Die Familie $v_1, \ldots, v_n$ ist linear unabhängig*

(ii) *Für alle $v \in \langle v_1, \ldots, v_n \rangle$, existiert eine* eindeutig bestimmte *Darstellung von v als Linearkombination von $v_1, \ldots, v_n$.*

(iii) *Für alle i gilt: $v_i \notin \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \rangle$.*

(iv) *Für alle i gilt: $\langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \rangle \subsetneq \langle v_1, \ldots, v_n \rangle$.*

(v) *Es sind $v_1, \ldots, v_{n-1}$ linear unabhängig und $v_n \notin \langle v_1, \ldots, v_{n-1} \rangle$.*

BEWEIS. Wir führen Induktion nach n. Für $n = 1$ ist die Sache klar: alle Bedingungen sind äquivalent zu $v_1 \neq 0$. Wir dürfen daher im folgenden annehmen, dass die 5 Aussagen für Familien von $n - 1$ Vektoren äquivalent sind.

Wir beweisen nun die folgenden Implikationen; daraus folgt die gewünschte Äquivalenz.

$$\text{(i)} \Leftrightarrow \text{(ii)}, \quad \text{(iii)} \Leftrightarrow \text{(iv)}, \quad \text{(i)} \Rightarrow \text{(iii)} \Rightarrow \text{(v)} \Rightarrow \text{(i)}.$$

(i) $\Leftrightarrow$ (ii). Wenn es ein v gäbe, das zwei verschiedene Darstellungen

$$v = a_1 v_1 + \cdots + a_n v_n = b_1 v_1 + \cdots + b_n v_n$$

hätte, so wäre

$$(a_1 - b_1) v_1 + \cdots + (a_n - b_n) v_n = 0$$

eine nichttriviale Linearkombination, die den Nullvektor darstellt, im Widerspruch zu (i).

(iii) $\Rightarrow$ (iv) ist klar und (iii) $\Leftarrow$ (iv) ist einfach.

(i) $\Rightarrow$ (iii). Beweis durch Widerspruch: Angenommen, es wäre $v_i \in \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \rangle$. Das hieße, dass sich v_i als Linearkombination von $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ schreiben ließe:

$$v_i = a_1 v_1 + \cdots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \cdots + v_n,$$

was wir umschreiben können zu

$$a_1 v_1 + \cdots + a_{i-1} v_{i-1} + (-1) v_i + a_{i+1} v_{i+1} + \cdots + v_n = 0.$$

Dies ist eine Linearkombination, die den Nullvektor darstellt. Da der Koeffizient von v_i aber $\neq 0$ ist, können dann die Vektoren $v_1, \ldots, v_n$ nicht linear unabhängig sein.

(iii) $\Rightarrow$ (v). Wenn (iii) gilt, so gilt erst recht $v_i \notin \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_{n-1} \rangle$ für $i = 1, \ldots, n-1$, also sind nach Induktionsvoraussetzung die Vektoren $v_1, \ldots, v_{n-1}$ linear unabhängig. Damit ist klar, dass aus (iii) Bedingung (v) folgt.

(v) $\Rightarrow$ (i). Sei

$$a_1 v_1 + \cdots + a_n v_n = 0$$

eine Linearkombination, die den Nullvektor darstellt. Wegen $v_n \notin \langle v_1, \ldots, v_{n-1} \rangle$ muss dann $a_n = 0$ sein. Weil $v_1, \ldots, v_{n-1}$ linear unabhängig sind, folgt daraus aber, dass alle a_i verschwinden. Also ist die Familie $v_1, \ldots, v_n$ linear unabhängig. □

6.4. Basen, Basissätze

SATZ 6.35. *Seien K ein Körper und V ein K-Vektorraum. Sei B eine Teilmenge von V. Dann sind äquivalent:*

(i) *B ist eine Basis von V.*

(ii) *B ist ein linear unabhängiges Erzeugendensystem von V.*

(iii) *B ist ein minimales Erzeugendensystem von V (d.h. B ist ein Erzeugendensystem von V, aber keine echte Teilmenge $B' \subsetneq B$ ist ein Erzeugendensystem von V).*

(iv) *B ist eine maximale linear unabhängige Teilmenge in V (d.h. B ist linear unabhängig und für jedes $v \in V \setminus B$ ist $B \cup \{v\}$ linear abhängig).*

BEWEIS. (i) $\Rightarrow$ (ii). Sei B eine Basis von V. Nach Definition des Begriffs *Basis* ist klar, dass B ein Erzeugendensystem ist. Da der Nullvektor (wie jeder andere Vektor) in eindeutiger Weise als Linearkombination der Elemente von B dargestellt werden kann, folgt auch, dass B linear unabhängig ist.

(ii) $\Rightarrow$ (iii). Sei B ein linear unabhängiges Erzeugendensystem von V. Angenommen, es gäbe $b \in B$, so dass auch $B \setminus \{b\}$ ein Erzeugendensystem ist. Dann existieren $b_1, \ldots, b_r \in B \setminus \{b\}$ und $a_1, \ldots, a_r \in K$ mit

$$b = a_1 b_1 + \cdots + a_r b_r,$$

also ist $a_1 b_1 + \cdots + a_r b_r - b = 0$ eine Linearkombination, die den Nullvektor darstellt. Da $b_i \neq b$ für alle i gilt, ist das ein Widerspruch dazu, dass B linear unabhängig ist.

(iii) $\Rightarrow$ (iv). Sei B ein minimales Erzeugendensystem von V. Wir zeigen zuerst, dass B linear unabhängig ist. Sonst gäbe es $b_1, \ldots, b_r \in B$ und eine Linearkombination $a_1 b_1 + \cdots + a_r b_r = 0$ mit $a_1 \neq 0$, und dann wäre

$$b_1 = -\frac{1}{a_1}(a_2 b_2 + \cdots a_r b_r),$$

und daher auch $B \setminus \{b_1\}$ ein Erzeugendensystem von V, im Widerspruch zur Minimalität von B. Da B ein Erzeugendensystem ist, ist andererseits auch klar, dass für $v \in V \setminus B$ die Vereinigung $B \cup \{v\}$ nicht linear unabhängig sein kann.

(iv) $\Rightarrow$ (i). Sei B eine maximale linear unabhängige Teilmenge von V. Wegen der linearen Unabhängigkeit kann jeder Vektor $v \in V$ in höchstens einer Weise als Linearkombination von Elementen aus B dargestellt werden (denn gäbe es zwei verschiedene Darstellungen, so wäre die Differenz eine nicht-triviale Linearkombination, die den Nullvektor darstellt). Es ist daher nur noch zu zeigen, dass B ein Erzeugendensystem ist. Ist $v \in B$, so lässt sich v trivialerweise als Linearkombination von Elementen in B darstellen. Ist $v \in V \setminus B$, so ist $B \cup \{v\}$ linear abhängig, es gibt also eine *nicht-triviale* Linearkombination

$$av + a_1 b_1 + \cdots a_r b_r = 0$$

mit $a, a_i \in K$, $b_i \in B$. Weil B linear unabhängig ist, kann hier nicht $a = 0$ sein. Daher können wir durch a teilen und sehen dann leicht, dass v eine Linearkombination von Elementen aus B ist. □

In den folgenden Ergebnissen dieses Abschnitts sind oftmals gewisse Endlichkeitsvoraussetzungen (wie »endlich erzeugt«) in eckigen Klammern angegeben. Das soll bedeuten, dass die Sätze zwar auch im allgemeinen Fall richtig sind, wir sie aber nur unter der genannten Voraussetzung beweisen. Siehe Ergänzung 6.47 für Hinweise zu den Beweisen im allgemeinen Fall.

SATZ 6.36. *Jeder [endlich erzeugte] K-Vektorraum besitzt eine Basis.*

BEWEIS. Wir geben hier den Beweis in dem Fall, dass V ein endliches Erzeugendensystem E besitzt. Ist das Erzeugendensystem E minimal, so haben wir schon eine Basis gefunden. Andernfalls ist die Menge E linear abhängig, und es existiert ein Element $v \in E$, das in der linearen Hülle der anderen Elemente aus E liegt. Daher ist auch $E \setminus \{v\}$ ein Erzeugendensystem von V. Indem wir diese Argumentation fortsetzen und gegebenenfalls weitere Elemente von E herausnehmen, finden wir in endlich vielen Schritten ein minimales Erzeugendensystem, also eine Basis. □

Siehe auch Satz 6.39 für eine präzisere Form des Satzes.

SATZ 6.37 (Basisaustauschsatz). *Seien K ein Körper, V ein K-Vektorraum, $v_1, \dots, v_n \in V$ eine Basis, $w_1, \dots, w_i \in V$ eine linear unabhängige Familie. Dann existiert eine Teilmenge $I \subseteq \{1, \dots, n\}$, $\#I = i$, so dass die n Elemente $w_1, \dots, w_i, v_j, j \notin I$, eine Basis von V bilden.*

BEWEIS. Wir können das Ergebnis des Satzes auch so formulieren: *Nach Umnummerieren der v_j* (falls erforderlich), ist $w_1, \dots, w_i, v_{i+1}, \dots, v_n$ eine Basis von V.

Wir beweisen diese Behauptung durch vollständige Induktion nach i. *Induktionsanfang:* $i = 0$. In diesem Fall ist nichts zu beweisen: Die Behauptung fällt nämlich mit der Annahme zusammen, dass $v_1, \dots, v_n$ eine Basis ist. (Wenn Ihnen mit der Optimierung, für den Induktionsanfang $i = 0$ zu wählen, unwohl ist, dann überlegen Sie sich den Fall $i = 1$ zusätzlich direkt. Dann können Sie die Induktion von dort fortsetzen.)

Induktionsschritt: $i - 1 \to i$. Sei nun $i \geq 1$ und sei der Satz für linear unabhängige Familien mit $i - 1$ Elementen bereits bewiesen. Sei eine linear unabhängige Familie $w_1, \dots, w_i$ gegeben. Dann ist erst recht die Familie $w_1, \dots, w_{i-1}$ linear unabhängig, nach Induktionsvoraussetzung können wir die v_j also so umnummerieren, dass $w_1, \dots, w_{i-1}, v_i, \dots, v_n$ eine Basis bildet. Dann können wir w_i als Linearkombination

$$w_i = a_1 w_1 + \cdots + a_{i-1} w_{i-1} + a_i v_i + \cdots + a_n v_n$$

schreiben. Da $w_1, \dots, w_i$ als linear unabhängig vorausgesetzt wurde, kann es keine Linearkombination von $w_1, \dots, w_{i-1}$ geben, wie w_i darstellt, es muss also mindestens einen Koeffizienten a_j mit $j \geq i$ geben, der nicht gleich 0 ist (wir sehen an dieser Stelle auch, dass automatisch $i \leq n$ gelten muss). Nach Umnummerieren können wir annehmen, dass $a_i \neq 0$ gilt. Wir können dann die obige Gleichheit umschreiben als

$$v_i = -\frac{1}{a_i}(a_1 w_1 + \cdots + a_{i-1} w_{i-1} - w_i + a_{i+1} v_{i+1} + \cdots + a_n v_n).$$

Es ist dann leicht zu sehen, dass $w_1, \dots, w_i, v_{i+1}, \dots, v_n$ wieder ein linear unabhängiges Erzeugendensystem von V ist, also eine Basis. □

Direkt aus dem Satz ergibt sich (weil eine Teilmenge von $\{1, \dots, n\}$ höchstens n Elemente haben kann):

KOROLLAR 6.38. *Seien K ein Körper, V ein K-Vektorraum, $v_1, \dots, v_n \in V$ eine Basis, $w_1, \dots, w_i \in V$ eine linear unabhängige Familie. Dann gilt $i \leq n$.*

SATZ 6.39 (Basisergänzungssatz). *Seien K ein Körper und V ein K-Vektorraum. Sei M eine linear unabhängige Teilmenge von V, und sei $E \subseteq V$ ein [endliches] Erzeugendensystem von V, das M enthält. Dann existiert eine Basis B von V mit $M \subseteq B \subseteq E$.*

Insbesondere: Jede linear unabhängige Teilmenge von V lässt sich zu einer Basis ergänzen, [sofern V endlich erzeugt ist.]

BEWEIS. Wir betrachten den Fall, dass E endlich ist. Wir können dann E zu einem minimalen Erzeugendensystem, also einer Basis, verkleinern. Mit dem Basisaustauschsatz können wir gegebenenfalls die Elemente von M, die bei diesem Prozess herausgefallen sind, wieder hinzunehmen (und dafür andere Elemente fortlassen).

Für den zweiten Teil ergänzen wir die gegebene linear unabhängige Teilmenge zunächst in beliebiger Weise zu einem endlichen Erzeugendensystem (zum Beispiel, indem wir irgendein endliches Erzeugendensystem hinzufügen). □

THEOREM 6.40. *Sei K ein Körper und sei V ein [endlich erzeugter] K-Vektorraum. Je zwei Basen von V besitzen dieselbe Mächtigkeit (d.h. im endlich erzeugten Fall einfach, dass je zwei Basen gleich viele Elemente haben; im allgemeinen Fall kann man sagen, dass es zwischen je zwei Basen eine Bijektion gibt).*

Diese Zahl wird als Dimension dim V *von V bezeichnet (zumindest sofern sie endlich ist, sonst sagen wir einfach, die Dimension von V sei unendlich; präziser kann man die Dimension als Kardinalzahl verstehen).*

BEWEIS. Wir beweisen den Satz in dem Fall, dass V endlich erzeugt ist. In diesem Fall folgt die Behauptung unmittelbar aus Korollar 6.38. □

BEISPIEL 6.41. (1) Es gilt $\dim(K^n) = n$, denn die Standardbasisvektoren $e_1, \ldots, e_n$ bilden eine Basis. (Ist $n = 0$, so ist $K^n = 0$ und die leere Menge eine Basis, also ist auch $\dim K^0 = 0$.)

(2) Es gilt $\dim(M_{m\times n}(K)) = mn$. Die mn Matrizen, in denen ein einziger Eintrag 1 und alle anderen Einträge 0 sind, bilden eine Basis.

(3) Ist $A \in M_{m\times n}(K)$ die Koeffizientenmatrix eines homogenen linearen Gleichungssystems, so ist die Zahl r der Spalten mit führenden Einsen in jeder Matrix in Zeilenstufenform, die aus A durch elementare Zeilenumformungen entsteht, gleich $n - \dim \operatorname{Ker} A$. Siehe Satz 6.21.

(4) Der $\mathbb{R}$-Vektorraum $\mathbb{C}$ hat Dimension $\dim_{\mathbb{R}} \mathbb{C} = 2$. (Natürlich können wir $\mathbb{C}$ auch als Vektorraum über sich selbst auffassen und es ist $\dim_{\mathbb{C}} \mathbb{C} = 1$.)

◊

Der Dimensionsbegriff gibt uns die Möglichkeit, die »Größe« eines Vektorraums (oder Untervektorraums in einem Vektorraum) zu messen/zu quantifizieren. Das ist der erste wichtige Schritt zur Beantwortung von Frage 5.27 (2).

THEOREM 6.42. *Seien K ein Körper und V ein n-dimensionaler Vektorraum, $n \in \mathbb{N}$.*

(1) *Jedes linear unabhängige System von n Vektoren in V ist eine Basis.*

(2) *Jedes Erzeugendensystem von V, das aus n Elementen besteht, ist eine Basis von V.*

BEWEIS. zu (1). Sei ein linear unabhängiges System gegeben, das aus n Vektoren besteht. Nach dem Basisergänzungssatz können wir dieses System zu einer Basis ergänzen. Da alle Basen aus genau n Elementen bestehen, kann eine echte Ergänzung in diesem Fall aber gar nicht erforderlich/möglich sein. Das gegebene System muss selbst schon eine Basis sein.

zu (2). Ähnlich wie Teil (1). □

Mit diesem Ergebnis kann man sich auch leicht überlegen, dass man im Basisergänzungssatz die Voraussetzung, dass E endlich sei, ersetzen kann durch die Bedingung, dass V endlich erzeugt ist, also überhaupt irgendein endliches Erzeugendensystem besitzt. (Mit dem Lemma von Zorn kann man natürlich, wie durch die eckigen Klammern angedeutet, die Endlichkeitsvoraussetzung ohnehin vollständig fallenlassen.)

SATZ 6.43. *Sei V ein endlich erzeugter K-Vektorraum und $U \subseteq V$ ein Untervektorraum.*

(1) *Der Vektorraum U ist endlich erzeugt und* $\dim U \leq \dim V$.

(2) *Gilt* $\dim U = \dim V$, *so folgt* $U = V$.

BEWEIS. Wäre U nicht endlich erzeugt, so müsste U zu jeder natürlichen Zahl r eine linear unabhängige Teilmenge mit r Elementen enthalten (denn sonst könnten wir eine endliche maximale linear unabhängige Teilmenge, also eine endliche Basis, finden). Es kann aber nicht sein, dass U eine linear unabhängige Teilmenge mit mehr als dim V Elementen enthält. Also ist U endlich erzeugt. Jede Basis von U ist linear unabhängig, auch als Teilmenge von V betrachtet, und wir können sie zu einer Basis von V ergänzen. Also muss $\dim(U) \leq \dim(V)$ gelten.

Gilt $\dim U = \dim V$, so folgt aus Theorem 6.42, dass jede Basis von U auch eine Basis von V ist. Das impliziert $U = V$. □

Wir können nun auch beweisen, dass jeder Untervektorraum in einem Vektorraum ein Komplement (Def. 6.12) besitzt.

KOROLLAR 6.44. *Sei V ein [endlich erzeugter] K-Vektorraum und sei $U \subseteq V$ ein Untervektorraum. Dann besitzt U einen Komplementärraum.*

BEWEIS. Wir wählen eine Basis $b_1, \ldots, b_m$ von U. Diese Vektoren sind linear unabhängig, egal, ob wir sie als Elemente von U oder von V betrachten. Wir können daher die Familie der b_i nach dem Basisergänzungssatz zu einer Basis $b_1, \ldots, b_n$ von V ergänzen. Dann ist $W := \langle b_{m+1}, \ldots, b_n \rangle$ ein Komplement von U. □

SATZ 6.45 (Dimensionsformel für den Durchschnitt von zwei Untervektorräumen). *Seien V ein [endlich erzeugter] K-Vektorraum und seien $U, W \subseteq V$ Untervektorräume. Dann gilt*

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W).$$

BEWEIS. Wir geben den Beweis im Fall dass V und damit auch alle Untervektorräume von V endlich erzeugt sind und demnach endliche Dimension haben.

Sei $v_1, \ldots, v_r$ eine Basis von $U \cap W$. Wir ergänzen diese einerseits durch Vektoren $u_1, \ldots, u_s$ zu einer Basis $v_1, \ldots, v_r, u_1, \ldots, u_s$ von U, andererseits durch Vektoren $w_1, \ldots, w_t$ zu einer Basis $v_1, \ldots, v_r, w_1, \ldots, w_t$ von W.

Es ist klar, dass es dann genügt, die folgende Behauptung zu zeigen:

Behauptung. $v_1, \ldots, v_r, u_1, \ldots, u_s, w_1, \ldots w_t$ ist eine Basis von $U + W$.

Begründung. Offenbar handelt es sich um ein Erzeugendensystem von $U + W$, weil die gegebene Familie sowohl ein Erzeugendensystem von U als auch eines von W enthält. Es bleibt also nur noch die lineare Unabhängigkeit zu zeigen. Sei dazu

$$a_1 v_1 + \cdots + a_r v_r + b_1 u_1 + \cdots + b_s u_s + c_1 w_1 + \cdots c_t w_t = 0$$

eine Linearkombination, die den Nullvektor darstellt. Dann gilt $-\sum c_i w_i = \sum a_i v_i + \sum b_i u_i \in U \cap W = 0$, also $\sum c_i w_i = 0$ und $\sum a_i v_i + \sum b_i u_i = 0$. Daraus folgt, dass alle Koeffizienten gleich Null sein müssen. □

ERGÄNZUNG 6.46. Es ist möglich, den Begriff der Dimension noch direkter auf der Theorie der linearen Gleichungssysteme aufzubauen. Dazu würde man zeigen, dass für jeden Vektorraum V mit einem endlichen Erzeugendensystem E und jede linear unabhängige Teilmenge $L \subseteq V$ die Abschätzung $\#L \leq \#E$ gilt.

