Lineare Algebra

Fabian Hebestreit

Contents

KAPITEL 1

Grundlagen

1. Aussagen

Um später im Ernstfall eine präzise Sprache zu ermöglichen, beginnen wir mit etwas Vokabular, das wir der Alltagssprache entreißen:

1.1. Konvention Eine *Aussage (statement)* ist ein Satz, der eindeutigerweise entweder *wahr (true)* oder *falsch (false)* ist.

1.2. Beispiel Typische Beispiele, die dieser Konvention sicherlich genügen, sind:

(1) Jede natürliche Zahl ist gerade.
(2) 6 ist durch 3 ohne Rest teilbar.
(3) 34 ist größer als 27.
(4) 27 ist größer als 34.

Diese Aussagen, so sind wir uns hoffentlich alle einig, sind in Reihenfolge falsch, wahr, wahr und falsch. Einige schon eher problematische Beispiele sind

(1) Milch kommt aus Tieren.
(2) Franz hat eine Brille auf.
(3) 7 ist meine Lieblingszahl.

aber Alltagsaussagen wie diese sind selten präzise genug um wirklich Aussagen im Sinne obiger Konvention zu sein (wie steht es um Hafermilch oder Sonnenmilch? Hat man eine Brille auch auf, wenn man sie nicht auf der Nase trägt, sondern in die Haare hochgeschoben hat? Was bedeutet eigentlich dieses "Lieblings-" genau?) Definitv keine Beispiele sind:

(1) Ich lüge gerade.
(2) Es regnet.
(3) Franziska hat graue Haare.

Der erste Satz ist eine Variante des berühmten Paradox des Epimenides: Ist die getroffene Aussage wahr, so muss sie eine Lüge sein, und daher in Wahrheit falsch. Ist die getroffene hingegen Aussage falsch, so ist sie nicht gelogen, muss also wahr sein. Ergo können wir nicht sinnvoll einen Wahrheitsgehalt zuweisen. Der zweite Satz ist viel zu vage: Regnet es jetzt gerade oder manchmal? Zählt Niesel schon als Regen? Und über welchen Ort wird überhaupt geredet. Der dritte Fall ist ähnlich: In der Alltagssprache meint man mit "hat graue Haare" manchmal, dass alle Haare einer Person grau sind, und manchmal nur dass einige Haare grau, aber durchaus noch braune, blonde, oder auch hell-pinke Haare auf dem Kopf zu finden sind. Wieder viel zu ungenau.

Eine erste große Herausforderung wird es nun sein sich daran zu gewöhnen, sehr scharf zwischen Aussagen im Sinne obiger Konvention und Alltagssprache zu trennen. Wir werden im weiteren im wesentlichen nur Aussagen erlauben, um über mathematische Inhalte zu reden, allein schon um Missverständnisse zu vermeiden. Ich wünschte mir manchmal, dies wäre auch eine Alltagskonvention...

1.3. Konstruktion Sind A und B zwei Aussagen, so konstruieren wir zwei neue Aussagen

$$(A) \vee (B) \quad \text{und} \quad (A) \wedge (B),$$

die *Disjunktion (disjunction)* bzw. *Konjunktion (conjunction)* von A und B: Ihre Wahrheitswerte sind durch folgende Vorschriften gegeben:

$$(A) \vee (B) \quad \text{ist} \quad \begin{cases} \text{wahr} & \text{falls } A \text{ und } B \text{ beide wahr sind} \\ \text{wahr} & \text{falls } A \text{ wahr ist und } B \text{ falsch} \\ \text{wahr} & \text{falls } A \text{ falsch ist und } B \text{ wahr} \\ \text{falsch} & \text{falls } A \text{ und } B \text{ falsch sind.} \end{cases}$$

$$(A) \wedge (B) \quad \text{ist} \quad \begin{cases} \text{wahr} & \text{falls } A \text{ und } B \text{ beide wahr sind} \\ \text{falsch} & \text{falls } A \text{ wahr ist und } B \text{ falsch} \\ \text{falsch} & \text{falls } A \text{ falsch ist und } B \text{ wahr} \\ \text{falsch} & \text{falls } A \text{ und } B \text{ falsch sind.} \end{cases}$$

Diese Konstruktion formalisiert die Alltagsbegriffe "und" und "oder". Man stellt die Vorschriften häufig als Wahrheitstafeln dar:

B \ A	w	f
w	w	w
f	w	f

$(A) \vee (B)$

B \ A	w	f
w	w	f
f	f	f

$(A) \wedge (B)$

1.4. Warnung Konjunktion und Diskjunktion enthalten keinerlei Hinweise auf logische, kausale oder sonstige Zusammenhänge zwischen den teilnehmenden Aussagen, anders als man dies aus dem Alltag kennt. Ein schönes Beispielsind etwa die zwei Sätze:

Er beging eine Straftat und ging ins Gefängnis.

Er ging ins Gefängnis und beging eine Straftat.

Intuitiv würden viele von uns aus dem ersten Satz wohl ablesen, dass die erwähnte Straftat der Grund für den Gefängnisgang ist (und insbesondere etwa bemerkt wurde), wohingegen man in den zweiten Satz eher hineinliest, dass der arme Protagonist wohl mittlerweile mindestens zweimal abseits des Gesetzes tätig war. Nichts davon ist aber wirklich gesagt, und von solchen Assoziation müssen Sie sich befreien. Die beiden Aussagen

(Er beging eine Straftat) $\wedge$ (Er ging ins Gefängnis)

(Er ging ins Gefängnis) $\wedge$ (Er beging eine Straftat)

sind für uns inhaltsgleich (sofern wir uns denn für den Zwecke dieses Beispiels einigen wollen wollen, dass "Er beging eine Straftat" und "Er ging ins Gefängnis" wirklich Aussagen sind).

Trotz dieser Diskrepanz werden wir häufig (A) *und* (B) anstatt $(A \wedge B)$ und (A) *oder* (B) anstatt $(A) \vee (B)$.

1.5. Beispiel (1) Hier sind zwei wahre Aussagen:
   (a) (34 ist größer als 27) und (rot ist eine Farbe).
   (b) (27 ist größer als 34) oder (rot ist eine Farbe).

(2) Im Sinne obiger Konstruktion muss die Antwort auf die Frage "Möchtest du Tee oder Kaffee" wohl "Ja" oder "Nein" lauten, je nachdem, welches von (Tee oder Kaffee) und (nichts) man denn will.

(3) Die Klammung, die beim verbinden von nur zwei Aussagen erstmal unnötig und vielleicht etwas nervig erscheint, ist enorm wichtig, sobald Disjunktion und Konjunktion beide im Spiel sind: Die beiden Aussagen

$$((A) \wedge (B)) \vee (C) \quad \text{und} \quad (A) \wedge ((B) \vee (C))$$

können sehr verschieden sein:

Paul went to the loo and did a number one or number two.

Nur bei einer Klammerung ist sichergestellt, dass Paul mit seiner Notdurft den Lokus erreicht hat.

1.6. Konstruktion Eine weitere wichtige Art aus alten Aussagen neue zu produzieren ist die *Negation (negation)*: Zu einer Aussage A bilden wir die Aussage $\neg(A)$, deren Wahrheitwert durch

$$\neg(A) \quad \text{ist} \quad \begin{cases} \text{falsch} & \text{falls } A \text{ wahr ist} \\ \text{wahr} & \text{falls } A \text{ falsch ist.} \end{cases}$$

Sie formalisiert den Alltagsbegriff "nicht" oder "Gegenteil von" und hat die Wahrheitstafel

A	w	f
	f	w

$\neg(A)$

1.7. Beispiel (1) $\neg$(Jede natürliche Zahl ist gerade) ist inhaltsgleich zu (Es gibt ungerade natürliche Zahlen), und ist natürlich wahr.

(2) $\neg$(Hans ist ein Untergebener von Lisa) hat den gleichen Gehalt wie (Hans ist kein Untergebener von Lisa), aber nicht unbedingt wie (Lisa ist eine Untergebene von Hans): Etwa könnten sie beide gleichen Rang haben.

Aus den Bausteinen $\wedge, \vee, \neg$ lassen sich viele andere Operationen zusammensetzen. Ein Beispiel ist die *Exklusivdisjunktion (exclusive disjunction)* $(A) \times (B)$, die definiert ist als

$$((A) \vee (B)) \wedge (\neg((A) \wedge (B))).$$

Etwas kürzer schreibt man in solchen Fällen gern

$$(A) \times (B) := ((A) \vee (B)) \wedge (\neg((A) \wedge (B)));$$

das Zeichen $:=$ ist als "ist definiert als" zu lesen und bedeutet, dass die linke Seite eine Abkürzende Schreibweise für die rechte Seite ist; man sollte diese Zeichen als ein einzelnes lesen, das nicht aus : und = zusammengesetzt ist (historisch kommt es natürlich daher).

Wichtiger als das in der Mathematik recht ungebräuchliche "exklusiv-oder" sind:

1.8. Definition Sind A und B Aussagen so setzen wir:

$$(A) \Rightarrow (B) := (\neg(A)) \vee (B)$$
$$(A) \Leftarrow (B) := (B) \Rightarrow (A)$$
$$(A) \Leftrightarrow (B) := ((A) \Rightarrow (B)) \wedge ((A) \Leftarrow (B))$$

Die ersten beiden nennt man *Implikationen (implications)* und die dritte *Äquivalenz (equivalence)*.

Gelesen werden Äquivalenzen als "genau dann, wenn" und die Implikationen demzufolge als "dann" ($\Rightarrow$) und "wenn" ($\Leftarrow$). Die Wahrheitstabellen lauten:

B \ A	w	f
w	w	w
f	f	w

$(A) \Rightarrow (B)$

B \ A	w	f
w	w	f
f	w	w

$(A) \Leftarrow (B)$

B \ A	w	f
w	w	f
f	f	w

$(A) \Leftrightarrow (B)$

1.9. Warnung Noch mehr als bei "und" und "oder" gibt es in vielen von uns den Impuls bei $(A) \Rightarrow (B)$ eine Kausalität in die Aussage hineinzulesen. Widerstehen Sie ihm. So ist etwa

$$(\text{Rot ist eine Farbe}) \Rightarrow (34 \text{ ist größer als } 27)$$

eine wahre Aussage, aber die Größe von 34 hat sicherlich nichts mit der Farbigkeit von rot zu tun.

Insbesondere gilt: Eine falsche Aussage impliziert jede Aussage. Nehmen Sie sich diese Weisheit zu Herzen: Es reicht ein einziger Fehler in einer Argumentationskette um das ganze Konstrukt zum Einsturz zu bringen.

Es gelten nun eine Myriade Rechenregeln für all diese Operationen. Um sie alle aufzuschreiben, sei noch vereinbart, dass w and f eine *Tautologie* und eine *Antinomie*, also eine wahre und eine falsche Aussage bezeichnen.

1.10. Satz *Sind A, B und C Aussagen so gelten*

(1) Assoziativität (associativity)

$$[((A)\vee(B))\vee(C)]\iff[(A)\vee((B)\vee(C))] \quad \textit{und} \quad [((A)\wedge(B))\wedge(C)]\iff[(A)\wedge((B)\wedge(C))]$$

(2) Kommutativität (commutativity)

$$[(A)\vee(B)]\iff[(B)\vee(A)] \quad \textit{und} \quad [(A)\wedge(B)]\iff[(B)\wedge(A)]$$

(3) Neutralität (neutrality)

$$[(A)\vee f]\iff(A) \quad \textit{und} \quad [(A)\wedge w]\iff(A)$$

(4) Absorption (absorption)

$$(A)\vee w \quad \textit{und} \quad \neg((A)\wedge f)$$

(5) Idempotenz (idempotency)

$$\neg(\neg(A))\iff(A)$$

(6) tertium non datur (law of the excluded middle)

$$(A)\vee(\neg(A)) \quad \textit{und} \quad \neg((A)\wedge\neg(A))$$

(7) de Morghan'schen Gesetze (de Morghan's laws)

$$[\neg((A)\vee(B))]\iff[(\neg(A))\wedge(\neg(B))] \quad \textit{und} \quad [\neg((A)\wedge(B))]\iff[(\neg(A))\vee(\neg(B))]$$

(8) Distributivität (distributivity)

$$[(A)\wedge((B)\vee(C))]\iff[((A)\wedge(B))\vee((A)\wedge(C))] \quad \textit{und} \quad [(A)\vee((B)\wedge(C))]\iff[((A)\vee(B))\wedge((A)\vee(C))]$$

(9) Transitivität (transivity)

$$[((A)\Rightarrow(B))\wedge((B)\Rightarrow(C))]\Longrightarrow[(A)\Rightarrow(C)]$$

(10) Substitution (substitution)

$$[(A)\Rightarrow(B)]\Longrightarrow[((A)\vee(C))\Rightarrow((B)\vee(C))]$$
$$[(A)\Rightarrow(B)]\Longrightarrow[((A)\wedge(C))\Rightarrow((B)\wedge(C))]$$

(11) Umkehrschluss (contraposition)

$$[(A)\Rightarrow(B)]\iff[(\neg(B))\Rightarrow(\neg(A))]$$

Die Assoziativität erlaubt es uns im weiteren viel der Klammern um Aussagen wegzulassen. So werden wir etwa eher $(A)\wedge(B)\wedge(C)$ schreiben und damit eine der äquivalenten Aussage in (1) meinen. In Wahrheit werden wir meist sogar $A\wedge B\wedge C$ schreiben und die Klammern nur setzen, wenn sie Verwirrung vermeiden (etwa wenn eine der Aussagen A, B oder C selbst wieder eine Disjunktion enthalten, sodass die Warnung 1.5 (3) zuschlägt. .

Beweis. Diese Regeln lassen sich alle durch simple Fallunterscheidung nachweisen. Am einfachsten sind wohl die beiden Absorptionsgesetze. Für sie reichen ein direkter Blick in die Wahrheitstabellen. Und das Idempotenzgesetz is nicht schwerer: Ist A wahr, so ist $\neg(A)$ falsch, ergo $\neg(\neg(A))$ wieder wahr, und ähnlich ist, falls A falsch ist, $\neg(A)$ wahr und dann $\neg(\neg(A))$ wieder falsch. Ein Blick in die Wahrheitstabelle Äquivalent zeigt dann aber, dass sowohl zwei wahre als auch zwei falsche Aussage eine wahre Aussage liefern. Die Neutralitätsgesetze sind auch einfach: Ist A wahr so nach Blick in die Wahrheitstabelle der Disjunktion auch $(A)\vee w$ und ist A falsch, so auch $(A)\vee w$, und wieder beendet ein Blick in die Wahrheitstabelle der Äquivalenz den Nachweis. Ähnliches für die Version der Konjugation. Um zu sehen, dass es etwas drittes nicht gibt, beobachten wir, dass immer genau eine der Aussagen A und $\neg(A)$ wahr ist, was durch Blick in die Wahrheitstabelle der Disjunktion verrät, dass $(A)\vee(\neq(A))$ immer wahr ist und in die der Konjugation, dass $(A)\wedge(\neg(A))$ nie wahr ist.

Für die Kommutativität stellt man fest, dass die Wahrheitstabelle von Disjunktion und Konjugation sich bei Vertauschen von A und B nicht verändern. Für die de Morghan'schen Gesetze ergeben sich für das erste und zweite jeweils auf beiden Seiten die Wahrheitstabellen

B \ A	w	f
w	f	f
f	f	w

B \ A	w	f
w	f	w
f	w	w

Assoziativität und Distributivität ergeben sich, indem man etwa Wahrheitstabellen erst C als wahr annimmt, und dann Wahrheitstabellen anfertigt, und dann ähnliches falls C falsch ist. Im ersten Fall, also falls C wahr ist ergeben sich in den vier Gesetzen jeweils

B \ A	w	f
w	w	w
f	w	w

B \ A	w	f
w	w	f
f	f	f

Assoziativitätsgesetze mit C wahr

B \ A	w	f
w	w	f
f	w	f

B \ A	w	f
w	w	w
f	w	f

Distrubutivitätsgesetzte mit C wahr

als Wahrheitstabellen beider Seiten, und falls C falsch ist erhalten wir

B \ A	w	f
w	w	w
f	w	f

B \ A	w	f
w	f	f
f	f	f

Assoziativitätsgesetze mit C falsch

B \ A	w	f
w	w	f
f	f	f

B \ A	w	f
w	w	f
f	w	f

Distrubutivitätsgesetzte mit C falsch

Damit bleiben noch die ersten beiden Substitutionsregeln und die Transitivität. Für die ersten beiden Substitutionsgesetze lauten die Wahrheitstabellen für die rechten Seiten der Implikationen

B \ A	w	f
w	w	w
f	w	w

B \ A	w	f
w	w	f
f	f	w

Rechte Seiten der Substitutionsgesetze mit C wahr

B \ A	w	f
w	w	f
f	f	w

B \ A	w	f
w	w	w
f	w	w

Rechte Seiten der Substitutionsgesetze mit C falsch

In allen Fällen taucht hier nur ein Eintrag "wahr" auf, wenn dieser auch in $(A) \Leftrightarrow (B)$ auftaucht. Das dritte Substitutionsgesetz ergibt sich wieder direkt durch einen Blick auf die Wahrheitstafel der Äquivalenz. Der Umkehrschluss folgt wieder direkt durch scharfes Hinsehen in der Wahrheitstafel der Implikation.

Zuletzt machen wir für die Transitivität eine Fallunterscheidung in B: Die Negation der linken Seite hat die Wahrheitstafel

C \ A	w	f
w	f	f
f	w	w

mit B wahr

B \ A	w	f
w	w	f
f	w	f

mit B falsch

In jedem Fall liefert die eintragsweise Disjunktion mit

C \ A	w	f
w	w	w
f	f	w

$$(A) \Rightarrow (C)$$

immer eine wahre Aussage. □

Hiermit haben wir nun wohl das Standardarsenal an Methoden zur Verfügung eine Aussage A als wahr nachzuweisen: Die leichteste Methode ist es eine schon als wahr bekannte Aussage zu finden und zu zeigen, dass $B \Rightarrow A$ wahr ist. Dann zeigt ein Blick in die Wahrheitstabelle der Implikation sofort, dass auch A wahr sein muss. Die Transitivität erlaubt es, hierfür noch weitere Aussagen zwischen zu schalten, also neben der wahren Aussage B etwa noch eine Aussage C zu finden und $B \Rightarrow C$ und $C \Rightarrow A$ als wahr nachzuweisen. Dann folgt nämlich $B \Rightarrow A$ und damit auch A. In diesem Fall spricht man oft von C als einem Zwischenschritt im Beweis von A.

Auf einem anderen Wege ist es etwa möglich, um A als wahr nachzuweisen, den Umkehrschluss zu verwenden: Hierzu muss man eine wahre Aussage B finden und nachweisen dass $\neg(A) \Rightarrow \neg(B)$ gilt. Es folgt dann nämlich $B \Rightarrow A$ und A folgt. Man spricht in diesem Fall von einem Beweis durch Widerspruch.

1.11. Beispiel Nachdem man Gesetze (1) - (10) nachgewiesen hat, kann man etwa den Umkehrschluss anstatt wie oben durch Blick auf die Wahrheitstafeln auch auf diese Weise herleiten: Ausgeschrieben bedeutet

$$(*) := \big([(A) \Rightarrow (B)] \Longrightarrow [(\neg(B)) \Rightarrow (\neg(A))]\big)$$

(und das ist eine Hälfte der Behauptung des Umkehrschlusses) dass

$$\neg(\neg A \vee B) \vee (\neg(\neg B) \vee \neg A).$$

Wegen des Idempotenzgesetzes gilt $\neg(\neg B) \Leftrightarrow B$, sodass eine Anwendung des Substitutionsgesetzes

$$[\neg(\neg A \vee B) \vee (B \vee \neg A)] \Longrightarrow (*)$$

liefert. Aber aufgrund des Kommutativitätsgesetzes gilt $[B \vee \neg A] \Longleftrightarrow [\neg A \vee B]$ und demzufolge liefert das Substitutionsgesetz

$$[\neg(\neg A \vee B) \vee (\neg A \vee B)] \Longrightarrow [\neg(\neg A \vee B) \vee (B \vee \neg A)]$$

und dann das Transitivitätsgesetz

$$[\neg(\neg A \vee B) \vee (\neg A \vee B)] \Longrightarrow (*).$$

Aber $\neg(\neg A \vee B) \vee (\neg A \vee B)$ ist wahr, da tertium non datur (etwas drittes gibt es nicht). Also ist auch $(*)$ wahr.

Das ist natürlich an dieser Stelle noch um einiges komplizierter als der Blick in die Wahrheitstafel, aber im Weiteren wird das letztere keine Option mehr sein. Um den Text etwas kürzer (und hoffentlich auch verständlicher) zu machen, lässt die Anwendungen von Substitution und Transitivität meist implizit und schreibt diesen Beweis etwa einfach wie folgt auf:

$$\begin{aligned}\neg(\neg A \vee B) \vee (\neg A \vee B)] &\Longrightarrow [\neg(\neg A \vee B) \vee (B \vee \neg A)] \\ &\Longrightarrow [\neg(\neg A \vee B) \vee (\neg(\neg B) \vee \neg A)]\end{aligned}$$

wobei im ersten Schritt Kommutativität und im zweiten Schritt Idempotenz benutzt wird, und die Ursprungsaussage wegen tertium non datur wahr ist.

Schon etwas besser.

2. Prädikate

2.1. Konvention Ein *Prädikat (predicate)* P ist ein Satz, der einen oder mehrere Platzhalter (oder Variablen) enthält, zusammen mit einem *Definitionsbereich (domain of definition)*, derart dass durch Einsetzen eines jeden Objektes d aus dem Definitionsbereich für den Platzhalter eine Aussage $P(d)$ entsteht.

2.2. Beispiel
(1) "x ist gerade" mit Variable x und Definitionsbereich die natürlichen Zahlen. Anstatt (x ist gerade)(5) schreiben wir natürlich "5 ist gerade". Das ist übrigends falsch.
(2) "x ist gerade" mit Variable x und Definitionsbereich die Bäume ist kein Beispiel. Was soll es schon heißen einen Baum durch 2 zu teilen? Oder wann ist ein Baum sonst gerade?
(3) "x ist gerade" mit Variablen x und y und Definitionsbereich die natürlichen Zahlen (für x) und die Bäume (für y). Insbesondere müssen die Variablen eines Prädikates nicht wirklich in ihm vorkommen.
(4) "y ist gerade" mit Variable x und Definitionsbereich die natürlichen Zahlen ist wieder kein Beispiel. Was soll y denn sein, wenn es nicht die Variable des Prädikats ist?

Der Sinn und Zweck von Prädikaten ist es, aus ihnen Aussagen zu gewinnen. Zum einen hat man natürlich die einzelnen Aussagen $P(d)$, aber interessant wird das ganze durch:

2.3. Konstruktion Ist P ein Prädikat mit Variable x, so bilden wir zwei neue Aussagen

$$\forall x \text{ in } D\colon P \quad \text{und} \quad \exists x \text{ in } D\colon P$$

die *Universal-* und *Existenzquantifizierung (universal-* und *existence quantification)* von P, deren Wahrheitswerte gegeben sind durch

$$\forall x \text{ in } D\colon P \quad \text{ist} \quad \begin{cases} \text{wahr} & \text{falls } P(d) \text{ für jedes Objekt } d \text{ des Definitionsbereiches von } P \text{ wahr ist} \\ \text{falsch} & \text{falls } P(d) \text{ für mindestens ein Objekt } d \text{ des Definitionsbereiches falsch ist.} \end{cases}$$

$$\exists x \text{ in } D\colon P \quad \text{ist} \quad \begin{cases} \text{wahr} & \text{falls } P(d) \text{ für mindestens ein Objekt } d \text{ des Definitionsbereiches wahr ist} \\ \text{falsch} & \text{falls } P(d) \text{ für jedes Objekt } d \text{ des Definitionsbereiches von } P \text{ falsch ist.} \end{cases}$$

Häufig lässt man den Definitionsbereich auch implizit und schreibt nur

$$\forall x\colon P \quad \text{und} \quad \exists x\colon P$$

Hat ein Prädikat mehrere Variable, etwa x, y, so kann man $\forall x\colon P$ und $\exists x\colon P$ ebenfalls bilden (man spricht von partieller Quantifizierung) und erhält ein neues Prädikat, nun mit Variable y, deren Definitionsbereich sich nicht ändert. Es ist so definiert, dass $(\forall x\colon P)(d)$ für ein d aus dem Definitionsbereich von y wahr ist genau dann, wenn $P(d', d)$ für alle d' aus dem Definitionsbereich von x wahr ist, und ähnliches für partielle Existenzquantifikation.

Insbesondere kann man für ein Prädikat P mit Variablen x, y doppelt quantifizieren und die Aussagen

$$\forall x\colon (\forall y\colon P) \quad \text{and} \quad \forall x\colon (\exists y\colon P) \quad \text{and} \quad \exists x\colon (\forall y\colon P) \quad \text{and} \quad \exists x\colon (\exists y\colon P)$$

bilden. Durch Schachtelung von Ausdrücke der mittleren Sorte kann man schnell recht komplexe Aussagen erzeugen. Auch hier spart man sich wann immer möglich die Klammern und auch den ersten der Doppelpunkte schreibt man nur aus, wenn er beim Lesen hilft.

2.4. Beispiel (1) "x ist kleiner als y" ist ein zweistelliges Prädikat mit Variablen x, y und Definitionsbereichen die natürlichen Zahlen. Die Aussagen $(\exists x, y\colon x \text{ ist kleiner als } y)$ und $(\forall x \exists y\colon x \text{ ist kleiner als } y)$ sind wahr, wohingegen die Aussagen $(\exists y \forall x\colon x \text{ ist kleiner als } y)$ und $(\forall x, y\colon x \text{ ist kleiner als } y)$ falsch sind. Machen Sie sich dies gerade bei den mittleren beiden wirklich klar: Zu jeder natürlichen Zahl d gibt es eine größere (etwa $d + 17$), aber es gibt keine natürliche Zahl, die größer als alle anderen ist.

(2) Bei Schachproblemen gibt es Brettisituationen, die man mit "Weiß gewinnt in zwei Zügen" bezeichnet. Das ist schon ein Beispiel einer nicht mehr ganz simplen Aussage: Sie entfaltet sich zu

$$\exists \text{ Zug von Weiß } x\colon \forall \text{ Züge von Schwarz } y\colon \exists \text{ Zug von Weiß } z\colon$$

Nach Durchführung der Züge x, dann y, dann z ist Schwarz Schachmatt.

(3) Geschachtelte Quantoren und Aussagen sind mehr die Norm als die Ausnahme in der Mathematik: Die Definition der Stetigkeit für eine Funktion $f\colon \mathbb{R} \to \mathbb{R}$ in der Analysis I wird einmal

$$\forall x \in \mathbb{R} \forall \epsilon > 0 \exists \delta > 0 \forall y \in \mathbb{R}\colon |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$$

lauten. Gewöhnen Sie sich also lieber schnell daran.

Prädikate können genau wie Aussagen verknüpft werden: Sind P und Q Prädikate mit gleichen Variablen und Definitionsbereichen so können wir die Prädikat $P \vee Q$ und $P \wedge Q$ deren Wahrheitswert bei einem Objekt d sinnvollerweise $P(d) \vee Q(d)$ bzw. $P(d) \wedge Q(d)$ sind.

Wieder gelten ein Haufen Rechenregeln:

2.5. Satz *Sind P und Q Prädikate mit Variable x und gleichem Definitionsbereich und R ein Prädikat mit Variablen x, y, so gelten folgende Aussagen:*

(1)

$$\neg(\forall x\colon P) \iff (\exists x\colon \neg P) \quad \textit{und} \quad \neg(\exists x\colon P) \iff (\forall x\colon \neg P)$$

(2)

$$(\forall x\colon P \wedge Q) \iff (\forall x\colon P) \wedge (\forall x\colon Q) \quad \textit{und} \quad (\exists x\colon P \vee Q) \iff (\exists x\colon P) \vee (\exists x\colon Q)$$

(3)

$$(\forall x\colon P \vee Q) \impliedby (\forall x\colon P) \vee (\forall x\colon Q) \quad \textit{und} \quad (\exists x\colon P \wedge Q) \implies (\exists x\colon P) \wedge (\exists x\colon Q)$$

(4)

$$\forall x \forall y\colon R \iff \forall y \forall x\colon R \quad \textit{und} \quad \exists x \exists y\colon R \iff \exists y \exists x\colon R$$

(5)

$$\exists x \forall y\colon R \implies \forall y \exists x\colon R$$

Beweis. Es verhält sich ähnlich zum Beweis von Satz 1.10: Die meisten Punkte erhält man durch scharfes Hinsehen und Fallunterscheidung. Etwa den ersten: Ist die Aussage auf der linken Seite korrekt, so ist es falsch, dass P für alle x gilt. Ergo muss es ein x geben für das P nicht gilt, was genau die Behauptung der rechten Seite ist. Es folgt nach Inspektion der Wahrheitstafel der Implikation, dass $\neg(\forall x\colon P) \implies (\exists x\colon \neg P)$. Ist andersherum die rechte Aussage wahr, gibt es ein x, für das P falsch ist. Aber dann stimmt ja sicherlich nicht, dass P für alle x gilt. Dies zeigt $(\exists x\colon \neg P) \implies \neg(\forall x\colon P)$. Die zweite Behauptung folgt analog.

Für den zweiten Punkt sind die getroffenen Aussagen hoffentlich ebenfalls offensichtlich: Etwa sind bei der linken Aussage beide Seiten genau dann wahr, wenn P und Q beide für alle x stimmen.

Etwas interessanter sind die Aussagen in Punkt (3), in den im allgemeinen jeweils nur eine Implikation gilt. Es ist klar, dass $(\forall c\colon P) \Rightarrow (\forall x\colon P \vee Q)$ und ähnliches mit Q anstelle des ersten $P's$, einfach weil ja generell $P(d) \Rightarrow P(d) \vee Q(d)$. Aber allgemein gilt

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

wie Sie auf dem ersten Übungszettel nachweisen müssen. Setzen wir für A, B, C die drei Aussagen

$$(\forall c\colon P), (\forall c\colon Q), (\forall c\colon P \vee Q)$$

ein haben wir gerade die linke Seite verifiziert und die rechte folgt wie gewünscht. Die zweite Behauptung ist analog.

Zur vierten Behauptung weiß ich gar nichts zu sagen, so offensichtlich ist sie.

Interessant ist nochmal die letzte: Die linke Seite besagt, dass ein x gibt, dass für jedes y dazu führt dass R wahr ist. Aber dann gibt es ja zu jedem y auch wirklich dieses x was R wahr macht.

Andersherum gilt das nicht: Bei Wahrheit der rechten Aussage könnte es zu verschiedenen y's verschiedene x'e geben, die R wahrmachen, auf der linken Seite reicht das nicht. □

2.6. Warnung In der Alltagssprache lässt man Quantoren oft implizit

Schnee ist weiß. Der Mann hat graues Haar.

Im ersten Falle scheint mir, man meint wohl "Aller Schnee ist weiß". Insbesondere ist dann ¬(Schnee ist weiß) die Aussage "Es gibt Schnee, der nicht weiß ist." und *nicht* (!!!) "Schnee ist nicht-weiß." Im zweiten Fall scheinen mir wohl beide Interpretationen

Alle Haare des Mannes sind grau. und Mindestens ein Haar des Mannes ist grau.

alltagskompatibel und ich nehme an, es gibt einige unter Ihnen, die intuitiv auf die eine, und einige, die es intuitiv auf die andere Weise interpretieren würden. Dies sind sehr verschiedene Aussagen. Noch seltsamer wird es, wenn man die "Aussage" negiert: Im ersten Fall ergibt sich

Mindestens ein Haar des Mannes ist nicht grau. und Kein Haar des Mannes ist grau.

Welche Bedeutung würden Sie intuitiv dem Satz "Der Mann hat nicht graues Haar." zuordnen? Mussten Sie vielleicht sogar das Camp wechseln?

Das Beispiel soll jedenfalls verdeutlichen, dass das unsere unrpäzise Alltagssprache ein großes (und wohl auch täglich genutzes) Potenzial für Verwirrungen und Missverständnisse bietet. Fügt man nun auch noch unseren Hang zum Hinzufügen von Zusammenhängen wie in Warnung 1.4 hinzu, erhält man ein unheiliges Gebräu bei dem es eher ein Wunder ist, dass überhaupt irgendwer irgendwen anders manchmal versteht (man überlege sich nur, welchen komplexes Konstrukt ein simples Wort wie "trotzdem" vermitteln soll).

Der Sinn und Zweck der formalen Sprache, die wir eingeführt haben ist es jedenfalls solchen Problemen vorzubeugen und präzise Argumente auch dann zu ermöglichen, wenn wir es mal mit wirklich komplizierten Aussagen zu tun bekommen.

Von vielen Aussagen weiß man bis heute nicht, ob sie wahr sind. Ein berühmtes Beispiel ist Goldbach's Vermutung:

$$\forall x\colon (\exists w\colon 2w = x \wedge w \geqslant 1) \Longrightarrow \big(\exists y, z\colon x = y + z$$
$$\wedge\big[\forall n, m\colon y = n \cdot m \Rightarrow (n = 1 \vee m = 1)\big] \wedge \big[\forall n, m\colon z = n \cdot m \Rightarrow (n = 1 \vee m = 1)\big]\big)$$

wobei alle Quantifikationen über die natürlichen Zahlen laufen. Oder mit anderen Worten: Jede gerade Zahl, die größer als 2 ist, ist Summe von zwei Primzahlen.

3. Mengen

Nun wo wir etwas sprechen gelernt haben, wenden wir uns als nächstes den Objekten zu, über die wir sprechen wollen:

3.1. Konvention (Cantor 1894) Eine *Menge (set)* M ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen.

Man nennt diese Objekte x die *Elemente (elements)* von M und schreibt $x \in M$. Wir nennen zwei Element $x, y \in M$ *gleich (equal)* und schreiben hierfür $x = y$, falls sich nicht unterscheidbar sind, und sonst $x \neq y$.

Man nennt N eine *Teilmenge (subset)* von M und schreibt $N \subseteq M$, falls jedes Element von N auch in M enthalten ist, in Formeln $\forall x\colon x \in N \Rightarrow x \in M$, quantifiziert über die Elemente von N.

Zwei Mengen M und N definieren wir als *gleich (equal)* und schreiben $M = N$, falls sie die gleichen Elemente enthalten, also falls $M \subseteq N$ und $N \subseteq M$.

Schlussendlich setzten wir noch

$$N \subsetneq M := N \subseteq M \wedge N \neq M$$

und sagen, dass N in diesem Fall eine *eigentliche (proper)* Teilmenge von M ist.

3.2. Bemerkung Als der deutsche Mathematiker Georg Cantor (1845-1918) diese Definitionen, zusammen mit dem Begriff der Mächtigkeit (den wir in ein paar wenigen Vorlesungen kennen lernen werden) einführte, kam dies einer Revolution gleich, da er es ermöglichte auch unendliche Menge endlich rigoros zu studieren ohne nur auf die Intuition zurückzugreifen; Cantor selbst wollte eigentlich Mengen reeller Zahlen studieren, auf denen bestimmte Reihen konvergieren und bedurfte hierfür einer neuen Sprache, die sich dann verselbstständigt hat. Der ebenfalls deutsche Mathematiker David Hilbert (1862-1943) sagte knapp 30 Jahre nach dem Erscheinen von Cantors Arbeit einmal:

"Fruchtbaren Begriffsbildungen und Schlußweisen wollen wir, wo immer nur die geringste Aussicht sich bietet, sorgfältig nachspüren und sie pflegen, stützen und gebrauchsfähig machen. Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können. Es ist nötig, durchweg dieselbe Sicherheit des Schließens herzustellen, wie sie in der gewöhnlichen niederen Zahlentheorie vorhanden ist, an der niemand zweifelt und wo Widersprüche und Paradoxien nur durch unsere Unaufmerksamkeit entstehen. Die Erreichung dieser Ziele ist offenbar nur möglich, wenn uns die volle Aufklärung über das Wesen des Unendlichen gelingt."

3.3. Beispiel (1) die Menge alle Kühe.
(2) die Menge aller Rechtshänder im Raum.
(3) die Mengen der natürlichen, ganzen, rationalen, reellen, p-adischen und komplexen Zahlen

Etwas ernsthafter: Eine Menge M nennen wir *leer (empty)* falls sie keine Elemente hat, also falls gilt

$$\forall x \colon x \notin \varnothing.$$

Wir beobachten sofort, dass wenn zwei Mengen M und N dieser Bedingung genügen, so gilt $M = N$. Oder mit anderen Worten es gibt nur eine leere Menge. Wir bezeichnen sie mit $\varnothing$.

3.4. Beispiel (1) Für jede Menge M gelten $\varnothing \subseteq M$ und $M \subseteq M$.
(2) Ist P ein Prädikat mit einer Variablen mit Definitionsbereich (die Elemente von) M, so kann man die Teilmenge

$$\{m \in M \mid P(m)\} \subseteq M$$

all derer Elemente $m \in M$ bilden, so dass $P(m)$ wahr ist. Andersherum ist für eine Teilmenge $N \subseteq M$ der Ausdruck $x \in N$ ein Prädikat mit Variable x und Definitionsbereich M.

Besteht der Definitionsbereich eines Prädikats P mit Variable m aus den Elementen einer Menge M so schreibt man in der Regel $\forall m \in M \colon P$ und $\exists m \in M \colon P$ bei der Quantifizierung.

(3) Ist $N \subseteq M$, so bezeichnet man die Teilmenge

$$M \backslash N := \{m \in M \mid m \notin N\}$$

als das *Komplement (complement)* von N in M.

(4) Möchte man gegebene Objekte zu einer Menge zusammenfassen benutzt man ebenfalls $\{\ \}$, etwa man bezeichnet für $x \in M$ die Teilmenge

$$\{m \in M \mid x = m\} \subseteq M$$

mit $\{x\}$. Ähnlich schreibt man $\{x, y\}$ für

$$\{m \in M \mid x = m \vee m = y\} \subseteq M$$

und so weiter. Es gilt insbesondere immer $\{x, y\} = \{y, x\}$, eine Reihenfolge oder ähnliches haben Mengen nicht. In der gesamten Diskussion ist durchaus zugelassen, dass $x = y$ gilt. In diesem Falle gelten auch $\{y\} = \{x, y\} = \{x\}$, sonst natürlich nicht.

(5) Es ist $\varnothing$ wohl zu unterscheiden von $\{\varnothing\}$. Die letztere Menge hat ein Element! Nämlich $\varnothing$. Die vordere nicht.
(6) Etwa gilt {natürliche Zahlen}\{gerade Zahlen} = {ungerade Zahlen}.

3.5. Definition Ist M eine Menge, so ist ihre *Potenzmenge (power set)* $\mathcal{P}(M)$ die Menge aller ihrer Teilmengen, also

$$\forall x\colon x \in \mathcal{P}(M) \Leftrightarrow x \subseteq M.$$

Ist $X \subseteq \mathcal{P}(M)$ eine Teilmenge, so definieren wir ihre *Vereinigung (union)* und *Durchschnitt (intersection)* als

$$\bigcup X := \{m \in M \mid \exists U \in X\colon m \in U\} \quad \text{and} \quad \bigcap X := \{m \in M \mid \forall U \in X\colon m \in U\}$$

Häufig schreibt man auch $\bigcup_{U\in X} U$ anstatt $\bigcup X$, was für so manches Gehirn etwas leichter zu parsen zu sein scheint. Wir werden das bestimmt öfter sehen. Definitiv benutzen werden wir

$$U \cup V := \bigcup\{U, V\} \quad \text{and} \quad U \cap V := \bigcap\{U, V\}$$

für zwei Teilmengen $U, V \subseteq M$. Zwei Teilmenge von M mit $U \cap V = \varnothing$ heißen *disjunkt (disjoint)*.

3.6. Beispiel (1) Es gelten

$$\mathcal{P}(\varnothing) = \{\varnothing\}$$
$$\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$$
$$\mathcal{P}(\{\varnothing, \{\varnothing\}\}) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$$

oder allgemeiner

$$\mathcal{P}(\{x\}) = \{\varnothing, \{x\}\} \quad \text{und} \quad \mathcal{P}(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$$

für je zwei Elemente $x, y \in M$.

(2) Es gelten

$$\{1, 2, 3\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\} \quad \text{und} \quad \{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}.$$

$$\bigcup\{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\} = \{1, 2, 3, 4, 5\} \quad \text{und} \quad \bigcap\{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\} = \{3\}.$$

Wieder gibt es eine Myriade Rechenregeln; hier eine Auswahl:

3.7. Satz *Für $U, V, W \subseteq M$ und $X, Y \subseteq \mathcal{P}(M)$ gelten:*

(1)

$$U \cup (M\backslash U) = M \quad \textit{und} \quad U \cap (M\backslash U) = \varnothing$$

(2)

$$M\backslash(U \cup V) = (M\backslash U) \cap (M\backslash V) \quad \textit{and} \quad M\backslash(U \cap V) = (M\backslash U) \cup (M\backslash V)$$

(3)

$$\bigcup\{U\} = U = \bigcap\{U\}$$

(4)

$$\bigcup \varnothing = \varnothing \quad \textit{und} \quad \bigcap \varnothing = M$$

(5)

$$\bigcup \mathcal{P}(M) = M \quad \textit{und} \quad \bigcap \mathcal{P}(M) = \varnothing$$

(6)

$$\bigcup X \cup \bigcup Y = \bigcup(X \cup Y) \quad \textit{und} \quad \bigcap X \cap \bigcap Y = \bigcap(X \cup Y)$$

insbesondere

$$(U \cup V) \cup W = U \cup (V \cup W) \quad \textit{und} \quad (U \cap V) \cap W = U \cap (V \cap W)$$

und

$$X \subseteq Y \Longrightarrow \bigcup X \subseteq \bigcup Y \quad \textit{und} \quad \bigcap Y \subseteq \bigcap X$$

und

(7)

$$\bigcap X \cup \bigcap Y = \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\}$$

und

$$\bigcup X \cap \bigcup Y = \bigcup\{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cap U'\}$$

insbesondere

$$(U \cup V) \cap W = (U \cap W) \cup (V \cap W) \quad \textit{und} \quad (U \cap V) \cup W = (U \cup W) \cap (V \cup W)$$

Beweis. Fangen wir mit der linken Aussage in (1) an: Für $U \cup (M\backslash U) \subseteq M$ müssen wir zeigen, dass $m \in U \vee m \in M\backslash U \Rightarrow m \in M$. Aber nach einer Übungsaufgabe ist das das gleiche wie zu zeigen, dass $m \in U \Rightarrow m \in M$ und $m \in M\backslash U \Rightarrow M$. Diese Aussage sind aber beide per definition (von U und $\backslash$) wahr. Für die umgekehrte Inlusion $M \subseteq U \cup M\backslash U$ müssen wir zeigen $m \in M \Rightarrow m \in U \vee m \in M\backslash U$. Aber wieder nach Übung können wir stattdessen, $m \in M \wedge m \notin U \Rightarrow m \in M\backslash U$ zeigen, was wieder nach Definition von $M\backslash U$ wahr ist.

Für die zweite Aussage $U \cap (M\backslash U) = \varnothing$ müssen wir zeigen, dass $U \cap (M\backslash U)$ leer ist. Mit anderen Worten, dass für alle $x \in M$ die Aussage $x \in U \wedge x \in M\backslash U$ falsch ist. Aber das is wieder nach Definition von $\backslash$ wahr, da tertium non datur.

Aussage (2) ist eine Übungsaufgabe werden.

Aussagen (3) sind direkt per Definition klar. Numero (4) ist amüsant: Die linke Gleichung folgt, da es per Definition für kein $x \in M$ eine Menge $U \in \varnothing$ gibt, mit $x \in U$: Es gibt ja einfach überhaupt kein $U \in \varnothing$, also ist $\bigcup \varnothing$ leer. Für die rechte stellen wir fest, dass aber für jedes $U \in \varnothing$ gilt $x \in U$, wieder weil es ja gar kein solches U gibt. Also ist $x \in \bigcap \varnothing$ und damit $M \subseteq \bigcap \varnothing$. Die andere Inklusion gilt per definitionem. Das Argument für (5) ist simpler: Für jedes $x \in M$ bezeugt $M \in \mathcal{P}(M)$, dass auch $x \in \bigcup \mathcal{P}(M)$, und $M\backslash\{x\} \in \mathcal{P}(M)$, dass $x \notin \bigcap \mathcal{P}(M)$.

Für Aussage (6) müssen wir zeigen, dass $x \in \bigcup X \vee x \in \bigcup Y$ genau dann gilt, wenn $x \in \bigcup X \cup Y$. Wir verwenden wie in (1) die Übungsaufgabe vom ersten Zettel, um für die Hinrichtung stattdessen $x \in \bigcup X \Rightarrow x \in \bigcup X \cup Y$ und $x \in \bigcup Y \Rightarrow x \in \bigcup X \cup Y$ zeigen zu dürfen. Aber das ist klar: Gibt es ein $U \in X$ mit $x \in U$, so gilt ja auch $U \in X \cup Y$, und analog für $U \in Y$. Für die Rückrichtung reicht es ebenfalls nach der Übungsaufgabe zu zeigen, dass $(\exists U \in X \cup Y \colon x \in U) \wedge \neg(\exists U \in Y \colon x \in U)$ impliziert, dass $x \in \bigcup X$. Aber auch das ist richtig: Die linke Seite der Konjunktion ist $(\exists U \in X \colon x \in U) \vee (\exists U \in X \colon x \in U)$, also die gesamte Konjunktion nach Distrubutivität und tertium non datur, sogar äquivalent zu $(\exists U \in X \colon x \in U)$, also in der Tat $x \in \bigcup X$.

Die linke der weiteren Behauptungen ergibt sich nun durch

$$(U \cup V) \cup W = \bigcup\{U, V\} \cup \bigcup\{W\} = \bigcup\{U, V, W\} = \bigcup\{U\} \cup \bigcup\{V, W\} = U \cup (V \cup W)$$

und die zweite durch

$$\bigcup X \subseteq \bigcup X \cup \bigcup(Y\backslash X) = \bigcup(Y \cup (Y\backslash X)) = \bigcup Y.$$

Die Behauptungen über Durchschnitte erhält man ähnlich.

Ich nutze den Beweis von der ersten Behauptung von (7) schlußendlich, um noch einmal einen Beweis soweit zu formalisieren, dass man ihn gerade noch lesen kann. Ein Beweis der für den menschlichen Konsum gedacht ist, folgt am Ende. Die zweite Behauptung nachzuweisen wird eine Übungsaufgabe.

Die Behauptung $\bigcap X \cup \bigcap Y \subseteq \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\}$ ist per Definition die Aussage:

$$(*) \qquad \forall x \in M \colon (x \in \bigcap X \cup \bigcap Y) \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\}).$$

Zuerst beobachten, dass nach Definition von $\cup$ gilt:

$$x \in \bigcap X \cup \bigcap Y \iff (x \in \bigcap X) \vee (x \in \bigcap Y)$$

Also ist $(*)$ nach Substitution in 1.10 äquivalent zu

$$\forall x \in M \colon [(x \in \bigcap X) \vee (x \in \bigcap Y)] \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\})$$

Aber nach dem ersten Übungszettel ist die äquivalent zu

$$\forall x \in M\colon [(x \in \bigcap X) \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$
$$\wedge [(x \in \bigcap Y) \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$

Und dies, und damit nach Transitivität auch $(*)$, ist nach 2.5 (2) wiederum zu

$$[\forall x \in M\colon (x \in \bigcap X) \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$
$$\wedge [\forall x \in M\colon (x \in \bigcap Y) \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$

äquivalent. Es reicht also diese beiden Aussagen als wahr nachzuweisen. Zeigen wir die erste, also

$$(**) \qquad \forall x \in M\colon (x \in \bigcap X) \Rightarrow (x \in \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})$$

die zweite ist völlig analog. Nach Einsetzen der Definitionen des Durchschnitts lautet $(**)$

$$\forall x \in M\colon [\forall U \in X\colon x \in U] \Rightarrow [\forall U \in X\colon \forall U' \in Y\colon x \in U \cup U']$$

Einsetzten der Definition von $\cup$ wird dies weiter zu

$$(***) \qquad \forall x \in M\colon [\forall U \in X\colon x \in U] \Rightarrow [\forall U \in X\colon \forall U' \in Y\colon (x \in U) \vee (x \in U')],$$

was wir nun als wahr nachweisen müssen. Aber sicherlich gilt

$$[\forall U \in X\colon x \in U] \Rightarrow [\forall U \in X\colon x \in U] \vee [\forall U' \in Y\colon x \in U']$$

($A \Rightarrow A \vee B$ ist sicherlich für je zwei Aussage A und B wahr: etwa ist es nach dem ersten Übungszettel äquivalent zu $A \wedge \neg A \Rightarrow B$ und $A \wedge \neg A$ ist falsch) und nach 2.5 (3) gilt auch

$$[\forall U \in X\colon x \in U] \vee [\forall U' \in Y\colon x \in U'] \Rightarrow [\forall U \in X\colon \forall U' \in Y\colon (x \in U) \vee (x \in U')],$$

sodass eine letzte Anwendung von Transitivität $(***)$ liefert. Damit haben wir

$$\bigcap X \cup \bigcap Y \subseteq \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\}$$

nachgewiesen.

Bleibt noch die andere Inklusion

$$(\times) \qquad \bigcap\{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\} \subseteq \bigcap X \cup \bigcap Y$$

zu zeigen. Dies lautet ausgeschrieben

$$\forall x \in M\colon [\forall U \in X\colon \forall U' \in Y\colon x \in U \vee x \in U'] \Longrightarrow [\forall U \in X\colon x \in U] \vee [\forall U' \in Y\colon x \in U']$$

Aber wieder nach dem ersten Übungszettel ist dies äquivalent zu

$$\forall x \in M\colon [\forall U \in X\colon \forall U' \in Y\colon x \in U \vee x \in U'] \wedge \neg[\forall U \in X\colon x \in U] \Longrightarrow [\forall U' \in Y\colon x \in U']$$

was nach 2.5 (1) (und natürlich Substitution aus 1.10) äquivalent ist zu

$$(\times\times) \qquad \forall x \in M\colon [\forall U \in X\colon \forall U' \in Y\colon x \in U \vee x \in U'] \wedge [\exists U \in X\colon x \notin U] \Longrightarrow [\forall U' \in Y\colon x \in U'],$$

was wir nun als wahr nachweisen müssen. Aber für je zwei Prädikate P und Q mit gleichem Definitionsbereich gilt:

$$(\forall x\colon P) \wedge (\exists x\colon Q) \Rightarrow (\exists x\colon P \wedge Q)$$

(zum einen ist das offensichtlich, zum andern gilt es auf dem zweiten Übungszettel einen symbolischen Beweis zu finden). Setzen wir dies ein erhalten wir

$$[\forall U \in X\colon (\forall U' \in Y\colon x \in U \vee x \in U')] \wedge [\exists U \in X\colon x \notin U]$$
$$\Longrightarrow \exists U \in X\colon \forall U' \in Y\colon x \notin U \wedge (x \in U \vee x \in U')$$

und es gilt

$$x \notin U \wedge (x \in U \vee x \in U') \Longleftrightarrow (x \notin U \wedge x \in U) \vee (x \notin U \wedge x \in U') \Longleftrightarrow (x \notin U \wedge x \in U') \Longrightarrow x \in U'$$

nach Distributivität aus 1.10, was nach Transivität durch Substitution $(\times\times)$ liefert. Uff.

Hier noch die menschenfreundlichere Art das gleiche in natürlicher Sprache zu formulieren (machen Sie sich klar, dass hier wirklich das gleiche passiert). Wir zeigen zuerst, dass die linke in der rechte Seite enthalten ist. Dafür gilt es also wieder zu zeigen, dass $\bigcap X$ und $\bigcap Y$ in der rechten

Seite liegen. Nehmen wir also etwa ein Element $x \in M$, mit $x \in U$ für alle $U \in X$. Dann gilt für jedes $U' \in Y$ sicherlich $x \in U \cup U'$, also ist x in der rechten Seite enthalten. Analog für $x \in V \in Y$. Für die umgekehrte Inklusion benutzen wir wieder die Umformulierung den Übungszettels und müssen zeigen, dass ein $x \in M$, mit $x \in U \cup U'$ für alle $U \in X$ und $U' \in Y$, das aber nicht in $\bigcap X$ liegt, in $\bigcap Y$ liegen muss. Aber nicht in $\bigcap X$ zu liegen, bedeutet dass es ein $U \in X$ gibt, so dass $x \notin U$. Da aber per Annahme $x \in U \cup U'$ für alle $U' \in Y$ gilt, muss also $x \in U'$ liegen.

Ich hoffe der Kontrast in der Länge macht deutlich, wie dicht mathematische Texte meist geschrieben sind. Auch hier: Gewöhnen Sie sich lieber schnell daran, es wird nicht besser. □

Zuletzt noch eine nützliche Abkürzung, die vieles einfach macht, und eine Anmerkung, die vieles komplizierter macht:

3.8. Definition Ist P ein einstelliges Prädikat mit Variable x und Definitionsbereich M, M eine Menge, so setzen wir

$$\exists! x \in M \colon P \coloneqq (\exists m \in M \colon P(m)) \wedge (\forall m, m' \in M \colon (P(m) \wedge P(m')) \Rightarrow m = m').$$

Gelesen wird $\exists!$ als "es existiert genau ein".

3.9. Bemerkung Man mag nun auf die furchtbare Idee kommen, in allem Überschwung diejenige Menge S zu bilden, deren Elemente genau alle Mengen sind. Dann kann man beobachten, dass $S \in S$ gilt. Überrascht, mag man dann noch versuchen die Teilmenge

$$T \coloneqq \{M \in S \mid M \notin M\}$$

zu betrachten und sich dann zu fragen, ob $T \in T$. Jetzt explodiert aber alles: Ist nämlich $T \in T$, so gilt nach Definition $T \notin T$. Und gilt aber $T \notin T$, so doch per definition doch $T \in T$. Dieses Paradox heißt die Russel'sche Antinomie und zeigt, dass es die Menge S nicht geben kann (Cantor's Paradies hat also doch seine Grenzen).

Um solchen Problemen vorzubeugen, fasst man Mengen heutzutage formal nicht mehr durch Cantor's (doch recht vage) Konvention 3.1, sondern rein axiomatisch. Eine genau Diskussion würde uns hier zu viel Zeit und Platz kosten; das Stichwort zum Weiterlesen sind die Zermelo-Fraenkel-Axiome. Für uns ist der Schluss erstmal, dass man nur die Konstruktionen durchführen sollte, die in diesem Kapitel angegeben sind, und keine solch wilden Experimente wie S.

4. Ordnungsrelationen

4.1. Definition Das *kartesische Produkt (cartesian product)* $M \times N$ zweier Mengen M und N ist die Menge der Paare (x, y) mit $x \in M$ und $y \in N$. Die Gleichheit von Paaren wiederum ist so definiert, dass

$$\forall x, x' \in M, y, y' \in N \colon (x, y) = (x', y') \Leftrightarrow (x = x') \wedge (y = y').$$

Benannt ist das kartesische Produkt nach dem französischen Mathematiker René Descartes (1596 - 1650) der zuerst die heute ebenfalls als kartesisch bekannten Koordinaten einführte um Punkte in der Ebene zu lokalisieren (in der Notation oben, die Ebene also als $\mathbb{R} \times \mathbb{R}$ identifizierte). Falsch geschrieben als Adjektiv im mathematischen Sprachgebrauch zu erscheinen ist in gewissen Weise wohl die höchste Ehre, die einem Mathematiker zu Teil werden kann. Von Descartes stammt auch der berühmte Ausspruch "Cogito, ergo sum!" (Ich denke, also bin ich.), der ein wunderbares Beispiel ist, dass die bei Anfänger (und leider auch in der wirklich wahren Welt) beliebte Variante $(A \Rightarrow B) \Rightarrow (B \Rightarrow A)$ des Umkehrschlusses wirklich Murks ist. Es scheint zumindest immer häufiger, dass nicht jeder, der ist, auch wirklich denkt.

4.2. Beispiel

(1) Gilt $M = \{x, y\}$, so gilt

$$M \times M = \{(x, x), (x, y), (y, x), (y, y)\}.$$

(2) Es gelten $M \times \varnothing = \varnothing = \varnothing \times M$.

4.3. Definition Eine *Relation (relation)* R zwischen zwei Mengen M und N (oder besser "zwischen den Elementen zweier Mengen M und N", aber das ist so lang) ist eine Teilmenge $R \subseteq M \times N$.

Man stelle sich hierbei R als die Menge derer Paare von Elementen zu die in der gegebenen Beziehung zu einander stehen. Folglich schreibt man häufig auch mRn anstatt $(m,n) \in R$. Gilt $M = N$ so spricht man meist von einer Relation auf M.

4.4. Beispiel (1) Die Gleichheitsrelation

$$\Delta_M = \{(m,m') \in M \mid m = m'\}$$

existiert auf jeder Menge M, ebenso wie

$$M \times M \backslash \Delta_M,$$

die Ungleichheit.

(2) Die trivialen Relationen

$$M \times N \subseteq M \times N \quad \text{and} \quad \varnothing \subseteq M \times N$$

für je zwei Mengen M und N.

(3) Größenvergleich $\geqslant$ und Teilbarkeit $|$ sind zwei Relationen auf den natürlichen Zahlen.

(4) Auf $\mathcal{P}(M)$ haben wir die Teilmengenrelation

$$\{(X,Y) \in \mathcal{P}(M) \mid X \subseteq Y\}.$$

Relationen kommen in verschiedensten Spielrichtungen. Wir werden in dieser under nächsten Vorlesung drei von ihnen genauer anschauen: Ordnungsrelationen, Funktionen und Äquivalenzrelationen.

4.5. Definition Eine Relation R auf einer Menge M heißt

(1) *reflexiv*, falls für alle $m \in M$ gilt mRm gilt,
(2) *transitiv*, falls für alle $m,n,k \in M$ gilt $(mRn \wedge nRk) \Rightarrow mRk$,
(3) *identitiv*, falls für alle $m,n \in M$ gilt $(mRn \wedge nRm) \Rightarrow n = m$,
(4) *total*, falls für alle $m,n \in M$ gilt $mRn \vee nRm$.

Eine Relation, die reflexiv, transitiv und identitiv ist heißt eine *partielle Ordnung (partial order)*. Ist sie zusätzlich total, so spricht man von einer *totalen Ordnung (total order)*.

Selten sich Autoren einig welches dieser Konzepte der Begriff "Ordnung" oder entweder "partiell" oder "total" davor bezeichnet. Ich werde daher versuchen ihn alleine zu vermeiden. Das Paar (M,R) wird zusammen übrigends häufig als *partiell/total geordnete Menge (partially/totally ordered set)* bezeichnet, wobei sich im englischen der Begriff *poset* für den ersten Fall durchgesetzt hat.

4.6. Beispiel (1) Die Teilmengenrelation auf $\mathcal{P}(M)$ ist für jede Menge M eine partielle Ordnung. Total ist sie genau auf $M = \varnothing$ und Mengen der Form $M = \{x\}$: Sobald es $x,y \in M$ gibt, mit $x \neq y$, gilt weder

$$\{x\} \subseteq \{y\} \quad \text{noch} \quad \{y\} \subseteq \{x\}.$$

(2) Ähnliches gilt typischer, wenn man eine Ansammlung Mitarbeiter nach dem Vorgesetztsein ordnet: Dies ist eine partielle, aber nur in etwas seltsamen Firmen eine totale Ordnung.

(3) Die Gleichheitsrelation ist eine (sehr sehr) partielle Ordnung, die nicht total ist sobald M zwei verschiedene Elemente hat.

(4) Die leere Relation $\varnothing$ ist nur auf der leeren Menge eine partielle Ordnung (sonst ist sie nicht reflexiv), und die volle Relation $M \times M$ ist nur eine partielle Ordnung falls $M = \varnothing$ oder $M = \{x\}$ (sonst ist sie nicht identitiv).

(5) Die Ordnung nach der Größe ist eine totale Ordnung auf den natürlichen, ganzen, rationalen und auch reellen Zahlen (visualisiert im üblichen Zahlenstrahl).

(6) Teilbarkeit ist eine weitere partielle, aber nicht totale Ordnung auf den natürlichen Zahlen (es gilt schließlich weder 2 die 3 noch 3 die 2).

