Lineare Algebra I

Wintersemester 2013/2014
Albert-Ludwigs-Universität Freiburg

Heike Mildenberger

9. Januar 2014

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Mengen, Axiome und das Axiomensystem von Zermelo und Fraenkel

Die meisten Definitionen enthalten den Ausdruck: „Sei X eine Menge." Daher stellen wir uns zu Anfang die Frage:

Was ist eine Menge?

Die folgende Antwort wird von den allermeisten mathematischen Schulen akzeptiert:

Definition 1.1. Jedes Objekt ist eine Menge, wenn es Element eines Modells des Axiomensystems ZFC ist, das heißt, wenn man seine Existenz aus den Axiomen von Zermelo und Fraenkel ZFC (mit den klassischen Beweisregeln) nicht widerlegen kann.

Wir betrachten in dieser Vorlesung vor allen Dingen Mengen, die in *allen* Modellen von ZFC vorkommen, das heißt Mengen, deren Existenz man in ZFC beweisen kann. Wir werden einige solcher Existenzbeweise führen, darunter Existenzbeweise für $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Vielleicht werden Sie im Laufe Ihres Studiums Beispiele für Mengen kennenlernen, die es nur in manchen ZFC-Modellen gibt. Wenn Sie sich für solche Mengen interessieren, können Sie später einmal eine Vorlesung über Unabhängigkeitsbeweise hören. ZFC hat viele verschiedene Modelle.

Nun folgen erste Erklärungsschritte der Begriffe, die in der ersten Definition vorkommen.

Beweise führen wir nach den klassischen Beweisregeln, die wir üben, aber hier nicht auflisten (Es sind etwa zehn Regeln.). Indirekte Beweise sind gestattet. Eine Aussage ist bewiesen, (genau dann) wenn ihr Negat widerlegt ist.

Ein ZFC-Modell besteht aus einem Universum aller Mengen und einer $\in$-Relation, $x \in y$ wird interpretiert als: „x ist eine Menge und y ist eine Menge und x ist Element von y." In einem ZFC-Modell soll alle ZFC-Axiome gelten.

Wir schauen uns im Duden den Eintrag „Axiom" an:

„1. als absolut richtig erkannter Grundsatz; gültige Wahrheit, die keines Beweises bedarf

2. nicht abgeleitete Aussage eines Wissenschaftsbereichs, aus der andere Aussagen deduziert werden"

Bei den Axiomen ZFC Zermelo[1], Fraenkel[2] und Choice (steht für Axiom of Choice, das Auswahlaxiom), handelt es sich eher um Axiome nach der ersten Definitionsmöglichkeit. Man kann sie nicht beweisen. Die meisten ZFC-Axiome und auch den Aufbau der Sprache der ersten Stufe kann man aus der Alltagserfahrung im Umgang mit endlich langen Zeichenreihen nachvollziehen, sozusagen in gewissem Maß experimentell verifizieren. Hingegen beim Unendlichkeitsaxiom und beim Auswahlaxiom hat man in der Natur kaum Vorbilder und kann außer Gedankenexperimenten keine Experimente machen. Das Wort „... keines Beweises bedarf" im Duden-Eintrag ist daher für unser Anliegen, die Mathematik auf sicheren Grundlagen möglichst rein deduktiv aufzubauen, eher eine beschönigende Notlösung. Mathematik heißt übrigens auf Deutsch: Kunst des Lernens. Wir schauen uns nun die Axiome, die ab 1930 etwa als Axiome der gesamten Mathematik gelten, an:

ZFC: Die Liste der Zermelo–Fraenkel–Axiome mit Auswahlaxiom

Abgeschrieben und zusammengestellt aus [12].

(1) Extensionalitätsaxiom.
Je zwei Mengen, die dieselben Elemente enthalten, sind gleich. Beispiel: $\{1,1,2\} = \{1,2\} = \{2,1\}$.

(2) Existenzaxiom.
Es gibt eine Menge x. Diese Axiom gehört streng genommen nicht zu ZFC sondern zu den logischen Axiomen. Da wir die Beweisregeln nicht auflisten werden, haben wir dieses Axiom hier aufgeschrieben.

(3) Paarmengenaxiom.
Zu je zwei Mengen x, y gibt es die Paarmenge $\{x,y\}$.

(4) Aussonderungsschema.
Zu jeder Menge x und zu jeder in der mengentheoretischen Sprache der ersten Stufe formulierbaren Eigenschaft φ und zu jeder Parametermenge p gibt es die Menge
$$\{u \in x \mid \varphi(u,p)\}.$$
Bsp: $\{n \in \mathbb{N} \mid n \text{ prim}\}$, $\{(n,m) \in \mathbb{N}\times\mathbb{N} \mid n,m \text{ Primzahlpaar}\}$, $\emptyset = \{u \in x \mid u \neq u\}$, hierbei sei x aus dem Existenzaxiom genommen.

(5) Vereinigungmengenaxiom.
Zu jeder Menge x gibt es die Vereinigungsmenge von x, das ist die Menge, die die Elemente jeder Menge, die Element von x ist, als Elemente enthält. Wir schreiben $\bigcup x$ dafür.
$$\bigcup x = \{z \mid \exists y(y \in x \wedge z \in y)\}.$$
Bsp. $\bigcup\{x,y\} = x \cup y$

(6) Potenzmengenaxiom.
Zu jeder Menge gibt es die Potenzmenge, $\mathscr{P}(x) = \{y \mid y \subseteq x\}$. Wir schreiben $y \subseteq x$ als Abkürzung für $\forall z(z \in y \to z \in x)$.

[1] Ernst Zermelo, 1871 – 1953
[2] Abraham Halevi Fraenkel, 1891 – 1965

(7) Unendlichkeitsaxiom.
Es gibt eine unendliche Menge. Formalisiert: Es gibt eine Menge x, so dass x induktiv ist. Letzteres heißt:

$$\emptyset \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x).$$

(8) Fundierungsaxiom.
Jede nicht leere Menge x hat ein $\in$-minimales Element u, d.h. $u \in x \wedge \forall z \in x \neg z \in u$.

Konsequenzen: $x \neq \{x\}$. Im Mengenuniversum gibt es keine unendlich lang ansteigendenden Ketten $x_0 \ni x_1 \ni x_2 \ldots$ und keine $\in$-Schleifen $x_0 \in x_1 \in \cdots \in x_n \in x_0$.

(9) Ersetzungsschema.
Sei φ eine erststufige Eigenschaft, die auf x einen funktionalen Zusammenhang beschreibt. Dann gibt es die Bildmenge von x unter dieser Funktion. Formal: $\forall u \in x \exists^{=1} w \varphi(u, w, p) \to \exists y \forall u \in x \exists w \in y \varphi(u, w, p)$

(10) Auswahlaxiom.
Zu jeder Menge nicht leerer Mengen gibt es eine Auswahlfunktion. $\forall y((y \in x \to y \neq \emptyset) \to \exists f \forall y \in x f(y) \in y))$

Axiome (1) bis (9) zusammen heißen ZF. Axiome (1) bis (10) zusammen heissen ZFC. Beweise, bei denen die axiomatischen Grundlagen nicht genannt sind, werden auf der Basis von ZFC geführt. Dies gilt wahrscheinlich so für alle Mathematik, die Sie hier in den ersten Jahren oder jemals hören.

Manche Mathematiker(innen) deklarieren bei Benutzung das Auswahlaxiom, da es wegen seinen inkonstruktiven Charakters vielleicht weniger plausibel aussieht. Sie haben in der Schule sicherlich schon das Auswahlaxiom benutzt in der Analysis, womöglich, ohne es bemerkt zu haben. Vom Anliegen der Widerspruchsfreiheit her ist das Auswahlaxiom hingegen eine ungefährliche Zugabe:

Satz 1.2. *(1) Gödel*[3] *1931 (Drei Anwendungen des zweite Gödelsche Unvollständigkeitssatzes). Wenn* ZF *widerspruchsfrei ist, dann beweist* ZF *nicht, dass es widerspruchsfrei ist. Wenn* ZFC *widerspruchsfrei ist, dann beweist* ZFC *nicht, dass es widerspruchsfrei ist. Die Zahlentheorie beweist nicht, dass sie widerspruchsfrei ist.*

(2) Gödel 1938. Wenn ZF *widerspruchsfrei ist, so auch* ZFC.

Beweise zum ersten dieser Sätze können Sie in der Vorlesung „Mathematische Logik" hören. Der zweite Satz wird manchmal in einer Vorlesung über axiomatische Mengenlehre bewiesen. Wir werden ZFC zu den Sätzen hinzuschreiben, die nicht in ZF alleine geführt werden können.

„Speziellere" Axiomensysteme: Gruppenaxiome, vollständige archimedisch angeordnete Körper, Ringaxiome, Ordnungsaxiome, Axiome für Boole'sche Algebren und viele mehr.

Bei vielen spezielleren Axiomensystemen beweist ZFC jeweils, dass das speziellere Axiomensystem widerspruchsfrei ist. Sie werden im Laufe Ihres Studiums eine Fülle solcher Axiomensysteme sehen.

Nun schauen wir uns noch an, was im Aussonderungsschema und im Ersetzungsschema mit „erststufiger mengentheoretischer Eigenschaft" gemeint ist:

[3] Kurt Gödel, 1906–1976

Atomare Eigenschaften sind: $x = y$, $x \in y$ (und nur diese). Wenn φ und ψ Eigenschaften sind und x eine Variable ist, so sind $(\varphi \wedge \psi)$, $(\varphi \to \psi)$, $(\varphi \vee \psi)$, $(\varphi \leftrightarrow \psi)$, $\neg\varphi$, $\exists x\varphi$, $\forall x\varphi$ Eigenschaften. Jede Eigenschaft lässt sich in endlich vielen Schritten aus den atomaren Eigenschaften aufbauen. Die Junktoren und die Quantoren tragen hierbei ihre übliche Bedeutung $\exists$ steht für „es gibt eine Menge" und $\forall$ steht für „für alle Mengen". Unsere Klammernkonventionen gestatten eindeutige Lesbarkeit. $\forall x \in y\varphi$ steht als Abkürzung für $\forall x(x \in y \to \varphi)$ und $\exists x \in y\varphi$ steht als Abkürzung für $\exists x(x \in y \wedge \varphi)$. „Es gibt genau ein x mit φ" schreibt man als $\exists^{=1} x\varphi$. Dies steht als Abkürzung für $\exists x(\varphi(x) \wedge \forall y(\varphi(y) \to x = y))$. Definierte Terme und Eigenschaften können, sozusagen als Abkürzungen, als Formeln in den Schemata und im Aufbau neuer Begriffe verwendet werden: Beispiele: $\emptyset$ (mit seinem Existenzbeweis von oben), $\{x\}$, $\bigcup x$, $\mathscr{P}(x)$, $x \subseteq y$ für $\forall z(z \in x \to z = y)$, und fast alles, was Sie im Lauf der Vorlesungen sehen werden, kann zum Aufbau weiterer Mengen verwendet werden.

Wir brauchen in den Schemata diese klare Festlegung der sprachlichen Möglichkeiten, um Paradoxa der Art

Die kleinste Zahl, die nicht mir vierzig Buchstaben definiert werden kann.

in den Definitionen in der Mathematik zu verbieten.

Definition 1.3. Wir nennen beliebige Zusammenfassungen von Mengen Klassen. Die Allklasse ist die Klasse aller Mengen.

Satz 1.4. *Die Allklasse ist keine Menge.*

Beweis: Annahme: Es gäbe die Menge x aller Mengen. Dann bilden wir die Russell'sche Menge [4]

$$y = y_{\text{Russell}} = \{u \in x \mid u \notin u\}.$$

Wir haben $y \in y$ impliziert $y \notin y$, und $y \notin y$ impliziert $y \in y$. □

Wir kennzeichnen das Ende eines Beweises mit einem Kästchen.

1.2 Die natürlichen Zahlen

Definition 1.5. Die Terme der Art $\underline{0} = \emptyset$,
$\underline{n+1} = \underline{n} \cup \{\underline{n}\}$, heißen die von Neumann'schen[5] natürlichen Zahlen.

Definition 1.6.

$$N = \{\underline{0}, \underline{1}, \dots\}.$$

heißt die von Neumann'sche Menge der natürlichen Zahlen.

Gibt es N?

Satz 1.7. *N ist eine Menge.*

Beweis: Wir nehmen ein x, wie es im Unendlichkeitsaxiom gegeben ist. Dann schreiben wir

$$N = \{z \in x \mid \forall y((y \subseteq x \wedge y \text{ induktiv}) \to z \in y)\}. \qquad (*)$$

Dies ist die offizielle Definition von N in ZFC. □

[4] Bertrand Russell, 1872 – 1970
[5] John von Neumann, 1903 – 1957

Die natürlichen Zahlen $(\mathbb{N}, 0, +1)$ sind nun irgendeine isomorphe Kopie der von Neumann'schen Menge mit ihrer Struktur. Die von Neumann'sche Struktur selbst ist gut, aber man darf sich auch etwas anderes aussuchen.

Bemerkung 1.8. x ist in y enthalten, ist im Deutschen zweideutig: Es kann sowohl $x \in y$ and auch $x \subseteq y$ gemeint sein.

Definition 1.9. (und Behauptung) Seien x, y Mengen. Dann gibt es folgende Mengen

(1) $x \cap y = \{z \in x \mid z \in y\}$ heißt die Schnittmenge von x und y.

(2) Sei $y \neq \emptyset$. $\bigcap y = \{z \in \bigcup y \mid \forall x \in y z \in x\}$ heißt der Schnitt über x. Als Randfall kann man definieren $\bigcap \emptyset =$ Allklasse.

(3) $x \cup y = \bigcup\{x, y\}$ heißt die Vereinigung von x und y.

(4) $x \setminus y = \{z \in x \mid z \notin y\}$ heißt x ohne y.

(5) $x \times y = \{(u, v) \mid u \in x, v \in y\}$ heißt das artesische[6] Produkt von x und y.

Bemerkung: Für den Beweis der Existenz des kartesischen Produkts wird man zunächst geordnete Tupel (u, v) als geeigenete Mengen modellieren, z.B. als $\{u, \{u, v\}\}$. Man braucht ja bei Tupeln immer nur folgende Eigenschaft

$$(x, y) = (u, z) \to (x = u \wedge y = z).$$

Dann zeigt man die Existenz des kartesischen Produkts am einfachsten mit dem Paarmengenaxiom, dem Vereinigungsmengenaxiom, dem Potenzmengenaxiom und dem Aussonderungsaxiom. Sportliche Leute schaffen es auch ohne das Potenzmengenaxiom, nehmen dafür das Ersetzungsschema mit geeigneten einfachen funktionalen Zuordnungen. Wenn Sie die Sache sehr interessiert, schauen Sie in einem Mengenlehrebuch nach. Man schaut am besten zuerst unter Kuratowski[7] pairs oder ordered pairs.

Relationen sind Teilmengen von kartesischen Produkten von Mengen, zum Beispiel $<$ auf $\mathbb{N}$: Diese Relation kann man mit $\{(m, n) \in \mathbb{N} \times \mathbb{N} \mid m < n\}$ identifizieren. Für klassengroße Pendants zu Relationen gibt es meines Wissens kein eigenes Wort. Beispiel: Die $\in$-Relation.

Definition 1.10. (und Bemerkungen) Seien x, y Mengen. Sei $f\colon x \to y$ eine Funktion, das heißt, $f \subseteq x \times y$ und für jedes $u \in x$ gibt es genau ein $v \in y$, so dass $(u, v) \in f$. Man schreibt für letzteres eher $f(u) = v$. Die Menge x heißt der Definitionsbereich von f, die Menge y heißt Zielbereich. Man kann eine Funktion f mit ihren Graphen

$$\{(u, v) \in x \times y \mid f(u) = v\}$$

identifizieren, verliert dabei jedoch die Information über den Zielbereich y. Er wird ersetzt durch den minimalen Zielbereich

$$\text{bild}(f) = f[x] = \{f(u) \mid u \in x\} \subseteq y$$

oder irgendeine Obermenge der Bildmenge. bild(f) heißt die Bildmenge von f. Zu einer klassen-großen eindeutigen Zuordnung sagt man auch Operation oder Funktional.