Um das zu zeigen, schreiben wir die Elemente von E als $e_1, ..., e_m$ und die von L als $l_1, ..., l_n$. Da E ein Erzeugendensystem ist, gibt es $a_{ij} \in K$ mit

$$l_j = a_{1j}e_1 + \cdots + a_{nj}e_n, \quad j = 1, ...n.$$

Sei $A = (a_{ij})_{i,j} \in M_{m\times n}(K)$. Für jede Lösung $(x_1, ..., x_n)^t$ des linearen Gleichungssystems $Ax = 0$ gilt dann $\sum_j a_{ij}x_j = 0$, also

$$\sum_{j=1}^{m} x_j l_j = \sum_{i,j} a_{ij}x_j e_i = 0,$$

also $x_1 = \cdots = x_n = 0$ wegen der linearen Unabhängigkeit von L. Das homogene Gleichungssystem $Ax = 0$ hat also nur die triviale Lösung, die Zeilenstufenform von A hat in jeder Spalte eine Stufe. Daher muss A mindestens so viele Zeilen wie Spalten haben, es gilt somit $m \geq n$. Siehe auch [**So**] 1.7. □ Ergänzung 6.46

ERGÄNZUNG 6.47 (Existenz von Basen, allgemeiner Fall). Wir haben in Satz 6.36 behauptet, aber nicht bewiesen, dass jeder Vektorraum eine Basis besitzt. Es ist klar, dass der Beweis, den wir für den endlich erzeugten Fall gegeben haben, nicht ohne weiteres auf den allgemeinen Fall übertragen werden kann. Es ist zwar klar, dass jeder Vektorraum V ein Erzeugendensystem besitzt (zum Beispiel die Menge V selbst). Aber wenn dieses unendlich ist, kann man nicht erwarten, es durch Entfernen endlich vieler Vektoren zu einem minimalen Erzeugendensystem zu machen.

Im allgemeinen Fall ist es daher günstiger zu zeigen, dass in V eine maximale linear unabhängige Teilmenge existiert. Wie wir gesehen haben, ist dies eine Basis von V.

Dafür verwenden wir das Lemma von Zorn, siehe Abschnitt A.1. Wir betrachten die Menge $\mathscr{U}$ aller linear unabhängigen Teilmengen von V mit der Inklusion als »partieller Ordnung«. Das Lemma von Zorn liefert uns die Existenz eines maximalen Elements in $\mathscr{U}$ bezüglich $\subseteq$, also einer Basis von V, wenn wir die folgende Behauptung zeigen können:

Behauptung. Sei $\mathscr{U}' \subseteq \mathscr{U}$ eine Teilmenge von $\mathscr{U}$ mit der Eigenschaft, dass für alle $L_1, L_2 \in \mathscr{U}'$ gilt, dass $L_1 \subseteq L_2$ oder $L_2 \subseteq L_1$. Dann existiert ein Element $L \in \mathscr{U}$, so dass $L' \subseteq L$ für alle $L' \in \mathscr{U}'$.

(Die Bedingung an $\mathscr{U}'$ beschreibt man, indem man sagt, $\mathscr{U}'$ sei bezüglich $\subseteq$ *total* geordnet. Das Element L von $\mathscr{U}$ nennt man eine *obere Schranke* von $\mathscr{U}$.)

Begründung. Sei also $\mathscr{U}'$ wie in der Behauptung gegeben. Wir definieren L als die Vereinigung aller Teilmengen von $\mathscr{U}'$. Es ist klar, dass $L' \subseteq L$ für alle $L' \in \mathscr{U}'$ gilt. Aber wir müssen noch zeigen, dass überhaupt $L \in \mathscr{U}$ gilt, dass also L eine lineare unabhängige Teilmenge von V ist.

Natürlich ist im allgemeinen die Vereinigung von linear unabhängigen Teilmengen nicht linear unabhängig; aber hier sind wir ja in einer speziellen Situation.

Wir beginnen mit dem folgenden Lemma:

LEMMA 6.48. *Seien V ein K-Vektorraum und $L \subseteq V$ eine Teilmenge. Die Teilmenge L ist genau dann linear unabhängig, wenn jede endliche Teilmenge von L linear unabhängig ist.*

BEWEIS. Wenn L linear unabhängig ist, dann ist erst recht jede Teilmenge von L linear unabhängig. Wenn L linear abhängig ist, dann gibt es eine nicht-triviale Linearkombination von Elementen aus L , die den Nullvektor darstellt, und in jeder Linearkombination treten nur endlich viele Vektoren auf. Daher existiert dann eine endliche Teilmenge von L, die linear abhängig ist. □

Nun zurück zum Beweis der obigen Behauptung. Es genügt also zu zeigen, dass jede endliche Teilmenge $\{v_1, ..., v_r\}$ von L linear unabhängig ist. Da L die Vereinigung der Elemente von $\mathscr{U}'$ ist, existieren $L_1, ..., L_r \in \mathscr{U}'$ mit $v_i \in L_i$. Da je zwei Elemente von $\mathscr{U}'$ ineinander enthalten sind, können wir, wenn wir die v_i und L_i umnummerieren, falls erforderlich, annehmen, dass

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r.$$

Dann liegen aber $v_1, ..., v_r$ alle in L_r, und da L_r linear unabhängig ist, folgt auch die lineare Unabhängigkeit der Familie $v_1, ..., v_r$. Damit ist die Behauptung bewiesen und wir können das Lemma von Zorn anwenden.

Es ist auch leicht, den Beweis so anzupassen, dass die Basis ein vorgegebenes linear unabhängiges System enthält und in einem vorgegebenen Erzeugendensystem von V enthalten ist, indem man die Definition von $\mathscr{U}$ entsprechend modifiziert.

Durch ein geschicktes Vorgehen kann man (mithilfe des Lemmas von Zorn) auch den Basisaustauschsatz auf unendliche Mengen erweitern und zeigen, dass für jeden Vektorraum V, jedes Erzeugendensystem E von V und jede linear unabhängige Teilmenge M von V eine injektive Abbildung $\iota\colon M \to E$ existiert, so dass auch $(E \setminus \iota(M)) \cup M$ ein Erzeugendensystem von V ist. Es werden also sozusagen die Elemente in $\iota(M)$ durch die Elemente in M ausgetauscht. Dazu versieht man die Menge aller injektiven Abbildungen $\iota'\colon M' \to E$, so dass $M' \subseteq M$ und $(E \setminus \iota'(M')) \cup M'$ ein Erzeugendensystem von V ist, mit einer geeigneten partiellen Ordnung, benutzt eine ähnliche Methode wie oben, um zu zeigen, dass die Voraussetzungen das Lemmas von Zorn erfüllt sind, und überlegt sich unter Ausnutzung des (»endlichen«) Basisaustauschprinzips, dass ein maximales Element dieser Menge notwendigerweise M als Definitionsbereich haben muss.

Zusammen mit dem Satz von Schröder-Bernstein (Theorem 3.85) erhält man dann, dass es zwischen je zwei Basen eines Vektorraums eine Bijektion gibt. Siehe auch [**So-AZT**] 5.3 für eine etwas ausführlichere Diskussion. □ Ergänzung 6.47

6.5. Wie berechne ich ...?

Ich habe etwas gezögert, ob es überhaupt sinnvoll ist, diesen Abschnitt ins Skript aufzunehmen, denn gerade für diese »Rechenverfahren« gilt: Es ist besser, wenn Sie sich selbst überlegen, wie Sie die uns zur Verfügung stehenden Verfahren (und das ist im Moment eigentlich nur der Gauß-Algorithmus) auf die zu bewältigende Aufgabe anwenden. Insbesondere rate ich davon ab, die Varianten, die unten diskutiert werden, auswendig zu lernen. Letztlich habe ich mich aber doch entschieden, einige Aufgabentypen hier zu sammeln, auch um illustrieren zu können, dass es am Ende von Kapitel 8 möglich sein wird, einiges noch klarer darzustellen. Konkrete Beispiele zu diesen Aufgabentypen finden Sie in den Online-Aufgaben.

Sei K ein Körper. Um Basen von Untervektorräumen in K^n, $n \in \mathbb{N}$, zu berechnen und damit zusammenhängende Fragen über Untervektorräume zu beantworten, erweist sich der Gauß-Algorithmus als Universalwerkzeug.

Wir haben bereits erwähnt, dass die Spalten einer Matrix $A \in M_{m\times n}(K)$ genau dann eine linear unabhängige Familie in K^m bilden, wenn das homogene Gleichungssystem $Ax = 0$

eindeutig lösbar ist, also nur die triviale Lösung besitzt. Ein Vektor $b \in K^m$ liegt genau dann im Untervektorraum von K^m, der von den Spalten von A erzeugt wird, wenn das Gleichungssystem $Ax = b$ lösbar ist.

6.5.1. Basis der Lösungsmenge eines homogenen linearen Gleichungssystems. Diese Aufgabenstellung haben wir bereits besprochen, siehe Satz 6.21.

Eine äquivalente Formulierung des Problems ist, eine Basis vom Kern $\mathrm{Ker}(A)$ einer Matrix A zu bestimmen, denn $\mathrm{Ker}(A)$ ist genau die Lösungsmenge des homogenen Gleichungssystems $Ax = 0$.

6.5.2. Eine Basis innerhalb eines gegebenen Erzeugendensystems. Sei $U \subseteq K^m$ ein Untervektorraum und sei $u_1, \ldots, u_n \in U$ ein Erzeugendensystem von U. Wir wissen, dass es eine Basis von U gibt, die aus Vektoren dieses Erzeugendensystems besteht. Um eine solche zu finden, betrachten wir die Matrix $A \in M_{m\times n}$, deren j-te Spalte der Spaltenvektoren $u_j \in K^m$ ist. Sei B eine Matrix in Zeilenstufenform, die aus A durch elementare Zeilenumformungen entsteht. Dann bilden die u_j für diejenigen Indizes j, die in B zu einer Spalte mit einer führenden Eins korrespondieren, eine Basis von U.

Begründung des Verfahrens. Sind $s_1, \ldots, s_n \in K^m$ die Spalten einer Matrix S, geht die Matrix S' mit den Spalten $s'_1, \ldots, s'_n$ aus S durch elementare Zeilenumformungen hervor und sind $c_j \in K$, so gilt $\sum_{j=1}^n c_j s_j = 0$ genau dann, wenn $\sum_{j=1}^n c_j s'_j = 0$. Das ist für alle drei Typen von elementaren Zeilenumformungen leicht einzusehen.

Das bedeutet, dass für eine Teilmenge $J \subseteq \{1, \ldots n\}$ die Spalten $s_j, j \in J$, genau dann linear unabhängig sind, wenn es $s'_j, j \in J$ sind.

Eine Basis innerhalb des gegebenen Erzeugendensystems ist eine maximale linear unabhängige Teilmenge darin. Für eine Matrix in Zeilenstufenform ist klar, dass die Spalten mit führenden Einsen eine solche maximale linear unabhängige Teilmenge bilden.

Eine äquivalente Formulierung des Problems ist, eine Basis vom Bild einer Matrix A zu bestimmen, denn das Bild von A ist genau der von den Spalten von A erzeugte Untervektorraum.

6.5.3. Eine linear unabhängige Teilmenge zu einer Basis ergänzen. In ähnlicher Weise kann man eine linear unabhängige Teilmenge L in einem Untervektorraum $U \subseteq K^m$ zu einer Basis ergänzen, wenn man irgendein Erzeugendensystem E von U kennt. Denn dann ist $L \cup E$ auch ein Erzeugendensystem, auf das man das Verfahren des vorherigen Abschnitts anwenden kann. Wenn man die Elemente von L als die linken Spalten der Matrix A schreibt, führt die lineare Unabhängigkeit dazu, dass diese Spalten in der Zeilenstufenform jedenfalls führende Einsen enthalten werden. An den zusätzlich auftretenden führenden Einsen kann man ablesen, welche Elemente von E man noch hinzunehmen kann, um eine Basis zu erhalten.

6.5.4. Eine Basis vom Durchschnitt und der Summe von Untervektorräumen. Seien $U, W \subseteq K^m$ Untervektorräume mit Basen $u_1, \ldots, u_r$ und $w_1, \ldots, w_s$. Wir wollen Basen von $U + W$ und $U \cap W$ finden.

Da $u_1, \ldots, u_r, w_1, \ldots, w_s$ die Summe $U + W$ erzeugen, können wir das vorher besprochene Verfahren anwenden, um innerhalb dieses Erzeugendensystems eine Basis von $U + W$ zu finden.

Um eine Basis von $U \cap W$ zu finden, verfahren wir folgendermaßen. Ein Element $v \in K^m$ liegt genau dann in $U \cap W$, wenn es sowohl als Linearkombination der u_j, als auch als Linearkombination der w_j darstellbar ist, wenn also a_j und b_j existieren mit

$$a_1 u_1 + \cdots + a_r u_r = v = b_1 w_1 + \cdots + b_s w_s.$$

Um alle Elemente von $U \cap W$ zu finden, müssen wir also alle Tupel $(a_1, ..., a_r, b_1, ..., b_s)$ finden mit

$$a_1 u_1 + \cdots + a_r u_r - b_1 w_1 - \cdots - b_s w_s = 0,$$

oder mit anderen Worten die Lösungsmenge des linearen Gleichungssystems $Ax = 0$, wo A die Matrix mit Spalten $u_1, ..., u_r, -w_1, ..., -w_s$ ist. Ist $(x_j)_j \in K^{r+s}$ ein Element der Lösungsmenge, so ist $\sum_{j=1}^{r} x_j u_j = \sum_{j=r+1}^{r+s} x_j w_j \in U \cap W$. Wir bezeichnen für den Moment für $x = (x_j)_j \in K^{r+s}$ mit $\overline{x}$ den Vektor $\sum_{j=1}^{r} x_j u_j$. Bilden dann $v_1, ..., v_t$ eine Basis der Lösungsmenge, so ist $\overline{v_1}, ..., \overline{v_t}$ ein Erzeugendensystem von $U \cap W$, und sogar eine Basis, wie wir gleich begründen werden.

Zunächst die folgende Bemerkung: Weil mit $w_1, ..., w_s$ auch $-w_1, ..., -w_s$ eine Basis ist, kann man auch die beiden Verfahren in einem Schritt durchführen und aus der Zeilenstufenform der Matrix A mit Spalten $u_1, ..., u_r, -w_1, ..., -w_s$ eine Basis von $U + W$ ablesen.

Insbesondere folgt, dass die Anzahl der führenden Einsen in der Zeilenstufenform von A genau $\dim(U + W)$ ist. Die Dimension t der Lösungsmenge ist also $r + s - \dim(U + W) = \dim(U) + \dim(W) - \dim(U + W) = \dim(U \cap W)$, siehe Satz 6.45. Weil das Erzeugendensystem $\overline{v_1}, ..., \overline{v_t}$ von $U \cap W$, das wir oben gefunden haben, genau $\dim(U \cap W)$ Elemente hat, handelt es sich um eine Basis. (Man kann sich die lineare Unabhängigkeit auch direkt überlegen, ohne die Dimensionsformel für den Durchschnitt von Untervektorräumen zu benutzen. Sehen Sie, wie?)

6.6. Produkt und direkte Summe von Vektorräumen

Sei K ein Körper. Sind $V_1, ..., V_n$ Vektorräume über K, so ist das kartesische Produkt $V_1 \times \cdots \times V_n$, also die Menge aller n-Tupel $(v_1, ..., v_n)$ mit $v_i \in V_i$, $i = 1, ..., n$ mit der *komponentenweisen Addition*

$$(v_1, ..., v_n) + (w_1, ..., w_n) := (v_1 + w_1, ..., v_n + w_n)$$

und der *komponentenweisen Skalarmultiplikation*

$$a \cdot (v_1, ..., v_n) = (av_1, ..., av_n)$$

ein K-Vektorraum. Dies prüft man leicht nach, weil sich alle Bedingungen in den einzelnen Einträgen separat überprüfen lassen und man nur benutzen muss, dass alle V_i Vektorräume sind. Wir nennen diesen Vektorraum das *Produkt* der Vektorräume $V_1, ..., v_n$.

Genauso definiert man das Produkt $\prod_{i \in I} V_i$ einer (möglicherweise unendlichen) Familie $(V_i)_{\in I}$ von Vektorräumen über K. Ist $V = V_i$ für alle I, so schreiben wir auch $V^I = \prod_{i \in I} V$ für diesen Vektorraum. Die Vektorraumstruktur auf dem Produkt ist dieselbe wie die, die wir in Beispiel 6.2 auf $\mathrm{Abb}(I, V)$ definiert haben.

Die Teilmenge

$$\bigoplus_{i \in I} V_i := \left\{ (v_i)_i \in \prod_{i \in I} V_i;\ \text{höchstens endlich viele } v_i \text{ sind } \neq 0 \right\}$$

von $\prod_{i \in I} V_i$ ist ein Untervektorraum und heißt die direkte Summe der Vektorräume V_i. Man spricht manchmal auch vom *Koprodukt* der Vektorräume V_i.

Wenn die Indexmenge I endlich ist, dann gilt natürlich $\bigoplus_{i \in I} V_i = \prod_{i \in I} V_i$.

BEMERKUNG 6.49. Wir hatten das Symbol $\oplus$ in Definition 6.12 schon in einer etwas anderen Weise definiert, und zwar hatten wir für Untervektorräume U, W eines Vektorraums V die Summe von U und W als $U \oplus W$ geschrieben, wenn $U \cap W = 0$ gilt. Wir können das leicht mit der neuen Schreibweise zusammenbringen, denn unter der Voraussetzung $U \cap W = 0$

können wir den Vektorraum $U \oplus W$ (im neu definierten Sinne) identifizieren mit der Summe $U + W$; das ist genau die Aussage von Lemma 6.15.

Wenn es notwendig ist, den kleinen Unterschied zwischen den beiden Sichtweisen zu betonen, dann bezeichnet man manchmal die in diesem Abschnitt definierte direkte Summe als die *äußere direkte Summe*, und die vorherige Bezeichnung als die *innere direkte Summe*. Die äußere direkte Summe ist also eine Konstruktion, die aus zwei (oder mehr) Vektorräumen einen neuen konstruiert; wir können $U \oplus W$ für beliebige Untervektorräume, sogar $V \oplus V$, und $V \oplus V'$ für Vektorräume V, V', die gar nicht Untervektorräume desselben Vektorraums sind, betrachten. Eine innere direkte Summe zu bilden, ist eine Eigenschaft, die Untervektorräume eines Vektorraums haben können, oder eben nicht – es ist gerade die Eigenschaft, dass die äußere direkte Summe dieser Untervektorräume mit der Summe innerhalb des umgebenden Vektorraums identifiziert werden kann. Siehe auch Bemerkung 7.13. ◊

6.7. Ergänzungen *

Wir können nun den folgenden Satz beweisen, den wir als Satz 5.35 als ein Beispiel für eine Aussage über Matrizen formuliert hatten, deren Beweis eine Weiterentwicklung der Theorie erfordert. In der Linearen Algebra 2 werden wir sehen, wie sich der Satz in die allgemeine Theorie der Eigenwerte einer Matrix einfügt.

SATZ 6.50. *Seien K ein Körper, $n \geq 1$, $A \in M_{n\times n}(K)$. Wenn eine natürliche Zahl N existiert mit $A^N = 0$, dann gilt $A^n = 0$.*

BEWEIS. Um zu zeigen, dass $A^n = 0$, zeigen wir $\mathrm{Ker}(A^n) = K^n$. Das impliziert $A^n = 0$, sonst würde für mindestens ein i gelten, dass $A^n e_i \neq 0$. Wir betrachten $U_i := \mathrm{Ker}(A^i)$. Dann ist $U_i \subset K^n$ ein Untervektorraum, und nach Voraussetzung gilt $U_N = K^n$. Wenn $A^i v = 0$, dann gilt erst recht $A^{i+1}v = AA^i v = 0$, die U_i sind also jeweils ineinander enthalten:

$$0 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_N = K^n.$$

Behauptung. Gilt $U_i = U_{i+1}$, so gilt $U_i = U_j$ für alle $j \geq i$.

Begründung. Es genügt zu zeigen, dass aus $U_i = U_{i+1}$ auch $U_{i+1} = U_{i+2}$ folgt. Danach kann man induktiv fortfahren. Wir wissen bereits, dass $U_{i+1} \subseteq U_{i+2}$. Sei nun $v \in U_{i+2}$, also $A^{i+2}v = 0$. Das bedeutet $Av \in U_{i+1} = U_i$, also $A^i(Av) = 0$. Wir sehen, dass $v \in U_{i+1}$, wie behauptet.