(7) Ist N eine Teilmenge von M und R eine partielle bzw. totale Ordnung auf M, so ist $R \cap N \times N$ wieder eine partielle bzw. totale Ordnung auf N. Man spricht von der auf N *eingeschränkten Ordnung (restricted order)*. Es kann passieren, dass diese total ist, obwohl R es auf ganz M nicht ist. In diesem Falle nennt man N eine *Kette (chain)* von M.
(8) Ist R eine partielle Ordnung auf M, so auch $R^{\text{rev}} = \{(m, m') \in M \times M \mid (m', m) \in R\}$. Eine Ordnungsrelation weiß also nicht intrinsisch, ob nun die rechte oder die linke Seite "größer" ist. Weitere Begriffe werden wir aber immer so festlegen, als wäre in n das "größere" Element falls mRn.

4.7. Definition Sei R eine partielle Ordnung auf M und $m \in M$. Das Element m heißt ein *größtes/kleinstes (largest/smallest)* Element von M, falls für alle $m' \in M$ gilt $m'Rm$ bzw. mRm', und *maximal/minimal*, falls für alle $m' \in M$ gilt $mRm' \Rightarrow m = m'$ bzw. $m'Rm \Rightarrow m' = m$.

Oft erweitert man diese Definition noch zu einer relativen Version: Ist $N \subseteq M$, so heißt m *obere/untere Schranke (upper/lower bound)* für N falls für alle $n \in N$ gilt nRm bzw. mRn gilt. Beachte, dass hierbei m kein Element von N sein muss.

4.8. Beobachtung Ist M von R partiell geordnet, so gilt:

(1) M hat höchstens ein größtes Element (also sind $x, y \in M$ größt, so folgt $x = y$).
(2) Jedes größte Element von M ist auch maximal.
(3) Besitzt M ein größtes Element, so ist jedes maximale Element von M auch größt.
(4) Ist M durch R total geordnet, so ist ebenfalls jedes maximale Element von M auch größt.

In Abwesenheit eines größten Elements, kann es in einer nur partiell geordneten Menge aber viele maximale Elemente geben, wie wir im nächsten Beispiel sehen werden.

Beweis. Die ersten beiden Aussagen folgen direkt aus der Identivität: Sind x und y beide größt, so gilt xRy weil y größt ist, und yRx weil x größt ist. Ergo $x = y$, also (1). Und für (2), ist x größt, und xRy, so gilt weil ja auch yRx gilt, wieder $x = y$. Für Aussage (3) sei $x \in M$ größt, und $y \in M$ maximal. Dann gilt wegen dem ersten yRx und damit dann wegen dem zweiten $x = y$, insbesondere ist y also auch größt. Für Aussage (4) sei $x \in M$ maximal. Dann muss wegen Totalität für alle $y \in M$ mindestens eins von xRy und yRx gelten. Aber xRy gilt nur für $y = x$, und in diesem Fall gilt auch yRx wegen Reflexivität. In allen anderen Fällen muss dann aber yRx gelten. □

4.9. Beispiel (1) M ist das größte Element von $\mathcal{P}(M)$ und $\varnothing$ das kleinste.
(2) In $\mathcal{P}(M)\backslash\{M\}$ ist für jedes $x \in M$ das Element $M\backslash\{x\} \in \mathcal{P}(M)\backslash\{M\}$ maximal, aber sobald M zwei verschiedene Elemente erhält nicht größt: Falls $x \neq y$ gilt weder $M\backslash\{x\} \subseteq M\backslash\{y\}$ noch $M\backslash\{y\} \subseteq M\backslash\{x\}$.
(3) Jede Teilmenge der natürlichen Zahlen besitzt unter Größenvergleich ein kleinstes Element. Die natürlichen Zahlen besitzen aber kein maximales, erst recht kein größtes Element.
(4) Betrachten wir die natürlichen Zahlen mit der Teilbarkeitsrelation so ist 1 die kleinste natürliche Zahl und 0 die größte. In der Teilmenge $\{\text{natürliche Zahlen}\}\backslash\{0, 1\}$ sind genau die Primzahlen die minimalen Elemente und es gibt keine maximalen (erst recht keine größten) Elemente. Die maximalen Elemente von $\{2, 3, 4, 5, 6\}$ sind 4, 5 und 6, insbesondere gibt es kein größtes Element.

Hier schon einmal formulieren möchte ich einen hochgradig nicht-trivialen Satz, mit dem wir uns wahrscheinlich später noch beschäftigen müssen.

4.10. Theorem (Zorn'sches Lemma, 1933) *Besitzt jede Kette einer partiell geordneten, nichtleeren Menge M eine obere Schranke, so besitzt M ein maximales Element.*

Spielen sie etwas mit dieser Aussage um sich zu überzeugen, dass sie nicht offensichtlich ist. Es ist irgendwie beeindruckend, was man mit so wenigen Begriffen, wie wir sie nun erst haben, schon an Komplexität erreichen kann. Unabhängig vom Amerikaner Max Zorn (1906 - 1993) bewies übrigends der Pole Kazimierz Kuratowski (1896 - 1980) diesen Satz schon 1922, aber der Namen zeugt davon, dass dies lange in der westlichen Welt nicht allgemein bekannt war.

5. Funktionen

Wir kommen zur zweiten Sorte Relationen, die wir genauer betrachten wollen:

5.1. Definition Eine Relation $R \subseteq M \times N$ heißt *Funktion* oder *Abbildung (function/map)* falls gilt:

$$\forall m \in M \exists! n \in N \colon mRn.$$

Man notiert R in diesem Falle auch also $R \colon M \to N$, und schreibt $R(m) = n$ anstatt mRn (n ist per definitionem ja eindeutig bestimmt. Die Menge M heißt die *Quelle (source)* von R und N das *Ziel (target)* von R.

Eine weiter Eigenheit der Sprache ist es, dass man häufig sagt, man beweist, dass eine Funktion *wohldefiniert (well-defined)* ist, anstatt zu sagen, dass man beweist, dass eine Relation eine Funktion ist. Auch das ist der Historie geschuldet. Wir bezeichnen mit

$$\mathrm{F}(M,N) := \{R \subseteq M \times N \mid R \text{ ist eine Funktion } M \to N\}$$

die Menge der Funktionen $M \to N$.

Man stelle sich eine Funktion immer so vor, dass sie jedem Element der Quelle genau ein Element des Ziels zuordnet und schreibt daher auch $m \mapsto R(m)$; man beachte die Unterschied zwischen dem Pfeil $\to$ in der Deklaration einer Funktion, und dem Pfeil $\mapsto$ hier. Diese Zuordnung muss aber erstmal in keinster Weise durch eine irgendwie geartete aufschreibbare Vorschrift erfolgen.

5.2. Bemerkung Wir beobachten direkt, dass für zwei Funktionen $f, g \colon M \to N$ gilt, dass $f = g$ genau dann, wenn $f(m) = g(m)$ für alle $m \in M$: Die rechte Seite besagt ja ausgeschrieben nichts anderes als $f(m) = n$ genau dann, wenn $g(m) = n$ für alle $m \in M$ und $n \in N$, und das übersetzt sich zu $(m,n) \in f \Leftrightarrow (m,n) \in g$, sodass die Gleichheitsdefinition für Mengen zuschlägt.

Ebenso gilt, dass $f \subseteq g \Rightarrow f = g$ für zwei Funktionen $f, g \colon M \to N$: Um $g \subseteq f$ zu zeigen, sei $(m,n) \in g$. Dann gibt es nach Existenzteil der Wohldefiniertheit von f ein $n \in N$ mit $(m,n') \in f$, und damit auch $(m,n') \in g$. Wegen des Eindeutigkeitsteils der Wohldefiniertheit von g gilt dann aber $n = n'$ und somit $(m,n) \in f$, was zu zeigen war.

5.3. Beispiel

(1) Die Gleichheitsrelation $\Delta_M \subseteq M \times M$ ist eine Funktion. In diesem Gewand bezeichnet man sie meist mit id_M, die *Identität (identity)* auf M. In Zeichen:

$$\mathrm{id}_M \colon M \longrightarrow M, \quad m \longmapsto m.$$

(2) Gegeben $x \in N$, so definiert

$$\{(m,n) \in M \times N \mid n = x\}$$

eine Funktion, die *konstante Funktion (constant function)* const_x mit Wert X. In Zeichen:

$$\mathrm{const}_x^M \colon M \longrightarrow N, \quad m \longmapsto x.$$

Achtung: Meist lässt man den Index M aus der Notation und schreibt nur const_x. Es gibt also durchaus viele Funktionen, die auch den Namen const_x hören.

(3) Für $x \in M$ definiert

$$\{(m,n) \in M \times N \mid m = x\}$$

hingegen nur dann eine Funktion, wenn $M = \{x\}$ und $N = \{y\}$ für ein $y \in N$.

(4) Ist M durch R partiell geordnet, so setzen (nur für die Dauer dieses Beispiels)

$$K(M,R) = \{N \subseteq M \mid N \text{ hat ein kleinstes Element bzgl. } R\}$$

Dann definiert

$$\{(N,m) \in K(M,R) \times M \mid m \text{ ist kleinstes Element von } N \text{ bzgl. } R\}$$

wegen Beobachtung 4.8 die Minimumsfunktion, in Zeichen

$$\min\colon K(M,R) \longrightarrow M, \quad N \longmapsto \min(N).$$

Ähnliches gilt für die Maximumsfunktion.

Dass sich die Bezeichnung "Minimumsfunktion" durchgesetzt hat, obwohl sie doch kleinste Element auswählt, ist nicht auf meinem Mist gewachsen.

(5) Ist $f\colon M \to N$ eine Funktion, so können wir zwei neue Funktionen

$$\mathrm{Im}_f\colon \mathcal{P}(M) \to \mathcal{P}(N) \quad \text{und} \quad \mathrm{Pre}_f\colon \mathcal{P}(N) \to \mathcal{P}(M)$$

definieren durch

$$U \longmapsto \{n \in N \mid \exists u \in U\colon f(u) = n\} \quad \text{und} \quad V \longmapsto \{m \in m \mid f(m) \in V\}$$

Sie heißen die *Bild- (image)* und *Urbildfunktion (preimage)* von f. Generell bezeichnet man auch

$$\mathrm{Im}(f) \coloneqq \mathrm{Im}_f(M) = \{n \in N \mid \exists m \in M\colon f(m) = n\}$$

als das Bild von f.

(6) Für $M = A \cup B$ mit $A \cap B = \varnothing$ und Funktionen $f\colon A \to N$ und $g\colon B \to N$ ist auch $h \coloneqq f \cup g \subseteq M \times N$ eine Funktion ist. Man schreibt sie als häufig als

$$h\colon M \longrightarrow N, \quad m \longmapsto \begin{cases} f(m) & m \in A \\ g(m) & m \in B \end{cases},$$

und spricht davon dass h stückweise definiert ist.

Etwa können wir so durch $\mathrm{const}^A_n \cup \mathrm{const}^B_{n'}$ eine Funktion definieren, die nicht mehr ganz konstant ist (zumindest wenn $n \neq n'$).

Allgemeiner kann man Funktionen stückweise auf einer Partition von M im Sinne der Definition 6.6 unten definieren.

Interessantere Funktionen, wie Addition, Multiplikation, Exponentiation auf den natürlichen Zahlen, Sinus, Kosinus und Polynome auf den reellen Zahlen und vieles mehr sind Beispiele, die wir uns in den Anfängervorlesungen nun Stück für Stück nähern wollen.

5.4. Definition Sind $R \subseteq M \times N$ und $S \subseteq N \times P$ Relationen, so setzen wir

$$S \circ R = \{(m,p) \in M \times P \mid \exists n \in N\colon mRn \wedge nSp\},$$

die *Komposition (composition)* von R mit S.

5.5. Lemma *Sind $R \subseteq M \times N$ und $S \subseteq N \times P$ Funktionen, so auch $S \circ R$. Desweiteren gelten für und $p \in P$*

$$S \circ \mathrm{id}_N = S \quad \textit{und} \quad \mathrm{id}_N \circ R = R$$

und

$$S \circ \mathrm{const}_n = \mathrm{const}_{S(n)} \quad \textit{und} \quad \mathrm{const}_p \circ R = \mathrm{const}_p.$$

Wenn man das auseinander schraubt gilt also per definitionem $(S \circ R)(m) = S(R(m))$. Und Achtung: In der letzten Gleichung des Lemmas bezeichnen die beiden const_p's verschiedene Abbildungen: Die linke hat Quelle N, die rechte Quelle M. Es scheint vielen (inklusive mir) so zu gehen, dass die Komposition $S \circ R$ irgendwie "falschherum" erscheint (man liest es gern als "erst S, dann R"), aber die Kovention, dass $S \circ R$ in Wahrheit "S nach R" bedeutet, liegt zu tief, als dass wir daran etwas ändern könnten. Der Grund ist wieder historisch: Man schreibt eben $f(x)$ und nicht $x(f)$ für den Wert einer Funktion f auf einem Element x und das erzwingt diese Konvention.

BEWEIS. Das ist eine Übungsaufgabe auf dem drittel Zettel. □

5.6. Bemerkung Transitivität einer Relation R bedeutet genau $R \circ R \subseteq R$.

5.7. Beobachtung Sind $f\colon M \to N, g\colon N \to T$ und $h\colon T \to S$ Abbildungen so gilt $h \circ (g \circ f) = (h \circ g) \circ f$. Wir rechnen nämlich

$$[h \circ (g \circ f)](m) = h((g \circ f)(m)) = h(g(f(m))) = (h \circ g)(f(m)) = [(h \circ g) \circ f](m)$$

für jedes $m \in M$. Wie zuvor können wir beim Komponieren also die Klammern weglassen.

5.8. Definition Eine Funktion $f\colon M \to N$ heißt *umkehrbar (invertible)* falls es eine Funktion $g\colon N \to M$ gibt, so dass

$$f \circ g = \mathrm{id}_N \quad \text{und} \quad g \circ f = \mathrm{id}_M.$$

5.9. Satz *Eine Abbildung $f\colon M \to N$ ist umkehrbar genau dann, wenn sie*

(1) injektiv, *das heißt* $\forall m, m' \in M\colon f(m) = f(m') \Rightarrow m = m'$, *und*
(2) surjektiv, *das heißt* $\forall n \in N \exists m \in M\colon f(m) = n$

ist. In diesem Fall nennt man sie auch bijektiv *und ein g, dass die Umkehrbarkeit von f bezeugt ist eindeutig bestimmt. Es heißt die* Umkehrfunktion (inverse function) *von f, und wird mit f^{-1} bezeichnet.*

Eine andere Art Bijektivität auszudrücken ist, dass für alle $n \in N$ ein $m \in M$ existiert, so dass $\mathrm{Pre}_f(\{n\}) = \{m\}$. Direkt aus der Definition folgt auch, dass für invertierbares f auch f^{-1} invertierbar ist mit $(f^{-1})^{-1} = f$.

BEWEIS. Wir zeigen zunächst einmal, dass f bijektiv wirklich f umkehrbar impliziert. Ist f bijektiv, dann ist nämlich $f^{\mathrm{rev}} \subseteq N \times M$ ebenfalls eine Funktion, diesmal aber $N \to M$: Sei nämlich $n \in N$. Dann gibt es wegen Surjektivität ein $m \in n$ mit $f(m) = n$, also formal $(m, n) \in f$, und damit $(n, m) \in f^{\mathrm{rev}}$. Dies zeigt den Existenzteil der Wohldefiniertheit. Für den Eindeutigkeitsteil seien andererseits $(n, m) \in f^{\mathrm{rev}}$ und $(n, m') \in f^{\mathrm{rev}}$. Dann folgt $(m, n) \in f$ und $(m', n) \in f$, mit anderen Worten $f(m) = n = f(m')$, was wegen der Injektivität von f, wie gewünscht $m = m'$ impliziert.

Wir behaupten weiter, dass f^{rev} eine Umkehrfunktion von f ist: Um $f^{\mathrm{rev}} \circ f = \mathrm{id}_M$ nachzuweisen, benutzen wir das zweite Kriterium aus 5.2 und zeigen $\Delta_M \subseteq f^{\mathrm{rev}} \circ f$. Aber zu $(m, m) \in \Delta_M$ gilt $(m, f(m)) \in f$ und $(f(m), m) \in f^{\mathrm{rev}}$, was zeigt, dass $(m, m) \in f^{\mathrm{rev}} \circ f$. Um auch $f \circ f^{\mathrm{rev}} = \mathrm{id}_N$ analog einzusehen, beobachten wir, dass es für jedes $n \in N$ ein $m \in M$ gibt mit $f(m) = n$. Mit anderen Worten es gelten dann $(n, m) \in f^{\mathrm{rev}}$ und $(m, n) \in f$, was $(n, n) \in f \circ f^{\mathrm{rev}}$ zeigt.

Die restlichen Behauptungen der Proposition sind Spezialfälle der beiden folgenden Lemmata. □

5.10. Lemma *Seien $f\colon M \to N$ und $g\colon N \to T$ Abbildungen. Dann gilt*

(1) Sind f und g injektiv bzw. surjektiv, so ist auch $g \circ f$ injektiv bzw. surjektiv.
(2) Ist $g \circ f$ injektiv, so ist auch f injektiv.
(3) Ist $g \circ f$ surjektiv, so ist auch g surjektiv.

PROOF. Das ist eine Übungsaufgabe auf dem dritten Zettel. □

5.11. Lemma *Sind $f\colon M \to N$ und $g, h\colon N \to M$ Abbildungen mit $g \circ f = \mathrm{id}_M$ und $f \circ h = \mathrm{id}_N$. Dann folgt $g = h$.*

PROOF. Es gilt

$$h = \mathrm{id}_M \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \mathrm{id}_N = g.$$

□

5.12. Beispiel Um ein illustratives Beispiel zu haben greifen wir etwas vor und schauen uns die Quadratur q mit $x \mapsto x^2$ auf verschiedenen Zahlmengen an:

(1) als Abbildung $q\colon \{\text{natürliche Zahlen}\} \to \{\text{natürliche Zahlen}\}$ ist sie injektiv, aber nicht surjektiv,
(2) als Abbildung $\{\text{ganze Zahlen}\} \to \{\text{ganze Zahlen}\}$ ist sie weder injektiv noch surjektiv,
(3) ebenso als Abbildung $\{\text{rationale Zahlen}\} \to \{\text{rationale Zahlen}\}$,
(4) und auch als Abbildung $\{\text{reelle Zahlen}\} \to \{\text{reelle Zahlen}\}$, aber
(5) als Abbildung $\{\text{positive reelle Zahlen}\} \to \{\text{positive reelle Zahlen}\}$ ist sie sogar bijektiv; eine Umkehrabbildung ist genau durch das Ziehen von zweiten Wurzeln gegeben,
(6) als Abbildung $\{\text{komplexe Zahlen}\} \to \{\text{komplexe Zahlen}\}$ ist sie schließlich surjektiv, aber nicht injektiv.

Wir charakterisieren nun noch Abbildungen die nur injektiv oder surjektiv sind:

5.13. Satz *Sei $f\colon M \to N$ eine Abbildung. Dann sind äquivalent:*

(1) f ist injektiv.
(2) Für alle Abbildungen $g, g'\colon T \to M$ gilt $f \circ g = f \circ g' \Rightarrow g = g'$.
(3) Für alle Abbildungen $g, g'\colon M \to M$ gilt $f \circ g = f \circ g' \Rightarrow g = g'$.

Diese Aussagen werden impliziert von

(4) Es gibt eine Abbildung $h\colon N \to M$ mit $h \circ f = \mathrm{id}_M$.

und gilt $M \neq \varnothing$, so ist die vierte ebenfalls äquivalent zu den anderen.

Proof. Wir zeigen zunächst (1) ⇒ (2): Per Annahme gilt für alle $m \in M$, dass $f(g(t)) = f(g'(t))$, also wegen Injektivität von f auch $g(t) = g'(t)$ also nach dem Kriterium oben $g = g'$. (2) ⇒ (3) ist klar: Das dritte ist ja der Spezialfall $T = M$ des zweiten. Alsdann beweisen wir (3) ⇒ (1) per Umkehrschluss. Nehmen wir also an, dass $f(m) = f(m')$ gilt mit $m \neq m'$. Dann definieren wir eine Funktion

$$s\colon M \longrightarrow M, \quad x \longmapsto \begin{cases} m & x = m' \\ m' & x = m \\ x & \text{sonst} \end{cases}$$

Es gilt dann $f \circ s = f = f \circ \mathrm{id}_M$, aber $s \neq \mathrm{id}_M$. Per Transitivität folgt nun, dass (1), (2) und (3) wirklich äquivalent sind (man nennt das einen Ringschluss). Als nächstes beweisen wir (4) ⇒ (1): Gilt nämlich $f(m) = f(m')$ für $m, m' \in M$, so folgt

$$m = \mathrm{id}_M(m) = (h \circ f)(m) = h(f(m)) = h(f(m')) = (h \circ f)(m') = \mathrm{id}_M(m') = m'$$

wie gewünscht.

Zuletzt bleibt (1) ⇒ (4) im Falle, dass $M \neq \varnothing$. Hierzu beobachten wir zunächst, dass f sich zu einer Abbildung $f'\colon M \to \mathrm{Im}(f)$ einschränkt, was nicht anderes bedeutet als dass $f \subseteq M \times \mathrm{Im}(f)$ gilt, und auch so aufgefasst immer noch die Wohldefiniertheitseigenschaft erfüllt. Aber per definitionem ist f' nun surjektiv, und sicherlich immer noch injektiv. Also hat f nach dem (schon bewiesenen Teil von) Proposition 5.9 eine Umkehrfunktion $h'\colon \mathrm{Im}(f) \to M$. Schnappen wir uns nun ein $x \in M$ (M ist ja nicht leer!), so können wir definieren

$$h\colon N \longrightarrow M, \quad n \longmapsto \begin{cases} h'(n) & n \in \mathrm{Im}(f) \\ x & \text{sonst} \end{cases}$$

Dieses h erfüllt dann offensichtlich das gewünschte: Für $m \in M$ gilt

$$(h \circ f)(m) = h(f(m)) = h'(f(m)) = m$$

per Konstruktion. □

5.14. Satz *Sei $f\colon M \to N$ eine Abbildung. Dann sind äquivalent:*

(1) f ist surjektiv.
(2) Für alle Abbildungen $g, g'\colon N \to T$ gilt $g \circ f = g' \circ f \Rightarrow g = g'$.
(3) Es gibt eine Abbildung $h\colon N \to M$ mit $f \circ h = \mathrm{id}_N$.

Diese implizieren

(4) Für alle Abbildungen $g, g' \colon N \to N$ gilt $g \circ f = g' \circ f \Rightarrow g = g'$.
und falls $M \neq \varnothing$ sind sie auch äquivalent zur vierten.

PROOF. Wieder fangen wir mit (1) $\Rightarrow$ (2) an: Ist $n \in N$, so gibt es per Annahme ein $m \in M$ mit $f(m) = n$. Damit rechnen wir

$$g(n) = g(f(m)) = (g \circ f)(m) = (g' \circ f)(m) = g'(f(m)) = g'(n)$$

und damit $g = g'$. (2) $\Rightarrow$ (4) ist wieder trivial, ebenso (2) $\Rightarrow$ (1) falls $M = \varnothing$. (4) $\Rightarrow$ (1) falls $M \neq \varnothing$, zeigen wir wieder per Umkehrschluss. Nehmen wir also an f ist nicht surjektiv, etwa weil $x \in N \backslash \mathrm{Im}(f)$. Weil $M \neq \varnothing$ folgt $\mathrm{Im}(f) \neq \varnothing$. Sei also $y \in \mathrm{Im}(f)$, sodass insbesondere $x \neq y$. Wir betrachten dann die Abbildung

$$s \colon N \longrightarrow N, \quad n \longmapsto \begin{cases} y & n = x \\ n & \text{sonst} \end{cases}$$

Es gilt dann $s \circ f = f = \mathrm{id}_N \circ f$, aber $s \neq \mathrm{id}_N$.

Alsdann zeigen wir noch (3) $\Rightarrow$ (1): Für $n \in N$ gilt

$$n = \mathrm{id}_N(n) = (f \circ h)(n) = f(h(n))$$

was zeigt, dass man $h(n)$ als Urbild von n wählen kann, ergo ist f surjektiv. Zuletzt kommen wir zu (1) $\Rightarrow$ (3): Hier wähle man zu jedem $n \in N$ ein $m \in M$ mit $f(m) = n$ und konstruiere die gesuchte Abbildung h, indem man n auf solch ein m schicke... □

Der letzte Punkt des vorigen Beweises ist, wie Sie hoffentlich merken, sehr vage. Dies hat einen guten Grund: Die Aussage lässt sich mit den bisher etablierten Mitteln nicht nachweisen, sie ist eine Grundwahrheit, ähnlich der Existenz von Potenzmengen oder kartesischer Produkte. Die grundlegende Aussage ist formalisiert im folgenden Satz; in obigen Beweis wendet man ihn auf

$$g = \mathrm{Pre}_f \circ \{-\} \colon N \longrightarrow \mathcal{P}(M), \quad n \longmapsto \mathrm{Pre}_f(\{n\})$$

an.

5.15. Fakt (Auswahlprinzip (axiom of choice)) Gegeben sei eine Abbildung $g \colon N \to \mathcal{P}(M)$, so dass $g(n) \neq \varnothing$ für jedes $n \in N$. Dann existiert eine Abbildung $h \colon N \to M$ mit $h(n) \in g(n)$ für alle $n \in N$.

So ein h heißt eine *Auswahlfunktion (choice function)* für g. Um sich die Problematik klarer zu machen, stelle man sich einen großen Schrank mit Schubladen vor (besonders gut ist es, sich einen unendlichen Schrank vorzustellen, aber das ist vielleicht etwas schwer) mit einem Paar Socken in jeder Schublade. Ist dann M die Menge der Schubladen und N die Menge der Socken, so gibt es eine offensichtliche Funktion $M \to \mathcal{P}(N)$, die jeder Schublade ihren Inhalt (also eine zweielementige Menge von Socken) zuordnet. Eine Auswahlfunktion sucht nun in jeder Schublade einen Socken aus. Mit Schuhen anstatt Socken wäre es einfach so eine Funktion anzugeben: Man nehme immer den linken Schuh. Da sich die beiden Socken eines Paares aber nicht unterscheiden (oder wir das zumindest für unser Gedankenexperiment einmal annehmen wollen), gibt es keine Möglichkeit eine Auswahlfunktion irgendwie wirklich zu *konstruieren*. Trotzdem sind wir es hoffentlich alle hinreichend gewohnt, Socken aus Schubladen zu nehmen, dass die *Existenz* einer Auswahlfunktion offensichtlich scheint.

Dass es wirklich unmöglich ist Auswahlfunktionen im Allgemeinen auf irgendeine Art zu konstruieren, bewies 1963 der Amerikaner Paul Cohen (1934 - 2007), er erhielt hierfür 1966 die Fields-Medaille) nachdem der Österreicher Kurt Gödel (1906 - 1978) schon 1938 gezeigt hatte, dass die allgemeine Existenz von Auswahlfunktion anzunehmen der Mathematik keine Widersprüche hinzufügt. Gödel hatte zuvor allgemein gezeigt, dass sich, sind hinreichend viele Grundannahmen einmal gemacht, *immer* Aussagen konstruieren lassen, zu denen sich kein Gegenbeispiel konstruieren lässt, die aber auch nicht beweisbar sind; dies ist der Gödel'sche Unvollständigkeitssatz, einer der Grundpfeiler der modernen Logik. In der Tat werden Sie im Laufe ihres Studiums wahrscheinlich mehrere weitere solcher Aussagen kennenlernen. Die berühmtesten sind vielleicht

die Kontinuumshypothese und Whiteheads Problem, aber nun hat uns dieser Ausflug weit genug von der Heimat entführt.

Als direkte Konsequenz der beiden Sätze erhalten wir:

5.16. Korollar *Sind A und B nicht-leere Mengen, so gilt: Es gibt eine Injektion $A \to B$ genau dann, wenn es eine Surjektion $B \to A$ gibt.*

5.17. Definition Wir sagen eine Menge M heißt *mächtiger (more potent)* als eine Menge N, falls es eine Injektion $N \to M$ gibt. Man schreibt $M \preccurlyeq N$. Die zwei Menge heißt *gleichmächtig (equipotent)*, falls es eine Bijektion $M \to N$ gibt. Wir werden hierfür $M \cong N$ schreiben.

Wir beenden diesen Abschnitt wieder mit zwei Sätzen, deren Beweise wir erst später führen werden:

5.18. Theorem *(Zermelo'scher Vergleichbarkeitssatz, 1904) Sind A und B Mengen, so existiert eine Injektion $A \to B$ oder eine Injektion $B \to A$. Mit anderen Worten $A \preccurlyeq B$ oder $B \preccurlyeq A$.*

5.19. Theorem *(Satz von Schröder und Bernstein, 1897) Sind A und B Mengen und existieren sowohl eine Injektion $A \to B$ und eine Injektion $B \to A$, so existiert auch eine Bijektion $A \to B$. Mit anderen Worten $A \preccurlyeq B$ und $B \preccurlyeq A$ implizieren $A \cong B$.*

Beide Sätze waren von Cantor schon in seiner ursprünglichen Arbeit, die den Begriff der Menge wie oben formulierte, vermutet worden. Felix Bernstein (1878 - 1956) bewies den ersten in seiner unter Cantor geschriebenen Doktorarbeit; Ernst Schröder (1841 - 1902) gab unabhängig und beinahe gleichzeitig ebenfalls einen Beweis. Der Vergleichbarkeitssatz benötigt übrigends (wie auch da Zorn'sche Lemma) das Auswahlaxiom und es war Ernst Zermelo (1871 - 1953) der es genau zu genau diesem Zweck das ersten Mal explizit formulierte, und mit den Worten "Dieses logische Prinzip läßt sich zwar nicht auf ein noch einfacheres zurückführen, wird aber in der mathematischen Deduktion überall unbedenklich angewendet." kommentierte (alle drei waren Deutsche): Die Auswahl von Elementen war vor seiner expliziten Diskussion (sogar von ihm selbst) als völlig selbstverständliche Beweismethode betrachtet worden und so wollen wir es von nun an auch wieder halten. Eine Begründung des ersten Teils gab er nicht und es dauerte in der Tat beinahe 60 Jahre bis Cohen Zermelos Behauptung beweisen konnte.

6. Äquivalenzrelationen

Wir wenden uns nun der dritte Sorte Relationen zu, die wir betrachten wollen:

6.1. Definition Eine Relation R auf einer Menge M heißt *Äquivalenzrelation (equivalence relation)* falls sie

(1) *reflexiv*, also für alle $m \in M$ gilt mRm gilt,
(2) *transitiv*, also für alle $m, n, k \in M$ gilt $(mRn \wedge nRk) \Rightarrow mRk$, und
(3) *symmetrisch* ist, also für alle $m, n \in M$ gilt $mRn \Rightarrow nRm$.

Reflexivität und Transitivität sind uns natürlich schon bei den Ordnungsrelationen begegnet.

6.2. Beispiel
(1) Die Gleichheitsrelation Δ_M ist auf jeder Menge eine Äquivalenzrelation (sie ist die einzige Äquivalenzrelation, die gleichzeitig eine partielle Ordnung ist). Ebenso ist die Allrelation $M \times M \subseteq M \times M$ eine Äquivalenzrelation.
(2) Ist $f\colon M \to N$ eine Abbildung und R eine Äquivalenzrelation (etwa die Gleichheit) auf N, so ist
$$f^*R := \{(m, m') \in M \times M \mid (f(m), f(m')) \in R\}$$
ein Äquivalenzrelation auf M. Für partielle/totale Ordnungen S stimmt das Analog nur für injektive Abbildungen f: Sonst ist f^*S nicht mehr identitiv. Man stelle sich etwa vor, dass f eine bestimmte Größe oder ähnliches der Elemente von M beschreibt. Dann gilt $m(f^*\Delta_N)m'$ genau dann, wenn $f(m) = f(m')$, also die gleiche Größe haben. Als informelles Beispiel ist etwa "gleichschwer" eine Äquivalenzrelation auf der Menge aller Menschen.

(3) Auf diese Weise lassen sich viele interessante Äquivalenzrelationen bauen. Fixieren wir beispielsweise eine natürliche Zahl $d \neq 0$, so nennt man zwei natürliche Zahlen n und m *äquivalent modulo* d, geschrieben $n \equiv_d m$, wenn sie den gleichen Rest bei Division mit d lassen; die Division mit Rest definiert schließlich eine Funktion $\{\text{natürliche Zahlen}\} \to \{0, 1, 2, \ldots, d-1\}$.
(4) Auf $\mathcal{P}(M)$ is die Gleichmächtigkeit eine äquivalenzrelation: Reflexivität folgt aus der Existenz der Identitätsabbildungen, Transivität aus (1) von Lemma 5.10, und Symmetrie aus der Existenz von Umkehrfunktionen.

Der Zweck von Äquivalenzrelationen ist es Mengen zu partionieren. Dazu haben wir:

6.3. Definition Gegeben eine Äquivalenzrelation R auf M heißen die nicht-leeren maximalen Elemente von

$$\{E \subseteq M \mid \forall m, m' \in E \colon mRm'\}$$

bzgl. der Teilmengenrelation die *Äquivalenzklassen (equivalence class)* von R. Die Menge der Äquivalenzklassen von R bezeichnet man mit $M/R \subseteq \mathcal{P}(M)$.

6.4. Lemma *Gegeben eine Äquivalenzrelation R auf M. Dann existiert zu jedem $m \in M$ genau eine Äquivalenzklasse $E \subseteq M$ mit $m \in E$, nämlich $E = \{x \in M \mid mRx\}$. Insbesondere ist*

$$\{(m, E) \in M \times M/R \mid m \in E\}$$

eine Funktion.

Man bezeichnet diese Funktion häufig mit $[-]_R \colon M \to M/R$. Es gilt dann mRm' genau dann, wenn $[m]_R = [m']_R$.

Beweis. Zur Existenz: Gegeben $x \in M$ bildet $[x]_R = \{m \in M \mid mRx\}$ wirklich eine Äquivalenzklasse mit $x \in [x]_R$ (letzteres wegen Reflexivität): Sind $m, m' \in [x]_R$, so gelten per definitionem mRx und $m'Rx$, also wegen Symmetrie auch xRm' und dann wegen Transitivität auch mRm', und erfüllt $[x]_R \subseteq E \subseteq \mathcal{P}(M)$ ebenfalls $m, m' \in E \Rightarrow mRm'$, gilt wegen $x \in [x]_R \subseteq E$ für alle $m \in E$ auf jeden Fall mRx und damit $E \subseteq [x]_R$. Also gilt dann $E = [x]_R$, was genau sagt, dass $[x]_R$ maximal ist. Dieses Argument zeigt auch die Eindeutigkeit: Ist E maximal und enthält x, so gilt auch $[x]_R \subseteq E$, und weil $[x]_R$ ja schon maximal ist, dann auch $E = [x]_R$. □

6.5. Beispiel
(1) Die Äquivalenzklassen der Gleichheitsrelation sind die Einpunktmengen $\{x\}$ für $x \in M$. Insbesondere ist $[-]_{\Delta_M} \colon M \to M/\Delta_M$ bijektiv. Die Allrelation hat nur eine Äquivalenzklasse, nämlich M selbst, also $M/(M \times M) = \{M\}$.
(2) Für die Äquivalenz modulo d auf den natürlichen Zahlen gibt es genau die d Äquivalenzklassen $[0]_{\equiv_d}, [1]_{\equiv_d}, \ldots, [d-1]_{\equiv_d}$. Etwa gilt $[0]_{\equiv_2} = \{\text{gerade Zahlen}\}$ und $[1]_{\equiv_2} = \{\text{ungerade Zahlen}\}$.
(3) Die Menge $\{\varnothing\}$ ist eine Äquivalenzklasse der Gleichmächtigkeit auf $\mathcal{P}(M)$, ebenso die Menge aller Einpunktmengen in M, und die Menge aller Zweipunktmengen, etc.

Die Äquivalenzklassen bilden immer eine Partition von M in folgendem Sinne:

6.6. Definition Eine *Partition (partition)* einer Menge M ist eine Teilmenge $X \subseteq \mathcal{P}(M)$, derart dass

(1) $U \neq \varnothing$ für alle $U \in X$,
(2) $\bigcup X = M$, und
(3) für alle $U, U' \in X$ gilt $U \neq U' \Rightarrow U \cap U' = \varnothing$.

Der folgende Satz ist Hauptsatz dieses Kapitels und diesmal beweisen wir ihn direkt.

6.7. Theorem *Für jede Menge ist die Abbildung*

$$\{R \subseteq M \times M \mid R \text{ ist Äquivalenzrelation}\} \longrightarrow \{X \subseteq \mathcal{P}(M) \mid X \text{ ist Partition}\}, \quad R \longmapsto M/R$$

eine Bijektion.

Die Umkehrfunktion ist durch

$$X \longmapsto \{(m, m') \in M \times M \colon \exists U \in X \colon m, m' \in U\}$$

gegeben.

Proof. Zunächst zeigen wir, dass M/R wirklich für jede Äquivalenzrelation R eine Partition ist: Per definition sind Äquivalenzklassen nicht leer und nach Lemma 6.4 ist jedes Element von M in einer enthalten, also $\bigcup M/R = M$. Und sind E, E' Äquivalenzklassen und $x \in E \cap E'$, so gelten mRx und $m'Rx$ für alle $m \in E$ und $m' \in E'$. Demzufolge gilt auch mRm' und damit $m' \in E$ und $m \in E'$, was $E = E'$ zeigt.

Bezeichnen wir zur Abkürzung

$$\varphi(X) := \{(m, m') \in M \times M \colon \exists U \in X \colon m, m' \in U\}.$$

Dann zeigen wir als erstes, dass $\varphi(X)$ wirklich eine Äquivalenzrelation ist. Reflexivität folgt direkt aus der zweiten Eigenschaft einer Partition, Transitität aus der dritten (gelten nämlich $x, y \in U$ und $y, z \in U'$ so ist $y \in U \cap U'$, demzufolge $U = U'$ und damit $x, z \in U$) und Symmetrie aus der Kommutativität von $\wedge$.

Nun gilt es noch $\varphi(M/R) = R$ und $M/\varphi(X) = X$ für alle Äquivalenzrelationen R und Partitionen X nachzuweisen. Die erste Aussage ist genau der Kommentar nach Lemma 6.4.

Für die zweite Aussage ist zu zeigen, dass genau die Elemente von X Äquivalenzklassen von $\varphi(X)$ sind. Zeigen wir zunächst, dass jedes $U \in X$ wirklich eine Äquivalenzklasse ist. Tautologischerweise gilt, dass für alle $m, m' \in U$ $m\varphi(X)m'$ gilt, und ist $U \subseteq V$ und für je zwei Elemente $m, m' \in V$ gilt $m\varphi(X)m'$, dann nehmen wir uns ein Element $xinU$ her (U ist wegen der ersten Eigenschaft einer Partition nicht leer), und erhalten $x\varphi(X)m$ für alle $m \in V$. Wegen der dritten Eigenschaft von X muss dies aber von U bezeugt werden, x ist ja in keinem anderen $U' \in X$ enthalten. Also $m \in U$ und demzufolge $U = V$ und demzufolge ist U eine Äquivalenzklasse. Ist andersherum E eine beliebige Äquivalenzklasse von $\varphi(X)$, so gibt es ein $x \in E$ und wegen der zweiten Eigenschaft von X ein $U \in X$ mit $x \in U$. Aber verschiedene Äquivalenzklassen sind nach dem ersten Teil des Beweises disjunkt, also folgt $E = U$. □

Zwei Beweise*

Wir holen nun noch die Beweise des Zorn'schen Lemmas 4.10 und des Vergleichssatzes von Zermelo 5.18 nach; der dritte liegen gebliebene Beweis, nämlich des Satzes von Schröder und Bernstein 5.19, muss noch bin zum nächstes Kapitel warten. Wir beginnen also mit dem Zorn'schen Lemma. Der folgende Beweis wurde vom Amerikaner Jonathan Lewin 1991 gefunden.

Beweis von 4.10. Nehmen wir an M hätte kein maximales Element und setzen $\mathrm{Ch}(M) = \{C \subseteq M \mid C \text{ ist eine Kette in } M\}$. Dann nimmt die Funktion

$$\mathrm{Ch}(M) \longrightarrow \mathcal{P}(M), \quad C \longmapsto \{m \in M \mid \forall c \in C \colon c < m\}$$

nie den Wert $\varnothing$ an, denn per Annahme gibt es zu C ein $u \in M$ mit $c \leqslant u$ für alle $c \in C$, aber da u nicht maximal ist gibt es noch ein $m \in M$ mit $u < m$.

Wir können dann also eine Auswahlfunktion $f \colon \mathrm{Ch}(M) \to M$ mit der Eigenschaft, dass $c < f(C)$ für alle $c \in C$ und Ketten $C \subseteq M$. Dies wollen wir zum Widerspruch führen. Dafür benutzen wir folgenden Trick: Wir nennen eine Menge $K \subseteq M$ f-konform, falls gilt

(1) $\leqslant$ restringiert zu einer Wohlordnung auf K (insbesondere ist K eine Kette), und
(2) für jedes $k \in K$ gilt $k = f(I(K, k))$.

Natürlich ist $\varnothing$ f-konform, aber sobald $K \neq \varnothing$, hat ein kleinstes Element x. Aber dann gilt $I(K, x) = \varnothing$ und damit $x = f(\varnothing)$ unabhängig von K, und in der Tat ist $\{f(\varnothing)\}$ f-komform. Ähnlich ist die einzige f-konforme Teilmenge mit 2 Elementen $\{f(\varnothing), f(\{f(\varnothing)\})\}$ und so weiter.

Wir behaupten nun, dass

$$W = \bigcup \{K \subseteq M \mid K \text{ ist } f\text{-konform}\} \subseteq M$$

selbst f-konform ist und damit sicherlich die größte aller f-konformen Teilmengen von M (bzgl. der Relation $\subseteq$ auf $\mathcal{P}(M)$). Aber es ist dann offenbar auch $W \cup \{f(W)\}$ f-konform und per Konstruktion von f gilt aber $f(w) \notin W$, was den gewünschten Widerspruch liefert.

Es bleibt noch die Behauptung zu verifizieren und hierfür beweisen wir zunächst: Sind A und A' f-konforme Teilmengen von M, so ist entweder A ein Initialsegment von A' oder andersherum.

Stimmen die beiden Mengen überein, so gibt es nicht zu tun. Ansonsten muss also $A\backslash A' \neq \varnothing$ oder $A'\backslash A \neq \varnothing$ gelten. Wir behandeln den ersten Fall. Sei dann x das kleinste Element von $A\backslash A'$, sodass per Definition $I(A,x) \subseteq A'$ gilt. Wir behaupten, dass hier Gleichtheit besteht. Wenn nicht, seien y das kleinste Element von $A'\backslash I(A,x)$ (die Annahme ist ja gerade, dass dies nicht leer ist) und z das kleinste Element von $A\backslash I(A',y)$. Dann gelten wieder per Konstruktion $I(A',y) \subseteq I(A,x)$ und $I(A,z) \subseteq I(A',y)$. Die zweite Inklusion ist aber sogar eine Gleichheit: Ist $a' \in I(A',y)$, so folgt $a' \in I(A,x)$ und damit $a' \in A$ und $a' < x$. Wegen $a', z \in A$ sind dann a' und z vergleichbar. Wäre $z \leqslant a'$ dann würde sowohl $z < x$ als auch $z < y$ gelten. Nach Definition von x folgt dann $z \in A'$, und damit $z \in I(A',y)$, was per definitionem nicht sein kann. Also muss $a' < z$ sein und damit $a' \in I(A,z)$ wie gewünscht.

Aber dann haben wir $y = f(I(A',y)) = f(I(A,z)) = z$ wegen der f-Komformität von A und A'. Es kann dann aber nicht auch noch $x = z$ gelten, da $y \in A'$, aber $x \notin A'$. Aber wegen $x, z \in A$ sind x und z vergleichbar, und wegen

$$I(A,z) \subseteq I(A',y) \subseteq I(A,x)$$

kann nicht $x < z$ gelten. Aber auch $z < x$ kann nicht sein, da dann $y = z \in I(A,x)$ im Widerspruch zur Definition von y gelten würde. Insgesamt, folgt also $A' = I(A,x)$ wie gewünscht.

Wir können nun verfizieren, dass W in der Tat f-konform ist, was den Beweis beendet. Zunächst ist W total geordnet: Dass $\leqslant$ wieder eine partielle Ordnung auf W definiert ist klar, und sind $w, w' \in W$ gegeben, etwa mittels $w \in A$ und $w' \in A'$ mit A, A' f-konform, so gilt entweder $A \subseteq A'$ oder andersherum. In jedem Falle ist $\{w, w'\}$ in einer f-konformen Menge enthalten, da diese total geordnet sind, insbesondere vergleichbar. W ist aber auch wohl geordnet: Ist $\varnothing \neq T \subseteq W$, so wähle ein $t \in T$ und dann ein A f-konform mit $t \in A$. Ist dann x das kleinste Element von $A \cap T$, so behaupten wir, dass x sogar in T kleinst ist. Ist nämlich $w \in T$ gegeben, etwa mit $w \in A'$ und A' f-konform. Gilt $w \in A$ so folgt offenbar $x \leqslant w$ per Definition von x. Gilt $w \notin A$ so muss nach Vorüberlegung $A \subset A'$ ein Initialsegment sein. Aber dann gilt $x \leqslant a'$, ja sogar für jedes$a' \in A'\backslash A$.

Zum Schluss gilt für $w \in W$ mit $w \in A$ mit A f-konform schon $I(w,W) = I(w,A)$, denn jedes $a \in W$, etwa mit $a \in A'$ und A' f-konform, und $a < w$ muss ja bei $A' \subseteq A$ sicherlich $a \in A$ gelten und sonst ist $A \subset A'$ ein Initialsegment, was auch $a \in A$ impliziert. Aber damit gilt

$$w = f(I(w,A)) = f(I(w,W))$$

und W ist f-konform. □

Als zweites wenden wir uns dann dem Vergleichssatz von Zermelo zu:

Beweis von 5.18. Betrachte die Menge

$$F = \{(X,Y,f) \in \mathcal{P}(A)\times\mathcal{P}(B)\times\mathcal{P}(A\times B) \mid f \subseteq X\times Y \text{ definiert eine bijektive Abbildung } X \to Y\}.$$

Auf F definieren wir eine Relation $\leqslant$ derart, dass $(X,Y,f) \leqslant (X',Y',f')$ genau dann, wenn $X \subseteq X'$, $Y \subseteq Y'$ und $f'(x) = f(x)$ für alle $x \in X$. Offenbar ist $\leqslant$ eine partielle Ordnung. Wir behaupten, dass $(F, \leqslant)$ die Voraussetzungen von Zorn's Lemma erfüllt. Glauben wir das für einen Moment, so erhalten wir ein maximales Element (M,N,g) von F. In so einem Element muss dann aber $M = A$ oder $N = B$ gelten: Sind sonst $a \in A\backslash M$ und $b \in B\backslash N$ so ist auch $(X \cup \{a\}, Y \cup \{b\}, g \cup \{(a,b)\}) \in F$ und offenbar größer. Im Falle $M = A$ ist aber $g \subseteq A \times B$ eine Injektion $A \to B$ im Falle $T = B$ definiert $g^{\text{rev}} \subseteq B \times A$ eine Injektion $B \to A$.

Bleibt noch zu zeigen, dass F wirklich die Voraussetzungen von Zorn's Lemma erfüllt: Sicherlich ist F nicht leer, etwa ist $(\varnothing, \varnothing, \varnothing) \in F$ (und falls A oder B leer sind, ist das auch das einzige

Element). Und ist $C \subseteq F$ eine Kette, so gilt

$$u = \left(\bigcup_{(X,Y,f)\in C} X, \bigcup_{(X,Y,f)\in C} Y, \bigcup_{(X,Y,f)\in C} f \right) \in F :$$

Ist $x \in \bigcup_{(X,Y,f)\in C} X$, etwa $x \in X'$ mit $(X', Y', f') \in C$, so gilt $f'(x) \in Y' \subseteq \bigcup_{(X,Y,f)} Y$, und gilt noch $x \in X''$ mit $(X'', Y'', f'') \in C$, so folgt $f'(x) = f''(x)$, weil mindestens eins von $(X', Y', f') \preccurlyeq (X'', Y'', f'')$ oder $(X'', Y'', f'') \preccurlyeq (X', Y', f')$ gilt. Damit liefert $\bigcup_{(X,Y,f)\in C} f$ wirklich eine Abbildung $\bigcup_{(X,Y,f)\in C} X \to \bigcup_{(X,Y,f)\in C} Y$. Das gleiche Argument angewandt auf die inversen Abbildungen zeigt, dass sie bijektiv ist.

Und sicherlich gilt $c \preccurlyeq u$ für jedes $c \in C$, sodass u wirklich eine obere Schranke von C ist. □

KAPITEL 2

Zahlsysteme

1. Die natürlichen Zahlen

Nach all diesen Vorbereitungen wenden wir uns endlich den ersten Objekten zu über die wir wirklich sprechen wollen, den Zahlen und fangen hier mit den natürlichen Zahlen an. Ein Problem ist natürlich, dass wir uns dafür im Prinzip erstmal einigen müssten, was eine Zahl wirklich ist. Eigentlich spielt das, wie Sie vielleicht schon in ihrem wirklich wahren Leben schon gemerkt haben aber gar keine Rolle. Man muss nicht so sehr wissen, was eine Zahl ist, man muss nur wissen wie man zählt. Dies formalisiert man wie folgt:

1.1. Definition (Peano, 1889) Ein *System natürlicher Zahlen (system of natural numbers)* oder auch eine *Peanomenge* besteht aus einer Menge N, einem Element $\alpha \in N$ und einer Funktion $s\colon N \to N$, derart dass

(1) s ist injektiv
(2) $\alpha \notin \mathrm{Im}(s)$
(3) $\forall A \subseteq N\colon (\alpha \in A \wedge (n \in A \Rightarrow s(n) \in A)) \Rightarrow A = N$.

Die Funktion s heißt die *Nachfolgefunktion (successor function)* und α die *Null (zero)* des Systems.

Informell besagen die drei Axiome also, dass man Weiterzählen (1) immer zu von Null verschiedenen Zahlen (2), (2) von verschiedenen Zahlen immer zu verschiedenen Zahlen und (3), das *Induktionsprinzip (principle of induction)*, man durch Weiterzählen von Null aus jede natürliche Zahl erreicht. Ich hoffe alle diese Eigenschaften leuchten ein. Es gilt mit anderen Worten informell gilt $N = \{\alpha, s(\alpha), s(s(\alpha)), s(s(s(\alpha))), \dots\}$ und die Definition oben formalisiert die Pünktchen.

Als fundamendalste Prinzip über die natürlichen Zahlen hat man dann:

1.2. Theorem (Rekursionsprinzip) *Gegeben ein System natürlicher Zahlen (N, α, s), eine Menge Y, eine Funktion $g\colon Y \to Y$ und ein Element $y \in Y$, so gibt es genau eine Abbildung $f\colon N \to Y$ mit*

$$f(\alpha) = y \quad \textit{and} \quad f \circ s = g \circ f.$$

Mit anderen Worten

$$f(\alpha) = y, \quad f(s(\alpha)) = g(f(\alpha)) = g(y), \quad f(s(s(\alpha))) = g(f(s(\alpha))) = g(g(y)), \quad \dots$$

Beweis*. Den Beweis gab es in der Analysisvorlesung. Der Vollständigkeit halber schreibe ich ihn hier noch einmal auf.

Zur Existenz: Man betrachte die Menge

$$B := \{A \subseteq N \times Y \mid (\alpha, y) \in A \wedge (n, x) \in A \Rightarrow (s(n), g(x)) \in A\}.$$

Wir behaupten, dass $f :== \bigcap B$ eine Funktion ist.

Um das zu sehen, betrachten wir

$$C := \{n \in N\colon \exists! x \in Y\colon (n, x) \in f\}$$

und zeigen $C = N$ mithilfe des Induktionsprinzips. Dafür zeigen wir zunächst $\alpha \in C$. Per Definition gilt $(\alpha, y) \in f$ und da $N \times Y \backslash \{(\alpha, x)\} \in B$ (wegen des zweiten Peanoaxioms) für alle $x \in Y$ mit $x \neq y$ gilt, folgt $(\alpha, x) \notin f$ für solche x und damit $\alpha \in C$. Für die zweite Eigenschaft nehmen wir an $n \in C$ an und müssen $s(n) \in C$ zeigen. Per Annahme gilt dann $(n, x) \in f$ für genau ein $x \in Y$, und damit nach Definition $(s(n), g(x)) \in f$. Und für $z \in Y$ mit $z \neq g(x)$ gilt dann

$f\backslash\{(s(n),z)\} \in B$ (wegen des ersten Peanoaxioms), und damit $(s(n),z) \notin f$, und damit $s(n) \in C$. Dies zeigt $C = N$ (wegen des dritten Peanoaxioms), und damit ist f eine Funktion.

Bleibt noch zu zeigen, dass f die zweite der gewünschten Eigenschaften hat; $f(\alpha) = y$ haben wir ja schon gesehen. Hierfür reicht es zu beobachten, dass $f \in B$ gilt (die zweite Bedingung aus der Definition von B sagt ja dann gerade $f(s(n)) = g(f(n))$ für alle $n \in N$). Aber $(n,x) \in f$ genau dann, wenn $(n,x) \in A$ für alle $A \in B$, was per Definition $(s(n), g(x) \in A$ für alle B impliziert, und damit $(s(n), g(x)) \in f$.

Zur Eindeutigkeit: Sind $f, f' \colon N \to X$ zwei Abbildungen, die die Bedingungen aus dem Theorem erfüllen, so betrachten wir

$$A := \{n \in N \mid f(n) = f(n')\}$$

und zeigen wieder $A = N$ mittels des Induktionsprinzips. Aus $f(\alpha) = y = f'(\alpha)$ folgt $\alpha \in A$ und gilt $n \in A$, so rechnen wir

$$f(s(n)) = g(f(n)) = g(f'(n)) = f'(s(n)),$$

was $s(n) \in A$ zeigt. □

Als unmittelbare Anwendung erhält man:

1.3. Korollar (Eindeutigkeit der natürlichen Zahlen) *Sind (N,α,s) und (M,β,t) Systeme natürlicher Zahlen, so gibt es genau eine Abbildung $f \colon N \to M$ mit $f(\alpha) = \beta$ and $f \circ s = t \circ f$. Sie ist umkehrbar.*

Es gibt also genau eine Art zwischen zwei Systemen natürlicher Zahlen hin- und her zu übersetzen.

Beweis. Die Existenz und Eindeutigkeit folgt direkt aus dem Rekursionsprinzip (mit Quelle (N,α,s) und $X = M, x = \beta$ und $g = t$). Um die Umkehrbarkeit einzusehen, wende man den Existenzteils des Rekursionssatzes nochmal andersherum an (also mit Quelle (M,β,t) und $X = N, x = \alpha, g = s$) um eine Abbildung $f' \colon M \to N$ mit $f' \circ t = s \circ f'$ zu erhalten. Aber $f' \circ f \colon N \to N$ ist dann eine Abbildung mit $(f' \circ f)(\alpha) = f'(\beta) = \alpha$ und

$$f' \circ f \circ s = f' \circ t \circ f = s \circ f' \circ f.$$

Aber ebenso gilt $\mathrm{id}_N(\alpha) = \alpha$ und $\mathrm{id}_N \circ s = s \circ \mathrm{id}_N$, sodass die Eindeutigkeit im Rekursionssatz $f' \circ f = \mathrm{id}_N$ erzwingt. Ähnliches für $f \circ f'$ und id_M. □

Beschäftigen wir uns nun mit der Existenz von Systemen natürlicher Zahlen:

1.4. Definition (Dedekind, 1888) Eine Menge M heißt *endlich (finite)* falls gilt $\forall f \colon M \to M \colon f$ injektiv $\Leftrightarrow f$ surjektiv. Ansonsten heißt sie *unendlich (infinite)*.

Per Definitionem ist die Menge N in einem System natürlicher Zahlen (N,α,s) unendlich: s ist injektiv, aber nicht surjektiv da $\alpha \neq \mathrm{Im}(s)$. Umgekehrt gilt:

1.5. Lemma (Existenz der natürlichen Zahlen) *Ist $f \colon M \to M$ injektiv und $x \notin \mathrm{Im}(f)$, so hat die Menge*

$$\{X \subseteq M \colon x \in X \wedge (m \in X \Rightarrow f(m) \in X)\}$$

ein kleinstes Element N. Die Abbildung f schränkt sich zu einer Abbildung $s \colon N \to N$ ein, und (N,x,s) ist dann ein System natürlicher Zahlen.

Gibt es also überhaupt eine unendliche Menge (und daran glauben wir natürlich), so gibt es auch ein System natürlicher Zahlen.

Beweis*. Wieder gab es den Beweis in der Analysisvorlesung, und ich schreibe ihn hier der Vollständigkeit nochmal auf:

Wir setzen

$$A = \{X \subseteq M \colon x \in X \wedge (m \in X \Rightarrow f(m) \in X)\}.$$

und $N = \bigcap A$. Man überprüft leicht, dass $N \in A$ (ähnlich zur Behauptung, dass $\bigcap B \in B$ im Beweis des Rekursionsprinzips), und per Definition gilt $N \subseteq X$ für alle $X \in A$, sodass N wirklich

ein kleinstes Element ist. Per Definition gilt $n \in N \Rightarrow f(n) \in N$, was zeigt, dass $s := f \cap N \times N$ eine Abbildung $s\colon N \to N$ definiert. Soviel zu den Vorüberlegungen.

Bleibt zu zeigen, dass (N, x, s) die Peanoaxiome erfüllt. Per Annahmen gilt $x \notin \mathrm{Im}_f$, also sicherlich $x \notin \mathrm{Im}_s$, und s ist als Einschränkung von f auch injektiv. Sei also zuletzt $B \subseteq N$, mit $x \in B$ und $m \in B \Rightarrow f(m) \in B$; wir müssen $B = N$ zeigen. Aber es gilt dann ja $B \in A$ und N ist das kleinste Element von A, also $N \subseteq B$ und damit $N = B$. □

Zusammen genommen erlauben uns die Existenz und Eindeutigkeit etwas missbräuchlich von *dem* System natürlicher Zahlen zu sprechen.

1.6. Definition Wir schreiben $\mathbb{N}$ für das System natürlicher Zahlen und 0 für sein Nullelement (und weiterhin s für die Nachfolgefunktion). Weiterhin sind heutzutage folgende Symbole gebräuchlich:

$$1 := s(0), 2 := s(1), 3 := s(2), 4 := s(3), 5 := s(4), 6 := s(5), 7 := s(6), 8 := s(7) \quad \text{und} \quad 9 := s(8)$$

Diese Anzahl fixer Symbole stimmt mit der Anzahl unserer Finger überein, was sicherlich kein Zufall ist. Natürlich kann man die natürlichen Zahlen ordnen:

1.7. Theorem *Es gibt genau eine partielle Ordnung $\leqslant$ auf $\mathbb{N}$, sodass $n \leqslant s(n)$ für alle $n \in \mathbb{N}$ gilt. Sie ist total, 0 ist ihr kleinstes Element und überhaupt hat jede nicht-leere Teilmenge von $\mathbb{N}$ ein kleinstes Element.*

Eine partiell geordnete Menge M, in der jede Teilmenge ein kleinstes Element hat, heißt *wohlgeordnet (well-ordered)*. Solche partiellen Ordnungen sind immer total: Man betrachte die zwei-elementigen Teilmengen von M. Offenbar ist jede Teilmenge einer wohlgeordneten Menge wieder wohlgeordnet.

Beweis*. Wieder gab es den Beweis in der Analysisvorlesung, und ich schreibe ihn hier der Vollständigkeit nochmal auf:

Zur Existenz: Für jedes $n \in \mathbb{N}$ hat

$$T(n) := \{A \subseteq \mathbb{N}\colon n \in A \wedge (m \in A \Rightarrow s(m) \in A)$$

ein kleinstes Element $S(n)$, nämlich seinen Durchschnitt, wie schon in den Beweisen des Rekursionsprinzips und der Existenz von $\mathbb{N}$. $S(n)$ ist die Menge der (iterierten) Nachfolger von n; beispielsweise gelten $S(0) = \mathbb{N}$ nach dem Induktionsprinzip.

Wir definieren nun

$$\leqslant := \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid m \in S(n)\}.$$

Dann sind Reflexivität ist klar, ebenso wie $n \leqslant s(n)$.. Alle anderen Eigenschaften bedürfen etwas Vorbereitung. Zunächst beobachten wir $S(m) \subseteq S(n) \Leftrightarrow m \in S(n)$. Die Vorwärtsimplikation folgt aus $m \in S(m)$. Die Rückrichtung weil $m \in S(n)$ impliziert, dass $S(n) \in T(m)$, und damit $S(m) \subseteq S(n)$, weil $S(m)$ ja das kleinste Element von $T(m)$ ist. Diese Überlegung zeigt sofort die Transitivität, da $\subseteq$ eine transitive Relation ist.