[6] René Descartes, 1596 – 1650
[7] Casimir Kuratowski, 1896–1980

Bem.: Wir schreiben nicht $f(x)$ für $f[x]$ (obwohl dieses in manchen Gebieten Usus ist), da wir uns der Möglichkeit, dass $f(x) \neq f[x]$, nicht begeben wollen. Denken Sie nur an die von Neumann'schen natürlichen Zahlen. Es gibt nur eine Funktion auf N, die $f(x) = f[x]$ für alle $x \in N$ erfüllt, nämlich die Identität. (Beweis: Übung). Natürlich wollen wir viele verschiedene Funktionen betrachten.

Wichtige Eigenschaften von Funktionen sind:

Definition 1.11. Sei $f\colon X \to Y$ eine Funktion, und sei $g\colon Y \to Z$ eine Funktion.

(1) $f\colon X \to Y$ heißt injektiv, wenn für je zwei $x, y \in X$, aus $f(x) = f(y)$ immer $x = y$ folgt.

(2) $f\colon X \to Y$ heißt surjektiv, wenn $\text{bild}(f) = Y$.

(3) f heißt bijektiv, wenn f injektiv und surjektiv ist.

(4) $g \circ f$ ist die Funktion zuerst f, dann g. Also für $x \in X$, $(g \circ f)(x) := g(f(x))$. $g \circ f\colon X \to Z$.

Nun wollen wir unter den Funktionen solche beschreiben, die gewisse Merkmale treu kopieren:

Definition 1.12. (1) Eine Struktur ist eine nicht leere Menge M zusammen mit Funktionen auf M^n für ein n, Konstanten aus der Trägermenge und Relationen, das sind Teilmengen von M^n. Zum Beispiel $(\mathbb{N}, +, 0, 1, \cdot, <)$. Eine Struktur kann auch von einer oder mehreren Sorten keine Bestandteile haben, zum Beispiel gehört zu einer Gruppe zunächst einmal keine Relation.

(2) Zwei Strukturen heißen isomorph, wenn es eine Isomorphismus zwischen ihnen gibt. Ein Isomorphismus ist eine Bijektion von der einen Trägermenge auf die andere, die alle Strukturmerkmale in beide Richtungen treu abbildet.

(3) Eine Einbettung ist eine Injektion, die alle Strukturmerkmale treu abbildet und die Relationen in beide Richtungen treu erhält.

(4) Ausgelassen Ein Homomorphismus $h\colon (A, f_A, R_A) \to (B, f_B, R_B)$ ist eine Funktion, die mit den Funktionen auf den jeweiligen Stukturen kommutiert, und die die Relationen in die Vorwärtsrichtung erhaelt: Zum Beispiel soll eine dreistellige Funktion homomorph abgebildet werden: $h(f_A(x, y, z)) = f_B(h(x), h(y), h(z))$ Für eine Relation soll gelten $xR_Ay \to f(x)R_Bf(y)$. Beachten Sie, dass hier wirklich nur die Implikation steht. Ende der Aulassung

Nun kehren wir zu unserem Anliegen, weitere Eigenschaften und Beschreibungen von N und $\mathbb{N}$ zu finden, zurück:

In unserem Fall gilt also für jede Möglichkeit von $\mathbb{N}$: Es gibt eine bijektive Abbildung $f\colon N \to \mathbb{N}$, nämlich $f(\underline{n}) = n$. f ist strukturerhaltend, denn $f(\underline{0}) = 0$ und $f(\underline{n+1}) = n + 1 = f(\underline{n}) + 1$.

Nun kommen wir zu einem viel kleineren und schwächeren Axiomensystem als ZFC: den Peano-Axiomen.

Definition 1.13. Sei X eine Menge, $0_X \in X$ und $\sigma_X\colon X \to X$ eine Funktion. Wir sagen $(X, 0_X, \sigma_X)$ erfüllt die Peano-Axiome[8], wenn folgendes gilt

(1) σ_X ist eine Bijektion von X auf $X \setminus \{0_X\}$.

(2) Für alle $M \subseteq X$ gilt: $\big(0_X \in M \wedge \forall y(y \in M \to \sigma_X(y) \in M)\big) \to M = X$.

[8] Giuseppe Peano 1858–1932

Satz 1.14. *Die von Neumann'schen natürlichen Zahlen N mit der leeren Menge und der Nachfolgerfunktion $x \mapsto x \cup \{x\}$ erfüllen die Peano-Axiome.*

Beweis: Wir zeigen das zweite Axiom. Annahme nicht. Sei M ein Gegenbeispiel. Dann ist M induktiv und eine echte Teilmenge von N, im Widerspruch zu $(*)$. □

Bemerkung 1.15. Das zweite Peano-Axiom ist gerade das Prinzip der vollständigen Induktion. d.h., für jedes Modell $(X, 0_X, \sigma_X)$ und jede (definierbare oder nicht definierbare) Eigenschaft gilt: Wenn 0_X die Eigenschaft hat und wenn sich die Eigenschaft auf Nachfolger vererbt, dann haben alle Elemente aus X die Eigenschaft.

Korollar 1.16. *Für die natürlichen Zahlen $(\mathbb{N}, 0, +1)$ gilt das Prinzip der vollständigen Induktion.*

Beweis: $(N, \emptyset,$ Nachfolgerfunktion) ist isomorph to $(\mathbb{N}, 0, +1)$. Isomorphe Strukturen erfüllen dieselben Wahrheiten. Nun folgt das Korollar aus Satz 1.14. □

Wir haben also in den Peano-Axiomen ein Beispiel für ein Axiomensystem, für das man in ZFC ein Modell bauen kann und für das man somit in ZFC einen Widerspruchsfreiheitsbeweis hat.

Frage 1.17. *Gibt es Strukturen, die nicht isomorph zu $(\mathbb{N}, 0, +1)$ sind und trotzdem vollständige Induktion gestatten?*

Ja, die gibt es. Es gibt Induktionen über längere lineare Ordnungen gewisser Art, sogenannte Wohlordnungen. Wir werden im Lauf dieses Semesters ein Beispiel kennenlernen. Der allgemeinste Induktionstyp ist die Induktion über fundierte mengenähnliche Relationen. Dieses können Sie bei Interesse später einmal studieren.

Nun fahren wir weiter mit den natürlichen Zahlen fort:

Satz 1.18. *Satz von der Definition durch Rekursion über $\mathbb{N}$. Sei φ eine Formel oder Rechenvorschrift, die 0 eine Menge $\varphi(0)$ zuordnet und für jedes $n \in \mathbb{N}$ der Ausgangsmenge $\{(0, \varphi(0)), \ldots, (n, \varphi(n))\}$ eine Fortsetzung $\{(0, \varphi(0)), \ldots, (n, \varphi(n)), (n+1, \varphi(n+1))\}$ zuordnet. Dann gibt es genau eine Funktion $f\colon \mathbb{N} \to V$, die der rekursiven Rechenvorschrift genügt und $f(n) = \varphi(n)$ erfüllt.*

Wir erinnern hier an Mathematikgeschichte: Zermelo hat in seiner Arbeit an den Axiomen (etwa von 1900 bis 1908) übersehen, dass man das Ersetzungsschema braucht. Dies fand Fraenkel in den 1920er Jahren (und unabhängig von ihm noch Skolem[9] und Mirimanoff[10]. Zur Veranschaulichung schildern wir ohne Beweise ein Beispiel: Ohne Ersetzungsaxiom kann man das Potenzmengenaxiom nur endlich oft iterieren, und erreicht so nur Mengen gewisser Schachtelungstiefe. Wenn man nun für jedes $n \in \mathbb{N}$ die Potenzmengenbildung (von einer festen Startmenge ausgehend) n Mal iteriert hat, dann möchte man gerne alle n-fachen Gebilde vereinigen. Aber sie sind nicht unbedingt Elemente einer gemeinsamen Menge, es sei denn, man hat das Ersetzungsaxiom.

(Beweisskizze, für später gedacht, wenn Sie schon etwas Erfahrung gesammelt haben.) Im einfacheren Fall, dass man schon eine Zielmenge y kennt, in der alle rekursiv definierten $\varphi(n)$ liegen, ist der Graph von f folgende Menge: $\{(n, u) \in \mathbb{N} \times y \mid \forall g \Big(\big(g(0) = \varphi(0) \wedge \forall m (g \restriction (m+1) = \{(0, \varphi(0)), \ldots, (m, \varphi(n))\} \to g(m+1) = \varphi(m+1))\big) \to g(n) = u \Big)\}$. In diesem Fall braucht man das Ersetzungsaxiom nicht.

[9] Thoralf Albert Skolem, 1887 – 1963
[10] Dmitry Semionovitch Mirimanoff, 1861 – 1945

Im allgemeinen Fall wendet man das Ersetzungsschema auf $\mathbb{N}$ und ψ an, wobei $\psi(n, w)$ sagt: $w = \{(0, \varphi(0)), \ldots, (n, \varphi(n))\}$. Danach ist die Vereinigungsmenge der vom Schema gelieferten Bildmenge eine Obermenge der gesuchten rekursiv definierte Funktion. Aus dieser Obermenge kann man wieder wie oben aussondern. □

Wir schauen uns Beispiele für rekursiv definierte Funktionen an:

Proposition 1.19. *Je zwei Modelle der Peano-Axiome sind isomorph. Wir sagen dazu auch: Die Peano-Axiome haben modulo Isomorphie genau ein Modell. Die Peano Axiome sind kategorisch.*

Beweis: Seien $(\mathbb{N}, 0, +1)$ und $(Y, 0_Y, \sigma_Y)$ zwei Modelle. Wir setzen $f(0) = 0_Y$. $f(n+1) = \sigma_Y(f(n))$. f ist injektiv, da für $m \neq n$, $f(n) \neq f(n)$, wie induktiv über n folgt: Für $n = 0$ ist nichts zu zeigen. Wir zeigen den Schritt von n auf $n+1$: Annahme $f(n+1) = f(m)$ für ein $m \neq m+1$. Dann ist $m > 0$ da $f(0) = 0_Y \neq \sigma_Y(f(n))$. Dann ist $\sigma_Y(f(n)) = \sigma_Y(f(m-1))$. Da σ_Y nach dem ersten Peano-Axiom injektiv ist, folgt $f(n) = f(m-1)$, im Widerspruch zur Induktionsvoraussetzung. Die Funktion f ist wohldefiniert und auf ganz $\mathbb{N}$ definiert nach dem Rekursionsprinzip. f ist surjektiv, da auch bild$(f) \subseteq Y$ induktiv ist. f ist ein Isomorphismus von $(\mathbb{N}, 0, +1)$ auf $(Y, 0_Y, \sigma_Y)$. □

Ab hier nicht gelesen bis zum folgenden Marker.

Definition 1.20. Die rekursive Definition der Addition, der Multiplikation und der Exponentiation auf $\mathbb{N}$. Sei $m \in \mathbb{N}$. m wird als sogenannter Parameter festgehalten. Die Rekursion läuft über n: Wir definieren

$m + 0 = m$,
$m + (n + 1) = (m + n) + 1$.
$m \cdot 0 = 0$,
$m \cdot (n + 1) = m \cdot n + m$.
$m^0 = 1$,
$m^{n+1} = n^m \cdot m$.

Definition 1.21. Eine Menge M heißt endlich, wenn es eine natürliche Zahl n und eine Bijektion f gibt, so dass

$$f\colon \{0, 1, \ldots, n-1\} \to M,$$

Falls $n = 0$, steht auf der linken Seite gerade die leere Menge. n heißt die Mächtigkeit von M, man schreibt $|M| = n$ oder auch $\#(M) = n$.

Definition 1.22. M und X heißen gleichmächtig, wenn es eine Bijektion $f\colon M \to X$ gibt.

Die Gleichmächtigkeit ist eine Äquivalenzrelation (siehe Def. 1.28) auf dem Mengenuniversum mit klassen-vielen klassen-großen Äquivalenzklassen. In einer späteren Vorlesung werden Sie vielleicht lernen: Ein Repräsentantensystem für die Gleichmächtigkeit sind die Kardinalzahlen. Die unendlichen Kardinalzahlen werden auch die Alephs oder ℵ's genannt nach dem ersten Buchstaben des hebräischen Alphabets.

Übung: Sind Teilmengen endlicher Mengen endlich? Gibt es eine „größte" endliche Menge?

Definition 1.23. (Schwache Definition, Dedekind-unendlich[11]) Eine Menge, die nicht endlich ist, heißt unendlich.

[11] Richard Dedekind, 1831–1916

Sie denken vielleicht an alternative, „positivere" Definitionen. Die gibt es in der Tat:

Satz 1.24. ZFC *Die folgenden Aussagen sind äquivalent:*

(1) M *ist nicht endlich.*

(2) Es gibt eine Injektion $f\colon \mathbb{N} \to M$.

(3) Es gibt eine Surjektion $f\colon M \to \mathbb{N}$.

Beweis: (1) impliziert (2). Sei h eine Auswahlfunktion auf $\mathscr{P}(M) \setminus \{\emptyset\}$. (Man kann auch beweisen, dass zu diesem Beweis wirklich ein Teil des Auswahlaxioms gebraucht wird.) Wir definieren rekursiv: Für $n \in \mathbb{N}$: $f(n) = h(M \setminus \{f(i) \mid i < n\})$. f ist injektiv, da für $n > m$, $f(n) \in M \setminus \{f(i) \mid i < n\}$, und insbesondere $f(m)$ in der Menge vorkommt, die abgezogen wird. Wir haben, dass für jedes n die Menge $M \setminus \{f(i) \mid i < n\} \neq \emptyset$ ist, denn andernfalls gäbe es ein n, so dass $f\colon \{0, \ldots, n-1\} \to M$ bijektiv ist. Nach dem Satz über die rekursive Definition $f\colon \mathbb{N} \to M$ wohldefiniert.

(2) impliziert (3): Sei $f\colon \mathbb{N} \to M$ injektiv. Wir definieren $g\colon$ bild(f) $\to \mathbb{N}$ durch $g(f(n)) = n$. Für $y \in M \setminus \text{bild}(f)$ setzen wir $g(y) = 0$. Dann ist $g\colon M \to \mathbb{N}$ surjektiv. Dies gilt allgemein:

Jede Umkehrfunktion ist surjektiv.

(3) $\Rightarrow$ (1): Annahme M ist endlich, und g sei ist eine Bijektion $g\colon \{0, 1, \ldots, n-1\} \to M$. Dann ist $f \circ g\colon \{0, \ldots, n-1\} \to \mathbb{N}$ surjektiv. Jedoch ist $\max\{(f \circ g)(i) \mid i < n\} + 1 \notin \text{bild}(f \circ g)$. Widerspruch. □

Auf den natürlichen Zahlen kann man die Addition die Multiplikation und die Exponentiation statt durch obige Rekursion auch (äquivalent) durch das Ausrechnen von Mächtigkeiten endlicher Mengen definieren:

Proposition 1.25. *Seien* M *und* N *endliche Mengen.* $|m| = m$.
$|M \cup N| = |M| + |N|$, *falls* $M \cap N = \emptyset$.
$|M \times N| = |M| \cdot |N|$.
$|M|^{|N|} = |\{f \mid f\colon N \to M\}|$.

Beweis: Induktiv über $|N|$.

Proposition 1.26. *Für* $(\mathbb{N}, +, \cdot, 0, 1)$ *gelten folgende Rechengesetze:*

(1) Assoziativgesetze
Für ℓ, m, $n \in \mathbb{N}$ *gelten*
$(l + m) + n = (l + m) + n$ *und*
$(lm)n = l(mn)$.