Um den Beweis abzuschließen, zeigen wir, dass aus der Behauptung die Gleichheit $U_n = K^n$ folgt. Weil $U_N = K^n$ gilt, zeigt die Behauptung, dass $U_i = U_{i+1}$ nur gelten kann, wenn $U_i = K^n$ gilt. Im Fall einer echten Inklusion $U_i \subsetneq U_{i+1}$ gilt $\dim(U_i) < \dim(U_{i+1})$ (Satz 6.43). Solange wir in der Kette der U_i nicht bei K^n »angekommen« sind, muss also in jedem Schritt die Dimension um mindestens Eins ansteigen. Deshalb gilt $\dim U_i \geq i$ für alle $i = 0, \ldots n$. Aus $\dim U_n \geq n = \dim K^n$ folgt $U_n = K^n$, wobei wir wieder Satz 6.43 anwenden. □

ERGÄNZUNG 6.51 (Die Kardinalität endlicher Körper). Sei K ein endlicher Körper. Wir haben in Abschnitt 4.2.2 gesehen, dass die Charakteristik von K eine Primzahl p ist. Es gilt dann $p_K = 1 + \cdots + 1 = 0$ in K (mit p Summanden in der Summe), und für alle $1 \leq n < p$ ist $n_K \neq 0$.

LEMMA 6.52. *Der Körper K wird durch die Körperaddition auf K und die Skalarmultiplikation*

$$\cdot : \mathbb{F}_p \times K \to K, \quad n_{\mathbb{F}_p} \cdot x = n_K x = \underbrace{x + \cdots + x}_{n \text{ Summanden}}$$

zu einem $\mathbb{F}_p$-Vektorraum.

BEWEIS. Das ist eine leichte Rechnung. Genauer kann man sagen, dass die Abbildung $\mathbb{F}_p \to K, n_{\mathbb{F}_p} \mapsto n_K$, den Körper K zu einem Erweiterungskörper von $\mathbb{F}_p$ macht (und wir hatten in Beispiel 6.2 angemerkt, dass dann der Erweiterungskörper auch ein Vektorraum über dem kleineren Körper ist). □

KOROLLAR 6.53. *Es gibt $r \in \mathbb{N}_{\geq 1}$ mit $\#K = p^r$.*

BEWEIS. Da K nach Voraussetzung endlich ist, ist K als $\mathbb{F}_p$-Vektorraum endlich erzeugt. Daher besitzt K eine Basis $b_1, \dots, b_r$, $r \in \mathbb{N}$. Weil K als Körper mehr als ein Element haben muss, kann nicht $r = 0$ gelten.

Wir können jedes Element von K in eindeutiger Weise als $\sum_{i=1}^{r} a_i b_i$ mit $a_i \in \mathbb{F}_p$ schreiben. Die Abbildung

$$\mathbb{F}_p^r \to K, \quad (a_1, \dots, a_r)^t \mapsto \sum_{i=1}^{r} a_i b_i,$$

ist also eine Bijektion, und wir sehen $\#K = \#\mathbb{F}_p^r = p^r$. □

□ Ergänzung 6.51

ERGÄNZUNG 6.54 (Die Fibonacci-Zahlen, Fortsetzung). In dieser Ergänzung beweisen wir die folgende Formel für die n-te Fibonacci-Zahl (vgl. Frage 2.1, Beispiel 5.60). Siehe auch Beispiel 11.9 für einen ganz anderen Beweis für diese Formel. Der Beweis, den wir hier geben, lässt sich auch auf andere, in ähnlicher Weise rekursiv definierte Folgen anpassen.

SATZ 6.55. *Sei $(F_n)_n$ die Folge der Fibonacci-Zahlen. Dann gilt*

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Auch wenn die Formel nicht nützlich ist, um F_n auszurechnen, handelt es sich dennoch um ein interessantes Ergebnis. Es ist ja nicht einmal völlig offensichtlich, dass es sich bei der rechten Seite der Formel überhaupt um eine ganze Zahl handelt.

BEWEIS. Wir betrachten den $\mathbb{R}$-Vektorraum $\mathbb{R}^{\mathbb{N}} = \prod_{n \in \mathbb{N}} \mathbb{R}$. Als Menge ist dies die Menge aller Folgen $(a_n)_{n \in \mathbb{N}}$ von reellen Zahlen a_n, und wir versehen diese Menge mit der komponentenweisen Addition und Skalarmultiplikation:

$$(a_n)_n + (b_n)_n = (a_n + b_n)_n, \quad a \cdot (a_n)_n = (a\, a_n)_n.$$

Es ist klar, dass wir so einen Vektorraum erhalten. (In der Sprechweise von Abschnitt 6.6 handelt es sich einfach um das Produkt des Vektorraums $\mathbb{R}$ mit sich selbst mit Indexmenge $\mathbb{N}$.)

Sei W der Untervektorraum von V, der aus denjenigen Folgen $(a_n)_n$ besteht, für die $a_{n+2} = a_{n+1} + a_n$ für alle $n \in \mathbb{N}$ gilt. Die Fibonacci-Folge ist ein Element von W. Ein anderes Element ist die Folge

$$(G_n)_n = (1, 0, 1, 1, 2, 3, 5, 8, 13, \dots).$$

Weil ein Element aus W durch seine ersten beiden Einträge vollständig bestimmt ist, bilden $(F_n)_n$ und $(G_n)_n$ ein Erzeugendensystem von W. Da sie nicht Vielfache von einander sind, handelt es sich sogar um eine Basis, und wir sehen, dass $\dim W = 2$.

Um den gesuchten Ausdruck für F_n zu finden, betrachten wir noch eine andere Basis von W, und zwar eine von einer besonders einfachen Form. Der Raum W enthält genau zwei Elemente der Form

$$(1, \varphi, \varphi^2, \varphi^3, \dots)$$

mit $\varphi \in \mathbb{R}^\times$. Denn die Folge aller Potenzen der reellen Zahl $\varphi \neq 0$ ist genau dann in W, wenn für alle n

$$\varphi^{n+2} = \varphi^{n+1} + \varphi^n$$

gilt, äquivalent:

$$\varphi^2 - \varphi - 1 = 0.$$

Die beiden Lösungen dieser quadratischen Gleichung in $\mathbb{R}$ sind

$$\varphi_1 = \frac{1+\sqrt{5}}{2}, \quad \varphi_2 = \frac{-1+\sqrt{5}}{2}.$$

Wir schreiben

$$w_1 = (\varphi_1^n)_n, \quad w_2 = (\varphi_2^n)_n.$$

Dann bilden auch w_1 und w_2 eine Basis von W, weil diese beiden Elemente offenbar linear unabhängig sind.

Es gilt dann $(F_n)_n = \frac{1}{\sqrt{5}} w_1 - \frac{1}{\sqrt{5}} w_2$, denn es genügt, das für die ersten beiden Einträge zu überprüfen. Es folgt daraus, dass

$$F_n = \frac{1}{\sqrt{5}}(\varphi_1^n - \varphi_2^n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

für alle $n \in \mathbb{N}$ – genau die Formel, die wir zeigen wollten. □

Für den Grenzwert des Verhältnisses F_{n+1} / F_n im Sinne der Analysis erhalten wir damit das folgende Ergebnis:

KOROLLAR 6.56. *Es gilt*

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}.$$

BEWEIS. Wir benutzen die Notation φ_1, φ_2 wie im Beweis des Satzes und die grundlegenden Rechenregeln für Grenzwerte. Dann gilt $|\varphi_2 / \varphi_1| = (\sqrt{5}-1)^2 / 4 < 1$, also

$$\lim_{n\to\infty} \frac{\varphi_2^n}{\varphi_1^n} = 0,$$

und daher

$$\lim_{n\to\infty} F_{n+1} / F_n = \lim_{n\to\infty} \frac{\varphi_1^{n+1} - \varphi_2^{n+1}}{\varphi_1^n - \varphi_2^n} = \lim_{n\to\infty} \frac{\varphi_1 - \varphi_2 \frac{\varphi_2^n}{\varphi_1^n}}{1 - \frac{\varphi_2^n}{\varphi_1^n}} = \varphi_1 = \frac{1+\sqrt{5}}{2}.$$

□

□ Ergänzung 6.54

ERGÄNZUNG 6.57 (Das quadratische Sieb, Fortsetzung). Wir können nun Frage 2.2 beantworten:

SATZ 6.58. *Gegeben seien eine natürliche Zahl $n \geq 1$ und n verschiedene Primzahlen $p_1, \ldots, p_n$. Wenn $a_1, \ldots, a_{n+1}$ natürliche Zahlen > 1 sind, in deren Primfaktorzerlegungen nur die Primzahlen $p_1, \ldots, p_n$ vorkommen, dann gibt es eine Möglichkeit, einige der Zahlen a_i so auszuwählen, dass ihr Produkt eine Quadratzahl ist.*

BEWEIS. Wir betrachten zu jedem a_i die eindeutige Primfaktorzerlegung, in der nach Voraussetzung nur die Primzahlen $p_1, \dots, p_n$ vorkommen, etwa

$$a_i = p_1^{a_{i1}} \cdot p_2^{a_{i2}} \cdot \dots \cdot p_n^{a_{in}}.$$

Die Primfaktorzerlegung eines Produkts von Zahlen a_i erhalten wir dann, indem wir die Exponenten addieren. Wir möchten ein Produkt von a_i's finden, in dem alle Exponenten in der Primfaktorzerlegung gerade sind, denn das bedeutet gerade, dass es sich um eine Quadratzahl handelt.

Wir können das auch folgendermaßen ausdrücken: Setze

$$v_{ij} = \begin{cases} 0 & a_{ij} \text{ gerade} \\ 1 & a_{ij} \text{ ungerade} \end{cases} \in \mathbb{F}_2$$

(es ist also v_{ij} die Restklasse von a_{ij} in $\mathbb{F}_2$) und sei $v_i = (v_{i1}, \dots, v_{in})^t \in \mathbb{F}_2^n$.

Aus den $n+1$ Zahlen $a_1, \dots, a_{n+1}$ erhalten wir so $n+1$ Vektoren $v_1, \dots, v_{n+1}$ in dem n-dimensionalen $\mathbb{F}_2$-Vektorraum $\mathbb{F}_2^n$. Diese Vektoren müssen also linear abhängig sein. Da die einzigen Elemente von $\mathbb{F}_2$ die 0 und 1 sind, hat eine nicht-triviale Linearkombination die Form

$$v_{i_1} + \dots + v_{i_r} = 0,$$

für eine nicht-leere Teilmenge $\{i_1, \dots, i_r\} \subseteq \{1, \dots, n+1\}$.

Das bedeutet aber gerade, dass die Summen der entsprechenden Zahlen $a_{i_v j}$ gerade sind, also dass das Produkt $a_{i_1} \cdot \dots \cdot a_{i_r}$ eine Quadratzahl ist. □

□ Ergänzung 6.57

ERGÄNZUNG 6.59 (Schiefkörper, Fortsetzung). Wir hatten in Ergänzung 4.9 den Begriff des Schiefkörpers und der Divisionsalgebra definiert. Für den Begriff der Divisionsalgebra lässt sich äquivalent die folgende Definition geben: Eine Divisionsalgebra über einem Körper K ist ein Schiefkörper D, der zugleich ein K-Vektorraum ist, und so dass die Schiefkörperaddition und die Vektorraumaddition übereinstimmen und die Multiplikation des Schiefkörpers D und die Skalarmultiplikation $K \times D \to D$ im folgenden Sinne kompatibel sind: $a(xy) = (ax)y = x(ay)$ für alle $a \in K, x, y \in D$.

Dann ist die Abbildung $K \to D, a \mapsto a \cdot 1_D$, eine injektive Abbildung (warum?), so dass wir K mit einer Teilmenge von D identifizieren können. Es ist dann nicht schwierig, die Äquivalenz der beiden Definitionen zu überprüfen.

Wir können nun mithilfe des Dimensionsbegriffs die folgenden Sätze formulieren. Dabei nennen wir eine Divisionsalgebra endlich-dimensional, wenn sie als Vektorraum betrachtet endliche Dimension hat.

SATZ 6.60. *Es gibt keine endlich-dimensionale Divisionsalgebra über dem Körper $\mathbb{R}$, die als Vektorraum ungerade Dimension > 1 hat.*

Wir werden diesen Satz in Ergänzung 11.14 beweisen. Genauer kann man zeigen, dass die einzigen möglichen Dimensionen für eine Divisionsalgebra über $\mathbb{R}$ die Zahlen 1, 2 und 4 sind. (Dass es für diese Dimensionen tatsächlich eine Divisionsalgebra gibt, ist mit dem, was wir wissen, klar: $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$ und die Hamiltonschen Quaternionen $\mathbb{H}$.)

SATZ 6.61. *Es gibt keine endlich-dimensionale Divisionsalgebra über den komplexen Zahlen $\mathbb{C}$ von Vektorraum-Dimension > 1.*

Auch diesen Satz werden wir in Ergänzung 11.14 beweisen. (Allerdings müssen wir benutzen, dass jede nicht-konstante Polynomfunktion über den komplexen Zahlen eine Nullstelle besitzt. Dieses Ergebnis nennt man den Fundamentalsatz der Algebra.) □ Ergänzung 6.59

KAPITEL 13

Kodierungstheorie *

13.1. Einführung und Definitionen

In diesem Abschnitt erklären wir einige grundlegende Konzepte der *Kodierungstheorie*, um zu illustrieren, wie der Begriff des endlichen Körpers und speziell Methoden der linearen Algebra über endlichen Körpern dabei helfen, ein »real world problem« einer mathematischen Behandlung zugänglich zu machen.

Das Grundproblem der Kodierungstheorie ist, eine Nachricht effizient über einen Kommunikationskanal (ein Netzwerkkabel, eine WLAN-Verbindung, Speichern und Auslesen von Daten auf einer Festplatte, CD etc.) zu übermitteln, der die übertragenen Nachrichten mit einer gewissen Wahrscheinlichkeit verfälscht. Mit anderen Worten: Auch wenn ein Kratzer auf der CD ist, soll es möglich sein, die gewünschten Informationen zu extrahieren. Eine naive Möglichkeit wäre, zum Beispiel die Zahl 321 654 987 in der Form

321 654 987 321 654 987 321 654 987

zu speichern, d.h. die Information wird dreimal wiederholt. Wenn eine dieser 27 Ziffern geändert wird, kann man durch Vergleich der drei Kopien immer noch herausfinden, was die ursprüngliche Zahl war. Allerdings braucht man mit dieser Methode erheblich mehr Speicherkapazität (oder: eine Übertragung der Nachricht würde entsprechend länger dauern), nämlich dreimal soviel, wie für die eigentliche Nachricht.

In der Kodierungstheorie werden Möglichkeiten gesucht (und gefunden und untersucht), dasselbe Ziel zu erreichen und die Ursprungsnachricht möglichst wenig zu verlängern. Dieses Ziel ist nicht zu verwechseln mit der Verschlüsselungstheorie oder Kryptographie, in der man versucht, Nachrichten so umzuschreiben (zu *verschlüsseln*), dass sie einem Außenstehenden nicht verständlich sind, aber vom Adressaten wieder lesbar gemacht (*entschlüsselt*) werden können. Auch dabei gibt es interessante mathematische Fragen, die jedoch hier nicht das Thema sind; siehe aber Abschnitt 13.5 für eine Verbindung zwischen diesen beiden Themen.

Wir machen zwei Grundannahmen: Erstens: Alle Codewörter werden mit der gleichen Wahrscheinlichkeit als Nachricht verschickt. (Sonst wäre es vielleicht besser, den Code auf die häufiger verschickten Nachrichten hin zu optimieren.) Zweitens setzen wir voraus, dass für jedes gesendete Zeichen auch genau ein Zeichen beim Empfänger ankommt (möglicherweise jedoch ein anderes) und dass es für $m < n$ wahrscheinlicher ist, dass m (also weniger) Fehler bei der Übertragung passieren, als dass n Fehler auftreten. (Es wären auch Kommunikationskanäle denkbar, die immer direkt mehrere Zeichen verändern, wo aber nur sehr selten einzelne Fehler auftreten.) In sehr vielen Praxisanwendungen sind das realistische Voraussetzungen. Man kann die Theorie erweitern auf Situationen, wo diese Annahmen verletzt sind, das wollen wir aber an dieser Stelle nicht tun.

BEISPIEL 13.1. Ein einfaches Beispiel, das das grundlegende Prinzip illustriert, ist die Verwendung eines Paritätsbits: Die zu sendende Nachricht wird in Pakete von »Wörtern« einer festen Länge (zum Beispiel sieben Zeichen), die jeweils 0 oder 1 sein können (man spricht von 7 *Bits*). Zusätzlich wird immer ein weiteres Zeichen hinzugefügt, und zwar eine 0 oder 1, so dass von den acht Bits eine gerade Anzahl gleich 1 ist.

Wenn bei der Übertragung genau ein Bit falsch übertragen wird, hat das empfangene Wort eine ungerade Anzahl von Einsen. Die Empfänger*in kann den Übertragungsfehler also feststellen (allerdings nicht herausfinden, was die ursprüngliche Nachricht war). ◊

Wenn über den Kommunikationskanal die Symbole 0 oder 1 übertragen werden können, und die Wahrscheinlichkeit der korrekten Übertragung für jedes Zeichen durch dieselbe Zahl p, $0 \leq p \leq 1$ gegeben ist (zum Beispiel bedeutet $p = 0,85$, dass in 85% der Fälle das gesendete Zeichen richtig übertragen wird), dann gilt der Satz von Shannon ([**vL**] Theorem 2.2.3), der umgangssprachlich ausgedrückt Folgendes besagt (die präzise Formulierung dort beinhaltet auch eine Aussage zur Übertragungsrate):

Sei $p \neq \frac{1}{2}$. Für jede vorgegebene positive (kleine) Wahrscheinlichkeit ε gibt es Codes, bei denen die Wahrscheinlichkeit, ein gesendetes Codewort falsch zu dekodieren, kleiner als ε ist. (Wichtig ist dabei, dass man sich erlaubt, ausreichend lange Codewörter zu benutzen. Je kleiner ε ist, desto längere Codewörter wird man in der Regel benötigen.)

Nachrichten zu betrachen, die als eine Folge von Nullen und Einsen geschrieben werden, ist oft naheliegend. Unter anderem, weil auch ein Computer seine Daten so abspeichert. Natürliche Zahlen haben die Binärdarstellung, die aus Nullen und Einsen besteht; Buchstaben können in Zahlen umgeschrieben und dann ebenso in Binärdarstellung geschrieben werden, usw. Zerlegt man die Nachricht in Abschnitte der Länge m, so kann man jeden solchen Abschnitt als ein Element von $\mathbb{F}_2^m$ betrachten.

Vom mathematischen Aufwand können wir aber an dieser Stelle statt $\mathbb{F}_2$ irgendeinen endlichen Körper betrachten und wollen das dementsprechend tun. (Sie können aber das Kapital auch einfach mit $q = 2$ weiterlesen.)

Sei K ein endlicher Körper, und sei q die Anzahl der Elemente von K. Man kann zeigen (Ergänzung 6.51), dass q eine Primzahlpotenz sein muss, etwa $q = p^d$ mit einer Primzahl p. Dann ist p die Charakteristik von K, also die kleinste positive Zahl, so dass $1 + \cdots + 1 = 0$ (mit p Summanden auf der linken Seite), vergleiche Abschnitt 4.2.2. Wir setzen wie oben voraus, dass alle Nachrichten in Abschnitte von k-Tupeln in K zerteilt werden, also als eine Folge von Vektoren in K^k. Sei $N \subseteq K^k$ die Menge aller »Wörter«, also aller Elemente von K^k, die tatsächlich als Nachrichten(-teile) verwendet werden sollen.