Als nächstes zeigen wir $S(s(n)) = S(n)\backslash\{n\}$.

Zunächst gilt $S(s(n)) \cup \{n\} = S(n)$: Nach der gerade getroffenen Überlegung gilt sicherlich $S(s(n)) \subseteq S(n)$ und $\{n\} \subseteq S(n)$ sowieso, also ist die linke in der rechten Seite enthalten und andersherum gilt $S(s(n)) \cup \{n\} \in T(n)$, sodass die rechte in der linken liegt. Es muss also $S(s(n)) = S(n)\backslash\{n\}$ oder $S(s(n)) = S(n)$ gelten und um den zweiten Fall auszuschließen beweisen wir noch $S(n)\backslash\{n\} \in T(s(n))$, sodass $S(s(n)) \subseteq S(n)\backslash\{n\}$. Dazu betrachten wir

$$B := \{n \in \mathbb{N} \mid S(n)\backslash\{n\} \in T(s(n))\}.$$

Dann gilt $0 \in B$ (nach dem zweiten von Peano's Axiomen), und falls $n \in B$ gilt, so hat man $S(s(n)) \subseteq S(n)\backslash\{n\}$, also insbesondere $n \notin S(s(n))$. Daraus folgt nun leicht $S(s(n))\backslash\{s(n)\} \in T(s(s(n)))$: Nach einer Aufgabe vom vierten Zettel gilt $s(s(n)) \neq s(n)$, sodass $s(s(n)) \in S(s(n))\backslash\{s(n)\}$ und falls $m \in S(s(n))\backslash\{s(n)\}$ so gilt sicher $s(m) \in S(s(n))$, und sollte $s(m) = s(n)$ so liefert die Injektivität von s, dass $n = m$, aber $n \notin S(s(n))$.

Als nächstes zeigen wir die Totalität, also dass immer entweder $S(n) \subseteq S(m)$ oder $S(m) \subseteq S(n)$ gilt. Wieder betrachten wir hierfür

$$A = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} \colon S(n) \subseteq S(m) \text{ oder } S(m) \subseteq S(n)\}$$

Dann gilt $S(m) \subseteq \mathbb{N} = S(0)$, also $0 \in A$. Sei dann $n \in A$ und $m \in \mathbb{N}$. Gilt $S(m) \subseteq S(n)$, so folgt wegen $S(s(n)) = S(n)\backslash\{n\}$ auch $S(m) \subseteq S(s(n))$, außer im Falle $n \in S(m)$. Aber in diesem Falle folgt, dann $S(n) \subseteq S(m)$ und dann sicherlich $S(s(n)) \subseteq S(n) \subseteq S(m)$, also in jedem Falle $s(n) \in A$. Also ist $\leqslant$ total.

Zu guter letzt bleibt noch die Identivität übrig: Mit anderen Worten gilt $S(n) = S(m)$ so folgt $n = m$. Wieder setzen wir

$$C \coloneqq \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} \colon S(n) = S(m) \Rightarrow n = m\}.$$

Für $m > 0$ ist $\mathbb{N}\backslash\{0\} \in T(0)$, also $0 \notin S(m)$ und damit $S(0) \neq S(m)$, ergo $0 \in C$. Ist dann $n \in C$, und $S(s(n)) = S(m)$, so ist $n \neq S(m)$, also $m \neq 0$. Dann gibt es ebenfalls nach einer Aufgabe des vierten Zettels ein $p \in \mathbb{N}$ mit $s(p) = m$ und damit

$$S(n)\backslash\{n\} = S(s(n)) = S(s(p)) = S(p)\backslash\{p\}.$$

Wegen Totalität gilt nun $S(p) \subseteq S(n)$ oder $S(n) \subseteq S(p)$. Nehmen wir etwa das erste an, so gilt $p \in S(n)$, also kann $p \notin S(n)\backslash\{n\}$ nur gelten, wenn $n = p$ ist, und andersherum ebenso.

Damit ist $\leqslant$ endlich als totale Ordnung auf $\mathbb{N}$ nachgewiesen. Wir berechnen dann noch die Mi

Zeigen wir nun noch, dass jede nicht-leere Teilmenge M ein kleinstes Element hat. Dazu sei

$$D \coloneqq \{n \in \mathbb{N} \colon \forall M \subseteq \mathbb{N} \colon \exists i \leqslant n \colon i \in M \Rightarrow M \text{ hat kleinstes Element}\}$$

Dann gilt $0 \in D$, da 0 ja sogar kleinstes Element von ganz $\mathbb{N}$, erst recht von jedem $M \subseteq \mathbb{N}$ mit $0 \in M$. Gilt $n \in D$, und $M \subseteq \mathbb{N}$ mit $s(n) \in M$, so kann entweder $i \in M$ für ein $i \leqslant n$ gelten, sodass M nach Annahme ein kleinstes Element hat oder es ist $s(n)$ eben das kleinste Element von M.

Zur Eindeutigkeit: Ist R eine weitere partielle Ordnung auf $\mathbb{N}$ mit $nRs(n)$, so folgt $\{m \in \mathbb{N} \mid nRm\} \in T(n)$, und damit $S(n) \subseteq \{m \in \mathbb{N} \mid nRm\}$, mit anderen Worten $n \leqslant m \Rightarrow nRm$, und damit $\leqslant \subseteq R$. Gilt nun aber nRm, so gilt wegen der Totalität von $\leqslant$ mindestens eins von $n \leqslant m$ und $m \leqslant n$. Im zweiten Falle folgt mRn und damit $n = m$, also $n \leqslant m$ und damit $R \subseteq \leqslant$, was noch zu zeigen war. □

Die Ordnung erlaubt uns nun zu formulieren:

1.8. Satz (Allgemeines Rekursionsprinzip) *Seien X und Y Mengen, $y \colon X \to Y$ and*

$$g \colon \mathrm{F}(X \times \mathbb{N}, Y) \times X \times \mathbb{N} \to Y$$

eine Funktion die für alle $h, h' \colon X \times \mathbb{N} \to Y$ und $n \in \mathbb{N}$ die Implikation

$$(\forall i \leqslant n, x \in X \colon h(x,i) = h'(x,i)) \Longrightarrow \forall x \in X \colon g(h,x,n) = g(h',x,n)$$

erfüllt. Dann existiert genau eine Abbildung $f \colon X \times \mathbb{N} \to Y$ mit

$$f(x,0) = y(x) \quad \textit{and} \quad f(x,s(n)) = g(f,x,n)$$

für alle $n \in \mathbb{N}$ und $x \in X$.

Der Satz sieht erstmal sehr viel komplizierter aus als das (spezielle) Rekursionsprinzip, aber diese Allgemeinheit ist wirklich nötig, wie wir jetzt und auf dem Übungszettel und auch im folgenden Satz sehen werden.

Scharfes Hinsehen zeigt, dass die Bedinung die wir an g hier stellen besagt, dass der Wert von $g(f,x,n)$ nur von x, n und $f(0), f(1), f(2), \ldots, f(n)$ abhängt, nicht aber von $f(s(n)), f(s(s(n))), \ldots$. Das erkennt man hoffentlich direkt als notwendige Bedingung, dass das rekursive Definieren von $f(x,s(n))$ als $g(f,x,n)$ nicht selbstreferentiell oder schlimmer noch vorgreifend wird.

Beweis*. Diesen Beweis gab es zwar in der Analysisvorlesung nicht, aber ich habe ihn in der Vorlesung trotzdem übersprungen.

Wir leiten den Satz aus dem eigentlichen Rekursionsprinzip mit einem Trick her (den ich auch jedes Mal wieder nachlesen muss): Nämlich, wir wenden 1.2 auf die Menge $\bar{X} = \mathrm{F}(X \times \mathbb{N}, Y) \times \mathbb{N}$ mit der Selbstabbildung $\bar{g}\colon \bar{X} \to \bar{X}$ gegeben durch

$$(h,n) \longmapsto \left((x,i) \mapsto \begin{cases} h(x,i) & i \leqslant n \\ g(h,x,n) & i > n \end{cases}, s(n) \right)$$

und das Element $\bar{y} = ((x,i) \mapsto y(x), 0)$ an. Wir erhalten also eine Abbildung $\bar{f}\colon \mathbb{N} \to \bar{X}$ mit

$$\bar{f}(0) = \bar{y} \quad \text{and} \quad \bar{f}(s(n)) = \bar{g}(\bar{f}(n)).$$

Bezeichnen wir nun den ersten Eintrag eines Paares $z = (m,n) \in M \times N$ der einfacheren Lesbarkeit halber einmal durchweg mit z_1 (also $z_1 = m$) und den zweiten mit z_2 (also $z_2 = n$), so können wir die gesuchte Funktion f durch

$$f(x,n) = (\bar{f}(n)_1)(x,n),$$

definieren. Bevor wir die gewünschten Eigenschaften nachweisen, beobachten wir als erstes, dass für alle $n \in \mathbb{N}$ gilt $\bar{f}(n)_2 = n$: Ist nämlich $A = \{n \in \mathbb{N} \mid \bar{f}(n)_2 = n\}$ so gilt per definitionem von $\bar{f}$, dass $0 \in A$ und ist $n \in A$, so rechnen wir

$$\bar{f}(s(n))_2 = \bar{g}(\bar{f}(n))_2 = s(\bar{f}(n)_2) = s(n).$$

Nach Induktionsprinzip gilt also $A = \mathbb{N}$, was wir zeigen wollten. Nun zum Nachweis der Eigenschaften von f: Es gilt zum einen

$$f(x,0) = [\bar{f}(0)_1](x,0) = \bar{y}_1(x,0) = [(x,i) \mapsto y(x)](x,0) = y(x)$$

und zum anderen

$$\begin{aligned} f(x,s(n)) &= [\bar{f}(s(n))_1](x,s(n)) \\ &= [\bar{g}(\bar{f}(n))_1](x,s(n)) \\ &= \left[(a,i) \mapsto \begin{cases} [\bar{f}(n)_1](a,i) & i \leqslant \bar{f}(n)_2 \\ g(\bar{f}(n)_1,a,n) & i > \bar{f}(n)_2 \end{cases} \right] (x,s(n)) \\ &= \left[(a,i) \mapsto \begin{cases} [\bar{f}(n)_1](a,i) & i \leqslant \bar{n} \\ g(\bar{f}(n)_1,a,n) & i > \bar{n} \end{cases} \right] (x,s(n)) \\ &= g(\bar{f}(n)_1,x,n) \end{aligned}$$

Wir behaupten nun, dass die Abbildung $\bar{f}(n)_1\colon X \times \mathbb{N} \to Y$ auf den Elementen (x,i) mit $x \in X$ und $i \leqslant n$ mit f selbst übereinstimmt. Sobald wir das gezeigt haben, kommt dann die Eigenschaft von g ins Spiel die wir noch nicht benutzt haben. Sie impliziert, dass dann wirklich $g(\bar{f}(n)_1,x,n) = g(f,x,n)$ gilt wie gewünscht. Die verbleibende Behauptung zeigen wir per Induktion: Sei nämlich

$$A = \{n \in \mathbb{N} \mid \forall x \in X, i \leqslant n\colon [\bar{f}(n)_1](x,i) = f(x,i)\}.$$

Dann gilt $0 \in A$ weil

$$[\bar{f}(0)_1](x,0) = \bar{y}_1(x,0) = y(x) = f(x,0)$$

wie wir oben schon gerechnet hatten, und falls $n \in A$, so gilt für $i \leqslant s(n)$

$$\begin{aligned}
[\bar f(s(n))_1](x,i) &= [\bar g(\bar f(n))_1](x,i)\\
&= \left[(a,j) \mapsto \begin{cases} [\bar f(n)_1](a,j) & j \leqslant f(n)_2 \\ g(\bar f(n)_1, a, n) & j > \bar f(n)_2 \end{cases}\right](x,i)\\
&= \left[(a,j) \mapsto \begin{cases} [\bar f(n)_1](a,j) & j \leqslant n \\ g(\bar f(n)_1, a, n) & j > n \end{cases}\right](x,i)\\
&= \begin{cases} [\bar f(n)_1](x,i) & i \leqslant n \\ g(\bar f(n)_1, x, n) & i = s(\bar f(n)_2) \end{cases}\\
&= \begin{cases} f(x,i) & i \leqslant n \\ f(x,s(n)) & i = s(n) \end{cases}\\
&= f(x,i)
\end{aligned}$$

wobei wir im vorletzten Schritt für den ersten Fall die Annahme $n \in A$ benutzen und im zweiten Fall die schon gemacht Berechnung von $f(x,s(n))$ oben. Dies beendet den Nachweis, dass $n \in A \Rightarrow s(n) \in A$. Dann schlägt aber das Induktionsprinzip zu und wir erhalten $A = \mathbb{N}$, was den Beweis beendet, dass$f$ die gewünschten Eigenschaften hat, und damit den gesamten Existenzteil des Beweises.

Die Eindeutigkeit ist leichter: Sind $f, f' \colon X \times \mathbb{N} \to Y$ zwei Abbildungen, die die Bedingungen des Satzes erfüllen, so setzen wir:

$$B = \{n \in \mathbb{N} \mid \forall x \in X, i \leqslant n \colon f(x,i) = f'(x,i)\}.$$

Wieder gilt $0 \in B$ weil $f(x,0) = y(x) = f'(x,0)$ und falls $n \in B$ so gilt auch

$$f(x,s(n)) = g(f,x,n) = g(f',x,n) = f'(x,s(n))$$

wegen der angenommen Eigenschaft von g. □

Als erste Anwendung zeigen wir, dass Dedekind's Begriff der Endlichkeit mit dem etwas naheliegenderen in Termen der natürlichen Zahlen übereinstimmt (der Punkt von Dedekind's Definition ist aber gerade, dass sie keine Referenz zu den natürlichen Zahlen macht).

1.9. Theorem *Eine Menge M ist endlich genau dann, wenn es ein $n \in \mathbb{N}$ und eine Bijektion $\{k \in \mathbb{N} \mid k < n\} \to M$ gibt. Solch ein $n \in \mathbb{N}$ (nicht aber die Bijektion) ist eindeutig bestimmt, und heißt die* Anzahl (number) *(der Elemente) von M, geschrieben $|M|$. Für zwei endliche Mengen gilt $M \leqslant N$ genau dann, wenn $|M| \leqslant |N|$.*

Eine Menge ist unendlich genau dann, wenn es eine Injektion $\mathbb{N} \to M$ gibt.

Etwa gilt $|\varnothing| = 0$, $|\{0\}| = 1$ und $|\{0,1,3,5\}| = 4$. Eine Menge M, für die es eine Surjektion $\mathbb{N} \to M$ nennt man *abzählbar (countable)*, und es war eine der revolutionären Entdeckungen Cantors, dass es unendliche Mengen gibt, die nicht abzählbar sind. Weiteres dazu gibt es ebenfalls in der Analysisvorlesung.

Beweis*. Wieder gab es den Beweis in der Analysisvorlesung, und ich schreibe ihn hier der Vollständigkeit nochmal auf.

Als erstes zeigen wir die letzte Aussage. Dass es zu unendlichen Mengen M eine Injektion $\mathbb{N} \to M$ gibt, ist Teil von 1.5. Und hat man umgekehrt eine Injektion $f \colon \mathbb{N} \to M$, so definiert man eine Abbildung

$$M \longrightarrow M, \quad m \longmapsto \begin{cases} m & m \notin \operatorname{Im}_f \\ f(s(n)) & m = f(n) \end{cases}$$

die injektiv ist und $f(0)$ nicht trifft.

Als nächstes zeigen wir, dass die Mengen $\{k \in \mathbb{N} \mid k < n\}$ wirklich endlich sind. Dazu setzen wir natürlich

$$A = \{n \in \mathbb{N} \mid \{k \in \mathbb{N} \mid k < n\} \text{ ist endlich}\}.$$

Dann gilt $0 \in \mathbb{N}$, denn die eindeutig bestimmte Abbildung $\varnothing \to \varnothing$ ist sowohl injektiv als auch surjektiv. Und gilt $n \in A$ und $f\colon \{k \in \mathbb{N} \mid k < s(n)\} \to \{k \in \mathbb{N} \mid k < s(n)\}$ ist injektiv, so betrachten wir die Abbildung

$$\sigma\colon \{k \in \mathbb{N} \mid k < s(n)\} \to \{k \in \mathbb{N} \mid k < s(n)\}, \quad m \longrightarrow \begin{cases} f(s(n)) & i = s(n) \\ s(n) & i = f(s(n)) \\ i & i \neq s(n), f(s(n)) \end{cases}.$$

Sie ist offenbar bijektiv, und desmzufolge $\sigma \circ f$ immer noch injektiv nach 5.10. Aber es gilt $\sigma(f(s(n)) = s(n)$, sodass sich $\sigma \circ f$ zu einer (immer noch injektiven) Abbildung $\{k \in \mathbb{N} \mid k < n\} \to \{k \in \mathbb{N} \mid k < n\}$ einschränkt. Diese muss dann nach Annahme bijektiv sein, und dann ist es aber auch $\sigma \circ f$ in Gänze, und damit auch f. Den Fall, dass f als surjektiv ist kann man ähnlich beweisen, oder er folgt, indem man einen Schnitt h von f wählt wie in 5.14, beobachtet, dass dieser injektiv ist nach 5.13, ergo bijektiv nach dem gerade bewiesenen. Aber dann muss nach 5.11 auch f bijektiv sein. Das bedeutet $s(n) \in A$, und eine Anwendung des Induktionsprinzips beendet den Beweis.

Als drittes zeigt man, dass es für $n < m$ (also $n \leqslant m \wedge n \neq m$) keine Surjektion $\{k \in \mathbb{N} \mid k < n\} \to \{k \in \mathbb{N} \mid k < m\}$ gibt (oder dann äquivalent keine Injektion in die andere Richtung); dies ist das sogenannte *Schubfachprinzip (pidgeon hole principle)*. Es zeigt zu gleich, dass eine Menge höchstens eine Anzahl hat (dass alle endlichen Mengen eine Anzahl haben, zeigen wir erst im letzten Schritt), und dass $M \preccurlyeq N$ genau dann, wenn $|M| \leqslant |N|$. Natürlich beweisen wir das Schubfachprinzip mit Induktion. Nämlich betrachten wir

$$C \coloneqq \{n \in \mathbb{N} \mid \forall n < m \in \mathbb{N}\colon \text{es existiert keine Surjektion} \{k \in \mathbb{N} \mid k < n\} \to \{k \in \mathbb{N} \mid k < m\}\}$$

Dann gilt $0 \in C$: Die leere Menge surjiziert nur auf die leere Menge. Und gilt $n \in C$, und $f\colon \{k \in \mathbb{N} \mid k < s(n)\} \to \{k \in \mathbb{N} \mid k < m\}$ eine Abbildung mit $s(n) < m$. Wir müssen zeigen, dass f nicht surjektiv ist. Liegt m nicht im Bild von f sind wir natürlich sofort fertig. Sonst sei $x < s(n)$ ein Urbild von m. Liefert

$$\tau\colon \{k \in \mathbb{N} \mid k < n\} \longrightarrow \{k \in \mathbb{N} \mid k < s(n)\}\backslash\{x\}, \quad a \longmapsto \begin{cases} i & i < x \\ s(i) & x \leqslant i \end{cases}$$

eine Bijektion, sodass per Induktionshypothese $f \circ \tau$ nicht surjektiv sein kann. Und liegt $y < m$ nicht im Bild von $f \circ \tau$, so liegt y auch nicht im Bild von f, da per Konstruktion ja $\mathrm{Im}_f = \mathrm{Im}_{f\circ\tau} \cup \{m\}$ gilt.

Als letztes beweisen wir, dass eine endliche Menge eine Bijektion zu einer der Mengen $\{k \in \mathbb{N} \mid k < n\}$ besitzt. Wir machen das mithilfe eines Umkehrschlusses. Sei also M eine Menge, die zu keinem $\{k \in \mathbb{N} \mid k < n\}$ in Bijektion steht. Wir werden zeigen, dass es eine Injektion $\mathbb{N} \to M$ gibt. Hierzu beobachten wir zuerst, dass es für jedes n zumindest eine Injektion $\{k \in \mathbb{N} \mid k < n\} \to M$ gibt. Dazu betrachten wir wieder die Menge B aller $n \in \mathbb{N}$ für die das wahr ist. Dann gilt $0 \in B$, da die eindeutige Abbildung $\varnothing \to M$ injektiv ist, und ist $f\colon \{k \in \mathbb{N} \mid k < n\} \to M$ injektiv, so ist f nach Annahme nicht surjektiv und für $x \notin \mathrm{Im}_f$ ist dann auch

$$\{k \in \mathbb{N} \mid k < s(n)\} \to M, \quad \begin{cases} f(i) & i \leqslant n \\ x & i = s(n) \end{cases}$$

injektiv, sodass $n \in B \Rightarrow s(n) \in B$, und damit $B = \mathbb{N}$ wie gewünscht. Das zeigt, dass man das Auswahlprinzip auf

$$\mathbb{N} \longrightarrow \mathcal{P}(\mathcal{P}(\mathbb{N} \times M)), \quad n \mapsto \{f \subseteq \mathbb{N} \times M \mid f \text{ ist eine injektive Funktion } \{k \in \mathbb{N} \mid k < n\} \to M\}$$

anwenden kann. Man erhält also eine Abbildung $u\colon \mathbb{N} \to \mathcal{P}(\mathbb{N}\times M)$ mit $u(n)\colon \{k \in \mathbb{N} \mid k < n\} \to M$ injektiv für alle $n \in \mathbb{N}$.

Nun definieren wir $f\colon \mathbb{N} \to M$ durch $f(0) = u_1(0)$ und informell indem wir $f(s(n))$ also $u_{s(n)}(i)$, wobei i das kleinste Element ist, derart dass $u_{s(n)}(i) \neq f(0), f(1), \ldots, f(n)$; so ein Element

gibt es dann genau nach dem eben bewiesenem Schubfachprinzip. Formal benutzen wir hierfür, dass allgemeine Rekursionsprinzip mit

$$g\colon \mathrm{F}(\mathbb{N}, M) \times \mathbb{N} \to M, \quad (h, n) \mapsto u_{s(n)}(\{\min\{i \leqslant s(n)\colon \forall j \leqslant n\colon u_{s(n)}(i) \neq h(j)\}\}).$$

Dass die resultierende Abbildung injektiv ist, ist hoffentlich klar. □

1.10. Bemerkung Dieses Theorem enthält insbesondere den Satz von Schröder und Bernstein im Falle endlicher Mengen. Ich wiederhole noch einmal, dass es nicht wahr ist, dass jede unendliche Menge eine Injektion nach $\mathbb{N}$ besitzt.

Bevor wir uns nun weiter mit den natürlichen Zahlen beschäftigen noch eine überraschende Konsequenz der Unendlichkeit einer Menge:

1.11. Theorem (Satz von Hessenberg, 1906) *Eine Menge X mit mehr als einem Element ist unendlich genau dann, wenn es eine Bijektion zwischen X und $X \times X$ gibt.*

Ist X endlich mit mehr als einem Element, so folgt aus dem gerade bewiesenen Satz, dass $X \times X$ mehr Elemente hat als X: Hat X etwa n Elemente, so hat ja $X \times \{x\}$ für jedes $x \in X$ ebenfalls n Elemente und per Annahme gilt $X \times \{x\} \subsetneq X \times X$. Die interessantere Umkehrung beweisen wir am Ende dieses Kapitels.

Als nächstes wollen wir die üblichen Rechenoperationen diskutieren. Einführen werden sie mit dem Rekursionsprinzip. Die Addition ist aber etwa eine Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sodass es sich nicht direkt anwenden lässt. Wir brauchen:

1.12. Korollar *Es gibt eindeutige Funktionen* $\mathrm{add}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *und* $\mathrm{mult}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*, die* Addition (addition) *und die* Multiplikation (multiplication)*, mit*

$$\mathrm{add}(m, 0) = n \quad \textit{und} \quad \mathrm{add}(m, s(n)) = s(\mathrm{add}(m, n))$$

und

$$\mathrm{mult}(m, 0) = 0 \quad \textit{und} \quad \mathrm{mult}(m, s(n)) = \mathrm{add}(m, \mathrm{mult}(m, n))$$

für alle $m, n \in \mathbb{N}$.

Wir werden natürlich meistens $n+m$ anstatt $\mathrm{add}(n, m)$ und $n \cdot m$ anstatt $\mathrm{mult}(n, m)$ schreiben.

Beweis. Für die Addition wende man das allgemeine Rekursionsprinzip mit $X = \mathbb{N} = Y, y = \mathrm{id}_{\mathbb{N}}$ und $g(h, x, n) = s(h(x, n))$ an. Für die Multiplikation wende man es mit $X = \mathbb{N} = Y, y = \mathrm{const}_0$ und $g(h, x, n) = \mathrm{add}(x, h(x, n))$ an. □

1.13. Beispiel (1) Etwa haben wir

$$n + 1 = \mathrm{add}(n, s(0)) = s(\mathrm{add}(n, 0)) = s(n)$$

$$n + 2 = \mathrm{add}(n, s(1)) = s(\mathrm{add}(n, 1)) = s(n + 1) = s(s(n))$$

und so weiter,

(2) und auch

$$n \cdot 1 = \mathrm{mult}(n, s(0)) = \mathrm{add}(n, \mathrm{mult}(n, 0)) = \mathrm{add}(n, 0) = n$$

$$n \cdot 2 = \mathrm{mult}(n, s(1)) = \mathrm{add}(n, \mathrm{mult}(n, 1)) = \mathrm{add}(n, n) = n + n$$

et cetera.

(3) Ein konkretes Beispiel:

$$3 + 3 = 3 + s(2) = s(3 + 2) = s(3 + s(1)) = s(s(3 + 1))$$

$$= s(s(3 + s(0))) = s(s(s(3 + 0))) = s(s(s(3))) = s(s(4)) = s(5) = 6$$

wie hoffentlich auch alle erwartet haben.

Es gelten nun eine große Zahl Rechengesetze, die uns immer wieder begegnen werden und denen wir deshalb vorab Namen geben:

1.14. Definition Eine Menge M zusammen mit einer Abbildung

$$M \times M \to M, \quad (m,n) \longmapsto m * n,$$

einer sogenannten *Verknüpfung (composition)*, und einem Element $e \in M$ heißt *Monoid (monoid)*, falls für alle $m,n,k \in M$ gilt

(1) Assoziativität
$$(m * n) * k = m * (n * k)$$
(2) Neutralität
$$m * e = m = e * m$$

So ein Monoid heißt *abelsch* oder *kommutativ*, wenn weiter gilt

(3) Kommutativität
$$m * n = n * m$$

Ist auf M auch noch eine partielle Ordnung $\leqslant$ auf M gegeben, so sagt man $(M, \leqslant, *, e)$ ist ein *partiell geordneter Monoid*, falls noch

(4) Monotonie
$$m \leqslant n \Longrightarrow m * k \leqslant n * k \quad \text{und} \quad k * m \leqslant k * n$$

gilt. Ist stattdessen eine zweite Verknüpfung

$$M \times M \to M, \quad (m,n) \longmapsto m \times n,$$

und ein weiteres Element $f \in M$ gegeben, so nennt man das Tupel $(M, *, \times, e, f)$ eine *Halbring (semiring)*, falls

(1) $(M, *, e)$ ist ein kommutativer Monoid,
(2) $(M, \times, f)$ ist ein Monoid, und
(3) Distributivität
$$(m * n) \times k = (m \times k) * (n \times k)$$
und
$$m \times (n * k) = (m * n) \times (m * k)$$
(4) Absorption
$$e \times m = e = m \times e$$

gelten. So ein Halbring heißt kommutativ, wenn auch die zweite Verknüpfung kommutativ ist. Ein *partiell geordneter Halbring* besteht schließlich aus all dem obigen, ist also ein Tupel $(M, \leqslant, *, \times, e, f)$ derart, dass

(1) $(M, *, \times, e, f)$ ist ein Halbring,
(2) Die Ordnung $\leqslant$ macht $(M, *, e)$ zu einem geordneten Monoiden, und
(3) $m \leqslant n$ und $e \leqslant k \Longrightarrow m \times k \leqslant n \times k$ und $k \times m \leqslant k \times n$.

Uff.

Ringe (also nicht nur halbe) werden uns ebenfalls bald begegnen. Die Haupteigenschaften der Addition und Multiplikation lassen sich also Zusammenfassen durch folgenden Satz, der in gewisser Form sicherlich schon in der Antike bekannt war (und natürlich obige Definition in seiner Gänze motiviert):

1.15. Satz (nach Adam Riese) *Das Tupel* $(\mathbb{N}, \leqslant, +, \cdot, 0, 1)$ *bildet einen total geordneten kommutativen Halbring, mit*

$$a \leqslant b \Longleftrightarrow \exists c \in \mathbb{N} \colon b = a + c.$$

Desweiteren gelten immer

$$a + b = a + c \Longrightarrow b = c \quad \textit{und} \quad a \cdot b = a \cdot c \Longrightarrow b = c$$

solange $a \neq 0$.

In Anlehnung an diesen Satz bezeichnet man die erste der beiden Verknüpfungen in einem Ring meist auch als Addition und die zweite als Mulitplikation, obwohl sie mit der Addition und Multiplikation von Zahlen nicht viel gemein haben müssen. Und natürlich stammt der Satz *nicht* vom Mathematiker Adam Riese (1492 - 1559), aber ich finde die Sprechweise so nett.

Beweis*. Wieder ist der Beweis Teil der Analysisvorlesung und er steht hier nur der Vollständigkeit halber.

Es gibt viele Einzelpunkte, keiner von ihnen schwer. Fangen wir etwa mit der Assoziativität der Addition an. Hierzu betrachten wir

$$A = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N}\colon (m+n)+k = m+(n+k)\}$$

Dann gilt $0 \in A$ weil

$$(m+n)+0 = m+n = m+(n+0).$$

Und ist $k \in A$ so folgt

$$(m+n)+s(k) = s((m+n)+k) = s(m+(n+k)) = m+s(n+k) = m+(n+s(k)).$$

Dann die Neutralität von 0: $m+0 = m$ gilt per Definition. Für die andere Richtung betrachte man

$$B = \{k \in \mathbb{N} \mid 0+k = k\}$$

dann gilt $0 \in B$ und ist $k \in B$, dann rechnen wir

$$0+s(k) = s(0+k) = s(k).$$

Für die Kommutativität der Addition brauchen wir zunächste eine Hilfsaussage: Nämlich, dass immer $s(k)+m = s(k+m)$ gilt. Hierfür betrachten wir

$$C = \{m \in \mathbb{N} \mid \forall k \in \mathbb{N}\colon s(k)+m = s(k+m)\}$$

Dann gilt $0 \in C$ wegen Neutralität und ist $m \in C$, so rechnen wir

$$s(k)+s(m) = s(s(k)+m) = s(s(k+m)) = s(k+s(m))$$

also $s(m) \in C$. Für die Kommutativität betrachte nun

$$D = \{k \in \mathbb{N} \mid \forall m \in \mathbb{N}\colon m+k = k+m\}$$

Wegen der Neutralität gilt $0 \in C$, und ist $k \in C$, so rechnen wir

$$m+s(k) = s(m+k) = s(k+m) = s(k)+m$$

wobei der letzte Schritt die Hilfsaussage benutzt.

Damit ist $(\mathbb{N}, +, 0)$ ein kommutativer Monoid. Als nächstes weisen wir die Distributivgesetze nach: Fürs erste betrachten wir

$$E = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N}\colon (m+n)\cdot k = m\cdot k + n\cdot k\}$$

Dann gilt $0 \in E$, weil

$$(m+n)\cdot 0 = 0 = 0+0 = m\cdot 0 + n\cdot 0$$

und wenn $k \in E$ gilt, so rechnen wir

$$(m+n)\cdot s(k) = m+n+(m+n)\cdot k = m+n+m\cdot k+n\cdot k = m+m\cdot k+n+n\cdot k = m\cdot s(k)+n\cdot s(k),$$

wo wir die schon gezeigten Gesetze für die Addition benutzt haben. Für das zweite Distrubitvgesetz gehen wir ähnlich vor und betrachten

$$F = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N}\colon m\cdot(n+k) = m\cdot n + m\cdot k\}$$

Dann gilt $0 \in F$, weil

$$m\cdot(n+0) = m\cdot n = m\cdot n+0 = m\cdot n + m\cdot 0$$

und ist $k \in F$, so rechnen wir

$$m\cdot(n+s(k)) = m\cdot s(n+k) = m+m\cdot(n+k) = m+m\cdot n+m\cdot k = m\cdot n+m+m\cdot k = m\cdot n+m\cdot s(k).$$

Als nächstes zeigen wir die Rechengesetze für die Multiplikation: Für die Neutralität haben wir $n \cdot 1 = n$ schon beobachtet und für die andere Richtung betrachten wir

$$G = \{n \in \mathbb{N} \mid 1 \cdot n = n\}.$$

Dann gilt $0 \in E$ per Definition und für $n \in E$ rechnen wir

$$1 \cdot s(n) = 1 + 1 \cdot n = 1 + n = s(0) + n = s(0 + n) = s(n)$$

nach dem Hilfssatz oben. Für die Kommutativität brauchen wir noch einen Hilfssatz, nämlich, dass $0 \cdot n = 0$ gilt. Dafür betrachten wir

$$H = \{n \in \mathbb{N} \mid 0 \cdot n = 0\}$$

Es gilt $0 \in H$ per Definition, und für $n \in H$ rechnen wir

$$0 \cdot s(n) = 0 + 0 \cdot n = 0 + 0 = 0.$$

Nun betrachten wir

$$I = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} \colon m \cdot n = n \cdot m\}.$$

Dann gilt $0 \in I$ nach obigem Hilfssatz, und für $n \in I$ rechnen wir

$$m \cdot s(n) = m + m \cdot n = 1 \cdot m + n \cdot m = (1 + n) \cdot m = s(n) \cdot m.$$

Für die Assoziativität zuletzt betrachten wir

$$J = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} \colon (m \cdot n) \cdot k = m \cdot (n \cdot k)\}$$

Dann gilt $0 \in E$, weil

$$(m \cdot n) \cdot 0 = 0 = m \cdot 0 = m \cdot (n \cdot 0)$$

und ist $k \in E$ so rechnen wir

$$(m{\cdot}n){\cdot}s(k) = m{\cdot}n{+}(m{\cdot}n){\cdot}k = m{\cdot}n{+}m{\cdot}(n{\cdot}k) = m{\cdot}(n{\cdot}1){+}m{\cdot}(n{\cdot}k) = m{\cdot}(n{\cdot}1{+}n{\cdot}k) = m{\cdot}(n{\cdot}(1{+}k)) = m{\cdot}(n{\cdot}s(k))$$

Damit ist $(\mathbb{N}, \cdot, 1)$ ein Monoid und $(\mathbb{N}, +, \cdot, 0, 1)$ ein kommutativer Halbring.

Dann zeigen wir den ersten Zusatz, nämlich, dass $a + (-) \colon \mathbb{N} \to \mathbb{N}$ für alle $a \in \mathbb{N}$ injektiv ist. Dafür betrachten wir

$$K = \{a \in \mathbb{N} \mid a + (-) \colon \mathbb{N} \to \mathbb{N} \text{ ist injektiv}\}.$$

Dann gilt $0 \in K$ weil $0 + (-) = \mathrm{id}_{\mathbb{N}}$ und falls $a \in K$ ist, und $s(a) + n = s(a) + m$, so folgt

$$a + 1 + n = s(a) + n = s(a) + m = a + 1 + m$$

und damit $s(n) = 1 + n = 1 + m = s(m)$ und dann $n = m$ da s injektiv ist.

Als nächstes zeigen wir die Charakterisierung der Ordnung in Termen der Addition. Dafür müssen wir nach dem Eindeutigkeitsteil von 1.7 nur nachweisen, dass

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \colon \exists c \in \mathbb{N} \colon b = a + c\}$$

eine partielle Ordnung ist mit $nRs(n)$. Hierzu verifizieren wir zuerst, dass sie kompatibel mit den Rechenoperationen ist: Letzteres ist klar wegen $s(n) = n + 1$. Dass $a = a + 0$ für alle $a \in \mathbb{N}$ gilt, zeigt die Reflexivität, und gelten $b = a + c$ und $b' = b + d$, so gilt

$$b' = b + d = a + (c + d)$$

was die Transitivität zeigt. Die Identitivität folgt, da wir bei $b = b' + d$ und $b' = b + c$

$$b' + 0 = b' = b + c = b' + d + c$$

rechnen können. Aber da die Abbildung $b' + (-) \colon \mathbb{N} \to \mathbb{N}$ injektiv ist, folgt $d + c = 0$. Nun betrachte man

$$X = \{c \in \mathbb{N} \mid \forall d \in \mathbb{N} \colon d + c = 0 \Rightarrow d = 0\}$$

Dann gilt wegen $d = d + 0$ zumindest $0 \in X$ und ist $c \in X$, so ist $c + s(d) = s(c + d) \neq 0$ nach dem zweiten Peanoaxiom, und deshalb folgt aus $d + s(c) = 0$ alles, insbesondere auch $d = 0$, sodass $s(c) \in K$. In obiger Situation folgt also aus $d + c = 0$ erst $c = 0$, aber dann auch $d = 0$ und damit $b = b'$. Damit ist R in der Tat eine partielle Ordnung, und damit gleich $\leqslant$.

Hieraus folgt leicht die Kompatibilität der Rechenoperationen mit der Ordnung: Gilt $m \leqslant n$ gibt es ein $a \in \mathbb{N}$ mit $n = m + a$, und dann gilt $n + k = m + a + k = m + k + a$, also $n + k \leqslant m + k$ und

$$n \cdot k = (m + a) \cdot k = m \cdot k + a \cdot k,$$

also $n \cdot k \leqslant m \cdot k$ (und wegen Kommutativität auch $k + n \leqslant k + m$ und $k \cdot n \leqslant k \cdot m$). Damit ist $(\mathbb{N}, \leqslant, +, \cdot, 0, 1)$ ein total geordneter Halbring.

Zuletzt sei $a \neq 0$ und $a \cdot n = a \cdot m$. Gilt dann etwa $n \leqslant m$, also $m = n + k$ für ein $k \in \mathbb{N}$, so rechnen wir

$$a \cdot n + 0 = a \cdot n = a \cdot m = a \cdot (n + k) = a \cdot n + a \cdot k$$

so dass wegen der Injektivität von $a \cdot n + (-) \colon \mathbb{N} \to \mathbb{N}$ auch

$$0 = a \cdot k.$$

Aber das ist nur möglich, wenn $k = 0$ gilt (was den Beweis beendet). Um diese letzte Behauptung zu sehen betrachten wir

$$L = \{k \in \mathbb{N} \mid a \cdot k > 0\} \cup \{0\}.$$

Dann gilt sicherlich $0 \in L$ und ist $k \in L$, dann kann entweder $k = 0$, in welchem Falle $0 < a = a \cdot 1 = a \cdot s(0)$ folgt, und sonst

$$0 < a \cdot k \leqslant a + a \cdot k = a \cdot s(k)$$

was in jedem Falle $s(k) \in L$ bedeutet. □

1.16. Beispiel Wir kennen schon einige weitere Monoide und Halbringe:

(1) Sowohl $(\mathcal{P}(M), \subseteq, \cup, \cap, \varnothing, M)$ als auch $(\mathcal{P}(M), \subseteq, \cap, \cup, M, \varnothing)$ bilden nach 3.7 partiell geordnete kommutative Halbringe. Dass man die Addition und Multiplikation in einem Halbring vertauschen kann und wieder einen erhält ist ein eher seltenes Phänomen; solche Halbringe nennt man *boolesch (boolean)* nach dem englischen Mathematiker George Boole (1815 - 1864), der sie 1847 einführte.

(2) Sicherlich ist zum Beispiel $(\mathbb{N}, \cdot, +, 1, 0)$ *kein* Halbring, da etwa

$$(1 \cdot 1) + 3 = 4 \neq 6 = (1 \cdot 3) + (1 \cdot 3)$$

(3) In den Halbringstrukturen auf der Potenzmenge gelten die beiden Kürzungsgesetze aus 1.15 ganz und gar nicht: $A \cup B = A \cup C$ impliziert nicht $B = C$, und ähnlich für Durchschnitte.

(4) $(\mathrm{F}(M, M), \circ, \mathrm{id}_M)$ ist nach 5.5 und 5.7 ebenfalls ein Monoid. Sobald M mehr als zwei Elemente besitzt ist er nicht kommutativ.

(5) Ist $(M, *, e)$ ein Monoid und X eine Menge, so können wir $\mathrm{F}(X, M)$ ebenfalls eine Verknüpfung geben indem wir $*_X \colon \mathrm{F}(X, M) \times \mathrm{F}(X, M) \to \mathrm{F}(X, M)$ durch

$$(f *_X g)(x) = f(x) * g(x)$$

definieren. Und in der Tat ist dann $(\mathrm{F}(X, M), *_X, \mathrm{const}_e)$ ebenfalls ein Monoid. Analog gilt: Ist $(R, *, \times, e, f)$ ein (kommutativer) Halbring, so auch $(\mathrm{F}(X, M), *_X, \times_X, \mathrm{const}_e, \mathrm{const}_f)$

(6) Sind $(M, *, e)$ und $(N, \times, e)$ Monoid, so erklären wir auf $M \times N$ eine Verknüpfung durch

$$((m, n), (m', n')) \longmapsto (m * m', n * n').$$

Diese liefert wieder eine Monoidstruktur mit (e, e') als neutralem Element.

(7) Auch die ganzen, rationalen, reellen und komplexen Zahlen bilden mit ihrer Addition und Multiplikation Halbringe.

Die Zusätze in 1.15 zeigen insbesondere, dass $x > y$ impliziert $x + z > y + z$ und $x \cdot z > y \cdot z$ falls $z > 0$. Damit erhalten wir sofort:

1.17. Korollar *Es gilt*

$$a + b = 0 \Longrightarrow a = 0 \wedge b = 0 \quad \textit{und} \quad a \cdot b = 1 \Longrightarrow a = 1 \wedge b = 1.$$

für je zwei natürlich Zahlen $a, b \in \mathbb{N}$.

Die erste Behauptung haben wir auch schon im Beweis von 1.15 durchgehen müssen, aber doppelt gemoppelt hält besser.

BEWEIS. Gilt etwa $a > 0$ so folgt $a + b > 0 + b = b \geqslant 0$, und ähnlich für b. Das zeigt die erste Behauptung. Für die zweite Behauptung sei dann $a \cdot b = 1$. Wäre $a = 0$ gilt $a \cdot b = 0 \neq 1$ und ähnlich wenn $b = 0$. Gilt aber $a > 1$ und $b \geqslant 1$ so, folgt $ab > 1 \cdot b = b \geqslant 1$. Also folgt $a = 1$ und damit auch $b = 1$. □

Und wir halten noch einen Fakt über die Ordnung fest, der sich leicht aus der Charakterisierung in 1.15 ergibt:

1.18. Korollar *Es gilt*

$$\min\{m \in \mathbb{N} \mid n < m\} = n + 1$$

für jede natürliche Zahl $n \in \mathbb{N}$.

BEWEIS. Wir zeigen die Behauptung zunächst für $n = 0$: Hierfür reicht es zu prüfen, dass $\{m \in \mathbb{N} \mid 1 \leqslant m\} \cup \{0\} = \mathbb{N}$, was unmittelbar aus dem Induktionsprinzip folgt. Für allgemeines n gilt nun $n < m$ genau dann, wenn es ein $0 \neq k \in \mathbb{N}$ gibt, mit $m = n + k$. Aber aus dem gerade schon bewiesenen Fall folgt $k \geqslant 1$ und somit $m = n + k \geqslant n + 1$. □

1.19. Konstruktion Der Zusatz von 1.15 zeigt, dass

$$\{(n, m, k) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \mid n = m + k\}$$

eine Abbildung

$$-\colon \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid m \leqslant n\} \to \mathbb{N}$$

definiert, die *Subtraktion (subtraction)*. Ähnliches gilt für die Multiplikation: Zunächst überlegt man sich, dass

$$\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N}\colon m = n \cdot k\}$$

eine partielle Ordnung auf $\mathbb{N}$ ist, die *Teilbarkeit (divisibility)*, geschrieben $n \mid m$; wir haben das in den Beispielen schonmal verwendet. Einzig die Identivität ist hier etwas subtil: Gilt $m = n \cdot k$ und $n = m \cdot l$, so folgt falls $m = 0$ gilt, sicher auch $n = 0 = m$. Ist $m \neq 0$, so folgt

$$m \cdot 1 = m = n \cdot k = m \cdot l \cdot k.$$

Also zeigt der Zusatz $l \cdot k = 1$, und damit $l = 1 = k$ nach 1.17, also $n = m$.

Nach 1.15 definiert auch

$$\{(n, m, k) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \mid m \neq 0 \wedge n = m \cdot k\}$$

eine Funktion

$$/\colon \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid m \neq 0 \wedge m \mid n\} \to \mathbb{N}$$

die *Division (division)*.

In einem Monoid $(M, *, e)$ kann man auch iterierte Verknüpfungen definieren:

1.20. Konstruktion Betrachte die Abbildung

$$g\colon \mathrm{F}(\mathrm{F}(\mathbb{N}, M) \times \mathbb{N}, M) \times \mathrm{F}(\mathbb{N}, M) \times \mathbb{N} \longrightarrow M, \quad (f, h, n) \longmapsto f(h, n) * h(s(n))$$

Dann existiert nach dem allgemeinen Rekursionsprinzip genau eine Abbildung $\circledast\colon \mathrm{F}(\mathbb{N}, M) \times \mathbb{N} \to M$ mit

$$\circledast(h, n) = g(\circledast, h, n) = \circledast(h, n) * h(s(n)) \quad \text{und} \quad \circledast(h, 0) = e.$$

Informell gilt also

$$\circledast(h, n) = h(1) * h(2) * \cdots * h(n-1) * h(n);$$

das Symbol ist wirklich eine vergrößerte Version des Verknüpfungszeichen.

Ist nun I eine endliche, total geordnete Menge so gibt es laut einer Aufgabe auf dem vierten Aufgabenzettel genau eine monotone Bijektion $\tau\colon \{1, \ldots, n\} \to I$. Ist $g\colon I \to M$ nun eine Abbildung, so definieren wir

$$\tilde{g}\colon \mathbb{N} \longrightarrow M, \quad i \longmapsto \begin{cases} g(\tau(i)) & 1 \leqslant i \leqslant n \\ e & \text{sonst} \end{cases}$$

und dann

$$\ast_I g := \ast(\tilde{g}, n).$$

Das gleiche funktioniert immer noch falls I unendlich ist, aber $\{i \in I \colon g(i) \neq e\}$ endlich. In diesem Fall sagt man, dass $g(i) = e$ für *fast alle* $i \in I$.

Ähnlich wie bei Durchschnitten schreibt man häufig auch $\ast_{i\in I} g(i)$ oder ähnliches anstatt $\ast_I g$. Gilt $I = \{k \in \mathbb{N} \mid n \leqslant k \leqslant m\}$ so schreibt man auch $\ast_n^m g$ oder gar $\ast_{i=n}^m g(i)$. Und ist die Verknüpfung des Monoiden mit $+$ bezeichnet, schreibt man meist $\sum_I h$ und ist sie mit $\cdot$ bezeichnet, so schreibt man $\prod_I h$.

1.21. Beispiel (1) Ist beispielsweise $q \colon \mathbb{N} \to \mathbb{N}, x \to x \cdot x$ die Quadratur, so gelten

$$\sum_{i=4}^{7} i^2 = \sum_{4}^{7} q = 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 + 7 \cdot 7 \quad \text{and} \quad \prod_{i=4}^{7} i^2 = \prod_{4}^{7} q = 4 \cdot 4 \cdot 5 \cdot 5 \cdot 6 \cdot 6 \cdot 7 \cdot 7.$$

(2) Für einen Monoiden $(M, *, e)$ und $m \in M$ und $n \in \mathbb{N}$ setzt man

$$m^{*n} := \ast_1^n \mathrm{const}_m.$$

In den natürlichen Zahlen gilt etwa

$$n \cdot m = \sum_{i=1}^{m} n = m^{+n},$$

da beide Seiten per Konstruktion die gleiche Rekursion erfüllen. Deshalb schreibt man häufig allgemein $n \cdot m$ falls die Verknüpfung in M mit $+$ bezeichnet ist. Heißt die Verknüpfung des Monoiden $\cdot$, schreibt man meist nur n^m anstatt $n^{\cdot m}$.

(3) Im Monoiden $(\mathcal{P}(M), \cup, \varnothing)$ gilt für jede Funktion $g \colon I \to \mathcal{P}(M)$ wirklich

$$\bigcup_I g = \bigcup \mathrm{Im}_g,$$

wobei die linke Seite die iterierte Vereinigung im Sinne von 1.20 bezeichnet, und die rechte Seite die Vereinigung im Sinne von 3.5. Hierzu prüft man leicht, dass die Funktion

$$\mathrm{F}(\mathbb{N}, \mathcal{P}(M)) \times \mathbb{N} \longrightarrow \mathcal{P}(M), \quad (h, n) \longmapsto \bigcup h(\{k \in \mathbb{N}, k \leqslant n\})$$

die definieren Eigenschaften aus obiger Konstruktion erfüllt. Analoges gilt für Durchschnitte.

(4) Insbesondere gilt $A^{\cup n} = A = A^{\cap n}$ für alle $A \in \mathcal{P}(M)$ und $n \geqslant 1$.

(5) Für einen abelschen Monoiden $(M, *, e)$ hängt $*_I f$ für beliebiges $f \colon I \to M$ nicht von der Ordnung von I ab. Dies ist eine Übungsaufgabe auf dem vierten Zettel.

2. Die natürlichen Zahlen II

Die einfachste (und historisch auch erste) Art natürliche Zahlen darzustellen ist einfach mit Strichen: Also

$$1 = I, \quad 2 = II, \quad 3 = III, \quad \ldots, \quad 7 = IIIIIII, \ldots$$

was den Vorteil hat, sich nur ein Symbol merken zu müssen. Große Zahlen werden aber schnell lang. Mithilfe der iterierten Verknüfungen wollen wir uns nun zwei besseren Darstellungen von natürlichen Zahlen zuwenden. Die eine ist das Stellensystem, in dem Zahlen heutzutage üblicherweise notiert werden, die andere ist die Primfaktorzerlegung. Beide haben ihre Vor- und Nachteile und fußen auf der *Division mit Rest (division with remainder)*:

2.1. Satz *Sei $b \in \mathbb{N}$ mit $b \geqslant 1$. Dann gibt es zu jedem $n \in \mathbb{N}$ genau ein Paar $(q, r) \in \mathbb{N} \times \mathbb{N}$ mit*

$$n = q \cdot b + r \quad \textit{und} \quad r < b.$$

Insbesondere definiert

$$\{(n, r) \in \mathbb{N} \times \mathbb{N} \mid \exists q \in \mathbb{N} \colon n = q \cdot b + r \textit{ und } r < b\}$$

eine Funktion $\mathrm{rem}_b \colon \mathbb{N} \to \{k \in \mathbb{N} \colon k < b\}$.

Ebenso definiert

$$\{(n,q) \in \mathbb{N} \times \mathbb{N} \mid \exists r \in \mathbb{N}\colon n = q \cdot b + r \text{ und } r < b\}$$

eine Funktion. Man bezeichnet ihren Wert bei n häufig mit mit $\lfloor n/b \rfloor$. Man prüft leicht, dass sie die Division erweitert, also $\lfloor n/b \rfloor = n/b$ falls b ein Teiler von n ist.

Beweis. Natürlich zeigen wir das per Induktion. Sei A also die Menge aller $n \in \mathbb{N}$, für die die Behauptung stimmt. Dann gilt $0 \in A$: Sicherlich gilt $0 = 0 \cdot b + 0$, sodass $(0,0)$ ein erlaubtes Paar für 0 ist, und gilt andersherum $0 = q \cdot b + r$, so folgt nach 1.17 $q \cdot b = 0$ und $r = 0$ und dann wegen der Kürzbarkeit von b auch $q = 0$.

Ist dann $n \in A$, also etwa $n = q \cdot b + r$ mit $r < b$, so gilt sicherlich

$$n + 1 = q \cdot b + r + 1.$$

Es gilt auf jeden Fall $r + 1 \leqslant b$ nach 1.18. Gilt sogar $r + 1 < b$ so ist $(q, r + 1)$ ein erlaubtes Paar für $n + 1$. Ist andererseits $r + 1 = b$, so rechnen wir weiter

$$n + 1 = q \cdot b + b = (q + 1) \cdot b + 0$$

und finden dass $(q+1, 0)$ ein erlaubtes Paar für $n+1$ ist. Dies zeigt die Existenz einer Darstellung wie gewünscht. Zur Eindeutigkeit gelte

$$q' \cdot b + r' = n + 1 = q \cdot b + r$$

mit $r', r < b$. Betrachen wir nun etwa den Fall $q' \leqslant q$ an. Dann folgt $q' \cdot b \leqslant q \cdot b$

$$r' = q \cdot b + r - q' \cdot b = r + (q - q') \cdot b.$$

Gilt nun aber $q' < q$, so folgt $q - q' \geqslant 1$ und damit

$$r = r + (q - q') \cdot b \geqslant r + b \geqslant b,$$

was der Annahme an r widerspricht, also muss $q' = q$ sein, und genauso schließt man im Fall $q \leqslant q'$. Aber wenn $q = q'$ gilt, so folgt aus

$$q \cdot b + r = q \cdot b + r'$$

auch $r = r'$. Dies zeigt $n+1 \in A$ und dann beendet das Induktionsprinzip den Beweis: Die letzten Behauptungen folgen nämlich direkt aus den Definitionen. □

2.2. Theorem (Stellenzerlegung) *Sei $b \geqslant 2$. Dann existiert zu jedem $n \in \mathbb{N}$ genau eine Abbildung*

$$a\colon \mathbb{N} \longrightarrow \{k \in \mathbb{N} \mid k < b\},$$

mit $a(i) = 0$ für fast alle $i \in \mathbb{N}$, und derart dass

$$n = \sum_i a(i) \cdot b^i.$$

Man beobachte, dass mit a auch die Funktion $i \mapsto a(i) \cdot b^i$ für fast alle i den Wert 0 annimmt, sodass die Summe wirklich definiert ist. Die Funktion a heißt die *b-adische Entwicklung* von n.

Der genaue Ursprung des Stellensystems ist (mir zumindest) nicht bekannt; es scheint häufig immer wieder unabhängig entdeckt worden zu sein. Archimedes hatte es wohl schon um das Jahr -250 einmal gefunden, aber langsame Verbreitung fand es erst um die erste Jahrtausendwende positiver Zeit (es war unabhängig etwa in China und Kombodscha und erfunden worden). In den europäischen Raum gelang diese Erkenntnis über Arabien erst wieder im 13. Jahrhundert und im deutschen Sprachraum fand es Verbreitung durch die Bücher von Adam Riese (daher auch der Ausspruch "nach Adam Riese"). Das Stellensystem bedarf unbedingt einer expliziten Null (man betrachtete lange die natürlichen Zahlen als bei 1 beginnend) und erst mit seiner Einführung war es möglich effizient mit den natürlichen Zahlen zu rechnen, was seinen Teil zum Aufstieg der Wissenschaft in der Aufklärung geleistet hat.

Der Beweis basiert außer der Division mit Rest noch auf folgendem:

2.3. Satz (Geometrische Summenformel) *Sei* $(R, +, \cdot, 0, 1)$ *ein Halbring. Dann gilt*

$$r \cdot \left(\sum_{i=0}^{n} r^{n-i} \cdot q^i \right) + q^{n+1} = \left(\sum_{i=0}^{n} r^{n-i} \cdot q^i \right) \cdot q + r^{n+1}$$

für alle $q, r \in R$ *und* $n \in \mathbb{N}$.

Es gibt extrem viele Anwendungen dieser Formel. Die klassischste ist wohl der Fall von $r = 1$ in den natürlichen Zahlen: Hier findet man

$$\left(\sum_{i=0}^{n} q^i \right) + q^{n+1} = q \cdot \left(\sum_{i=0}^{n} q^i \right) + 1$$

Ist nun $q \geqslant 1$, so folgt durch Kürzen

$$q^{n+1} = (q-1) \cdot \left(\sum_{i=0}^{n} q^i \right) + 1$$

und daher für $q \geqslant 2$

$$\frac{q^{n+1} - 1}{q - 1} = \sum_{i=0}^{n} q^i.$$

Allein, dass $q^{n+1} - 1$ überhaupt durch $q - 1$ teilbar ist, ist wohl nur für $q = 2, 3$ offensichtlich. In diesem Fall erhält man

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Beweis. Man rechnet schnell

$$r \cdot \left(\sum_{i=0}^{n} r^{n-i} \cdot q^i \right) + q^{n+1} = \left(\sum_{i=0}^{n} r^{n+1-i} \cdot q^i \right) + q^{n+1} = r^{n+1} + \left(\sum_{i=1}^{n} r^{n+1-i} \cdot q^i \right) + q^{n+1}$$

und ebenso

$$\left(\sum_{i=0}^{n} r^{n-i} q^i \right) \cdot q + r^{n+1} = \left(\sum_{i=0}^{n} r^{n-i} q^{i+1} \right) + r^{n+1} = q^{n+1} + \left(\sum_{i=0}^{n-1} r^{n-i} q^{i+1} \right) + r^{n+1}.$$

Aber für die beiden mittleren Terme gilt

$$\sum_{i=1}^{n} r^{n+1-i} q^i = \sum_{i=0}^{n-1} r^{n-i} q^{i+1};$$

in der Tat ist linke Seite unsere Definition der rechten, da $(-) + 1 \colon \{0, \ldots, n-1\} \to \{1, \ldots, n\}$ eine monotone Bijektion ist. □

Beweis von Theorem 2.2. Zur Existenz: Natürlich per Induktion. Sei also A die Menge all derer natürlichen Zahlen die eine b-adische Entwicklung haben. Dann gilt sicherlich $0 \in A$: Wir haben $\sum \mathrm{const}_0 = 0$. Und liegt $n \in A$, etwa $n = \sum_i a_i b^i$ so sei

$$l \coloneqq \min\{i \in \mathbb{N} \mid a(i) + 1 < b\};$$

die Menge rechts ist nicht leer, da a nur für endliche viele i einen anderen Wert als 0 annimmt (und $b \geqslant 2$). Damit rechnen wir los

$$\begin{aligned} n+1 &= 1 + \sum_i a(i)b^i \\ &= 1 + \sum_{i=0}^{l-1} (b-1)b^i + a(l)b^l + \sum_{i>l} a(i)b^i \\ &= 1 + (b-1)\left(\sum_{i=0}^{l-1} b^i\right) + a(l)b^l + \sum_{i>l} a(i)b^i \\ &= b^l + a(l)b^l + \sum_{i>l} a(i)b^i \\ &= (a(l)+1)b^l + \sum_{i>l} a(i)b^i \end{aligned}$$

wobei wir in der Mitte einmal die geometrische Summenformel benutzt haben. Setzen wir also

$$\bar{a}\colon \mathbb{N} \longrightarrow \{k \in \mathbb{N} \mid k < b\}, \quad i \longmapsto \begin{cases} 0 & i < l \\ a(l)+1 & i = l \\ a(i) & l < i \end{cases}$$

So erhalten wir $\sum_i \bar{a}(i)b^i = n+1$ und damit $n+1 \in A$.

Zur Eindeutigkeit: Wir beobachten zunächst, dass der 0te Eintrag jeder b-adischen Entwicklung eindeutig bestimmt ist: Wir berechnen

$$\operatorname{rem}_b\left(\sum_i a(i)b^i\right) = \operatorname{rem}_b\left(a(0) + b\left(\sum_{i>0} a(i)b^{i-1}\right)\right) = a(0)$$

da ja in der Tat $a(0) < b$.