(2) Neutrale Elemente. Für $n \in \mathbb{N}$ *ist*
$n + 0 = 0$
$n \cdot 1 = n$

(3) Kommutativgesetze
$m + n = n + m$,
$m \cdot n = n \cdot m$

(4) Distributivgesetz
$l(m + n) = lm + ln$

(5) *Kürzungsregeln*
$l + m = l + n \to m = n$
$l \cdot n = l \cdot m \to l = 0 \vee n = m$

Beweis: Man zeigt beim Kommutativgesetz erst durch Induktion $n + 1 = 1 + n$. Danach steigt man in die rekursive Definition von $+$ ein. Bei den Kürzungsregeln nimmt man $m \leq n$ an und beweist die Aussage $\forall m \leq n(l + m = l + n \to n = m)$ induktiv über n. Diese Technik ist bei Aussagen mit mehreren Variablen sehr nützlich. □

1.3 Ganze, rationale Zahlen und reelle Zahlen

Wir konstruieren nun $\mathbb{Z}$, so dass wir eine isomorphe Kopie von $(\mathbb{N}, 0, +)$ als Teilstruktur (Substruktur, Unterstruktur) von $(\mathbb{Z}, 0, +)$ wiederfinden. Unser Wunsch ist: $(\mathbb{Z}, 0, +)$ soll eine kommutative Gruppe bilden.

Definition 1.27. (a) Eine Struktur $(G, \circ)$ heißt Gruppe, gdw sie die Gruppenaxiome erfüllt. Diese sind:

(G1) das Assoziativgesetz:
Für all $x, y, z \in G$ gilt $(x \circ y) \circ z = x \circ (y \circ z)$.

(G2) das Gesetz vom neutralen Element e:
Es gibt ein e e ist linksneutral, d.h. Für alle $x \in G$ gilt $e \circ x = x$.

(G3) die Existenz vom Inversen:
Es gibt ein linksneutrales Element e so dass
jedes Element ein Linksinverses bezüglich e hat, d.h. zu jedem $x \in G$ gibt es $y \in G$, so dass $y \circ x = e$.

(b) Eine Struktur $(G, \circ)$ heißt abelsche Gruppe, gdw sie die Gruppenaxiome erfüllt und zusätzlich kommutativ (auch abelsch genannt) ist. D.h., das Kommutativgesetz gilt: Für alle $x, y \in G$ ist $x \circ y = y \circ x$.

Das Gesetz von inversen Element soll also gelten:

$$\forall z \in \mathbb{Z}\ \exists y \in \mathbb{Z}\ z + y = 0.$$

Die Idee ist, $\mathbb{Z}$ als geeigneten Teil von $\mathbb{N} \times \mathbb{N}$ wiederzufinden. Hierzu führen wir das Dividieren durch Äquivalenzrelationen ein, das im Jargon auch „Rechnen modulo ...” oder „faktorisieren” genannt wird.

Definition 1.28. Sei M eine Menge.

(1) R heißt (zweistellige) Relation auf M gdw $R \subseteq M \times M$.

(2) R heißt reflexiv gdw für alle $x \in M$, xRx.

(3) R heißt symmetrisch: Für alle $x, y \in M$ gilt $xRy \to yRx$.

(4) R heißt transitiv für alle $x, y, z \in M$ gilt: $(xRy \wedge yRz \to xRz)$.

(5) R heißt Äquivalenzrelation auf M gdw R reflexiv, symmetrisch und transitiv ist.

Definition 1.29. Sei R eine Äquivalenzrelation auf M und $x \in M$.

(1) Die folgende Teilmenge von M

$$[x]_R := \{y \in M \mid xRy\}$$

heißt die Äquivalenzklasse von x.

(2) Wir nennen M/R die Quotientenmenge.

$$M/R := \{[x]_R \mid x \in M\}$$

Bem.: $M/R \subseteq \mathscr{P}(M)$.

(3) $p\colon M \to M/R$ mit $p(x) = [x]_R$ heißt die Quotientenabbildung.

Frage 1.30. *Hat die Quotientenabbildung eine Umkehrung?*

Wir suchen eine Teilmenge $S \subseteq M$, so dass die Einschränkung von p auf S, geschrieben $p \restriction S$, injektiv ist. Solch eine Teilmenge heißt Repräsentantensystem für M und R. Wir geben eine äquivalente Definition:

Definition 1.31. $S \subseteq M$ heißt Repräsentantensystem für R auf M gdw

$$\forall y \in M/R\ \exists^{=1} x \in S\ x \in y$$

S ist als gerade die Bildmenge der Auswahlfunktion

$$\{(y, S(y)) \mid y \in M/R\}.$$

Nach dem Auswahlaxiom existiert eine Auswahlfunktion und somit ein Repräsentantensystem. In der Tat gilt:

Satz 1.32. *In* ZF *gilt: Das Auswahlaxiom ist wahr genau dann, wenn jede Äquivalenzrelation ein Repräsenantensystem hat.*

Beweis: Die eine Richtung haben wir gerade eben gezeigt. Habe nun also jede Äquivalenzrelation ein Repräsenantensystem. Sei eine Menge X nicht leerer Mengen gegeben. Wir betrachten nun

$$\hat{X} = \{\{x\} \times x \mid x \in X\}.$$

Dann ist $\hat{X}$ eine Menge disjunkter nicht leerer Mengen. Wir definieren eine Äquivalenzrelation R auf $\bigcup \hat{X}$ durch

$$(x, u)R(y, v) :\text{gdw } x = y.$$

Sei S ein Repräsentantensystem für R auf $\bigcup \hat{X}$. Dann ist S gerade eine Auswahlfunktion für X. □

Übung 1.33. Lösen Sie nun die Schlumpfaufgabe auf Seite 26 des Ersti-Heftes $\sqrt{-1}$ vom Oktober 2013. Jetzt können Sie die Schlümpfe sicherlich beraten, für welche Äquivalenzrelation sie sich bei ihrer Strategiebesprechung ein Repräsentantensystem aussuchen sollten.

Der folgende Satz beschreibt einige für die Algebra wichtige Eigenschaften von Quotienten.

Proposition 1.34. *es sei R eine Äquivalenzrelation auf M.*

(1) $y \in [x]_R$ *gdw* yRx.

(2) Die Quotientenabbbildung p *is surjektiv. Es gilt* $p(x) = p(y)$ *gdw* xRy.

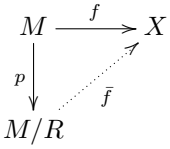
(3) Es sei X *eine Menge. Sei* $f\colon M \to X$ *eine Funktion. Dann sind äquivalent*

(a) $\forall x, y \in M(xRy \to f(x) = f(y))$. *(Man sagt dazu: „*$f$ *hängt nur von der Äquivalenzklasse ab" oder* f *ist unabhängig von den Repräsentanten)*

(b) Es gibt die von f *und* R *induzierte Abbildung* $\bar{f}\colon M/R \to X$, *so dass*

$$\forall x \in M\ \bar{f}(p(x)) = \bar{f}([x]_R) = f(x).$$

Man schreibt die Eigenschaft (3) (b) auch gerne in einem Diagramm



Beweis: (1) und (2) sind klar. (3): Die Implikation von (b) nach (a) ist einfach.

Wir zeigen die Implikation von (a) nach (b): Zuerst geben wir einen dummen Beweis, der mit Kanonen auf Spatzen schießt: Wir definieren $\bar{f}$. Sei hierzu S eine Auswahlfunktion für M und R. Wir setzen für $y \in M/R$,

$$\bar{f}(y) = f(S(y)).$$

Falls $y = p(x)$, so haben wir $\bar{f}(p(x)) = f(S(p(x))) = f(x)$, obwohl im Allgemeinen $S(p(x)) \neq x$ und nur $S(p(x))Rx$. Aber letzteres reicht ja aus, da f unabhängig von den Repräsentanten ist.

Nun geben wir einen Beweis, der das Auswahlaxiom nicht braucht: Wir setzen für $y \in M/R$,

$$\bar{f}(y) = \bigcup\{f(z) \mid z \in y\}.$$

Die Menge $\{f(z) \mid z \in y\}$ hat nur ein Element. Es gilt immer $\bigcup\{u\} = u$. Sei nun $y = p(x) = x/R$. Dann ist $x \in y$, und daher kommt $f(x)$ in der Menge $\{f(z) \mid z \in y\}$ als Element vor. Da diese Menge eine Einermenge ist, haben wir $\{f(z) \mid z \in y\} = \{f(x)\}$. Dann ist $\bigcup\{f(z) \mid z \in y\} = f(x)$, wie gewünscht. □

Man sagt „$\bar{f}$ is wohldefiniert", wenn Eigenschaft (3)(a) vorliegt.

Bei der Definition von $+$ und $\cdot$ auf $\mathbb{Z}$ werden wir Wohldefiniertheit auch für Funktionen $\bar{f}\colon M/R \times M/R \to X$ und für Relationen $<\subseteq M/R \times M/R$ benutzen. Proposition 1.34 gilt sinngemäß auch für diese: Im Kriterium (3)(a) wird man nun für beide Argumente unabhängig voneinander Unabhängigkeit von den Repräsentanten voraussetzen.

Definition 1.35. und Behauptung. (Die ganzen Zahlen)

(1) Wir definieren eine Relation R auf $\mathbb{N} \times \mathbb{N}$, d.h. $R \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ wie folgt

$$(m, n)R(p, q) \text{ :gdw } m + q = p + n.$$

(2) Wir setzen

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R$$

(3) Wir definieren die Addition auf $\mathbb{Z}$:

$$[(m,n)]_R + [(p,q)]_R = [(m+p, n+q)]_R.$$

Überlegen Sie sich, ob dies wohldefiniert ist.

(4) Wir definieren die Multiplikation auf $\mathbb{Z}$ durch

$$[(m,n)]_R \cdot [(p,q)]_R = [(mp+nq, mq+np)]_R.$$

(5) Wir definieren das additive Inverse $-[(m,n)]_R$ als

$$-[(m,n)]_R = [(n,m)]_R.$$

(6) Wir definieren die lineare Ordnung $<$ auf $\mathbb{Z}$ durch

$$[(m,n)]_R < [(p,q)]_R \text{ :gdw } m+p <_{\mathbb{N}} n+q.$$

Auch dies ist wohldefiniert: Wieder weist man nach, dass die Definition nicht von den Repräsentanten abhängt.

Überlegen Sie sich: In Übereinstimmung mit Proposition 1.34 müssten wir in (3) bis (6) nun $\bar{+}, \bar{\cdot}, \bar{<}$ auf der linken Seite schreiben. Wir schenken uns die Oberstriche.

Beweis: Wir beweisen (4), da es am kompliziertesten aussieht. Sei

$$(m', n')R(m,n).$$

Das heißt

$$m' + n = m + n'.$$

Wir sollen zeigen

$$(mp+nq, mq+np)R(m'p+n'q, m'q+n'p),$$

d.h.

$$mp + nq + m'q + n'p = m'p + n'q + mq + np.$$

Nach dem Distributivgesetz und das Kommutativgesetz ist die linke Seite $(m+n')p+(n+m')q$. Nun setzt man hierin $m+n' = m'+n$ ein, tauscht also beide Vorfaktoren aus. Dann hat man nach einer weiteren Anwendung des Distributivgesetzes gerade die rechte Seite. Danach ersetzt man (p,q) durch ein äquivalentes (p',q') und zeigt mit der analogen Technik, dass

$$(m'p+n'q, m'q+n'p)R(m'p'+n'q', m'q'+n'p').$$

Führte man beide Ersetzungen geichzeitig durch, geriete man in längere Arbeit mit dem Umordnen von Termen und Hinzufügen geeigneter Summanden. □

Definition 1.36. Eine Gruppe $(G, 0, \circ, <)$ heißt angeordnete Gruppe, wenn die Kürzungsregel gilt: $a < b \leftrightarrow a \circ c < b \circ c$.

Definition 1.37. Ein Ring $(R, +, \cdot, 0, 1, <)$ heißt angeordneter Ring, wenn $(R, +\cdot, 0, 1)$ ein Ring ist und wenn $(R, +, <)$ eine angeordnete Gruppe ist und wenn auch für $\cdot$ die Kürzungsregel gilt: $c > 0 \to (a < b \leftrightarrow ac < bc)$.

Definition 1.38. Ein angeordneter Ring $(R, +, \cdot, 0, 1, <)$ heißt archimedisch oder archimedisch angeordnet, gdw es eine Einbettung $i\colon (\mathbb{N}, +, \cdot, 0, 1, <) \to (R, +, \cdot, 0, 1, <$) gibt, so dass $i[\mathbb{N}]$ konfinal in $(R, <)$ liegt, d.h. $\forall r \in R \exists n \in \mathbb{N} r \leq i(n)$.

Nun rechnet man nach:

Proposition 1.39. *(1)* $i(n) = [(n, 0)]_R$ *ist eine Einbettung von* $(\mathbb{N}, +, 0)$ *in* $(\mathbb{Z}, +, [(0, 0)]_R)$.

(2) $(\mathbb{Z}, +, [(0, 0)]_R)$ *ist eine abelsche Gruppe.*

(3) $(\mathbb{Z}, +, \cdot, (20, 20)/R, [(21, 20)]_R, <)$ *ist ein kommutativer archimedisch angeordneter Ring mit Eins.*

Definition 1.40. und Behauptung. (Die rationalen Zahlen)

(1) Wir definieren eine Relation E auf $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$, d.h. $R \subseteq (\mathbb{Z} \times (\mathbb{N} \setminus \{0\})) \times (\mathbb{Z} \times (\mathbb{N} \setminus \{0\}))$ wie folgt

$$(m, n)E(p, q) \text{ :gdw } m \cdot q = p \cdot n.$$

(2) Wir setzen

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{N} \setminus \{0\}))/E$$

(3) Wir definieren die Addition auf $\mathbb{Q}$:

$$[(m, n)]_E + [(p, q)]_E = [(mq + pn, nq)]_E.$$

Überlegen Sie sich, ob dies wohldefiniert ist.

(4) Wir definieren die Multiplikation auf $\mathbb{Q}$ durch

$$[(m, n)]_E \cdot [(p, q)]_E = [(mp, qn)]_E.$$

(5) Wir definieren für $m \neq 0$ das multiplikative Inverse $([(m, n)]_E)^{-1}$ als

$$([(m, n)]_E)^{-1} := \begin{cases} [(n, m)]_E, & \text{wenn } m > 0, \\ [(-n, -m)]_E, & \text{wenn } m < 0. \end{cases}$$

(6) Wir setzen $0_{\mathbb{Q}} = [(0, 1000)]_E$, $1_{\mathbb{Q}} = [(17, 17)]_E$.

(7) Wir definieren die lineare Ordnung $<$ auf $\mathbb{Q}$ durch

$$[(m, n)]_E < [(p, q)]_E \text{ :gdw } mq <_{\mathbb{N}} pn.$$

Auch dies ist wohldefiniert: Wieder weist man nach, dass die Definition nicht von den Repräsentanten abhängt.

Beweis: Wir beweisen (3), da es am kompliziertesten aussieht. Sei

$$(m', n')E(m, n).$$

Das heißt

$$m' \cdot n = m \cdot n'.$$

Wir sollen zeigen

$$(mq + np, nq)E(m'q + n'p, n'q),$$

d.h.

$$(mq + np)n'q = (m'q + n'p)nq.$$

Nach dem Distributivgesetz und das Kommutativgesetz ist die linke Seite $mqn'p + npn'q$. Nun setzt man hierin $m \cdot n' = m' \cdot n$ ein, tauscht also den ersten Vorfaktor aus. Dann ist die linke Seite also $m'qnp + npn'q$. Die rechte Seite ist $m'qnp + n'pnq$ nach dem Distributivgesetz, stimmt also mit der linken Seite überein. Danach ersetzt man (p, q) durch ein äquivalentes (p', q') und zeigt mit der analogen Technik, dass

$$(m'q + n'p, n'q)E(m'q' + n'p', n'q').$$

□

Definition 1.41. Eine lineare Ordnung heißt *dicht*, gdw $\forall x < z \exists y(x < y < z)$.

Nun rechnet man (Skeptiker müssen viel rechnen) nach:

Proposition 1.42. *(1)* $i(z) = (z, 1)/E$ *ist eine Einbettung von* $(\mathbb{Z}, +, \cdot, 0, 1, <)$ *in* $(\mathbb{Q}, +\cdot, 0_{\mathbb{Q}}, 1_{\mathbb{Q}}, <)$.