Das Grundprinzip der Kodierungstheorie ist nun, die Nachrichtenwörter vor der Übertragung durch andere Wörter zu ersetzen und damit auf geschickte Weise eine Redundanz hinzuzufügen, die es der Empfänger*in ermöglicht, Übertragungsfehler festzustellen und bestenfalls automatisch zu korrigieren. Dazu suchen wir eine injektive Abbildung $c\colon N \to K^n$ von der Menge aller Nachrichtenwörter nach K^n (für ein geeignetes n, das in der Regel größer sein wird als m). Statt einer Nachricht $v \in K^k$ wird dann $c(v)$ übertragen. Entscheidend ist dabei, eine geeignete Wahl für die Abbildung c zu treffen, d.h. zu entscheiden, welche der q^n Elemente von K^n in ihrem Bild liegen und daher tatsächlich verwendet werden, damit man auch bei (wenigen) Fehlern in der Übertragung noch auf den gesendeten Vektor zurückschließen kann. Das Bild der Abbildung c nennt man den verwendeten *Code*; c ist die *Kodierungsfunktion*. Für unsere weiteren Betrachtungen werden N und c keine große Rolle spielen. Wir konzentrieren uns auf das Bild der Abbildung c und machen die folgende Definition:

Definition 13.2. Sei K ein endlicher Körper, sei $n \geq 1$. Ein *Code* der Länge n über K ist eine Teilmenge $C \subseteq K^n$. ⊣

Wie in der Kodierungstheorie üblich, wollen wir in diesem Kapitel **die Elemente von K^n als Zeilenvektoren verstehen**, wir identifizieren also $K^n = M_{1\times n}(K)$.

Um der Empfänger*in einer Nachricht ein Verfahren an die Hand zu geben, um Übertragungsfehler festzustellen und sie gegebenenfalls korrigieren zu können, definiert man

DEFINITION 13.3. Seien K ein endlicher Körper und C ein Code der Länge n über K.

(1) Für $v = (v_1, ..., v_n), w = (w_1, ..., w_n) \in K^n$ ist die *Hamming-Distanz* zwischen v und w definiert als
$$d(v, w) = \#\{i;\ v_i \neq w_i\},$$
also die Anzahl der Einträge der Vektoren v und w, die sich unterscheiden.

(2) Die (minimale) Hamming-Distanz von C ist
$$d(C) = \min\{d(v, w);\ v, w \in C,\ v \neq w\}.$$

⊣

Es ist klar, dass man keine vernünftigen Aussagen treffen kann, wenn der Kommunikationskanal zu viele Einträge der gesendeten Nachricht verfälscht. Der Begriff der Hamming-Distanz ermöglicht uns eine präzise Aussage (Satz 13.5), mit wie vielen Fehler in einer Nachricht es noch möglich ist festzustellen, dass ein Übertragungsfehler aufgetreten sein muss, und bei wie vielen Fehlern sogar die ursprüngliche Nachricht gefunden werden kann.

Der Code aus Beispiel 13.1 hat die minimale Hamming-Distanz 2: Es gibt zwar Codewörter, die sich an nur zwei Stellen unterscheiden. Die Paritätsbedingung, dass die Anzahl der Einsen in jedem Codewort gerade sein muss, bewirkt aber, dass es keine zwei Codewörter mit Hamming-Distanz 1 geben kann.

BEISPIEL 13.4. Der folgende Code $C \subset \mathbb{F}_2^7$ hat Hamming-Distanz 3, wie man leicht überprüft. Wir schreiben die Zeilenvektoren hier ohne Kommata, um es etwas übersichtlicher zu machen.

$$\begin{aligned} C = \{&(1000111),\\ &(0100110),\\ &(0010101),\\ &(0001011)\} \end{aligned}$$

Wenn bei der Übertragung eines der Wörter aus C ein oder zwei Einträge falsch übertragen werden, kommt bei der Empfänger*in ein Wort an, das kein Element von C ist. Dieser Übertragungsfehler lässt sich also erkennen. Wenn genau ein Eintrag falsch übertragen wird, dann lässt sich durch Vergleich mit den Elementen von C auch feststellen, welches Wort übertragen wurde. Der Code kann also 1 Fehler »korrigieren«. Siehe Satz 13.5.

Es gibt Teilmengen $C' \subset \mathbb{F}_2^7$, die C als echte Teilmenge enthalten, und auch Hamming-Distanz 3 haben (und daher »bessere« Codes sind). Versuchen Sie, ein möglichst großes C' zu finden! Siehe auch Abschnitt 13.4. ◊

Die Funktion $d\colon K^n \times K^n \to \mathbb{Z}_{\geq 0}$ hat die Eigenschaften einer Metrik (oder Distanzfunktion), d.h.

(a) Es gilt $d(v, w) = 0$ genau dann, wenn $v = w$,

(b) Es gilt $d(v, w) = d(w, v)$ für alle $v, w \in K^n$,

(c) Es gilt die *Dreiecksungleichung*
$$d(u, v) + d(v, w) \geq d(u, w) \qquad \text{für alle } u, v, w \in K^n.$$

Alle drei Eigenschaften sind leicht einzusehen.

Im folgenden Satz bezeichnet $\lceil - \rceil$ die *Aufrundungsfunktion*, manchmal auch die *obere Gauß-klammer* genannt: Für eine reelle Zahl x ist $\lceil x \rceil$ die kleinste ganze Zahl, die $\geq x$ ist. Zum Beispiel ist $\lceil x \rceil = x$ für alle $x \in \mathbb{Z}$ und $\lceil \frac{1}{2} \rceil = 1$. Wie man leicht sieht, gilt $2\lceil \frac{d}{2} \rceil \leq d + 1$ für jede ganze Zahl d. Das werden wir im Beweis benutzen.

SATZ 13.5. *Sei C ein Code der Länge n über K. Wir betrachten das Szenario, dass die Absender∗in eine Nachricht $v \in K^n$ verschickt. Den Vektor, den die Empfänger∗in erhält, nennen wir w.*

(1) *Wenn bei der Übertragung höchstens $d(C) - 1$ Einträge des Vektors v falsch übertragen werden, dann gilt: Ist $w \in C$, so ist $w = v$. Ist $w \notin C$, so muss es Übertragungsfehler gegeben haben. Wir sagen, dass der Code C bis zu $d(C) - 1$ Übertragungsfehler erkennen kann.*

(2) *Wenn bei der Übertragung höchstens $\lceil d(C) / 2 \rceil - 1$ Einträge des Vektors v falsch übertragen werden, dann ist v das eindeutig bestimmte Element von C mit $d(v, w) \leq \lceil d(C) / 2 \rceil - 1$. Wir können also die Originalnachricht aus w rekonstruieren. Wir sagen, dass der Code C bis zu $\lceil d(C) / 2 \rceil - 1$ Übertragungsfehler erkennen kann.*

BEWEIS. zu (1). Da höchstens $d(C) - 1$ Einträge falsch übertragen wurden, gilt $d(v, w) < d(C)$. Ist $w \in C$, so folgt daraus $v = w$ nach Definition von $d(C)$ als Minimum der Distanzen von verschiedenen Elementen aus C.

Ist $w \notin C$, dann müssen natürlich Übertragungsfehler aufgetreten sein, da *alle* Nachrichten Elemente aus C sind.

zu (2). Es ist klar, dass die Voraussetzung $d(v, w) \leq \lceil d(C) / 2 \rceil - 1$ impliziert. Es ist nur noch zu zeigen, dass es kein Element $v' \in C$, $v \neq v'$, geben kann mit $d(v', w) \leq \lceil d(C) / 2 \rceil - 1$. In diesem Fall wäre aber

$$d(C) \leq d(v, v') \leq d(v, w) + d(v', w) \leq d(C) - 1,$$

ein Widerspruch. Hier haben wir benutzt, dass die Hamming-Distanz die Dreiecksungleichung erfüllt und symmetrisch ist. □

Bei der Wahl eines Codes würden wir also prinzipiell C gerne so wählen, dass $\#C$ groß, $d(C)$ groß und n klein sind. Außerdem ist es für die praktische Anwendung wichtig, dass die Funktionen *Kodieren einer Nachricht* und *Dekodieren einer Nachricht* möglichst einfach sind. Zum Beispiel wäre es praktisch, das De-/Kodieren einer Nachricht durch eine einfache Rechnung durchzuführen (im Vergleich dazu, dass man ein riesiges »Wörterbuch« speichern müsste, in dem jede Übersetzung nachgeschlagen werden muss).

13.2. Lineare Codes

Bisher haben wir noch keine lineare Algebra gesehen. Das wollen wir jetzt ändern. Nach dem vorherigen Abschnitt stellt sich die Frage, wie man geeignete Codes C findet. Dabei ist es naheliegend, die Vektorraumstruktur von K^n auszunutzen.

DEFINITION 13.6. Ein Code $C \subseteq K^n$ heißt *linearer Code*, wenn C ein K-Untervektorraum von K^n ist.

Wenn $k = \dim C$ ist, dann sagt man auch, C sei ein $[n, k]$-Code (oder ein $[n, k, d]$-Code wobei $d = d(C)$ die minimale Hamming-Distanz von C ist). ⊣

Wenn C ein Untervektorraum ist, können wir die minimale Hamming-Distanz berechnen, indem wir alle Vektoren mit 0 vergleichen:

LEMMA 13.7. *Ist C ein linearer Code, so gilt*

$$d(C) = \min\{d(0, v);\ v \in C \setminus \{0\}\}.$$

BEWEIS. Für $v, w \in K^n$ gilt $d(v, w) = d(v - w, 0)$, wie man unmittelbar nachprüft. Weil für $v, w \in C$ auch $v - w$ in C liegt, folgt daraus die Behauptung. □

Wir suchen dann lineare Codes, so dass dim C und $d(C)$ möglichst groß sind, aber dabei n möglichst klein ist.

Wie oben gesagt, wollen wir die Elemente von K^n als *Zeilenvektoren* betrachten.

DEFINITION 13.8. Sei $C \subseteq K^n$ ein linearer Code. Eine *Erzeugermatrix* (oder *Generatormatrix*) ist eine Matrix, deren Zeilen eine Basis von C bilden.

Wir sagen, eine Erzeugermatrix sei in *Standardform*, wenn sie eine Blockmatrix der Form $\begin{pmatrix} E_k & A \end{pmatrix}$ mit $A \in M_{k\times(n-k)}(K)$ ist. ⊣

Wenn G eine Erzeugermatrix des linearen Codes C ist, dann ist die Abbildung $w \mapsto wG$ ein Isomorphismus $K^k \to C$. Wenn wir die Ursprungsnachrichten als Wörter in K^k schreiben, ist die Kodierungsfunktion also einfach die durch G gegebene lineare Abbildung (im Zeilenvektor-Sinn).

BEISPIEL 13.9. Wir hatten zu Beginn den Paritätscheck-Code betrachtet, der einem Wort aus sieben Bits (Nullen und Einsen) eine achte Null oder Eins so hinzufügt, dass die Gesamtzahl der Einsen gerade ist.

Die Menge der Nachrichten ist also $\mathbb{F}_2^7$, der Code C ist gegeben durch

$$C = \{(x_1, \ldots, x_8) \in \mathbb{F}_2^8;\ \sum_{i=1}^{8} x_i = 0\},$$

wobei die Summe in $\mathbb{F}_2$ zu bilden ist. Der Code C besitzt eine Erzeugermatrix in Standardform, und zwar

$$G = \begin{pmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \end{pmatrix}.$$

◊

Ist C ein linearer Code, so hat C höchstens eine Erzeugermatrix in Standardform.

Für die Qualität eines Codes tut es offenbar nichts zur Sache, wenn wir eine Permutation der Standardbasisvektoren von K^n durchführen (also C durch sein Bild unter einem Automorphismus von K^n ersetzen, der durch eine Permutationsmatrix gegeben ist). Wir nennen zwei Codes, die durch eine Operation dieser Art ineinander übergehen, *äquivalent*. Da wir jede Matrix durch elementare Zeilenumformungen auf reduzierte Zeilenstufenform bringen können und diese den von den Zeilen aufgespannten Untervektorraum nicht verändern, ist klar, dass es zu jedem linearen Code einen äquivalenten Code gibt, der eine Erzeugermatrix in Standardform besitzt.

DEFINITION 13.10. Sei C ein linearer $[n,k]$-Code über K. Eine Paritätsprüfmatrix ist eine Matrix $H \in M_{(n-k)\times n}(K)$, so dass für alle $c \in K^n$ gilt:

$$c \in C \quad \Leftrightarrow \quad Hc^t = 0,$$

d.h. C ist die Lösungsmenge des durch $Hx = 0$ gegebenen linearen Gleichungssystems (wenn wir die Elemente von C zu Spaltenvektoren transponieren). ⊣

Ist $G = (E_k \mid A)$ eine Erzeugermatrix von C in Standardform, dann ist $H = (-A^t | E_{n-k})$ eine Paritätsprüfmatrix, denn es gilt offenbar $HG^t = 0$, also $\{c^t;\ c \in C\} \subseteq \mathrm{Ker}(H)$, und $\mathrm{rg}(H) = n - k$, so dass sogar $\{c^t;\ c \in C\} = \mathrm{Ker}(H)$ folgt.

Die minimale Hamming-Distanz eines Codes hat die folgende Interpretation in Termen einer Paritätsprüfmatrix:

LEMMA 13.11. *Sei C ein linearer $[n,k]$-Code mit minimaler Hamming-Distanz $d(C)$. Sei H eine Paritätsprüfmatrix von C, und sei d die kleinste Zahl, so dass je $d-1$ Spalten von H stets linear unabhängig sind, aber so dass es d Spalten in H gibt, die linear abhängig sind. Dann gilt $d = d(C)$.*

BEWEIS. Dass es d Spalten in H gibt, die linear abhängig sind, ist äquivalent dazu, dass die Lösungsmenge des linearen Gleichungssystems $Hx = 0$ einen Vektor x enthält, in dem höchstens d Einträge $\neq 0$ sind. Aus diesem Argument und Lemma 13.7 folgt sofort die Behauptung. □

13.3. Die Gilbert-Varshamov-Schranke

13.4. Hamming-Codes

13.5. Das McEliece-Verfahren

Ein wichtiger Aspekt, den wir bisher außen vor gelassen haben (und den wir auch hier nur indirekt streifen), ist die Frage nach einer effizienten Kodierungs- bzw. Dekodierungsfunktion für einen Code. Je nach Anzahl der Codewörter ist es sicherlich unpraktikabel, ein empfangenes Wort mit jedem Codewort zu vergleichen und dasjenige mit minimalem Hammingabstand herauszusuchen. Wenn man nur irgendeine Erzeugermatrix G eines Codes kennt, sind die Möglichkeiten der schnellen Dekodierung (bei großen Codes) eingeschränkt. Das Kodieren geht aber relativ schnell, weil man hierzu nur ein Matrizenprodukt der Form wG (für ein zu versendendes Wort w) berechnen muss.

Dass es Codes gibt, bei denen es auch für große Codes schnelle Dekodierfunktionen gibt (zum Beispiel die sogenannten Goppa-Codes) macht sich das Verschlüsselungsverfahren von Robert McEliece zu Nutze, das wir hier skizzieren wollen. Es handelt sich um ein Public-Key-Verfahren, das auf Kodierungstheorie und Linearer Algebra basiert. Eine Besonderheit ist, dass es nach jetzigem Kenntnisstand nicht anfällig ist für Angriffe mit Quantencomputern (anders als die meisten Verfahren, die momentan gängig sind). Ein Nachteil ist, dass die Schlüssel, die man dafür speichern und versenden muss, relativ groß sind.

Unter einem Public-Key-Verfahren versteht man ein Verschlüsselungsverfahren, bei dem die spätere Empfänger*in einer verschlüsselten Nachricht alle Informationen, die die Absender*in der Nachricht zum Verschlüsseln benötigt, öffentlich zur Verfügung stellen kann (insbesondere könnte man diese Informationen über Kanäle verschicken, die von anderen abgehört werden können). Dieser »Public Key« muss natürlich die Eigenschaft haben, dass er zwar das Verschlüsseln, jedoch nicht das Entschlüsseln einer Nachricht erlaubt.

Die Empfängerin der verschlüsselten Nachricht, die wir wie in der Kryptographie üblich Alice nennen wollen, wählt die folgenden Informationen. Diese bilden den *privaten Schlüssel*, den sie geheim hält.

Einen (geeigneten) linearen $[n,k]$-Code C über $\mathbb{F}_2$, der bis zu t Fehler korrigieren kann. (Damit das Verfahren sicher ist, werden Werte von $n = 2048$, $k = 1751$, $t = 27$ empfohlen; für Sicherheit gegen Quantencomputerangriffe noch höhere Werte.) Sie wählt den Code so, dass sie eine schnelle Dekodierfunktion kennt. Sei G eine Erzeugermatrix dieses Codes in Standardform.

Alice wählt außerdem eine invertierbare Matrix $S \in GL_k(\mathbb{F}_2)$ und eine Permutationsmatrix $P \in GL_n(\mathbb{F}_2)$. Sie berechnet das Matrizenprodukt $G' := SGP$ und veröffentlicht dann den folgenden

$$\text{Öffentlichen Schlüssel:} \quad (G', t).$$

Während die Matrix G (in Standardform) in der Regel Rückschlüsse darauf zulassen wird, aus welcher Familie von Codes Alice ihren Code gewählt hat, und damit auf eine effektive Dekodierfunktion, ist das für die Matrix G' nicht der Fall.

Bob, der Alice eine Nachricht schicken möchte, schreibt seine Nachricht im Klartext als Folge von Wörtern $m \in \mathbb{F}_2^k$. Für jedes m bildet er $c' := mG'$ (die »regulär« mit dem Code mit Erzeugermatrix G' kodierte Nachricht), wählt zufällig ein Element $z \in \mathbb{F}_2^n$ mit t Einsen und $n - t$ Nullen, und schickt Alice die Nachricht $c := c' + z$. Es werden durch die Addition von z also künstlich t Fehler eingefügt.

Alice berechnet aus c das Word $cP^{-1} (= c'P^{-1} + zP^{-1})$. Da P eine Permutationsmatrix ist, unterscheidet sich dieses Wort an genau t Stellen von mSG. Mit der Dekodierfunktion für den Code mit Erzeugermatrix G kann Alice daraus mS berechnen, und findet damit die ursprüngliche Nachricht als $m = (mS)S^{-1}$.

Die Sicherheit des Verfahrens beruht darauf, dass die Werte n, k und t so gewählt werden, dass die Berechnung von m aus $mG' + z$ nicht in akzeptabler Zeit möglich ist. (Die Durchführbarkeit beruht darauf, dass es eben doch möglich ist, wenn man die zusätzlichen strukturellen Informationen kennt, die Alice zur Hand hat.)

Weitere Informationen: Wikipedia (English)[I]

13.6. Quellen/Weiterführende Literatur

J. H. van Lint, Introduction to Coding Theory, Springer Graduate Texts in Mathematics **86**, 3rd ed., Springer 1999.

J. H. van Lint, G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar **12**, Birkhäuser 1988.

Siehe auch [**Ma**] Kap. 28, Kap. 29 für weiterführende Fragen in der Kodierungstheorie, die man mit linearer Algebra beantworten kann.

[I] `https://en.wikipedia.org/wiki/McEliece_cryptosystem`

KAPITEL 14

Graphentheorie *

14.1. Definition

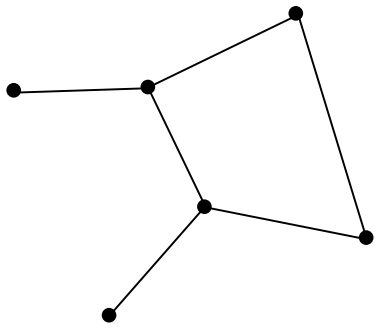
DEFINITION 14.1. Ein (endlicher) Graph $G = (\mathbb{E}, \mathbb{K})$ ist ein Paar, das besteht aus

(a) einer Menge $\mathbb{E}$, deren Elemente die *Ecken* oder *Knoten* des Graphen genannt werden,

(b) einer Menge $\mathbb{K}$ von zweielementigen Teilmengen von $\mathbb{E}$, deren Elemente die *Kanten* des Graphen G genannt werden.

⊣

Wir können einen Graphen durch eine Zeichnung visualisieren, indem wir die Ecken des Graphen als »dicke Punkte« zeichnen, und zwei Ecken P_1, P_2 genau dann verbinden, wenn die Teilmenge $\{P_1, P_2\}$ ein Element der Menge $\mathbb{K}$ ist.
Die Abbildung zeigt einen Graphen mit 6 Ecken.
Man beachte aber: Nicht jeder Graph lässt sich »überschneidungsfrei« in der Ebene zeichnen. Siehe Abschnitt 14.6.



Der hier definierte Begriff des Graphen hat nichts mit Funktionsgraphen zu tun.

BEMERKUNG 14.2. In unserer Definition

- kann keine Kante einen Knoten mit sich selbst verbinden,
- gibt es zwischen zwei Knoten entweder keine oder eine Kante (aber nicht mehrere).

Je nachdem, wozu man die Theorie benutzen möchte, könnte man die Definition abändern und allgemeinere Formen von Graphen erlauben, als wir es hier tun.