Sei nun $\sum_i a(i)b^i = n = \sum_i a'(i)b^i$. Betrachte dann $B = \{j \in \mathbb{N} \mid \forall i \leqslant j\colon a(i) = a'(i)\}$. Dann gilt $a(0) = \operatorname{rem}_b(n) = a'(0)$, also $0 \in B$. Und ist $j \in B$, so finden wir

$$\sum_i a(i+j+1)b^i = \sum_{j<i} a(i)b^{i-j} = \left(\sum_{j<i} a(i)b^j\right)/b^j = \left(\sum_i a(i)b^i - \sum_{i=0}^{j} a(i)b^i\right)/b^j = \left(n - \sum_{i=0}^{j} a(i)b^i\right)/b^j$$

und analog für die gestrichene Version. Da aber $\sum_{i=0}^{j} a(i)b^i = \sum_{i=0}^{j} a'(i)b^i$ per Annahme, folgt

$$\sum_i a(i+j+1)b^i = \sum_i a'(i+j+1)b^i.$$

Aber dies sind selber b-adische Entwicklungen, ergo folgt aus unserer Vorüberlegung $a(j+1) = a'(j+1)$ und damit $j+1 \in B$. Und dann schlägt das Induktionsprinzip zu. □

2.4. Beispiel Für gegebene Basis $b \geqslant 2$ bezeichnet man die zu einem $a\colon \mathbb{N} \to \{k \in \mathbb{N} \mid k < b\}$ gehörige Zahl oft mit $(a)_b$. Desweiteren, schreibt man häufig einfach die Werte von a in umgekehrter Reihung ohne Kommas hintereinander und lässt die Nullen am Anfang weg: Etwa

$$(425)_7 = 5 + 2 \cdot 7 + 4 \cdot 7^2$$

$$(10)_b = b, \quad (11)_b = b+1, \quad \text{und} \quad (110)_b = b + b^2$$

$$(1s(9))_{s(s(9))} = s(9) + s(s(9)) = 2 \cdot s(9) + 1$$

Besonders häufig ist natürlich die Basis $b = s(9)$, man spricht vom *Dezimalsystem* und für genau diesen Fall haben wir genügend Symbole eingeführt. Man kürzt diesem Fall noch weiter ab, indem man die Basis aus der Notation weglässt. Also etwa

$$10 = s(9), \quad 11 = s(s(9)) \quad \text{und} \quad 21 = 2 \cdot 10 + 1.$$

Eine weiteres häufiges Beispiel ist $b = 2$ mit den Anfangszahlen

$$(0)_2 = 0, \quad (1)_2 = 1, \quad (10)_2 = 2, \quad (11)_2 = 3, \quad (100)_2 = 4, \quad (101)_2 = 5, \ldots$$

Dieses *Binärsystem* ist in der Informatik sehr viel gebräuchlicher als das Dezimalsystem.

Im Stellensystem ist es sehr leicht die Größe zweier Zahlen zu vergleichen und sowohl Addition als auch Multiplikation sind nicht schwer durchzuführen (das haben sie wahrscheinlich bis zum Verrecken in der Schule geübt). Es ist jedoch bis heute keine vollständige Beschreibung der Teilbarkeitsrelation im Stellensystem bekannt (und hierauf basiert die Sicherheit vieler Kryptographieverfahren). Um sich das Problem zu vergegenwärtigen, versuch sie einmal per Hand herauszufinden, ob

$$1893742374923487 \quad \text{durch} \quad 49381$$

teilbar oder gar eine Primzahl ist.

Kommen wir nun zur zweiten Art natürliche Zahlen darzustellen, bei der genau diese Eigenschaft sehr leicht abzulesen ist. Hierfür brauchen wir:

2.5. Definition Eine Zahl $p \in \mathbb{N}$, $p \neq 0, 1$, heißt *Primzahl (prime number)*, falls sie nur durch 1 und p teilbar ist.

Der folgende Satz heißt manchmal auch der *Fundamentalsatz der Arithmetik*.

2.6. Theorem (Primfaktorzerlegung) *Für jede natürliche Zahl $n \in \mathbb{N}$, $n \neq 0$, gibt es genau eine Abbildung $m\colon \{\text{Primzahlen}\} \to \mathbb{N}$ mit $m(p) = 0$ für fast alle $p \in \mathbb{N}$ prim, so dass*

$$n = \prod_{p \text{ prim}} p^{m(p)}.$$

Man beachte, dass die Funktion $p \mapsto p^{m(p)}$ für fast alle i den Wert 1 annimmt, sodass obiges Produkt wohldefiniert ist. Zum Beweis brauchen wir wieder noch etwas Hilfe:

2.7. Satz (Lemma des Euklid, -400) *Ist $p \in \mathbb{N}$ und $p \mid n \cdot m$, so folgt $p \mid n$ oder $p \mid m$.*

Allgemeiner folgt hieraus per Induktion (über k), dass wenn p ein beliebiges Produkt $\prod_{i=0}^{k} n_i$ teilt, dann teilt p schon eins der n_i: Die Aussage ist sicher wahr für $k = 0$ (dann kann p so ein Produkt nicht teilen), und teilt

$$\prod_{i=0}^{k+1} n_i = \left(\prod_{i=0}^{k} n_i\right) \cdot n_{k+1},$$

so teilt p nach obigen Lemma n_{k+1} oder $\prod_{i=0}^{k} n_i$ und hier schlägt die Induktionshypothese zu.

Beweis. Nehmen wir also an, dass p nicht n teilt und zeigen, dass dann $p \mid m$. Hierfür betrachten wir

$$A = \{i \in \mathbb{N} \mid i \neq 0 \wedge p \mid i \cdot m\}.$$

Die Menge A ist nicht leer (etwa gelten ja $n \in A$), und hat deshalb ein kleinstes Element $k \in A$ nach 1.7. Wir zeigen nun dass k jedes Element aus A teilt. Aber es gilt auch $p \in A$, also muss entweder $k = p$ oder $k = 1$ gelten. Aber es gilt $n \in A$, und p teilt n per Annahme nicht. Also muss $k = 1$ gelten, und damit teilt p nach Definition von A wie gewünscht m.

Zum Beweis der Behauptung sei $x \in A$. Dann können wir nach 2.1 $x = q \cdot k + r$ schreiben mit $r < k$. Per Definition gilt $x \cdot m = p \cdot a$ und $k \cdot m = p \cdot b$ für irgendwelche $a, b \in \mathbb{N}$, und wegen $x \geqslant k$ folgt $a \geqslant b$. Aber dann gilt

$$r \cdot m = (x - q \cdot k) \cdot m = x \cdot m - q \cdot k \cdot m = p \cdot a - q \cdot p \cdot b = p \cdot (a - q \cdot b).$$

Aber weil $r < k$ gilt, kann nicht $r \in A$ gelten, was $r = 0$ erzwingt und die Behauptung beweist. □

Beweis von Theorem 2.6. Betrachte $A = \{n \in \mathbb{N} \mid \forall 0 < i \leqslant n\colon i \text{ hat genau eine Primfaktorzerlegung}\}$. Dann gilt offenbar $0 \in A$. Ist nun $n \in A$, so unterscheiden wir drei Fälle. Ist $s(n)$ selbst prim, so gilt $s(n) \in A$ bezeugt von

$$p \longmapsto \begin{cases} 0 & p \neq s(n) \\ 1 & p = s(n) \end{cases},$$

und per Definition von Primzahlen kann es keine weitere Zerlegung von $s(n)$ geben. Ist $n = 0$, so haben wir $s(0) = 1 \in A$ bezeugt von $m = \text{const}_0$, und nach 1.17 kann es keine weitere Zerlegung geben. Ansonsten muss $s(n) = k \cdot l$ für $k, l \in \mathbb{N}$ mit $1 < k, l < n$. Dann haben aber k und l Primfaktorzerlegungen, etwa

$$k = \prod_{p \text{ prim}} p^{m(p)} \quad \text{und} \quad l = \prod_{p \text{ prim}} p^{m'(p)}$$

Es folgt, dass

$$s(n) = k \cdot l = \left(\prod_{p \text{ prim}} p^{m(p)}\right) \cdot \left(\prod_{p \text{ prim}} p^{m'(p)}\right) = \prod_{p \text{ prim}} p^{m(p)+m'(p)}.$$

Dies zeigt die Existenz einer Primfaktorzerlegung von $s(n)$. Nun noch zur Eindeutigkeit: Gilt

$$\prod_{p \text{ prim}} p^{m(p)} = s(n) = \prod_{p \text{ prim}} p^{m'(p)}$$

so sei q die kleinste Primzahl mit $m(q) \neq 0$ (wäre $m(q) = 0$ für alle Primzahlen q, so wäre $s(n) = 1$, aber den Fall haben wir schon abgeschlossen). Dann gilt $q \mid s(n)$. Nach Euklid's Lemma (oder dem Kommentar direkt danach) muss es dann zunächst einen Faktor $p^{m'(p)}$ der rechten Seite geben den q teilt. Das bedeutet nach 1.17 natürlich $m'(p) > 0$. Ist $m'(p) = 1$ bedeutet das $p \mid q$, und falls $m'(p) > 1$, so liefert eine zweite Anwendung von Euklid's Lemma ebenfalls $q \mid p$. Aber da p prim ist, bleibt also nur $q = p$. Also $m'(q) \geqslant 1$. Es folgt dann

$$\prod_{p \text{ prim}} p^{\bar{m}(p)} = s(n)/q = \prod_{p \text{ prim}} p^{\bar{m}'(p)}$$

für

$$\bar{m} \colon \{\text{Primzahlen}\} \longrightarrow \mathbb{N}, \quad p \longmapsto \begin{cases} m(p) & p \neq q \\ m(q) - 1 & p = q \end{cases}$$

und analogem $\bar{m}'$. Aber dies sind beides Primfaktorzerlegungen von$s(n)/q$ und weil $0 \neq s(n)/q < s(n)$ gibt es hiervon nur eine. Also folgt $\bar{m} = \bar{m}'$ und damit $m = m'$. Das zeigt $s(n) \in A$ und das Induktionsprinzip liefert die Behauptung. □

3. Die ganzen Zahlen

Wir haben in 1.19 gesehen, dass die Subtraktion in den natürlichen Zahlen nur manchmal funktioniert, etwa kann man nicht $2 - 4$ bilden. Die Idee der ganzen Zahlen ist es dies zu beheben. Zunächst etwas Terminologie:

3.1. Definition Ist $(M, *, e)$ ein Monoid, so heißt ein $m \in M$ eine *Einheit (unit)* falls es ein $m' \in M$ gibt mit

$$m' * m = e = m' * m.$$

So ein m' heißt *invers* zu m. Ein Monoid in dem jedes Element ein Inverses besitzt, heißt eine *Gruppe (group)*, und ein Halbring in dem die Addition eine Gruppenstruktur liefert heißt ein *Ring (ring)*.

So ein m' ist eindeutig bestimmt, da

$$m' = e * m' = m'' * m * m' = m''$$

wann immer m'' ebenfalls inverse zu m ist. Man schreibt m^{-1} (oder genauer m^{*-1}, aber das sieht oft sehr seltsam aus) für das Inverse. Wird die Vernüpfung als + geschrieben so schreibt man $-m$ anstatt dem nun wirklich sehr seltsamen m^{+-1}.

3.2. Beispiel
(1) In jedem Monoiden $(M, *, e)$ ist e eine Einheit mit $e^{-1} = e$.
(2) In $(\mathbb{N}, +, 0)$ und $(\mathbb{N}, \cdot, 1)$ sind nur 0 bzw. 1 Einheiten nach 1.17.
(3) In $(\mathrm{F}(M, M), \circ, \mathrm{id}_M)$ ist ein Element f genau dann eine Einheit, wenn f bijektiv ist nach 5.9 und auch die Definition von f^{-1} dort passt zu der gerade gegebenen.

(4) Ist u eine Einheit in $(M, *, e)$, so ist im Wesentlichen per Definition auch u^{-1} eine Einheit und $(u^{-1})^{-1} = u$.
(5) ist $(M, \leqslant, *, e)$ ein partiell geordneter Monoid und $u, v \in M$ sind Einheiten, so gilt $u \leqslant v$ genau dann, wenn $v^{-1} \leqslant u^{-1}$.
(6) Sind u, v Einheiten in $(M, *, e)$ so ist auch $u * v$ eine Einheit und $(u * v)^{-1} = v^{-1} * u^{-1}$.

3.3. Beobachtung Sei $(M, *, e)$ ein Monoid. Dann sind äquivalent:

(1) $(M, *, e)$ ist eine Gruppe.
(2) Zu jeden $m, n \in M$ genau ein $k \in M$ gibt mit $m * k = n$.
(3) Zu jedem $m \in M$ gibt es ein $k \in M$ mit $m * k = e$.
(4) Zu jeden $m, n \in M$ genau ein $k \in M$ gibt mit $k * m = n$.
(5) Zu jedem $m \in M$ gibt es ein $k \in M$ mit $k * m = e$.

In diesem Fall definieren

$$\{(n, m, k) \in M \times M \times M \mid n = m * k\}$$

und

$$\{(n, m, k) \in M \times M \times M \mid n = k * m\}$$

Funktionen

$$M \times M \to M, \quad (n, m) \longmapsto m^{-1} * n \quad \text{und} \quad n * m^{-1}.$$

Ist M kommutativ so stimmt diese natürlich überein.

Der Monoid $(M, *, e)$ ist also eine Gruppe genau dann, wenn das Analog von Subtraktion bzw. Division (je nach Namen der Verknüpfung) uneingeschränkt möglich ist.

Beweis: Wir zeigen als erstes (1) $\Rightarrow$ (2): Zur Existenz nehme man einfach $k = m^{-1} * n$. Zur Eindeutigkeit rechnet man

$$k = e * k = m^{-1} * m * k = m^{-1} * n = m^{-1} * m * k' = e * k' = k'$$

wann immer die mittleren beiden Gleichungen gelten. Natürlich gilt (2) $\Rightarrow$ (3). Und dann (3) $\Rightarrow$ (1): Wir müssen zeigen, dass auch $k * m$ gilt. Per Annahme gibt es aber zumindest ein $n \in M$ mit $k * n = e$. Dann rechnen wir aber

$$m = m * e = m * k * n = n.$$

Die Implikationen (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1) sind vollständig analog. □

Einen Begriff von Zahl zu finden in dem man uneingeschränkt subtrahieren kann, ist die Grundidee der Erweiterung zu den ganzen Zahlen. Zur Formalisierung dieser Idee benötigen wir:

3.4. Definition Sind $(M, *, e)$ and $(M', *', e')$ Monoide, so heißt eine Funktion $f\colon M \to N$ ein *Monoidhomomorphismus* falls

$$f(e) = e' \quad \text{and} \quad f(m * n) = f(m) *' f(n)$$

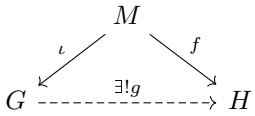
für alle $m, n \in M$. Sind $(R, *, \times, e, f)$ und $(R', *', \times', e', f')$ (Halb-)Ringe, so heißt $f\colon R \to R'$ ein *(Halb-)Ringhomomorphismus*, falls f sowohl ein Monoidhomomorphismus $(R, *, e) \to (R', *', e')$ als auch $(R, \times, f) \to (R', \times', f')$ ist.

Ein Homomorphismus heißt ein *Mono-*, *Epi-* bzw. *Isomorphismus*, falls er injektiv, surjektiv bzw. bijektiv ist.

Wir formalisieren nun die Idee einer kleinsten Erweiterung zu einer Gruppe:

3.5. Definition Ist M ein Monoid, so heißt ein Paar bestehend aus einer Gruppe G und einem Monoidmonomorphismus $\iota M \to G$ eine *Gruppenvervollständigung (group completion)* von M, falls es für jede Gruppe H und jeden Monoidmonomorphismus $f\colon M \to H$ genau einen Monoidmonomorphismus $g\colon G \to H$ gibt, derart dass $g \circ \iota = f$.

Man zeichnet die Bedingung oft als



Wir zeigen als nächstes Eindeutigkeit und Existenz von Gruppenvervollständigungen:

3.6. Lemma (Eindeutigkeit von Gruppenvervollständigungen) *Sind $\iota\colon M \to G$ und $\iota'\colon M \to G'$ Gruppenvervollständigungen von M so gibt es genau einen Monomorphismus $f\colon G \to G'$ mit $f \circ \iota = \iota'$. Dieser ist ein Isomorphismus.*

Beweis. Die Existenz und Eindeutigkeit von f folgen direkt aus der Definition. Wir konstruieren nun eine Umkehrabbildung zu f. Nämlich gibt es (indem man die Rollen von ι und ι' vertauscht auch genau einen Monoidmonomorphismus $g\colon G' \to G$ mit $g \circ \iota' = \iota$. Aber $f \circ g\colon G' \to G'$ erfüllt

$$f \circ g \circ \iota' = f \circ \iota = \iota' = \mathrm{id}_{G'} \circ \iota',$$

sodass der Eindeutigkeitsteil der Definition von Gruppenvervollständigungen $f \circ g = \mathrm{id}_{G'}$ liefert und damit, dass f surjektiv ist. □

Dies Lemma ist völlig analog zur Eindeutigkeit der natürlichen Zahlen. Wir sprechen von nun an also wieder missbräuchlich von *der* Gruppenvervollständigung von M und bezeichnen sie mit M^{grp}, sofern sie existiert, oder M_*^{grp} falls die Verknüpfung $*$ auf M nicht aus dem Kontext klar ist.

3.7. Theorem (Existenz von Gruppenvervollständigungen) *Ein abelscher Monoid $(M, +, 0)$ besitzt eine Gruppenvervollständigung genau dann, wenn jedes Element in M gekürzt werden kann, also wenn für alle $m, n, k \in M$ gilt, dass $k + m = k + n \Rightarrow m = n$.*

Es gelten Verallgemeinerungen dieses Satzes auf nicht abelsche und nicht kürzbare Monoide, aber wir wollen uns mit dieser Version begnügen. Sie reicht nämlich um zu setzen:

3.8. Definition Wir definieren die abelsche Gruppe der *ganzen Zahlen (integers)* als $\mathbb{Z} := \mathbb{N}_+^{\mathrm{grp}}$.

Da das Bild von $\iota\colon \mathbb{N} \to \mathbb{Z}$ zusammen mit $0 \in \mathbb{Z}$ und der Funktion $(-) + 1$ wieder ein System natürlicher Zahlen bildet, werden wir 'die' natürlichen Zahlen immer als Teilmenge von $\mathbb{Z}$ auffassen, und ι aus der Notation unterdrücken.

Kommen wir nun zum Beweis von Theorem 3.7. Die Notwendigkeit der Kürzbarkeit ist schon in Beobachtung 3.3 enthalten. Um sie beim Aufbau der rationalen Zahlen wiederverwenden zu können, geben wir die Konstruktion von Gruppenvervollständigungen in etwas größerer Allgemeinheit:

3.9. Konstruktion Es sei $(M, +, 0)$ ein abelscher Monoid und $W \subseteq M$ eine Teilmenge mit

(1) $m, m' \in W \Rightarrow m + m' \in W$
(2) $0 \in W$
(3) jedes Element in $k \in W$ kann gekürzt werden, also für alle $m, m' \in M$ gilt $k + m = k + m' \Rightarrow m = m'$.

Dann konstruieren wir einen neuen Monoid $\mathrm{K}(M, W)$ zusammen mit einem Monoidhomomorphismus (M^{grp} erhalten wir für $W = M$). Die Idee ist, dass $\mathrm{K}(M, W)$ aus 'formalen' Differenzen $m - w$ besteht, mit denen wir rechnen indem man $(m - w) + (m' - w') := (m + m') - (w + w')$. Um das zu formalisieren müssen wir uns überlegen, wann solche formalen Differenzen übereinstimmen sollen (sicherlich soll ja in $\mathbb{N}^{\mathrm{grp}}$ etwa $2 - 3$ das gleiche Element bezeichnen wie $5 - 6$). Genau hierfür können wir Äquivalenzrelationen benutzen.

Auf $M \times W$ führen wir die Relation

$$(m, w) \sim (m', w') :\Longleftrightarrow m + w' = m' + w.$$

Sie ist eine Äquivalenzrelation: Reflexivität und Symmetrie sind hoffentlich klar. Für die Transitivität rechnet man bei

$$m + w' = m' + w \quad \text{und} \quad m' + w'' = m'' + w'$$

dass

$$m + w' + w'' = m' + w + w'' = m'' + w' + w''.$$

Nun kürze man w'' um $(m, w) \sim (m'', w'')$ zu erhalten. Die Äquivalenzklassen von $\sim$ benutzen wir nun genau als die Definition der 'formalen Differenz' oben. Es gilt etwa $[(0,0)]_\sim = \{(m,w) \in M \times W \mid m = w\}$.

Als nächstes konstruieren wir die neue Verknüpfung. Nach Beispiel 1.16 ist $M \times W$ ist ein Monoid durch

$$(m, w) + (m', w') = (m + m', w + w'),$$

mit neutralem Element $(0,0)$ und offenbar definiert $m \mapsto (m, 0)$ definiert einen Monoidhomomorphismus $M \to M \times W$.

Diese Struktur passt mit der Äquivalenzrelation in folgendem Sinne zusammen: Gelten $(m, w) \sim (m', w')$ und $(n, v) \sim (n', v')$ so folgt $(m, w) + (n, v) \sim (m', w') + (n', v')$; man sagt $\sim$ ist eine *Kongruenzrelation* auf $M \times W$. Eine weitere Aufgabe ist es zu zeigen, dass in dieser Situation die Abbildung $+\colon (M \times W) \times (M \times W) \to M \times W$ zu einer Abbildung

$$+\colon (M \times W)/\!\sim \times\, (M \times W)/\!\sim \longrightarrow M \times W$$

absteigt, derart dass $[(m, w)]_\sim + [(m', w')]_\sim = [(m+m, w+w')]_\sim$ für alle $(m, w), (m', w') \in M \times W$ gilt. Diese Abbildung macht die Menge der Äquivalenzklassen $(M \times W)/\!\sim\, =: \mathrm{K}_+(M, W)$ mit neutralem Element $[(0,0)]$.

Insbesondere ist

$$[-]_\sim \colon M \times W \to \mathrm{K}_+(M, W)$$

ein Monoidhomomorphismus und damit auch $\iota\colon M \to \mathrm{K}_+(M, W)$.

Von hier ab, kürzen wir $\mathrm{K}_+(M, W)$ erstmal einfach zu $\mathrm{K}(M, W)$ ab; die relevant Verknüpfung sei immer mit $+$ bezeichnet.

3.10. Satz *Für $W \subseteq M$ wie in Konstruktion 3.9 ist $\iota\colon M \to \mathrm{K}(M, W)$ injektiv und für jedes $w \in W$ ist $\iota(w) = [(w, 0)]_\sim$ eine Einheit in $\mathrm{K}(M, W)$ mit $-[(w, 0)]_\sim = [(0, w)]_\sim$.*

Weiter gibt es zu jedem Monoidhomomorphismus $f\colon M \to H$ mit der Eigenschaft, dass $f(w)$ eine Einheit für jedes $w \in W$ ist, genau einen Monoidomomorphimus $g\colon \mathrm{K}(M, W) \to H$ mit $g \circ \iota = f$. Dieser ist injektiv genau dann, wenn f es ist.

Im Falle $M = W$ beweist dies insbesondere Theorem 3.7: Es bleibt nur zu beobachten, dass $M^{\mathrm{grp}} = \mathrm{K}(M, M)$ wirklich eine Gruppe ist: Aber per Konstruktion ist jedes Element aus $\mathrm{K}(M, M)$ von der Form $\iota(m) - \iota(n)$ für $m, n \in M$ und hierzu ist $\iota(n) - \iota(m)$ ein Inverses (oder mit anderen Worten $[(n, m)]_\sim$ ist invers zu $[(m, n)]_\sim$).

Im anderen Extremfall, dass W vollständig aus Einheiten besteht, folgt dass $\iota\colon M \to \mathrm{K}(M, W)$ ein Isomorphismus ist: In diesem Falle ist ja $H = M$ und $f = \mathrm{id}_M$ eine erlaubte Wahl in obigem Satz. Der resultierende Homomorphismus $g\colon \mathrm{K}(M, W) \to M$ ist dann nach 5.14 surjektiv, also bijektiv und damit ist in diesem Fall auch $\iota = g^{-1}$ bijektiv.

Beweis. Gilt etwa $\iota(m) = \iota(m')$, also $[(m, 0)] = [(m', 0)]$, so folgt nach 6.4 $(m, 0) \sim (m', 0)$ mit anderen Worten $m + 0 = m' + 0$, also $m = m'$. Das zeigt, dass ι injektiv ist. Für die zweite Behauptung rechnen wir

$$[(w, 0)]_\sim + [(0, w)]_\sim = [(w, w)]_\sim = [(0, 0)]_\sim.$$

Ist nun $f\colon M \to H$ wie im Satz gegeben, wo $(H, *, e)$ eine Monoid ist, so definieren wir $g\colon K(M, W) \to H$ wie folgt: Zunächst setzen wir

$$\tilde{g}\colon M \times W \longrightarrow H, \quad (m, w) \longmapsto f(m) * f(w)^{-1}.$$

Dies ist ein Monoidhomomorphismus: Es gilt $\tilde{g}(0,0) = e * e^{-1} = e * e = e$ und

$$\begin{aligned}\tilde{g}((m,w)+(m',w')) &= \tilde{g}(m+m', w+w')\\ &= f(m+m') * f(w+w')^{-1}\\ &= f(m+m') * f(w'+w)^{-1}\\ &= f(m) * f(m') * (f(w') * f(w))^{-1}\\ &= f(m) * f(m') * f(w)^{-1} * f(w')^{-1}\end{aligned}$$

Nun beobachten wir

$$\begin{aligned}f(m') * f(w)^{-1} &= e * f(m') * f(w)^{-1}\\ &= f(w)^{-1} * f(w) * f(m') * f(w)^{-1}\\ &= f(w)^{-1} * f(w+m') * f(w)^{-1}\\ &= f(w)^{-1} * f(m+w') * f(w)^{-1}\\ &= f(w)^{-1} * f(m') * f(w) * f(w)^{-1}\\ &= f(w)^{-1} * f(m') * e\\ &= f(w)^{-1} * f(m')\end{aligned}$$

Einsetzen liefert

$$\tilde{g}((m,w)+(m',w')) = f(m) * f(w)^{-1} * f(m') * f(w')^{-1} = \tilde{g}(m,w) * \tilde{g}(m',w').$$

Desweiteren gilt $(m,w) \sim (m',w') \Rightarrow \tilde{g}(m,w) = \tilde{g}(m',w')$: Ist $m + w' = m' + w$, so folgt $f(m) * f(w') = f(m') * f(w)$ und damit

$$\begin{aligned}\tilde{g}(m,w) &= f(m) * f(w)^{-1}\\ &= f(m) * e * f(w)^{-1}\\ &= f(m) * f(w') * f(w')^{-1} * f(w)^{-1}\\ &= f(m') * f(w) * f(w')^{-1} * f(w)^{-1}\\ &= f(m') * f(w) * (f(w) * f(w'))^{-1}\\ &= f(m') * f(w) * f(w+w')^{-1}\\ &= f(m') * f(w) * f(w'+w)^{-1}\\ &= f(m') * f(w) * (f(w') * f(w))^{-1}\\ &= f(m') * f(w) * f(w)^{-1} * f(w')^{-1}\\ &= f(m') * e * f(w')^{-1}\\ &= f(m') * f(w')^{-1}\\ &= \tilde{g}(m',w')\end{aligned}$$

Dann folgt aus einer Aufgabe auf dem dritten Zettel, dass $\tilde{g}$ eine Abbildung

$$g\colon \mathrm{K}(M,W) \longrightarrow H$$

induziert mit $g([m,w]_\sim) = \tilde{g}(m,w)$. Man prüft leicht, dass diese immer noch ein Monoidhomomorphismus ist, was den Existenzbeweis für g beendet. Zur Eindeutigkeit sei g' ein weiterer Homomorphismus mit $g' \circ \iota = f$. Dann rechnen wir

$$\begin{aligned}g'([m,w]_\sim) = g'([(m,0)] + [(0,w)]) = g'(\iota(m)) * g'(-\iota(w))\\ = f(m) * g'(\iota(w))^{-1} = f(m) * f(w)^{-1} = g([m,w]_\sim).\end{aligned}$$

Zuletzt zur Injektivität: Ist g injektiv, so folgt, dass auch f injektiv ist, nach einer Aufgabe vom dritten Zettel. Ist andersherum f injektiv, und $f(m) * f(w)^{-1} = f(m') * f(w')^{-1}$, so folgt

$$f(m+w') = f(m) * f(w') = f(m) * e * f(w') = f(m) * f(w)^{-1} * f(w) * f(w')$$

$$= f(m') * f(w')^{-1} * f(w') * f(w) = f(m') * e * f(w) = f(m') * f(w') = f(m'+w),$$

und damit nach der Injektivität von f auch $m+w = m'+w'$, also $[(m,w)]_\sim = [(m',w')]_\sim$. □

Natürlich kann man ganze Zahlen auch ordnen und multiplizieren:

3.11. Konstruktion Ist M ein durch $\leqslant$ total geordneter Monoid, so definieren wir auf $\mathrm{K}(M,W)$ eine Relation durch

$$E \leqslant E' :\Longleftrightarrow \forall (m,w) \in E, (m',w') \in E' \colon m + w' \leqslant m' + w$$

Es ist leicht zu sehen, dass dies wieder eine totale Ordnung ist: Reflexivität folgt direkt aus der Definition von $\sim$ und Transitivität folgt genau wie die von $\sim$. Für die Identitivität sei $(m,w) \in E$ und $(m',w') \in E$. Dann folgt aus $E \leqslant E'$, dass $m + w' \leqslant m' + w$ und aus $E' \leqslant E$, dann $m' + w \leqslant m + w'$. Da $\leqslant$ identitiv ist, erhalten wir also $(m,w) \sim (m',w')$ und damit $E = E'$. Die Totalität folgt zum Schluss direkt aus der von $\leqslant$. Weiterhin gilt offensichtlich $m \leqslant m'$ genau dann wenn $[(m,0)] \leqslant [(m',0)]$ was zeigt, dass $\iota \colon M \to \mathrm{K}(M,W)$ monoton ist.

3.12. Konstruktion Trägt M noch eine Multiplikation $\cdot$ mit neutralem Element 1, die M zu einem Halbring machen, so können wir versuchen eine neue Multiplikation auf $\mathrm{K}(M,W)$ zu definieren: Da $[(m,w)]$ die formale Differenz $m-w$ darstellen soll, und dann besser $(m-w)(m'-w') = (mm'+ww') - (mw'+m'w)$ gelten sollte, müssen wir hierfür noch fordern, dass $w \cdot m \in W$ für alle $m \in M$ und $w \in W$. Dann definieren wir

$$\cdot \colon (M \times W) \times (M \times W) \longrightarrow M \times W, \quad (m,w),(m',w') \mapsto (m \cdot m' + w \cdot w', m \cdot w' + w \cdot m')$$

Man überprüft leicht, dass

$$\begin{aligned}((m,w) \cdot (m',w')) \cdot (m'',w'') &= (m \cdot m' \cdot m'' + w \cdot w' \cdot m'' + m \cdot w' \cdot w'' + m' \cdot w \cdot w'',\\ &\quad m \cdot m' \cdot w'' + w \cdot w' \cdot w'' + m \cdot w' \cdot m'' + w \cdot m' \cdot m'')\\ &= (m,w) \cdot ((m',w')) \cdot (m'',w'')\end{aligned}$$

Ebenso, dass $(1,0)\cdot(m,w) = (1\cdot m+0\cdot w, 1\cdot w+0\cdot m) = (m,w)$ and similarly $(m,w)\cdot(0,1) = (m,w)$. Mit anderen Worten: $\mathrm{K}(M,W)$ ist ein Monoid unter $\cdot$ mit neutralem Element $(1,0)$. Ähnlich prüft man leicht auch die Distributivgesetze und $(0,0)\cdot(m,w) = (0,0) = (m,w)\cdot(0,0)$, sodass $(\mathrm{K}(M,W),+,\cdot,(0,0),(1,0))$ wieder ein Halbring ist. Desweiteren ist $\sim$ auch bezüglich dieser Multiplikation auf $M \times M$ eine Kongruenzrelation (und das ist eine Übungsaufgabe auf dem sechsten Zettel), sodass wir eine Multiplikation

$$\cdot \colon \mathrm{K}(M,W) \times \mathrm{K}(M,W) \to \mathrm{K}(M,W)$$

erhalten. Per Konstruktion ist dann $(\mathrm{K}(M,W),+,\cdot,(0,0),(1,0))$ ein Ring und $\iota \colon M \to \mathrm{K}(M,W)$, wegen $(m,0)\cdot(m',0) = (m\cdot m',0)$ ein Halbringhomomorphismus. Man sieht auch sofort, dass $\mathrm{K}(M,W)$ kommutativ ist genau dann, wenn die Multiplikation von M es ist.

3.13. Satz *Sei $(M,+,0)$ ein kommutativer Monoid und $W \subseteq M$ wie in 3.9.*

1. *Macht dann $\leqslant$ den Monoid M zu einem total geordneten Monoiden, so ist die in 3.11 definierte die eindeutige totale Ordnung die $\mathrm{K}(M,W)$ zu einem geordneten Monoid macht und $\iota \colon M \to \mathrm{K}(M,W)$ monoton.*
2. *Machen $\cdot \colon M \times M \to M$ und $1 \in M$ den Monoiden M zu einem Halbring, und gilt $m \cdot w \in W$ für alle $m \in M$ and $w \in W$, so ist die in 3.12 definierte die eindeutige Multiplikation die $\mathrm{K}(M,W)$ zu einem Halbring macht und $\iota \colon M \to \mathrm{K}(M,W)$ zu einem Halbringhomomorphismus.*
3. *Ist M ein total geordneter Halbring, so ist $\mathrm{K}(M,W)$ unter diesen Strukturen wieder ein geordneter Halbring, wenn gilt*

$$\forall a,b,m \in M, w \in W \colon w \leqslant m, a \leqslant b \Longrightarrow w \cdot b + m \cdot a \leqslant w \cdot a + m \cdot b$$

Diese Forderung in (3) ist insbesondere dann wahr, wenn $a \leqslant b \in M$ impliziert, dass es ein $k \in M$ gibt und $a + k = b$.

Der Fall $w = 0$ in (3) ist genau die geforderte Kompatibilität zwischen Ordnung und Mulitplikation in einem geordneten Halbring. Gilt die letzte Eigenschaft sagt man, dass $\leqslant$ eine *natürliche Ordnung* auf M ist. Insbesondere ist $\leqslant$ nach 1.15 eine natürliche Ordnung auf $\mathbb{N}$ (daher auch der Name), aber auch die Ordnung einer jeden total geordneten Gruppe ist trivialerweise natürlich. Wir erhalten in jedem Falle:

3.14. Korollar *Die abelsche Gruppe $\mathbb{Z}$ trägt genau eine totale Ordnung $\leqslant$ und eine Multiplikation $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, derart dass $(\mathbb{Z}, \leqslant, +, \cdot, 0, 1)$ ein total geordneter Ring ist und $\mathbb{N} \to \mathbb{Z}$ ein monotoner Halbringhomomorphismus.*

Beweis von Satz 3.13. Wir müssen noch zeigen, dass die Ordnung auf $\mathrm{K}(M, W)$ mit der Addition verträglich ist: Sei also $[(m', w')]_\sim \leqslant [(m'', w'')]_\sim$, das heißt $m' + w'' \leqslant m'' + w'$. Dann folgt $m + w + m' + w'' \leqslant m + w + m'' + w'$, also $[(m, w)]_\sim + [(m', w')]_\sim \leqslant [(m, w)]_\sim + [(m'', w'')]_\sim$, wie gewünscht.

Ist $\preccurlyeq$ eine zweite totale Ordnung auf $\mathrm{K}(M, W)$ wie im Theorem, dann gilt bei $m + w' \leqslant m' + w$ auch $\iota(m) + \iota(w') \preccurlyeq \iota(m') + \iota(w)$ und damit nach den Rechengesetzen für geordnete Monoide auch

$$[(m, w)]_\simeq = \iota(m) - \iota(w) = \iota(m) + \iota(w') - \iota(w') - \iota(w)$$

$$\preccurlyeq \iota(m') + \iota(w) - \iota(w') - \iota(w) = \iota(m') - \iota(w') = [(m', w')]_\sim$$

sodass $E \leqslant E' \Rightarrow E \preccurlyeq E'$ für alle $E, E' \in \mathrm{K}(M, W)$ gilt. Da aber $\leqslant$ schon total ist, erzwingt dass wegen der Identitvität von $\preccurlyeq$ schon $E \leqslant E' \Leftrightarrow E \preccurlyeq E'$.

Und ist $*$ eine zweite Multiplikation auf $\mathrm{K}(M, W)$ wie im Theorem, so rechnen wir

$$\begin{aligned}
[(m, w)]_\sim * [(m', w')]_\sim &= (\iota(m) - \iota(w)) * (\iota(m') - \iota(w')) \\
&= (\iota(m) * \iota(m') + \iota(w) * \iota(w')) - (\iota(m) * \iota(w') + \iota(w) * \iota(m')) \\
&= \iota(m \cdot m' + w \cdot w') - \iota(m \cdot w' + w \cdot m') \\
&= [(m \cdot m' + w \cdot w', m \cdot w' + w \cdot m')]_\sim \\
&= [(m, w)]_\sim \cdot [(m', w')]_\sim
\end{aligned}$$

Nun zur Kompatibilität von Ordnung und Multiplikation. Sei dann $[(0, 0)]_\sim \leqslant [(m, w)]_\sim$, also $w \leqslant m$ und $[(m', w')]_\sim \leqslant [(m'', w'')]_\sim$, also $m' + w'' \leqslant m'' + w'$. Wir rechnen

$$m \cdot m' + w \cdot w' + m \cdot w'' + w \cdot m'' = m \cdot (m' + w'') + w \cdot (w' + m'')$$

und

$$m \cdot m'' + w \cdot w'' + m \cdot w' + w \cdot m = m \cdot (m'' + w') + w \cdot (w'' + m').$$

Nehmen wir nun die Bedingung aus dem Satz an so ist der obere Ausdruck $\leqslant$ dem unteren, was per Konstruktion zu $[(m, w)]_\sim \cdot [(m', w')]_\sim \leqslant [(m, w)]_\sim \cdot [(m', w'')]_\sim$ äquivalent ist.

Gilt andersherum immer $[(m, w)]_\sim \cdot [(m', w')]_\sim \leqslant [(m, w)]_\sim \cdot [(m', w'')]_\sim$ so erhalten wir im Falle $w' = 0 = w''$ genau die Bedingung aus dem Satz.

Zuletzt zum Zusatz: Gelten etwa $b = a + k$ und $m = w + l$ so beobachten wir, dass sicherlich $k, l \geqslant 0$ gelten muss (sonst wäre ja etwa $k < 0$ und demzufolge $b = a + k < a$) und damit auch $k \cdot l \geqslant 0$. Dann rechnen wir

$$w \cdot b + m \cdot a = w \cdot (a + k) + (w + l) \cdot a = w \cdot a + w \cdot k + w \cdot a + l \cdot a$$

und

$$w \cdot a + m \cdot b = w \cdot a + (w + l) \cdot (a + k) = w \cdot a + w \cdot a + l \cdot a + w \cdot k + l \cdot k$$

und wegen der Vorüberlegung ist der obere Ausdruck in der Tat $\leqslant$ dem unterem. □

3.15. Bemerkung Nach dem Zusatz hat jeder total geordnete Ring die stärkere Eigenschaft aus 3.13 (3). Ich weiß nicht, ob sie in jedem total geordneten, kürzbaren Halbring stimmt; ich glaube aber nicht daran.

Sie gilt sicherlich nicht in jedem partiell geordneten Halbring: Etwa stimmt sie in $(\mathcal{P}(M), \subseteq, \cup, \cap, \varnothing, M)$ aber allgemein nicht in $(\mathcal{P}(M), \subseteq, \cap, \cup, M, \varnothing)$.

Damit sind die ganzen Zahlen vollends konstruiert. Wir halten zum Schluss noch einige simple Eigenschaften fest:

3.16. Beobachtung Ist $(M, \leqslant, +, 0)$ ein natürlich (insbesondere total) geordneter Monoid und $\iota\colon M \to M^{\mathrm{grp}}$ eine Gruppenvervollständigung, so gilt $m \in \mathrm{Im}(\iota)$ oder $-m \in \mathrm{Im}(\iota)$ für jedes $m \in M^{\mathrm{grp}}$, je nachdem ob $0 \leqslant m$ oder $m \leqslant 0$.

Insbesondere ist wirklich $\mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3, \dots\}$.

Beweis. Zum Beispiel nach Konstruktion von $\mathrm{K}(M, M)$ ist jedes Element von M^{grp} von der Form $\iota(n) - \iota(k)$ für $k, n \in M$. Da M total geordnet ist, gilt nun eins von $k \leqslant n$ oder $n \leqslant k$. Im ersten Falle gibt es dann ein $l \in M$ mit $n = k + l$ und damit $m = \iota(n) - \iota(k) = \iota(l)$. Im zweiten Falle gibt es ein $l \in M$ mit $k = n + l$ und damit $-m = \iota(k) - \iota(n) = \iota(l)$. □

3.17. Korollar *Gilt $n \cdot m = 1$ für $n, m \in \mathbb{Z}$ so folgt $n = 1 = m$ oder $n = -1 = m$, und gilt $n \cdot m = 0$ so folgt $n = 0$ oder $m = 0$.*

Insbesondere sind 1 und -1 die einzigen Einheiten von $(\mathbb{Z}, \cdot, 1)$.

Proof. Gilt $m, n \in \mathbb{N}$ so haben wir das schon in 1.17 bewiesen. Ist aber $m \notin \mathbb{N}$ so ist nach obiger Beobachtung $-m \in \mathbb{N}$. Ist dann $n \in \mathbb{N}$ so folgt $-m \cdot n = (-m) \cdot n \geqslant 0$ also $m \cdot n \leqslant 0 < 1$. Also gilt dann $n \notin N$, damit $-n \in \mathbb{N}$ und damit $-m = 1 = -n$.

Die andere Behauptung folgt ähnlich: Sind $n, m \in \mathbb{N}$ so haben wir es schon in 1.17 bewiesen. Ist $m \notin \mathbb{N}$ so folgt $-m \in \mathbb{N}$. Ist dann $n \in \mathbb{N}$ folgt immer noch $(-m) \cdot n = -m \cdot n = -0 = 0$ und damit $n = 0$ und ist $n \notin \mathbb{N}$ so gilt $-n \in \mathbb{N}$ und $(-m) \cdot (-n) = m \cdot n = 0$ und damit $0 = -n$. □

4. Die rationalen Zahlen

Ebenso wie der Übergang von den natürlichen Zahlen zu den ganzen Zahlen die Subtraktion uneingeschränkt ermöglicht, so wünschen wir uns in diesem Abschnitt eine Erweiterung der ganzen Zahlen herbei in der die Division uneingeschränkt möglich ist, bis natürlich auf die Einschränkung, dass wir nicht sinnvoll durch 0 teilen können: Für die meisten Zahlen $k \in \mathbb{Z}\backslash\{-1, 0, 1\}$ scheitert das Teilen durch k daran, dass es für gegebenes $n \in \mathbb{Z}$ keine Lösung von $m \cdot k = n$ gibt. Für $k = 0$ scheitert es mal hieran (falls $n \neq 0$), aber manchmal auch daran, dass es mehr als eine Lösung gibt $n = 0$. Daran können wir aber nichts ändern.

4.1. Definition Ein Ring $(R, +, \cdot, 0, 1)$ mit $0 \neq 1$ heißt *Schiefkörper (skew field)*, falls jedes Element $0 \neq r \in R$ eine Einheit bzgl $\cdot$ ist. Ein kommutativer Schiefkörper heißt einfach *Körper (field)*.

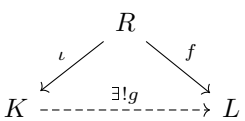
Für einen Körper K gibt es also eine wohldefinierte Abbildung

$$-/-\colon K \times K\backslash\{0\} \longrightarrow K, \quad (k, l) \mapsto k \cdot l^{-1}$$

die Division (für einen Schiefkörper gibt es zusätzlich noch die Division auf der anderen Seite).

4.2. Definition Sei R ein Ring. Dann heißt ein Paar bestehend aus einem Schiefkörper K und einem Ringmonomorphismus $\iota\colon R \to K$ ein *Quotientenkörper (field of fractions)* von R, falls es zu jedem Ringmonomorphismus $f\colon R \to L$ in einen weiteren Körper L genau einen Ringmonorphismus $g\colon K \to L$ gibt, derart dass $g \circ \iota = f$.

Man zeichnet die Bedingung wieder oft als



Wir zeigen als nächstes Eindeutigkeit und Existenz von Quotientenkörpern:

4.3. Lemma (Eindeutigkeit von Quotientenkörpern) *Sind $\iota\colon R \to K$ und $\iota'\colon R \to K'$ Quotientenkörper von R so gibt es genau einen Monomorphismus $f\colon K \to K'$ mit $f \circ \iota = \iota'$. Dieser ist ein Isomorphismus.*

Der Beweis ist beinahe wortwörtlich der gleiche wie in 3.6.

Beweis. Die Existenz und Eindeutigkeit von f folgen direkt aus der Definition. Wir konstruieren nun eine Umkehrabbildung zu f. Nämlich gibt es (indem man die Rollen von ι und ι' vertauscht auch genau einen Ringmonomorphismus $g\colon G' \to G$ mit $g \circ \iota' = \iota$. Aber $f \circ g\colon G' \to G'$ erfüllt

$$f \circ g \circ \iota' = f \circ \iota = \iota' = \mathrm{id}_{G'} \circ \iota',$$

sodass der Eindeutigkeitsteil der Definition von Quotientenkörpern $f \circ g = \mathrm{id}_{G'}$ liefert und damit, dass f surjektiv ist. □

Wir sprechen von nun an also wieder missbräuchlich von *dem* Quotientenkörper von R und bezeichnen ihn mit R^{frc}, sofern er existiert.

4.4. Theorem (Existenz von Quotientenkörpern) *Ein kommutativer Ring $(R, +, \cdot, 0, 1)$ besitzt einen Quotientenkörper genau dann, wenn jedes Element in R außer 0 bezüglich der Multiplikation gekürzt werden kann, also wenn für alle $r, s, t \in R$ gilt, dass $r \cdot t = s \cdot t \wedge t \neq 0 \Rightarrow r = s$.*

Man überlegt sich leicht, dass diese Bedingung sich noch weiter vereinfach lässt: Sie gilt genau dann wenn $a \cdot b = 0 \to a = 0 \wedge b = 0$ für alle $a, b \in R$ gilt: Auf der einen Seite ist dies der Spezialfall $s = 0$ in obiger Bedingung, und auf der anderen Seite gilt $r \cdot t = s \cdot t$ genau dann, wenn $(r - s) \cdot t = 0$, und bei $t \neq 0$ folgt dann $r - s = 0$ also $r = s$.

4.5. Definition Ein Ring mit obiger Kürzbarkeitseigenschaft heißt *Integritätsbereich (integral domain)*.

Insbesondere ist $\mathbb{Z}$ nach 3.17 ein Integegritätsbereich und:

4.6. Definition Wir definieren den Körper der *rationalen Zahlen (rational numbers)* als $\mathbb{Q} := \mathbb{Z}^{\mathrm{frc}}$.

Weitere Beispiele von Körpern folgen am Ende dieses Abschnitts. Als erstes wenden wir uns dem Beweis von Theorem 4.4 zu.

4.7. Konstruktion Hier zahlt sich jetzt die allgemeinere Konstruktion $\mathrm{K}_+(M, W)$ für kürzbare Monoide aus. Nämlich können wir uns für einen kommutativen Halbring R den Monoiden $\mathrm{K}_\cdot(R, W)$ anschauen, wobei $W \subseteq R$ wieder eine Teilmenge ist mit

(1) $m, m' \in W \Rightarrow m \cdot m' \in W$
(2) $1 \in W$
(3) jedes Element in $k \in W$ kann gekürzt werden, also für alle $m, m' \in M$ gilt $k \cdot m = k \cdot m' \Rightarrow m = m'$.

Die Annahme, dass R ein Integritätsbereich ist, besagt genau, dass $W = R \backslash \{0\}$ eine zulässige Wahl ist und wir werden in der Tat $R^{\mathrm{frc}} = \mathrm{K}_\cdot(R, R\backslash\{0\})$ setzen. Aber wieder bringt es einige Vorteile W erst einmal beliebig zu lassen und R kann ohne Einschränkungen ein Halbring (anstatt eines Rings) sein. Man stelle sich die Elemente von $\mathrm{K}_\cdot(R, R\backslash\{0\})$ als formale Quotienten r/w vor.

Aus 3.10 erhalten wir nämlich erstmal direkt, dass $\iota\colon R \to \mathrm{K}_\cdot(R, W)$ ein injektiver Homomorphismus von Monoiden ist, wenn wir R mit der Multiplikation ausstatten. Wir werden nun $K_\cdot(R, W)$ noch mit einer Addition $+$ austatten, die $(K_\cdot(R, W), +, \cdot, [(0, 1)]_\sim, [(1, 1)]_\sim)$ zu einem Halbring werden lässt.

Da wir uns hoffentlich einig sind, dass $r/w + r'/w' = rw'/ww' + wr'/ww' = (rw' + wr')/ww'$ gelten soll, betrachten wir die Verknüpfung

$$+\colon (R \times W) \times (R \times W) \longrightarrow R \times W, \quad ((r, w), (r', w')) \longmapsto (r \cdot w' + w \cdot r', w \cdot w')$$

Sie ist kommutativ und assoziativ; letzteres sieht man wie folgt:

$$\begin{aligned}(r,w)+((r',w')+(r'',w'')) &= (r,w)+(r'\cdot w''+w'\cdot r'', w'\cdot w'')\\ &= (r\cdot w'\cdot w''+w\cdot r'\cdot w''+w\cdot w'\cdot r''w\cdot w'\cdot w''\\ &= ((r\cdot w'+w\cdot r', w\cdot w'))+(r'',w'')\\ &= ((r,w)+(r',w'))+(r'',w'')\end{aligned}$$

Ersteres ist hoffentlich offensichtlich. Und es gilt $(0,1)+(r,w)=(r,w)=(r,w)+(0,1)$, sodass $(R\times W,+,(0,1))$ ein abelscher Monoid ist. Desweiteren ist $\sim$ eine Kongruenzrelation für $+$, das ist eine Aufgabe auf dem sechsten Übungszettel. Damit steigt die Addition auf $R\times W$ zu einer Abbildung $+\colon \mathrm{K}_\cdot(R,W)\times K_\cdot(R,W)\to K_\cdot(R,W)$ ab, und macht $K_\cdot(R,W)$ mit zu einem abelschen Monoid mit neutralem Element $[(0,1)]_\sim$.

4.8. Satz *Für jeden kommutativen Halbring R und $W\subseteq R$ wie in 4.7 ist $\mathrm{K}_\cdot(R,W)$ bezüglich der gerade konstruierten Verknüfungen ein Halbring, $\iota\colon R\to \mathrm{K}_\cdot(R,W)$ ist ein Halbringmonomorphismus und $\iota(w)$ ist für jedes $w\in W$ eine Einheit in $\mathrm{K}_\cdot(R,W)$ (bezüglich der Multiplikation). Ist R ein Ring, dann auch $\mathrm{K}_\cdot(R,W)$.*

Weiter gibt es zu jedem Halbringhomomorphismus $f\colon R\to S$ mit der Eigenschaft, dass $f(w)$ eine Einheit ist für jedes $w\in W$, genau einen Halbringhomomorphismus $g\colon \mathrm{K}_\cdot(R,W)\to S$ mit $g\circ\iota=f$. Dieser ist injektiv genau dann, wenn f es ist.

Wie schon mit 3.10 beweist dieser Satz im Falle $W=R\backslash\{0\}$ insbesondere 4.4, sobald wir beobachten, dass $R^{\mathrm{frc}}=\mathrm{K}_\cdot(R,R\backslash\{0\})$ wirklich ein Körper ist: Aber per Konstruktion ist jedes Element aus $\mathrm{K}_\cdot(R,R\backslash\{0\})$ von der Form $\iota(r)/\iota(s)$ für $r,s\in R$, $s\neq 0$ und hierzu ist $\iota(s)/\iota(r)$ ein Inverses.

Proof. Als erstes prüfen wir, dass $\mathrm{K}_\cdot(R,W)$ wirklich ein Halbring ist. Es bleiben zwei Axiome zu prüfen: Das erste ist leicht, denn offenbar gilt

$$[(0,1)]_\sim\cdot[(r,w)]_\sim=[(0,1)]_\sim=[(r,w)]_\sim\cdot[(0,1)]_\sim$$

Die Distributivität ist etwas langwieriger, da es in $R\times W$ noch nicht gilt: Wir rechnen nämlich

$$\begin{aligned}((r,w)\cdot(s,v))+((r,w)\cdot(t,u)) &= (r\cdot s, w\cdot v)+(r\cdot t, w\cdot u)\\ &= (r\cdot s\cdot w\cdot u+w\cdot v\cdot r\cdot t, w\cdot v\cdot w\cdot u)\end{aligned}$$

und

$$\begin{aligned}(r,w)\cdot((s,v)+(t,u)) &= (r,w)\cdot(s\cdot u+v\cdot t, v\cdot u)\\ &= (r\cdot s\cdot u+r\cdot v\cdot t, w\cdot v\cdot u)\\ &\sim (w\cdot r\cdot s\cdot u+w\cdot r\cdot v\cdot t, w\cdot w\cdot v\cdot u)\end{aligned}$$

und diese Ausdrücke stimmen aufgrund der Kommutativität von R überein. Es folgt also

$$[(r,w)]_\sim\cdot([(s,v)]_\sim+[(t,u)]_\sim)=([(r,w)]_\sim\cdot[(s,v)]_\sim)+([(r,w)]_\sim\cdot[(t,u)]_\sim)$$

und das zweite Distriutivgesetz gilt ebenfalls aufgrund der Kommutativität von $\cdot$.

Dass ι mit der Multiplikation verträglich und injektiv ist, und jedes Element von W auf eine Einheit schickt, ist alles Teil von 3.10. Für die Verträglichkeit mit der Addition rechnen wir

$$\iota(r)+\iota(s)=[(r,1)]_\sim+[(s,1)]_\sim=[(r+s,1)]_\sim=\iota(r+s).$$

Dann prüfen wir, dass $\mathrm{K}_\cdot(R,W)$ ein Ring ist, falls R einer ist. Aber es gilt

$$[(r,w)]_\sim+[(-r,w)]_\sim=[(r\cdot w+(-r)\cdot w, w\cdot w)]_\sim=[(0,w\cdot w)]_\sim=[(0,1)]_\sim,$$

sodass in der Tat jedes Element ein additives Inverses besitzt.

Nun zur letzten Behauptung: Dass es genau einen Monoidhomomorphismus g wie gefordert gibt (bezüglich der Multiplikationen $\mathrm{K}_\cdot(R,W)$ und S), ist wieder Teil von 3.10, ebenso dass g

injektiv ist, genau dann wenn f es ist. Es bleibt zu prüfen, dass g ein Halbringhomomorphismus ist, wenn f einer ist. Dafür rechnen wir

$$\begin{aligned}
g\left(\frac{\iota(r)}{\iota(w)}+\frac{\iota(r')}{\iota(w')}\right) &= g\left(\frac{\iota(r)\cdot\iota(w')}{\iota(w)\cdot\iota(w')}+\frac{\iota(w)\cdot\iota(r')}{\iota(w)\cdot\iota(w')}\right)\\
&= g\left(\frac{\iota(r)\cdot\iota(w')+\iota(w)\cdot\iota(r')}{\iota(w)\cdot\iota(w')}\right)\\
&= g\left(\frac{\iota(r\cdot w'+w\cdot r')}{\iota(w\cdot w')}\right)\\
&= \frac{g(\iota(r\cdot w'+w\cdot r'))}{g(\iota(w\cdot w'))}\\
&= \frac{f(r\cdot w'+w\cdot r')}{f(w\cdot w')}\\
&= \frac{f(r)\cdot f(w')+f(w)\cdot f(r')}{f(w)\cdot f(w')}\\
&= \frac{f(r)}{f(w)}+\frac{f(r')}{f(w')}\\
&= \frac{g(\iota(r))}{g(\iota(w))}+\frac{g(\iota(r'))}{g(\iota(w'))}\\
&= g\left(\frac{\iota(r)}{\iota(w)}\right)+g\left(\frac{\iota(r')}{\iota(w')}\right)
\end{aligned}$$

wobei wir in den ersten beiden Umformungen die Rechengesetze in S verwendet haben, dann dass ι ein Halbringhomomorphismus ist, dann dass g ein Monoidhomomorphismus ist, dann $g\circ\iota=f$ und in der Mitte, dass f ein Halbringhomomorphismus ist; dann wieder die Rechengesetze in S, nochmal $g\circ\iota=f$ und dass g ein Monoidhomomorphismus ist. □

Zuletzt übertragen wir wieder noch die Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$:

4.9. Konstruktion Gilt in einem durch $\leqslant$ total geordneten kommutativen Halbring R immer $0\leqslant w^2$ für alle $w\in W$, so definieren wir auf $\mathrm{K}_\cdot(R,W)$ eine Relation durch

$$E\leqslant E' :\Longleftrightarrow \forall (r,w)\in E,(r',w')\in E' \colon r\cdot w\cdot w'\cdot w'\leqslant r'\cdot w'\cdot w\cdot w.$$

Reflexivität und Totalität sollten klar sein, für die Identivität kürze man $w\cdot w'$ um aus $E\leqslant E'$ und $E'\leqslant E$ die Gleichheit $r\cdot w'=r'\cdot w$ zu erhalten und damit $E=E'$. Für die Transitivität sei schließlich $E\leqslant E'$ und $E'\leqslant E''$. Für drei Elemente hieraus gilt dann

$$r\cdot w\cdot w'\cdot w'\leqslant r'\cdot w'\cdot w\cdot w \quad\text{and}\quad r'\cdot w'\cdot w''\cdot w''\leqslant r''\cdot w''\cdot w'\cdot w'.$$

Damit rechnen wir

$$r\cdot w\cdot w'\cdot w'\cdot w''\cdot w''\leqslant r'\cdot w'\cdot w\cdot w\cdot w''\cdot w''\leqslant r''\cdot w''\cdot w'\cdot w'\cdot w\cdot w$$

wobei wir im ersten Schritt $0\leqslant w''\cdot w''$ und im zweiten $0\leqslant w\cdot w$ benutzt haben. Nun benutzt man noch $0\leqslant w'\cdot w'$ um durch Kürzen $r\cdot w\cdot w''\cdot w''\leqslant r''\cdot w''\cdot w\cdot w$ und damit $E\leqslant E''$ zu erhalten. Damit ist $\leqslant$ in der Tat eine totale Ordnung auf $\mathrm{K}_\cdot(R,W)$ und $\iota\colon R\to\mathrm{K}_\cdot(M,W)$ ist monoton, da $[(r,1)]_\sim\leqslant[(r',1)]_\sim$ sich zu $r\leqslant r'$ übersetzt.

4.10. Satz *Ist R ein durch $\leqslant$ total geordneter Halbring, und $W\subseteq R$ wie in 4.7, derart dass $0\leqslant w^2$ für alle $w\in W$. Dann ist die in 4.9 konstruierte Ordnung die eindeutige totale Ordnung, die $\mathrm{K}_\cdot(R,W)$ zu einem geordneten Halbring und $\iota\colon R\to\mathrm{K}_\cdot(R,W)$ monoton macht.*

Wir beobachten noch, dass $0\leqslant w^2$ ein Spezialfall der Bedinung $a\leqslant b, r\leqslant s\Rightarrow a\cdot s+b\cdot r\leqslant a\cdot r+b\cdot s$ für alle Elemente eines Halbrings ist, nämlich der Fall $a=0=r$ und $b=w=s$. Inbesondere ist sie nach 3.13 in jedem Ring automatisch erfüllt. Der Halbring $(\mathcal{P}(M),\subseteq,\cap,\cup,M,\varnothing)$ zeigt aber wieder, dass sie nicht immer erfüllt ist. Wir erhalten aber insbesondere:

4.11. Korollar *Der Körper $\mathbb{Q}$ trägt genau eine totale Ordnung $\leqslant$, derart dass $(\mathbb{Q}, \leqslant, +, \cdot, 0, 1)$ ein geordneter Ring ist und der Ringhomomorphismus $\mathbb{Z} \to \mathbb{Q}$ monoton.*

Beweis von Satz 4.10. Wir überlegen uns zuerst, dass $\leqslant$ kompatibel mit der Multiplikation von $\mathrm{K}.(R, W)$ ist. Sei also $[(0,1)]_\sim \leqslant [(r,w)]_\sim$, mit anderen Worten $0 \leqslant r \cdot w$. Dann gilt für $[(r',w')]_\sim \leqslant [(r'',w'')]_\sim$, also

$$r' \cdot w' \cdot w'' \cdot w'' \leqslant r'' \cdot w'' \cdot w' \cdot w'$$

auch durch Multiplikation mit $0 \leqslant r \cdot w$ und $0 \leqslant w \cdot w$

$$r \cdot r' \cdot w \cdot w' \cdot w \cdot w'' \cdot w \cdot w'' \leqslant r \cdot r'' \cdot w \cdot w'' \cdot w \cdot w' \cdot w \cdot w'$$

was genau $[(r \cdot r', w \cdot w')]_\sim \leqslant [(r \cdot r'', w \cdot w'')]_\sim$ bedeutet, also $[(r,w)]_\sim \cdot [(r',w')]_\sim \leqslant [(r,w)]_\sim \cdot [(r'',w'')]_\sim$. Dann mit der Addition: Gilt wieder $[(r',w')]_\sim \leqslant [(r'',w'')]_\sim$, also

$$r' \cdot w' \cdot w'' \cdot w'' \leqslant r'' \cdot w'' \cdot w' \cdot w'$$

so folgt

$$r \cdot w' \cdot w' \cdot w'' \cdot w \cdot w'' + r' \cdot w' \cdot w'' \cdot w'' \cdot w \cdot w \leqslant r \cdot w'' \cdot w'' \cdot w' \cdot w \cdot w' + r'' \cdot w'' \cdot w' \cdot w' \cdot w \cdot w$$

durch Multiplikation mit $0 \leqslant w \cdot w$ und anschließende Addition der linken Terme. Nochmalige Multiplikation mit $0 \leqslant w \cdot w$ liefert

$$(r \cdot w' + w \cdot r') \cdot w \cdot w' \cdot w \cdot w'' \cdot w \cdot w'' \leqslant (r \cdot w'' + w \cdot r'') \cdot w \cdot w'' \cdot w \cdot w' \cdot w \cdot w'$$

was genau $[(r \cdot w' + w \cdot r', w \cdot w')]_\sim \leqslant [(r \cdot w'' + w \cdot r'', w \cdot w'')]_\sim$ bedeutet, also $[(r,w)]_\sim + [(r',w')]_\sim \leqslant [(r,w)]_\sim + [(r'',w'')]_\sim$. Uff.