(2) $(\mathbb{Q}, +, \cdot, 0_{\mathbb{Q}}, 1_{\mathbb{Q}}, <)$ *ist ein archimedisch angeordneter Körper mit einer dichten linearen Ordnung.*

Definition 1.43. Wir definieren die Betragsfunktion auf $\mathbb{Q}$, durch

$$|q| = \begin{cases} q, & \text{wenn } q \geq 0, \\ -q, & \text{wenn } q < 0. \end{cases}$$

Erinnern Sie sich an die Cauchyfolgen.

Definition 1.44. Eine Funktion $f\colon \mathbb{N} \to \mathbb{Q}$ heißt Cauchyfolge (mit rationalen Einträgen)[12] oder Cauchyfolge in $\mathbb{Q}$, wenn

$$\forall \varepsilon > 0 \; \exists n_0 \; \forall m, m' \geq n_0 \; |f(m) - f(m')| < \varepsilon. \tag{1.1}$$

Mit „Cauchyfolge" meint man meistens eine reellwertige Cauchyfolge, d.h. eine Funktion $f\colon \mathbb{N} \to \mathbb{R}$ (siehe unten), für die wiederum (1.1) gilt.

Definition 1.45. und Behauptung. (Die reellen Zahlen)

(1) Wir definieren eine Relation eq auf $\{f \mid f\colon \mathbb{N} \to \mathbb{Q}, f \text{ Cauchyfolge}\} \subseteq \mathscr{P}(\mathbb{N} \times \mathbb{Q})$ wie folgt

$$f \text{ eq } g \text{ :gdw } \lim_{n \to \infty} |f(n) - g(n)| = 0.$$

Dies ist eine Äquivalenzrelation.

(2) Wir setzen

$$\mathbb{R} = \{f \mid f\colon \mathbb{N} \to \mathbb{Q}, f \text{ Cauchyfolge}\}/\text{eq}$$

(3) Wir definieren die Addition auf $\mathbb{R}$:

$$[f]_{\text{eq}} + [g]_{\text{eq}} = [(f + g)]_{\text{eq}}.$$

Hier ist für $n \in \mathbb{N}$, $(f + g)(n) = f(n) + g(n)$. Überlegen Sie sich, ob die Addition wohldefiniert ist.

(4) Wir definieren die Multiplikation auf $\mathbb{R}$ durch

$$[f]_{\text{eq}} \cdot [g]_{\text{eq}} = [(f \cdot g)]_{\text{eq}}.$$

Hier ist für $n \in \mathbb{N}$, $(f \cdot g)(n) = f(n) \cdot g(n)$. Überlegen Sie sich, ob die Multiplikation wohldefiniert ist.

[12] Augustin-Louis Cauchy, 1789–1857

(5) $0_{\mathbb{R}}$ sei die eq-Klasse einer Funktion mit $\lim_{n\to\infty} f(n) = 0_{\mathbb{Q}}$. $1_{\mathbb{R}}$ sei die eq-Klasse irgendeiner Funktion mit $\lim_{n\to\infty} f(n) = 1_{\mathbb{Q}}$.

(6) Wir definieren die lineare Ordnung $<$ auf $\mathbb{R}$ durch

$$[f]_{\text{eq}} \leq [g]_{\text{eq}} :\text{gdw } \lim_{n\to\infty} g(n) - f(n) \geq 0.$$

Auch dies ist wohldefiniert: Wieder weist man nach, dass die Definition nicht von den Repräsentanten abhängt.

(7) Wir definieren $|[f]_{\text{eq}}| := [(n \mapsto |f(n)|)]_{\text{eq}}$. Durch diese Setzung wird die Betragsfunktion von $i[\mathbb{Q}](= i(\mathbb{Q}))$ auf $\mathbb{R}$ erweitert.

Nun kommt ein sehr schöner Satz, im Original von Cantor[13].

Satz 1.46. *(1) $i(q) = [c_q]_{\text{eq}}$ mit $c_q(n) = q$ für $n \in \mathbb{N}$ ist eine Einbettung von $(\mathbb{Q}, +, \cdot, 0_{\mathbb{Q}}, 1_{\mathbb{Q}}, <)$ in $(\mathbb{R}, +, \cdot, 0_{\mathbb{R}}, 1_{\mathbb{R}}, <)$.*

(2) $(\mathbb{R}, +, \cdot, 0_{\mathbb{R}}, 1_{\mathbb{R}}, <)$ ist ein vollständiger archimedisch geordneter Körper.

Beweis: Wir beweisen die meiner Meinung nach schwierigste Aussage:

Lemma 1.47. *In $\mathbb{R}$ hat jede Cauchyfolge einen Grenzwert.*

Beweis: Sei $(r_n)_{n\in\mathbb{N}}$ eine Cauchyfolge, und sei $r_n = [f_n]_{\text{eq}}$, f_n eine Cauchyfolge mit rationalen Einträgen.

Dann gilt, da $(r_n)_n$ eine Cauchyfolge ist:

$$\forall \varepsilon > 0 \exists n_0 = n_0(\varepsilon) \forall m, m' \geq n_0(\varepsilon) \lim_{k\to\infty} |f_m(k) - f_{m'}(k)| < \varepsilon. \tag{1.2}$$

Dies heißt ausgeschrieben

$$\forall \varepsilon > 0 \exists n_0 = n_0(\varepsilon) \forall m, m' \geq n_0 \forall \varepsilon_1 > 0$$
$$\exists k_{\text{riesig}}(\varepsilon, m, m', \varepsilon_1) \forall k \geq k_{\text{riesig}}(\varepsilon, m, m', \varepsilon_1) |f_m(k) - f_{m'}(k)| < \varepsilon + \varepsilon_1.$$

Außerdem ist jedes f_u eine Cauchyfolge, daher gilt für jedes u:

$$\forall \varepsilon > 0 \exists k_0 = k_0(\varepsilon, u) \forall m, m' \geq k_0(\varepsilon, u) |f_u(m') - f_u(m)| < \varepsilon. \tag{1.3}$$

Wir definieren nun eine (schnell wachsende) Funktion $g\colon \mathbb{N} \to \mathbb{N}$ wie folgt.

Gegeben n nehmen wir $g(n)$, so dass

$$\forall m, m' \geq g(n)\ \forall k \leq n\ |f_k(m) - f_k(m')| \leq \frac{1}{n}. \tag{1.4}$$

Überlegen Sie sich, dass es so ein g tatsächlich gibt: Wir nutzen zum Finden von $g(n)$ endlich oft die Voraussetzung (1.3). Wir setzen nun

$$f_{\text{diag}}(n) := f_n(g(n)).$$

Man nennt solche Definitionen, die aus einer Folge von Folgen durch Einsetzung eines Arguments einmal als Index und einmal als Argument eine quer darüberlaufende Folge bilden, Diagonalisierungen. Diagonalisierung ist ein wichtiger Kunstgriff in vielen Gebieten der Mathematik. Auch in (1.4) haben wir n schon an zwei verschiedenen Stellen eingesetzt.

Wir behaupten

[13] Georg Cantor, 1845 – 1918

(a) f_{diag} ist eine Cauchyfolge und

(b)

$$\lim_{n\to\infty} r_n = [f_{\text{diag}}]_{\text{eq}}.$$

Wir zeigen zuerst (a). Sei $\varepsilon > 0$ gegeben. Wir nehmen n_0, so dass $\varepsilon < \frac{1}{3\cdot n_0}$ und für $m, m' \geq n_0, |r_m - r_{m'}| < \frac{\varepsilon}{6}$. Dann ist für $m, m' \geq n_0$,

$$\begin{aligned}
&f_{\text{diag}}(m) - f_{\text{diag}}(m') = \\
&f_m(g(m)) - g_{m'}(g(m')) = \\
&(f_m(g(m)) - f_m(k)) + (f_m(k) - f_{m'}(k)) + (f_{m'}(k) - f_{m'}(g(m'))).
\end{aligned}$$

Jeder Summand hat Betrag $< \frac{\varepsilon}{3}$, wenn wir $k \geq \max(g(m), g(m'))$ so groß wählen, dass $|f_m(k) - f_{m'}(k)| < |r_m - r_{m'}| + \frac{\varepsilon}{6} < \frac{\varepsilon}{6} + \frac{\varepsilon}{6}$. Solch ein k gibt es, da $r_m = [f_m]_{\text{eq}}$ und $r_{m'} = [f_{m'}]_{\text{eq}}$.

Nun zeigen wir (b). Wir haben zu zeigen:

$$\forall \varepsilon > 0 \exists n_0 \forall m \geq n_0 \lim_{k\to\infty} |f_m(k) - f_{\text{diag}}(k)| < \varepsilon.$$

Dies bedeutet ausgeschrieben:

$$\begin{aligned}
&\forall \varepsilon > 0 \exists n_0 = n_0(\varepsilon) \forall m \geq n_0 \forall \varepsilon_1 > 0 \exists k_0(\varepsilon, m, \varepsilon_1) = k_0 \\
&\forall k \geq k_0 |f_m(k) - f_{\text{diag}}(k)| < \varepsilon + \varepsilon_1.
\end{aligned} \tag{1.5}$$

Gegeben ε, wir nehmen n_0 wie $n_0(\varepsilon)$ in (1.2).
Damit erhalten wir

$$\forall m, m' \geq n_0 \lim_{k\to\infty} |f_m(k) - f_{m'}(k)| < \varepsilon.$$

Letzteres heißt ausgeschrieben:

$$\forall m, m' \geq n_0 \forall \varepsilon_1 > 0 \exists k_0 \forall k \geq k_0 |f_m(k) - f_{m'}(k)| < \varepsilon + \varepsilon_1. \tag{1.6}$$

Gegeben m und ε_1 nehmen wir nun $k_0(\varepsilon, m, \frac{\varepsilon_1}{3}) \geq \max(n_0, \frac{3}{\varepsilon_1})$ als k_0 zur Cauchyfolge $(f_m(u))_{u\in\mathbb{N}}$ wie in (1.3). Damit erhalten wir

$$\forall k, k' \geq k_0 |f_m(k') - f_m(k)| < \frac{\varepsilon_1}{3} \tag{1.7}$$

Dann haben wir für jedes $k \geq k_0 \geq n_0$ eine Zahl $k_{\text{riesig}}(\varepsilon, k, m, \varepsilon_1) \geq \max(k, g(k))$ zur Cauchyfolge $|f_m - f_k|$ wie in (1.6) zu $\varepsilon + \frac{\varepsilon_1}{3}$.

Nun haben wir nach unseren Vorgehen
ε gegeben,
$n_0 = n_0(\varepsilon)$ gewählt,
$m \geq n_0$, ε_1 gegeben,
$k_0 = k_0(\varepsilon, m, \frac{\varepsilon_1}{3})$ gewählt,
$k \geq k_0$ gegeben,
$k_{\text{riesig}} = k_{\text{riesig}}(\varepsilon, k, m, \frac{\varepsilon_1}{3})$ gewählt. Wir rechnen nun:

$$\begin{aligned}
&f_m(k) - f_{\text{diag}}(k) = f_m(k) - f_m(k_{\text{riesig}}) + f_m(k_{\text{riesig}}) - \\
&f_k(k_{\text{riesig}}) + f_k(k_{\text{riesig}}) - f_k(g(k)).
\end{aligned}$$

Nach der Dreieicksungleichung und nach nach (1.7), (1.6) und (1.4) (jeweils zur Abschätzung der drei Summanden) ergibt sich

$$|f_m(k) - f_{\text{diag}}(k)| \leq$$
$$|f_m(k) - f_m(k_{\text{riesig}})| + |f_m(k_{\text{riesig}}) - f_k(k_{\text{riesig}})| + |f_k(k_{\text{riesig}}) - f_k(g(k))| <$$
$$\frac{\varepsilon_1}{3} + \varepsilon + \frac{\varepsilon_1}{3} + \frac{\varepsilon_1}{3} \leq \varepsilon + \varepsilon_1.$$

Damit haben wir die Behauptung (1.5) mit ihrer recht komplexen Schachtelung der Quantoren gezeigt. In (1.5) kommt k_{riesig} nicht vor, die Vorgabe k hingegen schon. Die Zahl k_{riesig} haben wir nur als Hilfsmittel benutzt. □

Proposition 1.48. *In $\mathbb{R}$ gilt für Cauchyfolgen mit rationalen Einträgen: $[f]_{\text{eq}} = \lim_{n\to\infty} i(f(n))$. Hierbei ist $i\colon \mathbb{Q} \to \mathbb{R}$ die in Aussage (1) des Satzes genannte Einbettung.*

Beweis: Übung.

Übung 1.49. 1. Basteln Sie für $n \in \mathbb{N}$ jeweils eine rationalwertige Cauchyfolge $(f_n(k))_{k\in\mathbb{N}}$, so dass $([f_n]_{\text{eq}})$ eine Cauchyfolge in $\mathbb{R}$ ist und so dass $(f_n(n))_{n\in\mathbb{N}}$ keine Cauchyfolge ist.

2. Vielleicht könnte man sich im Beweis gerade eben auf Cauchyfolgen mit gewisser schneller Konvergenzrate beschränken und den Beweis so hoffentlich vereinfachen. Wir dürfen uns ja beliebige Repräsentanten für die f_n mit $r_n = [f_n]_{\text{eq}}$ auswählen. So kann man, nach Vorbereitung, zu $g(n) = n$ kommen. Überlegen Sie sich, wie man das genau durchführen kann.

3. Jemand möchte gerne noch mehr reelle Zahlen haben und faktorisiert daher bei der Konstruktion von $\mathbb{R}$ nicht nach eq. Kann man dann noch rechnen? Was passiert mit der Archimedizität? Wenn Sie diese Frage interessiert, können Sie sich über Nichtstandard-Analysis informieren.

Korollar 1.50. *(*ZF *beweist:) Das Axiomensystem* KAV *für die vollständigen archimedisch geordneten Körper ist hat ein Modell, ist also widerspruchsfrei.*

Satz 1.51. KAV *hat bis auf in beide Richtungen stetige Isomorphismen genau ein Modell. Man sagt dazu: Das Axiomensystem* KAV *ist kategorisch.*

Beweis: Seien $(\mathbb{R}, +, \cdot, 0, 1, <)$ und $(S, +_s, \cdot_S, 0_S, 1_S, <_S)$ zwei vollständige archimedisch angeordnete Körper. Wir geben einen Isomorphismus $f\colon \mathbb{R} \to S$ an. Wir vereinfachen die Schreibweise für $\mathbb{R}$, und nehmen an, dass $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ nicht nur in $\mathbb{R}$ eingebettet sind, sondern Teilmengen sind. Wir setzen $f(0) = 0_S$, $f(n+1) = f(n)+_S 1_S$, $f(-n) = -_S f(n)$, $f(\frac{p}{q}) = \frac{f(p)}{f(q)}$. Hier ist auf de rechten Seite der Bruch in S und $\cdot_S$ ausgerechnet gemeint. Dann haben wir f schon auf $\mathbb{Q}$ definiert. Nun setzen wir f auf eindeutige Weise stetig fort, indem wir zu $r \in \mathbb{R}$ eine Cauchyfolge mit rationalen Einträgen wählen (wir brauchen nach dem Beweis von Prop. 1.34 das Auswahlaxiom nicht), sagen wir $(q_n)_n$. Dann setzen wir $f(r) = \lim_n f(q_n)$, hier wird der Limes in S gebildet. f ist surjektiv, da auch S ein vollständig archimedisch angeordneter Körper ist. Auch die Umkehrabbildung von f ist stetig.

f kommutiert mit $+$ und $\cdot$ nach Konstruktion: $f(r + r') = f(r) +_S f(r')$. Dies zeigt man wieder von den rationalen Zahlen ausgehend. Ebenso zeigt man, dass f die lineare Ordnung von $\mathbb{R}$ treu auf die lineare Ordnung von S abbildet. □

Ab hier wieder gelesen

Kapitel 2

Vektorräume

Ab hier ist das meiste aus den sehr guten Skripten von Herrn Bangert [2] und Herrn Ziegler [17] abgeschrieben. An etlichen Stellen flossen auch folgende Quellen ein: [1], [4], [5], [7], [8], [9] [10], [11].