Eine andere nützliche Variante ist der Begriff des *gerichteten Graphen*, in dem jede Kante des Graphen mit einer Richtung versehen wird (und dann auch erlaubt ist, dass zwei Knoten durch je eine Kante in die beiden möglichen Richtungen miteinander verbunden sind). Die Netzwerke in Frage 2.7 kann man als gerichtete Graphen betrachten. ◊

Wie genau die Ecken eines Graphen benannt werden (ob mit $1, 2, 3, \ldots$ oder $A, B, C, \ldots$, oder noch anders) spielt für uns keine Rolle. Wir definieren deshalb:

DEFINITION 14.3. Seien $G = (\mathbb{E}, \mathbb{K})$ und $G' = (\mathbb{E}', \mathbb{K}')$ Graphen. Ein *Isomorphimus* ist eine Bijektion $\varphi\colon \mathbb{E} \to \mathbb{E}'$, so dass für alle $i, j \in \mathbb{E}$ gilt: $\{i, j\} \in \mathbb{K} \Leftrightarrow \{\varphi(i), \varphi(j)\} \in \mathbb{K}'$. Zwei Graphen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt. ⊣

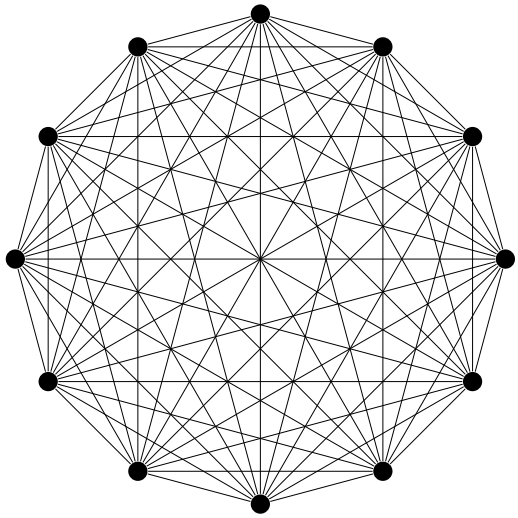


ABBILDUNG 1. Der Graph K_{12}: Jede der 12 Ecken ist mit jeder anderen Ecke durch eine Kante verbunden.

Alle Eigenschaften von Graphen, die wir im folgenden betrachten, werden durch Isomorphismen erhalten.

Es ist allerdings mitunter nicht leicht festzustellen, ob zwei gegebene Graphen zueinander isomorph sind oder nicht. (Natürlich gibt es prinzipiell die Möglichkeit, alle Bijektionen zwischen den Eckenmengen durchzuprobieren und zu testen, ob es sich um Isomorphismen von Graphen handelt. Wenn die Anzahl der Ecken nicht sehr klein ist, ist das aber nicht praktikabel.)

DEFINITION 14.4. Sei $G = (\mathbb{E}, \mathbb{K})$ ein Graph. Ein Graph $G' = (\mathbb{E}', \mathbb{K}')$ heißt ein *Teilgraph* von G, wenn $\mathbb{E}' \subseteq \mathbb{E}$ und $\mathbb{K}' \subseteq \mathbb{K}$. ⊣

14.2. Ramsey-Zahlen

BEISPIEL 14.5. Sei $n \geq 1$ eine natürliche Zahl. Der *vollständige Graph* mit n Ecken ist der Graph K_n mit Eckenmenge $\mathbb{E} = \{1, ..., n\}$ und Kantenmenge $\{\{i, j\};\ i, j = 1, ..., n,\ i \neq j\}$, d.h. je zwei verschiedene Punkte sind durch eine Kante verbunden. ◊

Zum Beispiel ist der Graph K_3 einfach ein »Dreieck«, d.h. er besteht aus drei Ecken, die jeweils durch eine Kante miteinander verbunden sind. Mit wachsendem n steigt die Anzahl der Kanten in K_n allerdings sehr schnell.

Sei $n \geq 1$ eine fixierte natürliche Zahl. Wir wollen nun als zusätzliche Information in dem Graphen K_n jede Kante entweder blau oder rot einfärben, wie im Beispiel $n = 5$ in Abbildung 2 gezeigt. Die Frage, die wir dann betrachten, ist, ob der eingefärbte Graph K_n einen Teilgraphen der Form K_m hat, dessen Kanten alle blau oder alle rot sind. In dieser Sache gilt der folgende Satz.

SATZ 14.6 (Ramsey). *Seien $b, r \geq 1$ natürliche Zahlen. Dann existiert eine Zahl N, so dass für alle $n \geq N$ und jede blau/rote Kantenfärbung des Graphen K_n ein roter r-Teilgraph oder ein blauer b-Teilgraph existiert.*

Die kleinste solche Zahl N nennen wir die Ramsey-Zahl *zu b und r und bezeichnen sie mit $R(b, r)$.*

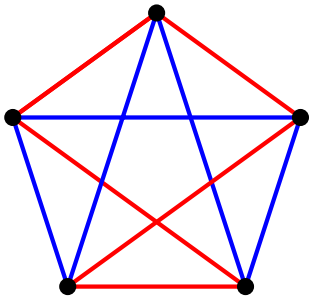


ABBILDUNG 2. Der Graph K_5 mit blau/rot eingefärbten Kanten. Es gibt weder ein blaues noch ein rotes Dreieck.

REFERENZ ZUM BEWEIS. Man kann dies durch Induktion nach $b + r$ beweisen, siehe zum Beispiel Ramsey's theorem (Wikipedia)[I]. □

BEISPIEL 14.7. Es ist $R(3,3) = 6$. In der Tat zeigt Abbildung 2, dass $R(3,3) > 5$ sein muss. Es ist daher nur noch zu zeigen, dass es in jedem rot/blau gefärbten Graphen K_6 ein rotes Dreieck oder ein blaues Dreieck gibt.

Wir fixieren eine Färbung der Kanten von K_6. Sei i eine fixierte Ecke. Wie jede Ecke in K_6 ist sie mit 5 anderen Ecken verbunden, und von diesen Kanten können wir mindestens 3 finden, die dieselbe Farbe haben. Indem wir rot und blau vertauschen, falls erforderlich, können wir für das Argument ohne Einschränkung annehmen, dass von i drei rote Kanten ausgehen. Wenn von den Verbindungen zwischen den drei Endpunkten dieser Kanten eine rot ist, dann haben wir ein rotes Dreieck gefunden. Sind die Verbindungen alle drei blau, dann bilden sie ein blaues Dreieck.

Wir können der Aussage folgendermaßen einen Alltagsbezug geben (auch wenn der Nutzen fragwürdig ist): Stellen Sie sich vor, auf einer Party sind mindestens 6 Personen anwesend, von denen je zwei entweder miteinander bekannt, oder einander unbekannt sind. Dann gibt es eine Dreiergruppe von Personen, die sich alle gegenseitig kennen, oder eine Dreiergruppe von Personen, die sich gegenseitig nicht kennen. ◊

BEISPIEL 14.8. Die Ramsey-Zahl $R(5,5)$ ist nicht bekannt!

Man kann zeigen, dass

$$43 \leq R(5,5) \leq 48,$$

es handelt sich also nicht um eine besonders große Zahl. Dennoch ist die Berechnung so komplex, dass sie bisher nicht gelungen ist. (Das Problem ist, dass zum Beispiel K_{43} insgesamt 946 Kanten hat und damit die Zahl der möglichen Kantenfärbungen astronomisch hoch ist.) ◊

14.3. Die Adjazenzmatrix eines Graphen

Problemstellung Was ist eine gute Methode, um in einem gegebenen Graphen alle Wege einer fixierten Länge zu zählen? Wir werden dieses Problem mithilfe des Matrizenprodukts »lösen«. Je nachdem, wie groß der Graph ist, ist die Rechnung eventuell nicht ohne Weiteres durchführbar. Den Matrizenkalkül ins Spiel zu bringen ist aber jedenfalls eine Verbesserung.

Wir stellen durch die folgende Definition eine Verbindung zur linearen Algebra her, die zwar recht banal aussieht, aber dennoch sehr nützlich ist.

[I] https://en.wikipedia.org/wiki/Ramsey%27s_theorem

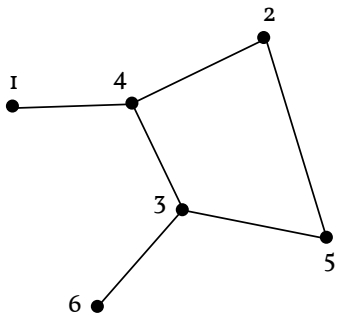
DEFINITION 14.9. Sei $G = (\mathbb{E}, \mathbb{K})$ ein Graph. Wir fixieren eine Identifizierung $\mathbb{E} = \{1, ..., n\}$. Die *Adjazenzmatrix* (oder *Nachbarschaftsmatrix*) von G ist die Matrix $A = (a_{ij}) \in M_{n\times n}(\mathbb{Q})$ mit

$$a_{ij} = \begin{cases} 1 & i, j \text{ sind durch eine Kante verbunden,} \\ 0 & \text{sonst.} \end{cases}$$

⊣

BEISPIEL 14.10. (1) Die Adjazenzmatrix des Graphen in der nebenstehenden Abbildung ist

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$



(2) Die Adjazenzmatrix von K_n ist die Matrix, deren Diagonaleinträge 0 und deren andere Einträge alle 1 sind.

◊

Interessanterweise haben auch die Potenzen der Adjazenzmatrix eine graphentheoretische Interpretation. Sei G ein Graph mit Eckenmenge $\{1, ..., n\}$ und Adjazenzmatrix A. Ein Produkt der Form $a_{ij}a_{jk}$ ist genau dann 1, wenn in G ein »Weg« $i - j - k$ existiert, d.h. wenn sowohl i und j als auch j und k miteinander verbunden sind. Wir definieren

DEFINITION 14.11. Sei G ein Graph. Ein *Weg* (oder *Pfad*) in G ist ein Tupel $(e_0, ..., e_l)$ von Ecken in G, so dass für alle i die Ecken e_i und e_{i+1} durch eine Kante verbunden sind. Wir sprechen auch von einem Weg von e_0 nach e_l.

Die Zahl l heißt die *Länge des Wegs*. ⊣

Dann ist $\sum_{j=1}^{n} a_{ij}a_{jk}$ gerade die Anzahl der Wege der Länge 2 von i nach k.

SATZ 14.12. *Sei G ein Graph mit Eckenmenge $\{1, ..., n\}$ und Adjazenzmatrix A. Sei l eine natürliche Zahl. Sei $B = (b_{ij})_{i,j} = A^l$. Dann ist b_{ij} die Anzahl der Wege der Länge l von i nach j in G.*

BEWEIS. Wir führen Induktion nach l. Für $l = 1$ ist die Sache klar. (Und auch für $l = 0$, wenn man möchte: Ein Weg der Länge 0 ist nichts anderes als eine Ecke in G.)

Sei nun $l > 1$, und sei $B = (b_{ij})_{i,j} = A^{l-1}$. Ein Weg der Länge l von i nach k lässt sich zerlegen als ein Weg von i zu einer Ecke j der Länge $l - 1$ und dem letzten Schritt des Weges von j nach k, d.h. j muss mit k benachbart sein. Die Anzahl der Wege der Länge l ist daher die Summe aller b_{ij} für diejenigen j, die mit k benachbart sind – also die Summe $\sum_{j=1}^{n} b_{ij}a_{jk}$, und das ist gerade der Eintrag von A^l an der Stelle (i, j). □

Wir können also Matrizenrechnung benutzen, um die Anzahl der Wege einer vorgegebenen Länge zwischen zwei Knoten in einem Graphen zu berechnen. Um zum Beispiel alle Wege der Länge 16 zu zählen, muss man für die Adjazenzmatrix A die 16-te Potenz ausrechnen. Ähnlich wie in Beispiel 5.60 kann man das mit 4 Matrixmultiplikationen machen ($A^2 = AA$, $A^4 = A^2A^2$, ...). Das ist wesentlich effizienter, als direkt im Graphen »herumzuprobieren«.

BEMERKUNG 14.13. Offenbar ist ein Graph durch seine Adjazenzmatrix (bis auf Isomorphie, also bis auf die Benennung der Ecken) eindeutig bestimmt. Überlegen Sie sich zur Übung, welche Matrizen als Adjazenzmatrix eines Graphen auftreten.

Andererseits ist die Adjazenzmatrix eines Graphen erst dann eindeutig festgelegt, wenn wir eine Nummerierung der Ecken fixieren, denn wir müssen ja wissen, auf welche Ecke sich die Einträge der ersten Zeile beziehen, usw. Wenn wir die Ecken anders nummerieren, erhalten wir in aller Regel eine andere Matrix. Es ist aber leicht zu sehen, wie sich die beiden Matrizen voneinander unterscheiden: Wir müssen die Zeilen und die Spalten der ersten Matrix so vertauschen, wie es der Umnummerierung der Ecken entspricht. Das bedeutet, dass die Matrizen durch Konjugation mit einer Permutationsmatrix auseinander hervorgehen.

Das gleiche Argument können wir benutzen, um zu sehen, dass die Adjazenzmatrizen von zwei isomorphen Graphen zueinander konjugiert sind. Daraus ergibt sich eine Möglichkeit, um zu zeigen, dass zwei Graphen nicht isomorph sind: Nämlich zu zeigen, dass die zugehörigen Adjazenzmatrizen nicht zueinander konjugiert sind (zum Beispiel, weil sie nicht dieselben Eigenwerte haben). ◊

14.4. Teildreiecke suchen

In diesem Abschnitt untersuchen wir die Frage, wie wir in einem Graphen G »Dreiecke«, das heißt Teilgraphen der Form K_3, finden können. Dazu arbeiten wir wieder mit der Adjazenzmatrix des Graphen.

Sei also A die Adjazenzmatrix (für eine fixierte Eckennummerierung) und sei $B = (b_{ij})_{i,j} = A^2$.

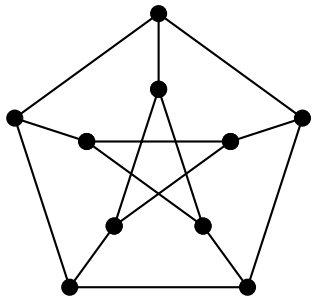
Dann können wir die Frage nach einem Dreieck in G auch so umformulieren: Wir suchen Paare (i, j) von Ecken in G mit $a_{ij} \neq 0$, $b_{ij} \neq 0$ (denn das bedeutet erstens, dass i und j benachbart sind, und zweitens, dass zwischen i und j ein Weg der Länge 2 existiert; bezeichnet k den Zwischenschritt auf diesem Weg, dann sind i, j und k paarweise miteinander verbunden und bilden daher ein Dreieck).

Abgesehen davon, dass das ursprüngliche Problem damit (vielleicht) eleganter ausgedrückt ist, kann man auch (für sehr große Graphen) einen Vorteil daraus ziehen, was die konkrete Berechnung angeht. Wenn man naiv in dem Graphen G nach einem Dreieck sucht, müsste man alle drei-elementigen Teilmengen der Eckenmenge $\mathbb{E}$ untersuchen; das wären größenordnungsmäßig $(\#\mathbb{E})^3$ Rechenoperationen. Für die Berechnung des Quadrats A^2 der Adjazenzmatix braucht man mit dem naiven Verfahren zur Berechnung des Matrizenprodukts zwar auch größenordnungsmäßig $(\#\mathbb{E})^3$ Rechenoperationen. Es gibt aber bessere Algorithmen (vgl. Ergänzung 5.33).

Quelle: [**Ma**] Kap. 10.

14.5. Eigenwerte der Adjazenzmatrix

Der Petersen-Graph ist der hier abgebildetete Graph. Er hat 10 Ecken und an jeder Ecke gehen 3 Kanten ab. Es ist klar, dass wir ihn als Teilgraph des vollständigen Graphen K_{10} mit 10 Ecken einbetten können. Da in K_{10} an jeder Ecke 9 Kanten abgehen, ist es denkbar, dass man den Graphen K_{10} vollständig überdecken kann, indem man den Petersen-Graph auf drei verschiedene Weisen als Teilgraph einbettet (also so, dass insgesamt jede Kante von K_{10} in einem der drei Teilgraphen vorkommt).
Wir werden unten sehen, dass dies nicht möglich ist. Es ist aber klar, dass es eine sehr langwierige (und langweilige) Aufgabe wäre, das »per Hand« durch direktes Überprüfen aller Möglichkeiten zu beweisen. Stattdessen gibt es eine elegante Beweismethode mit linearer Algebra.



Zur Lösung dieses Problems untersuchen wir die Eigenwerte der Adjazenzmatrix.

Die Adjazenzmatrix A von K_{10} ist sehr einfach: Es ist die (10×10)-Matrix mit Nullen auf der Diagonalen und Einsen in allen anderen Feldern. Wir schreiben J_{10} für die Matrix, deren Einträge sämtlich $= 1$ sind. Dann gilt also $A = J_{10} - E_{10}$.

Wenn wir den Petersen-Graph als Teilgraph in K_{10} einbetten, so ergibt sich eine Bijektion auf den Eckenmengen. Wir können die Situation also so beschreiben, dass wir die Ecken $\{1, \ldots, 10\}$ von K_{10} so mit Kanten verbinden, dass sich ein zum Petersen-Graph isomorpher Graph ergibt. Je nachdem, wie wir das machen, ergibt sich eine unterschiedliche Adjazenzmatrix (bezogen auf die Eckenmenge $\{1, \ldots, 10\}$, die wir festhalten).

Angenommen, es gäbe drei Einbettungen des Petersen-Graphs als Teilgraphen von K_{10}, die insgesamt alle Kanten überdecken. Wegen der zahlenmäßigen Übereinstimmung wird dann jede Kante genau einmal getroffen. Sind M_1, M_2, M_3 die drei Adjazenzmatrizen dieser Teilgraphen, so gilt also

$$A = M_1 + M_2 + M_3.$$

Außerdem sind die Matrizen M_i alle zueinander und zur Adjazenzmatrix des Petersen-Graphen (bezüglich irgendeiner fixierten Eckennummerierung) konjugiert (Bemerkung 14.13). Das bedeutet, dass M_1, M_2 und M_3 dieselben Eigenwerte haben, und dass die zugehörigen Eigenräume dieselben Dimensionen haben, Lemma 11.5.

LEMMA 14.14. *Sei M eine der drei Matrizen M_1, M_2, M_3. Dann gilt:*

(1) *Der Eigenraum von M zum Eigenwert 1 hat Dimension 5.*

(2) *Der Eigenraum von M zum Eigenwert 1 ist enthalten in dem Untervektorraum*

$$U_0 := \{(x_1, \ldots, x_{10}); \sum_{i=1}^{10} x_i = 0\}$$

von $\mathbb{Q}^{10}$.

BEWEIS. zu (1). Berechne mit dem Gauß-Algorithmus die Dimension von $\mathrm{Ker}(M - E_{10})$. Wir lassen die einfache Rechnung hier aus.

zu (2). In jede Spalte von $M - E_{10}$ sind genau drei Einträge gleich 1, genau einer gleich -1 (der Diagonaleintrag) und alle anderen gleich 0. Die Summe aller Zeilen vom $M - E_{10}$ ist

also $(2, \ldots, 2)$. Das bedeutet, dass alle Lösungen $(x_1, \ldots, x_{10})$ des linearen Gleichungssystems $(M - E_{10})x = 0$ auch die Gleichung

$$2x_1 + \cdots + 2x_{10} = 0$$

erfüllen, also in U_0 liegen. □

Die Eigenräume zum Eigenwert 1 von M_1 und M_2 liegen in dem 9-dimensionalen Vektorraum U_0, müssen sich also nicht-trivial schneiden. Sei $x \neq 0$ ein Element des Durchschnitts. Es gilt dann $J_{10}x = 0$, weil $x \in U_0$. Wir rechnen nun

$$M_3x = (A - M_1 - M_2)x = (J_{10} - I_{10} - M_1 - M_2)x = -3x.$$

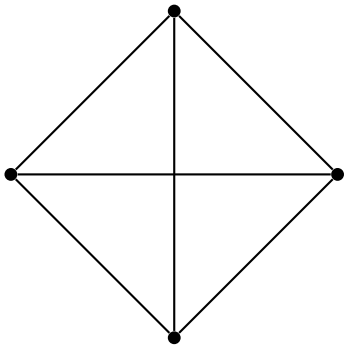
Den gewünschten Widerspruch erhält man nun, indem man (wieder mit dem Gauß-Algorithmus) überprüft, dass der Kern von $M_3 + 3E_{10}$ trivial ist, also dass -3 kein Eigenwert der Adjazenzmatrix des Petersen-Graphen ist.