Zuletzt zur Eindeutigkeit: Ist $\preccurlyeq$ eine zweite totale Ordnung wie im Satz, so gilt bei $r \cdot w \cdot w' \cdot w' \leqslant r' \cdot w' \cdot w \cdot w$ auch $\iota(r) \cdot \iota(w) \cdot \iota(w)' \cdot \iota(w') \preccurlyeq \iota(r') \cdot \iota(w') \cdot \iota(w) \cdot \iota(w)$ und damit rechnen wir

$$[(r,w)]_\sim = \frac{\iota(r)}{\iota(w)} = \frac{\iota(r) \cdot \iota(w') \cdot \iota(w) \cdot \iota(w')}{\iota(w) \cdot \iota(w) \cdot \iota(w') \cdot \iota(w')} \preccurlyeq \frac{\iota(r') \cdot \iota(w') \cdot \iota(w) \cdot \iota(w)}{\iota(w) \cdot \iota(w) \cdot \iota(w') \cdot \iota(w')} = \frac{\iota(r')}{\iota(w')} = [(r',w')]_\sim$$

da aus $\iota(0) \preccurlyeq \iota(w)^2$ auch $0 \preccurlyeq 1/\iota(w)^2$ folgt (wäre dem nicht so, multipliziere $1/\iota(w)^2 \prec 0$ mit $\iota(w)^2$ um einen Widerspruch zu erhalten). Damit gilt also genau wie schon in 3.13 $E \leqslant E' \Rightarrow E \preccurlyeq E'$ für alle $E, E' \in \mathrm{K}(M, W)$ gilt. Da aber $\leqslant$ schon total ist, erzwingt dass wegen der Identitvität von $\preccurlyeq$ schon $E \leqslant E' \Leftrightarrow E \preccurlyeq E'$. □

Wir beobachten noch zwei Darstellungen für rationale Zahlen:

4.12. Satz *Zu jeder positiven rationalen Zahl $q \in \mathbb{Q}$ gibt es genau eine Funktion $m\colon \{\text{Primzahlen}\} \to \mathbb{Z}$ mit $m(p) = 0$ für fast alle Primzahlen $p \in \mathbb{N}$, so dass*

$$q = \prod_{p \text{ prim}} p^{m(p)}.$$

Es gilt $q \in \mathbb{N}$ genau dann, wenn $0 \leqslant m(p)$ für alle $p \in \mathbb{N}$ prim.

Hier (und allgemeiner für Einheiten in Monoiden, anstatt $p \in \mathbb{Q}$) setzen wir für $m(p) < 0$ noch $p^{m(p)} \coloneqq (p^{-1})^{-m(p)}$, vergleiche die letzte Aufgabe vom siebten Zettel.

Beweis. Wir schreiben $q = r/s$ für zwei natürliche Zahlen $r, s \in \mathbb{N}$ und benutzen dann die Primfaktorzerlegungen

$$r = \prod_p p^{n(p)} \quad \text{and} \quad s = \prod_p p^{l(p)}$$

und damit

$$q = \prod_p \frac{p^{n(p)}}{p^{l(p)}} = \prod_p p^{n(p)-l(p)}$$

zu erhalten. Das zeigt die Existenz. Dann zum Zusatz: Gilt $q = \prod_p p^{m(p)}$ mit $0 \leqslant m(p)$ so gilt sicherlich $q \in \mathbb{N}$. Und umgekehrt setze bei $q \in \mathbb{N}$,

$$I = \{p \in \mathbb{N} \mid p \text{ prim} \wedge m(p) < 0\},$$

sodass

$$q = \frac{\prod_{p\notin I} p^{m(p)}}{\prod_{p\in I} p^{-m(p)}},$$

wo beide Produkte natürliche Zahlen sind. Aber dann folgt

$$\prod_{p\notin I} p^{m(p)} = q \cdot \prod_{p\in I} p^{-m(p)}$$

und insbesondere dass jede Primzahl p mit $m(p) < 0$ das Produkt auf der linken Seite teilt, aber das ist nach Euklid's Lemma nicht möglich. Also folgt, dass I leer ist und $0 \leqslant m(p)$ für alle Primzahlen p.

Für die Eindeutigkeit gelte zuletzt etwa auch $q = \prod_p p^{m'(p)}$. folgt

$$1 = q/q = \prod_p \frac{p^{m(p)}}{p^{m'(p)}} = \prod_p p^{m(p)-m'(p)}$$

und damit nach dem gerade bewiesenen $0 \leqslant m(p) - m'(p)$ für alle Primzahlen p. Aber ganz analog folgt auch $0 \leqslant m'(p) - m(p)$, also $m(p) = m'(p)$ wie gewünscht. □

4.13. Korollar *Zu jeder rationalen Zahl $q \in \mathbb{Q}$ existiert ein eindeutiges Paar $(r, s) \in \mathbb{Z} \times \mathbb{N}\backslash\{0\}$, derart dass $q = r/s$ und teilt eine Zahl $n \in \mathbb{N}$ sowohl r (in $\mathbb{Z}$) als auch s (in $\mathbb{N}$) so folgt $n = 1$. Es gilt $q \in \mathbb{Z}$ genau dann, wenn $s = 1$.*

Man sagt r/s ist der *gekürzte Bruch (short fraction)*, der q darstellt. Man sagt auch r und s seien *teilerfremd (coprime)*.

Beweis. Offenbar lässt sich $0 = 0/1$ darstellen, und diese Darstellung ist eindeutig mit obiger Bedingung, da jede natürliche Zahl 0 teilt. Alsdann betrachten wir positives q. Man zerlege dann $q = \prod_p p^{m(p)}$ und setze wie im vorigen Beweis

$$I = \{p \in \mathbb{N} \mid p \text{ prim} \wedge m(p) < 0\},$$

so dass $q = r/s$ mit $r = \prod_{p\notin I} p^{m(p)}$ und $s = \prod_{p\in I} p^{-m(p)}$, zwei natürliche Zahlen. Und gilt noch $q = r'/s'$ mit teilerfremden r' und s', dann ist zunächst einmal r' ebenfalls positiv und gilt etwa $r' = \prod_p p^{n(p)}$ und $s' = \prod_p p^{l(p)}$, so kann für keine Primzahl p gelten, dass $n(p) > 0$ und $l(p) > 0$ (sonst würde p ja wider der Annahme sowohl r' als auch s' teilen). Aber da $m(p) = n(p) - l(p)$ wegen der Eindeutigkeit in 4.12 gelten muss, folgt dann

$$n(p) = \begin{cases} m(p) & 0 \leqslant m(p) \\ 0 & \text{sonst} \end{cases} \quad \text{und} \quad l(p) = \begin{cases} -m(p) & m(p) \leqslant 0 \\ 0 & \text{sonst} \end{cases}$$

sodass $r = r'$ und $s = s'$.

Für eine Zerlegung eines negativen q zerlege man einfach $-q = r/s$ und erhalten $q = -r/s$, ebenso für die Eindeutigkeit. □

4.14. Beispiel Konstruktion 4.7 erlaubt es uns noch einige weitere Ringe zu basteln.

(1) Zum Beispiel kann man für eine Primzahl p und $P_p = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}\colon p^k = n\}$ den geordneten kommutativen Ring $\mathrm{K}_\cdot(\mathbb{Z}, P_p)$ bilden, in dem jedes Element die Form r/p^k für $r \in \mathbb{Z}$ und $k \in \mathbb{N}$ besitzt. Er wird meist mit $\mathbb{Z}[1/p]$ bezeichnet. Eine ganze Zahl ist hierin also eine Einheit genau dann, wenn p ihr einziger Primteiler ist.

(2) Analog kann man für $C_p = \{n \in \mathbb{N} \mid p \nmid n\}$ den geordneten kommutativen Ring $\mathrm{K}_\cdot(\mathbb{Z}, C_p)$ bilden, der meist als $\mathbb{Z}_{(p)}$ bezeichnet wird. Hierin ist eine natürliche Zahl eine Einheit genau dann, wenn sie von p nicht geteilt wird.

Diese Ringe benutzt man in der Zahlentheorie häufig um Teilbarkeitsfragen zur Primzahl p entweder zu isolieren oder zu ignorieren.

5. Die modularen Zahlen

Zum Abschluss wollen wir beobachten, dass wir auch schon weitere Körper kennen. Auf dem sechsten Übungsblatt galt es zu verifizieren, dass für $b \in \mathbb{N}, b \geqslant 1$ die Relation

$$n \equiv_b m :\Longleftrightarrow \mathrm{rem}_b(n) = \mathrm{rem}_b(m)$$

eine Kongruenzrelation auf $\mathbb{N}$ sowohl bezüglich der Addition als auch der Multiplikation darstellt. Folglich ist $\mathbb{N}/\equiv_b$ wieder ein Halbring, und da für $n \in \mathbb{N}$ gilt

$$[n]_b + [b - \mathrm{rem}_b(n)]_b = [n - \mathrm{rem}_b(n) + b]_b = [q \cdot b + b]_b = [0]_b$$

falls $n = q \cdot b + \mathrm{rem}_b(n)$, ist $\mathbb{N}/\equiv_b$ sogar ein Ring. Er wird meist mit $\mathbb{Z}/b$ bezeichnet. In der Tat liefert uns die letzte Aufgabe von siebten Zettel einen eindeutigen Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}/b$ für jedes $b \in \mathbb{N}$. Der Ring $\mathbb{Z}/b$ hat genau die b Elemente

$$[0]_b, [1]_b, \ldots, [b-2]_b, [b-1]_b,$$

insbesondere ist $\mathbb{Z}/1$ der triviale Ring mit nur einem Element. Wir beobachten nun:

5.1. Satz *Der Ring $\mathbb{Z}/b$ ist ein Körper genau dann, wenn b eine Primzahl ist.*

Man schreibt in Anerkennung dieser Tatsache auch häufig $\mathbb{F}_p$ anstatt $\mathbb{Z}/p$ für eine Primzahl p.

Beweis. Dne trivialen Fall $b = 1$ haben wir oben abgearbeitet. Ist $b \geqslant 2$ zerlegbar, etwa $b = n \cdot m$ mit $1 < n, m < b$, so folgt $[n]_b \neq 0 \neq [m]_b$ aber

$$[n]_b \cdot [m]_b = [n \cdot m]_b = [b]_b = [0]_b = [0]_b \cdot [m]_b.$$

Insbesondere ist $[m]_b$ keine Einheit: Sonst würde Multiplikation mit $[m]_b^{-1}$ ja $[n]_b = [0]_b$ liefern.

Ist aber b prim, so folgt, dass $\mathbb{Z}/b$ ein Integritätsbereich ist: Gilt $[n \cdot m]_b = [n]_b \cdot [m]_b = [0]_b$, bedeutet das $b \mid n \cdot m$. Aber dann folgt nach dem Lemma des Euklid schon $b \mid n$ oder $b \mid m$, also $[n]_b = [0]_b$ oder $[m]_b = [0]_b$. Und jetzt schlägt das folgende Lemma zu. □

5.2. Lemma *Ein endlicher kommutativer Ring R ist ein Integritätsbereich genau dann, wenn er ein Körper ist.*

Analoges gilt auch für nicht kommutative Ringe.

Proof. Allgemein ist jeder Körper ein Integritätsbereich. Umgekehrt ist R ein Integritätsbereich, so ist $r \cdot -\colon R \to R$ injektiv für alle $r \neq 0$. Aber ist R endlich, so ist dann $r \cdot -\colon R \to R$ auch surjektiv, es gilt also insbesondere $r \cdot s = 1$ für ein $s \in R$. □

5.3. Beispiel

(1) Besonders hervorzuheben ist hier wohl der Körper $\mathbb{Z}/2$, der nur aus den Elementen 0 und 1 besteht. Schreiben wir etwa $0 = f$ und $1 = w$ so entsprechen seine Rechenoperationen genau $\times$, der Exklusivdisjunktion, für die Addition und $\wedge$ für die Multiplikation. In dieser Form taucht dieser Körper in der Informatik sehr prominent auf.

(2) Gegeben die bisher erarbeiteten Mittel ist es gar nicht so einfach Inverse in den Ringen $\mathbb{Z}/p$ explizit zu bestimmen, außer durch herumprobieren. Leicht sind immer die Inversen der Teiler von $p + 1$, da aus $n \cdot m = p + 1$ natürlich $[n]_p^{-1} = [m]_p$ folgt. Etwa gilt $[2]_{17}^{-1} = [9]_{17}$, was man gern etwas informeller als

$$1/2 = 9 \text{ in } \mathbb{Z}/17$$

schreibt. Ebenso gelten hier $1/3 = 6$ und auch $1/6 = 3$ und $1/9 = 2$. Aus der ersten Gleichung lernt man weiter $1/4 = (1/2)^2 = 9^2 = 81 = 13$ und $1/8 = 1/2 \cdot 1/4 = 13 \cdot 9 = 117 = 15$, und auch $1/16 = (1/4)^2 = 13^2 = 169 = 16$, wobei das auch einfacher aus $16^2 = (-1)^2 = 1$ folgt. Andersherum folgt noch $1/13 = 4$ und $1/15 = 8$. Ähnlich findet man $1/12 = 1/3 \cdot 1/4 = 6 \cdot 13 = 78 = 10$. Aber damit erhalten wir auch $1/5 = 1/-12 = -(1/12) = -10 = 7$ und dann $1/7 = 5$, $1/10 = 1/-7 = -(1/7) = -5 = 12$ und $1/12 = 10$. Zuletzt findet man noch $1/11 = -(1/6) = -3 = 14$, und damit $1/14 = 11$, was die Tabelle vervollständigt.

5.4. Bemerkung (1) Keiner der Ringe $\mathbb{Z}/n$ ist kompatibel total ordenbar: Aus $[0]_p < [1]_p$ würde induktiv $[0]_p < n \cdot [1]_p = [n]_p$ für jedes $n \in \mathbb{N}$ folgen, was bei bei $n = p$ zu einem Widerspruch führt.

(2) Aus der Analysisvorlesung kennen Sie wahrscheinlich auch schon zwei weitere Körper: $\mathbb{R}$, den Körper der reellen Zahlen, eine weitere total geordnete Erweiterung von $\mathbb{Q}$, und $\mathbb{C}$, den Körper der komplexen Zahlen, eine Erweiterung von $\mathbb{R}$, die aber nicht mehr ordenbar ist. Beide werden uns auch begegnen, aber erst etwas später, wenn Bedarf besteht.

(3) Schiefkörper zu finden, die keine Körper sind, ist gar nicht so einfach (sie werden aber etwas später in Ihrem Studium ganz natürlich auftauchen, etwa als Endomorphismenringe irreduzibler reeller oder rationaler Darstellungen endlicher Gruppen, was auch immer das genau jetzt ist). Das einfachste Beispiel, Hamilton's Quaternionen $\mathbb{H}$, ist auch typischer Untersuchungsgegenstand in einem Bachelorseminar. Echte Schiefkörper sind wohl auch wegen des folgenden bemerkenswerten Satzes von Wedderburn (nach dem Schotten Joseph Wedderburn, 1882 - 1948) aus dem Jahre 1905 so selten: Jeder endliche Schiefkörper ist ein Körper. Dieser Satz geht über unsere Vorlesung hier ebenso hinaus wie eine Diskussion der Quaternionen.

Nicht kommutative Ringe werden uns aber noch zu Hauf begegnen.

Zwei weitere Beweise*

Mit den nun etablierten natürlichen Zahlen, können wir endlich den Satz von Schröder-Bernstein führen:

Beweis von 5.19. Seien also $f\colon A \to B$ und $g\colon B \to A$ injektiv. Dann können wir uns für ein $a \in A$ die Folge

$$a, f(a), g(f(a)), f(g(f(a))), \dots$$

der Bilder von a anschauen und sie versuchen nach links durch Urbilder von a fortzusetzen; da f und g injektiv sind, ist dies höchstens auf eine Art möglich. Es gibt drei Fälle: Entweder die Folge lässt sich beliebig weit nach links fortsetzen (dabei kann sie periodisch werden, oder auch nicht), sie endet bei einem Element von $A\backslash\mathrm{Im}(g)$ oder bei einem Element von $B\backslash\mathrm{Im}(f)$. Diese letztere dieser Mengen ist genau durch

$$A' = \{a \in A \mid \exists n \in \mathbb{N}, b \in B\backslash\mathrm{Im}(f)\colon a = (g \circ (f \circ g)^{\circ n})(b)\}$$

gegeben. Wir können nun eine Abbildung $h\colon A \to B$ angegeben durch

$$a \longmapsto \begin{cases} g^{-1}(a) & a \in A' \\ f(a) & a \notin A' \end{cases}$$

da g aufgefasst als Abbildung $g\colon A \to \mathrm{Im}(g)$ bijektiv ist, und $A' \subseteq \mathrm{Im}(g)$. Wir behaupten, diese ist bijektiv: Seien nämlich $a, a' \in A$ mit $h(a) = h(a')$ gegeben, gelten dann entweder $a, a' \in A'$ oder $a, a' \in A$, so folgt $a = a'$ aus der Injektivität von f und g^{-1}. Aber ist $a' \in A'$, so ist $h(a') = g^{-1}(a)$ ein Element von

$$B' = \{x \in B \mid \exists n \in \mathbb{N}, b \in B\backslash\mathrm{Im}(f)\colon x = (f \circ g)^{\circ n}(b)\}$$

Aber gilt auch $f(a) \in B'$, etwa $f(a) = (f \circ g)^{\circ m}(b)$, so kann sicherlich nicht $m = 0$ gelten (da $f(a) \in \mathrm{Im}(f)$) und dann folgt $a = (g \circ (f \circ g)^{\circ m-1})(b)$, was $a \in A'$ impliziert. Also ist h injektiv.

Ist auf der anderen Seite ein $b \in B$ gegeben, so unterscheiden wir ebenfalls zwei Fälle: Ist $b \in B'$, so ist offenbar $g(b) \in A'$ und damit $h(g(b)) = g^{-1}(g(b)) = b$. Ist andererseits $b \notin B'$, so ist sicherlich $b \in \mathrm{Im}(f)$ (sonst würde $m = 0$ der definierenden Gleichung von B' genügen). Und $f^{-1}(b) \notin A'$: Aus $f^{-1}(b) = (g \circ (f \circ g)^{\circ n})(b')$ würde ja sicherlich $b = (f \circ g)^{\circ n+1}(b')$ folgen. Also gilt $h(f^{-1}(b)) = f(f^{-1}(b)) = b$. □

Und dann beweisen wir auch noch den Satz von Hessenberg. Das benötigt ein wenig Vorbereitung. Zunächst erinnere ich an folgenden Spezialfall:

5.5. Lemma (Cantor'scher Diagonalsatz) *Die Abbildung $p\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, induktiv gegeben durch*

$$p(0) = (0, 0), \quad p(n + 1) = g(p(n))$$

mit

$$g\colon \mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}\times\mathbb{N},\quad (k,l)\longrightarrow\begin{cases}(k-1,l+1) & k>0\\ (l+1,0) & k=0\end{cases},$$

ist bijektiv.

BEWEIS. Der Beweis war Teil der Analysis-Vorlesung. □

5.6. Lemma *Ist X eine unendlichen Menge, so gibt es eine Injektion $h\colon X\to X$ die genau ein $b\in X$ nicht trifft, für die also gilt $\operatorname{Im}(f)=X\backslash\{b\}$.*

Insbesondere gibt es für jede endliche Teilmenge $T\in X$ eine Bijektion $X\backslash T\to X$.

BEWEIS. Nach 1.5 gibt es für unendliches X eine Injektion $i\colon\mathbb{N}\to X$. Dann definieren wir h durch

$$x\longmapsto\begin{cases}x & x\notin\operatorname{Im}(i)\\ i(n+1) & x=i(n)\end{cases}$$

Das ist offenbar eine Injektion die genau $b=f(0)$ nicht trifft.

Man prüft dann leicht, dass $h^{\circ n}\colon X\to X$ eine Injektion ist, die genau die Menge $S=\{i(0),\dots,i(n-1)\}$ nicht trifft, sodass der Zusatz zumindest für diese n-elementige Menge gilt. Aber für jede andere n-elementige Teilmenge T, wählen wir Bijektionen

$$j\colon\{1,\dots,l\}\longrightarrow T\backslash S\quad\text{and}\quad k\colon\{1,\dots,l\}\longrightarrow S\backslash T,$$

wo $l=n-|T\cap S|$. Damit können wir die Bijektion

$$X\backslash T\longrightarrow X\backslash S,\quad x\longmapsto\begin{cases}x & x\notin S\\ k(m) & x=j(m)\end{cases}$$

angeben, was den Zusatz beweist. □

Desweiteren benötigen wir noch folgende leichtere Version vorab:

5.7. Lemma *Ist X unendlich, so gibt es eine Bijektion $X\to X\times\{0,1\}$.*

BEWEIS. Der Beweis ist dem des Vergleichssatzes von Zermelo 5.18 recht ähnlich. Wir betrachten

$$F=\{(Z,f)\in\mathcal{P}(X)\times\mathcal{P}(X\times X\times X)\mid f\text{ definiert eine Bijektion }Z\to Z\times\{0,1\}\}$$

zusammen mit der Relation $\preccurlyeq$ definiert durch $(Z,f)\preccurlyeq(Z',f')$ falls $Z\subseteq Z'$ und $f(z)=f'(z)$ für alle $z\in Z$.

Dann erfüllt $(F,\preccurlyeq)$ die Voraussetzungen des Zorn'schen Lemmas, genau wie die analoge Menge im Beweis des Zermelo'schen Vergleichssatzes. Sei dann (S,g) also ein maximales Element von F. Wir zeigen nun, dass es eine Bijektion $h\colon S\to X$ gibt, womit dann auch die Komposition

$$X\xrightarrow{h^{-1}}S\xrightarrow{g}S\times\{0,1\}\xrightarrow{h\times\mathrm{id}}X\times\{0,1\}$$

eine Bijektion ist, wie gewünscht.

Gäbe es nämlich keine Bijektion $S\to X$ so wäre nach dem vorigen Lemma zumindest $X\backslash S$ nicht endlich. Also gibt es wieder nach 1.5 eine Injektion $i\colon\mathbb{N}\to X\backslash S$. Aber dann wäre $S\cup\operatorname{Im}(i)$ zusammen mit folgender bijektiver Fortsetzung

$$h\colon S\cup\operatorname{Im}(i)\longrightarrow(S\cup\operatorname{Im}(i))\times\{0,1\}=(S\times\{0,1\})\cup(\operatorname{Im}(i)\times\{0,1\})$$

von g ebenfalls ein Element von F im Widerspruch zur Maximalität von (S,g): Es gelte $h(s)=g(s)$ für alle $s\in S$ und $h(s)=p(s)$ wo p die Komposition von Bijektionen

$$\operatorname{Im}(i)\xrightarrow{i^{-1}}\mathbb{N}\xrightarrow{q}\mathbb{N}\times\{0,1\}\xrightarrow{i\times\mathrm{id}}\operatorname{Im}(i)\times\{0,1\}$$

ist, mit

$$q(n)=\begin{cases}\left(\frac{n}{2},0\right) & n\text{ gerade}\\ \left(\frac{n-1}{2},1\right) & n\text{ ungerade}\end{cases}.$$

□

Nun zum eigentlichen Beweis des Satzes von Hessenberg, der dem des obigen Lemmas gleicht:

BEWEIS VON 1.11. Wir betrachten

$$F = \{(Z, f) \in \mathcal{P}(X) \times \mathcal{P}(X \times X \times X) \mid f \text{ definiert eine Bijektion } Z \to Z \times Z\}$$

zusammen mit der Relation $\preccurlyeq$ definiert durch $(Z, f) \preccurlyeq (Z', f')$ falls $Z \subseteq Z'$ und $f(z) = f'(z)$ für alle $z \in Z$.

Dann erfüllt $(F, \preccurlyeq)$ die Voraussetzungen des Zorn'schen Lemmas, genau wie die analoge Menge im Beweis des Zermelo'schen Vergleichssatzes. Sei dann (S, g) also ein maximales Element von F. Wir zeigen nun, dass es eine Bijektion $h\colon S \to X$ gibt, womit dann auch die Komposition

$$X \xrightarrow{h^{-1}} S \xrightarrow{g} S \times S \xrightarrow{h \times h} X \times X$$

eine Bijektion ist, wie gewünscht.

Gäbe es nämlich keine Bijektion $S \to X$ so folgern wir diesmal zunächst, dass es eine Injektion $i\colon X \to X \backslash S$ geben muss: Es gibt schließlich eine Injektion $a\colon X \backslash S \to S$ oder $b\colon S \to X \backslash S$ nach dem Zermelo'schen Vergleichssatz. Aber im ersten Fall gibt es dann die Injektion

$$X = (X \backslash S) \cup S \longrightarrow S \times \{0, 1\}, \quad x \longmapsto \begin{cases} (a(x), 0) & x \notin S \\ (x, 1) & x \in S \end{cases}$$

Nach dem vorigen Lemma impliziert dies aber, dass es eine Injektion $X \to S$ gibt, und damit nach dem Satz von Schröder-Bernstein doch eine Bijektion $X \to S$. Im zweiten Fall erhält man analog eine Bijektion $X \to X \backslash S$ wie behauptet.

Aber nun können wir wieder wie im vorigen Lemma vorgehen: Die Menge $S \cup \mathrm{Im}_i(S)$ zusammen mit folgender bijektiver Fortsetzung

$$h\colon S \cup \mathrm{Im}_i(S) \longrightarrow (S \cup \mathrm{Im}_i(S)) \times (S \cup \mathrm{Im}_i(S)) = (S \times S) \cup (\mathrm{Im}_i(S) \times S) \cup (S \times \mathrm{Im}_i(S)) \cup (\mathrm{Im}(i) \times \mathrm{Im}_i(S))$$

von g ebenfalls ein Element von F im Widerspruch zur Maximalität von (S, g): Es gelte $h(s) = g(s)$ für alle $s \in S$ und $h(i(s)) = p(s)$ wo p die folgende Komposition von Bijektionen ist:

$$\mathrm{Im}_i(S) \xrightarrow{i^{-1}} S \xrightarrow{f} S \times \{0, 1, 2\} \xrightarrow{g \times \mathrm{id}} S \times S \times \{0, 1, 2\} \xrightarrow{q} (\mathrm{Im}_i(S) \times S) \cup (S \times \mathrm{Im}_i(S)) \cup (\mathrm{Im}(i) \times \mathrm{Im}_i(S))$$

with f arising from a two-fold application of the previouos lemma, and

$$q(s, s, k) = \begin{cases} (i(s), s') & k = 0 \\ (s, i(s')) & k = 1 \\ (i(s), i(s')) & k = 2 \end{cases}$$

□

Hier ist noch eine nützliche Umformulierung des Satzes von Hessenberg:

5.8. Korollar *Ist $A \subseteq \mathcal{P}(X)$ mit $A \preccurlyeq Z$ und auch $B \preccurlyeq Z$ für jedes $B \in A$, wo Z eine unendliche Menge. Dann gilt auch $\bigcup A \preccurlyeq Z$.*

Wählt man $Z = \mathbb{N}$, so sagt dies genau, dass abzählbaren Vereinigungen abzählbarer Mengen wieder abzählbar sind. Etwa folgt sofort, dass $\mathbb{Q}$ abzählbar ist.

BEWEIS. Die zweite Voraussetzung besagt, dass für

$$g\colon A \longrightarrow \mathcal{P}(\mathrm{F}(Z, A)), \quad B \longmapsto \{f\colon Z \Rightarrow A \mid \mathrm{Im}(f) = B\}$$

immer $g(B) \neq \varnothing$ gilt. Wir können also eine Abbildung $h\colon A \to \mathrm{F}(Z, A)$ auswählen, sodass $h_B\colon Z \to B$ surjektiv ist. Wählen wir weiter eine Surjektion $k\colon Z \to A$, so ist auch

$$Z \times Z \xrightarrow{p} \{(B, a) \in A \times X \mid a \in B\} \xrightarrow{q} \bigcup A$$

surjektiv wo

$$p(z, z') = (k(z), h_{k(z)}(z')) \quad \text{und} \quad q(B, a) = a.$$

Eine Anwendung des Satzes von Hessenberg liefert dann eine Surjektiv $Z \to \bigcup A$. □

KAPITEL 3

Lineare Gleichungen

1. Matrizen

1.1. Definition Sei R ein Ring und $k, n \in \mathbb{N}$. Dann ist eine $k \times n$-*Matrix (matrix)* A über R eine Abbildung $A\colon \{1,\dots,k\} \times \{1,\dots,n\} \to R$. Man sagt, A habe k Zeilen und n Spalten und schreibt meinst $A_{i,j}$ anstatt $A(i,j)$. Wir bezeichnen die Menge aller $k \times n$-Matrizen mit $\mathrm{Mat}(k,n,R)$.

Mit anderen Worten $\mathrm{Mat}(k,n,R) = \mathrm{F}(\{1,\dots,k\} \times \{1,\dots,n\}, R)$. Oft stellt man eine Matrix A als

$$\begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,n} \\ A_{2,1} & A_{2,2} & \dots & A_{2,n} \\ \vdots & \vdots & & \vdots \\ A_{k,1} & A_{k,2} & \dots & A_{k,n} \end{pmatrix}$$

dar.

Der Zweck von Matrizen ist es lineare Gleichungssysteme zu kodieren. Wir setzen noch $R^m = \mathrm{F}(\{1,\dots,m\}, R)$, und damit insbesondere $R^2 \cong R \times R$ und allgemeiner

$$R^n \cong R \times R \times \cdots \times R$$

mit n Faktoren auf der rechten Seite. Ziel ist es dann für gegebenes $b \in R^k$ die Menge aller $x \in R^n$ zu verstehen für die gilt

$$\begin{aligned} A_{1,1} \cdot x_1 + A_{1,2} \cdot x_2 + \cdots + A_{1,n} x_n &= b_1 \\ A_{2,1} \cdot x_1 + A_{2,2} \cdot x_2 + \cdots + A_{2,n} x_n &= b_2 \\ \vdots \qquad\qquad & \qquad\qquad \vdots \\ A_{k,1} \cdot x_1 + A_{k,2} \cdot x_2 + \cdots + A_{k,n} x_n &= b_k \end{aligned}$$

Etwas formaler definieren eine Abbildung

$$\mathrm{L}\colon \mathrm{Mat}(k,n,R) \longrightarrow \mathrm{F}(R^n, R^k), \quad A \longmapsto [x \mapsto (i \mapsto \sum_{j=1}^{n} A_{i,j} \cdot x_j)]$$

Für $b \in R^k$ ist dann die *Lösungsmenge (solution set)* $\mathrm{L}(A;b)$ des zu A und b assoziierten Gleichungssystems genau das Urbild $\mathrm{Pre}_{\mathrm{L}(A)}(\{b\}) \subseteq R^n$.

1.2. Beispiel (1) Der einfachste (nicht leere) Fall ist natürlich $k = 1 = m$, wo wir für $a \in R$ und $b \in R$ die Menge

$$\mathrm{L}(a;b) = \{x \in R \mid a \cdot x = b\}$$

verstehen müssen. Insbesondere sieht man sofort, dass die Schwierigkeit der Antwort sehr von den Eigenschaften von R abhängt: Eine Lösung existiert (per Definitionem) genau falls a das Element b von links teilt. Ist a eine Einheit, so gibt es genau eine Lösung, nämlich $1/a \cdot b$. Ist a wenigstens kürzbar, so gibt es immer noch höchstens eine Lösung aber etwa hat $2 \cdot x = 3$ natürlich keine Lösung in den ganzen Zahlen. Noch allgemeiner kann aber vieles passieren. Etwa hat $n \cdot x = 0$ im Ring $\mathbb{Z}/m$ genau n Lösungen, falls n die Zahl m teilt.

Wir werden uns der Einfachheit halber in dieser Vorlesung meist auf den Fall beschränken, dass R ein Körper ist.

(2) Der nächst einfache Fall ist wohl der einer *Diagonalmatrix* D im Falle $k = n$: Dies ist eine $n \times n$-Matrix mit $D_{i,j} = 0$ falls $i \neq j$, also

$$D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

für irgendwelche $d_1, \dots, d_n \in R$. Hier geht es um die Menge

$$\mathrm{L}(D; b) = \{x \in R^n \mid \forall 1 \leqslant i \leqslant n \colon d_i \cdot x_i = b_i\}$$

$$= \{x \in R \mid d_1 \cdot x = b_1\} \times \cdots \times \{x \in R \mid d_n \cdot x = b_n\}$$

die wir wohl ebensogut verstehen, wie die Lösungen von einzelnen Gleichungen wie in (1). Sind etwa alle d_i Einheiten in R so hat die Lösungsmenge wieder genau ein Element.

Ein weiterer fundamentaler Fall ist der folgende:

1.3. Definition Eine Matrix $Z \in \mathrm{Mat}(k, n, R)$ ist in *Zeilenstufenform (row echelon form)*, falls es ein $0 \leqslant l \leqslant k$ und eine streng monotone Funktion $r \colon \{1, \dots, l\} \to \{1, \dots, n\}$ gibt (also $i < j \Rightarrow r(i) < r(j)$), derart dass

(1) $Z_{i,j} = 0$ falls $l < i$,
(2) $Z_{i,j} = 0$ falls $i \leqslant l$ und $j < r(i)$, und
(3) $Z_{i,r(i)}$ ist eine Einheit in R, falls $i \leqslant l$.

Die Matrix Z hat *strikte* Zeilenstufenform, falls auch noch

(4) $Z_{i,r(j)} = 0$ für $i < j$ gilt.

1.4. Beispiel (1) Jede Diagonalmatrix hat strikte Zeilenstufenform.

(2) Ein typischeres Beispiel einer nicht strikten Zeilenstufenform ist etwa

$$Z = \begin{pmatrix} 0 & 0 & -1 & 2 & 3 & 7 & 4 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 5487 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{Mat}(6, 7, \mathbb{Z})$$

mit $l = 4$ und $r(1) = 3, r(2) = 4, r(3) = 6, r(4) = 7$. Die Matrix

$$\begin{pmatrix} 0 & 0 & -1 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{Mat}(6, 7, \mathbb{Z})$$

ist in strikter Zeilenstufenform.

(3) Allgemein folgt aus der strengen Monotonie von r in Definition 1.3, dass $r(i) \geqslant i$ und demzufolge ist jede Matrix in Zeilenstufenform eine *obere Dreiecksmatrix (upper triangular matrix*, mit anderen Worten $Z_{i,j} = 0$ falls $j < i$.

(4) Umgekehrt ist eine obere Dreiecksmatrix T sicherlich in Zeilenstufenform falls $T_{i,i}$ eine Einheit ist für alle $1 \leqslant i \leqslant \min(k,n)$ gilt, also zum Beispiel falls bei $n \leqslant k$

$$T = \begin{pmatrix} 1 & T_{1,2} & \dots & T_{1,n-1} & T_{1,n} \\ 0 & 1 & \dots & T_{2,n-1} & T_{2,n} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & T_{n-1,n} \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

oder bei $k \leqslant n$

$$T = \begin{pmatrix} 1 & T_{1,2} & \dots & T_{1,k} & T_{1,k+1} & \dots & T_{1,n} \\ 0 & 1 & \dots & T_{2,k} & T_{2,k+1} & \dots & T_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & T_{k,k+1} & \dots & T_{k,n} \end{pmatrix}$$

Sie ist strikt falls sie von der Form

$$\begin{pmatrix} 1 & 0 & \dots & 0 & T_{1,k+1} & \dots & T_{1,n} \\ 0 & 1 & \dots & 0 & T_{2,k+1} & \dots & T_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & T_{k,k+1} & \dots & T_{k,n} \end{pmatrix}$$

ist.

(5) Die Zahl $l \in \{0,\dots,k\}$ und die Funktion $r\colon \{1,\dots,l\} \to \{1,\dots,n\}$ aus Definition 1.3 sind (falls existent) durch $Z \in \mathrm{Mat}(k,n,R)$ offenbar eindeutig bestimmt, durch die Position der Nullzeilen in Z, also $l = k$ falls es keine solche gibt und sonst

$$l = \min\{i \in \{0,\dots,k\} \mid \forall 1 \leqslant j \leqslant n\colon Z_{i+1,j} = 0\}$$

und die Position der Einsen, i.e.

$$r(i) = \min\{j \in \{1,\dots,n\} \mid Z_{i,j} \text{ ist eine Einheit}\}.$$

Die Zahl l heißt der *Zeilenrang (row rank)* von Z und wir werden r die Zeugenfunktion nennen.

Das Gleichungssystem assoziiert zu so einem $Z \in \mathrm{Mat}(k,n,R)$ in Zeilenstufen form sieht schematisch wie folgt aus:

$$\begin{aligned} Z_{1,r(1)} \cdot x_{r(1)} + \dots + Z_{1,r(2)} \cdot x_{r(2)} + \dots + Z_{1,r(l)} \cdot x_{r(l)} + \dots + Z_{1,n} x_n &= b_1 \\ Z_{2,r(2)} \cdot x_{r(2)} + \dots + Z_{2,r(l)} \cdot x_{r(l)} + \dots + Z_{1,n} x_n &= b_2 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots & \\ Z_{l,r(l)} \cdot x_{r(l)} + \dots + Z_{l,n} x_n &= b_l \\ 0 &= b_{l+1} \\ \vdots \quad \vdots & \\ 0 &= b_k, \end{aligned}$$

wobei die Zeilen von oben nach unten in den ersten l Schritten strikt kürzer werden da ja $r(1) < r(2) < \dots < r(l)$. Und Z ist strikt, falls der Koeffizient vor $x_{r(j)}$ nur in der $j$ten Zeile nicht verschwindet. Das macht es besonders leicht zu lösen:

1.5. Beobachtung Seien R ein Ring, $Z \in \mathrm{Mat}(k,n,R)$ in strikter Zeilenstufenform mit Zeilenrank l und Zeugenfunktion $r\colon \{1,\dots,l\} \to \{1,\dots,n\}$ und $b \in R^k$. Dann ist $\mathrm{L}(Z;b) \neq \varnothing$ genau dann, wenn $b_i = 0$ für alle $l \leqslant i \leqslant k$. In diesem Falle ist die Komposition

$$\begin{aligned}\mathrm{L}(Z;b) \subseteq R^n = \mathrm{F}(\{1,\dots,n\},R) &\longrightarrow \mathrm{F}(\{1,\dots,n\}\backslash\mathrm{Im}(r),R)\\ x &\longmapsto x_{|\{1,\dots,n\}\backslash\mathrm{Im}(r)}\end{aligned}$$

bijektiv.

Für jeden Index $j \notin \mathrm{Im}(r)$ können wir uns die Komponenten $x_j \in R$ eines Elements $x \in R^n$ also beliebig vorgeben und es gibt dann genau eine Art die übrigen Werte $x_{r(i)}$ zu ergänzen, derart dass x eine Lösung des Gleichungssystems ist. Tatsächlich kann man die Werte $x_{r(i)}$ einfach durch Auflösen der i-ten Gleichung

$$\sum_{j=r(i)}^{n} Z_{i,j} \cdot x_j = b_i$$

zu

$$x_{r(i)} = Z_{i,r(i)}^{-1} \cdot (b_i - \sum_{j=r(i)+1}^{n} Z_{i,j} \cdot x_j) = Z_{i,r(i)}^{-1} \cdot (b_i - \sum_{\substack{j=r(i)+1\\ j\notin\mathrm{Im}(r)}}^{n} Z_{i,j} \cdot x_j)$$

bestimmen, da ja die auf der rechten Seite verschwundenen Summanden $Z_{i,r(k)} \cdot x_{r(k)}$ mit $i < k$ genau nach der Striktheitsannahme an Z verschwinden.

1.6. Beispiel Nehmen wir uns etwa

$$Z = \begin{pmatrix} 0&0&1&0&3&0&0\\ 0&0&0&1&2&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix} \in \mathrm{Mat}(6,7,\mathbb{Z})$$

her und suchen für gegebenes $b = (b_1,\dots,b_6) \in \mathbb{Z}^6$ die jenigen $x = (x_1,\dots,x_7)$ mit

$$\begin{aligned} x_3 + 3\cdot x_5 + &= b_1\\ x_4 + 2\cdot x_5 &= b_2\\ x_6 &= b_3\\ x_7 &= b_4\\ 0 &= b_5\\ 0 &= b_6 \end{aligned}$$

Das Lemma besagt nun, dass es solches x schon dann wirklich gibt, wenn die offensichtlich notwendige Bedingung $b_5 = 0 = b_6$ erfüllt ist. Desweiteren können wir uns in diesem Fall x_1, x_2 und x_5 beliebig vorgeben und es gibt dann eindeutige x_3, x_4, x_6, x_7 die zusammen eine Lösung bilden. Nämlich lösen wir die nach Streichung der trivialen letzten beiden Gleichungen die übrigen auf und erhalten

$$\begin{aligned} x_3 &= b_1 - 3\cdot x_5\\ x_4 &= b_2 - 2\cdot x_5\\ x_6 &= b_3\\ x_7 &= b_4 \end{aligned}$$

Mit anderen Worten

$$\mathrm{L}(Z;b) = \mathrm{Im}(f_b)$$

wobei $f_b\colon R^3 \to R^7$ gegeben ist durch

$$(x,y,z) \longmapsto (x, y, -3\cdot z + b_1, -2\cdot z + b_2, z, b_3, b_4).$$

Wir beobachten noch, dass sich dies auftrennen lässt in

$$f_b(x,y,z) = (\mathrm{L}(A))(x,y,z) + (\mathrm{L}(B))(b_1,\ldots,b_4)$$

mit

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -3 \\ 0 & 0 & -2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Dass sich die Lösungen eines linearen Gleichungssystems selbst wieder durch zwei Matrizen darstellen lässt, wird sich als allgemeines Phänomen erweisen. Und auch was diese konreten Matrizen mit der Ursprungsmatrix Z zu tun haben, werden wir erörtern.

2. Der Eliminationsalgorithmus

Nach diesen leichten Gleichungssystemen wollen wir uns nun ein im wesentlichen beliebiges ansehen. Es ist ein extrem nützlicher Satz, dass solange der Grundring R ein (Schief-)Körper ist, *jedes* Gleichungssystem in Zeilenstufenform überführt werden kann. Hierzu benötigt man nur zwei grundlegende Operationen:

2.1. Konstruktion Gegeben $1 \leqslant a, c \leqslant k$ mit $a \neq c$ und $\lambda \in R$ so definieren wir eine Abbildung

$$\mathrm{s}^{\lambda}_{a,c} \colon \mathrm{Mat}(k,n,R) \longrightarrow \mathrm{Mat}(k,n,R)$$

durch Addition von der um λ vervielfachten $a$ten Zeile auf die $c$te, in Formeln

$$A \longmapsto \left[(i,j) \mapsto \begin{cases} A_{i,j} & i \neq c \\ A_{c,j} + \lambda \cdot A_{a,j} & i = c \end{cases} \right]$$

Diese Operation heißt *elementare Zeilenoperation vom Typ I*.

Gegeben $1 \leqslant a, c \leqslant k$ so definieren wir eine Abbildung

$$\mathrm{t}_{a,c} \colon \mathrm{Mat}(k,n,R) \longrightarrow \mathrm{Mat}(k,n,R)$$

durch das tauschen der $a$ten mit der $c$ten Zeile, in Formeln

$$A \longmapsto \left[(i,j) \mapsto \begin{cases} A_{i,j} & i \neq a,c \\ A_{c,j} & i = a \\ A_{a,j} & i = c \end{cases} \right]$$

Diese Operation heißt *elementare Zeilenoperation vom Typ III*.

Etwas weniger wichtig ist die noch fehlende Operation vom Typ II: Gegeben $1 \leqslant a \leqslant k$ und $\lambda \in R$ eine Einheit so definieren wir eine Abbildung

$$\mathrm{m}^{\lambda}_{a} \colon \mathrm{Mat}(k,n,R) \longrightarrow \mathrm{Mat}(k,n,R)$$

durch multiplizieren der $a$ten Zeile mit λ, in Formeln

$$A \longmapsto \left[(i,j) \mapsto \begin{cases} A_{i,j} & i \neq a \\ \lambda \cdot A_{a,j} & i = a \end{cases} \right]$$

Im Falle $n = 1$ beobachten wir, dass sich diese Operationen auch auf $b \in R^k$ anwenden lassen (man stelle sich b als Matrix mit nur einer Spalte vor).

2.2. Beobachtung Für jedes $A \in \mathrm{Mat}(k,n,R)$ und $b \in R^k$ und $\lambda \in R$

$$\mathrm{L}(A;b) = \mathrm{L}(\mathrm{s}^{\lambda}_{a,c}(A); \mathrm{s}^{\lambda}_{a,c}(b))$$

$$\mathrm{L}(A;b) = \mathrm{L}(\mathrm{t}_{a,c}(A); \mathrm{t}_{a,c}(b))$$

und falls λ eine Einheit ist auch

$$\mathrm{L}(A;b) = \mathrm{L}(\mathrm{m}_a^\lambda(A); \mathrm{m}_a^\lambda(b)).$$

2.3. Theorem (Gauß'scher Eliminierungssatz) *Ist R ein Ring und hat $Z \in \mathrm{Mat}(k,n,R)$ Zeilenstufenform vom Rang l, so gibt es eine Abbildung*

$$f\colon \left\{1,\dots,\frac{(l-1)l}{2}\right\} \longrightarrow \mathrm{F}(\mathrm{Mat}(k,n,R), \mathrm{Mat}(k,n,R))$$

derart, dass $f(i)$ eine elementare Zeilenoperation vom Typ I ist für jedes i, und derart dass die Matrix

$$\left(\bigcirc_{i=1}^{\frac{(l-1)l}{2}} f(i)\right)(Z)$$

strikte Zeilenstufenform hat.

Ist K ein (Schief-)Körper, so gibt es zu jeder Matrix $A \in \mathrm{Mat}(k,n,K)$ eine Abbildung

$$e\colon \left\{1,\dots,\frac{k(k+1)}{2}\right\} \longrightarrow \mathrm{F}(\mathrm{Mat}(k,n,R), \mathrm{Mat}(k,n,R))$$

derart, dass $e(i)$ eine elementare Zeilenoperation von Typ I oder III ist für jedes i, und derart dass die Matrix

$$\left(\bigcirc_{i=1}^{\frac{k(k+1)}{2}} e(i)\right)(A)$$

Zeilenstufenform hat.

Dieser Satz wurde sicherlich nicht zuerst von Carl Friedrich Gauß (1777 - 1855), dem berühmtesten aller deutschen Mathematiker (sein Antlitz zierte die 10 Marknote) gefunden. Aber er scheint der erste gewesen zu sein, der auch einen vollständigen Beweis für beliebiges n gegeben hatte, und in der ersten Dekade des 19. Jahrhunderts.

Da sicherlich $l \leqslant k$ gilt, besagt der Satz, dass wir beliebiges $A \in \mathrm{Mat}(k,n,K)$ für einen (Schief-)Körper K in höchstens

$$\frac{k(k+1)}{2} + \frac{(k-1)k}{2} = k^2$$

in strikte Zeilenstufenform überführen können. Wir werden die benötigten Abbildungen e und f direkt konstruieren. Zunächst zwei Beispiele:

2.4. Beispiel (1) Betrachte etwa

$$\begin{pmatrix} 2 & 3 & 0 \\ 1 & 0 & 1 \\ 3 & 2 & 1 \end{pmatrix} \in \mathrm{Mat}(3,3,\mathbb{Q})$$

Dann können wir im ersten Schritt $\mathrm{s}_{1,2}^{-1/2}$ anwenden und erhalten

$$\begin{pmatrix} 2 & 3 & 0 \\ 0 & -3/2 & 1 \\ 3 & 2 & 1 \end{pmatrix}$$

Dann wenden wir $\mathrm{s}_{1,3}^{-3/2}$ an und erhalten

$$\begin{pmatrix} 2 & 3 & 0 \\ 0 & -3/2 & 1 \\ 0 & -5/2 & 1 \end{pmatrix}$$

und zum Schluss $s_{2,3}^{-5/3}$ um

$$\begin{pmatrix} 2 & 3 & 0 \\ 0 & -2/3 & 1 \\ 0 & 0 & -2/3 \end{pmatrix}$$

zu erhalten. Diese Matrix hat dann Zeilenstufenform.

Um sie in strike Zeilenstufenform zu überführen, wenden wir noch $s_{2,1}^{9/2}$ an um

$$\begin{pmatrix} 2 & 0 & 9/2 \\ 0 & -2/3 & 1 \\ 0 & 0 & -2/3 \end{pmatrix}$$

zu erhalten, dann $s_{3,2}^{3/2}$, was zu

$$\begin{pmatrix} 2 & 0 & 9/2 \\ 0 & -2/3 & 0 \\ 0 & 0 & -2/3 \end{pmatrix}$$

führt und final $s_{3,1}^{27/4}$ um zu

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -2/3 & 0 \\ 0 & 0 & -2/3 \end{pmatrix}$$

zu kommen und das hat strikte Zeilenstufenform.

Wollen wir nun etwa das assoziierte Gleichungssystem für $b = (1, 3, 4)$ lösen, so müssen wir die gleichen Schritte mit b durchführen, also erst

$$s_{2,3}^{-5/3} s_{1,3}^{-3/2} s_{1,2}^{-1/2}(1,3,4) = s_{2,3}^{-5/3} s_{1,3}^{-3/2}(1,5/2,4) = s_{2,3}^{-5/3}(1,5/2,5/2) = (1,5/2,-5/3)$$

und dann

$$s_{3,1}^{27/4} s_{3,2}^{3/2} s_{2,1}^{9/2}(1,5/2,-5/3) = s_{3,1}^{27/4} s_{3,2}^{3/2}(49/4,5/2,-5/3) = s_{3,1}^{27/4}(49/4,0,-5/3) = (1,0,-5/3)$$

(im letzten Schritte haben wir

$$\frac{49}{4} - \frac{27}{4} \cdot \frac{5}{3} = \frac{147}{12} - \frac{135}{12} = \frac{12}{12} = 1$$

benutzt). Aus 2.2 erhalten wir also

$$\mathrm{L}\left(\begin{pmatrix} 2 & 3 & 0 \\ 1 & 0 & 1 \\ 3 & 2 & 1 \end{pmatrix}; \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}\right) = \mathrm{L}\left(\begin{pmatrix} 2 & 3 & 0 \\ 0 & -2/3 & 1 \\ 0 & 0 & -2/3 \end{pmatrix}; \begin{pmatrix} 1 \\ 5/2 \\ -5/3 \end{pmatrix}\right) = \mathrm{L}\left(\begin{pmatrix} 2 & 0 & 0 \\ 0 & -2/3 & 0 \\ 0 & 0 & -2/3 \end{pmatrix}; \begin{pmatrix} 1 \\ 0 \\ -5/3 \end{pmatrix}\right)$$

und letzteres lässt sich mit Hilfe von 1.5 lösen (oder in diesem Fall sogar mit der Formel für Diagonalmatrizen). Das Ergebnis ist

$$\mathrm{L}\left(\begin{pmatrix} 2 & 3 & 0 \\ 1 & 0 & 1 \\ 3 & 2 & 1 \end{pmatrix}; \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}\right) = \left\{ \begin{pmatrix} 1/2 \\ 0 \\ 5/2 \end{pmatrix} \right\}$$

Der Einfachheit halber notiert man diese Übergänge oft einfach nur mit

$$\left(\begin{array}{ccc|c} 2 & 3 & 0 & 1 \\ 1 & 0 & 1 & 3 \\ 3 & 2 & 1 & 4 \end{array}\right) \overset{II-1/2I}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2 & 3 & 0 & 1 \\ 0 & -3/2 & 1 & 5/2 \\ 3 & 2 & 1 & 4 \end{array}\right)$$

$$\overset{III-3/2I}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2 & 3 & 0 & 1 \\ 0 & -3/2 & 1 & 5/2 \\ 0 & -5/2 & 1 & 5/2 \end{array}\right) \overset{III-5/3I}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2 & 3 & 0 & 1 \\ 0 & -2/3 & 1 & 5/2 \\ 0 & 0 & -2/3 & -5/3 \end{array}\right)$$

$$\overset{I+9/2II}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2 & 0 & 9/2 & 49/4 \\ 0 & -2/3 & 1 & 5/2 \\ 0 & 0 & -2/3 & -5/3 \end{array}\right) \overset{II+3/2III}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2 & 0 & 9/2 & 49/4 \\ 0 & -2/3 & 0 & 0 \\ 0 & 0 & -2/3 & -5/3 \end{array}\right)$$

$$\overset{I+27/4III}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2 & 0 & 0 & 1 \\ 0 & -2/3 & 0 & 0 \\ 0 & 0 & -2/3 & -5/3 \end{array}\right)$$

oder ähnlichem.

(2) Fassen wir die gleiche Matrix in $\mathbb{Z}/2$ auf erhalten wir

$$\begin{pmatrix}2&3&0\\1&0&1\\3&2&1\end{pmatrix} = \begin{pmatrix}0&1&0\\1&0&1\\1&0&1\end{pmatrix} \in \mathrm{Mat}(3,3,\mathbb{Z}/2)$$

Versuchen wir allgemein zu lösen, so müssen wir noch einen Zeilentausch vornehmen, bevor die Elimination beginnen kann. Wir erhalten

$$\left(\begin{array}{ccc|c}0&1&0&b_1\\1&0&1&b_2\\1&0&1&b_3\end{array}\right) \overset{I\leftrightarrow II,}{\rightsquigarrow} \left(\begin{array}{ccc|c}1&0&1&b_2\\0&1&0&b_1\\1&0&1&b_3\end{array}\right) \overset{III+1\cdot I}{\rightsquigarrow} \left(\begin{array}{ccc|c}1&0&1&b_2\\0&1&0&b_1\\0&0&0&b_2+b_3\end{array}\right)$$

Diese ist direkt in strikter Zeilenstufenform und wir können die Lösungsmenge ablesen: Es gibt eine Lösung genau dann, wenn $b_2 = b_3$. In diesem Fall können wir den dritten Eintrag frei wählen und erhalten dann das Bild von

$$\mathbb{Z}/2 \to \mathbb{Z}/2^3, \quad t \longmapsto (t+b_2, b_1, t)$$

als Beschreibung der Lösungsmenge. Wieder ist dies von der Gestalt

$$(t+b_2,b_1,t) = (\mathrm{L}(A))(t) + (\mathrm{L}(B))(b_1,b_2,b_3)$$

mit

$$A = \begin{pmatrix}t\\0\\t\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix}.$$

Der Beweis von Theorem 2.3 wird die Form einer induktiven Konstruktion der gesuchten Operationen haben. Wir brauchen noch eine Notation: Es sei $A[i,j] \in \mathrm{Mat}(k-1,n-1,R)$ diejenige Matrix, die aus $A \in \mathrm{Mat}(k,n,R)$ durch Streichen der $i$ten Zeile und $j$ten Spalte hervorgeht, also formal

$$A[i,j]_{a,b} = \begin{cases} A_{a,b} & a<i, b<j \\ A_{a+1,b} & i \leqslant a, b<j \\ A_{a,b+1} & a<i, j \leqslant b \\ A_{a+1,b+1} & i \leqslant a, j \leqslant b \end{cases}$$

2.5. Konstruktion Wir konstruieren zuerst die zweite Folge von Operationen. Wir konstruieren e induktiv über k, die Zeilenanzahl. Für $k=1$ (und n beliebig), also Matrizen mit nur einer Zeile ist nichts zu tun. Ebenso ist die Behauptung für die Nullmatrix offensichtlich. Sei dann $0 \neq A \in \mathrm{Mat}(k+1,n,R)$ und für jede Matrix mit höchstens k Zeilen sei die Aussage wahr. Sei noch $h = \frac{(k+1)(k+2)}{2}$. Sei n_0 der kleinste Index einer Spalte in A, die nicht komplett aus 0 besteht. Ist dann etwa $A_{j,1} \neq 0$ für $1 \leqslant j \leqslant n$ so setzen wir $e(h) = \mathrm{t}_{1,j}$ und $e(h-i) = \mathrm{s}_{1,i+1}^{-A_{i+1,n_0}/A_{j,n_0}}$ für $1 \leqslant i \leqslant k$ (die auftauchende Division hier ist möglich, da es um Matrizen mit Einträgen in einem Körper geht). Setze dann

$$B := \big(e(h-k) \circ e(h-k+1) \circ \cdots \circ e(h)\big)(A).$$

Die Spalten vor n_0 bestehen sicherlich immer noch nur aus 0. Weiterhin gilt per Konstruktion

$$B_{i,n_0} = \begin{cases} A_{j,1} & i=1 \\ 0 & 2 \leqslant i \leqslant k+1 \end{cases}$$

Mit anderen Worte die ersten n_0 Spalten von B sehen aus wie bei einer Matrix in Zeilenstufenform.

Betrachte dann $B[1,n_0] \in \mathrm{Mat}(k,n-1,R)$. Per Induktionsannahme gibt es eine Folge $e'(i)$ mit $1 \leqslant i \leqslant \frac{k(k+1)}{2}$, von Elementaroperationen die $B[1,n_0]$ in Zeilenstufenform überführen. Zu jeder Zeilenoperation $e'(i)$ auf $k \times (n-1)$-Matrizen, sei $e(i)$ die "gleichnamige Zeilenoperation eine Zeile niedriger" auf $(k+1) \times n$-Matrizen, also

$$e(i) = \mathrm{s}_{a+1,b+1}^{\lambda} \quad \text{falls} \quad e'(i) = \mathrm{s}_{a,b}^{\lambda}$$

und

$$e(i) = \mathrm{t}_{a+1,b+1} \quad \text{falls} \quad e'(i) = \mathrm{t}_{a,b}$$

Wir rechnen dann noch

$$\frac{(k+1)k}{2} = \frac{(k+1)k+2}{2} - 1 = \frac{(k+1)(k+2)-2k}{2} - 1 = h-k-1$$

so dass wir diese $e(i)$ vorne an die oben definierten $e(h-k), \dots, e(h)$ anhängen können. Die Matrix

$$\big(e(1) \circ \cdots \circ e(h-k-1) \circ e(h-k) \circ \cdots \circ e(l)\big)(A) = \big(e(1) \circ \cdots \circ e(h-k-1)\big)(B)$$

hat dann Zeilenstufenform, wie man leicht überprüft.