Ab hier etliche Beweise, besonders die leichteren, noch nicht getext.

2.1 Einstieg: Lineare Gleichungssysteme

Beispiele: eine Gleichung mit einer Unbekannten, eine Gleichung mit zwei Unbekannten, zwei Gleichungen mit 2 Unbekannten

Geometrische Interpretation

Definition 2.1. Sei K ein Körper. Seien $m, n \in \mathbb{N} \setminus \{0\}$, $a_{i,j}, b_i \in \mathbb{R}$ für $i = 1, \ldots, m, j = 1, \ldots, n$. Eine Konjunktion der Form

$$\text{Für } i = 1, \ldots, m \quad \sum_{j=1}^{n} a_{i,j} \cdot x_j = b_i \tag{I}$$

heißt lineares Gleichungssystem mit m Gleichungen in n Unbekannten.

Definition 2.2. (Zeilen-)Stufenform für ein lineares Gleichungssystem über einem Körper K mit n Unbekannten und m Zeilen. Eine Anordnung der Form

$$\begin{array}{cccccccccccccc}
0 & \cdots & 0 & a_{1,j_1} & * & \ldots & * & * & * & \ldots & * & * & * & \cdots & a_{1,n} & b_1 \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_{2,j_2} & * & \ldots & * & * & * & \cdots & a_{2,n} & b_2 \\
\vdots & & & & & & & & & & & & & & & \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \ldots & 0 & a_{k,j_k} & * & \cdots & a_{k,n} & b_k \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \cdots & 0 & b_{k+1} \\
\vdots & & & & & & & & & & & & & & & \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \cdots & 0 & b_m
\end{array}$$

heißt Stufenform oder auch Zeilenstufenform (der Koeffizienten) eines linearen Gleichungssystems. Hierbei ist für $i = 1, \ldots, k$, $a_{i,j_i} \neq 0$, und die Sterne stehen für beliebige Elemente von K. Die Zahl $k \leq m, n$ heißt der Rang des linearen Gleichungssystems.

Definition 2.3. Ein Lineares Gleichungssystem heißt homogen, wenn $b_1 = \cdots = b_m = 0$.

Definition 2.4. Sei $r \in R$. Wir definieren $G_2 - rG_1$ für zwei lineare Gleichungen G_i der Form $\sum_{j=1}^{n} a_{i,j}x_j = b_i$, $i = 1, 2$, als $\sum_{j=1}^{n}(a_{2,j} - ra_{1,j})x_j = b_2 - rb_1$.

Definition 2.5. $L_I = \{(x_1, \ldots, x_n) \,|\, (x_1, \ldots, x_n) \text{ löst I}\}$

Lemma 2.6. *Aus G_1 und G_2 folgen $G_2 - rG_1$ und G_1. Aus $G_2 - rG_1$ und G_1 folgem G_1 und G_2.*

Ein Einzelschritt im Gauß-Verfahren: Sei I mit den Gleichungen $I_1, \ldots, I_m$ gegeben. Sei $a_{1,1} \neq 0$. Dann bilden wir I' mit $I'_1 = I_1$, $I'_i = I_i - \frac{a_{i,1}}{a_{1,1}}I_1$. Dann gilt $L_I = L_{I'}$.

Die Beschreibung des Gauß-Algorithmus[1] [2].

Satz 2.7. *Jedes lineare Gleichungssystem lässt sich in ein Gleichungssystem in Stufenform umwandeln, das dieselbe Lösungsmenge hat (zwei solche lineare Gleichungssysteme nennt man äquivalent).*

2.2 Relationen

Definition 2.8. Seien M, N Mengen. $R \subseteq M \times N$ heißt Relation auf (M, N). Falls $M = N$, so sagt man Relation auf M. Wir schreiben auch xRy für $(x, y) \in R$

Beispiel 2.9. Sei $f\colon M \to N$ eine Funktion. Dann ist $\text{graph}(f) = \{(x, y) \in M \times N \,|\, f(x) = y\}$ eine Relation. $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x = y^2\}$.

Definition 2.10. Sei R eine Relation auf M.

(1) R heißt reflexiv :gdw $\forall x xRx$.

(2) symmetrisch :gdw $\forall x, y \in M(xRy \to yRx)$.

(3) transitiv :gdw $\forall x, y, z \in M(xRy \wedge yRz \to xRz)$.

(4) Äquivalenzrelation :gdw R is reflexiv symmetrisch und transitiv.

(5) antisymmetrisch :gdw $\forall x, y \in M(xRy \wedge yRx \to x = y)$.

(6) Halbordnung :gdw R antisymmetrisch, reflexiv und transitiv ist.

(7) lineare Ordnung :gdw R eine Halbordnung ist, die konnex ist, d.h. $\forall x, y(xRy \vee yRx \vee x = y)$.

Beispiel 2.11. $C = \{f\colon \mathbb{N} \to \{0, 1\}\}$ heißt die Cantormenge. $R = \{(f, g) \in C \times C \,|\, \exists k \forall n \geq k f(n) = g(n)\}$ ist eine Äquivalenzrelation auf C.

Definition 2.12. Sei R eine Äquivalenzrelation auf M, $x \in M$.

(1) $[x]_R = \{y \,|\, xRy\}$ heißt die Äquivalenzklasse von x.

2) $M/R = \{x_R \,|\, x \in M\}$ heißt die Quotientenmenge .

(3) $S \subseteq M$ heißt Repräsentantensystem für R: $\forall x \in M/R \exists^{=1} y \in Sy \in x$.

Satz 2.13. ZFC. *Jede Äquivalenzrelation hat ein Repräsentantensystem.*

Definition 2.14. Seien p, $m \in \mathbb{Z}$.

(1) p teilt $m :\Leftrightarrow \exists z \in \mathbb{Z} p \cdot z = m$. Wir schreiben $p \mid m$ für p teilt m .

[1] Carl Friedrich Gauß, 1777 - 1855

[2] Abu Dscha'far Muhammad ibn Musa al Chwarizmi, 770 - (835-850)

(2) $m \equiv n \mod (p) :\Leftrightarrow p \mid m - n$.

(3) $[x]_p = \{y \mid y \equiv x \mod (p)\}$.

(4) $\mathbb{Z}_p = \{[x]_p \mid x \in \mathbb{Z}\}$.

Definition 2.15. $\mathcal{Z} \subseteq \mathscr{P}(M)$ heißt Zerlegung oder Partition von M :gdw $\bigcup \mathcal{Z} = M$, $\emptyset \notin \mathcal{Z}$, und $\forall Z, Z' \in \mathcal{Z} Z \cap Z' = \emptyset$.

Satz 2.16. *Sei M eine Menge. Korrespondenz von Zerlegungen von M und Äquivalenzrelationen auf M. Es gibt*

$$F\colon \{\mathcal{Z} \mid \mathcal{Z} \text{ Zerlegung auf } M\} \to \{R \mid R \text{ Äquivalenzrelation auf } M\}$$

und

$$G\colon \{R \mid R \text{ Äquivalenzrelation auf } M\} \to \{\mathcal{Z} \mid \mathcal{Z} \text{ Zerlegung auf } M\},$$

so dass für alle R und $\mathcal{Z}$, $F(G(R)) = R$ und $G(F(\mathcal{Z})) = \mathcal{Z}$.

Beweis: $xF(\mathcal{Z})y \Leftrightarrow \exists Z \in \mathcal{Z} x, y \in Z.\ G(R) = M/R$. □

2.3 Gruppen

Wir beginnen mit einem schwachen Axiomensystem für Gruppen:

Definition 2.17. (a) Eine Struktur $(G, \circ)$ heißt Gruppe, gdw sie die Gruppenaxiome erfüllt. Diese sind:

(G1) das Assoziativgesetz:
Für all $x, y, z \in G$ gilt $(x \circ y) \circ z = x \circ (y \circ z)$.

(G2) das Gesetz vom neutralen Element e:
Es gibt ein e, so dass e linksneutral ist, d.h. Für alle $x \in G$ gilt $e \circ x = x$.

(G3) die Existenz vom Inversen:
Es gibt ein linksneutrales Element e, so dass
jedes Element ein Linksinverses bezüglich e hat, d.h. zu jedem $x \in G$ gibt es $y \in G$, so dass $y \circ x = e$.

(b) Eine Struktur $(G, \circ)$ heißt abelsche[3] Gruppe, gdw sie die Gruppenaxiome erfüllt und zusätzlich kommutativ (auch abelsch genannt) ist. D.h., das Kommutativgesetz gilt: Für alle $x, y \in G$ ist $x \circ y = y \circ x$.

Wir zeigen, dass e eindeutig ist, wenn (G1) bis (G3) gelten. Meistens quantifiziert man e nicht ab.

Lemma 2.18. *Sei G eine Gruppe und sei e ein linksneutrales Element wie im Gesetz (G3). Dann gilt*

$$\forall a, b \in G\ a \circ b = e \to b \circ a = e$$

Lemma 2.19. *Sei G eine Gruppe.*

(a) Es gibt nur ein linksneutrales Element. Dieses ist auch rechtsneutrales Element.

[3] Nils Henrik Abel, 1802 – 1829

(b) $\forall a \exists^{=1} b\, b \circ a = e$ *und dieses* b *ist auch rechtsinvers zu* a.

Wir schreiben von nun an a^{-1} für das Inverse zu a.

Definition 2.20. Ordnung einer Gruppe Die Mächtigkeit von G, $|G|$ heißt die Ordnung der Gruppe G.

Im Falle endlicher G ist $|G|$ das eindeitig bestimmte n so dass es eine Bijektion von G auf $\{0, \ldots, n-1\}$ gibt. Falls $n = 0$, ist letzteres die leere Menge. Im Falle unendlicher G, ist $|G|$ eine Kardinalzahl (siehe z.B. [16]).

Definition 2.21. Sei M eine Menge.

$$S(M) = \{f \colon M \to M \mid f \text{ bijektiv}\}.$$

$(S(M), \circ)$ heißt die symmetrische Gruppe auf M.

Beobachtung 2.22. *(a)* $(a^{-1})^{-1} = a$.

(b) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Beispiele 2.23. für Gruppen.

(1) Die einelementige Gruppe.

(2) Die zweielementige Gruppe.

(3) Die Gruppen $\mathbb{Z}_p$. Wohldefiniertheit der Addition $[x]_p + [y]_p$.

(4) Symmetriegruppen von geometrischen Figuren im $\mathbb{R}^2$.

2.4 Körper

Definition 2.24. Ein Körper ist eine Struktur $(K, +, \cdot)$ mit folgenden Gesetzen:

(K1) $(K, +)$ ist eine abelsche Gruppe.

(K2) $(K \setminus \{0\}, \cdot)$ ist eine ablsche Gruppe.

(K3) $(a + b)c = ac + bc$.

Definition 2.25. Verzichtet man in (K2) auf die Kommutativität, so erhält man einen Schiefkörper. Verzichtet an in (K2) auf das Inverse, so erhält man einen kommutativen Ring mit 1 . Verzichtet man in (K2) auf die Kommutativität und das Inverse, so erhält man einen Ring mit 1.

Beispiele: Körper $\mathbb{Q}$, $\mathbb{R}$, Gegenbeispiel $\mathbb{Z}$ nur Ring mit Eins.

Rechenregeln 2.26. *in Körpern.*

(1) $-(-a) = a$.

(2) $-(a + b) = -a - b$.

(3) $0 \cdot a = 0$.

(4) $a \cdot (-b) = -ab$.

(5) $(ab)c = a(bc)$.

Definition 2.27. Die Definition der komplexen Zahlen durch Cardano[4]. Die Menge der komplexen Zahlen ist $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$. Wir definieren $+\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ und $\cdot\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ durch:
$(a + ib) + (c + id) = a + c + i(b + d)$
$(a + ib) \cdot (c + id) = ac - bd + i(bc + ad)$.

Definition 2.28. Die Gauß'sche Zahlenebene $\mathbb{C}_g = \{(a, b) \mid a, b \in \mathbb{R}\}$ Wir definieren $+\colon \mathbb{C}_g \times \mathbb{C}_g \to \mathbb{C}_g$ und $\cdot\colon \mathbb{C}_g \times \mathbb{C}_g \to \mathbb{C}_g$ durch:

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d),\\ (a, b) \cdot (c, d) &= (ac - bd, bc + ad).\end{aligned}$$

$f\colon \mathbb{C} \to C_g$, $f(a + ib) = (a, b)$ ist ein Isomorphismus von $(\mathbb{C}, +, \cdot)$ auf $(\mathbb{C}_g, +, \cdot)$.

Satz 2.29. *Der Fundamentalsatz der Algebra. Jedes nicht konstante Polynom über $\mathbb{C}$ hat eine Nullstelle in $\mathbb{C}$. D.h.: Für alle $n \in N \setminus \{0\}$, für alle $a_0, \ldots, a_n \in \mathbb{C}$ mit $a_n \neq 0$ gibt es ein $x \in \mathbb{C}$ so dass*

$$\sum_{i=0}^{n} a_i x^i = 0.$$

(In der Vorlesung nicht bewiesen!)

Lemma 2.30. *Sei $p \in \mathbb{N}$. Sei $f\colon \underline{p} \to \underline{p}$ injektiv. $\underline{p} = \{\underline{x} \mid x < p\}$. Dann ist f surjektiv.*

Definition 2.31. Sei $p \in N \setminus \{0\}$. $[x]_p \cdot [y]_p = [x \cdot y]_p$.

Dies ist wohldefiniert.

Lemma 2.32. *Sei p prim. Dann ist $\mathbb{Z}_p$ ein Körper. Wenn $p \geq 2$ nicht prim ist, dann ist $\mathbb{Z}_p$ kein Körper.*

2.5 Vektorräume

Wir treffen die Konvention, dass wir nun griechische Buchstaben als Variablen für die Körperelemente schreiben und lateinische Buchstaben vorerst für (Variablen für) Vektoren (und Elemente von Halbordnungen und vieles mehr) stehen.

Definition 2.33. $(V, K, +_K, \cdot_K, +_V, \cdot_s)$ ist ein K-Vektorraum oder Vektorraum über K, wenn folgendes gilt:

(1) $(K, +_K, \cdot_K)$ ist ein Körper. Sei 1 das neutrale Element bezüglich $\cdot_K$.

(2) $(V, +_V)$ ist eine abelsche Gruppe mit neutralem Element 0_V. V heißt die Menge der Vektoren, die Elemente aus V heißen Vektoren.

(3) $\cdot_s\colon K \times V \to V$ wird die skalare Multiplikation genannt.

(4) $\forall \alpha, \beta \in K, \forall v \in V, (\alpha \cdot_K \beta) \cdot_s v = \alpha \cdot_s (\beta \cdot_s v)$.

(5) $\forall \alpha, \beta \in K, \forall v \in V, (\alpha +_K \beta) \cdot_s v = \alpha \cdot_s v +_V \beta \cdot_s v$.

(6) $\forall \alpha \in K, \forall v, w \in V, \alpha \cdot_s (v +_V w) = \alpha \cdot_s v +_V \alpha \cdot_s w$.

(7) $\forall v \in V\ 1 \cdot_s v = v$.

[4] Gerolamo Cardano, 1501 – 1576

Man schreibt oft nur V statt $(V, K, +_K, \cdot_K, +_V, \cdot_s)$, wenn man die Strukturmerkmale aus dem Kontext ablesen kann. Außerdem schreiben wir nicht immer die Indizes unter $+$ und $\cdot$.

Beispiele:

(1) Der Nullraum $\{0_v\}$.

(2) Sei K ein Körper, $n \in \mathbb{N}$. K^n, $\mathbb{R}^n$. (Hierbei ist $K^0 = \{0\}$).

(3) $\mathbb{R}^{(\mathbb{N})} = \{f \colon \mathbb{N} \to \mathbb{R} \mid \exists k \forall n \geq k f(n) = 0\}$,

(4) $\mathbb{R}^{\mathbb{N}} = \{f \colon \mathbb{N} \to \mathbb{R}\}$.

Alle Mengen sind jeweils mit komponentenweiser Addition und komponentenweiser skalarer Multiplikation zu versehen, damit man sie als Vektorräume auffassen kann.