Quelle: [**Ma**] Kap. 13; Matoušek verweist auf eine Arbeit von Lossers und Schwenk. Für ein ähnliches aber etwas komplizierteres Problem siehe auch loc. cit. Kap. 14.

14.6. Ausblick: Planare Graphen

Zum Schluss noch ein kleiner Ausblick auf ein weiteres Thema der Graphentheorie, auch wenn wir es hier nicht mit Methoden der Linearen Algebra in Verbindung bringen.

Definition 14.15. Sei G ein Graph. Wir sagen, G sei ein *planarer Graph*, wenn sich G *ohne Überschneidung von Kanten* in der Ebene zeichnen lässt. ⊣



Die Definition ist ein bisschen salopp, soll an dieser Stelle aber genügen. Der subtile Punkt dabei ist, dass man es einem Graphen nicht unbedingt auf den ersten Blick ansieht, ob er planar ist. Zum Beispiel ist der Graph K_4 ein planarer Graph, auch wenn er hier mit einer Kantenüberschneidung gezeichnet ist. Man kann denselben Graphen nämlich auch so zeichnen, dass sich keine zwei Kanten schneiden (zum Beispiel, indem man die vertikale Kante außen um das Quadrat herumführt). Entsprechend ist es auch nicht trivial zu zeigen, dass ein gegebener Graph *nicht* planar ist; auch wenn es nicht gelingt, den Graph überschneidungsfrei in der Ebene zu zeichnen, könnte es ja sein, dass man eine geschickte Möglichkeit übersehen hat.

Ein berühmter Satz über planare Graphen ist der

Satz 14.16 (Vierfarbensatz). *In jedem planaren Graphen lassen sich die Ecken mit höchstens 4 Farben so einfärben, dass je zwei benachbarte Ecken unterschiedliche Farben haben.*

Drei Farben reichen im allgemeinen nicht aus, um einen planaren Graphen in dieser Weise einzufärben, wie das Beispiel des Graphen K_4 zeigt.

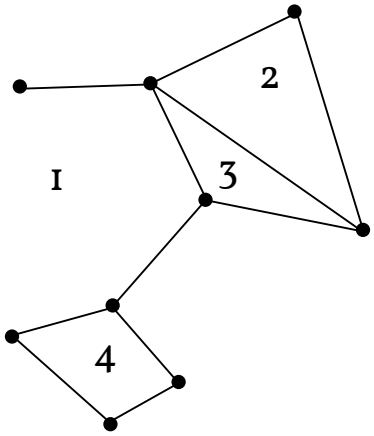
Der Vierfarbensatz lässt sich auch so uminterpretieren, dass man jede Landkarte so einfärben kann, dass je zwei entlang einer Grenze benachbarte Länder unterschiedlich gefärbt werden. Der Satz wurde 1976 von Appel und Haken mit Hilfe von Computern bewiesen. Es ist der erste berühmte mathematische Satz, der mit einem computergestützen Beweis gezeigt wurde. Bis heute ist kein Beweis bekannt, der ohne Computerberechnungen auskommt.

Gleichzeitig ist dieses Problem eine Quelle von Beispielen für Fehler und falsche Beweise. Siehe Vierfarbensatz (Wikipedia)[2].

Für die folgende Diskussion definieren wir:

DEFINITION 14.17. Ein Graph heißt *zusammenhängend*, wenn je zwei Ecken durch einen Weg verbunden sind (und die Eckenmenge nicht leer ist). ⊣

Für zusammenhängende planare Graphen gilt die Eulersche Formel, die zurückgeht auf L. Euler (um 1750). Euler hat mit seiner Lösung des Königsberger Brückenproblems[3] sozusagen die Graphentheorie begründet.



Um die Euler-Formel anzugeben, beobachten wir, dass ein (in der Ebene ohne Kantenüberschneidungen gezeichneter) planarer Graph durch seine Kanten die Ebene in endlich viele »Gebiete« unterteilt. Das »äußere«, unbegrenzte Gebiet zählen wir dabei mit. Die Form und Lage der Gebiete hängt natürlich davon ab, wie der Graph gezeichnet wird. A priori hängt auch die Anzahl der Gebiete davon ab, die Euler-Formal zeigt allerdings, dass das nicht der Fall ist.
Der hier gezeichnete Graph unterteilt die Ebene in 4 Gebiete.

SATZ 14.18 (Eulersche Formel für planare Graphen). *Sei G ein zusammenhängender planarer Graph, den wir uns in der Ebene gezeichnet vorstellen, sei E die Anzahl seiner Ecken, K die Anzahl der Kanten, und F die Anzahl der Gebiete (»Flächen«), in die G die Ebene unterteilt. Dann gilt*

$$E - K + F = 2.$$

Der Beweis des Satzes ist nicht sehr schwierig. Eine naheliegende Möglichkeit ist es, induktiv vorzugehen. Dazu überlegt man sich, dass man jeden zusammenhängenden planaren Graphen, ausgehend vom Graphen mit einer einzigen Ecke, schrittweise aufbauen kann, indem man entweder eine Kante zwischen zwei Ecken hinzufügt, oder eine Ecke und eine Kante, die die neue Ecke mit einer anderen Ecke verbindet, hinzufügt. Da die Formel für den Graphen mit einem einzigen Punkt gilt, muss man sich dann nur noch überlegen, dass diese beiden Schritte die Gültigkeit der Formel erhalten. Versuchen Sie, die Details einzufüllen! Oder schauen Sie zum Beispiel bei Grieser [**Gr**] nach.

Eng mit dieser Formel verwandt ist die Eulersche Polyederformel[4], die besagt, dass dieselbe Relation $E - K + F = 2$ gilt, wenn E die Anzahl der Ecken, K die Anzahl der Kanten und F die Anzahl der Außenflächen eines konvexen Polyeders in $\mathbb{R}^3$ ist. Ein Beispiel ist der Würfel mit 8 Ecken, 12 Kanten und 6 Flächen; in der Tat gilt $8 - 12 + 6 = 2$.

KOROLLAR 14.19. *Sei G ein zusammenhängender planarer Graph mit $E > 2$ Ecken und K Kanten.*

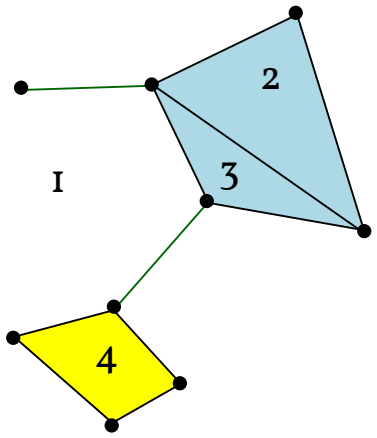
(1) *Es gilt $3E - 6 \geq K$.*

(2) *Es gibt eine Ecke, von der weniger als 6 Kanten abgehen.*

BEWEIS. zu (1). Wir stellen uns G in der Ebene gezeichnet vor und betrachten wie bei der Eulerschen Formel die Gebiete, in die die Ebene durch G zerteilt wird. Sei F_i die Anzahl

[2] https://de.wikipedia.org/wiki/Vier-Farben-Satz
[3] https://de.wikipedia.org/wiki/K%C3%B6nigsberger_Br%C3%BCckenproblem
[4] https://de.wikipedia.org/wiki/Eulerscher_Polyedersatz

der Gebiete, die durch i Kanten von G begrenzt werden. (Dabei zählen wir Kanten doppelt, wenn das Gebiet auf beiden Seiten der Kante liegt.



Die beiden hellblau gefärbten Gebiete haben jeweils 3 Begrenzungskanten (also $F_3 = 2$), das gelbe Gebiet hat 4 Begrenzungskanten (also $F_4 = 1$) und das weiße Außengebiet hat 12 Begrenzungskanten, weil wir die beiden dunkelgrün gezeichneten Kanten jeweils doppelt zählen. Also ist $F_{12} = 1$. Für $i \notin \{3, 4, 12\}$ gilt $F_i = 0$.

Dann gilt für die Gesamtzahl F der Gebiete:

$$F = F_3 + F_4 + F_5 + \cdots,$$

denn jedes Gebiet muss von mindestens 3 Kanten begrenzt werden.

Andererseits ist jede Kante eine »Begrenzungskante« für genau zwei Gebiete, es gilt also auch

$$2K = 3F_3 + 4F_4 + 5F5 + \cdots$$

Wenn wir das Dreifache der ersten Gleichung von der zweiten abziehen, dann erhalten wir

$$K - 3F = F_4 + 2F_5 + \cdots \geq 0,$$

folglich unter Ausnutzung der Euler-Formel

$$2K \geq 3F = 3(2 + K - E) = 6 + 3K - 3E,$$

also $3E - 6 \geq K$, und das wollten wir zeigen.

zu (2). Angenommen, von jeder Ecke würden 6 oder mehr Kanten abgehen. Dann hätten wir

$$K \geq 6E \,/\, 2 = 3E > 3E - 6,$$

also einen Widerspruch zu Teil (1). □

KOROLLAR 14.20. *Der Graph K_5 ist kein planarer Graph.*

BEWEIS. Dies folgt aus Teil (1) des vorherigen Korollars. Der Graph K_5 hat 5 Ecken und 10 Kanten. Es gilt aber nicht $3 \cdot 5 - 6 \geq 10$. □

Außerdem können wir den »Sechsfarbensatz« beweisen, eine (wesentlich) abgeschwächte Version des Vierfarbensatzes:

KOROLLAR 14.21 (Sechsfarbensatz). *Sei G ein planarer Graph. Dann lässt sich jeder Ecke eine von sechs Farben zuordnen, derart dass niemals zwei benachbarte Ecken dieselbe Farbe haben.*

Dies ist natürlich eine wesentlich schwächere Aussage als der oben genannte Vierfarbensatz, aber weil der Beweis so einfach ist, soll er hier trotzdem skizziert werden. (Auch der analoge Fünffarbensatz ist wesentlich einfacher zu beweisen als der Vierfarbensatz.)

BEWEIS. Wir führen Induktion nach Anzahl der Ecken. Für alle Graphen mit 6 oder weniger Ecken ist die Aussage klar. Für den Induktionsschritt wählen wir eine Ecke, von der höchstens 5 Ecken abgehen. Eine solche existiert nach Korollar 14.19. Den Graphen G', der aus G entsteht indem wie diese Ecke und alle Kanten, die von ihr ausgehen, entfernen, können

wir nach Induktionsvoraussetzung mit höchstens 6 Farben einfärben, so dass benachbarte Ecken stets unterschiedliche Farben zugewiesen bekommen.

Nun färben wir G, indem wir für alle Ecken in G' die Färbung übernehmen. Für die eine verbleibende Ecke können wir auch noch eine gültige Farbe finden, weil ja von dieser Ecke höchstens 5 Kanten ausgehen, also höchstens 5 der 6 Farben ausgeschlossen sind. □

14.7. Weitere Literatur

R. Diestel, *Graphentheorie*, Springer Spektrum 2017

Im Buch [**Ma**] befinden sich mehrere Beispiele (über die oben genannten hinaus), in denen Methoden der linearen Algebra in der Graphentheorie zur Anwendung kommen.

ANHANG A

Mathematische Ergänzungen *

A.1. Das Lemma von Zorn

Wir haben in Lemma 3.61 gesehen, dass endliche Produkte von nicht-leeren Mengen stets nicht leer sind – eine Aussage, die sehr einleuchtend ist. Interessanterweise hat die entsprechende Aussage für unendliche Produkte eine besondere Stellung unter den Axiomen der Mengenlehre:

AXIOM A.1 (Auswahlaxiom). *Seien I eine Menge und X_i, $i \in I$, nicht-leere Mengen. Dann ist das Produkt $\prod_{i\in I} X_i$ nicht leer.*

Dieses Axiom wurde erstmals 1904 von Zermelo formuliert, gehört aber nicht zu dem Axiomensystem von Zermelo und Fraenkel, das heutzutage mit dem Kürzel ZF bezeichnet wird (diese Axiome wurden nach Vorarbeiten von Zermelo 1921 von Fraenkel formuliert). Es wurde 1938 von Gödel bewiesen, dass das Auswahlaxiom nicht im Widerspruch zu den Axiomen ZF steht, und erst 1963 konnte Cohen zeigen, dass es andererseits auch nicht aus diesen Axiomen folgt.

Das Axiomensystem »ZF + Auswahlaxiom« bezeichnet man mit ZFC (»C« für »axiom of choice«), und es ist das in überwiegenden Teilen der heutigen Mathematik gängige Axiomensystem für die Mengenlehre und damit die Grundlage der allermeisten mathematischen Theorien. Dass das Auswahlaxiom eine Sonderstellung hat, liegt daran, dass man einerseits einen großen Teil der Mathematik auch ohne Auswahlaxiom aus dem Axiomensystem ZF herleiten kann, und andererseits, dass das Auswahl auch einige Konsequenzen hat, die der Intuition widersprechen.

Ein bekanntes Beispiel dafür ist das Banach-Tarski-Paradoxon[I]. Dieses hängt eng damit zusammen, dass es *nicht* möglich ist, jeder beschränkten Teilmenge von $\mathbb{R}^3$ ein »Volumen«, also eine Zahl in $\mathbb{R}_{\geq 0}$ zuzuordnen, so dass das Volumen nicht konstant 0, additiv für endliche disjunkte Vereinigungen und invariant unter Verschiebungen, Drehungen und Spiegelungen ist.

Video[a] zum Banach-Tarski-Paradoxon von Vsauce.

[a] https://www.youtube.com/watch?v=s86-Z-CbaHA

> The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?
>
> Jerry Bona
> Fundort: https://mathoverflow.net/a/7194

[I] https://de.wikipedia.org/wiki/Banach-Tarski-Paradoxon

Auch wenn das Auswahlaxiom einige Herausforderungen an unsere Intuition stellt, ist die oben formulierte Aussage doch so überzeugend, dass es üblicherweise (und auch in diesem Skript) in die Liste der verwendeten Axiome aufgenommen wird. Wie erwähnt, ist bewiesen worden, dass es nicht im Widerspruch zu den Axiomen in ZF steht, so dass es aus mathematischer Sicht unkritisch ist, dieses Axiom zu verwenden. Und es ist oft praktisch, weil es so mächtig ist. In der linearen Algebra erlaubt es uns zu beweisen, dass jeder Vektorraum eine Basis besitzt (siehe Ergänzung 6.47).

Man kann zeigen, dass das Auswahlaxiom zu der Aussage, dass jeder Vektorraum eine Basis besitzt, äquivalent ist.

Leicht zu sehen ist, dass das Auswahlaxiom äquivalent ist zu

SATZ A.2. *Sei $f\colon X \to Y$ eine surjektive Abbildung. Dann existiert ein* Schnitt *von f, d.h. eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$.*

BEWEIS. Die Existenz von g entspricht der Existenz eines Elements von $\prod_{y\in Y} f^{-1}(\{y\})$. Wegen der Surjektivität von f sind die Mengen $f^{-1}(\{y\})$ alle nicht-leer. □

Um aus dem Satz das Auswahlaxiom abzuleiten, betrachtet man für eine Familie X_i die surjektive Abbildung $\coprod_{i\in I} X_i \to I$, wobei $\coprod_{i\in I} X_i$ die »disjunkte Vereinigung« der X_i ist. Dies ist eine Menge, die alle X_i als Teilmengen enthält, die gleich der Vereinigung aller dieser Teilmengen X_i ist, und die $X_i \cap X_j = \emptyset$ für alle $i \neq j$ erfüllt. (Formal definiert man die disjunkte Vereinigung der X_i, indem man X_i identifiziert mit $\{i\} \times X_i$, $i \in I$, und dann die Vereinigung aller dieser Mengen bildet. Durch das Hinzufügen der Komponente i erreicht man, dass die Kopien der verschiedenen X_i sich nicht schneiden. Hier wird eine Vereinigung von Mengen gebildet, die nicht Teilmenge einer vorgegebenen Menge sind. Diese Konstruktion ist im Rahmen von ZF durchführbar.)

Eine andere bekannt Aussage, die äquivalent ist zum Auswahlaxiom, ist der

SATZ A.3 (Wohlordnungssatz). *Sei X eine Menge. Dann existiert eine Wohlordnung auf X, d.h. eine totale Ordnung $\preceq$, derart dass jede nicht-leere Teilmenge von X ein kleinstes Element bezüglich $\preceq$ hat.*

Siehe Abschnitt 3.13.3 für die hier verwendeten Begriffe. So plausibel das Auswahlaxiom ist, so schwierig ist es, sich beispielsweise eine Wohlordnung der Menge der reellen Zahlen vorzustellen.

Um zu beweisen, dass jeder Vektorraum eine Basis hat, benötigen wir eine andere zum Auswahlaxiom äquivalente Aussage, und zwar das sogenannte Lemma von Zorn.

Dafür benötigen wir zuerst einige Sprechweisen: Zunächst benutzen wir die Begriffe der *partiellen* und der *totalen Ordnung*, wie sie in Abschnitt 3.13.3 eingeführt wurden. Ein besonders passendes Beispiel in unserem Kontext ist die Teilmengenbeziehung: Ist M eine Menge, so bezeichnen wir mit $P(M)$ die Potenzmenge von M, also die Menge aller Teilmengen von M. Diese ist mittels der Inklusion $\subseteq$ partiell geordnet, das bedeutet: Für Elemente $X, Y, Z \in P(M)$ (also Teilmengen $X, Y \subseteq M$) gilt

(1) $X \subseteq X$,
(2) aus $X \subseteq Y$ und $Y \subseteq Z$ folgt $Y \subseteq Z$,
(3) aus $X \subseteq Y$ und $Y \subseteq X$ folgt $X = Y$.

Bei einer totalen Ordnung müssen zusätzlich je zwei Elemente vergleichbar sein (wie bei der üblichen Anordnung der ganzen Zahlen: Für $x, y \in \mathbb{Z}$ gilt $x \leq y$ oder $y \leq x$). Bei der Inklusion von Teilmengen ist das offensichtlich nicht der Fall: In vielen Situationen gilt weder $X \subseteq Y$ noch $Y \subseteq X$. Man spricht daher von einer *partiellen* Ordnung. Jede Teilmenge $U \subseteq P(M)$, also

eine Menge von Teilmengen von M, der nicht alle Teilmengen angehören müssen, ist dann auch durch die Inklusion $\subseteq$ partiell geordnet. Während die folgende Diskussion für $P(M)$ mit der partiellen Ordnung $\subseteq$ nicht so interessant ist, genügt es, wenn Sie sich alles im Fall einer Teilmenge $U \subseteq P(M)$ der Potenzmenge irgendeiner Menge M vorstellen (mit $\subseteq$ als partieller Ordnung).

Sei nun U eine Menge mit einer partiellen Ordnung $\preceq$. Wir hatten in Definition 3.80 definiert, dass ein Element $x \in U$ *maximal* (bezüglich $\preceq$) heißt, wenn für alle $y \in U$ aus $x \preceq y$ schon $x = y$ folgt.

Beispiel A.4. (1) Sei M eine Menge und $U = P(M)$ mit $\subseteq$ als partieller Ordnung. Dann ist M ein maximales Element, und zwar das einzige.

(2) Sei M eine nicht-leere Menge und $U \subset P(M)$ die Teilmenge von $P(M)$, die aus allen echten Teilmengen $X \subsetneq M$ von M besteht. Dann ist für jedes $m \in M$ das Element $M \setminus \{m\}$ ein maximales Element von U bezüglich $\subseteq$.

(3) Seien K ein Körper und V ein K-Vektorraum. Sei $U \subset P(V)$ die Menge aller linear unabhängigen Teilmengen von V. Wir haben in Satz 6.35 gesehen, dass die maximalen Elemente von U genau die Basen von V sind. Das Lemma von Zorn wird uns ein Kriterium für die Existenz eines maximalen Elements in irgendeiner partiell geordneten Menge zur Verfügung stellen. Angewandt auf das Beispiel hier erhalten wir damit das Ergebnis, dass jeder Vektorraum eine Basis besitzt. Siehe Ergänzung 6.47.