Um von hier zur strikten Zeilenstufenform zu gelangen gehen wir ähnlich vor. Für $k = 1$ ist jede Zeilenstufenmatrix schon strikt. Für $0 \neq Z \in \mathrm{Mat}(k+1, n, R)$ mit Zeilenrang l und Zeugenfunktion $r\colon \{1, \dots, l\} \to \{1, \dots, n\}$, setzen wir wieder $h = \frac{l(l-1)}{2}$ und dann $f(h-i) = \mathrm{s}_{i+2,1}^{-Z_{1,r(i+2)}/Z_{i+2,r(i+2)}}$ für $0 \leqslant i \leqslant l-2$ (diesmal ist die auftauchende Division möglich, da $Z_{j,r(j)}$ für alle j als Einheit angenommen ist). Dann ist in

$$W = \big(f(h-l+2) \circ \cdots \circ f(h)\big)(Z)$$

die erste Zeile in strikter Form: Es gilt $W_{1,r(i)} = 0$ für $2 \leqslant i \leqslant l$. Dann betrachte $W[1,1] \in \mathrm{Mat}(k, n-1, R)$. Per Induktionsannahme gibt es dann eine Folge $f'(i)$ mit $1 \leqslant i \leqslant \frac{(l-2)(l-1)}{2}$ bestehend aus elementaren Operationen vom Typ I auf $\mathrm{Mat}(k, n-1, R)$. Wir lassen $f(i)$ wie oben die Operationen mit dem gleichen Namen auf $\mathrm{Mat}(k+1, n, r)$ "eine Zeile niedriger" bezeichnen und rechnen

$$\frac{(l-2)(l-1)}{2} = \frac{l(l-1)-2\cdot l+2}{2} = h-l+1 = h-(l-2)-1,$$

sodass wir diese wieder zu einer Folge $f(1), \cdots, f(h)$ zusammenfügen können. Wieder prüft man leicht, dass

$$\big(f(1) \circ \cdots \circ f(h-l+1) \circ f(h-l+2) \circ \cdots \circ (h)\big)(Z) = \big(f(1) \circ \cdots \circ f(h-l+1)\big)(W)$$

nun wirklich strikte Zeilenstufenform hat.

2.6. Korollar *Für jede Matrix $A \in \mathrm{Mat}(k, n, K)$ mit Einträgen in einem (Schief-)Körper K, gibt es eine Teilmenge $S \subseteq \{1, \dots, n\}$ mit $|S| \geqslant n-k$ derart dass, für alle $b \in K^k$ die Menge $\mathrm{L}(A; b)$ entweder leer ist, oder die Abbildung*

$$\begin{aligned} \mathrm{L}(A;b) \subseteq K^n = \mathrm{F}(\{1,\dots,n\}, K) &\longrightarrow \mathrm{F}(S, K) \cong K^{|S|} \\ x &\longmapsto x_{|S} \end{aligned}$$

bijektiv ist.

Insbesondere folgt, dass, über einem endlichen Körper mit k Elementen, die Anzahl der Lösungungen eine linearen Gleichung immer eine Potenz von k ist (nämlich $k^{|S|}$ in der Terminologie des Korollars), ein Fakt der wohl nicht auf der Hand liegt.

Die Anzahl $|S|$ der Elemente von S heißt in der Physik meist die Anzahl der Freiheitsgrade des Gleichungssystems. Man beachte aber, dass eine Teilmenge S wie im Korollar nicht eindeutig bestimmt ist: Im zweiten Beispiel von 2.4 könnte man anstatt der dritten Koordinate, etwa auch die erste frei wählen: Das Bild der Abbildung

$$\mathbb{Z}/2 \longrightarrow \mathbb{Z}/2^3, \quad t \longmapsto (t, b_1, t+b_2)$$

stimmt mit dem der dort berechneten Abbildung

$$\mathbb{Z}/2 \longrightarrow \mathbb{Z}/2^3, \quad t \longmapsto (t+b_2, b_1, t)$$

überein. Und es ist überhaupt nicht klar, dass verschiedene Teilmengen S, die die Conclusio von 2.6 erfüllen, die *gleiche* Anzahl haben, sobald K unendlich viele Elemente hat, wie etwa im Falle $K = \mathbb{Q}$.

Dies ist eine der ersten strukturellen Aussagen, denen wir uns nun zuwenden wollen. Als ein weiteres Phänomen haben wir in den Beispielen beobachten können, dass sich die Lösungsmenge

$\mathrm{L}(A;b)$ durch Angabe zweier Matrizen beschreiben lässt, wenn sie nicht leer ist: Eine, die den Fall $b = 0$ abdeckt und das verhalten der freien zu wählenden Variablen beschreibt, und eine die die Abhängigkeit von b beschreibt. Auch das ist ein allgemeines Phänomen wie wir sehen werden.

3. Moduln und Vektorräume

Die Entwicklung einer systematischeren Theorie beginnt mit folgenden Beobachtungen. Die Menge R^n erbt eine Gruppenstruktur durch komponentenweise Addition in R, also $(x+y)_i = x_i+y_i$ (das haben wir auch oben schon benutzt, und es war eine Übungsaufgabe auf dem sechsten Zettel). Desweiteren gibt es eine Abbildung $R^n \times R \longrightarrow R^n$, die *Skalarmultiplikation*, gegeben durch $(x \cdot r)_i = x_i \cdot r$. Mit diesen beiden Strukturen können wir die Abbildungen $\mathrm{L}(A)$ für Matrizen A genau charakterisieren:

3.1. Lemma *Die Abbildung*

$$\mathrm{L}\colon \mathrm{Mat}(k,n,R) \longrightarrow \mathrm{F}(R^n,R^k)$$

ist injektiv und ihr Bild besteht aus genau denjenigen Abbildungen $\varphi\colon R^n \to R^k$, die die folgenden Eigenschaften haben:

(1) φ ist ein Gruppenhomomorphismus, also $\varphi(x+y) = \varphi(x) + \varphi(y)$ für alle $x, y \in R^n$, und
(2) φ ist homogen, also $\varphi(x \cdot r) = \varphi(x) \cdot r$ für alle $x \in R^n$ und $r \in R$.

Bezeichnen wir das Bild von L im Vorgriff auf 3.2 unten einmal mit $\mathrm{Lin}_R(R^n,R^k)$, so ist die Umkehrabbildung durch

$$\mathrm{M}\colon \mathrm{Lin}_R(R^n,R^k) \longrightarrow \mathrm{Mat}(k,n,R), \quad \varphi \longmapsto [(i,j) \mapsto (\varphi(e_j))_i]$$

gegeben, wobei

$$e_j\colon \{1,\dots,n\} \to R, \quad i \longmapsto \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

den $j$ten *Einheitsvektor (unit vector)* bezeichnet.

Beweis. Zunächst überprüfen wir, dass $\mathrm{L}(A)$ wirklich immer R-linear ist: Dazu rechnen wir

$$\begin{aligned}
(\mathrm{L}(A)(x+y))_i &= \sum_{j=1}^{n} A_{i,j} \cdot (x+y)_i \\
&= \sum_{j=1}^{n} A_{i,j} \cdot (x_i + y_i) \\
&= \sum_{j=1}^{n} A_{i,j} \cdot x_i + A_{i,j} \cdot y_i) \\
&= \left(\sum_{j=1}^{n} A_{i,j} \cdot x_i\right) + \left(\sum_{j=1}^{n} A_{i,j} \cdot y_i\right) \\
&= (\mathrm{L}(A)(x))_i + (\mathrm{L}(A)(y))_i \\
&= (\mathrm{L}(A)(x) + \mathrm{L}(A)(y))_i
\end{aligned}$$

und

$$\begin{aligned}
(\mathrm{L}(A)(x \cdot r))_i &= \sum_{j=1}^{n} A_{i,j} \cdot (x \cdot r)_i \\
&= \sum_{j=1}^{n} A_{i,j} \cdot x_i \cdot r \\
&= \left(\sum_{j=1}^{n} A_{i,j} \cdot x_i\right) \cdot r \\
&= (\mathrm{L}(A)(x)) \cdot r)_i
\end{aligned}$$

Als dann beweisen wir, dass M und L wirklich invers zueinander sind: Für alle $\varphi\colon R^n \to R^k$ und $x \in \mathrm{R}^n$ rechnen wir:

$$\begin{aligned}
\mathrm{L}(\mathrm{M}(\varphi))(x) &= [i \mapsto \sum_{j=0}^{n} \mathrm{M}(\varphi)_{i,j} \cdot x_j] \\
&= [i \mapsto \sum_{j=0}^{n} \varphi(e_j)_i \cdot x_j] \\
&= [i \mapsto \sum_{j=0}^{n} \varphi(e_j \cdot x_j)_i] \\
&= \left[i \mapsto \varphi\left(\sum_{j=0}^{n} e_j \cdot x_j \right)_i \right] \\
&= [i \mapsto \varphi(x)_i] \\
&= \varphi(x)
\end{aligned}$$

und für jedes $A \in \mathrm{Mat}(k, n, R)$

$$\mathrm{M}(\mathrm{L}(A))_{i,j} = ((\mathrm{L}(A))(e_j))_i = \sum_{k=0}^{n} A_{i,k} \cdot (e_j)_k = A_{i,j}.$$

□

Insbesondere spielt die komponentenweise Multiplikation auf R^n, die es natürlich auch gibt, keine Rolle in diesen Betrachtungen. Wir axiomatisieren die benötigte Struktur in der wohl zentralen Definition dieses ganzen Semesters:

3.2. Definition Sei R ein Ring. Ein *Modul (module)* über R ist eine abelsche Gruppe $(M, +, 0)$ zusammen mit einer Funktion

$$\cdot\colon M \times R \longrightarrow M$$

der *Skalarmultiplikation (scalar multiplication)* derart, dass

(1) $m \cdot 1 = m$,
(2) $m \cdot (r \cdot s) = (m \cdot r) \cdot s$,
(3) $m \cdot (r + s) = (m \cdot r) + (m \cdot s)$, und
(4) $(m + n) \cdot r = (m \cdot r) + (n \cdot r)$

für alle $m, n \in M$ und $r, s \in R$ gelten. Ist R eine (Schief-)Körper so spricht man anstatt von einem Modul meist von einem *Vektorraum (vector space)*.

Für zwei R-Moduln M und N heißt eine Abbildung $f\colon M \to N$ *R-linear* oder auch ein *R-Modulhomomorphismus*, falls

(1) f ist ein Gruppenhomomorphismus
(2) $f(m \cdot r) = f(m) \cdot r$ für alle $m \in M$ und $r \in R$.

Wir bezeichnen die Menge der R-linearen Abbildungen $M \to N$ mit

$$\mathrm{Lin}_R(M, N) \subseteq \mathrm{F}(M, N).$$

Weil wir es häufig benutzen müssen, beobachten wir sofort, dass

$$m \cdot 0 + 0 = m \cdot 0 = m \cdot (0 + 0) = m \cdot 0 + m \cdot 0$$

woraus durch Addition des Inversen von $m \cdot 0$ sofort $m \cdot 0 = 0$ folgt. Weiter rechnen wir:

$$m + m \cdot (-1) = m \cdot 1 + m \cdot (-1) = m \cdot (1 + (-1)) = m \cdot 0 = 0$$

was $-m = m \cdot (-1)$ für dieses Inverse bedeutet.

3.3. Beispiel Es gibt viele Beispiele von Moduln: Das wohl wichtigste haben wir natürlich schon gesehen: R^n für irgendein $n \in \mathbb{N}$.

Allgemeiner sieht man aber leicht, dass für einen R-Modul M auch $\mathrm{F}(S, M)$ für jede Menge S einen R-Modul bildet: Die Addition ist gegeben durch die Verknüpfung

$$\mathrm{F}(S, M) \times \mathrm{F}(S, M) \to \mathrm{F}(S, M) \quad (f, g) \longmapsto [s \to f(s) + g(s)],$$

das neutrale Element ist $\mathrm{const}_0 \colon S \to M$ und die Skalarmultiplikation durch

$$\mathrm{F}(S, M) \times R, \quad (f, r) \longmapsto [s \to f(s) \cdot r].$$

Hieraus kann man schon extrem viele neue Beispiele kreieren:

3.4. Definition Ist M ein R-Modul und $N \subseteq M$ so heißt N ein *Untermodul (submodule)* von M, falls gilt

(1) $0 \in N$,
(2) $m + m' \in N$ für alle $m, m' \in N$, und
(3) $m \cdot r \in N$ für alle $m \in N$ und $r \in R$.

Die Bedingungen besagt genau, dass sich die Addition und Skalarmulitplikation von M zu Abbildungen

$$+ \colon N \times N \longrightarrow N \quad \text{und} \cdot \colon N \times R \longrightarrow N$$

einschränken, die dann offenbar N für sich genommen zu einem R-Modul machen: Die einzige Beobachtung, die man machen muss ist, dass N auch abgeschlossen unter additiven Inversen ist. Aber wir haben oben $-m = m \cdot (-1)$ gesehen, und für $m \in N$ ist die rechte Seite per Definition in N.

3.5. Beispiel

(1) Ist $f \colon M \to N$ R-linear und $U \subseteq N$ ein R-Untermodul, so ist $f^{-1}(U) \subseteq M$ ebenfalls ein R-Untermodul. Insbesondere trifft dies auf

$$\ker(f) := f^{-1}(0) = \{m \in M \mid f(m) = 0\}$$

zu und damit auch für jede Matrix $A \in \mathrm{Mat}(k, n, R)$ auf $\mathrm{L}(A)^{-1}(0) \subseteq R^n$, die Menge der Lösungen des linearen Gleichungssystems mit rechter Seite 0, zu.

(2) Ist $f \colon M \to N$ R-linear und $U \subseteq M$ ein R-Untermodul, so ist $f(U) \subseteq N$ ebenfalls ein R-Untermodul. Insbesondere trifft dies auf $\mathrm{Im}(f)$ selbst zu, und damit auch für für jede Matrix $A \in \mathrm{Mat}(k, n, R)$ auf die Menge

$$\{b \in R^k \mid \mathrm{L}(A; b) \neq \varnothing\} = \mathrm{Im}(\mathrm{L}(A)) \subseteq R^k$$

aller derjenigen rechten Seiten des zu A gehörigen linearen Gleichungssystems, für die es eine Lösung gibt.

(3) Für jede Menge S und jeden R-Modul M ist die Menge

$$\mathrm{F}^{\mathrm{fs}}(S, M) := \{f \colon S \to M \mid f(s) = 0 \text{ für fast alle } s \in S\} \subseteq \mathrm{F}(S, M)$$

ein Untermodul von $\mathrm{F}(S, M)$ (fs steht hier für finite support und natürlich besteht Gleichheit falls S endlich ist). Die Summierungsabbildung

$$\Sigma \colon \mathrm{F}^{\mathrm{fs}}(S, M) \longrightarrow M$$

aus 1.20 ist R-linear.

(4) Wann immer M und N R-Moduln sind und R kommutativ ist, bildet $\mathrm{Lin}_R(M, N) \subseteq \mathrm{F}(M, N)$ einen R-Untermodul, wenn wir dem Ziel die Modulstruktur aus 3.3 geben (die insbesondere nicht von der Modulstruktur von M abhängt, sondern nur von der unterliegenden Menge).

(5) Besonders hervorzuheben ist hier der Fall $N = R$. Der Modul $\mathrm{Lin}_R(M, R)$ heißt der zu M *duale* Modul, oder im Falle, dass R ein Körper ist einfach der *Dualraum* von M; wieder bedarf dies der Kommutativität von R.

(6) Ist R kommutativ, so bildet die Menge der *polynomiellen Abbildungen (polynomial functions)* $R \to R$, also

$$\mathrm{Pol}(R) := \left\{ f\colon R \to R \mid \exists r_0, \dots r_n \in R\colon \forall s \in R\colon f(s) = \sum_{i=0}^{n} r_i s^i \right\} \subseteq \mathrm{F}(R,R)$$

einen R-Untermodul.

(7) Ähnlich bildet für R einen kommutativen geordneten Ring bildet die Menge der Funktionen mit höchstens polynomiellem Wachstum

$$\{f\colon R \to R \mid \exists g, h \in \mathrm{Pol}(R)\colon g(r) \leqslant f(r) \leqslant h(r) \forall r \in R\} \subseteq \mathrm{F}(R,R)$$

einen R-Untermodul. Insbesondere für $R = \mathbb{R}$, den Körper der reellen Zahlen, aber auch schon für $R = \mathbb{Z}$ spielt dieser eine große Rolle in in verschiedensten Disziplinen der Mathematik. Die polynomiellen Wachstumsschranken, kann man übrigends durch Schranken aus jedem Untermodul von $\mathrm{F}(R,R)$ ersetzen.

(8) Es gibt noch viele weitere Beispiele von interessanten Untermoduln von $\mathrm{F}(S,R)$ für verschiedenste S und R. In der Analysis sind Ihnen vielleicht schon die Untervektorräume

$$\{f\colon \mathbb{N} \to \mathbb{R} \mid f \text{ ist konvergent}\}$$

und

$$\{f\colon \mathbb{N} \to \mathbb{R} \mid \text{die Partialsummen von } f \text{ sind absolut konvergent}\}$$

von $\mathrm{F}(\mathbb{N},\mathbb{R})$ begegnet, und sie werden zum Beispiel noch auf die vier Untervektorräume

$$\mathrm{C}(I,\mathbb{R}), \quad \mathrm{C}^{\mathrm{n}}(I,\mathbb{R}), \quad \mathrm{C}^{\infty}(I,\mathbb{R}) \quad \text{und} \quad \mathrm{C}^{\omega}(I,\mathbb{R})$$

von $\mathrm{F}(I,\mathbb{R})$ der stetigen, n-fach stetig differenzierbaren für $1 \leqslant n \in \mathbb{N}$, glatten und analytischen Funktionen $I \to \mathbb{R}$ auf einem offenen Intervall $I \subseteq \mathbb{R}$ treffen. Ebenso wird es mit

$$\{f\colon I \to \mathbb{R} \mid f \text{ ist Riemann integrierbar}\}$$

und später noch

$$\{f\colon I \to \mathbb{R} \mid f \text{ ist Lebesque integrierbar}\}$$

sein.

Abbildungen wie

$$\lim\colon \{f\colon \mathbb{N} \to \mathbb{R} \mid f \text{ ist konvergent}\} \longrightarrow \mathbb{R}$$

$$(-)'\colon \mathrm{C}^{\mathrm{n}+1}(I,\mathbb{R}) \longrightarrow \mathrm{C}^{\mathrm{n}}(I,\mathbb{R})$$

$$\int_I\colon \{f\colon I \to \mathbb{R} \mid f \text{ ist Riemann integrierbar}\} \longrightarrow \mathbb{R}$$

für I kompakt sind alle $\mathbb{R}$-linear.

3.6. Beobachtung Sind $\varphi\colon M \to N$ und $\psi\colon N \to P$ R-lineare Abbildungen zwischen R-Moduln, so ist auch $\psi \circ \varphi$ R-linear. Ist φ bijektiv, so ist auch φ^{-1} R-linear.

Das bedeutet insbesondere, dass für $M = R^m$, $N = R^n$ und $P = R^k$ und $A \in \mathrm{Mat}(k,n,R)$, $B \in \mathrm{Mat}(n,m,R)$ die Abbildung $\mathrm{L}(A) \circ \mathrm{L}(B)$ wieder von der Form $\mathrm{L}(C)$ für eindeutiges $C \in \mathrm{Mat}(k,m,R)$. Dieses C ist gegeben als Bild von (A,B) unter:

3.7. Definition Die komponierte Abbildung

$$\mathrm{Mat}(k,n,R) \times \mathrm{Mat}(n,m,R) \xrightarrow{\mathrm{L}\times\mathrm{L}} \mathrm{Lin}_R(R^n,R^k) \times \mathrm{Lin}_R(R^m,R^n) \xrightarrow{\circ} \mathrm{Lin}_R(R^m,R^k) \xrightarrow{\mathrm{M}} \mathrm{Mat}(k,m,R)$$

heißt *Matrixmultiplikation*.

Es gelten dann per Konstruktion

$$\mathrm{L}(A) \circ \mathrm{L}(B) = \mathrm{L}(A \cdot B) \quad \text{und} \quad \mathrm{M}(\varphi \circ \psi) = \mathrm{M}(\varphi) \cdot \mathrm{M}(\psi).$$

3.8. Lemma *Für einen Ring R und $A \in \mathrm{Mat}(k,n,R), B \in \mathrm{Mat}(n,m,R)$ gilt*

$$(A \cdot B)_{i,j} = \sum_{p=1}^{n} A_{i,p} \cdot B_{p,j}$$

für alle $1 \leqslant i \leqslant k$ und $1 \leqslant j \leqslant n$.

Als Schlagwort sagt man, dass man $(A \cdot B)_{i,j}$ erhält, indem man die i-te Zeile von A mit der j-ten Spalte von B termweise multipliziert und aufsummiert. Insbesondere kann man Matrizen A und B wirklich nur dann multiplizieren, wenn die Spaltenzahl von A mit der Zeilenzahl von B übereinstimmt.

Beweis. Wir rechnen:

$$\begin{aligned}
(A \cdot B)_{i,j} &= \mathrm{M}(\mathrm{L}(A) \circ \mathrm{L}(B))_{i,j} \\
&= \big(\mathrm{L}(A)((\mathrm{L}(B))(e_j))\big)_i \\
&= \big(\mathrm{L}(A)(l \mapsto \sum_{p=1}^{m} B_{l,p} \cdot (e_j)_p)\big)_i \\
&= \big((\mathrm{L}(A))(l \mapsto B_{l,j})\big)_i \\
&= (l \mapsto \sum_{p=1}^{n} A_{l,p} \cdot B_{p,j})_i \\
&= \sum_{p=1}^{n} A_{i,p} \cdot B_{p,j}
\end{aligned}$$

□

3.9. Beispiel (1) Für $A \in \mathrm{Mat}(k,n,R)$ gilt $(\mathrm{L}(A))(x) = A \cdot x$, wenn man $x \in R^n$ als $n \times 1$-Matrix auffasst. Insbesondere ist

$$\mathrm{L}(A;b) = \{x \in R^n \mid A \cdot x = b\}.$$

(2) Die Matrixmultiplikation erbt Assoziativität von der Verknüpfung von Funktionen und

$$\mathbb{I}_n := \mathrm{M}(\mathrm{id}_{R^n}) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in \mathrm{Mat}(n,n,R),$$

die *Einheitsmatrix*, erfüllt $A \cdot \mathbb{I}_n = A$ und $\mathbb{I}_n \cdot B = B$.

(3) Insbesondere bildet $(\mathrm{Mat}(n,n,R), \cdot, \mathbb{I}_n)$ einen Monoid für jedes $n \in \mathbb{N}$, der vermöge L und M isomorph zu $(\mathrm{Lin}_R(R^n,R^n), \circ, \mathrm{id}_{R^n})$ ist. Eine Matrix $A \in \mathrm{Mat}(n,n,R)$ heißt *invertierbar*, falls sie eine Einheit in diesem Monoiden ist, also genau dann wenn $\mathrm{L}(A)$ bijektiv ist.

(4) Die Matrizenmultiplikation ist ebenso wie die Komposition von Funktionen nicht kommutativ; allgemein ergibt es für eine Matrizen $n \times k$-Matrix und eine $k \times m$-Matrix nicht einmal Sinn, sie in umgekehrter Reihenfolge zu multiplizieren. Aber selbst wenn $m = n$ gilt, sodass dies möglich ist, stimmen die Ergebnisse nicht überein:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 10 \\ 11 & 24 \end{pmatrix} \neq \begin{pmatrix} 13 & 18 \\ 11 & 16 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

in $\mathrm{Mat}(2,2,\mathbb{Z})$.

(5) Die elementaren Zeilenoperationen lassen sich durch Matrixmultiplikation realisieren: Zu $1 \leqslant a, c \leqslant n$ mit $a \neq c$ und $\lambda \in R$ definieren wir $\mathrm{S}^{\lambda}_{a,c} \in \mathrm{Mat}(n,n,R)$ durch

$$(\mathrm{S}^{\lambda}_{a,c})_{i,j} = \begin{cases} 1 & i = j \\ \lambda & i = c \wedge j = a \\ 0 & \text{sonst} \end{cases}$$

Dann gilt $\mathrm{s}^\lambda_{a,c}(A) = \mathrm{S}^\lambda_{a,c} \cdot A$ für alle $A \in \mathrm{Mat}(n,k,R)$. Und die Matrix $\mathrm{S}^\lambda_{a,c}$ ist als Konsequenz von 2.2 invertierbar; das Inverse ist $\mathrm{S}^{-\lambda}_{a,c}$.

Ähnliches findet man für die Operationen $\mathrm{t}_{a,c}$ und m^λ_a, das ist eine Aufgabe auf dem 9. Zettel.

(6) Hier noch ein konrektes Beispiel: Es gilt

$$\begin{pmatrix}1&2&0\\0&3&5\end{pmatrix}\cdot\begin{pmatrix}1&0&2&5\\0&0&3&2\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&0&8&9\\5&10&24&26\end{pmatrix}$$

in $\mathrm{Mat}(2,4,\mathbb{Z})$.

3.10. Beobachtung Ist $\varphi\colon M \to N$ eine R-lineare Abbildung zwischen zwei R-Moduln, so gilt für jedes $x \in M$ mit $\varphi(x) = n$, dass

$$-+x\colon \ker(\varphi) \longrightarrow \varphi^{-1}(b)$$

bijektiv ist. Die Umkehrabbildung ist durch $m \mapsto m - x$ gegeben.

Man beobachte nur, dass $\varphi(m+x) = \varphi(m) + \varphi(x) = \varphi(m) + b$, sodass $\varphi(x+m) = b$ genau dann gilt, wenn $\varphi(m) = 0$.

3.11. Korollar *Ist $\varphi\colon M \to N$ eine R-lineare Abbildung zwischen zwei R-Moduln, so ist φ schon dann injektiv, wenn $\ker(\varphi) = \{0\}$ gilt.*

3.12. Beispiel (1) Für $A \in \mathrm{Mat}(k,n,R)$ und jedes $x \in \mathrm{L}(A;b)$ ist

$$-+x\colon \ker(\mathrm{L}(A)) = \mathrm{L}(A;0) \longrightarrow \mathrm{L}(A,b)$$

bijektiv. Gibt es also überhaupt ein Element $x \in R^n$ mit $A \cdot x = b$, so lässt sich eine beliebige Lösung in $l \in \mathrm{L}(A;b)$ eindeutig als Summe $x+m$ schreiben, mit $A \cdot m = 0$. Der Slogan ist: Die allgemeine Lösung eines inhomogenen linearen Gleichungssystem, ist Summe einer partikulären Lösung und der allgemeinen Lösung des homogenen Gleichungssystems. Das Wort *homogen* bezeichnet hier Gleichungssysteme mit verschwindender rechter Seite.

(2) Die Beobachtung lässt sich aber auch in vieler anderer Situation anwenden: Suchen wir etwa die Stammfunktionen einer gegebenen stetigen Funktion $b\colon I \to \mathbb{R}$, also alle stetig differenzierbaren Funktionen $f\colon I \to \mathbb{R}$ mit $f' = b$, so ist nach Wahl irgendeiner Stammfunktion $F\colon I \to \mathbb{R}$, jede andere von der Form $F + g$ für genau ein $g\colon I \to \mathbb{R}$ mit $g' = 0$, was genau bedeutet, dass g constant ist. Insbesondere liefert für jedes $i \in I$ die Abbildung $g \mapsto g(i)$ eine Bijektion zwischen den Stammfunktionen von f und $\mathbb{R}$, vollständig analog zu 2.6.

Um die Struktur der linearen Gleichungssysteme assoziiert zu A zu verstehen, reicht es also $\mathrm{Ker}(\mathrm{L}(A))$ (die Menge der homogenen Lösungen) und $\mathrm{Im}(\mathrm{L}(A))$ (die Menge der lösbaren Systeme) zu verstehen.

Die Matrixmultiplikation erlaubt uns auch eine konzeptionelle Perspektive auf das Eliminationsverfahren, die genau dies leistet: Gegeben $A \in \mathrm{Mat}(k,n,K)$, wo K ein (Schief-)Körper ist, so lässt sich die Serie der nötigen Zeilenoperationen um A in Zeilenstufenform zu überführen nach 3.9 durch eine Serie von Linksmultiplikationen mit invertierbaren Matrizen in $\mathrm{Mat}(k,k,K)$ realisieren. Ihr Produkt ist dann ebenfalls invertierbar, sodass wir erhalten:

3.13. Korollar *Zu jedem $A \in \mathrm{Mat}(k,n,K)$ mit K einem (Schief-)Körper, existiert ein invertierbares $B \in \mathrm{Mat}(k,k,K)$, sodass $B \cdot A \in \mathrm{Mat}(k,n,K)$ strikte Zeilenstufenform hat.*

Hat $B \cdot A$ etwa Zeilenrang l, so können wir 1.5 und 2.6 wie folgt uminterpretieren: Das Inverse der linearen Bijektion $\mathrm{Ker}(\mathrm{L}(A)) \longrightarrow K^{n-l}$ die wir dort produziert haben (und dies lässt sich direkt aus dem Eliminationsalgorithmus ablesen!), gibt eine lineare Injektion

$$\varphi\colon K^{n-l} \longrightarrow K^n$$

derart, dass

$$\mathrm{Im}(\varphi) = \mathrm{Ker}(\mathrm{L}(B \cdot A)) = \mathrm{Ker}(\mathrm{L}(A)).$$

Und $\mathrm{L}(A;b) \neq \varnothing$ gilt genau dann, wenn die letzten $k-l$ Einträge von $B \cdot b$ verschwinden. Die letzten $(k-l)$-Zeilen von B definieren also eine Abbildung

$$\psi\colon K^k \longrightarrow K^{k-l}$$

mit

$$\mathrm{Im}(\mathrm{L}(A)) = \mathrm{Ker}(\psi)$$

Man prüft leicht, dass ψ automatisch surjektiv ist.

Insgesamt stellt man diesen Sachverhalt gerne graphisch dar indem man sagt, dass

$$K^{n-l} \xrightarrow{\varphi} K^n \xrightarrow{\mathrm{L}(A)} K^k \xrightarrow{\psi} K^{k-l}$$

eine *exakte* Folge linearer Abbildungen ist.

Solche Abbildungen φ und ψ zu finden, führt zum Verständinis des Gleichungssystem in folgendem Sinne: Das Gleichungssystem $A \cdot x = b$ ist lösbar genau dann, wenn $\mathrm{M}(\varphi) \cdot b = 0$, und für eine fixe Lösung $x \in \mathrm{L}(A;b)$, lässt sich jede andere Lösung $\bar{x}$ eindeutig beschreiben als

$$\bar{x} = x + \mathrm{M}(\psi) \cdot y$$

für $y \in K^{n-l}$.

Die Frage, die es also noch zu klären gilt (wir hatten sie schon nach 2.6 formuliert), lautet also: Ist l, die Anzahl der Freiheitsgrade der linearen Gleichung durch A, eindeutig bestimmt?

4. Basen I

Um diese Frage anzugehen haben wir das Konzept einer Basis.

4.1. Beobachtung Ist M ein R-Modul und $S \subseteq M$, so ist

$$\langle S\rangle_R = \{x \in M \mid \exists r\colon S \to R\colon r(s) = 0 \text{ für fast alle } s \in S \wedge x = \sum_{s\in S} s \cdot r(s)\}$$

der kleinste R-Untermodul von M, der S enthält.

Man nennt $\langle S\rangle_R$ den von S *aufgespannten* Untermodul von M. Seine Elemente heißen *Linearkombinationen* von Elementen aus S.

4.2. Definition Ist M ein R-Modul und $S \subseteq M$, so heißt S ein *Erzeugendensystem (generating set)* von M, falls $\langle S\rangle_R = M$ gilt. S heißt *linear unabhängig (linearly independent)*, falls alle Darstellungen von Elementen in $\langle S\rangle_R$ als Linearkombinationen eindeutig sind, also falls für je zwei Funktionen $r, \bar{r}\colon S \to R$, mit $r(s) = 0 = \bar{r}(s)$ für fast alle $s \in S$ gilt, dass

$$\sum_{s\in S} s \cdot r(s) = \sum_{s\in S} s \cdot \bar{r}(s)$$

impliziert, dass $r = \bar{r}$. S heißt eine *Basis (basis)* von M, falls S ein linear unabhängiges Erzeugendensystem ist.

4.3. Beispiel (1) Per Konstruktion bilden die Funktionen

$$e_s\colon S \longrightarrow R, \quad t \longmapsto \begin{cases} 1 & t = s \\ 0 & t \neq s \end{cases}$$

eine Basis von $\mathrm{F}^{\mathrm{fs}}(S,R)$: Es gilt ja schließlich tautologischerweise

$$\sum_{s\in S} e_s \cdot f(s) = f.$$

Insbesondere bilden $\{e_1, \ldots, e_n\} \subseteq R^n$ eine Basis.

(2) Jede Teilmenge einer linear unabhängigen Menge ist selbst wieder linear unabhängig. Andersherum ist jede Teilmenge die ein Erzeugendensystem enthält, selbst wieder ein Erzeugendensystem.

(3) Da in einer Linearkombination immer nur endlich viele Koeffizienten nicht verschwinden, ist eine Teilmenge $S \subseteq M$ genau dann linear unabhängig, wenn alle ihre endlichen Teilmengen es sind.
(4) Die leere Teilmenge ist immer linear unabhängig, und M selbst (und auch $M\backslash\{0\}$) ist immer ein Erzeugendensystem von M. Insbesondere ist $\varnothing$ eine Basis den R-Moduls $\{0\}$.
(5) Ist $\varphi\colon M \to N$ injektiv, so ist $\varphi(S)$ linear unabhängig, falls S es ist, und ist $\varphi\colon M \to N$ surjektiv so ist $\varphi(S)$ ein Erzeugendensystem, falls S es ist. Ist φ bijektiv, so schickt es also Basen auf Basen.
(6) Insbesondere ist für jedes invertierbare $B \in \mathrm{Mat}(n, n, R)$ auch $\{B_1, \ldots, B_n\}$ mit $B_i = B \cdot e_i$ eine Basis von R^n. Bemerke, dass B_i genau die i-te Spalte der Matrix B ist.
(7) Allgemeiner ist für jedes $A \in \mathrm{Mat}(k, n, R)$ die Menge $\{A_1, \ldots, A_n\}$ der Spalten von A ein Erzeugendensystem von R^k, aber nicht unbedingt eine Basis.
(8) Ist K ein (Schief-)Körper, so kann man laut 2.6 eine Basis von $\ker(\mathrm{L}(A)) = \mathrm{L}(A; 0)$ wie folgt erhalten: Man wähle eine Teilmenge $S \subseteq \{1, \ldots, n\}$ derart, dass die Projektion
$$p\colon \mathrm{L}(A; 0) \longrightarrow \mathrm{F}(S, K),$$
(die natürlich linear ist !) bijektiv ist. Dann bilden die Urbilder $p^{-1}(e_s)$ von den e_s mit $s \in S$ eine Basis von $\mathrm{L}(A; 0)$.
(9) Nicht jeder Modul hat eine Basis, etwa kann $\mathbb{Z}/n$ keine Basis über $\mathbb{Z}$ haben: Da $x \cdot n = 0 = x \cdot 0$ für jedes $x \in \mathbb{Z}/n$ gilt, ist $\varnothing$ die einzige linear unahängige Teilmenge von $\mathbb{Z}/n$. Auch $\mathbb{Q}$ hat als $\mathbb{Z}$-Modul keine Basis.

4.4. Beobachtung Eine Teilmenge $S \subseteq M$ ist genau dann linear unabhängig, wenn für jede Funktion $r\colon S \to R$ mit $r(s) = 0$ für fast alle $s \in S$ aus $\sum_S s \cdot f(s) = 0$ schon $r = \mathrm{const}_0$ folgt. Mit anderen Worten S ist linear unabhängig, wenn es Darstellung der 0 als Linearkombination aus S gibt.

Für den Beweis betrachte man einfach
$$0 = m - m = \sum_S s \cdot r(s) - \sum_S s \cdot \bar{r}(s) = \sum_S s \cdot (r(s) - \bar{r}(s))$$
falls sich m durch r und $\bar{r}$ darstellen lässt, und schließt $r(s) - \bar{r}(s) = 0$.

4.5. Beobachtung Mithilfe dieser Beobachtung können wir also nun einfach entscheiden, ob eine gegebene Ansammlung von k Elementen $\{v_1, \ldots, v_k\} \in K^n$ linear unabhängig ist: Hierfür muss man einfach nur prüfen, ob
$$\{(\lambda_1, \ldots, \lambda_k) \in K^k \mid \sum_{i=1}^{n} v_i \cdot \lambda_i = 0\} = \{(0, \ldots, 0)\}$$
gilt. Aber die linke Seite ist nichts anderes als $\mathrm{Ker}(\mathrm{L}(V)) = \mathrm{L}(V, 0)$, wo $V \in \mathrm{Mat}(n, k, K)$ diejenige Matrix ist, deren $i$te Spalte genau v_i ist. Und $\mathrm{L}(V, 0)$ können wir mittels des Gauß-Algorithmus einfach bestimmen.

Ähnlich können wir bestimmen, ob $\{v_1, \ldots, v_k\} \in K^n$ ein Erzeugendensystem ist: Das ist schließlich genau die Frage, ob
$$\{(\lambda_1, \ldots, \lambda_k) \in K^k \mid \sum_{i=1}^{n} v_i \cdot \lambda_i = b\} \neq \varnothing$$
für jedes $b \in K^n$ gilt, aber die linke Seite ist genau $\mathrm{L}(V, b)$, sodass wir auch dies mittels des Gauß-Algorithmus entscheiden können.

4.6. Beispiel Sei $R = \mathbb{Z}/5$. Wir betrachten folgende Vektoren $v_1, v_2, v_3 \in \mathbb{Z}/5^4$:
$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 3 \\ 2 \\ 1 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ 0 \\ 3 \\ 4 \end{pmatrix}$$

Daraus konstruieren wir die Matrix $V \in \mathrm{Mat}(4,3,\mathbb{Z}/5)$, deren $j$te Spalte durch v_j gegeben ist, und wenden darauf den Gauß-Algorithmus an, um sie in Zeilenstufenform zu bringen (dabei fassen wir einige Schritte zusammen):

$$\begin{pmatrix}1&0&1\\2&3&0\\3&3&3\\4&1&4\end{pmatrix} \overset{\substack{II-2I\\III-3I\\IV-4I}}{\rightsquigarrow} \begin{pmatrix}1&0&1\\0&3&4\\0&3&0\\0&1&0\end{pmatrix} \overset{\substack{III-II\\IV-2II}}{\rightsquigarrow} \begin{pmatrix}1&0&1\\0&3&4\\0&0&1\\0&0&2\end{pmatrix} \overset{IV-III}{\rightsquigarrow} \begin{pmatrix}1&0&1\\0&3&4\\0&0&1\\0&0&0\end{pmatrix}$$

Hier können wir nun sowohl ablesen, ob $\{v_1, v_2, v_3\}$ linear unabhängig ist, als auch, ob es ein Erzeugendensystem ist:

- Die Menge $\{v_1, v_2, v_3\}$ ist linear unabhängig, weil in der Zeilenstufenform in jeder Spalte eine neue Stufe hinzukommt: Das bedeutet gerade, dass die Zeugenfunktion $r : \{1,2,3\} \to \{1,2,3\}$ surjektiv ist, also ist mit Beobachtung 1.5 $L(V;0) = \{0\}$. In anderen Worten: Für $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}/5$ mit $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0$ folgt bereits, dass $\lambda_1 = \lambda_2 = \lambda_3 = 0$ ist.
- Die Menge $\{v_1, v_2, v_3\}$ ist kein Erzeugendensystem, weil in der Zeilenstufenform mindestens eine Nullzeile vorkommt: Das bedeutet gerade, auch nach Beobachtung 1.5, dass $\big(L(V)\big)(x) = b$ nicht für alle $b \in \mathbb{Z}/5^4$ lösbar ist, also kann nicht jeder Vektor in $\mathbb{Z}/5^4$ als Linearkombination der v_i dargestellt werden.

Wir betrachten nun die folgenden Vektoren $w_1, w_2, w_3, w_4 \in \mathbb{Z}/5^3$:

$$w_1 = \begin{pmatrix}1\\2\\3\end{pmatrix}, w_2 = \begin{pmatrix}0\\3\\2\end{pmatrix}, w_3 = \begin{pmatrix}1\\0\\0\end{pmatrix}, w_4 = \begin{pmatrix}1\\0\\3\end{pmatrix}$$

Wir konstruieren eine Matrix $W \in \mathrm{Mat}(3,4,\mathbb{Z}/5)$, deren $j$te Spalte durch w_j gegeben ist. Darauf wenden wir wieder den Gauß-Algorithmus an:

$$\begin{pmatrix}1&0&1&1\\2&3&0&0\\3&2&0&3\end{pmatrix} \overset{\substack{II-2I\\III-3I}}{\rightsquigarrow} \begin{pmatrix}1&0&1&1\\0&3&3&3\\0&2&2&0\end{pmatrix} \overset{III-4II}{\rightsquigarrow} \begin{pmatrix}1&0&1&1\\0&3&3&3\\0&0&0&3.\end{pmatrix}$$

Wieder lässt sich ablesen, ob $\{w_1, w_2, w_3, w_4\}$ linear unabhängig und/oder ein Erzeugendensystem ist:

- Die Menge $\{w_1, w_2, w_3, w_4\}$ ist nicht linear unabhängig, da nun mindestens eine Spalte (nämlich die dritte) keine neue Stufe enthält: Das heißt gerade, dass mit Beobachtung 1.5 $L(W;0)$ in Bijektion zu $\mathbb{Z}/5^1$ steht, also keine eindeutige Lösung hat. Genauer heißt es sogar, dass sich die dritte Spalte (also w_3) als Linearkombination der ersten zwei Spalten darstellen lässt, es ist nämlich $w_3 = w_1 + w_2$.
- Die Menge $\{w_1, w_2, w_3, w_4\}$ ist aber ein Erzeugendensystem, da in der Zeilenstufenform keine Nullzeile erscheint: Mit Beobachtung 1.5 heißt das genau, dass das lineare Gleichungssystem $\big(L(W)\big)(x) = b$ für jedes $b \in \mathbb{Z}/5^3$ lösbar ist, sich also jeder Vektor in $\mathbb{Z}/5$ als Linearkombination von w_1, w_2, w_3, w_4 darstellen lässt.

Die folgenden Sätze sind in gewisser Weise die Hauptergebnisse der gesamten Vorlesung:

4.7. Satz *Sei R ein Ring mit $1 \neq 0$, M ein R-Modul und $S \subseteq M$ eine Basis. Dann folgt:*

(1) S ist maximal unter allen linear unabhängigen Teilmengen von V, und
(2) S ist minimal unter allen Erzeugendensystemen von V.

Ist R ein (Schief-)Körper, so gilt gelten auch die Umkehrungen: S ist eine Basis genau dann, wenn S eine maximale linear unabhängige Teilmenge ist und auch genau dann, wenn S ein minimales Erzeugendensystem ist.

4.8. Bemerkung Der Fall, wo $1 = 0$ in R gilt ist in jeder Hinsicht uninteressant: Es folgt, dann für jeden R-Modul M, dass $m = m \cdot 1 = m \cdot 0 = 0$, also $M = \{0\}$ und angewandt auf $M = R$ insbesondere auch $R = \{0\}$. Wir haben also nur den Fall des Nullrings ausgeschlossen. Und für ihn stimmt die Aussage auch nicht: $\varnothing$ und $\{0\}$ sind beides Basen von $\{0\}$. Ist $1 \neq 0$ in R, so

ist aber $\{0\}$ in keinem R-Modul linear unabhängig, da ja immer $0 \cdot 1 = 0 = 0 \cdot 0$, sodass es dann mindestens zwei Darstellungen der 0 also Linearkombinationen von $\{0\}$ gibt.

BEWEIS. Wir zeigen als erstes, dass jede Basis maximal linear unabhängig ist. Sei also $m \in M \backslash S$ derart, dass auch $S \cup \{m\}$ linear unabhängig ist. Dann existiert, da S ein Erzeugendensystem bildet eine Funktion $r\colon S \to M$ mit endlichem Träger, so dass

$$m = \sum_{s \in S} s \cdot r(s)$$

oder mit anderen Worten

$$0 = m \cdot (-1) + \sum_{s \in S} s \cdot r(s) = \sum_{s \in S \cup \{m\}} s \cdot \bar{r}(s)$$

mit

$$\bar{r}\colon S \cup \{m\} \longrightarrow R, \quad s \longmapsto \begin{cases} r(s) & s \neq m \\ -1 & s = m \end{cases}.$$

Es folgt dann aus der linearen Unabhängigkeit von $S \cup \{m\}$ also $-1 = 0$ und damit $0 = 1$, was wir ausgeschlossen hatten.

Ähnlich zeigen wir, dass jede Basis ein minimales Erzeugendensystem ist: Ist nämlich für ein $m \in S$ auch $S \backslash \{m\}$ ein Erzeugendensystem, so gibt es eine Funktion $r\colon S \backslash \{m\} \to R$ mit endlichem Träger, derart dass

$$m = \sum_{s \in S \backslash \{m\}} s \cdot r(s)$$

mit anderen Worten

$$0 = m \cdot (-1) + \sum_{s \in S \backslash \{m\}} s \cdot r(s) = \sum_{s \in S} s \cdot \bar{r}(s)$$

mit

$$\bar{r}\colon S \longrightarrow R, \quad s \longmapsto \begin{cases} r(s) & s \neq m \\ -1 & s = m \end{cases}$$

was der linearen Unabhängigkeit von S widerspricht.

Sei nun R ein (Schief-)Körper. Wir behaupten, dass für S linear unabhängig und $m \in M \backslash \langle S \rangle_R$ auch $S \cup \{m\}$ linear unabhängig ist. Schreiben wir nämlich

$$0 = \sum_{s \in S \cup \{m\}} s \cdot r(s)$$

für eine Funktion $r\colon S \cup \{m\} \to R$ mit endlichem Träger, so folgt aus $r(m) = 0$ sicherlich $r = \text{const}_0$ wegen der linearen Unabhängigkeit von S. Aber für $r(m) \neq 0$ folgt aufgrund der Annahme an R, dass $r(m)$ eine Einheit ist. Damit können wir schreiben

$$m = m \cdot r(m) \cdot \frac{1}{r(m)} = (m \cdot r(m) - \sum_{s \in S \cup \{m\}} s \cdot r(s)) \cdot \frac{1}{r(m)} = \sum_{s \in S} s \cdot \frac{r(s)}{r(m)},$$

im Widerspruch zu $m \notin \langle S \rangle_R$. Also kann es für maximal linear unabhängiges S kein $m \in M \backslash \langle S \rangle_R$ geben, mit anderen Worten, es muss $\langle S \rangle_R = M$ gelten, was S zu einer Basis macht.

Ist andererseits S ein Erzeugendensystem und

$$0 = \sum_{s \in S} s \cdot r(s)$$

für eine Funktion $r\colon S \to R$ mit endlichem Träger und $r(m) \neq 0$ für ein $m \in S$,

$$m = m \cdot r(m) \cdot \frac{1}{r(m)} = (m \cdot r(m) - \sum_{s \in S} s \cdot r(s)) \cdot \frac{1}{r(m)} = \sum_{s \in S \backslash \{m\}} s \cdot \frac{-r(s)}{r(m)}$$

Aber damit gilt für jedes $x \in M = \langle S \rangle_R$ mit Darstellung $x = \sum_{s\in S} s \cdot t(s)$ schon

$$x = \sum_{s\in S} s{\cdot}t(s) = m{\cdot}t(m) + \sum_{s\in S\setminus\{m\}} s{\cdot}t(s) = \sum_{s\in S\setminus\{m\}} s{\cdot}\frac{-r(s)}{r(m)} + \sum_{s\in S\setminus\{m\}} s{\cdot}t(s) = \sum_{s\in S\setminus\{m\}} s{\cdot}\frac{t(s)\cdot r(m) - r(s)}{r(m)}$$

und damit $x \in \langle S\setminus\{m\}\rangle_R$. Mit anderen Worten $S\setminus\{m\}$ ist dann auch ein Erzeugendensystem. In einem minimalen Erzeugendensystem kann in einer Darstellung $0 = \sum_{s\in S} s \cdot r(s)$ nie $r(m) \neq 0$ gelten, also muss $r = \text{const}_0$ sein. Nach 4.4 ist S dann aber linear unabhängig, also eine Basis. □

4.9. Korollar *Ist V ein Vektorraum über einem (Schief-)Körper K und E ein endliches Erzeugendensystem von V, so enthält E eine (sicherlich dann ebenfalls endliche) Basis S von V.*

Wir wollen uns nun überlegen, dass je zwei endliche Basen eines Vektorraums die gleiche Anzahl an Elementen haben. Dafür beobachten wir zunächst:

4.10. Beobachtung Im wesentlichen per definitionem ist $S \subseteq M$ genau dann eine Basis, wenn die Abbildung

$$\mathrm{L}_S \colon \mathrm{F}^{\mathrm{fs}}(S, R) \longrightarrow M, \quad f \longmapsto \sum_{s\in S} s \cdot f(s)$$

bijektiv ist; dass S ein Erzeugendensystem ist, bedeutet genau dass sie surjektiv ist, und dass S linear unabhängig ist, genau dass sie injektiv ist. Das Urbild eines Elementes $m \in M$ heißt die *Koordinatenfunktion* von m bezüglich S.

Ist S endlich, und $b \colon \{1, \dots, n\} \to S$ bijektiv, so erhalten wir insbesondere einen Isomorphismus von Vektorräumen (also eine bijektive lineare Abbildung)

$$\mathrm{L}_b \colon R^n \longrightarrow M, \quad x \longmapsto \sum_{i=1}^{n} b_i \cdot x_i.$$

Ein R-Modul, der eine n-elementige Basis besitzt, sieht also in gewisser Weise für alle Belange der linearen Algebra genau aus wie R^n mit der Standardbasis $\{e_1, \dots, e_n\}$.

4.11. Theorem *Sei K ein (Schief-)Körper und V ein K-Vektorraum, der eine endliche Basis B besitzt, sagen wir mit n Elementen. Ist dann $S \subseteq V$ linear unabhängig, so hat S höchstens n Elemente.*

Insbesondere ist jede Basis von V endlich und hat ebenfalls genau n Elemente.

Dieser Satz ermöglicht folgende Definition:

4.12. Definition Sei K ein (Schief-)Körper und V ein K-Vektorraum, der eine endliche Basis B besitzt. Dann heißt $|B| \in \mathbb{N}$ die *Dimension* $\dim_K(V)$ von V über K.

Insbesondere ist jeder endlich erzeugte K-Vektorraum V isomorph zu $K^{\dim_K(V)}$, jedoch auf ganz und gar nicht eindeutige Art.

Beweis. Wählen wir eine Nummerierung $b \colon \{1, \dots, n\} \to B$ mit zugehörigem Isomorphismus $\mathrm{L}_b \colon K^n \longrightarrow V$. Dann ist auch die Menge $\mathrm{Pre}_{\mathrm{L}_b}(S) \subseteq K^n$ linear unabhängig. Hat S mehr als n Element, so sei T eine $n+1$-elementige Teilmenge von S, zusammen mit einer Bijektion $v \colon \{1, \dots, n\} \to T$. Nach 4.5 hat dann die Matrix V mit den v_i als Spalten trivialen Kern. Sie hat aber n-Zeilen und $n+1$-Spalten, also folgt aus 2.6, dass der Kern in Bijektion mit K^r ist für ein $r \geqslant 1$. Insbesondere enthält er mehr als ein Element, was nicht sein kann. S kann also nur n Elemente enthalten.

Ist nun B' eine zweite Basis, so folgt ebenfalls $|B'| \leqslant n = |B|$. Vertauschen wir die Rollen von B und B' so erhalten wir auch $|B| \leqslant |B'|$. □

5. Basen II

Hiermit lässt sich nun unser Leitproblem lösen:

5.1. Satz (Dimensionsformel) *Ist V ein endlich dimensionaler Vektorraum über einem (Schief-)Körper K und $\varphi\colon V \to W$ K-linear $B \subseteq V$ derart, dass $\varphi_{|B}$ injektiv ist und $\varphi(B)$ eine Basis von $\mathrm{Im}(\varphi)$ ist, und $B' \subseteq V$ eine Basis von $\mathrm{Ker}(\varphi)$, so ist $B \cup B'$ eine Basis von V. Insbesondere gilt:*

$$\dim_K(\mathrm{Ker}(\varphi)) + \dim_K(\mathrm{Im}(\varphi)) = \dim_K(V)$$

Mengen B wie in diesem Satz existieren immer: Ist S eine (endliche!) Basis von V, so ist sicherlich $\varphi(S)$ ein (immer noch endliches) Erzeugendensystem von $\mathrm{Im}(\varphi)$. Verkleinern wir es zu einer Basis S' von $\mathrm{Im}(\varphi)$, siehe 4.9, und wählen für jedes Element von S' genau ein Urbild unter φ, so erhalten wir eine Menge $B \subseteq V$ wie oben gewünscht.

Auf der anderen Seite kennen wir nicht unmittelbar eine Basis oder überhaupt ein Erzeugendensystem von $\ker(\varphi)$. Im Falle $V = K^n$ und $W = K^k$ berechnet das ja gerade der Eliminationsalgorithmus! Dass $\mathrm{Ker}(\varphi)$ überhaupt eine Basis besitzt, ist aber auch a priori klar: Die maximale Anzahl linear unabhängiger Elemente von $\mathrm{Ker}(\varphi)$ ist schließlich durch die Dimension von V beschränkt. Der Prozess, einem gegebenen linear unabhängigen System in $\mathrm{Ker}(\varphi)$ einfach ein weiteres Element hinzufügen, falls das System noch nicht maximal ist, terminiert also nach spätestens $\dim_K(V)$ Schritten. Diese Methode ist aber für unendliches K natürlich völlig unpraktikabel.

5.2. Korollar *Lässt sich eine Matrix $A \in \mathrm{Mat}(k, n, K)$ für einen (Schief-)Körper K mittels elementarer Zeilenumformungen in Zeilenstufenform Z mit Zeilenrang l bringen, so gelten*

$$l = \dim_K \mathrm{Im}(\mathrm{L}(A)) \quad \textit{and} \quad n - l = \dim_K \mathrm{Ker}(\mathrm{L}(A)).$$

Insbesondere hat jedes solche Z den gleichen Zeilenrang.

5.3. Definition Ist V ein endlich dimensionaler Vektorraum über einem (Schief-)Körper K und $\varphi\colon V \to W$ K-linear, so nennt man $\dim_K(\mathrm{Im}(\varphi))$ den *Rang (rank)* von φ.

Beweis von 5.1 und 5.2. Wir prüfen, dass $B \cup B'$ ein Erzeugendensystem ist: Sei also $x \in V$. Dann gilt $\phi(x) = \sum_{b\in B} \varphi(b) \cdot r(b)$ für eine Funktion $r\colon B \to R$ mit endlichem Träger, da $\varphi(B)$ eine Basis von $\mathrm{Im}(\varphi)$ ist. Dann gilt aber

$$\varphi\left(x - \sum_{b\in B} b \cdot r(b)\right) = \varphi(x) - \sum_{b\in B} \varphi(b) \cdot r(b) = \varphi(x) - \varphi(x) = 0,$$

also $x - \sum_{b\in B} b \cdot r(b) \in \mathrm{Ker}(\varphi)$. Demzufolge gilt

$$x - \sum_{b\in B} b \cdot r(b) = \sum_{c\in B'} c \cdot s(c)$$

und damit

$$x = \sum_{b\in B} b \cdot r(b) + \sum_{c\in B'} c \cdot s(c),$$

was wir zeigen wollten.

Dann prüfen wir noch, dass $B \cup B'$ linear unabhängig ist. Sei dazu

$$0 = \sum_{b\in B} b \cdot r(b) + \sum_{c\in B'} c \cdot s(c).$$

Dann gilt

$$0 = \varphi(0) = \sum_{b\in B} \varphi(b) \cdot r(b) + \sum_{c\in B'} \varphi(c) \cdot s(c) = \sum_{b\in B} \varphi(b) \cdot r(b) = \sum_{y\in\varphi(B)} y \cdot r(\varphi_{|B}^{-1}(y)),$$

wobei der letzte Schritt benutzt, dass $\varphi_{|B}\colon B \to \varphi(B)$ per Annahme bijektiv ist. Es folgt, dann $r(b) = 0$ für alle $b \in B$ wodurch sich die erste Gleichung zu

$$0 = \sum_{c\in B'} c \cdot s(c)$$

vereinfacht, was $s(c) = 0$ impliziert.

In der konkreten Situation des Korollars, lernen wir aus 2.2, dass $\mathrm{Ker}(\mathrm{L}(A)) = \mathrm{Ker}(\mathrm{L}(Z))$ gilt und aus 4.3, dass $\mathrm{Ker}(\mathrm{L}(Z))$ eine Basis mit $n - l$ Elementen besitzt. Das zeigt die erste Formel, und die zweite ist dann eine Konsequenz der Dimensionsformel. □

5.4. Korollar *Sei K ein (Schief-)Körper und V ein endlichdimensionaler K-Vektorraum mit $\dim_K(V) = n$ und $S \subseteq V$ eine Teilmenge mit $|S| = n$. Dann sind äquivalent:*

(1) S ist eine Basis von V,
(2) S ist linear unabhängig, und
(3) S ist ein Erzeugendensystem.

Beweis. Ist nämlich S linear unabhängig, so ist es nach 4.11 auch maximal linear unabhängig, also eine Basis nach 4.7. Und ist S eine Erzeugendensystem, so enthält es nach 4.9 eine Basis, aber diese hat nach 4.11 ebenfalls n Elemente, es kann also auch nicht weggenommen werden. □

5.5. Korollar *Sei K ein (Schief-)Körper und $\varphi\colon V \to W$ eine K-linear zwische endlich dimensionalen K-Vektorräumen mit $\dim_K(V) = \dim_K(W)$. Dann sind äquivalent:*

(1) φ is injektiv,
(2) φ is surjektiv, und
(3) φ is bijektiv,

Beweis. Ist φ injektiv und B eine Basis von V, so hat $\varphi(B) \subseteq W$ immer noch n Elemente und ist linear unabhängig. Ergo ist es nach vorigem Korollar ein Erzeugendensystem von W und damit φ surjektiv, da $\mathrm{Im}(\varphi)$ natürlich ein Untervektorraum von W ist.

Ist φ surjektiv, so folgt aus der Dimensionsformel $\dim_K(\mathrm{Ker}(\varphi)) = 0$ und damit $\mathrm{Ker}(\varphi) = 0$, was nach 3.10 impliziert, dass φ injektiv ist. □

Formulieren wir dieses Resultat für Matrizen, so erhalten wir:

5.6. Korollar *charinjsurjbij Für eine Matrix $A \in \mathrm{Mat}(n, n, K)$ über einem (Schief-)Körper K sind äquivalent:*

(1) A ist invertierbar.
(2) die Spalten von A bilden eine Basis von K^n,
(3) die Zeilen von A bilden eine Basis von K^n,
(4) es existiert eine Matrix $B \in \mathrm{Mat}(n, n, K)$ mit $B \cdot A = \mathbb{1}_n$,
(5) es existiert eine Matrix $B \in \mathrm{Mat}(n, n, K)$ mit $A \cdot B = \mathbb{1}_n$.

Im Falle von (4) und (5) ist so eine Matrix B automatisch das Inverse A^{-1} von A.

Insbesondere gelten für lineare Gleichungssystem mit der gleichen Anzahl Variablen und Gleichungen (also solche die von $n \times n$-Matrizen kodiert werden) folgende Äquivalenzen:

(1) $\mathrm{L}(A; b)$ hat für irgendein $b \in K^n$ höchstens eine Lösung.
(2) $\mathrm{L}(A; b)$ hat für alle $b \in K^n$ höchstens eine Lösung.
(3) $\mathrm{L}(A; b)$ hat für jedes $b \in K^n$ mindestens eine Lösung.
(4) $\mathrm{L}(A; b)$ hat für jedes $b \in K^n$ genau eine Lösung.

Proof. Die Spalten von A sind gerade die Bilder der Basis $\{e_1, \ldots, e_n\}$ von K^n und $\mathrm{L}(A)$ und wenn A invertierbar ist, ist $L(A)$ bijektiv, und dieses Bild ist wieder eine Basis, also (1) ⇒ (2), und umgekehrt, bilden die Spalten ein Erzeugendensystem so ist $\mathrm{L}(A)$ surjektiv, also invertierbar nach vorigem Korollar und damit (2) ⇒ (1).

Ähnlich implizieren (4) bzw. (5), dass $\mathrm{L}(A)$ surjektiv bzw. injektiv ist, und damit nach vorigem Kororllar bijektiv. Sie implizieren also beide (1), und (1) ⇒ (4), (5) gilt nach Definition.