Definition 2.34. Sei V ein Vektorraum $U \subseteq V$ heißt Unter(vektor)raum von V, gdw $U \neq \emptyset$ und

$$\forall \alpha, \beta \in K \forall v, w \in U \alpha v + \beta w \in U.$$

Lemma 2.35. *Unterräume sind Vektorräume.*

Rechenregeln 2.36. *in Vektorräumen*

(1) $\forall v \in V 0_K \cdot_s v = 0_V$.

(2) $\forall \alpha \in K \alpha \cdot_s 0_V = 0_V$.

(3) $\forall v \in V \alpha \in K \alpha \cdot_s v = 0 \to (\alpha = 0_K \vee v = 0_V)$.

(4) $\forall v \in V \alpha \in K (-\alpha) \cdot_s v = \alpha \cdot_s (-v) = -(\alpha \cdot_s v) =: -\alpha v$.

Beispiele 2.37. für Unterräume:

(1) $\{0\}$, V sind Unterräume von V.

(2) Sei $m \leq n$.

$$K^m \times \{\underbrace{(0, \ldots, 0)}_{m-n}\} = \{(x_1, \ldots, x_n) \in K^n \mid x_{m+1} = \cdots = x_n = 0\}$$

ist ein Unterraum von K^n.

(3) $\mathbb{R}^{(\mathbb{N})}$ ist ein Unterraum von $\mathbb{R}^{\mathbb{N}}$.

Satz 2.38. *Die Lösungsmenge eines (=jedes) homogenen linearen Gleichungssystems ist ein Unterraum.*

Lemma 2.39. *Der Schnitt beliebig vieler Unterräume ist ein Unterraum.*

Definition 2.40. Sei V ein Verktorraum und $M \subseteq V$. Wir setzen

(1) $\mathcal{U}_M = \{U \mid U \text{ Unterraum von } V, U \supseteq M\}$.

(2) $\operatorname{span}(M) = \bigcap \mathcal{U}_M$.

(3) M heißt Erzeugendensystem für/von V :gdw $\operatorname{span}(M) = V$.

Beobachtung 2.41. *(1)* $M \subseteq M' \subseteq V$. *Dann ist* $\operatorname{span}(M) \subseteq \operatorname{span}(M')$.

(2) Falls U *Unterraum, so ist* $\operatorname{span}(U) = U$.

(3) $\operatorname{span}(\operatorname{span}(M)) = \operatorname{span}(M)$.

(4) $\operatorname{span}(\emptyset) = \operatorname{span}(\{0_V\}) = \{0_V\}$.

Satz 2.42. *Sei V ein K-Vektorraum, $M \neq \emptyset$, $M \subseteq V$. Dann ist*

$$\operatorname{span}(M) = \{\sum_{i=1}^{n} \alpha_i v_i \,|\, n \in \mathbb{N} \setminus \{0\}, \alpha_i \in K, v_i \in M\}.$$

Definition 2.43. Ein Term des Typs $\sum_{i=1}^{n} \alpha_i v_i$ heißt Linearkombination. Eine Linearkombination heißt nicht trivial :gdw $\exists i \in \{1, \ldots, n\} \alpha_i \neq 0$.

Beispiele 2.44. (1) Sei V ein K-Vektorraum. Dann ist in V:

$$\operatorname{span}(\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}) = K^n.$$

(2) $\operatorname{span}(\{v_0, v_1\}) = \mathbb{R}^2$, falls v_0, v_1 linear unabhängig sind (s.u.).

Definition 2.45. Sei V ein K-Vektorraum.

(1) Sei $n \in \mathbb{N} \setminus \{0\}$, seien $v_1, \ldots, v_n \in V$. $v_1, \ldots, v_n$ heißen linear unabhängig :gdw

$$\forall \alpha_1 \ldots \forall \alpha_n (\sum_{i=1}^{n} \alpha_i v_i = 0_V \to \alpha_1 = \cdots = \alpha_n = 0).$$

Andernfalls heißen die $v_1, \ldots, v_n$ linear abhängig.

(2) Sei $L \subseteq V$. L heißt linear unabhängig :gdw

$$\forall n \forall v_1 \in L \ldots \forall v_n \in L (\bigwedge_{i \neq j} v_i \neq v_j \to v_1, \ldots, v_n \text{ ist linear unabhängig}).$$

Andernfalls heißt L linear abhängig.

Beobachtung 2.46. *(1) Sei T linear unabhängig und sei $S \subseteq T$. Dann ist S linear unabhängig.*

(2) T ist linear unabhängig gdw jede endliche Teilmenge $S \subseteq T$ linear unabhängig ist. Man sagt hierzu auch: Linear Unabhängigkeit ist eine Eigenschaft von endlichem Charakter.

(3) Seien T_i, $i \in I$, linear unabhängig, sei $(I, <_I)$ linear geordnet und gelte für $i <_I j$ $T_i \subseteq T_j$. Dann ist $\bigcup_{i \in I} T_i$ linear unabhängig. Man sagt hierzu auch: Die (=jede) „aufsteigende Vereinigung" linear unabhängiger Mengen ist linear unabhängig.

Die Vereinigung linear unabhängiger Mengen ist i.A. nicht linear unabhängig.

Definition 2.47. $B \subseteq V$ heißt Basis von V :gdw B ein linear unabhängiges Erzeugendensystem für V ist.

Für $V = \{0\}$ ist $\emptyset$ eine (die einzige) Basis.

Lemma 2.48. *(1) Wenn $v \in \operatorname{span}(M)$, so ist $\operatorname{span}(M \cup \{v\}) = \operatorname{span}(M)$.*

(2) Wenn $v \in \operatorname{span}(M) \setminus M$, so ist $M \cup \{v\}$ linear abhängig.

2.6 Basen

Lemma 2.49. *Eine Vorstufe des Austauschlemmas von Steinitz.* [5] *Sei $A \subseteq V$ linear abhängig und sei $L \subseteq A$ linear unabhängig. Dann gibt es $v \in A \setminus L$, das sich als Linearkombination von Vektoren aus $A \setminus \{v\}$ darstellen lässt.*

Beweis: Da A linear abhängig ist, gibt es eine nicht triviale Linearkombination

$$\sum_{a \in A_0} \alpha_a a = 0$$

mit einem endlichen $A_0 \subseteq A$. Nun ist mindestens ein $a \in A_0 \setminus L$ in dieser Summe so dass $\alpha_a \neq 0$. Denn wären alle $a \in A_0 \setminus L$ in dieser Summe so, dass $\alpha_a = 0$, dann wäre schon

$$\sum_{a \in L \cap A_0} \alpha_a a = 0$$

eine nicht triviale Linearkombination, im Gegensatz zur linearen Unabhängigkeit von L. Wir halten also ein $a \in A_0 \setminus L$ mit $\alpha_a \neq 0$ fest. Dann ist

$$\sum_{b \in A_0 \setminus \{a\}} \alpha_b b = -\alpha_a a.$$

Wir dividieren beide Seiten durch $-\alpha_a$ und erhalten somit

$$a = \sum_{b \in A_0 \setminus \{a\}} \alpha_b (-\alpha_a)^{-1} b,$$

wie gewünscht. □

Bemerkung 2.50. Für Moduln (d.h. Vektorräume über Ringen mit 1) ist das Lemma falsch. Im (Hauptideal-)Ring $\mathbb{Z}$ ist $2 \cdot 3 - 3 \cdot 2 = 0$, aber wir können die 3 nicht darstellen aus der 2.

Definition 2.51. (1) Eine Halbordnung $(H, \leq_H)$ heißt induktive Halbordnung , :gdw jede durch $\leq_H$ linear geordnete Teilmenge $K \subseteq H$ (man sagt zu solchen Teilmengen auch Ketten) eine obere Schranke hat, d.h. es gibt $s \in H$, so dass für alle $k \in K$, $k \subseteq s$.

(2) Ein Element m in einer Halbordnung $(H, \leq_H)$ heißt maximales Element :gdw $\forall n \in H (n \geq_H m \to n = m)$. (Verwechseln Sie dies nicht mit dem größten Element von weiter unten. In linearen Ordnungen fallen die beiden Begriffe zusammen, aber nicht in Halbordnungen.)

$(\mathbb{N}, \leq)$ ist keine induktive Halbordnung, obwohl $\mathbb{N}$ isomorph zu einer induktiven Menge ist Die beiden Begriffe haben nichts miteinander zu tun.

Vorspann: Der Basisergänzungssatz braucht zum Beweis das Lemma von Zorn, dessen Beweis nicht zum Stoff einer Anfängervorlesung gehört. Der Satz über die Existenz von Basen reicht tief in unsere Auffassung der Axiome hinein:

Satz 2.52. *(Blass[6], 1984 [3])* ZF*. Wenn jeder Vektorraum eine Basis hat, dann gilt das Auswahlaxiom.*

[5] Ernst Steinitz, 1871–1928
[6] Andreas Blass, geb. 1947

Der Beweis dieses Satzes ist nicht Gegenstand einer Anfängervorlesung. Er könnte bei Interesse einmal in einem Seminar in etwa drei oder vier Sitzungen durchgeführt werden.

Lemma 2.53. *Das Lemma von Zorn*[7] *. Jede induktive Halbordnung hat ein maximales Element.*

Beweisskizze: Ich habe unten einen Beweis aufgeschrieben, falls Sie Interesse haben. Er ist nicht Prüfungsstoff.

Wenn man das Lemma von Zorn akzeptiert, dann kann man die anderen Beweisschritte durchführen:

Satz 2.54. ZFC *Der Basisergänzungssatz von Steinitz (Im Original wohl in [14], aber wir geben einen späteren Beweis mit Hilfe des Lemmas von Zorn.). Sei V ein K-VR und sei A linear unabängig, und sei E ein Erzeugendensystem. Dann gibt es $E' \subseteq E$, so dass $A \cup E'$ eine Basis bildet.*

Beweis: Wie schreiben

$$H = \{D \mid A \subseteq D \subseteq A \cup E, D \text{ ist linear unabhängig}\}.$$

Wir ordnen H mit $\subseteq$. Dann ist $(H, \subseteq)$ eine sogenannte induktive Halbordnung.

Wir zeigen dies: $\subseteq$ ist eine antisymmetrische, reflexive und transitive Relation. Sei K eine Kette in $(H, \subseteq)$. Wir bilden $\bigcup K$. Dann ist $\bigcup K \subseteq V$, $A \subseteq \bigcup K \subseteq A \cup E$. K ist linear unahängig, denn jede Abhängigkeit bräuchte nur endlich viele Vektoren, und die kämen in einem einzigen Kettenglied schon vor, was der Voraussetzung $K \subseteq H$ widerspräche. Also ist $\bigcup K$ eine obere Schranke von K.

Nun gibt es nach dem Lemma von Zorn ein maximales Element E' in H. E' ist linear unabhängig, da $E' \in H$. E' erzeugt V, denn Annahme nicht. Es gibt $v \in V \setminus \text{span}(E')$. Dann ist $E' \cup \{v\}$ linear unabhängig, denn andernfalls könnte man nach der Vorstufe des Austauschlemmas v als Linearkombination von E' darstellen. $E' \cup \{v\}$ zeigt also, dass E' nicht maximal ist. □

Beweis des Lemmas von Zorn und des Wohlordnungssatzes nicht vorgelesen in der Vorlesung

Definition 2.55. Sei A eine Menge. $(A, <)$ heißt Wohlordnung gdw $(A, <)$ eine lineare Ordnung ist, in der jede nicht leere Teilmenge ein $<$-minimales Element hat.

Eine Menge A hat eine Wohlordnung, gdw es eine Relation $<$ aus A gibt, so dass $(A, <)$ eine Wohlordnung ist.

Wir beweisen gleich zwei sehr nützliche Äquivalente zum Auswahlaxiom:

Satz 2.56. *Der Wohlordnungssatz und das Lemma von Zorn. Folgende sind äquivalent auf der Basis von* ZF*:*

(1) Das Auswahlaxiom.

(2) Jede induktive Halbordnung hat ein maximales Element.

(3) Jede Menge hat eine Wohlordnung.

Beweis

[7] Max Zorn, 1906 – 1993

(1) impliziert (3) Dies ist er Zermelo'sche Wohlordnungssatz von 1904 [15]. Der Beweis braucht Ordinalzahlen und den Rekursionssatz für Ordinalzahlen, siehe z.B [6], [16, Kapitel 2]. Diese Gegenstände werden erst in späteren Vorlesungen gelehrt.

Sei A gegeben. Wir konstruieren eine Wohlordnung $\prec$ auf A wie folgt. Wir nehmen eine Auswahlfunktion h auf $\mathscr{P}(A) \setminus \{\emptyset\}$. Dann definieren wir rekursiv über die Klasse On aller Ordinalzahlen mit der $\in$-Ordnung $(\mathrm{On}, \in)$ eine Einbettung $F\colon \mathrm{On} \to A \cup \{A\}$ wie folgt:

$$F(\alpha) := h(A \setminus \{F(\beta) \mid \beta \in \alpha\}),$$

falls $\{F(\beta) \mid \beta \in \alpha\} \neq A$. Falls $\{F(\beta) \mid \beta \in \alpha\} = A$, dann ist $F(\alpha) := A$. Nach dem Rekursionssatz für On ist F eine wohldefinierte Operation. Da A eine Menge ist und da F injektiv ist, solange der Wert A nicht angenommen wird, gibt es nach dem Ersetzungsschema ein α mit $F(\alpha) = A$. Sei α minimal mit $F(\alpha) = A$. Dann ist $F \restriction \alpha =: f\colon \alpha \to A$ eine Bijektion (also insbesondere eine Funktion, ein Element des Mengenuniversums), die nun die Wohlordnung von $(\alpha, \in)$ auf A überträgt durch $a \prec b \leftrightarrow f^{-1}(a) \in f^{-1}(b)$. Von der klassengroßen Operation F wird also am Ende nur der mengengroße Anfangsabschnitt $F \restriction \alpha$ gebraucht.

(3) impliziert (1). Sei X eine Menge nicht leerer Mengen. Wir nehmen eine Wohlordnung $\prec$ auf $\bigcup X$. Dann setzen wir für $x \in X$, $f(x) =$ das $\prec$-minimale Element von x.

(1) impliziert (2) [18]. Auch diese Implikation braucht Ordinalzahlen. Sei eine induktive Halbordnung $(H, \leq_H)$ gegeben. Wir konstruieren ein maximales Element von H wie folgt. Wir nehmen eine Auswahlfunktion h auf $\mathscr{P}(A) \setminus \{\emptyset\}$. Dann definieren wir rekursiv über die Klasse aller Ordinalzahlen mit der $\in$-Ordnung $(\mathrm{On}, \in)$ eine Einbettung $F\colon \mathrm{On} \to A \cup \{A\}$ wie folgt:

$$F(\alpha) := h\big((\text{Menge der oberen Schranken von } \{F(\beta) \mid \beta \in \alpha\}) \setminus \{F(\beta) \mid \beta \in \alpha\}\big),$$

falls (Menge der oberen Schranken von $\{F(\beta) \mid \beta \in \alpha\}) \setminus \{F(\beta) \mid \beta \in \alpha\} \neq \emptyset$, und $F(\alpha) = A$ sonst. Nach dem sogenannten Rekursionssatz für On ist F eine wohldefinierte Operation. Da A eine Menge ist und da F injektiv ist, solange der Wert A nicht angenommen wird, gibt es nach dem Ersetzungsschema ein α mit $F(\alpha) = A$. Sei α minimal mit $F(\alpha) = A$. Da $\{F(\beta) \mid \beta \in \alpha\} = K$ eine Kette ist, gibt es nur dann keine obere Schranke außerhalb K, wenn K ein größtes Element in K hat. Dann ist α eine Nachfolgerordinalzahl, $\alpha = \beta + 1$, und $F(\beta)$ ist ein maximales Element von H.