$\Diamond$

Definition A.5. Sei U eine durch $\preceq$ partiell geordnete Menge. Sei U' eine Teilmenge von U. Ein Elemente $x \in U$ heißt *obere Schranke* von U', wenn für alle $y \in U'$ gilt, dass $y \preceq x$. $\dashv$

In der vorherigen Definition ist es wichtig, dass wir nicht verlangen, dass die obere Schranke x ein Element von U' ist. Im Zornschen Lemma wird die Existenz oberer Schranken für gewisse Teilmengen von U verlangt. (Eine obere Schranke von U selbst wäre gerade ein größtes Element; dessen Existenz wollen wir sicherlich nicht zur Voraussetzung machen.) Dafür bemerken wir, dass jede Teilmenge $U' \subseteq U$ einer partiell geordneten Menge selbst wieder partiell geordnet ist. Je nachdem kann es natürlich passieren, dass die partielle Ordnung von U auf der Teilmenge U' sogar eine *totale* Ordnung induziert; in diesem Fällen fordert man im Lemma von Zorn die Existenz einer oberen Schranke.

Satz A.6 (Lemma von Zorn). *Sei U eine nicht-leere Menge mit einer partiellen Ordnung $\preceq$, die die folgende Eigenschaft hat: Jede Teilmenge $U' \subseteq U$, die durch $\preceq$ total geordnet ist, besitzt eine obere Schranke in U.*

Dann existiert in U ein maximales Element bezüglich $\preceq$.

Formal gesehen kann man darauf verzichten, die Voraussetzung $U \neq \emptyset$ in die Aussage des Lemmas aufzunehmen, weil die folgende Bedingung, angewandt auf die total geordnete Teilmenge $U' := \emptyset$, garantiert, dass U ein Element enthält, nämlich eine obere Schranke der leeren Teilmenge.

Man nennt total geordnete Teilmengen einer partiell geordneten Menge manchmal auch *Ketten*, und nennt eine partiell geordnete Menge *induktiv geordnet*, wenn jede Kette eine obere Schranke besitzt. Dann kann man das Lemma von Zorn formulieren als: Jede induktiv geordnete Menge besitzt ein maximales Element.

Wir verzichten darauf, an dieser Stelle zu beweisen, dass das Lemma von Zorn aus dem Auswahlaxiom folgt. Siehe [**So**] 1.9 für einen gut lesbaren Beweis. Man kann auch zeigen, dass das Auswahlaxiom aus dem Zornschen Lemma folgt (das ist eher noch einfacher zu

beweisen als die andere Implikation). Die beiden Aussagen sind also (unter den Axiomen in ZF) äquivalent. Sie könnten daher auch einfach das Zornsche Lemma als eines der Axiome betrachten, die der Mengenlehre zugrunde liegen sollen.

BEMERKUNG A.7. Wenn in der obigen Situation eine Kette U' nur endlich viele Elemente hat, so können wir sie uns in der Form

$$u_0 \preceq \cdots \preceq u_n$$

vorstellen. Dann ist natürlich u_n eine obere Schranke. Sobald es unendlich viele Elemente in U' gibt, wird die Sache offenbar komplizierter. Es genügt nicht, den Fall von Ketten der Form

$$u_0 \preceq u_1 \preceq u_1 \preceq \ldots,$$

die durch $\mathbb{N}$ indiziert sind, zu betrachten! Um das Zornsche Lemma anwenden zu können, muss man zeigen, dass *jede* Kette eine obere Schranke besitzt, und eine Kette muss nicht abzählbar sein.

Sonst könnte man zum Beispiel zeigen, dass die Menge der reellen Zahlen eine maximale abzählbare Teilmenge besitzt. Das ist offenbar nicht möglich, da eine abzählbare Teilmenge von $\mathbb{R}$ eine echte Teilmenge sein muss, und sie nach Hinzufügen eines weiteren Elements abzählbar bleibt. ◊

ANHANG B

Verschiedenes *

B.1. Mathematische Sprechweisen, Code words

B.1.1. Begriffe. In der mathematischen Fachsprache gibt es eine ganze Menge von Wörtern, die man kennen muss, um einen mathematischen Text zu lesen, die aber nicht ein mathematisches Objekt im engeren Sinne bezeichnen und daher nicht Bestandteil einer Definition sind. Einige davon werden in diesem Abschnitt erklärt. Wenn Sie andere Wörter sehen, deren Bedeutung Sie nicht verstehen, fragen Sie nach! Einige der Wörter in der folgenden Liste haben eine mathematische Bedeutung (und werden also an geeigneter Stelle definiert). Sie befinden sich hier, weil sie auch Bestandteil der Alltagssprache sind, so dass man die präzise mathematische Bedeutung womöglich leicht vergisst (zum Beispiel: es ist ein wichtiger Unterschied, ob ein Element das *kleinste* Element einer partiell geordneten Menge, oder ein *minimales* Element ist).

Absolutterm, absolutes Glied – In einem polynomialen Ausdruck $a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0$ heißt a_0 (also der Summand, der nicht mit einer positiven Potenz von x multipliziert wird) der Absolutterm oder das absolute Glied.

a fortiori – Dies ist Latein und bedeutet *erst recht*. Wenn man schon eine stärkere Aussage bewiesen hat, aber nur ein schwächeres Ergebnis im weiteren Verlauf verwenden möchte, kann man diese Sprechweise benutzen. (»Wir haben gesehen, dass $n > 5$ ist, a fortiori ist n positiv.«)

a priori – Dies ist Latein und bedeutet *von vorneherein*. Der Ausdruck wird (auch) in mathematischen Texten benutzt, um etwas zu kennzeichnen, was man erwarten könnte, aber dann doch nicht eintritt. (»A priori könnte n negativ sein, aber weil … gilt, kann das nicht sein.«)

Annahme, angenommen – Auch wenn das nicht immer so strikt gesehen wird, finde ich es sinnvoll, die Wörter *Annahme* und *angenommen* (nur) dann zu verwenden, wenn man in einem Widerspruchsbeweis (siehe Abschnitt 3.6.3) die Annahme angibt, die dann zum Widerspruch geführt werden soll. Die Tatsachen, die in einem Satz vorausgesetzt werden, sollte man auch so nennen: *Voraussetzungen*.

im allgemeinen/in der Regel – Diese Ergänzung schiebt die Mathematiker∗in gerne ein, wenn eine Aussage zwar so gut wie immer wahr ist, es aber ein paar wenige Ausnahmefälle gibt: Ist n eine natürliche Zahl, dann gibt es im allgemeinen mehr als eine Bijektion $\{1, \ldots, n\} \to \{1, \ldots, n\}$. (Aber für die Ausnahmefälle $n = 0$ und $n = 1$ gibt es eben nur eine einzige. Die obige Formulierung ist klarer, als zu sagen, dass es mehr als eine Bijektion $\{1, \ldots, n\} \to \{1, \ldots, n\}$ geben kann; denn das ließe im Dunklen, dass es nur in ganz wenigen Fällen nicht so ist. Manchmal ist es natürlich noch besser, die Ausnahmen genau anzugeben.)

Implikation – Dies ist ein anderes Wort für Folgerung, oder genauer für den Sachverhalt, dass eine Aussage aus einer anderen folgt (»Beweisen Sie die Implikation $A \Rightarrow B$.«).

Inklusion – Die Eigenschaft, eine Teilmenge zu sein. (»Die Inklusion $X \subseteq Y$ ist leicht zu zeigen.«)

kleinstes, größtes, minimales, maximales Element bezüglich einer (partiellen) Ordnung – siehe Abschnitt 3.13.3.

kanonisch – Man bezeichnet ein mathematisches Objekt (oft eine Abbildung) als kanonisch, wenn es sich um die »offensichtliche« Wahl handelt. Dieser Begriff hat also keine mathematische Definition. Man könnte ihn auch umschreiben mit »so wie wir es immer machen«. Zum Beispiel nennt man die Standardbasis von K^n manchmal die *kanonische Basis*. Ähnlich gelagert ist die Sache mit dem Begriff *natürlich*, wobei man hiermit je nach Kontext auch eine mathematische Bedeutung verbindet (die Eigenschaft der Funktorialität, die wir hier nicht genauer erläutern).

Lemma – Ein Lemma ist eine mathematische Aussage, die untergeordnete Bedeutung hat, aber doch im Text ausdrücklich (und in der Regel mit einer Nummer versehen) festgehalten werden soll, damit man später darauf verweisen kann. Für den großen Überblick braucht man sich die Lemmata (so der Plural dieses griechischstämmigen Worts; Lemmas ist aber auch gebräuchlich) eher nicht zu merken. Statt von einem Lemma spricht man auch manchmal von einem Hilfssatz. Demgegenüber ist ein Satz (oder eine Proposition) und erst recht ein Theorem (manchmal auch: Lehrsatz) ein Ergebnis von großer (oder sogar überragender) Bedeutung. Ein Korollar ist ein Ergebnis, dass sich ohne große zusätzliche Arbeit aus einem bereits bewiesenen Satz (oder Theorem …) ableiten lässt.

loc.cit. – Dies ist die Abkürzung für den lateinischen Ausdruck *loco citato*, am angegebenen Orte, und bedeutet, dass sich die Literaturangabe auf dieselbe Quelle bezieht, die davor angegeben wurde.

Ohne Einschränkung / ohne Beschränkung der Allgemeinheit – (Abkürzung: OE beziehungsweise OBdA) Diese Floskel benutzt man um zu begründen, dass es (in einem Beweis) erlaubt ist, sich auf einen speziellen Fall zurückzuziehen. Zum Beispiel, weil die ausgeschlossenen Fälle ohnehin leicht zu erledigen sind, oder weil eine symmetrische Situation vorliegt.

paarweise – Wenn man über eine Eigenschaft spricht, die eine Menge (oder eine Familie) haben kann, meint man manchmal, dass die Eigenschaft für je zwei Elemente gelten soll, und ergänzt deshalb das Wort *paarweise*. Zum Beispiel sind die Zahlen 3, 5, 18 teilerfremd, denn es gibt keine natürliche Zahl > 1, die alle drei Zahlen teilt. Aber 3 und 18 sind nicht teilerfremd, und deshalb sind 3, 5, 18 nicht paarweise teilerfremd. In ähnlicher Weise ist es ein Unterschied, ob Teilmengen einer Menge disjunkt (der Durchschnitt ist leer) oder paarweise disjunkt (der Durchschnitt von je zweien ist leer) sind. Oder ob eine Familie von Vektoren linear unabhängig, oder paarweise linear unabhängig ist. (Wenn man sagt, dass Zahlen/Objekte $x_1, \dots, x_n$ verschieden sein sollen, dann meint man aber in der Regel, dass sie paarweise verschieden sind, ohne das explizit dazuzusagen.)

Schubfachprinzip – Unter dem Schubfachprinzip (das manchmal noch pompöser als das Dirichletsche Schubfachprinzip bezeichnet wird) versteht man die folgende banale (aber manchmal sehr nützliche) Feststellung: Wenn man n Dinge in weniger als n Fächer legt, dann sind in mindestens einem Fach mindestens zwei Dinge. (Oder mathematischer ausgedrückt: Ist $f\colon X \to Y$ eine Abbildung zwischen endlichen Mengen und ist $\#X > \#Y$, dann ist f nicht injektiv. Siehe Lemma 3.63.)

trivial – Das Wort *trivial* wird in zwei Kontexten verwendet. Einerseits sagt man gelegentlich, ein Beweis (oder ein Ergebnis) sei trivial, wenn der Beweis sehr einfach ist. (Man sollte sich allerdings zwingen, mindestens ein zweites Mal nachzudenken, bevor man das schreibt, denn viele Fehler in mathematischen Texten verstecken sich gerade an den Stellen, wo etwas als trivial oder offensichtlich bezeichnet wird. Dann war es eben nicht als *Das ist einfach.* zu verstehen, sondern eher als *Das sollte kein Problem sein, aber ich bin zu faul, es mir genau zu überlegen und erst recht es aufzuschreiben*, und da kommt es dann leicht zu Fehlern.)

Zweitens spricht man manchmal von trivialen Objekten oder Abbildungen, meist solche, die besonders uninteressant sind: Die Gruppe $\{1\}$ mit einem einzigen Element wird als die

triviale Gruppe bezeichnet. Andere Beispiele: Die triviale Lösung eines homogenen linearen Gleichungssystems, die triviale Linearkombination einer Familie von Vektoren.

wohldefiniert – Man sagt, ein Begriff (oder ein mathematisches Objekt; sehr oft eine Abbildung) sei *wohldefiniert*, wenn die Definition zwar a priori von gewissen zusätzlichen Wahlen abhängt, diese aber letztlich keine Rolle spielen. Zum Beispiel: Wir definieren die Summe von zwei Bruchzahlen $\frac{a}{b}$ und $\frac{c}{d}$ als $\frac{ad+cb}{bd}$. Um zu überprüfen, dass dies eine *wohldefinierte* Abbildung $+\colon \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ liefert, müssen wir sicherstellen, dass das Ergebnis nicht davon abhängt, wie wir den Bruch $\frac{a}{b}$ (und entsprechend $\frac{c}{d}$) schreiben. Da man Brüche kürzen und erweitern kann, gilt ja $\frac{a}{b}=\frac{a'}{b'}$ für viele a', b', und die obige Vorschrift ergibt nur dann Sinn, wenn dann auch $\frac{ad+cb}{bd}=\frac{a'd+cb'}{b'd}$ gilt (was in der Tat der Fall ist). Die Vorschrift $\left(\frac{a}{b},\frac{c}{d}\right)\mapsto\frac{a+c}{b+d}$ ist dahingegen nicht wohldefiniert – wenn man einen der Brüche $\frac{a}{b}$, $\frac{c}{d}$ erweitert, erhält man in der Regel ein ganz anderes Ergebnis. Die Frage nach Wohldefiniertheit tritt immer dann auf, wenn sich eine Definition auf eine Äquivalenzklasse (Abschnitt 3.13.2) bezieht, aber für die Definition ein Repräsentant der Äquivalenzklasse herangezogen wird. Ein anderers Beispiel ist Definition 3.58, in der wir die Mächtigkeit einer endlichen Menge X definiert haben; dort wählt man eine Bijektion $X\to\{1,\dots,n\}$ und muss wissen, dass die Zahl n, die dabei auftritt, eindeutig bestimmt ist (auch wenn es natürlich in der Regel viele solche Bijektionen gibt). Sie sollten den Begriff wohldefiniert *nicht* verwenden, um auf andere Punkte hinzuweisen, die für die Korrektheit einer Definition erforderlich sind. (Beispiel: Wollen Sie eine Abbildung $f\colon X\to Y$ durch eine Formel für $f(x)$ angeben, so ist es erforderlich, dass $f(x)$ für alle x ein Element von Y ist; dass das so ist, beschreibt man aber nicht mit dem Wort wohldefiniert.)

B.1.2. Abkürzungen. Vor allem an der Tafel benutzt man manchmal die folgenden Abkürzungen, um etwas Zeit und Platz zu sparen:

- gdw. – genau dann, wenn (auf Englisch: iff, if and only if)
- IA, IS, IV – Induktionsanfang, Induktionsschritt, Induktionsvoraussetzung.
- Kp. – Körper
- l. u., l. a. – linear unabhängig, linear abhängig
- OE, OBdA (s.o.), auf Englisch: WLOG – without loss of generality
- TFAE (Englisch) – the following are equivalent, die folgenden Aussagen sind äquivalent
- VR – Vektorraum
- zz, gzz – zu zeigen, genügt zu zeigen (auf Englisch: ETS – enough to show)

B.2. Mathematische Texte am Computer schreiben.

Zu Beginn Ihres Studiums besteht keine Notwendigkeit, mathematische Texte am Computer zu schreiben. Was die Hausaufgaben betrifft, ist meine Empfehlung, diese handschriftlich anzufertigen.

Irgendwann, spätestens, wenn Sie Ihre Bachelor-Arbeit schreiben, wird sich diese Anforderung aber ergeben.

Das Standardprogramm für mathematischen Textsatz ist LaTeX (gesprochen Latech, das X am Ende ist der große griechische Buchstabe Chi; auf Englisch wird er üblicherweise als K gesprochen). Mathematik mit einem herkömmlichen Textverarbeitungsprogramm wie LibreOffice oder Word zu schreiben, ist einerseits viel mehr Arbeit, andererseits sieht das Ergebnis deutlich schlechter aus (speziell die mathematischen Formeln, aber auch bei gewöhnlichem Text sind die Algorithmen von LaTeX in der Regel besser, um optimale Zeilenumbrüche zu finden).

Das zugrundeliegende TEX und LATEX wurden von D. Knuth und L. Lamport Ende der 1970'er, Anfang der 1980'er entwickelt und haben das Verfassen und Veröffentlichen von mathematischen Texten revolutioniert. Die Programme werden seitdem behutsam weiterentwickelt. Sie werden von praktisch allen Mathematikern benutzt, um ihre Ergebnisse in Artikeln und Büchern festzuhalten (und auch in vielen anderen Fachgebieten). Dieses Skript wurde natürlich auch mit LATEX geschrieben, genauer mit LuaLaTex. Das ist eine Varianten, die unter anderem besser mit verschiedenen Schriftarten umgehen kann und modernere Schnittstellen zur Programmierung bietet. Eine andere Variante ist XeLaTex.

Daher sollten Sie bei Gelegenheit, zum Beispiel in den Semesterferien, wenn Sie etwas Zeit haben, LATEX lernen. Die LATEX-Umgebung lässt sich auf allen gängigen Plattformen (Windows, Mac OS, Linux, ...) installieren. Es gibt im Netz dazu jede Menge Anleitungen, und es gibt auch entprechende Lehrbücher, wenn Sie es gerne etwas ausführlicher hätten.

Etwas mehr Informationen und weitere Referenzen: Wikipedia[a].
Eine Suche nach »Latex Einführung« liefert auch jede Menge brauchbarer Treffer.
Ein Buch über LATEX benötigen Sie erstmal wahrscheinlich nicht.
Mein Tipp wäre: Suchen Sie sich jemanden, der LATEX auf einem Rechner mit demselben Betriebssystem benutzt, wie Sie es haben, und lassen Sie sich die ersten Schritte direkt am Computer erklären. Danach können Sie vieles mit »learning by doing« machen.

[a] `https://de.wikipedia.org/wiki/LaTeX`

Einige wichtige Grundregeln des mathematischen Schriftsatzes, die nicht offensichtlich sind:

- Es sollte nie ein mathematisches Symbol direkt am Satzanfang stehen.
- Es sollten nie zwei Symbole direkt aufeinander folgen (mindestens ein Komma oder anderes Satzzeichen muss dazwischen sein, um Missverständnisse zu vermeiden).
- Operatoren sind nicht dasselbe wie eine Folge von Variablen: $\det(A)$ und nicht $det(A)$. In TEX muss man also `\det(A)` schreiben, und für Namen von Operatoren, die noch nicht in TEX definiert sind, ein entsprechendes Makro selber schreiben (keine Angst, das ist nur eine Zeile, zum Beispiel `\newcommand\Spur{\mathop{\rm Spur}}`).

Wesentlich ausführlicher hat das K. Conrad als Advice on mathematical writing[1] aufgeschrieben, zwar auf Englisch, aber das meiste lässt sich direkt auf deutsche Texte übertragen.

B.2.1. Mathematik im Forum auf der Moodle-Seite. Auch auf der Moodle-Seite können Sie die gängigen mathematischen Notationen verwenden. Auch dort wird die LATEX-Notation verwendet. Mathematische Ausdrücke müssen in *doppelte Dollar-Zeichen* eingeschlossen werden, um erkannt zu werden. Zum Beispiel:

`$$a^n$$`	a^n
`$$A=(a_{ij})_{i, j}$$`	$A=(a_{ij})_{i,j}$
`$$\sum_{i=1}^n i = \frac{(n+1)n}{2}$$`	$\sum_{i=1}^{n} i = \frac{(n+1)n}{2}$
`$$A=\begin{pmatrix} 1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix}$$`	$A=\begin{pmatrix} 1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix}$

[1] `https://kconrad.math.uconn.edu/blurbs/proofs/writingtips.pdf`

ANHANG C

Bemerkungen zur Literatur *

Vorbemerkungen:

- Sie brauchen neben dem Material, das Ihnen im Rahmen der Vorlesung zur Verfügung gestellt wird, nicht unbedingt weitere Quellen. Die unten genannten Verweise dienen nur der Ergänzung – für den Fall, dass Sie das Material, das wir in der Vorlesung behandeln, noch einmal in etwas anderer Form anschauen möchten.
- Auch wenn die Liste unten schon recht lang ist, ist sie bei weitem nicht vollständig. Es gibt sehr viele Lehrbücher und Skripte zur Linearen Algebra, und Sie können und sollten ruhig auch selbst einmal schauen, was Sie sonst noch an Material finden – sei es im Internet, sei es in der Bibliothek. Da der Stoff der Linearen Algebra sehr weitgehend standardisiert ist, ist das Risiko klein, dass Sie woanders »etwas Falsches« lernen.
- Als Anknüpfung an den letzten Punkt, aber als eigener Punkt, weil er so wichtig ist und sich auf alle Quellen bezieht, egal, ob Sie sie selbst gefunden haben oder ob sie unten erwähnt werden (und genauso gilt der Punkt für dieses Skript): Da in der Mathematik ohnehin alle Aussagen zu beweisen sind, können (und **müssen**) Sie selbst überprüfen, ob das, was Sie lesen, überhaupt richtig ist. *Glauben Sie niemandem!*

  Mit den Definitionen verhält es sich natürlich ein bisschen anders, denn eine Definition kann ja nicht falsch sein (höchstens kann sie ungeschickt oder nutzlos sein). Hier muss man tatsächlich manchmal ein bisschen aufpassen. Was den Begriff des Vektorraums oder des Körpers angeht, gibt es wohl keine Unterschiede, aber in manchen Büchern werden nur Vektorräume über den reellen und komplexen Zahlen betrachtet. Die Null wird manchmal nicht als Element der Menge der natürlichen Zahlen betrachtet.