Und die lineare Unabhängigkeit der Zeilen schließlich ist nach scharfem Hinsehen äquivalent zu $\mathrm{Ker}(\mathrm{L}(A)) = \{0\}$, und damit nach 3.11 zur Injektivität von $\mathrm{L}(A)$, sodass das vorige Korollar noch eine drittes Mal zuschlägt. □

5.7. Bemerkung Die Charakterisierung des Inversen einer Matrix $A \in \mathrm{Mat}(n, n, K)$ in 5.6 liefert uns eine Möglichkeit es wirklich auszurechnen: Das Eliminationsverfahren bestimmt nach 3.13 ja schließlich eine invertierbare Matrix $B \in \mathrm{Mat}(n, n, K)$, derart dass $B \cdot A$ strikte Zeilenstufenform

hat. Aber A ist nach obigen Überlegungen genau dann invertierbar wenn $B \cdot A$ keine Nullzeile hat, aber im Falle quadatischer Matrix impliziert dies natürlich schon, dass $B \cdot A$ eine Diagonalmatrix ist (ohne Nullen auf der Diagonale). Multipliziert man nun noch (von links) mit derjenigen Diagonalmatrix D, mit $D_{i,i} = (B \cdot A)_i i^{-1}$ (das bedeutet genau Zeilenoperationen vom Typ II durchzuführen) so erhält man $D \cdot B \cdot A = \mathbb{1}_n$ und damit $D \cdot B = A^{-1}$.

5.8. Beispiel Sei $K = \mathbb{Z}/5$, $n = 3$ und

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix}.$$

Wir führen nun den Gauß-Algorithmus durch, um A auf strikte Zeilenstufenform zu überführen. Dann können wir die Matrix B, die die entsprechenden Zeilenumformungen vornimmt, wie folgt direkt mitberechnen: Wir schreiben neben A die Einheitsmatrix $\mathbb{1}_n$, und nehmen alle Zeilenoperationen auch an dieser vor:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 0 & 2 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & 0 & 1 \end{array}\right) \overset{II+1\cdot I}{\rightsquigarrow} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 3 & 0 & 0 & 1 \end{array}\right) \overset{III+2\cdot II}{\rightsquigarrow} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 3 & 2 & 2 & 1 \end{array}\right)$$

$$\overset{I-1\cdot II}{\rightsquigarrow} \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 0 & 4 & 0 \\ 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 3 & 2 & 2 & 1 \end{array}\right) \overset{I-1\cdot III}{\rightsquigarrow} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & 2 & 4 \\ 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 3 & 2 & 2 & 1 \end{array}\right) \overset{\substack{II\cdot 3 \\ III\cdot 2}}{\rightsquigarrow} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & 2 & 4 \\ 0 & 1 & 0 & 3 & 3 & 0 \\ 0 & 0 & 1 & 4 & 4 & 2 \end{array}\right).$$

Dabei ist die Matrix schon im vorletzten Schritt in strikter Zeilenstufenform, durch eine Zeilenmultiplikation können wir sie dann zu der Einheitsmatrix überführen. Somit haben wir auf der rechten Seite eine Matrix B, sodass $B \cdot A = \mathbb{1}_3$ ist—es ist also

$$A^{-1} = B = \begin{pmatrix} 3 & 2 & 4 \\ 3 & 3 & 0 \\ 4 & 4 & 2 \end{pmatrix}.$$

Basen erlauben es uns auch lineare Abbildungen zwischen anderen Moduln als den Standardbeispielen R^n zu beschreiben.

5.9. Lemma *Ist B eine Basis von einem R-Modul M, und N ein weiterer R-Modul, so ist die Einschränkungsabbildung*

$$\mathrm{Lin}_R(M, N) \longrightarrow \mathrm{F}(B, N), \quad \varphi \longmapsto \varphi_{|B}$$

bijektiv.

Mit anderen Worten die Werte einer linearen Abbildung auf einer Basis bestimmen die Abbildung vollständig, und können andererseits beliebig vorgegeben werden.

Beweis. Zur Injektivität: Sind φ und ψ zwei lineare Abbildungen, so ist

$$\{m \in M \mid \varphi(m) = \psi(m)\} = \mathrm{Ker}(\varphi - \psi)$$

ein Untermodul von M. Aber gilt $\varphi_{|B} = \psi_{|B}$, so enthält er mit B ein Erzeugendensystem von M, ist also schon ganz M und damit $\varphi = \psi$.

Zur Surjektivität: Eine Abbildung $f\colon B \to N$ bestimmt die Abbildung

$$\bar{f}\colon \mathrm{F}^{\mathrm{fs}}(B, R) \longrightarrow N, \quad g \longmapsto \sum_{b \in B} f(b) \cdot g(b)$$

von der man leicht prüft, dass sie R-linear ist. Auf der anderen Seite bestimmt B als Basis eine bijektive R-lineare Abbildung

$$\mathrm{L}_B\colon \mathrm{F}^{\mathrm{fs}}(B, R) \longrightarrow M, \quad g \longmapsto \sum_{b \in B} b \cdot g(b).$$

Die Komposition

$$M \xrightarrow{\mathrm{L}_B^{-1}} \mathrm{F}^{\mathrm{fs}}(B, R) \xrightarrow{\bar{f}} N$$

schickt ein $b \in B$ dann erst auf $e_b \in \mathrm{F}^{\mathrm{fs}}(B,R)$ und dieses auf $f(b) \in N$ wie gewünscht. □

Um dieses Lemma effektiv zu nutzen, haben wir noch:

5.10. Theorem (Steinitz'scher Ergänzungssatz) *Ist K ein (Schief-)Körper, und V ein K-Vektorraum, so existiert zu jeder linear unabhängigen Menge $S \subseteq V$ und jedem Erzeugendensystem $E \subseteq V$ eine Teilmenge $U \subseteq E\backslash S$, derart dass $S \cup U$ eine Basis von V bildet und $S \cap U = \varnothing$.*

Für endliche E ist der Beweis wieder konstruktiv, für allgemeines E jedoch nicht.

Beweis. Betrachte die Menge

$$X := \{V \subseteq E\backslash S \mid S \cup V \text{ ist linear unabhängig} \wedge S \cap V = \varnothing\}.$$

Ist E endlich, so auch die Potenzmenge $\mathcal{P}(E)$ und damit X. Es folgt aus einer Aufgabe auf dem 4. Zettel, dass X ein maximales Element U besitzt. Für allgemeines E werden wir dies unten aus dem Zorn'schen Lemma herleiten.

Wir behaupten: Für ein maximales Element U von X ist in jedem Falle $S \cup U$ eine Basis von V. Hierfür reicht es natürlich zu zeigen, dass $S \cup U$ ein Erzeugendensystem ist. Sei also $v \in V$ gegeben. Da E ein Erzeugendensystem ist gibt es eine Lineardarstellung

$$v = \sum_{e \in E} e \cdot r(e).$$

Aber für jedes $e \in E\backslash(S \cup U)$ ist $S \cup U \cup \{e\}$ nach Definition von U linear abhängig. Es gibt dann also eine Darstellung

$$0 = e \cdot q_e(e) + \sum_{s \in S \cup U} s \cdot q_e(s)$$

in der nicht alle Koeffizienten verschwinden. Aber wäre $q_e(e) = 0$, so würde aus der linearen Unabhängigkeit von $S \cup U$ schon $q_e = 0$ folgen. Also muss $q_e(e) \neq 0$ gelten, und damit lässt sich obigen Gleichung zu

$$e = \sum_{s \in S \cup U} s \cdot \frac{-q_e(s)}{q_e(e)}$$

umstellen. Einsetzen liefert

$$v = \sum_{e \in E} e \cdot r(e) = \sum_{s \in S \cup U} s \cdot r(s) + \sum_{e \in E\backslash(S \cup U)} e \cdot r(e) = \sum_{s \in S \cup U} s \cdot r(s) + \sum_{e \in E\backslash(S \cup U)} \sum_{s \in S \cup U} s \cdot \frac{-q_e(s) \cdot r(e)}{q_e(e)}$$

$$= \sum_{s \in S \cup U} s \cdot \left(r(s) + \sum_{e \in E\backslash(S \cup U)} \frac{-q_e(s) \cdot r(e)}{q_e(e)} \right) \in \langle S \cup U \rangle_R,$$

was zu zeigen war.

Erklären wir zum Schluss noch, woher ein maximales Element im allgemeinen kommt: Hierfür wenden wir das Zorn'sche Lemma auf X an, wofür wir nur prüfen müssen, dass jede Kette $C \subseteq X$ eine obere Schranke besitzt, also ein Element $D \in X$ mit $B \subseteq D$ für alle $B \in C$. Aber hierfür können wir $D = \bigcup C$ nehmen: Wir müssen nur $D \in X$ zeigen. Aber sicherlich gilt $S \cap D = \varnothing$, da für ein $v \in S \cap D$ per Definition von D ein $B \in C$ existieren muss mit $v \in S \cap B$, was aber unmöglich ist. Und ähnlicherweise ist $S \cup D$ linear unabhängig. Hierfür reicht es zu prüfen, dass jede endliche Teilmenge von $T \subseteq S \cup D$ linear unabhängig ist (da in einer beliebigen Linearkombination per Definition nur endlich viele Koeffizienten nicht verschwinden dürfen). Aber dann gilt schon $T \subseteq S \cup B$ für ein $B \in C$: Ist etwa $T = \{t_i, \ldots, t_k\}$, so gibt es per Definition von D Mengen $B_1, \ldots, B_k \in C$ mit $t_i \in S \cup B_i$. Aber da C eine Kette ist, muss eines der B_i ein größtes Element von $\{B_1, \ldots, B_k\}$ sein, und damit gilt $T \subset B_i$ wie gewünscht. □

5.11. Korollar *Ist K ein (Schief-)Körper, so hat jeder K-Vektorraum eine Basis.*

Proof. Man nehme $S = \varnothing$ und $E = V$ in obigem Satz. □

Wie versprochen, lassen sich mit Hilfe des Ergänzungssatzes lineare Abbildungen mit gegebenen Eigenschaften konstruieren. Zum Beispiel:

5.12. Korollar *Jeder Untervektorraum $U \subseteq K^n$ eines K-Vektorraums V ist Lösungsmenge eines homogenen Gleichungssystems, das heißt $\mathrm{L}(A, 0) = U$ für ein $A \in \mathrm{Mat}(n - \dim_K(U), n, K)$.*

Beweis. Sei B eine Basis von U. Nach dem Ergänzungssatz gibt es eine Teilmenge $T \subseteq \{e_1, \ldots, e_n\}$, sodass $B \cup T$ eine Basis von K^n bildet und $B \cap T = \varnothing$. Wähle weiter eine bijektive Abbildung $c\colon \{1, \ldots, n - \dim_K(U)\} \to T$.

Sei dann gemäß 5.9 $\varphi\colon K^n \to K^{n-\dim_K(U)}$ die eindeutige lineare Abbildung mit

$$\varphi(c) = \begin{cases} 0 & b \in B \\ e_i & b = c(i) \end{cases}.$$

Dann gilt sicherlich $U \subseteq \mathrm{Ker}(\varphi)$ und da φ alle Einheitsvektoren von $K^{n-\dim_K(U)}$ trifft, ist φ surjektiv. Nach der Dimensionsformel gilt dann aber

$$\dim_K(\mathrm{Ker}(\varphi)) = n - (n - \dim_K(U)) = \dim_K(U)$$

und damit nach 5.4 $\mathrm{Ker}(\varphi) = U$. Die Matrix $A = \mathrm{M}(\varphi)$ tut also das gewünschte. □

5.13. Korollar *Ist V ein endlich dimensionaler K-Vektorraum, K ein (Schief-)Körper und sind $v, w \in V$ Elemente mit $v \neq 0$ und $w \neq 0$, so gibt es eine bijektive lineare Abbildung $\varphi\colon V \to W$ mit $\varphi(v) = w$.*

Man sagt, dass endlichdimensionale Vektorräume weg von 0 *homogen* sind: Es gibt keinerlei Eigenschaften, die sich nur in Termen der Vektorraumaxiome formulieren lassen, mit denen sich Elemente v von V unterscheiden lassen, außer eben $v = 0$. Für Moduln über allgemeineren Ringen ist das nicht wahr: Etwa ist "teilbar durch 2" eine solche Eigenschaft auf dem $\mathbb{Z}$-Modul $\mathbb{Z}$: Keine bijektive lineare Selbstabbildung $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ kann jemals 1 und 2 vertauschen (überhaupt kann nie $\varphi(2) = 1$ gelten).

Proof. Sei B eine Basis von V. Dann können wir $\{v\}$ durch Elemente von B zu einer Basis B' ergänzen, und ebenso $\{w\}$ zu einer Basis B''. Diese haben beide ebensoviele Element wie B, insbesondere gibt es eine Bijektion $f\colon B'\backslash\{v\} \to B''\backslash\{w\}$. Wir können dann φ als die jenige lineare Abbildung wählen mit

$$\varphi(b) = \begin{cases} w & b = v \\ f(b) & b \in B'\backslash\{v\} \end{cases}.$$

Zu prüfen ist nur noch, dass φ bijektiv ist, aber man prüft leicht, dass die eindeutige Abbildung $\psi\colon V \to V$ mit

$$\psi(b) = \begin{cases} v & b = w \\ f^{-1}(b) & b \in B''\backslash\{w\} \end{cases}$$

invers zu φ ist. □

6. Eine Anwendung auf endliche Körper

Als eine vielleicht etwas unerwartete Anwendung der Existenz von Basen haben wir:

6.1. Theorem *Ist K ein endlicher Körper, so gibt es eine eindeutige Primzahl p und ein eindeutiges $n \in \mathbb{N}$ mit $n > 0$, derart dass $|K| = p^n$.*

Es gibt also keine endlichen Körper mit 6 oder 10 Elementen. Für den Beweis starten wir mit zwei einfachen Beobachtungen:

6.2. Beobachtung (1) Ist $\varphi\colon R \to S$ ein Ringhomomorphismus und M ein S-Modul, so definiert

$$M \times R \longrightarrow M, \quad (m, r) \longmapsto m \cdot \varphi(r)$$

eine R-Modulstruktur auf M. Den so entstehenden R-Modul nennt man häufig $\varphi^* M$.

(2) Ist R ein (Schief-)Körper und $S \neq \{0\}$, so ist φ automatisch injektiv: Aufgefasst als Abbildung $R \to \varphi^* S$ ist φ nämlich R-linear, und daher $\operatorname{Ker}(\varphi) \subseteq R$ ein Untervektorraum. Aber da $\dim_R R = 1$ (das Element 1 ist schließlich eine Basis von R über R), folgt entweder $\dim_R(\operatorname{Ker}(\varphi)) = 0$ oder $\dim_R(\operatorname{Ker}(\varphi)) = 1$. Im ersten Fall ist φ nach 3.11 injektiv, im zweiten Fall erhalten wir aus 5.4, dass $\operatorname{Ker}(\varphi) = R$ also $\varphi = \operatorname{const}_0$ und damit $1 = \varphi(1) = 0$ in S, was $S = \{0\}$ bedeutet.

Wir wollen dies anwenden auf einen Homomorphismus $\mathbb{Z}/p \to K$. Diesen erhalten wir aus:

6.3. Satz *Ist K ein Integritätsbereich und der eindeutig bestimmte Ringhomomorphismus $\psi\colon \mathbb{Z} \to K$ nicht injektiv, so ist die Menge*

$$\{n \in \mathbb{N} \mid n > 0 \wedge \psi(n) = 0\}$$

nicht leer und ihr kleinstes Element p prim. Weiter faktorisiert ψ über einen eindeutigen Homomorphismus

$$\varphi\colon \mathbb{Z}/p \to K,$$

welcher injektiv ist.

Ist insbesondere K ein Körper, so nennt man das p aus diesem Satz die *Charakteristik* von K, geschrieben $\operatorname{char}(K) = p$. Ist $\psi\colon \mathbb{Z} \to K$ andererseits injektiv, so erweitert ψ zu einem injektiven Homomorphismus $\mathbb{Q} \to K$ (im wesentlichen nach Definition von $\mathbb{Q}$). In diesem Falle setzt man $\operatorname{char}(K) = 0$.

Jeder Körper K einhält also einen der Körper $\mathbb{Z}/p$ oder $\mathbb{Q}$, welche man deshalb die *Primkörper (prime fields)* nennt, je nach Charakteristik.

Beweis. Fassen wir ψ als $\mathbb{Z}$-lineare Abbildungn $\mathbb{Z} \to \psi^* K$ auf, folgt aus 3.11, dass $\operatorname{Ker}(\psi) \neq \{0\}$. Mit einem $n \in \mathbb{Z}$ enthält $\operatorname{Ker}(\psi)$ dann aber auch $-n$, und damit sicherlich eine positive natürliche Zahl, wie behauptet. Sei nun p die kleinste solche. Gilt dann $p = k \cdot l$ für $1 < k, l < p$, so folgt

$$0 = \varphi(p) = \varphi(k \cdot l) = \varphi(k) \cdot \varphi(l)$$

und damit $0 = \varphi(k)$ oder $0 = \varphi(l)$, da R ein Integritätsbereich ist, im Widerspruch zur Wahl von p. Also muss p prim sein. Zuletzt prüfen wir, dass die Komposition $\mathbb{N} \to \mathbb{Z} \to K$ mit der Äquivalenzrelation, die $\mathbb{Z}/p$ definiert, verträglich ist. Sind also $m, n \in \mathbb{N}$ mit $\operatorname{rem}_p(m) = \operatorname{rem}_p(n)$, etwa

$$m = q \cdot p + b \quad \text{und} \quad n = r \cdot p + b,$$

so folgt in der Tat

$$\psi(m) = \psi(q \cdot p + b) = \psi(q) \cdot \psi(p) + \psi(b) = \psi(b) = \psi(r) \cdot \psi(p) + \psi(b) = \psi(n).$$

Wir erhalten also in der Tat eine eindeutig bestimmte Abbildung $\varphi\colon \mathbb{Z}/p \to K$ mit $\varphi([m]_p) = \psi(m)$ für alle $m \in \mathbb{N}$. Dass sie ein Ringhomomorphismus ist, folgt direkt aus der Definition von Addition und Multiplikation auf $\mathbb{Z}/p$, und dass ψ injektiv ist, folgt aus obiger Beobachtung, da $\mathbb{Z}/p$ ja ein Körper ist. □

Beweis von 6.1. Sicherlich kann der Homomorphismus $\mathbb{Z} \to K$ nicht injektiv sein, wenn K endlich ist, also gibt es nach 6.3 einen Ringhomomorphismus $\varphi\colon \mathbb{Z}/p \to K$, wo p die Charakteristik von K ist. Benutzen wir ihn um K als $\mathbb{Z}/p$-Vektorraum $\varphi^* K$ aufzufassen, so ist $\varphi^* K$ sicherlich endlich erzeugt (etwa von K selbst), hat also nach 4.9 eine endliche Basis, sagen wir $\dim_{\mathbb{Z}/p}(\varphi^* K) = n$. Dann gibt es aber eine $\mathbb{Z}/p$-lineare Bijektion

$$(\mathbb{Z}/p)^n \longrightarrow \varphi^* K$$

und die linke Seite hat p^n Elemente, also $\varphi^* K = K$ ebenfalls. □

Der Beweis liefert noch etwas mehr Information, als nur die Anzahl der Elemente von K: Wir sehen beispielsweise auch, dass die der Addition in K unterliegende abelsche Gruppe isomorph zu $\mathbb{Z}/p^n$ sein muss. Über die Multiplikation in K liefert obiger Beweis allerdings keine Information, ebensowenig darüber, ob es zu gegeben p und n wirklichen einen (und wenn ja wie viele) Körper mit p^n Elementen gibt.

7. Basiswechsel

Schlussendlich wollen wir noch sehen, dass Basen auch in abstrakten Vektorräumen benutzt werden können um lineare Abbildungen zu verstehen:

7.1. Definition Ist M ein Modul über einem Ring R vor, so nennen wir eine Abbildung $b\colon \{1,\dots,n\} \to V$ eine *nummerierte Basis* von M, falls b injektiv ist und $\mathrm{Im}(b)$ eine Basis von M.

Ist nun N ein weiterer R-Modul so können wir zu einer R-linearen Abbildung $\varphi\colon M \to N$ die Komposition

$$R^n \xrightarrow{\mathrm{L}_b} M \xrightarrow{\varphi} N \xrightarrow{\mathrm{L}_{b'}^{-1}} R^k$$

betrachten, die auf eindeutige Weise von einer Matrix in $\mathrm{Mat}(k,n,R)$ beschrieben wird.

7.2. Korollar *Haben M und N nummerierte Basen b und b' der Länge n und k wie oben, so ist*

$$\mathrm{Lin}_R(M,N) \longrightarrow \mathrm{Mat}(k,n,R), \quad \varphi \longmapsto \mathrm{M}(\mathrm{L}_{b'}^{-1} \circ \varphi \circ \mathrm{L}_b)$$

eine R-lineare Bijektion. Insbesondere bilden für $1 \leqslant i \leqslant k$ und $1 \leqslant j \leqslant n$ die eindeutigen R-linearen Abbildungen $\varphi_{i,j}\colon M \to N$ mit

$$\varphi_{i,j}(b_a) = \begin{cases} 0 & a \neq j \\ b'_i & a = j \end{cases}$$

eine Basis von $\mathrm{Lin}_R(M,N)$

7.3. Definition Die Matrix $\mathrm{M}(\mathrm{L}_{b'}^{-1} \circ \varphi \circ \mathrm{L}_b)$ heißt die *Darstellungsmatrix (representing matrix)* von φ bezüglich der nummerierten Basen b und b'. Wir bezeichnen sie mit mit $\mathrm{M}(\varphi, b, b')$.

Per Konstruktion ist $\mathrm{M}(\varphi,b,b')_{i,j}$ der i-te Koeffizient in einer linearen Darstellung von $\varphi(b_j)$ in Termen der Basis b'. Mit anderen Worten, die Matrix $\mathrm{M}(\varphi,b,b')$ ist durch die Gleichungen

$$\varphi(b_j) = \sum_{i=1}^{k} b'_i \cdot \mathrm{M}(\varphi,b,b')_{i,j}$$

eindeutig bestimmt.

Beweis. Aus vorigem Lemma entnehmen wir, dass die Restriktionsabbildung

$$\mathrm{Lin}_R(M,N) \xrightarrow{-\circ b} \mathrm{F}(\{1,\dots,n\},N)$$

bijektiv ist. Aber mit $\mathrm{L}_{b'}$ ist auch

$$\mathrm{F}(\{1,\dots,n\},N) \xrightarrow{\mathrm{L}_{b'}^{-1}} \mathrm{F}(\{1,\dots,n\},R^k)$$

bijektiv und eine Aufgabe vom dritten Übungszettel liefert eine Bijektion

$$\mathrm{F}(\{1,\dots,n\},R^k) = \mathrm{F}(\{1,\dots,n\},\mathrm{F}(\{1,\dots,k\},R)) \longrightarrow \mathrm{F}(\{1,\dots,k\}\times\{1,\dots,n\},R) = \mathrm{Mat}(k,n,R).$$

Man prüft nun leicht, dass die Komposition dieser drei R-linearen Abbildungen genau die Abbildung aus dem Korollar ist. Für die letzte Aussage reicht es zu beobachten, dass die Abbildungen $\varphi_{i,j}$ und dem Isomorphismus zu $\mathrm{Mat}(k,n,R)$ genau denjenigen Matrizen entsprechen, deren Einträge alle 0 sind, außer dem an Stelle (i,j), wo eine 1 steht. Diese bilden offenbar eine Basis von $\mathrm{Mat}(n,k,R)$. □

7.4. Korollar *Es gilt*

$$\dim_K(\mathrm{Lin}_K(V,W)) = \dim_K(V) \cdot \dim_K(W)$$

für endlich dimensionale Vektorräume V und W über einem (Schief-)Körper K.

7.5. Beobachtung Darstellende Matrizen sind in folgendem Sinne mit Komposition kompatibel: Ist $b''\colon \{1,\dots,l\} \to P$ eine nummierte Basis und $\psi\colon N \to P$ eine weitere lineare Abbildung, so gilt

$$\mathrm{M}(\psi \circ \varphi, b, b'') = \mathrm{M}(\psi, b', b'') \cdot \mathrm{M}(\varphi, b, b'),$$

da

$$(\psi \circ \varphi)(b_j) = \psi(\varphi(b_j)) = \psi\left(\sum_{i=1}^{k} b'_i \cdot \mathrm{M}(\varphi, b, b')_{i,j}\right) = \sum_{i=1}^{k} \psi(b'_i) \cdot \mathrm{M}(\varphi, b, b')_{i,j}$$

$$= \sum_{i=1}^{k}\sum_{a=1}^{l} b''_a \cdot \mathrm{M}(\psi, b', b'')_{a,i} \cdot \mathrm{M}(\varphi, b, b')_{i,j} = \sum_{a=1}^{l} b''_a \cdot (\mathrm{M}(\psi, b', b'') \cdot \mathrm{M}(\varphi, b, b'))_{a,j}$$

7.6. Beispiel Hier einige tautologische Beispiele:

(1) Es gilt $M(\varphi, e, e) = M(\varphi)$ für $M = R^n$ und $N = R^k$ und die Standardbasis auf beiden Seiten, was die ähnliche Notation rechtfertigt.
(2) Es gilt $\mathrm{M}(\mathrm{id}, b, b) = \mathbb{1}_n$ für jede nummerierte Basis b. Insbesondere folgt $\mathrm{M}(\mathrm{id}, b, \bar{b}) = \mathrm{M}(\mathrm{id}, \bar{b}, b)^{-1}$ für je zwei nummierte Basen des gleichen Moduls.
(3) Direkt nach Definition ist die i-te Spalte von $\mathrm{M}(\mathrm{id}, b, e)$ ist immer genau b_i; mit anderen Worten, die Basiswechselmatrix $\mathrm{M}(\mathrm{id}, e, b)$ entsteht durch nebeneinanderfügen der Vektoren b_i und invertieren der enstandenen Matrix.
(4) Ist φ bijektiv, so ist mit b auch $\varphi \circ b$ eine nummerierte Basis und es gilt $\mathrm{Mat}(\varphi, b, \varphi \circ b) = \mathbb{1}_n$.

7.7. Definition Die Matrix $\mathrm{M}(\mathrm{id}, b, \bar{b}) \in \mathrm{Mat}(n, n, R)$ heißt die *Basiswechselmatrix (base change matrix)* von b zu b' für zwei nummerierte Basen der Länge n eines R-Moduls M.

Insbesondere sind Basiswechselmatrizen immer invertierbar, und erfüllen

$$b_j = \sum_{i=1}^{n} b'_i \cdot \mathrm{M}(\mathrm{id}, b, \bar{b})_{i,j},$$

sie bestehen also genau aus den Koeffizienten um b als Linearkombinationen von b' darzustellen.

Sind nun b und $\bar{b}$ nummerierte Basen von M und b' und $\bar{b}'$ nummierte Basen von N, so haben wir

$$\mathrm{M}(\varphi, \bar{b}, \bar{b}') = \mathrm{M}(\mathrm{id}_N, b', \bar{b}') \cdot \mathrm{M}(\varphi, b, b') \cdot \mathrm{M}(\mathrm{id}_M, \bar{b}, b)$$

und die äußeren beiden Matrizen sind invertierbar.

Dies erlaubt es uns den Eliminationsalgorithmus noch einmal umzuinterpretieren. Für das beste Ergebnis, führen wir noch ein:

7.8. Definition Eine Matrix $Z \in \mathrm{Mat}(k, n, R)$ in strikter Zeilenstufenform heißt *reduziert*, falls für die Zeugenfunktion $r\colon \{1,\dots,l\} \to \{1,\dots,n\}$ und jedes $1 \leqslant i \leqslant l$ gilt, dass $Z_{i,r(i)} = 1$ gilt (und nicht nur, dass $Z_{i,r(i)}$ eine Einheit ist). Wir nennen die Spalte von Z an Position $r(i)$, die $i$te *Pivotspalte* von Z.

Um eine Matrix A in strikter Zeilenstufenform in reduzierte Zeilenstufenform zu überführen reichen offenbar genau Zeilenoperationen vom Typ II aus, die bisher noch kaum eine Rolle gespielt hatten. Insbesondere gibt es zu jedem $A \in \mathrm{Mat}(k, n, K)$ wieder eine invertierbare Matrix $B \in \mathrm{Mat}(k, k, K)$, so dass $B \cdot A$ reduzierte Zeilenstufenform hat.

7.9. Korollar *Sind V und W endlichdimensionale Vektorräume über einem (Schief-)Körper K, $\varphi\colon V \to W$ K-linear, so gibt es zu jeder nummierten Basis b von V eine nummerierte Basis b' von W, sodass $\mathrm{M}(\varphi, b, b')$ reduzierte Zeilenstufenform hat.*

Diese Form erklärt das Prozedere wohl am besten: Anstatt in der Standardbasis zu rechnen, lohnt es sich meist zuerst eine Basis zu wählen in der das gegebene Problem (in unserem Fall das lineare Gleichungssystem) möglichst leicht erscheint. Das leistet der Eliminationsalgorithmus genau.

BEWEIS. Wählen wir uns irgendeine Basis $\bar{b}'$ von W, so finden wir wie gerade besprochen eine invertierbare Matrix $B \in \mathrm{Mat}(n,n,K)$, sodass $B \cdot \mathrm{M}(\varphi, b, \bar{b}')$ reduzierte Zeilenstufenform hat, wo $n = \dim_K(W)$. Nun betrachte

$$K^n \xrightarrow{\mathrm{L}(B)^{-1}} K^n \xrightarrow{\mathrm{L}_{\bar{b}'}} W$$

und nehme als b' das Bild der Standardbasis auf der linken Seite. Dann gilt

$$\mathrm{M}(\varphi, b, b') = \mathrm{M}(\mathrm{id}_W, \bar{b}', b') \cdot \mathrm{M}(\varphi, b, \bar{b}')$$

und $\mathrm{M}(\mathrm{id}_W, \bar{b}', b') = B$, da nach Definition

$$\mathrm{M}(\mathrm{id}_W, \bar{b}', b') = \mathrm{M}(K^n \xrightarrow{\mathrm{L}_{\bar{b}'}} W \xrightarrow{\mathrm{L}_{b'}^{-1}} K^n)$$

aber per Konstruktion gilt ja $\mathrm{L}_{b'} = \mathrm{L}_{\bar{b}'} \circ \mathrm{L}(B)^{-1}$, sodass sich dies zu $\mathrm{M}(\mathrm{L}(B)) = B$ vereinfacht. □

Stärker finden wir sogar:

7.10. Theorem (Eindeutigkeit reduzierter Zeilenstufenformen) *Sind V und W endlichdimensionale Moduln über einem Ring K, $\varphi\colon V \to W$ K-linear, b eine nummierte Basis von V und $b', \bar{b}'$ nummerierte Basen von W, so dass $\mathrm{M}(\varphi, b, b')$ und $\mathrm{M}(\varphi, b, \bar{b}')$ reduzierte Zeilenstufenform haben. Dann gilt schon*

$$\mathrm{M}(\varphi, b, b') = \mathrm{M}(\varphi, b, \bar{b}')$$

und $b'_i = \bar{b}'_i$ für alle $1 \leqslant i \leqslant \mathrm{rk}(\varphi)$.

Die übrigen $\dim_K(W) - \mathrm{rk}(\varphi)$ Einträge der Basis b' können aber offenbar beliebig verändert werden, ohne dass sich $\mathrm{M}(\varphi, b, b')$ ändert, sind also keinesfalls eindeutig bestimmt.

BEWEIS. Zunächst wissen wir aus 7.5, dass

$$\mathrm{M}(\varphi, b, \bar{b}') = \mathrm{M}(\mathrm{id}_W, b', \bar{b}') \cdot \mathrm{M}(\varphi, b, \bar{b}').$$

Damit übersetzt sich die Behauptung genau dazu zu zeigen, dass die ersten l Spalten von $\mathrm{M}(\mathrm{id}_W, b', \bar{b}')$ die ersten l Einheitsvektoren sind.

Sei nun allgemein $B \in \mathrm{Mat}(k,k,K)$ invertierbar und $A \in \mathrm{Mat}(k,n,K)$ derart, dass $Z = B \cdot A$ reduzierte Zeilenstufenform hat mit Zeugenfunktion $r\colon \{1,\dots,l\} \to \{1,\dots,n\}$.

Dann hatten wir in 4.5 beobachtet, dass für $A' \in \mathrm{Mat}(n,k',K)$ und für $x \in K^n$ die Gleichung $A' \cdot x = 0$ genau bedeutet, dass $\sum_{i=1}^n A'_i \cdot x_i = 0$ gilt, wo A'_i die $i$te Spalte von A bezeichnet, also $\mathrm{L}(A', 0)$ genau aus den Koffizienten aller Linearkombinationen der Spalten von A' zu 0 besteht. Aber es gilt

$$\{x \in K^k \mid A' \cdot x = 0\} = \{x \in K^k \mid B \cdot A' \cdot x = 0\}.$$

Wenden wir dies auf Matrizen an, die aus A durch Streichen irgendwelcher Spalten entstehen, so sehen wir, dass eine Ansammlung von Spalten von A genau dann linear unabhängig ist, wenn die gleichen Spalten in Z es sind.

Wegen $Z_{r(i)} = e_i$ sind etwa die $Z_{r(1)}, \dots, Z_{r(l)}$ linear unabhängig und demzufolge auch die Spalten $A_{r(1)}, \dots, A_{r(i)}$. Andererseits ist für $p < r(j+1)$ die Spalte Z_p offenbar linear abhängig von den Spalten $Z_{r(1)}, \dots, Z_{r(i)}$, nämlich gilt

$$Z_p = e_1 \cdot Z_{1,p} + \dots + e_i \cdot Z_{i,p} = Z_{r(1)} \cdot Z_{1,p} + \dots + Z_{r(i)} \cdot Z_{i,p}.$$

Demzufolge ist auch die Spalte A_p von den Spalten $A_{r(1)}, \dots, A_{r(i)}$ linear abhängig und es gilt

$$A_p = A_{r(1)} \cdot Z_{1,p} + \dots + A_{r(i)} \cdot Z_{i,p}.$$

Aber dies sagt zunächst, dass die Pivotspalten von $B \cdot A$ sich direkt aus A ablesen lassen: $r(0)$ ist der kleinstmögliche Index einer nicht verschwindenden Spalte von A, und $r(i+1)$ ist der kleinste Index einer Spalte, die von $A_{r(1)}, \dots, A_{r(i)}$ linear unabhängig ist. Und da die Spalten $A_{r(1)}, \dots, A_{r(i)}$ linear unabhängig sind bestimmt die letzte Gleichung die Koeffzienten $Z_{j,p}$ und damit die ganze Spalte Z_p eindeutig.

Insbesondere gibt es nur eine reduzierte Zeilenstufenform, in die sich A durch Multiplikation von links mit einer invertierbaren Matrix überführen lässt.

Ist also A selbst schon in reduzierter Zeilenstufenform (wie in der Situation des Theorems), so folgt $A = Z$. Damit rechnen wir

$$(B \cdot A)_{i,r(j)} = (B \cdot Z)_{i,r(j)} = \sum_{k=1}^{n} B_{i,k} \cdot Z_{k,r(j)} = B_{i,j}$$

und

$$(B \cdot A)_{i,r(j)} = Z_{i,r(j)} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

für $j \leqslant l$, was genau besagt, dass die ersten l Spalten von B die ersten l Einheitsvektoren sind. □

So eine Basis zu finden ist also nicht schwer: Ist etwa $A \in \mathrm{Mat}(k, n, K)$ gegeben, so suchen wir eine nummerierte Basis b' von K^k, derart dass $\mathrm{M}(\mathrm{L}(A), e, b')$ reduzierte Zeilenstufenform hat.

Haben wir eine invertierbare Matrix $B \in \mathrm{Mat}(n, n, K)$ (etwa mittels Eliminationsalgorithmus) gefunden, derart dass $B \cdot A$ reduzierte Zeilenstufenform hat, so folgt aus obigem Beweis, dass die Spalten von B^{-1} gerade eine solche Basis liefern.

7.11. Bemerkung Im Falle, dass $\mathrm{rk}(A) = k$ braucht man B^{-1} auch gar nicht mehr zu invertieren: In diesem Fall ist die $i$te Spalte von B^{-1} einfach durch die $r(i)$te Spalte von A gegeben, wo $r\colon \{1, \ldots, k\} \to \{1, \ldots, n\}$ bezeugt, dass $B \cdot A$ reduzierte Zeilenstufenform hat. Dies sieht man sofort, wenn man beachtet, dass der Eliminationsalgorithmus schematisch die Form

$$\left(\begin{array}{c|c} A & \mathbb{1}_k \end{array}\right) \rightsquigarrow \left(\begin{array}{c|c} B \cdot A & B \end{array}\right)$$

hat: Streicht man alle Spalten auf der linken Seite des Trennungsstrichs, die nicht Pivotspalten von $B \cdot A$ sind, so erhält man aus A eine $k \times k$-Matrix, nennen wir sie A' und aus $B \cdot A$ wird $\mathbb{1}_k$, sodass wirklich $B \cdot A' = \mathbb{1}_k$ wie gewünscht.

Ist insbesondere A invertierbar, so bilden einfach die Spalten von A die gewünschte Basis.

Gilt andererseits $l = \mathrm{rk}(A) < k$, so sind immer noch die ersten l Spalten von der gesuchten Basis als diejenigen Spalten von A bestimmt, die in $B \cdot A$ zu Pivotspalten werden bestimmt und können dann auf beliebige Art zu einer Basis ergänzen (etwa durch Invertieren von B).

7.12. Beispiel Hier ein konkretes Beispiel: Sei

$$A = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 4 & 2 & 0 & 0 \\ 1 & 2 & 1 & 1 \end{pmatrix} \in \mathrm{Mat}(3, 4, \mathbb{Q})$$

Dann wenden wir den Eliminationsalgorithmus an:

$$\left(\begin{array}{cccc|ccc} 2 & 3 & 1 & 1 & 1 & 0 & 0 \\ 4 & 2 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \overset{I \leftrightarrow III}{\rightsquigarrow} \left(\begin{array}{cccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 & 1 \\ 4 & 2 & 0 & 0 & 0 & 1 & 0 \\ 2 & 3 & 1 & 1 & 1 & 0 & 0 \end{array}\right)$$

$$\overset{\substack{II-4I \\ III-2I}}{\rightsquigarrow} \left(\begin{array}{cccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 & 1 \\ 0 & -6 & -4 & -4 & 0 & 1 & -4 \\ 0 & -1 & -1 & -1 & 1 & 0 & 2 \end{array}\right) \overset{II \leftrightarrow III}{\rightsquigarrow} \left(\begin{array}{cccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & -1 & 1 & 0 & 2 \\ 0 & -6 & -4 & -4 & 0 & 1 & -4 \end{array}\right)$$

$$\overset{\substack{-II \\ III+6II}}{\rightsquigarrow} \left(\begin{array}{cccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & -1 & 0 & -2 \\ 0 & 0 & 2 & 2 & -6 & 1 & 8 \end{array}\right) \overset{\substack{1/2III \\ I-2II}}{\rightsquigarrow} \left(\begin{array}{cccc|ccc} 1 & 0 & -1 & -1 & 2 & 0 & 3 \\ 0 & 1 & 1 & 1 & -1 & 0 & -2 \\ 0 & 0 & 1 & 1 & -3 & 1/2 & 4 \end{array}\right)$$

$$\overset{\substack{I+IIII \\ II-III}}{\rightsquigarrow} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & -1 & 1/2 & 1 \\ 0 & 1 & 0 & 0 & 2 & -1/2 & -2 \\ 0 & 0 & 1 & 1 & -3 & 1/2 & 4 \end{array}\right).$$

und können ablesen, dass

$$(2, 4, 1), (3, 2, 2), (1, 0, 1) \in \mathbb{Q}^3$$

in dieser Reihefolge eine nummerierte Basis b' ist für die

$$\mathrm{M}(\mathrm{L}A, e, b') = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

und wir uns das Mitschleifen der rechten Seite hätten sparen können. An der rechten Seite können wir ablesen, dass

$$\mathrm{M}(\mathrm{id}, e, b') = \begin{pmatrix} -1 & 1/2 & 1 \\ 2 & -1/2 & -2 \\ -3 & 1/2 & 4 \end{pmatrix}$$

gilt; und natürlich gilt

$$\mathrm{M}(\mathrm{id}, b', e) = \begin{pmatrix} 2 & 3 & 1 \\ 4 & 2 & 0 \\ 1 & 2 & 1 \end{pmatrix}$$

Wir beenden, das Kapitel mit der Beobachtung, dass man natürlich anstatt in der Quelle eine Basis ebenso im Ziel fixieren kann. Dual zu 7.9 und 7.10 hat man dann:

7.13. Satz *Sind V und W endlichdimensionale Vektorräume über einem (Schief-)Körper K, $\varphi\colon V \to W$ K-linear, so gibt es zu jeder nummierten Basis b' von W eine nummerierte Basis b von V, sodass $\mathrm{M}(\varphi, b, b')$ reduzierte Spaltenstufenform hat, und ist $\bar{b}$ eine zweite nummerierte Basis von V mit dieser Eigenschaft so gilt $\mathrm{M}(\varphi, b, b') = \mathrm{M}(\varphi, \bar{b}, b')$*

Berechnen kann man solche Basen und auch die Spaltenstufenform, durch elementare Spaltenumformung, also Rechtsmultiplikation mit invertierbaren Matrizen, vollständig analog zu unseren Überlegungen.

Zuletzt, kann man noch beide Basen variieren:

7.14. Theorem (Rangsatz) *Sind V und W endlichdimensionale Vektorräume über einem (Schief-)Körper K, $\varphi\colon V \to W$ K-linear, so gibt es nummierte Basen b von V und b' von W, derart, dass*

$$\mathrm{M}(\varphi, b, b') = \begin{pmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} \in \mathrm{Mat}(\dim_K(W), \dim_K(V), K)$$

eine Diagonalmatrix ist, wobei die Anzahl Einsen genau der Rang von φ ist.

Mit anderen Worten, die einzige unter Basiswechsel invariante Eigenschaft einer linearen Abbildung ist ihr Rang. Anders gesagt: Für je zwei Matrizen $A, A' \in \mathrm{Mat}(k, n, K)$ mit gleichem Rang gibt es invertierbare Matrizen $B \in \mathrm{Mat}(k, k, K)$ und $C \in \mathrm{Mat}(n, n, K)$ mit $A = B \cdot A' \cdot C$.

Beweis. Nach 7.9 gibt es Basen $\bar{b}$ und b', derart dass $\mathrm{M}(\varphi, \bar{b}, b')$ reduzierte Zeilenstufenform hat. Aber offenbar kann eine solche Matrix durch elementare Spaltenoperationen in die Gestalt des Rangssatzes überführt werden. Mit anderen Worten, es existiert eine invertierbare Matrix $C \in \mathrm{Mat}(\dim_K(V), \dim_K(V), K)$ derart, dass $\mathrm{M}(\varphi, b, \bar{b}') \cdot C$ die gewünschte Form hat.

Aber dann können wir C wie in 7.9 benutzen um die Basis $\bar{b}$ derart zu einer Basis b zu verändern, dass

$$\mathrm{M}(\varphi, \bar{b}, b') \cdot C = \mathrm{M}(\varphi, b, b'),$$

nämlich sei b das Bild der Einheitsbasis unter

$$K^{\dim_K(W)} \xrightarrow{\mathrm{L}(C)} K^{\dim_K(W)} \xrightarrow{\mathrm{L}_{\bar{b}}} W.$$

□

Es gibt hiernach noch einen letzten Fall: Ist $\varphi\colon V \to V$ K-linear, so kann man sich fragen, was die einfachste Form einer Dartstellungsmatrix für φ, wobei wir in Ziel und Quelle die *gleiche* Basis verwenden. Das ist natürlich von enormen Interesse, wenn φ etwa eine Iteration eines Prozesses beschreibt, etwa falls $V = \mathbb{Q}^n$, die Populationen von n Proben modelliert, und $\varphi(v)$, die zu erwartenden Populationen nach einem gewissen Zeitraum bei Startpopulation v kodiert. Dann interessiert man sich etwa für $\varphi^{\circ n}(v)$, die zu erwartenden Populationen nach n Zeitschritten. Verwendet man in V zweimal die gleiche nummerierte Basis b, so gilt

$$\mathrm{M}(\varphi^{\circ n}, b, b) = \mathrm{M}(\varphi, b, b)^{\cdot n},$$

aber ähnliches gilt nicht, für zwei verschiedene Basen.

Das Ergebnis in diesem Fall ist allerdings um einiges komplizierter und involviert insbesondere Eigenschaften des Grundkörpers K; es ist wohl etwas überraschend, dass der Rangsatz so uniform für jeden Körper K gilt. Jedenfalls, wird diese Problemstellung uns im zweiten Semester intensiv beschäftigen.

Und nochmal zwei*

Erstes Ziel dieses Kapitels ist es zunächst folgenden Satz zu beweisen:

7.15. Theorem *Ist R ein Ring, M ein R-Modul und $B \subseteq M$ eine unendliche Basis. Dann gibt es zu jeder weiteren Basis B' von M eine Bijektion $B \to B'$.*

Mit anderen Worten: Die Mächtigkeit einer unendlichen Basis ist wohlbestimmt. Für R ein Schiefkörper haben wir das Analog für endliche Basen in 4.11 oben bewiesen, und für R kommutativ werden wir es weiter unten in 3.6 beweisen. Für beliebige Ringe ist die Aussage, dass je zwei endliche Basen gleich viele Elemente besitzen allerdings überraschenderweise falsch, wie wir in den Übungen sehen werden. Die Situation für unendliche Basen ist also in gewisser Hinsicht leichter als im Falle endlicher Basen.

Beweis. Seien B und B' zunächst eine beliebige (möglicherweise endliche) Basen von M. Betrachte, dann die Abbildung

$$g\colon B \longrightarrow \mathcal{P}(B'), \quad b \longmapsto \{b* \in B' \mid f_b(b') \neq 0\}$$

wo $f_m\colon B' \to R$ für ein $m \in M$ die eindeutige Funktion mit $f(b') = 0$ für fast alle $b' \in B'$ bezeichnet mit

$$m = \sum_{b' \in B'} b' \cdot f_m(b').$$

Per Definition ist dann $g(b)$ für jedes $b \in B$ endlich. Wir behaupten nun, dass $\cup\mathrm{Im}(g) = B'$ gilt. Dafür beobachten wir, dass für jedes $b \in B$

$$b \in \langle g(b)\rangle_M \subseteq \langle \bigcup \mathrm{Im}(g)\rangle_M.$$

Damit enthält $\langle \bigcup \mathrm{Im}(g)\rangle_M$ ein Erzeugendensystem von M also muss $\langle \bigcup \mathrm{Im}(g)\rangle_M = M$ gelten, und $\bigcup \mathrm{Im}(g)$ ist ein Erzeugendensystem, aber als Teilmenge von B' auch linear unabhängig, also eine Basis. Aber nach 4.7 sind Basen maximal linear unabhängig, also kann nicht $\bigcup \mathrm{Im}(g) \subsetneq B'$ gelten.

Aus $\cup\mathrm{Im}(g) = B'$ leiten wir nun den Satz ab:

Ist B endlich, so haben wir B' also als endliche Vereinigung endlicher Mengen geschrieben, und damit ist auch B' endlich. Dies zeigt, dass jede Basis eines Moduls M endlich ist, falls auch nur eine dies ist. Und im Umkehrschluss, dass jede Basis unendlich ist, falls auch nur eine es ist.

Ist nun B unendlich, wie im Theorem angenommen. Dann schließen wir aus 5.8, dass $B' \preccurlyeq B$ und aus der vorigen Überlegung, dass B' unendlich ist. Aber dann können wir in obigem Argument die Rollen von B und B' vertauschen und erhalten auch $B \preccurlyeq B$, und damit nach dem Satz von Schröder und Bernstein die Behauptung. □

Als eine zweite Anwendung der Technologie unendlicher Basen zeigen wir folgende, hoffentlich extrem überraschende Aussage, für die wir die Grundeigenschaften der reellen Zahlen aus der Analysis einmal benutzen wollen:

7.16. Satz *Als $\mathbb{Q}$-Vektorräume, und insbesondere als abelsche Gruppen gilt*

$$\mathbb{R}^n \cong \mathbb{R}$$

für alle $n \geqslant 1$.

Sicherlich ist dies nicht als $\mathbb{R}$-Vektorraum: Wir haben schließlich $\dim_{\mathbb{R}}(\mathbb{R}^n) = n$. Aber da $\mathbb{R}$ überabzählbar ist, muss $\dim_{\mathbb{Q}}(\mathbb{R}^n) = \infty$ für jedes $n \geqslant 1$ gelten, sodass die rationale Dimension kein Hindernis ist.

Proof. Offenbar reicht es $\mathbb{R}^2 \cong \mathbb{R}$ zu beweisen, für höheren n folgt die Behauptung dann per Induktion. Nach 5.11 gibt es eine Basis I von $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum, und wie in der Vorbemerkung etabliert muss I unendlich sein. Aber es ist $J = I \times \{0\} \cup \{0\} \times I$ eine Basis von $\mathbb{R}^2$, wie man leicht prüft und 5.7 liefert dann unmittelbar eine Bijektion $g\colon J \to I$. Aber dann haben wir

$$\mathbb{R} \xrightarrow{\mathrm{L}_I^{-1}} \mathrm{F}^{\mathrm{fs}}(I, \mathbb{Q}) \xrightarrow{-\circ g} \mathrm{F}^{\mathrm{fs}}(J, \mathbb{Q})\mathrm{L}_{\mathrm{J}}\mathbb{R}^2,$$

bestehend aus drei Isomorphismen gemäß 4.10. □

Eine $\mathbb{Q}$-Basis von $\mathbb{R}$ bezeichnet man auch als eine *Hamelbasis* nach dem deutschen Mathematiker Georg Hamel (1877 - 1954), der ihre Existenz 1905 bewies. Ihre Existenz stützt sich hochgradig auf das extrem inexplizite Zorn'sche Lemma, das wir in 5.11 entscheidend verwendet haben. Mit anderen Worten: Obwohl wir ihre Existenz nachweisen können, hat noc nie hat jemand eine Hamelbasis, oder einen Isomorphismus wie in obigem Satz wirklich gesehen.

KAPITEL 4

Determinanten

1. Alternierende Multilinearformen

Ziel dieses Kapitels ist es invertierbare Matrizen besser zu verstehen. Insbesondere würden wir gerne eine Methode besitzen um zu entscheiden, ob eine gegebene Matrix $A \in \mathrm{Mat}(n,n,R)$ invertierbar ist, ohne ihr Inverses wirklich ausrechnen zu müssen. In diesem Falle wissen wir ja etwa, dass es für jede $b \in R^n$ genau ein $x \in R^n$ gibt mit $A \cdot x = b$, also alle zu A gehörigen linearen Gleichungssysteme eindeutig lösbar sind.

Hierfür gibt es im Falle $K = \mathbb{Q}$ oder $K = \mathbb{R}$ eine einfache Methode in kleinen Dimensionen: Ist

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2,2,\mathbb{Q})$$

so wissen wir aus 5.6, dass A invertierbar ist genau dann, wenn die Spalten (a,c) und (b,d) von A linear unabhängig sind, also nicht in einem 1-dimensionalen Unterraum von $\mathbb{Q}^2$ enthalten sind. Die Idee ist nun, dass sich dies überprüfen lässt, indem man den Flächeninhalt des Parallelogramms mit Ecken $(0,0),(a,c),(b,d),(a+b,c+d)$ berechnet: Dieser ist 0 nur dann, wenn das Parallelogramm zu einer Linie degeneriert. Setzen wir einmal voraus, dass $a,b,c,d \geqslant 0$ gilt und $c/a \geqslant b/d$ gilt, sodass die Linie von $(0,0)$ zu (a,c) oberhalb der von $(0,0)$ zu (b,d) verläuft. Um den Flächeninhalt des Parallelogramms zu berechnen, betrachten wir nun das Rechteck mit Ecken $(0,0),(a+b,0),(0,c+d),(a+b,c+d)$, dessen Flächeninhalt natürlich $(a+b)\cdot(c+d)$ ist. Wir unterteilen es nun in das gesuchte Parallelogramm, die beiden Rechtecke mit Ecken $(0,c),(a,c),(0,c+d),(a,c+d)$ und $(b,0),(a+b,0),(b,d),(a+b,d)$ und die vier rechtwinkligen Dreiecke mit Ecken

$$(0,0),(0,c),(a,c) \quad (a,c),(a,c+d),(a+b,c+d) \quad (0,0),(b,0),(b,d) \quad (b,d),(a+b,d),(a+b,c+d)$$

und erhalten

$$(a+b)\cdot(c+d) = p + a\cdot d + a\cdot d + \frac{a\cdot c}{2} + \frac{b\cdot d}{2} + \frac{b\cdot d}{2} + \frac{a\cdot c}{2}$$

wo p der gesuchte Flächeninhalt ist (ein Bild hilft ungemein bei der Visualisierung). Umstellen liefert

$$p = a\cdot d - b\cdot c$$

und geht man durch die anderen möglichen Fälle, so erhält man insgesamt, dass der Flächeninhalt des aufgespannten Parallelogramms immer $|a\cdot d - b\cdot c|$ ist. Wir können also hoffen, dass die Zahl $a\cdot d - b\cdot c$ etwas über die Invertierbarkeit von A weiß. Und tatsächlich haben wir:

1.1. Beobachtung Ist R ein kommutativer Ring, so ist

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2,2,R)$$

genau dann invertierbar, wenn $a\cdot d - b\cdot c$ eine Einheit in R ist.

Der Beweis ist eine Übungsaufgabe. Für

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & i & h \end{pmatrix} \in \mathrm{Mat}(3,3,\mathbb{Q})$$

kann man sich mit mehr Aufwand überlegen, dass das Volumen des Parallelepipeden mit Ecken

$$(0,0,0),(a,d,g),(b,e,i),(c,f,h),(a+b,d+e,g+i),$$

$$(a+c, d+f, g+h), (b+c, e+f, i+h), (a+b+c, d+e+f, g+i+h)$$

durch

$$|a \cdot e \cdot h + b \cdot f \cdot g + c \cdot d \cdot i - c \cdot e \cdot g - b \cdot d \cdot h - a \cdot f \cdot i|$$

gegeben ist, und sich fragen, ob die Formel in den Betragstrichen ähnliches liefert. Wir werden dies, als Teil der allgemeinen Theorie beweisen. Die Suche nach analogen Formeln für höhere Dimensionen ist natürlich etwas komplizierter. Erstmal formalisieren wir unserern Wunsch:

1.2. Definition Sei R ein kommutativer Ring und M und N R-Moduln. Dann heißt eine Abbildung $d\colon M^k \to N$ eine *k-fach multilineare Abbildung*, falls für sie für jedes $(m_1, \ldots, m_k) \in M^k$ und $1 \leqslant i \leqslant k$ die Abbildung

$$M \longrightarrow N, \quad m \longmapsto d(m_1, \ldots, m_{i-1}, m, m_{i+1}, \ldots, m_k)$$

R-linear ist, also

(1) für alle $\lambda \in R$ und $(m_1, \ldots, m_k) \in M^k$ gilt

$$d(m_1, \ldots, m_{i-1}, m_i \cdot \lambda, m_{i+1}, \ldots, m_k) = d(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_k) \cdot \lambda,$$

und

(2) für alle $(m_1, \ldots, m_k) \in M^k$ und $m_i' \in M$ haben wir

$$d(m_1, \ldots, m_{i-1}, m_i + m_i', m_{i+1}, \ldots, m_k)$$
$$= d(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_k) + d(m_1, \ldots, m_{i-1}, m_i', m_{i+1}, \ldots, m_k).$$

Eine solche Abbildung heißt *alternierend*, falls

$$d(m_1, \ldots, m_k) = 0$$

sobald $m_i = m_j$ für $i \neq j$.

Wir bezeichnen

$$\mathrm{Mult}_R^k(M, N) := \{d\colon M^k \to N \mid d \text{ ist } k\text{-fach multilinear}\}$$

und

$$\mathrm{Alt}_R^k(M, N) := \{d \in \mathrm{Mult}_R^k(M, N) \mid d \text{ ist alternierend}\}$$

Natürlich ist sind Summe zweier (alternierender) mulitlinearer Abbildungen wieder (alternierend) multilinear und gleiches gilt für Vielfache, sodass

$$\mathrm{Alt}_R^k(M, N) \subseteq \mathrm{Mult}_R^K(M, N) \subseteq \mathrm{F}(M^k, N)$$

R-Untermoduln sind. Im Fall $k = 1$ gilt natürlich

$$\mathrm{Alt}_R^k(M, N) = \mathrm{Mult}_R^k(M, N) = \mathrm{Lin}_R(M, N).$$

Erstes Ziel dieses Kapitels ist es folgendes Theorem zu beweisen:

1.3. Theorem *Ist R ein kommutativer Ring, M und N R-Moduln, und $b\colon \{1, \ldots, k\} \to M$ eine nummerierte Basis von M. Dann gibt es zu jedem $n \in N$ genau eine k-fach multilineare alternierende Abbildung $d \in \mathrm{Alt}_R^k(M, N)$ mit $d(b_1, \ldots, b_k) = n$, mit anderen Worten, die Abbildung*

$$\mathrm{Alt}_R^k(M, N) \longrightarrow N, \quad d \longmapsto d(b_1, \ldots, b_k)$$

ist bijektiv.

Dies erlaubt uns:

1.4. Definition Ist dann $d \in \mathrm{Alt}^k(R^k, R)$ die eindeutig bestimmte Abbildung mit $d(e_1, \ldots, e_k) = 1$, so setzen wir für eine Matrix $A \in \mathrm{Mat}(k, k, R)$ mit Spalten A_i

$$\det(A) := d(A_1, \ldots, A_k),$$

die *Determinante (determinant)* von A.

1.5. Beispiel (1) Für $k = 1$, ist die Abbildung $\mathrm{id}\colon R \to R$ das gesuchte d und folglich gilt für $\begin{pmatrix} a \end{pmatrix} \in \mathrm{Mat}(1, 1, R)$ einfach $\det \begin{pmatrix} a \end{pmatrix} = a$.

(2) Für $k = 2$, erfüllt die Abbildung

$$R^2 \times R^2 \longrightarrow R, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto a \cdot d - b \cdot c$$

genau die defininierenden Eigenschaften vom benötigten d, sodass

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$$

wie gewünscht gilt.

(3) Für $k = 3$, erfüllt die Abbildung

$$R^3 \times R^3 \times R^3 \to R,$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \longmapsto a \cdot e \cdot i + b \cdot f \cdot g + c \cdot d \cdot h - c \cdot e \cdot g - b \cdot d \cdot i - a \cdot f \cdot h$$

die definierenden Eigenschaften von d, wie man leicht nachprüft, sodass in der Tat

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = a \cdot e \cdot i + b \cdot f \cdot g + c \cdot d \cdot h - c \cdot e \cdot g - b \cdot d \cdot i - a \cdot f \cdot h$$

In diesen Beispielen besteht det immer aus eine Summe über alle Arten aus einer $k \times k$-Matrix genau k viele Element zu entnehmen, derart dass in jeder Spalte und Zeile ein solches Element ist, und sie dann nach Einfügen eines Vorzeichens zusammen zu multiplizieren, also etwa

$$\det(A) = \sum_{\sigma} (-1)^{?} A_{1,\sigma(1)} \cdot \dots \cdot A_{k,\sigma(k)},$$

wo die Summe alle bijektiven Abbildungen $\sigma \colon \{1, \dots, k\} \to \{1, \dots, k\}$ durchläuft. Für den Beweis von **??** müssen wir also noch die Vorzeichen verstehen. Das ist der Inhalt der nächsten Sektion.

2. Permutationen

2.1. Definition Eine *Permutation (permutation)* auf einer Menge M ist einfach eine bijektive Abbildung $M \to M$. Wir bezeichnen die Menge aller solcher mit Σ_M und kürzen $\Sigma_{\{1,\dots,n\}}$ zu Σ_n, der *Permutationsgruppe (symmetric group)* von n Elementen, ab.

In der Tat bildet Σ_M für jede M unter Komposition eine Gruppe mit neutralem Element id_M.