(2) impliziert (1). Sei Y eine Menge nicht leerer Mengen. Wir nehmen

$$H = \{(X, h) \mid X \subseteq Y, h \text{ Auswahlfunktion auf } X\},$$

und halbordnen mit $(X, h) \leq_H (X', h')$:gdw $X \subseteq X'$ und $h' \restriction X = h$. $(H, \leq_H)$ ist eine induktive Halbordnung, denn jede Kette hat als eine obere Schranke die Vereinigung der Kette. Nach dem Zorn'schen Lemma gibt es ein maximales Element (M, h). Man rechnet nach, dass wegen der Maximalität von M die Gleichheit $M = Y$ gilt. h ist also eine Auswahlfunktion auf Y. □

Ende der nicht vorgelesenen Passage.

Lemma 2.57. *Das Austauschlemma von Steinitz. Sei* $b \in \mathrm{span}(A \cup \{a\}) \setminus \mathrm{span}(A)$. *Dann ist* $a \in \mathrm{span}(A \cup \{b\})$.

Satz 2.58. *Der Austauschsatz von Steinitz. Sei B eine Basis von V mit $n \geq 1$ Elementen. Sei L linear unabhängig. Dann gilt*

(a) $|L| \leq n$, *und*

(b) Es gibt $n - |L|$ Vektoren aus $B = \{b_1, \ldots, b_n\}$, bei geeigneter Nummerierung sind dies $v_{n-|L|+1}, \ldots, v_n$, so dass $L \cup \{v_{n-|L|+1}, \ldots, v_n\}$ eine Basis ist.

Definition 2.59. Sei V ein Vektorraum. Die Dimension von V ist die Mächtigkeit einer (= jeder) Basis von V. Wir schreiben $\dim(V)$ dafür.

(Wir kennen nur endliche Mächtigkeiten bis jetzt in der Vorlesung.)

2.7 Der Verband der Unterräume

Definition 2.60. Sei $(H, \leq)$ eine Halbordnung.

(1) $m \in H$ heißt größtes Element gdw $\forall h \in H h \leq m$. $k \in H$ heißt kleinstes Element gdw $\forall h \in H h \geq k$.

(2) Sei $A \subseteq H$. Mit $\sup(A)$ (das nicht zu existieren braucht) bezeichnen wir die kleinste obere Schranke von A, also das Element s, so dass

$$\forall a \in A a \leq s \wedge \forall b(\forall a \in A b \geq a \to b \geq s).$$

Mit $\inf(A)$ (das nicht zu existieren braucht) bezeichnen wir die größte untere Schranke von A, also das Element i, so dass

$$\forall a \in A a \geq i \wedge \forall b(\forall a \in A b \leq a \to b \leq i).$$

(3) Wir schreiben $\sup(a, b)$ für $\sup(\{a, b\})$.

Definition 2.61. Eine Halbordnung mit größtem und mit kleinstem Element heißt Verband, wenn je zwei Elemente ein Supremum und ein Infimum haben.

Definition 2.62. Sei V ein Vektorraum, und seien U_1, U_2 Unterräume von V. Wir setzen

$$U_1 + U_2 = \{u_1 + u_2 \,|\, u_1 \in U_1, u_2 \in U_2\}.$$

Beobachtung 2.63. $U_1 + U_2 = \operatorname{span}(U_1 \cup U_2)$.

Satz 2.64. *Sei V ein Vektorraum. Dann ist die durch Inklusion geordnete Menge der Unteräume von V ein Verband. Dabei ist* $\sup(U_1, U_2) = U_1 + U_2$, $\inf(U_1, U_2) = U_1 \cap U_2$.

Bemerkung 2.65. Das Distributivgesetz $(U_1 + U_2) \cap U_3 = U_1 \cap U_3 + U_2 \cap U_3$ ist im Allgemeinen ab Dimension 2 falsch.

Lemma 2.66. *Sei V ein Vektorraum. Das Modularitätsgesetz: Sei $U_2 \subseteq U_3$. Dann ist*

$$(U_1 + U_2) \cap U_3 = U_1 \cap U_3 + U_2.$$

Man sagt hierzu: Das Modularitätsgesetz gilt im Verband der Unterräume.

Definition 2.67. (1) Sei V ein Vektorraum. U ein Unterraum von V. Ein Unterraum U' heißt zu U komplementärer Unterraum, :gdw $U \cap U' = \{0\}$ und $U + U' = V$.

(2) Sei $(H, \leq_H)$ ein Verband, $h \in H$. k heißt Komplement von/zu h, falls $\sup(h,k)$ das größte Element ist, und $\inf(h,k)$ das kleinste Element im Verband ist.

Satz 2.68. ZFC *Sei V ein Vektorraum. Jeder Unterraum hat einen komplementären Unterraum U' (der im Falle $V \neq U' \neq \{0\}$ nicht eindeutig ist).*

Lemma 2.69. *Sei V ein endlichdimensionaler Vektorraum, und U ein Unterraum. und U' ein Komplement zu U. Dann ist*

$$\dim(V) = \dim(U) + \dim(U').$$

Das Lemma gilt auch für unendlichdimensionale Vektorräume, allerdings braucht man dann Kenntnisse über Kardinalzahlen und kardinale Addition.

Wir verlassen den Verband der Unterräume in der folgenden Definition.

Definition 2.70. Seien V_1 und V_2 zwei K-Vektorräume. Dann definieren wir folgende Struktur:

$$V = V_1 \bigoplus V_2 = (V_1 \times V_2, K, +_K, \cdot_K, +_V, \cdot_s)$$

durch

$$\begin{aligned} (u_1, u_2) +_V (v_1, v_2) &:= (u_1 +_{V_1} v_1, u_2 +_{V_2} u_2), \\ \alpha \cdot_s (v_1, v_2) &:= (\alpha v_1, \alpha v_2). \end{aligned}$$

$V_1 \bigoplus V_2$ heißt die direkte Summe der Vektorräume V_1, V_2. Die direkte Summe ist nicht kommutativ.

Definition 2.71. Seien $V_1 = (V_1, K, +, \cdot, +_{V_1}, \cdot_{s,V_1})$ und $V_2 = (V_2, K, +, \cdot, +_{V_2}, \cdot_{s,V_2})$ zwei K-Vektorräume.

(1) $f\colon V_1 \to V_2$ heißt linear oder auch Vektorraumhomomorphismus :gdw

$$\forall \alpha, \beta \in K \forall v, w \in V_1 f(\alpha \cdot_{s,V_1} v +_{V_1} \beta \cdot_{s,V_1} w) = \alpha \cdot_{s,V_2} f(v) +_{V_2} \beta \cdot_{s,V_2} f(w).$$

(2) $f\colon V_1 \to V_2$ heißt Vektorraumisomorphismus :gdw f bijektiv und linear ist. Wir schreiben $V_1 \cong V_2$ oder $f\colon V_1 \stackrel{\cong}{\to} V_2$.

Lemma 2.72. *Sei V ein Vektorraum, seien U_1, U_2 Unterräume, und sei $U_1 \cap U_2 = \{0\}$. Dann gilt*

$$\begin{aligned} f \quad : \quad & U_1 \times U_2 \to U_1 + U_2, \\ & (u_1, u_2) \mapsto u_1 + u_2 \end{aligned}$$

ist bijektiv und ein Vektorraumisomorphismus von $U_1 \bigoplus U_2$ auf $U_1 + U_2$.

Korollar 2.73. *Wenn V ein Vektorraum ist und U ein Unterraum und U' ein zu U in V komplementärer Unterraum ist, dann ist*

$$V = U + U' \cong U \bigoplus U'.$$

Korollar 2.74. *Wenn V ein Vektorraum ist und U ein Unterraum. Dann sind je zwei Komplemente isomorph.*

Definition 2.75. Sei V ein Vektorraum und sei U ein Unterraum.

(1) Wir definieren für $v, w \in V$:

$$v \sim_U w :\Leftrightarrow v - w \in U.$$

(2) $v + U := \{v + u \mid u \in U\}$ nennt man Nebenklasse (von v bezüglich U).

(3) $V/U = \{[v]_{\sim_U} \mid v \in V\}$ heißt die Menge der Nebenklassen oder (wie früher) die Quotientenmenge.

(4) $\pi\colon V \to V/U$, $\pi(v) = [v]_{\sim_U}$ heißt die kanonische Projektion.

Beobachtung 2.76. *Sei V ein Vektorraum und sei U ein Unterraum, $v \in V$.*

(1) $[v]_{\sim_U} = v + U$.

(2) Die Relation $\sim_U$ ist eine Äquivalenzrelation. Daher sind je zwei Nebenklassen entweder gleich oder disjunkt.

Satz 2.77. *V/U trägt eine K-Vektorraumstruktur, die eindeutig dadurch bestimmt ist, dass die kanonische Projektion*

$$\pi\colon V \to V/U$$

linear ist.

Lemma 2.78. *Sei U' ein Komplement von U in V. Dann induziert die kanonische Projektion $\pi\colon V \to V/U$ via Einschränkung einen Isomorphismus*

$$\pi' = \pi \restriction U'\colon U' \xrightarrow{\cong} V/U.$$

Bemerkung 2.79. und *Denkaufgabe, die in der Vorlesung gemacht wurde*: U' ist also ein Repräsentantensystem von V/U. Sei $\dim(V) \geq 2$. Dann gibt es einen Unterraum U von V, so dass V/U ein Repräsentantensystem hat, das kein Unterraum ist.

Korollar 2.80. *Wenn V endlichdimensional ist, dann ist* $\dim(V) = \dim(U) + \dim(V/U)$.

Das Korollar gilt auch für unendlichdimensionale Vektorräume.

Definition 2.81. $\operatorname{codim}_V(U) = \dim(V/U)$ heißt die Kodimension von U in V.

Satz 2.82. *Sei V endlichdimensional, und seien U_1 und U_2 Unterräume. Dann ist* $\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim(U_1) + \dim(U_2)$.

Der Satz gilt auch für unendlichdimensionale Vektorräume.

Definition 2.83. Sei V ein Vektorraum und sei H ein Unterraum. H heißt Hyperebene, :gdw es einen eindimensionalen komplementären Unterraum H' gibt mit $V = H + H'$.

Bemerkung 2.84. Im Endlichdimensionalen ist die Definition äquivalent zu $\dim(H) = \dim(V) - 1$. Im Unendlichen gibt es nur die Addition von Kardinalzahlen, keine Subtraktion, daher ist die obige Definition in mehr Situationen geeignet.

Wir beweisen eine Verfeinerung des Satzes 2.68:

Satz 2.85. ZFC *Sei V ein Vektorraum. Seien U und U' Unterräume und $V = U + U'$. Dann hat U hat einen komplementären Unterraum U'', so dass $U'' \subseteq U'$.*

Nicht gemacht Im Spezialfall, dass U' endlichdimensional ist, kommt man ohne Auswahl aus:

Satz 2.86. ZF *Sei V ein Vektorraum. Sei H ein Unterraum und U' ein endlichdimensionaler Unterraum und $V = H + U'$. Dann hat H hat einen komplementären Unterraum U'', so dass $U'' \subseteq U'$.*

Beweis: Da $H + U' = V$, gilt: U'/H erzeugt V/H. Wir nehmen (z. B. Wie in Aufgabe 3 des Blattes 7) ein linear unabhängiges Erzeugendensystem B für $\subseteq U'/H$. Dieses ist endlich. Dann nehmen wir Vertreter für $b+H$ in U' für jedes $b+H \in B$. Die endliche Menge dieser Vertreter spannt einen Unterraum U'' mit den gewünschten Eigenschaften auf. □

Ab hier wieder gemacht, eben unnötigerweise ZFC vorausgesetzt.

Korollar 2.87. ZF *Sei V ein Vektorraum und H eine Hyperebene, und sei U ein Unterraum. Dann ist entweder $U \subseteq H$, oder $U \cap H$ ist eine Hyperebene in U.*

Beweis: Falls $U \subseteq H$, so ist $U \cap H = U$, und U ist keine Hyperebene in U. Falls $U \not\subseteq H$, so ist $U/H = H'/H$ für jedes Komplement H' von H. Wir nehmen nun mit dem vorigen Satz ein Komplement H' von H, so dass $H' \subseteq U$. Dann gilt nach dem Modularitätsgesetz, angewandt auf, $H + H' = V$, die Gleichung $(H + H') \cap U = H \cap U + H' = U$. Somit ist H' ein eindimensionales Komplement von $U \cap H$ in U. □

Beispiel 2.88. Sei $V = K^n$, $n \in \mathbb{N} \setminus \{0\}$, und seien $\alpha_i \in K$ und sei $\alpha_i \neq 0$ für ein i. Dann ist

$$H = \{(x_1, \ldots, x_n) \mid \sum_{i=1}^{n} \alpha_i x_i = 0\}$$

eine Hyperebene im Raum K^n.

Kapitel 3

Lineare Abbildungen

3.1 Grundlegende Eigenschaften

Wir wiederholen Def 2.71.

Definition 3.1. Seien V und W K-Vektorräume. $f\colon V \to W$ heißt lineare Abbildung oder Vektorraumhomomorphismus :gdw

$$\forall \alpha, \beta \in K \forall v_1, v_2 \in V f(\alpha v_1 + \beta v_2) = \alpha f(v_1) + \beta f(v_2).$$

Definition 3.2. Sei $f\colon X \to Y$ eine Abbildung.

(1) Gelte $\forall y \in Y \exists^{=1} x \in X f(x) = y$. Dann schreiben wir f^{-1} für die Umkehrabbildung. $f^{-1}(y) = x$ gdw $f(x) = y$.

(2) Sei $Z \subseteq X$. $f[Z] := \{f(z) \mid z \in Z\} (= \mathrm{Im}(f \restriction Z))$ heißt das f-Bild von Z.

(3) Sei $Z \subseteq Y$. $f^{-1}[Z] := \{x \mid f(x) \in Z\}$ heißt die Urbildmenge von Z. Im Falle bijektiver f ist $f^{-1}[Z] = \{f^{-1}(z) \mid z \in Z\}$.

Definition 3.3. Seien V, W K-Vektorräume. Sei $f\colon V \to W$ eine lineare Abbildung.

(1) $\mathrm{Im}(f) = \{f(v) \mid v \in V\}$ heißt der Bildraum von f.

(2) $\ker(f) = \{v \in V \mid f(v) = 0_W\}$ heißt Kern von f.

Definition 3.4. Seien V, W K-Vektorräume.

(1) $\mathrm{Hom}(V, W) = \{f\colon V \to W \mid f \text{ linear}\}$.

(2) $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ heißt die Menge (später Algebra mit $+$, $\cdot_s$ und $\circ$) der Endomorphismen von V.

(3) $V^* = \mathrm{Hom}(V, K)$ heißt der Dualraum zu V.

Beispiele 3.5. für lineare Abbildungen.

(1) Integration. Sei $V = \{f\colon [a, b] \to \mathbb{R} \mid f \text{ stetig}\}$. Wir definieren $L\colon V \to V$ via $L(f) = \int_a^b f(x)dx$.

(2) Differentiation. Sei $V = \{f\colon [a, b] \to \mathbb{R} \mid f \text{ stetig differenzierbar}\}$, und sei $W = \{f\colon [a, b] \to \mathbb{R} \mid f \text{ stetig}\}$. Wir definieren $L\colon V \to W$ via $L(f) = f'$.

Lemma 3.6. *Sei $f\colon V \to W$ eine lineare Abbildung, und sei $f(a) = b$. Dann ist $f^{-1}[\{b\}] = a + \ker(f)$.*

Lemma 3.7. *Sei $f\colon V \to W$ eine lineare Abbildung.*

(1) $\ker(f)$ *ist ein Unteraum von V.*

(2) $\mathrm{Im}(f)$ *ist ein Unterraum von W.*

Lemma 3.8. *Sei $f\colon V \to W$ eine lineare Abbildung. Dann ist* $\ker(f) = \{0_V\}$*, gdw f injektiv ist.*

Lemma 3.9. *Sei $f\colon V \to W$ eine lineare Abbildung.*

(1) Sei Z ein Unterraum von W. $f^{-1}[Z]$ ist ein Unteraum von V.

(2) Sei Z ein Unterraum von V. $f[Z]$ ist ein Unterraum von W.