Viele der Bücher können Sie als Studierende der Universität Duisburg-Essen kostenfrei herunterladen. Dazu müssen Sie aus dem Adressbereich der Universität auf die Verlagsseiten zugreifen; entweder von einem Rechner aus, der sich an der Uni befindet (oder über Eduroam das WLAN der Uni nutzt), oder über eine VPN-Verbindung[I].

Alle Quellen, zu denen unten ein Link angegeben ist, sollten entweder allgemein zugänglich, oder aus dem Netz der Universität Duisburg-Essen zugänglich sein.

C.1. Lehrbücher

(Alphabetisch nach den Namen der Autoren.)

C. Baer, *Lineare Algebra und Analytische Geometrie*, Springer Spektrum 2018,
https://doi.org/10.1007/978-3-658-22620-6

S. Bosch, *Lineare Algebra*, Springer 2014,
https://doi.org/10.1007/978-3-642-55260-1

E. Brieskorn, *Lineare Algebra und Analytische Geometrie I*, Vieweg+Teubner 1983

[I] https://www.uni-due.de/zim/services/internetzugang/vpn

Das Buch von Brieskorn ist sehr ausführlich und enthält auch Abschnitte über die Geschichte der linearen Algebra (und analytischen Geometrie) und Bemerkungen zur Motivation vieler Begriffe. (Es gibt auch noch einen zweiten und dritten Band.)

Fischer, *Lineare Algebra*, Springer Spektrum 2014,
https://doi.org/10.1007/978-3-658-03945-5

Vielleicht *das* Standard-Lehrbuch der linearen Algebra im deutschsprachigen Raum. Der »Fischer« wurde auch schon empfohlen, als ich im ersten Semester war.

Fischer, Lernbuch Lineare Algebra und Analytische Geometrie, Springer 2019,
https://doi.org/10.1007/978-3-658-27343-9

K. Jänich, *Lineare Algebra*, Springer 2008, https://doi.org/10.1007/978-3-662-08382-6

Mit ausführlichen Bemerkungen zu den Querverbindungen zur Physik.

J. Liesen, V. Mehrmann, *Lineare Algebra*, Vieweg+Teubner 2012,
https://doi.org/10.1007/978-3-8348-8290-5

F. Lorenz, *Lineare Algebra I*, Spektrum Akad. Verlag 2004.

C.2. Vorlesungsskripte zur Linearen Algebra

R. Pink, *Lineare Algebra I und II*, Zusammenfassung, 2016. https://people.math.ethz.ch/~pink/ftp/Lineare-Algebra-Zusammenfassung-20161006.pdf

Der Stoff der Vorlesungen Lineare Algebra 1 und 2 auf circa 100 Seiten (allerdings großenteils ohne Beweise), dazu ungefähr 20 Seiten an lesenswerten »Vorbemerkungen«.

W. Soergel, *Lineare Algebra I*,
http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXLA1.pdf

Ein ausführliches Skript zur Linearen Algebra 1 mit vielen Bemerkungen, die den Zugang zum Stoff erleichtern sollen.

J. Stix, *Lineare Algebra*,
https://www.uni-frankfurt.de/74414804/Stix_LineareAlgebra_Skript.pdf

Dieses Skript ist in einem relativ knappen Stil geschrieben, enthält aber eine Menge an Material (das wir teilweise erst in der Linearen Algebra 2 behandeln werden).

A. Werner, *Lineare Algebra I*,
Basiskurs: https://www.uni-frankfurt.de/50581195/basiskurs_LA1.pdf,
Aufbaukurs: https://www.uni-frankfurt.de/50581204/Aufbaukurs_LA1.pdf

Das Skript von A. Werner ist etwas anders aufgebaut als die meisten hier genannten Skripte und Bücher: Es ist unterteilt in einen Basiskurs und einen Aufbaukurs. Im Basiskurs wird ein »rechnerischer« Zugang gewählt, und der theoretische Aufbau der Theorie hintangestellt bzw. teilweise in den Aufbaukurs verlagert.

C.3. Bücher übers Problemlösen und Beweisen

C. Ableitinger, A. Herrmann, *Lernen aus Musterlösungen zur Analysis und Linearen Algebra*, Vieweg+Teuber 2011, https://doi.org/10.1007/978-3-8348-8335-3

Ausführlich diskutierte Musterlösungen zu Aufgaben zu den Vorlesungen Analysis 1/2 und Lineare Algebra 1/2.

D. Grieser, *Mathematisches Problemlösen und Beweisen*, Springer Spektrum 2017, https://doi.org/10.1007/978-3-658-14765-5

Der Untertitel *Eine Entdeckungsreise in die Mathematik* beschreibt das Buch gut: Anhand von gut zugänglichen Problemstellungen werden verschiedene Beweismethoden und Strategien, um mathematische Probleme zu lösen, vorgestellt. Das Buch richtet sich explizit an Studienanfänger*innen und ist mit Schulmathematikkenntnissen (und Neugier auf Mathematik) lesbar.

C. Alsina, R. Nelsen, *Bezaubernde Beweise*, Springer Spektrum 2013
C. Alsina, R. Nelsen, *Perlen der Mathematik*, Springer Spektrum 2015, https://doi.org/10.1007/978-3-662-45461-9

Zwei Bücher derselben Autoren, die jeweils eine große und reich illustrierte Sammlung von mathematischen Problemen, Bemerkungen und (teilweise) Kuriositäten enthalten, deren Lösung überwiegend mit einfachen Mitteln möglich ist. Leider ist nur das Neuere im E-Book-Paket enthalten, das Uni-Mitgliedern der Universität Duisburg-Essen zur Verfügung steht.

In seiner Rezension über das Buch *Bezaubernde Beweise* schreibt der Rezensent M. Drmota: »Es ist ein schönes Buch zum Schmökern und zur mathematischen Entspannung und kann allen mathematisch Interessierten wärmstens empfohlen werden.« (Math. Semesterberichte **60** (2013), 274–275.)

K. Houston, *Wie man mathematisch denkt*, Springer Spektrum 2012

Eine Einführung in das »Beweisen« und allgemeiner die mathematische Arbeitstechnik an der Universität.

C.4. Englische Lehrbücher zur linearen Algebra

Schauen Sie ruhig auch einmal in ein Buch, das auf Englisch geschrieben ist, und sei es nur um zu sehen, dass »mathematisches Englisch« in aller Regel sehr leicht zu verstehen ist. Später im Studium werden Sie mit hoher Wahrscheinlichkeit Quellen auf Englisch lesen müssen.

D. Austin, *Understanding Linear Algebra*, http://merganser.math.gvsu.edu/david/linear.algebra/ula/ula/ula.html

Ein Skript/Buch zur linearen Algebra mit vielen Anwendungsbeispielen und eingebetteten Berechnungen/Berechnungsaufgaben mit dem Computeralgebra-System *Sage*.

J. Hefferon, *Linear Algebra*, http://joshua.smcvt.edu/linearalgebra/

Dieses Buch enthält viele *Topics* (Ausblicke, Ergänzungen) zu Anwendungen und Verbindungen mit anderen Themen.

S. Axler, *Linear Algebra Done Right*, Springer 2015,
https://doi.org/10.1007/978-3-319-11080-6

S. Treil, *Linear Algebra Done Wrong*,
https://www.math.brown.edu/~treil/papers/LADW/LADW.html.

Zum Schluss noch zwei »fortgeschrittenere« Bücher, in denen die lineare Algebra als eines von mehreren Themen behandelt wird.

T. Hungerford, *Algebra*, Springer Graduate Texts in Math. **73**, 1974.

Ein Standard-Lehrbuch im US-amerikanischen Raum, das allerdings wesentlich mehr Stoff als die lineare Algebra enthält (die Algebra und ein Teil der kommutativen Algebra sind auch dabei, und noch ein paar andere Themen). Dafür finden Sie hier das meiste, was wir in der Vorlesung machen, kurz und knapp zusammengefasst.

E. Vinberg, *A Course in Algebra*, Graduate Studies in Math. **56**, AMS 2003.

Dieses Buch enthält ebenfalls wesentlich mehr Stoff als die lineare Algebra. Es ist vielleicht insgesamt etwas einfacher zu lesen als das Buch von Hungerford.

C.5. Verschiedene Buchempfehlungen

C.5.1. Was ist Mathematik? Diese Frage ist natürlich nicht so leicht zu beantworten. Was ist Ihre Antwort? Die folgenden Bücher versuchen in sehr unterschiedlicher Weise, eine Antwort zu geben.

T. Gowers, *Mathematik*, Reclam-Sachbuch 2011 (oder das englische Original: *Mathematics. A very short introduction*, Oxford Univ. Press 2002).

Eine kurze Abhandlung zur Fragestellung *Was ist Mathematik* (aber vielleicht doch nicht *very short*, auch wenn es dem Autor Timothy Gowers, der 1998 für seine Forschung mit der Fields-Medaille ausgezeichnet wurde, womöglich so vorkam). Gut lesbar, auch vor dem Beginn des Mathematikstudiums, und mit einem Preis von aktuell 5,60 € mehr als preiswert. Besondere Empfehlungen: Die Kapitel 3 (Beweise), 5 (Dimension), 6 (Geometrie).

T. Gowers, *The Princeton Companion to Mathematics*, Princeton Univ. Press 2008.

Tausend Seiten über Mathematik, von einem Kapitel über die Geschichte der Mathematik über mathematische Konzepte, Theoreme und Vermutungen, Kurzbiographien von Mathematikern zum Einfluss der Mathematik in Biologie, Chemie, Informatik, den Wirtschaftswissenschaften sowie Kunst und Musik. Wenn Sie anfangen, in diesem Buch zu blättern, finden Sie sicher etwas, was Sie interessiert.

Behrends, Fünf Minuten Mathematik https://doi.org/10.1007/978-3-8348-9529-5

100 Beiträge aus der Mathematik-Kolumne, die E. Behrends für die Tageszeitung *Die Welt* geschrieben hat. Die *5 Minuten* sind durchaus wörtlich zu nehmen, so dass die einzelnen Texte nicht in die Tiefe gehen. Dafür lassen sie sich aber eben mal schnell zwischendurch lesen, geben einen Eindruck von der Vielseitigkeit der Mathematik und machen oft Appetit auf mehr.

R. Courant, H. Robbins, *Was ist Mathematik*, Springer 1992

Ein Klassiker (der inzwischen vielleicht ein bisschen angestaubt ist), der schon deshalb nicht in dieser Liste fehlen darf, weil der Abschnitt mit dem Titel dieses Buchs überschrieben ist. Das Buch richtet sich (auch) an Studienanfänger∗innen (und teils an Schüler∗innen), ist aber nicht immer leicht zu lesen.

C.5.2. Dies und das. Verschiedene Buchtipps, die nicht unbedingt etwas mit linearer Algebra zu tun haben – für den Fall, dass Sie sich langweilen oder noch etwas suchen, was Sie sich zu Weihnachten wünschen können (und dabei einen intellektuellen Eindruck hinterlassen).

T. Körner, *The pleasures of counting*, Cambridge Univ. Press 1996 (Es gibt auch eine deutsche Übersetzung: *Mathematisches Denken – vom Vergnügen am Umgang mit Zahlen*, Birkhäuser 1998)

Ein dickes Buch (über 500 Seiten), in dem alle möglichen Anwendungen von Mathematik beschrieben werden, beginnend mit der Bekämpfung der Cholera um 1850, bei der man durch eine simple Statistik feststellen konnte, dass die Krankheit über das Trinkwasser übertragen wird – damals ein Durchbruch, über Verschlüsselungstheorie bis zu verschiedenen Anwendungen von Methoden der Analysis.

T. Körner, *Calculus for the ambitious*, Cambridge Univ. Press 2014.

Auch wenn dieses Buch gar nichts mit linearer Algebra zu tun hat, nehme ich es in die Liste auf, weil es mir so gut gefallen hat. Eine Einführung in den Stoff der Vorlesung Analysis I, in der der formale Anspruch, wie er in einer Vorlesung (aus guten Gründen) besteht, zurückgestellt wird und die Theorie von einem intuitiven Standpunkt aus entwickelt wird. Das macht das Buch nicht unbedingt leichter zu lesen als ein herkömmliches Lehrbuch, ich denke aber, dass es sehr lehrreich ist, sich auf diese Lektüre einzulassen.

J. Matoušek, *Thirty-three Miniatures*, Mathematical and Algorithmic Applications of Linear Algebra, Student Math. Library **35**, AMS 2010.
Siehe auch https://kam.mff.cuni.cz/%7Ematousek/stml-53-matousek-1.pdf

Ein Buch mit direktem Bezug zur linearen Algebra (das auch im Text mehrfach zitiert wird), aber kein Lehrbuch. Stattdessen hat der Autor 33 Problemstellungen ausgewählt und beschrieben, bei deren Lösung die Methoden der linearen Algebra nützlich sind und oft auf überraschende Art und Weise eingesetzt werden.

M. Aigner, G. Ziegler, *Das BUCH der Beweise*, Springer 2018
https://doi.org/10.1007/978-3-662-57767-7

Der Mathematiker Paul Erdős hat die Redensart vom *Buch der Beweise* geprägt, in dem Gott für jedes mathematische Ergebnis den perfekten Beweis aufgeschrieben hat. Das Buch von Aigner und Ziegler ist sozusagen ein Auszug davon. Einige der Beweise sind auch mit wenig Grundkenntnissen zugänglich.

C. Rousseau, Y. Saint-Aubin, *Mathematik und Technologie*, Springer 2012,
https://doi.org/10.1007/978-3-642-30092-9

In fünfzehn Kapiteln werden verschiedene Anwendungen von mathematischen Methoden auf »Alltagsprobleme« erklärt. Es wird dadurch hervorragend sichtbar, wie viel Mathematik in der Technologisierung der Gesellschaft steckt. Zum Beispiel: Navigation mit GPS, Radiochirurgie/Computertomographie, Robotik, das RSA-Verfahren aus der Kryptographie, Zufallszahlengeneratoren. Auch einige der im Skript angesprochenen Themen werden diskutiert (zum Beispiel der Page-rank-Algorithmus und Codes).

C.5.3. Mathematik (auf-)schreiben. Mathematik verständlich aufzuschreiben, ist nicht immer einfach. Im Grunde sollte es ausreichen, wenn Sie das mit den Übungsaufgaben trainieren, aber es gibt auch Texte, in denen das explizit thematisiert wird. (Für den technischen Aspekt des mathematischen Schriftsatzes am Computer siehe B.2.)

Beutelspacher, *Das ist o.B.d.A. trivial!*, Vieweg 2006
https://doi.org/10.1007/978-3-8348-9075-7

Vielleicht ist es übertrieben, ein ganzes Buch zu dem Thema zu lesen, wie man Mathematik klar verständlich aufschreibt, aber einmal in dieses Buch hereinzuschauen, kann sich lohnen.

K. Conrad, Advice on mathematical writing[2]

(auf Englisch, aber das meiste lässt sich direkt auf deutsche Texte übertragen)

J. P. Serre, How to write mathematics badly,
https://www.youtube.com/watch?v=ECQyFzzBHlo.

Der berühmte Mathematiker J. P. Serre erklärt in diesem unterhaltsamen Vortrag, wie man es nicht machen sollte …

C.6. Webseiten, Videos

Unter dem Namen 3blue1brown[3] hat G. Sanderson viele verschiedene kurze Videos zu mathematischen Themen produziert und veröffentlicht, die ich großenteils sehr gelungen finde, darunter eine Serie *Essence of linear algebra*. Von einigen dieser Videos gibt es auch eine deutsche Version. Direkt zum Youtube-Kanal[4].

mathe-vital.de[5] ist ein Projekt des Lehrstuhls »Geometrie und Visualisierung« der TU München, das von J. Richter-Gebert gegründet wurde. Sie finden dort viele Visualisierungen und Applets zu Themen aus der linearen Algebra und aus anderen Gebieten.

C. Baer hat eine Seite mit Übungsaufgaben[6] zu verschiedenen Themen.

Es gibt natürlich noch viel, viel mehr Videos und Webseiten zur Linearen Algebra und allgemeiner zur Mathematik, auch zu Themen des Mathematikstudiums – von unterschiedlich hoher Qualität…Wenn Sie einen Vorschlag haben, was an dieser Stelle noch ergänzt werden sollte (das gilt natürlich auch für Bücher), teilen Sie es mir mit!

[2] https://kconrad.math.uconn.edu/blurbs/proofs/writingtips.pdf
[3] https://www.3blue1brown.com/
[4] https://www.youtube.com/c/3blue1brown
[5] http://www.mathe-vital.de/
[6] https://www.cbaer.eu/joomla/index.php/en/mathematics/practice

Literaturverzeichnis

[Ba] C. Baer, *Lineare Algebra und Analytische Geometrie*, Springer Spektrum 2018, https://doi.org/10.1007/978-3-658-22620-6

[Bo] S. Bosch, *Lineare Algebra* https://doi.org/10.1007/978-3-642-55260-1

[Fi] G. Fischer, *Lineare Algebra* https://doi.org/10.1007/978-3-658-03945-5

[Go] T. Gowers, *Mathematik*, Reclam-Sachbuch 2011 (oder das englische Original: *Mathematics. A very short introduction*, Oxford Univ. Press 2002)

[Gr] D. Grieser, *Mathematisches Problemlösen und Beweisen*, Springer Spektrum 2017, https://doi.org/10.1007/978-3-658-14765-5

[He] H. Heuser, *Lehrbuch der Analysis, Teil 1*, Teubner-Verlag, 9. Aufl., 1991.

[Ho] K. Houston, *Wie man mathematisch denkt*, Springer Spektrum 2012

[Hu] T. Hungerford, *Algebra*, Springer Graduate Texts in Math. **73**, 1974.

[Jä] K. Jähnich, *Lineare Algebra*, Springer Hochschultext, 2. Aufl., 1981.

[LM] J. Liesen, V. Mehrmann, *Lineare Algebra*, Springer 2015. https://doi.org/10.1007/978-3-658-06610-9

[Lo] F. Lorenz, *Lineare Algebra 1*, Spektrum Akad. Verlag 2004.

[Ma] J. Matoušek, *Thirty-three Miniatures*, Mathematical and Algorithmic Applications of Linear Algebra, Student Math. Library **35**, AMS 2010. Siehe auch preliminary version[7].

[Pi] R. Pink, *Lineare Algebra I und II*, Zusammenfassung, 2016. https://people.math.ethz.ch/~pink/ftp/Lineare-Algebra-Zusammenfassung-20161006.pdf

[RS] C. Rousseau, Y. Saint-Aubin, *Mathematik und Technologie*, Springer 2012, https://doi.org/10.1007/978-3-642-30092-9

[So] W. Soergel, *Lineare Algebra 1*, http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXLA1.pdf

[So-AZT] W. Soergel, *Algebra und Zahlentheorie*, http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXAL.pdf

[VK] S. Verma, J. P. Krishna, Image compression and linear algebra[8], 2013.

[vL] J. van Lint, *Introduction to Coding Theory*, Springer Graduate Texts in Mathematics **86**, 3rd ed., 1999.

[7] https://kam.mff.cuni.cz/%7Ematousek/stml-53-matousek-1.pdf

[8] https://www.cmi.ac.in/%7Eksutar/NLA2013/imagecompression.pdf

Index