2.2. Beispiel (1) Ist $a \colon \{1, \dots, k\} \to \{1, \dots, n\}$ injektiv, so ist

$$\{1, \dots, n\} \longrightarrow \{1, \dots, n\}, \quad i \longmapsto \begin{cases} i & i \notin \mathrm{Im}(a) \\ a_{l+1} & i = a(l), l < k \\ a_1 & i = a_k \end{cases}$$

eine sogenannte *zyklische Permutation (cyclic permutation)* der Länge k. Man notiert sie oft als $(a_1, \dots, a_k)$, obwohl das natürlich auch das Element $a \in \{1, \dots, n\}^k$ bezeichnen könnte und es der Notation nach nicht klar ist, in genau welcher Σ_n wir den Zykel auffassen wollen. Beobachte auch noch, dass

$$(a_1, \dots, a_k) = (a_k, a_1, \dots, a_{k-1})$$

gilt. Man fixiert, deshalb oft noch, dass a_1 das kleinste der Elemente a_i sein solle, aber das sollte man nicht zu ernsthaft durchzuhalten versuchen. Ein konkretes Beispiel ist dann also $(1, 4, 3, 12) = (12, 1, 4, 3) = (3, 12, 1, 4) = (4, 3, 12, 1) \in \Sigma_{14}$, welches die Elemente $2, 5, 6, 7, 8, 9, 10, 11, 13, 14$ fixiert.

(2) Es gilt immer $(a_1, \dots, a_k)^{-1} = (a_k, \dots, a_1)$.

(3) Eine zyklische Permutation der Länge 2 heißt eine *Transposition (transposition)*. Sie vertauscht einfach nur zwei Elemente. Insbesondere ist $\tau^{\circ 2} = \mathrm{id}$ für jede Transposition τ.

(4) Es gelten
$$\Sigma_1 = \{\mathrm{id}\}$$
$$\Sigma_2 = \{\mathrm{id}, (1,2)\}$$
$$\Sigma_3 = \{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$$
und Σ_4 enthält mit $(1,2)\circ(3,4)$ eine erste Permutation die nicht zyklisch ist.

(5) Das Produkt $(1,3)\circ(3,4,5)\circ(4,5) \in \Sigma_5$ ist durch
$$1 \mapsto 1 \mapsto 1 \mapsto 3$$
$$2 \mapsto 2 \mapsto 2 \mapsto 2$$
$$3 \mapsto 3 \mapsto 4 \mapsto 4$$
$$4 \mapsto 5 \mapsto 3 \mapsto 1$$
$$5 \mapsto 4 \mapsto 5 \mapsto 5$$
gegeben, und stimmt daher mit $(1,3,4)$ überein.

2.3. Satz *Für $n \geqslant 1$ ist jede Permutation in Σ_n ein Produkt von höchstens $n-1$ Transpositionen.*

Beweis. Wir beweisen das per Induktion. Für $n = 1$ ist die Aussage trivial. Stimmt die Aussagen für n, und wir geben uns $\sigma \in \Sigma_{n+1}$ vor, so sei $\tau = (n+1, \sigma(n+1))$, eine Transposition. Es gilt dann $(\tau\circ\sigma)(n+1) = n+1$, sodass sich $\tau\circ\sigma$ zu einer sicherlich immer noch injektiven, also bijektiven, Abbildung $\{1,\dots,n\} \to \{1,\dots,n\}$ ein. Es gilt also $\tau\circ\sigma = \tau_1 \cdot \dots \cdot \tau_k$ für irgendwelche Transpositionen $\tau_1,\dots,\tau_k$ mit $k \leqslant n-1$. Aber dann gilt
$$\sigma = \tau\circ\tau\circ\sigma = \tau\circ\tau_1\circ\dots\circ\tau_k,$$
ein Produkt von $k+1 \leqslant n-1+1 = n$ Permutationen wie gewünscht. □

Nun ist so eine Darstellung als Produkt von Transpositionen keineswegs eindeutig, etwa gilt
$$(a_1,a_2)\circ(a_2,a_3)\circ\dots\circ(a_{k-1},a_k) = (a_1,\dots,a_k) = (a_k,a_1,\dots,a_{k-1}) = (a_k,a_1)\circ(a_1,a_2)\circ\dots\circ(a_{k-2},a_{k-1})$$
oder auch konkreter
$$(1,3)\circ(4,7)\circ(3,5)\circ(1,5)\circ(4,6)\circ(3,5) = (4,6,7) = (4,6)\circ(6,7).$$
Aber es gilt:

2.4. Theorem *Sind $\tau_1,\dots,\tau_k \in \Sigma_n$ und $\sigma_1,\dots,\sigma_l \in \Sigma_n$ Transpositionen mit*
$$\tau_1\circ\dots\circ\tau_k = \sigma_1\circ\dots\circ\sigma_l$$
so folgt $k \equiv_2 l$, mit anderen Worten, entweder sind k und l beide gerade oder beide ungerade.

Zusammen mit 2.3 erlaubt uns das zu setzen:

2.5. Definition Ist $\sigma \in \Sigma_n$ ein Produkt von k Transpositionen so definieren wir das *Vorzeichen* oder *Signum (sign)* als
$$\mathrm{sgn}(\sigma) = (-1)^k \in \{\pm 1\} \subseteq \mathbb{Z}.$$
Man sagt eine Permutation ist *gerade* oder *ungerade (even/odd)*, falls k gerade oder ungerade ist.

2.6. Korollar *Die Abbildung* $\mathrm{sgn}\colon \Sigma_n \to \{\pm 1\}$ *ist ein Gruppenhomomorphismus.*

Für den Beweis von 2.4 führen wir eine a priori wohlbestimmt Zahl $F(\eta)$ für jede Permutation $\eta \in \Sigma_n$ ein, und zeigen, dass für $\eta = \tau_1\circ\dots\tau_k$ folgt, dass $k \equiv_2 F(\eta)$ gilt; das reicht sicherlich um das Theorem zu beweisen.

Die Zahl $F(\eta)$ ist die Anzahl der *Fehlstände (inversions)* der Permutation η, wo ein Fehlstand von σ ein Paar (i,j) mit $1 \leqslant i < j \leqslant n$ ist mit $\eta(j) < \eta(i)$, mit anderen Worten
$$F(\eta) = |\{(i,j) \in \{1,\dots,n\}^2 \mid i < j \wedge \eta(j) < \eta(i)\}|.$$
Wir zeigen nun folgendes Lemma, welches insbesondere 2.4 beweist.

2.7. Lemma *Für eine Permutation $\sigma = \tau_k\circ\dots\circ\tau_1$ mit Transpositionen $\tau_i \in \Sigma_n$ gilt $F(\sigma) \equiv_2 k$.*

PROOF. Wir zeigen das per Induktion über k. Wegen $F(\mathrm{id}) = 0$ stimmt das sicherlich für $k = 0$. Wir zeigen nun

$$F((a,b)\circ\eta) \equiv_2 F((a,b)\circ\eta) + 1$$

für $1 \leqslant a < b \leqslant n$, was den Induktionsschritt impliziert. Dafür prüfen wir, ob (i,j) mit $i < j$ ein Fehlstand von $(a,b)\circ\eta$ ist, mit einer Fallunterscheidung (mit disjunkten Fällen):

(1) Ist $\{\eta(i),\eta(j)\} \cap \{a,b\} = \varnothing$ so gilt $((a,b)\circ\eta)(i) = \eta(i)$ und $((a,b)\circ\eta)(j) = \eta(j)$, sodass (i,j) ein Fehlstand von $(a,b)\circ\eta$ ist genau dann, wenn (i,j) ein Fehlstand von η ist.
(2) Ist $\eta(i) < a$ und $\eta(j) = a,b$, so ist (i,j) weder Fehlstand von $(a,b)\circ\eta$ noch η.
(3) Ist $\eta(i) = a$, $\eta(j) < a$, dann gilt $((a,b)\circ\eta)(i) = b$ und $((a,b)\circ\eta)(j) = \eta(j)$, so ist (i,j) ein Fehlstand sowohl von $(a,b)\circ\eta$ als auch η.
(4) Ist $\eta(i) = a$, $a < \eta(j) \leqslant b$, so ist (i,j) ist ein Fehlstand von $(a,b)\circ\eta$, obwohl es keiner von η ist.
(5) Ist $\eta(i) = a$, $b < \eta(j)$, so ist (i,j) weder ein Fehlstand von $(a,b)\circ\eta$ noch von η.
(6) Ist $a < \eta(i) < b$, $\eta(j) = a$, so ist (i,j) kein Fehlstand von $(a,b)\circ\eta$ aber einer von η.
(7) Ist $a < \eta(i) < b$, $\eta(j) = b$, so ist (i,j) Fehlstand von $(a,b)\circ\eta$ aber keiner von η.
(8) Ist $\eta(i) = b$, $\eta(j) < a$, so gilt $((a,b)\circ\eta)(i) = a$ und (i,j) ein Fehlstand von sowohl $(a,b)\circ\eta$ und η.
(9) Ist $\eta(i) = b$, $a \leqslant \eta(j) < b$, so ist (i,j) kein Fehlstand von $(a,b)\circ\eta$ aber einer von η.
(10) Ist $\eta(i) = b$, $b < \eta(j)$, so ist (i,j) Fehlstand weder von $(a,b)\circ\eta$ noch η.
(11) Ist $b < \eta(i)$, $\eta(j) = a,b$ so ist (i,j) Fehlstand von sowohl $(a,b)\circ\eta$ als auch η.

Es tut sich also nur in den Fällen (4),(6),(7), und (9) etwas. Nennen wir die Anzahlen der Paare (i,j) in diesen Fällen der Reihenfolge nach $x,y,w,z \in \mathbb{N}$ so gilt also

$$F((a,b)\circ\eta) = F(\eta) + x - y + w - z \equiv_2 F(\eta) + x + y + w + z$$

Wir behaupten nun, dass $x + y + w + z = 2(b-a) - 1$ gilt, was dann in der Tat zu

$$F((a,b)\circ\eta) \equiv_2 F(\eta) + 2(b-a) - 1 \equiv_2 F(\eta) + 1$$

führt. Dazu beobachten wir, dass

$$x = |\{a < x \leqslant b \mid \eta^{-1}(a) < \eta^{-1}(x)\}|, \quad y = |\{a < x < b \mid \eta^{-1}(x) < \eta^{-1}(a)\}|$$

$$w = |\{a < x < b \mid \eta^{-1}(x) < \eta^{-1}(b)\}|, \quad \text{und} \quad z = |\{a \leqslant x < b \mid \eta^{-1}(b) < \eta^{-1}(x)\}|$$

und dass die auftauchenden Mengen disjunkt sind. Falls nun $\eta^{-1}(a) < \eta^{-1}(b)$, so gelten

$$\{a < x \leqslant b \mid \eta^{-1}(a) < \eta^{-1}(x)\} \cup \{a < x < b \mid \eta^{-1}(x) < \eta^{-1}(a)\} = \{a+1,\dots,b\}$$

$$\{a < x < b \mid \eta^{-1}(x) < \eta^{-1}(b)\} \cup \{a \leqslant x < b \mid \eta^{-1}(b) < \eta^{-1}(x)\} = \{a+1,\dots,b-1\}$$

und falls $\eta^{-1}(b) < \eta^{-1}(a)$ gilt

$$\{a < x \leqslant b \mid \eta^{-1}(a) < \eta^{-1}(x)\} \cup \{a < x < b \mid \eta^{-1}(x) < \eta^{-1}(a)\} = \{a+1,\dots,b-1\}$$

$$\{a < x < b \mid \eta^{-1}(x) < \eta^{-1}(b)\} \cup \{a \leqslant x < b \mid \eta^{-1}(b) < \eta^{-1}(x)\} = \{a,\dots,b-1\}$$

In jedem Falle hat eine der beiden Vereinigungen $b-a$ und die andere $b-a-1$ Elemente, insgeamt $2(b-a)-1$, wie behauptet. □

2.8. Bemerkung Die Anzahl der Fehlstände einer Permutation definiert eine Funktion $F\colon \Sigma_n \to \mathbb{Z}$, aber diese ist nicht besonders wohlverhalten, insbesondere ist sie *kein* Gruppenhomomorphismus.

3. Die Leibniz'sche Formel

Wir wenden uns nun langsam dem Beweis von 1.3 zu. Nach unseren Vorüberlegungen ist der Existenzteil nun einfach: Wir definieren zunächst die *Leibniz'sche Form* durch

$$\det_n\colon R^n \times \cdots \times R^n \longrightarrow R, \quad (x_1,\dots,x_n) \longmapsto \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}.$$

Benannt ist sie nach dem deutschen Mathematiker Gottfried Wilhelm Leibniz (1646 - 1716), der zusammen mit dem Briten Isaac Newton (1643 - 1727) als Begründer der modernen Analysis gilt.

3.1. Satz *Für jeden kommutativen Ring R gilt* $\det_n \in \mathrm{Alt}^n_R(R^n, R)$ *und* $\det_n(e_1, \ldots, e_n) = 1$.

Insbesondere setzen wir für eine Matrix $A \in \mathrm{Mat}(n, n, R)$ also

$$\det(A) = \sum_{\sigma \in \Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} A_{\sigma(i),i}.$$

Beweis. Die Multilinearität ist einfach, da für jedes $\sigma \in \Sigma_n$ die Abbildung

$$R^n \times \cdots \times R^n \longrightarrow R, \quad (x_1, \ldots, x_n) \longmapsto \prod_{i=1}^{n} x_{\sigma(i),i}$$

offenbar multilinear ist (hier benutzen wir die Kommutativität von R!) und damit auch negative hiervon und Summen. Aber natürlich ist keine einzelne dieser Abbildungen alternierend. Gilt aber $x_k = x_l$, so können wir auftrennen:

$$\sum_{\sigma \in \Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i} = \sum_{\sigma \text{ gerade}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i} + \sum_{\sigma \text{ ungerade}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}$$

aber für jede ungerade Permutation σ gilt $(k, l) \circ \tau$ für genau eine gerade Permutation (nämlich $\tau = (k, l) \circ \sigma$), sodass wir dies umschreiben können zu

$$\begin{aligned} &= \sum_{\sigma \text{ gerade}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i} + \sum_{\sigma \text{ gerade}} \mathrm{sgn}((k, l) \circ \sigma) \prod_{i=1}^{n} x_{((k,l)\circ\sigma)(i),i} \\ &= \sum_{\sigma \text{ gerade}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i} - \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{((k,l)\circ\sigma)(i),i} \end{aligned}$$

aber per Annahme gilt $x_{((k,l)\circ\sigma)(i)} = x_{\sigma(i)}$, sodass sich hier alle Summanden wegheben

.

Bleibt noch die letzte Behauptung. Hierfür beobachten wir, dass $e_{\sigma(i),i} = 0$ falls nicht $\sigma(i) = i$, und demzufolge $\prod_{i=1}^{n} x_{\sigma(i),i} = 0$ außer für $\sigma = \mathrm{id}$. Es bleibt also in $\det(e_1, \ldots, e_n)$ nur ein Summand übrig, nämlich

$$\sum_{\sigma \in \Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} e_{\sigma(i),i} = \prod_{i=1}^{n} e_{i,i} = 1.$$

□

3.2. Beispiel (1) Evaluieren wir die Formel einmal im Fall

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & i & h \end{pmatrix} \in \mathrm{Mat}(3, 3, R).$$

Nach 2.2 gilt

$$\Sigma_3 = \{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}.$$

Summieren wir in dieser Reihenfolge erhalten wir

$$a \cdot e \cdot h - d \cdot b \cdot h - g \cdot e \cdot c - a \cdot i \cdot f + d \cdot i \cdot c + g \cdot b \cdot f$$

was mit der Formal aus dem ersten Abschnitt übereinstimmt. Diese Formel wird häufig als die *Regel von Sarrus* (nach dem Franzosen Pierre Sarrus (1798 - 1861), obwohl sie keineswegs auf ihn zurückgeht; Leibniz war etwa schon 1716 gestorben) bezeichnet.

(2) Ist $A \in \mathrm{Mat}(n, n, R)$ eine obere Dreiecksmatrix, so gilt $\det(A) = A_{1,1} \cdot \cdots \cdot A_{n,n}$: Per Annahme gilt $A_{i,j} = 0$ für $i > j$, sodass $\prod_{i=1}^{n} A_{\sigma(i),i}$ nur dann nicht verschwindet, wenn $\sigma(i) \leqslant i$ für alle $1 \leqslant i \leqslant n$, was bedeutet dass $\sigma = \mathrm{id}$ gilt. Es gibt also in der Leibniz'schen Formel nur einen nicht verschwindenden Summanden, den für $\sigma = \mathrm{id}$ und der ist $A_{1,1} \cdot \cdots \cdot A_{n,n}$ wie gewünscht.

Um auch die Eindeutigkeit der Determinante herzuleiten, beobachten wir einige allgemeine Eigenschaften für alternierende Multilinearformen:

3.3. Satz *Ist R ein kommutativer Ring, $d \in \mathrm{Alt}^k_R(M,N)$ und $\sigma \in \Sigma_k$, so gilt*

(1) $d(m_1,\dots,m_{j-1},m_j+m_i\cdot\lambda,m_{j+1},\dots,m_k) = d(m_1,\dots,m_k)$
(2) $d(m_{\sigma(1)},\dots,m_{\sigma(k)}) = d(m_1,\dots,m_k)\cdot\mathrm{sgn}(\sigma)$

für alle $m \in M^k$ und $\lambda \in R$.

3.4. Bemerkung Die zweite Eigenschaft ist der Grund für den Namen von alternierenden Formen: Vertauscht man zwei Argumente alterniert das Vorzeichen. Multilinearformen mit dieser Eigenschaft nennt man allgemein *schiefsymmetrisch (skew symmetric)*. Falls $2 \in R$ eine Einheit ist, stimmen die beiden Konzepte überein, aber im allgemeinen gibt es schiefsymmetrische Formen die nicht alternierend sind. Etwa sind bei $2 = 0$ in R, etwa $R = \mathbb{F}_2$, schiefsymmetrische Formen das gleiche wie *symmetrische (symmetric)* Formen, also solche die sich nicht verändern, wenn man die Argumente vertauscht. Etwa ist

$$R \times R \longrightarrow R, \quad (x,y) \longmapsto x\cdot y$$

für jeden kommutativen Ring eine symmetrische Bilinearform, und für $R = \mathbb{F}_2$ ist sie schiefsymmetrisch, aber nicht alternierend.

Proof. Für die erste Gleichung beobachten wir einfach und das im rechten Term zwei Einträge übereinstimmen, er also verschwindet. Die zweite Gleichung zeigen wir per Induktion über die Anzahl der Transposition, die man braucht um σ zu zerlegen: Für $\sigma = (i,j)$ haben wir

$$\begin{aligned}
0 &= d(m_1,\dots,m_{i-1},m_i+m_j,m_{i+1},\dots,m_{j-1},m_i+m_j,m_{j+1},\dots m_k)\\
&= d(m_1,\dots,m_{i-1},m_i,m_{i+1},\dots,m_{j-1},m_i,m_{j+1},\dots m_k)\\
&+ d(m_1,\dots,m_{i-1},m_i,m_{i+1},\dots,m_{j-1},m_j,m_{j+1},\dots m_k)\\
&+ d(m_1,\dots,m_{i-1},m_j,m_{i+1},\dots,m_{j-1},m_i,m_{j+1},\dots m_k)\\
&+ d(m_1,\dots,m_{i-1},m_j,m_{i+1},\dots,m_{j-1},m_j,m_{j+1},\dots m_k)\\
&= d(m_1,\dots,m_k) + d(m_{(i,j)(1)},\dots m_{(i,j)(k)})
\end{aligned}$$

Ist dann $\sigma \in \Sigma_k$ eine Permutation die man aus n Transpositionen schreiben kann, so haben wir

$$d(m_{\tau(\sigma(1))},\dots,m_{\tau(\sigma(1))}) = -d(m_{\sigma(1)},\dots,m_{\sigma(k)}) = -d(m_1,\dots,m_k)\cdot\mathrm{sgn}(\sigma) = d(m_1,\dots,m_k)\cdot\mathrm{sgn}(\tau\circ\sigma).$$

□

Ist nun $e_1,\dots,e_n$ ein Erzeugendensystem von einem R-Modul M, und $d \in \mathrm{Alt}^k_R(M,N)$, so können wir

$$m_1 = \sum_{i=1}^n e_i\cdot r_{1,i},\dots,m_k = \sum_{i=1}^n e_i\cdot r_{k,i}$$

schreiben und dann rechnen

$$\begin{aligned}
d(m_1,\dots,m_k) &= d\left(\sum_{i=1}^n e_i\cdot r_{1,i},\dots,\sum_{i=1}^n e_i\cdot r_{k,i}\right)\\
&= \sum_{i\in\{1,\dots,n\}^k} d(e_{i_1},\dots,e_{i_k})\cdot\prod_{j=1}^k r_{j,i_j}.
\end{aligned}$$

Für nicht injektives $i\colon \{1,\dots,k\} \to \{1,\dots,n\}$ hat der entsprechende Summand nun zwei gleiche Argumente und verschwindet damit. Jedes injektive $i\colon \{1,\dots,k\} \to \{1,\dots,n\}$ lässt sich hingegen auf eindeutige Art in eine Permutation $\sigma \in \Sigma_k$ gefolgt von einer monotonen Injektion $\bar{i}\colon \{1,\dots,k\} \to \{1,\dots,n\}$ zerlegen und wir erhalten

$$= \sum_{\substack{i\in\{1,\dots,k\}\to\{1,\dots,n\}\\ \text{monoton, injektiv}}} \sum_{\sigma\in\Sigma_k} d(e_{i_{\sigma(1)}},\dots,e_{i_{\sigma(k)}}) \cdot \prod_{j=1}^{k} r_{j,i_{\sigma(j)}}$$

$$= \sum_{\substack{i\in\{1,\dots,k\}\to\{1,\dots,n\}\\ \text{monoton, injektiv}}} \sum_{\sigma\in\Sigma_k} d(e_{i_1},\dots,e_{i_k}) \cdot \operatorname{sgn}(\sigma) \cdot \prod_{j=1}^{k} r_{j,i_{\sigma(j)}}$$

Insbesondere finden wir:

3.5. Lemma *Ist $e_1,\dots,e_n$ ein nummiertes Erzeugendensystem von einem R-Modul M, so ist die Abbildung*

$$\operatorname{Alt}^k_R(M,N) \longrightarrow \mathrm{F}(\operatorname{Moin}(k,n),N), \quad d \longmapsto d(e\circ i)$$

injektiv, wo

$$\operatorname{Moin}(k,n) = \{i\colon \{1,\dots,k\} \to \{1,\dots,n\} \mid i \text{ injektiv und monoton}\}.$$

Insbesondere stimmen zwei alternierende n-Formen auf M schon dann überein, wenn sie auf $(e_1,\dots,e_n)$ übereinstimmen.

Damit haben wir 1.3 im Wesentlichen bewiesen:

Beweis von 1.3. Existenz: Gegeben $n \in N$ so prüft man leicht, dass

$$R^n \times \cdots \times R^n \xrightarrow{\det} R \xrightarrow{n\cdot -} N$$

eine Form wie gesucht ist.

Eindeutigkeit folgt direkt aus obigem Lemma. □

Aus der allgemeineren Form von 3.5 erhalten wir noch eine enorm wichtige Folgerung:

3.6. Korollar *Ist R ein kommutativer Ring, und hat M eine Erzeugensystem mit n Elementen, so gilt $\operatorname{Alt}^k_R(M,N) = 0$ für alle $k > n$. Hat M insbesondere eine Basis mit n Elementen, so hat jede Basis von M ebenfalls n Elemente.*

Beweis. Für die erste Behauptung beobachten wir einfach, dass es in diesem Fall keine injektive Abbildung $\{1,\dots,k\} \to \{1,\dots,n\}$ gibt, sodass

$$\operatorname{Alt}^k_R(M,N) \longrightarrow \mathrm{F}(\operatorname{Moin}(k,n),N) = \mathrm{F}(\varnothing,N) = \{\varnothing\}$$

injektiv ist, was sicherlich $\operatorname{Alt}^k_R(M,N) = \{0\}$ impliziert.

Die zweite Behauptung folgt, da eine weitere Basis B sicherlich endlich sein muss: Jedes e_i lässt sich durch endlich viele Elemente aus B linear kombinieren, alle diese Element zusammen bilden aber eine endliche Teilmenge von B, die immer noch ein Erzeugendensystem ist; aber B ist als Basis ein minimales Erzeugendensystem kann also nur aus diesen endlich vielen Elementen bestehen.

Und jede nummerierte Basis b mit m Elementen liefert den Isomorphismus $\mathrm{L}_b\colon R^m \to M$ und damit erhalten wir

$$M \times \cdots \times M \xrightarrow{\mathrm{L}_b^{-1}\times\cdots\times\mathrm{L}_b^{-1}} R^m \times \cdots \times R^m \xrightarrow{\det_m} R,$$

ein nicht-triviales Element in $\operatorname{Alt}^m_R(M,R)$, was nach der ersten Aussage $m \leqslant n$ impliziert. Vertauschen der Rollen von m und n liefert auch $n \leqslant m$. □

Insbesondere haben freie R-Moduln für kommutatives R wieder eine wohldefinierte Dimension.

3.7. Bemerkung (1) Für einen Modul M über einem beliebigen kommutativen Ring ist es nicht immer richtig, dass jedes minimale Erzeugendensystem schon eine Basis ist, und das gleiche für maximal linear unabhängige Systeme. Hierfür reicht es, sich den $\mathbb{Z}$-Modul $\mathbb{Z}$ anzuschauen:

Die Menge $\{2,3\}$ ist ein Erzeugendensystem, da $k = 3 \cdot k + 2 \cdot (-k)$ für jedes $k \in \mathbb{Z}$, aber keins der beiden Elemente kann entfernt werden da $\langle i \rangle_{\mathbb{Z}} = \{k \in \mathbb{Z} \mid i \text{ teilt } k\}$ und sicherlich ist $\{2,3\}$ auch keine Basis von $\mathbb{Z}$: Es ist ja schließlich $0 = 3 \cdot 2 + 2 \cdot (-3)$ eine nicht-triviale Linearkombination der 0.

Die Menge $\{2\}$ ist linear unabhängig, da $2 \cdot k = 0$ sicherlich $k = 0$ impliziert und maximal, da für jedes $i \in \mathbb{Z}$ sicherlich $0 = 2 \cdot i + i \cdot (-2)$ eine nicht-triviale Linearkombination der 0 ist, aber sicherlich kein Erzeugendensystem.

Die Argumente, die wir im Falle von Schiefkörpern benutzt haben übertragen sich also nicht auf den Fall allgemeiner (kommutativer) Ringe.

(2) Wir wissen nun, dass der Begriff der Dimension für Moduln über Schiefkörpern und kommutativen Ring wohldefiniert ist (wobei im letzteren Fall nicht jeder Modul überhaupt eine Basis besitzt!). Man kann sich also sofort fragen, ob das auch für beliebige Ringe korrekt ist. Ist es nicht! Es gibt wirklich Ringe R mit der Eigenschaft, dass $R \cong R^2$ als R-Moduln gilt. Wir werden ein Beispiel in den Übungen sehen.

4. Grundlegende Eigenschaften von Determinanten

Die Eindeutigkeitsaussage in 1.3 liefert uns leicht auch folgende fundamentale Eigenschaft:

4.1. Korollar *Sind $A, B \in \mathrm{Mat}(n,n,R)$ für einen kommutativen Ring R, so gilt*

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Insbesondere ist $\det(A)$ eine Einheit in R für jede invertierbare Matrix A.

Dieser Satz wurde historisch erst eine ganze Weile nach Entwicklung der Determinantentheorie bewiesen, wohl von Augustin Louis Cauchy (1789 - 1857) im Jahr 1812, der auch den Cauchy-Folgen, dem Cauchy'schen Integralsatz und vielen weiteren Resultaten seinen Namen leiht.

Beweis. Für fixes A betrachte man die Abbildung

$$d_A \colon (R^n)^n \longrightarrow R, \quad (B_1, \ldots, B_n) \longmapsto \det(A \cdot B).$$

Ich behaupte dies ist eine alternierende n-fach multilineare Abbildung. Hierzu beobachte man nur, dass die i-te Spalte von $A \cdot B$ genau $A \cdot B_i$ ist und die Multiplikation mit A linear. Aber $\det(A) \cdot \det(-)$ ist ebenfalls eine n-fach alternierende Multilinearform und es gilt

$$d_A(e_1, \ldots, e_n) = \det(A \cdot \mathbb{I}_n) = \det(A) = \det(A) \cdot \det(e_1, \ldots e_n)$$

also stimmen beide überein.

Die Determinante ist also ein Monoidhomomorphismus $(\mathrm{Mat}(n,n,R), \cdot) \to (R, \cdot)$ und wir hatten uns schon auf einen frühen Übungszettel überlegt, dass solche immer Einheiten auf Einheiten schicken. □

Für einen Körper erhalten wir auch unmittelbar die gesucht Verstärkung:

4.2. Satz *Ist K ein Körper und $A \in \mathrm{Mat}(n,n,K)$ so ist A invertierbar genau dann, wenn* $\det(A) \neq 0$.

Beweis. Nach 3.13 gibt es eine invertierbare Matrix $B \in \mathrm{Mat}(n,n,K)$, derart, dass $B \cdot A$ Zeilenstufenform hat, insbesondere also obere Dreiecksform, wie wir uns schon in 1.4 überlegt hatten. Aber nun ist A invertierbar genau dann, wenn $B \cdot A$ es ist genau dann, wenn $B \cdot A$ keine Nullzeile hat genau dann, wenn alle Diagonaleinträge von $B \cdot A$ nicht verschwinden genau dann, wenn $\det(B \cdot A) \neq 0$ nach 3.2.

Aber nach vorigem Satz gilt nun $\det(B \cdot A) = \det(B) \cdot \det(A)$ und $\det(B) \neq 0$, sodass $\det(B \cdot A) \neq 0$ genau dann, wenn $\det(A) \neq 0$. □

Die Multiplikativität der Determinante erlaubt es im Fälle von Körpern eine einfachere Methode zur Berechnung von Determinanten anzugeben: Nämlich entsprechen ja elementaren Zeilenoperationen Linksmultiplikationen mit bestimmten Matrizen, hiermit kann man für quadratische Matrizen Dreiecksgestalt erreichen, und für Dreiecksmatrizen sind Determinanten nach 3.2 einfach (das Produkt der Diagonaleinträge). Wir müssen als nur die Determinanten der Elementarmatrizen (die wir in einer Aufgabe auf einem Übungszettel bestimmt haben) berechnen:

4.3. Beobachtung (1) Elementare Zeilenoperationen vom Typ I sind durch Matrizen $\mathrm{S}_{i,j}^{\lambda}$ mit nur 1'en auf der Diagonale, 0'en überall anders, bis auf eine einzelne Position (i,j) (außerhalb der Diagonale) an der ein beliebiges $\lambda \in R$ steht. So eine Matrix hat immer Dreiecksgestalt (obere oder untere, je nachdem ob $i > j$ oder $j < i$), also haben wir immer

$$\det(\mathrm{S}_{i,j}^{\lambda}) = 1$$

(2) Elementare Zeilenoperationen vom Typ II sind durch Matrizen M_i^{λ} mit nur 1'en auf der Diagonale außer an Stelle (i,i), wo ein λ steht, und nur 0'en außerhalb der Diagonale. Also haben wir

$$\det(\mathrm{M}_i^{\lambda}) = \lambda$$

(3) Elementare Zeilenoperationen vom Typ III sind duch Matrizen $\mathrm{T}_{i,j}$ gegeben, die aus $\mathbb{1}_n$ entstehen, indem man die i-te mit der j-ten Spalte vertauscht. Also gilt

$$\det(\mathrm{T}_{i,j}) = -1.$$

4.4. Beispiel Betrachten wir hiermit einmal die Matrix

$$A = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 4 & 2 & 0 & 5 \\ 0 & -6 & 1 & -2 \end{pmatrix} \in \mathrm{Mat}(4,4,\mathbb{Q})$$

Die Leibnizformel liefert die $4! = 24$ Summanden

$$\begin{aligned} \det(A) = {} & 2\cdot 3\cdot 0\cdot(-2) - 2\cdot 3\cdot 1\cdot 5 + 2\cdot 2\cdot 0\cdot(-2) + 2\cdot 2\cdot 1\cdot 2 + 2\cdot(-6)\cdot 0\cdot 5 - 2\cdot(-6)\cdot 0\cdot 2 \\ & -0\cdot 1\cdot 0\cdot(-2) + 0\cdot 1\cdot 1\cdot 5 + 0\cdot 2\cdot 0\cdot(-2) - 0\cdot 2\cdot 1\cdot 2 - 0\cdot(-6)\cdot 0\cdot 5 + 0\cdot(-6)\cdot 0\cdot 2 \\ & +4\cdot 1\cdot 0\cdot(-2) - 4\cdot 1\cdot 1\cdot 2 - 4\cdot 3\cdot 0\cdot(-2) + 4\cdot 3\cdot 1\cdot 2 + 4\cdot(-6)\cdot 0\cdot 2 - 4\cdot(-6)\cdot 0\cdot 2 \\ & -0\cdot 1\cdot 0\cdot 5 + 0\cdot 1\cdot 0\cdot 2 - 0\cdot 3\cdot 0\cdot 5 + 0\cdot 3\cdot 0\cdot 2 - 0\cdot 2\cdot 0\cdot 2 + 0\cdot 2\cdot 0\cdot 2 \\ = {} & -30 + 8 - 8 + 24 = -6 \end{aligned}$$

Dahingegen können wir mit dem Eliminationsalgorithmus

$$\begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 4 & 2 & 0 & 5 \\ 0 & -6 & 1 & -2 \end{pmatrix} \overset{III-2I}{\rightsquigarrow} \begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & -6 & 1 & -2 \end{pmatrix} \overset{IV+2II}{\rightsquigarrow} \begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \overset{III\leftrightarrow IV}{\rightsquigarrow} \begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

erreichen. Die ersten beiden Schritte ändern die Determinante nicht, der dritte fügt ein Vorzeichen ein. Also erhalten wir

$$\det(A) = -\det \begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} = -6$$

Man kann übrigends ebenso von rechts mit den Elemtarmatrizen multiplizieren (also Spaltenoperationen vornehmen); dies hat nach 4.1 den gleichen Effekt auf die Determinante.

Die Multiplikativität der Determinante hat noch eine weitere wichtige Konsequenz: Sind $A, B \in \mathrm{Mat}(n,n,R)$ mit kommutativem Ring R und B ist invertierbar, so gilt

$$\det(B^{-1}\cdot A\cdot B) = \det(B)^{-1}\cdot\det(A)\det(B) = \det(A).$$

Damit erhalten wir:

4.5. Korollar *Sind b und b' zwei endliche numerierte Basen eines R-Moduls M und $\varphi\colon M \to M$ ist R-linear, so gilt*

$$\det(\mathrm{M}(\varphi, b, b)) = \det(\mathrm{M}(\varphi, b', b').$$

Beweis. Nach 3.6 haben die beiden Basen gleich viele Elemente, und nach 7.5 und dem darauf folgenden Beispiel gilt

$$\mathrm{M}(\varphi, b, b) = \mathrm{M}(\mathrm{id}_M, b', b)^{-1} \cdot \mathrm{M}(\varphi, b, b) \cdot \mathrm{M}(\mathrm{id}, b', b)$$

sodass die Behauptung aus der Vorüberlegung folgt. □

Das erlaubt uns zu setzen:

4.6. Definition Ist R ein kommutativer Ring, M ein R-Modul der eine endliche Basis besitzt und $\varphi\colon M \to M$ eine R-linear Abbildung so setzen wir

$$\det(\varphi) = \det(\mathrm{M}(\varphi, b, b))$$

für irgendeine numerierte Basis b von M.

Lasst mich explizit die Warnung aussprechen, dass es hier von größter Wichtigkeit ist, in Ziel und Quelle die gleiche Basis von M zu verwenden (und damit insbesondere auch, dass Ziel und Quelle von φ übereinstimmen). Die Determinante ist also in Wahrheit eine Invariante einer linearen Abbildung und nicht von der gewählten Basis abhängig. Dies wird inbesondere bei der Suche nach einer möglichst leichten Gestalt für die darstellende Matrix $\mathrm{M}(\varphi, b, b)$ eine bedeutende Rolle spielen.

4.7. Bemerkung Man kann die Determinante einer R-linearen Abbildung $\varphi\colon M \to M$ übrigends auch ohne die Wahl einer Basis definieren: Hierzu betrachte man für $k \in \mathbb{N}$ die Abbildungen

$$\varphi^*\colon \mathrm{Alt}^k_R(M, R) \longrightarrow \mathrm{Alt}^k_R(M, R), \quad d \longmapsto \left[M \times \cdots \times M \xrightarrow{\varphi \times \cdots \times \varphi} M \times \cdots \times M \xrightarrow{d} R\right]$$

und für einen R-Modul N

$$\mu\colon R \longrightarrow \mathrm{Lin}_R(N, N), \quad \lambda \longmapsto (- \cdot \lambda),$$

deren Existenz ebenfalls benutzt, dass R kommutativ ist: Die R-Linearität von $- \cdot \lambda\colon N \to N$ besagt

$$(n \cdot r) \cdot \lambda = (n \cdot \lambda) \cdot r$$

für alle $n \in N$ und $r \in R$, was ohne Kommutativität von R nicht stimmen muss.

Wir können nun jedenfalls

$$\varphi^* \in \mathrm{Lin}_R(\mathrm{Alt}^k_R(M, R), \mathrm{Alt}^k_R(M, R))$$

auffassen. Hat dann M eine Basis aus n Elementen, und wir wählen $k = n$ so findet man als Konsequenz von **??**, dass die Abbildung

$$\mu\colon R \to \mathrm{Lin}_R(\mathrm{Alt}^n_R(M, R), \mathrm{Alt}^n_R(M, R))$$

bijektiv ist ($\mathrm{Alt}^n_R(M, R)$ hat dann ja eine Basis aus einem einzigen Element d, und seine linearen Selbstabbildungen werden folglich durch 1×1-Matrizen beschrieben). Es gilt dann

$$\det(\varphi) = \mu^{-1}(\varphi^*),$$

was man ebenfalls zur Definition der Determinante benutzen kann. In gewisser Weise ist diese Definition, obwohl sehr viel abstrakter als die oben gewählte, die bessere: Sie hängt a priori nur von der Existenz einer Basis, aber nicht von ihrer recht willkürlichen Auswahl ab. Desweiteren zeigt sie, dass die Existenz einer Basis eine hinreichende, aber eigentlich keine notwendige Bedingung für die Definition von Determinanten ist: Findet man zu gegebenem M ein k, derart dass

$$\mu\colon R \to \mathrm{Lin}_R(\mathrm{Alt}^k_R(M, R), \mathrm{Alt}^k_R(M, R))$$

bijektiv ist, ist man im Geschäft. Und hiervon gibt es tatsächlich mehr Beispiele als nur Moduln mit endlichen Basen. Etwa werden sie in späteren Semestern die sogenannten projektiven Moduln, als Verallgemeinerung der mit Basen kennen lernen, und für jeden solchen gibt es ein k (den Rang von M), das das gewünschte leistet.

Im für diese Vorlesung wichtigsten Spezialfall von Vektorräumen über einem Körper K erweitert sich der Definitionsbereich der Determinanten hiermit aber nicht: Es ist nicht schwer zu sehen, dass für unendlichdimensionales V auch $\mathrm{Alt}^n_K(V,R)$ unendlich dimensional ist, und damit auch $\mathrm{Lin}_K(\mathrm{Alt}^n_K(V,R),\mathrm{Alt}^n_K(V,R))$, sodass μ sicherlich nicht surjektiv ist.

Zum Schluss überlegen wir uns noch:

4.8. Satz *Ist $A \in \mathrm{Mat}(n,n,A)$ so gilt*

$$\det(A^t) = \det(A),$$

wo A^t die Transponierte (transposite) *Matrix zu A bezeichnet, mit $(A^t)_{i,j} = A_{j,i}$.*

Beweis. Wir haben

$$\begin{aligned}
\det(A) &= \sum_{\sigma\in\Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^n A_{\sigma(i),i} \\
&= \sum_{\sigma\in\Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^n A_{i,\sigma^{-1}(i)} \\
&= \sum_{\sigma\in\Sigma_n} \mathrm{sgn}(\sigma^{-1}) \prod_{i=1}^n A_{i,\sigma(i)} \\
&= \sum_{\sigma\in\Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^n A^t_{\sigma(i),i} \\
&= \det(A^t)
\end{aligned}$$

wo wir im ersten Schritt die Multiplikationstreihenfolge um die Bijektion $\sigma^{-1}\colon \{1,\dots,n\} \to \{1,\dots,n\}$ verändert haben, im zweiten die Summationsreihenfolgen um die Bijektion $(-)^{-1}\colon \Sigma_n \to \Sigma_n$ und im letzten Schritt $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)$ verwendet haben. □

5. Der Laplace'sche Entwicklungssatz

Es gibt noch eine dritte wichtige Art Determinanten zu berechnen, benannt nach dem Franzosen Pierre-Simon Laplace (1749 - 1827). Hierzu erinnere ich an die Matrix $A[i,j] \in \mathrm{Mat}(k-1,n-1,R)$, die aus $A \in \mathrm{Mat}(k,n,R)$ durch Streichen der $i$ten Zeile und $j$ten Spalte hervorgeht.

5.1. Theorem (Laplace'scher Entwicklungssatz) *Ist R ein kommutativer Ring, $A \in \mathrm{Mat}(n,n,R)$ und $1 \leqslant i \leqslant n$, so gelten*

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} \cdot A_{i,j} \cdot \det(A[i,j]) \quad \textit{and} \quad \det(A) = \sum_{j=1}^n (-1)^{i+j} \cdot A_{j,i} \cdot \det(A[j,i]).$$

Mit anderen Worten, man kann eine Zeile (oder Spalte) von A auswählen, die Determinanten aller n $(n-1)\times(n-1)$-Matrizen berechnen, die man durch Streichen dieser Zeile (oder Spalte) und Streichen einer beliebigen Spalte (oder Zeile) berechnen, und aus den n Ergebnissen, die Determinante von A zusammenfügen.

5.2. Beispiel Betrachten wir wieder die Matrix

$$A = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 0 & 3 & 0 & 2 \\ 4 & 2 & 0 & 5 \\ 0 & -6 & 1 & -2 \end{pmatrix} \in \mathrm{Mat}(4,4,\mathbb{Q})$$

aus 4.4. Wählen wir etwa die zweite Zeile zur Entwicklung (es geht natürlich geschickter, wie wir gleich sehen werden) so erhalten wir

$$\det(A) = (-1)^{1+2}\cdot 0 \cdot \det\begin{pmatrix} 1 & 0 & 2 \\ 2 & 0 & 5 \\ -6 & 1 & -2 \end{pmatrix} + (-1)^{2+2}\cdot 3 \cdot \det\begin{pmatrix} 2 & 0 & 2 \\ 4 & 0 & 5 \\ 0 & 1 & -2 \end{pmatrix}$$

$$+(-1)^{2+3}\cdot 0\cdot\det\begin{pmatrix}2&1&2\\4&2&5\\0&-6&-2\end{pmatrix}+(-1)^{2+4}\cdot 2\cdot\det\begin{pmatrix}2&1&0\\4&2&0\\0&-6&1\end{pmatrix}$$

und reduziert das Problem auf zwei Determinanten von 3×3-Matrizen. Entwickelt man etwa die Determinante im zweiten Summanden nun nach der zweiten Spalte, so erhält man

$$\det\begin{pmatrix}2&0&2\\4&0&5\\0&1&-2\end{pmatrix}=(-1)^{2+3}\cdot 1\cdot\det\begin{pmatrix}2&2\\4&5\end{pmatrix}=(-1)\cdot(10-8)=-2$$

und entwickelt man die im vierten Summanden nach der dritten Spalte so erhält man

$$\det\begin{pmatrix}2&1&0\\4&2&0\\0&-6&1\end{pmatrix}=(-1)^{3+3}\cdot 1\cdot\det\begin{pmatrix}2&1\\4&2\end{pmatrix}=(-1)\cdot(4-4)=0$$

Und damit insgesamt

$$\det(A)=3\cdot(-2)=-6.$$

Geschickter wäre es natürlich direkt nach der dritten Spalte zu entwickeln. Das liefert

$$\det\begin{pmatrix}2&1&0&2\\0&3&0&2\\4&2&0&5\\0&-6&1&-2\end{pmatrix}=-\det\begin{pmatrix}2&1&2\\0&3&2\\4&2&5\end{pmatrix}$$

$$=-2\cdot\det\begin{pmatrix}3&2\\2&5\end{pmatrix}-4\det\begin{pmatrix}1&2\\3&2\end{pmatrix}=-2(15-4)-4(2-6)=-22+16=-6$$

was die wohl schnellste Art ist diese Determinante zu bestimmen.

Der Laplace'sche Entwicklungssatz lässt sich immer dann gewinnbringend einsetzen, wenn es die gegebene Matrix viele 0'en enthält (sogenannte dünn besetzte Matrizen); sowohl der Eliminationsalgorithmus als auch die Leibnizformel sind gegebenüber diesem Phänomen gegenüber etwas blind. Für dicht besetzte Matrizen liefert er zu einer $n\times n$-Matrix n $(n-1)\times(n-1)$-Matrizen, und damit benötigt er genau wie die Leibniz-Formel $n!$ Berechnungen. Hier ist dann der Eliminationsalgorithmus mit seinen n^2 Schritten sehr viel schneller. Im allgemeinen sollte man natürlich alle Berechnungsmethoden mischen, so wie sie gerade passen (etwa erst nach einer dünn besetzten Spalte oder Zeile entwickeln, dann den Gauß-Algorithmus anwenden, bis wieder so eine Zeile/Spalte auftaucht etc)

Nun zum Beweis. Er beginnt mit folgendem Spezialfall:

5.3. Lemma *Ist $A\in\mathrm{Mat}(n,n,R)$, R kommutativer Ring, von der Form*

$$\begin{pmatrix}A_{1,1}&\dots&A_{1,j-1}&0&A_{1,j+1}&\dots&A_{1,n}\\\vdots&&\vdots&\vdots&\vdots&&\vdots\\A_{i-1,1}&\dots&A_{i-1,j-1}&0&A_{i-1,j+1}&\dots&A_{i-1,n}\\A_{i,1}&\dots&A_{i,j-1}&\lambda&A_{i,j-1}&\dots&A_{i,n}\\A_{i+1,1}&\dots&A_{i+1,j-1}&0&A_{i+1,j+1}&\dots&A_{i+1,n}\\\vdots&&\vdots&\vdots&\vdots&&\vdots\\A_{n,1}&\dots&A_{n,j-1}&0&A_{n,j+1}&\dots&A_{n,n}\end{pmatrix}$$

Dann gilt

$$\det(A)=(-1)^{i+j}\cdot\lambda\cdot\det(A[i,j]).$$

BEWEIS. Durch $(n-j)$ Spaltentausche und $(n-i)$ Zeilentausche können wir aus A die Matrix

$$B = \begin{pmatrix} A_{1,1} & \dots & A_{1,j-1} & A_{1,j+1} & \dots & A_{1,n} & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ A_{i-1,1} & \dots & A_{i-1,j-1} & A_{i-1,j+1} & \dots & A_{i-1,n} & 0 \\ A_{i+1,1} & \dots & A_{i+1,j-1} & A_{i+1,j+1} & \dots & A_{i+1,n} & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ A_{n,1} & \dots & A_{n,j-1} & A_{n,j+1} & \dots & A_{n,n} & 0 \\ A_{i,1} & \dots & A_{i,j-1} & A_{i,j-1} & \dots & A_{i,n} & \lambda \end{pmatrix}$$

produzieren. Es gilt also

$$\det(A) = (-1)^{(n-i)+(n-j)}\det(B) = (-1)^{i+j}\det(B)$$

und $A[i,j] = B[n,n]$. Wir rechnen

$$\det(B) = \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma)\cdot\prod_{i=1}^{n} B_{\sigma(i),i}$$

Aber scharfes Hinsehen zeigt, dass $B_{\sigma(n),n} = 0$ außer für $\sigma(n) = n$, sodass sich diese Summe vereinfacht zu

$$= \sum_{\substack{\sigma\in\Sigma_n \\ \sigma(n)=n}} \operatorname{sgn}(\sigma)\cdot\prod_{i=1}^{n} B_{\sigma(i),i} = \sum_{\sigma\in\Sigma_{n-1}} \operatorname{sgn}(\sigma)\cdot\left(\prod_{i=1}^{n-1} B_{\sigma(i),i}\right)\cdot\lambda,$$

da eine Permutation $\sigma\in\Sigma_n$ mit $\sigma(n) = n$ das gleich Vorzeichen hat, wie ihre Restriktion zu Σ_{n-1}, z.B. da sich die Menge der Fehlstände nicht verändert. Aber damit erhalten wir

$$= \det(B[n,n])\cdot\lambda = \det(A[i,j]).$$

Einfügen in die obige Rechnung liefert die Behauptung. □

BEWEIS VON 5.1. Wir beweisen die linke der beiden Formeln. Sei hierzu $B(i,j)\in \mathrm{Mat}(n,n,R)$ diejenige Matrix, die man aus A erhält, indem man die j-te Spalte A_j von A durch den Einheitsvektor e_i ersetzt. Es gilt dann $(B(i,j))[i,j] = A[i,j]$. Weiterhin haben wir natürlich$A_j = \sum_{i=1}^{n} e_i\cdot A_{i,j}$ und damit rechnen wir

$$\det(A) = \det_n(A_1,\dots,A_n) = \det_n(A_1,\dots,\sum_{i=1}^{n} e_i\cdot A_{i,j},\dots,A_n)$$

$$= \sum_{i=1}^{n}\det_n(A_1,\dots,e_i,\dots,A_n)\cdot A_{i,j} = \sum_{i=1}^{n}\det(B(i,j))\cdot A_{i,j}$$

Aber die Matrizen $B(i,j)$ haben nun die Form aus dem vorigen Lemma, und damit erhalten wir

$$= \sum_{i=1}^{n}(-1)^{i+j}\cdot\det((B(i,j))[i,j])\cdot A_{i,j} = \sum_{i=1}^{n}(-1)^{i+j}\cdot\det(A[i,j])\cdot A_{i,j}$$

was wir zeigen wollten.

Die zweite Formel, kann man völlig analog beweisen, oder man benutzt 4.8 zweimal: Es gilt nach der ersten Formel nämlich

$$\det(A) = \det(A^t) = \sum_{i=1}^{n}(-1)^{i+j}\cdot\det(A^t[i,j])\cdot A^t_{i,j} = \sum_{i=1}^{n}(-1)^{i+j}\cdot\det(A[j,i]^t)\cdot A_{j,i}$$

$$= \sum_{i=1}^{n}(-1)^{i+j}\cdot\det(A[j,i])\cdot A_{j,i}.$$

□

6. Die Cramer'sche Regel

Da wir aus 4.2 wissen, dass die Determinante einer Matrix über einem Körper ihre Invertierbarkeit entscheiden kann, gibt es Hoffnung auch das Inverse mittels Determinanten zu beschreiben. Das ist der Inhalt dieses Abschnitts. Wir brauchen:

6.1. Definition Zu einer Matrix $A \in \mathrm{Mat}(n,n,R)$ mit kommutativen Ring R heißen die Zahlen

$$\mathrm{cf}(A)_{i,j} := (-1)^{i+j}\det(A[i,j])$$

die *Kofaktoren (cofactors)* von A. Sie bilden selbst wieder eine Matrix $\mathrm{cf}(A) \in \mathrm{Mat}(n,n,R)$, die *Kofaktormatrix (cofactor matrix)* von A. Die Matrizen $A[i,j] \in \mathrm{Mat}(n-1,n-1,R)$ selber heißen die *Hauptminoren (principal minors)* von A.

Hiermit können wir nun folgenden Satz formulieren:

6.2. Theorem *Ist $A \in \mathrm{Mat}(n,n,R)$ mit kommutativen Ring R so gilt*

$$\mathrm{cf}(A)^t \cdot A = \det(A) \cdot \mathbb{I}_n = A \cdot \mathrm{cf}(A)^t.$$

Damit können wir 4.2 auf beliebige kommutative Ringe erweitern und erhalten die gesuchte Formel für das Inverse einer Matrix:

6.3. Korollar *Ist $A \in \mathrm{Mat}(n,n,R)$ mit kommutativen Ring R, so ist A invertierbar genau dann, wenn $\det(A) \in R$ eine Einheit ist. In diesem Fall gilt*

$$A^{-1} = \mathrm{cf}(A)^t \cdot \frac{1}{\det(A)}.$$

Man beobachte noch, dass $\mathrm{cf}(A)^t = \mathrm{cf}(A^t)$: Wir rechnen

$$\mathrm{cf}(A)^t_{i,j} = \mathrm{cf}(A)_{j,i} = (-1)^{i+j}\det(A[j,i]) = (-1)^{i+j}\det(A[j,i]^t) = (-1)^{i+j}\det(A^t[i,j]) = \mathrm{cf}(A^t)_{i,j}$$

mittels 4.8.

6.4. Beispiel (1) Für $n = 2$ haben wir

$$\mathrm{cf}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

und demzufolge

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \frac{1}{ad-bc}$$

falls $ad - bc$ eine Einheit in R ist.

(2) Für $n = 3$ haben wir

$$\mathrm{cf}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} ei-fh & fg-di & dh-eg \\ ch-bi & ai-cg & bg-ah \\ bf-ce & cd-af & ae-bd \end{pmatrix}$$

und demzufolge

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1} = \begin{pmatrix} ei-fh & ch-bi & bf-ce \\ fg-di & ai-cg & cd-af \\ dh-eg & bg-ah & ae-bd \end{pmatrix} \cdot \frac{1}{aei+bfg+cdh-ceg-bdi-afh}$$

falls $aei + bfg + cdh - ceg - bdi - afh \in R$ invertierbar ist.

Die Komplexität dieser Formeln nehmen mit wachsendem n rapide zu und sind deshalb für konkrete Berechnungen oft ungeschickt. Sie haben aber trotzdem viel theoretischen Wert. Etwa sehen wir sofort, dass für eine Matrix $A \in \mathrm{Mat}(n,n,\mathbb{Z})$ mit $\det(A) \neq 0$ das Inverse von A in $\mathrm{Mat}(n,n,\mathbb{Q})$ genau dann wieder in $\mathrm{Mat}(n,n,\mathbb{Z})$ liegt, falls $\det(A) = \pm 1$ gilt, und sonst zumindest die auftauchenden Nenner in den gekürzten Brüchen alle $\det(A)$ teilen.

Beweis von 6.2. Wir beweisen wieder die linke Formel zuerst. Wir haben

$$(\mathrm{cf}(A)^t \cdot A)_{i,j} = \sum_{k=1}^{n} \mathrm{cf}(A)_{k,i} \cdot A_{k,j}$$

und andererseits natürlich

$$(\det(A) \cdot \mathbb{1}_n)_{i,j} = \begin{cases} \det(A) & i = j \\ 0 & i \neq j \end{cases}.$$

Dass diese Ausdrücke für $i = j$ übereinstimmen ist gerade der Laplace'sche Entwicklungssatz 5.1. Für $i \neq j$ bilden wir die Matrix B aus A indem wir die i-te Spalte von A durch die j-te ersetzen. Dann gilt $B[k,i] = A[k,i]$ für jedes $1 \leqslant k \leqslant n$ und B hat zwei gleiche Spalten, und damit $\det(B) = 0$. Auf der anderen Seite rechnen wir mittels des Entwicklungssatzes um die i-te Spalte

$$\det(B) = \sum_{k=1}^{n} (-1)^{i+k} \cdot B_{k,i} \cdot \det(B[k,i]) = \sum_{k=1}^{n} (-1)^{i+k} \cdot A_{k,j} \cdot \det(A[k,i]) = \sum_{k=1}^{n} \mathrm{cf}(A)_{k,i} \cdot A_{k,j}.$$

Die zweite Formel kann man analog zeigen, oder wieder auf 4.8 zurückgreifen um sie aus der ersten herzuleiten:

$$A \cdot \mathrm{cf}(A)^t = (A^t)^t \cdot \mathrm{cf}(A^t) = (\mathrm{cf}(A^t)^t \cdot A^t)^t = (\det(A^t) \cdot \mathbb{1}_n)^t = \det(A) \cdot \mathbb{1}_n.$$

□

Fassen wir also noch einmal zusammen:

6.5. Korollar *Ist $\varphi\colon M \to M$ eine R-lineare Abbildung eines R-Moduls M, der eine endliche Basis besitzt, in sich selbst. Dann sind äquivalent:*

(1) φ ist bijektiv,
(2) φ ist surjektiv,
(3) φ besitzt ein R-lineares Linksinverses,
(4) φ besitzt ein R-lineares Rechtsinverses,
(5) $\det(\varphi) \in R$ ist eine Einheit.

Falls R ein Körper ist, kann man der Liste auch noch

(6) φ ist injektiv

hinzufügen.

Beweis. Offenbar gelten (1)⇒(2) und (1)⇒(3). Weiterhin gilt (2)⇒(4): Ist b eine numerierte Basis von M, so wählen wir Urbilder b'_i von b_i und können laut 5.9 eine eindeutige lineare Abbildung $\psi\colon M \to M$ mit $\psi(b_i) = b'_i$ finden. Aber dann gilt $\varphi \circ \psi(b_i) = b_i$ und damit folgt ebenfalls nach 5.9, dass $\varphi \circ \psi = \mathrm{id}_M$. Als nächstes beobachten wir, dass (3)⇒(5): Es gilt ja schließlich

$$1 = \det(\mathrm{id}_M) = \det(\psi \circ \varphi) = \det(\psi) \circ \det(\varphi)$$

und damit folgt (R ist kommutativ!), dass $\det(\varphi) \in R$ eine Einheit ist; genauso folgt (4)⇒(5). Dass schließlich, (5)⇒(6) gilt, haben wir gerade in 6.3 gesehen. Ist R ein Körper, so wissen wir schon aus 5.5, dass auch die Injektivität zur Bijektivität von φ äquivalent ist. □

6.6. Bemerkung Ist R ein kommutativer Ring, so folgt wirklich nicht, dass die Injektivität von φ schon die Surjektivität impliziert: Man betrachte etwa $- \cdot 2\colon \mathbb{Z} \to \mathbb{Z}$. Ebenso sind andere Bedingungen die wir für Selbstabbildungen von Vektorräumen als äquivalent erkannt haben (siehe 5.6) über beliebigen kommutativen Ringen nicht äquivalent: Die Zeilen einer Matrix A sind etwa genau dann linear unabhängig, wenn $\mathrm{L}(A)$ injektiv ist, und das reicht eben für die Surjektivität nicht aus.

Mit der Formel fürs Inverse im Gepäck, kann man nun auch explizite Gleichungen lösen.

6.7. Korollar (Cramer'sche Regel) *Ist $A \in \mathrm{Mat}(n,n,R)$ invertierbar und R kommutativ, und $b \in R^n$, so ist das eindeutig bestimmte $x \in R^n$ mit $A \cdot x = b$ gegeben durch*

$$x_i = \frac{\det(A(b,i))}{\det(A)},$$

wo $A(b,i) \in \mathrm{Mat}(n,n,R)$ diejenige Matrix ist, die aus A durch Ersetzen der i-ten Spalte durch b entsteht.

Dies wunderschön konzise Formel wurde vom Schweizer Gabriel Cramer (1704 - 1752) kurz vor seinem Tod veröffentlicht, allerdings ohne Beweis; soweit ich die Historie verstehe, ist dieser von Laplace gegeben worden. Sie war auch schon vorher vom Japaner Seki Takakazu (1642 - 1708) entdeckt worden, aber dies war in Europa in der Zeit nicht bekannt.

Beweis. Man beobachte, dass nach Laplace'schem Entwicklungssatz angewendet auf die i-te Spalte

$$\det(A(b,i)) = \sum_{k=1}^{n} \mathrm{cf}(A)_{k,i} \cdot b_k$$

gilt, und die rechte Seite ist nach 6.3 nichts weiter als der i-te Eintrag von $A^{-1} \cdot b = x$. □

6.8. Beispiel Im Falle $n = 3$ und

$$A = \begin{pmatrix} a & \beta & c \\ d & e & f \\ g & h & i \end{pmatrix}, \quad b = \begin{pmatrix} k \\ l \\ m \end{pmatrix}$$

so gilt für die Lösung von $A \cdot x = b$ bei invertierbarem A

$$x_1 = \frac{\det \begin{pmatrix} k & \beta & c \\ l & e & f \\ m & h & i \end{pmatrix}}{\det \begin{pmatrix} a & \beta & c \\ d & e & f \\ g & h & i \end{pmatrix}}, \quad x_2 = \frac{\det \begin{pmatrix} a & k & c \\ d & l & f \\ g & m & i \end{pmatrix}}{\det \begin{pmatrix} a & \beta & c \\ d & e & f \\ g & h & i \end{pmatrix}}, \quad x_3 = \frac{\det \begin{pmatrix} a & \beta & k \\ d & e & l \\ g & h & m \end{pmatrix}}{\det \begin{pmatrix} a & \beta & c \\ d & e & f \\ g & h & i \end{pmatrix}}$$

Index