Lemma 3.10. *Sei $f\colon V \to W$ eine lineare Abbildung. Dann ist* $\ker(f) = \{0_V\}$ *gdw f linear unabhängige Mengen auf linear unabhängige Mengen abbildet.*

Lemma 3.11. *Sei $f\colon V \to W$ eine lineare Abbildung, $M \subseteq V$. Dann ist* $\mathrm{span}(f[M]) = f[\mathrm{span}(M)]$.

Korollar 3.12. *Sei $f\colon V \to W$ eine injektive lineare Abbildung, B eine Basis von V. Dann ist $f[B]$ eine Basis von $f[V]$. Falls f bijektiv ist, ist $f[B]$ eine Basis von W.*

Korollar 3.13. *Sei $f\colon V \to W$ eine lineare Abbildung. Folgende sind äquivalent:*

(1) f ist bijektiv.

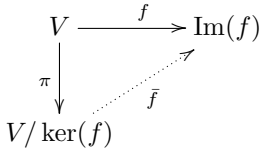
(2) Für jede Teilmenge B von V gilt: B ist Basis von V gdw $f[B]$ eine Basis von W ist.

(3) Es gibt eine Basis B von V, so dass $f[B]$ eine Basis von W ist.

Definition 3.14. Seien V, W K-Vektorräume. V und W heißen isomorph :gdw es eine bijektive lineare Abbildung $f\colon V \to W$ gibt. Solch eine Abbildung heißt Vektorraumisomorphismus.

Satz 3.15. *Der Noether'sche*[1] *Isomorphiesatz [13]. Seien V, W K-Vektorräume. Sei $f\colon V \to W$ eine lineare Abbildung. Dann induziert f einen Isomorphismus $\bar{f}\colon V/\ker(f) \xrightarrow{\cong} \mathrm{Im}(f)$ via $\bar{f}(v + \ker(f)) = f(v)$.*

Man schreibt die Situation auch gerne in einem Diagramm



Hierbei ist $\pi(v) = v + \ker(f)$. Wir haben also $\bar{f} \circ \pi = f$. Man sagt hierzu auch: „f faktorisiert durch π" und „das Diagramm kommutiert."

Wir kombinieren den Isomorphiesatz mit Satz über die Dimension von Quotienten 2.80 und erhalten für jede lineare Abbildung eine nützliche Aufspaltung des Definitionsbereichsraumes:

Korollar 3.16. *Wenn V endlichdimensional ist und $f\colon V \to W$ linear ist, dann ist* $\dim(V) = \dim(\ker(f)) + \dim(\mathrm{Im}(f))$.

[1] Emmy Noether, 1882 – 1953

3.2 Lineare Abbildungen und Matrizen

Definition 3.17. Sei K ein Körper, und $m, n \in \mathbb{N} \setminus \{0\}$. Eine m-n-Matrix über K ist ein Schema der Form

$$A = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \cdots & \alpha_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1} & \alpha_{m,2} & \cdots & \alpha_{m,n} \end{pmatrix}$$

mit $a_{i,j} \in K$. Man kann A als Funktion von $\{1, \ldots, m\} \times \{1, \ldots, n\} \to K$ auffassen mit $A(i, j) = \alpha_{i,j}$. Kürzere Schreibwseisen für A sind auch

$$(\alpha_{i,j})_{\substack{i=1,\ldots,n \\ j=1\ldots,n}}$$

oder nur $(\alpha_{i,j})_{i,j}$ oder nur $(\alpha_{i,j})$. Wichtig ist, dass es auf die Anordnung ankommt.

Wenn die $a_{i,j}$ paarweise verschieden sind, gibt es $(m \cdot n)!$ Anordnungen auf der Menge $\{\alpha_{i,j} \mid i = 1, \ldots, m, j = 1, \ldots, n\}$, die die Menge zu einer m-n-Matrix machen.

Definition 3.18. Sei K ein Körper, und $m, , n \in N \setminus \{0\}$.

(1) Die m-n-Nullmatrix ist gegeben durch $\alpha_{i,j} = 0$ für $i = 1, \ldots, m$, $j = 1, \ldots, n$.

(2) Sei nun $m = n$. Die m-m-Einheitsmatrix $1_{M_{m,m}(K)}$ ist gegeben durch $\alpha_{i,j} = \delta_{i,j}$ für $i = 1, \ldots, m$, $j = 1, \ldots, m$. Hierbei ist

$$\delta_{i,j} = \begin{cases} 0, & \text{falls } i \neq j; \\ 1, & \text{falls } i = j. \end{cases}$$

das Kronecker-Delta[2]

Definition 3.19. und Behauptung Sei K ein Körper, und $m, , n \in \mathbb{N}\setminus\{0\}$. $M_{m,n}(K)$ bezeichnet die Menge der m-n-Matrizen über K. Wir definieren die komponentenweise Addition $+$ und die komponentenweise Sklarenmultiplikation $\cdot_s$ auf $M_{m,n}(K)$ durch $(\alpha_{i,j}) + (\beta_{i,j}) = (\gamma_{i,j})$ mit $\gamma_{i,j} = \alpha_{i,j} + \beta_{i,j}$ und $\xi \cdot_s (\alpha_{i,j}) = (\beta_{i,j})$ mit $\beta_{i,j} = \xi \cdot_K \alpha_{i,j}$. So wird

$$(M_{m,n}(K), K, +_K, \cdot_K, +, \cdot_s)$$

zu einem Vektorraum über K, den wir ebenfalls mit $M_{m,n}(K)$ bezeichnen.

Definition 3.20. und Behauptung Sei K ein Körper, V, W K-Vektorräume. Dann ist $\mathrm{Hom}(V, W)$ mit der komponentenweise Addition $(f + g)(v) = f(v) + g(v)$ und der komponentenweise skalaren Multiplikation $(\alpha f)(v) = \alpha f(v)$ ein Vektorraum.

Satz 3.21. *Seien V, W Vektorräume der Dimension n bzw m. Dann ist* $\mathrm{Hom}(V, W)$ *isomorph zu $M_{m,n}(K)$. Für je zwei geordnete Basen $\vec{B} = (b_1, \ldots, b_n)$ von V und $\vec{C} = (c_1, \ldots, c_m)$ von W gilt folgendes: Jedes $f \in \mathrm{Hom}(V, W)$ bestimmt durch*

$$\text{für } j = 1, \ldots, n: \quad f(b_j) = \sum_{i=1}^{m} \alpha_{i,j} c_i$$

[2]Leopold Kronecker, 1823 – 1891

eine Matrix $\mathrm{Mat}_{\vec{B}}^{\vec{C}}(f) = A_f = (\alpha_{i,j})$. *Bei festen* $\vec{B}$, $\vec{C}$ *ist die Abbildung*

$$\begin{aligned} i\colon \mathrm{Hom}(V,W) &\to M_{m,n}(K); \\ f &\mapsto i(f) = A_f \end{aligned}$$

ein Vektorraumisomorphismus.

Wir nennen die Umkehrung dieses Isomorphismus: Seien immer noch $\vec{B}$ *und* $\vec{C}$ *geordnete Basen von* V *bzw.* W. *Jede Matrix* $A \in M_{m,n}(K)$ *bestimmt genau eine lineare Abbildung* f_A *mit*

$$\text{für } j = 1, \ldots, n: \quad f_A(b_j) = \sum_{i=1}^{m} \alpha_{i,j} c_i.$$

Es gilt $A_{f_A} = A$ *und* $f_{A_f} = f$.

Definition 3.22. Seien $\ell, m, n \in \mathbb{N} \setminus \{0\}$, und sei $B = (\beta_{i,j}) \in M_{m,n}(K)$ $A = (\alpha_{k,i}) \in M_{\ell,m}(K)$. Wir definieren die Matrizenmultiplikation

$$\begin{aligned} \cdot : M_{\ell,m}(K) \times M_{m,n}(K) &\to M_{\ell,n}(K); \\ (A, B) &\mapsto A \cdot B = AB = C = (\gamma_{\ell,j}) \end{aligned}$$

durch die folgenden Gleichungen

$$\text{für } k = 1, \ldots, \ell, j = 1, \ldots, n \quad \gamma_{\ell,j} = \sum_{i=1}^{m} \alpha_{\ell,i} \beta_{i,j}.$$

Beobachtung 3.23. *Die Matrizenmultiplikation ist in beiden Argumenten linear. D.h., für alle* $\alpha, \beta\gamma, \delta$, A, $A' \in M_{\ell,m}(K)$, B, $B' \in M_{m,n}(K)$ *gilt:* $(\alpha A + \beta A')(\gamma B + \delta B') = \alpha\gamma AB + \beta\gamma A'B + \beta\gamma A'B + \beta\delta A'B'$.

Satz 3.24. *Seien* U, V, W *Vektorräume der Dimension* n *bzw* m *bzw* ℓ *mit geordneten Basen* $\vec{B} = (b_1, \ldots, b_n)$, $\vec{C} = (c_1, \ldots, c_m)$, $\vec{D} = (d_1, \ldots, d_\ell)$. *Sei* $g\colon U \to V$ *linear und bzg.* $\vec{B}$ *und* $\vec{C}$ *gegeben durch* $g = f_B$, $B \in M_{m,n}(K)$. *Sei* $h\colon V \to W$ *linear und bzg.* $\vec{C}$ *und* $\vec{D}$ *gegeben durch* $h = f_A$, $A \in M_{\ell,m}(K)$. *Dann ist* $h \circ g\colon U \to W$ *bzgl* $\vec{B}$ *und* $\vec{D}$ *gegeben durch* f_{AB}. *Wir haben also* $A_{h\circ g} = A_h A_g$, *ausführlicher*

$$\mathrm{Mat}_{\vec{B}}^{\vec{D}}(h \circ g) = \mathrm{Mat}_{\vec{C}}^{\vec{D}}(h) \cdot \mathrm{Mat}_{\vec{B}}^{\vec{C}}(g)$$

und $f_{AB} = f_A \circ f_B$.

Beweis: Für $j = 1, \ldots, n$ ist $g(b_j) = f_B(b_j) = \sum_{i=1}^{m} \beta_{i,j} c_i$. Für $i = 1, \ldots, m$ ist $h(c_i) = f_A(c_i) = \sum_{k=1}^{\ell} \alpha_{k,i} d_k$. Nun setzen wir ein und erhalten für $j = 1, \ldots, n$:

$$(h \circ g)(b_j) = h(\sum_{i=1}^{m} \beta_{i,j} c_i) = \sum_{i=1}^{m} \beta_{i,j} \sum_{k=1}^{\ell} \alpha_{k,i} d_k = \sum_{k=1}^{\ell} \sum_{i=1}^{m} \alpha_{k,i} \beta_{i,j} d_k = \sum_{k=1}^{\ell} \gamma_{k,j} d_k.$$

Hierbei haben wir sehr oft Distributivität und Kommutativität, also die Vektorraumgesetze, benutzt, um die Summationszeichen zu vertauschen. Wer skeptisch ist, kann die Korrektheit der vorgenommenen Vertauschung per Induktion über m und ℓ aus den Gesetzen, die über $m = 2$ und $\ell = 2$ sprechen, herleiten. □

Beispiel 3.25. Wir leiten aus Satz 3.21 und der Definition der Multiplikation eine wichtige Anwendung her: Nun nehmen wir den Spezialfall $V = K^n$, $W = K^m$ und die Standardbasen $\vec{B} = (e_1, \ldots, e_n)$ mit $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$ mit einer 1 an i-ter Stelle, und als Spaltenvektor, also als ein Element von $M_{n,1}$ aufgefasst. $\vec{C} = (e_1, \ldots, e_m)$. Sei $f\colon K^n \to K^m$ gegeben durch A. Dann stehen in der j-ten Spalte von A genau das f-Bild von e_j (als Spaltenvektor), d.h.,

$$f(\sum_{j=1}^{n} \xi_j e_j) = A \cdot \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}. \tag{3.1}$$

Konvention: Wir fassen die Multiplikation mit $A \in M_{n,m}(K)$ als Abbildung f_A von K^n in den K^m auf, eben als Multiplikation der Matrix von links aus an einen Spaltenvektor nach dem Muster (3.1). Wir schreiben auch φ_A hierfür, wenn $V = K^n$ mit der Standardbasis $\vec{B} = (e_1, \ldots, e_n)$ und $W = K^m$ mit der Standardbasis $\vec{C} = (e_1, \ldots, e_m)$.

Wir übertragen unsere Resultate über Nebenklassen, Umkehrbarkeit und Isomorphie auf $\varphi_A\colon K^n \to K^m$, $A \in M_{m,n}(K)$:

Korollar 3.26. *Sei $A \in M_{m,n}(K)$ und sei $H = \{x \in K^n \mid Ax = 0\}$. Dann gilt*

(1) Für jedes $b \in K^m$ ist $\{x \in K^n \mid Ax = b\}$ leer oder eine Nebenklasse von H.

(2) Falls $m < n$, so ist H nicht der Nullraum. Falls $m > n$, so hat nicht für jedes b die Gleichung $Ax = b$ eine Lösung.

(3) Falls $m = n$, so sind äquivalent:

- *(a) H ist der Nullraum.*
- *(b) $Ax = b$ ist lösbar für alle $b \in K^m$.*
- *(c) Für alle $b \in K^m$ gibt es höchstens ein $x \in K^m$ mit $Ax = b$.*

Definition 3.27. und Behauptungen

(1) Falls $A \in M_{m,m}(K)$ und der Fall (3) vorliegt, sagt man A ist regulär oder A ist invertierbar. Wir schreiben A^{-1} für die inverse Matrix. Dann ist $A^{-1}A = AA^{-1} = 1_{M_{m,m}(K)}$. Nicht reguläre quadratische Matrizen heißen auch ausgeartete Matrizen.

(2) $\mathrm{GL}_n(K)$ bezeichnet die Menge (oder auch, mit der Matrizenmultiplikation, die Gruppe) der regulären n-n-Matrizen über K. Die Gruppe $(\mathrm{GL}_n(K), \cdot)$ (mit der Matrizenmultiplikation $\cdot$) wird die allgemeine lineare Gruppe über K genannt, GL steht für general linear.

Die Gruppe $(\mathrm{GL}_n(K), \cdot)$ ist nicht abelsch für $n \geq 2$.

Definition 3.28. (1) Sei V ein endlichdimensionaler Vektorraum. Sei $f \in \mathrm{Hom}(V, W)$. Wir definieren den Rang von f als

$$\mathrm{rang}(f) = \dim(\mathrm{Im}(f)).$$

(2) Seien $m, n \in \mathbb{N} \setminus \{0\}$ und sei $A \in M_{m,n}(K)$. Wir definieren den Rang von A als die maximale Zahl linear unabhängiger Spalten von A. Dieser Rang wird manchmal auch Spaltenrang genannt.

Lemma 3.29. *Seien V, W endlichdimensional, $f \in \mathrm{Hom}(V,W)$, gegeben durch $f = f_A$ (bezüglich irgendwelcher geordneter Basen). Dann ist* $\mathrm{rang}(f) = \mathrm{rang}(A)$. *Außerdem ist* $\mathrm{rang}(A)$ *auch das k aus der Stufenform (das manchmal Zeilenrang genannt wird).*

Beweis: $\dim(\mathrm{Im}(f)) = \mathrm{rang}(A)$ fúr jedes A mit $A = \mathrm{Mat}_{\vec{B}}^{\vec{C}}(f)$. □

Lemma 3.30. *Sei $A \in M_{m,n}(K)$, $b \in K^m$. Die Gleichung $Ax = b$ ist genau dann lösbar, wenn* $\mathrm{rang}(A) = \mathrm{rang}(Ab)$. *Hierbei ist Ab die um die Spalte b erweiterte Matrix A.*

Beweis: $\mathrm{rang}(A) = \mathrm{rang}(Ab)$ gdw $b \in \mathrm{span}(\{a_1, \ldots, a_n\})$, wobei a_i die Spaltenvektoren aus A sind. $b \in \mathrm{span}(\{a_1, \ldots, a_n\})$ gdw $b \in \mathrm{Im}(f_A)$. □

3.3 Basiswechsel und Normalformen modulo Äquivalenz

Sei $\pi_{\vec{B}}(e_j) = b_j$ für $j = 1, \ldots, n$, $\pi_{\vec{C}}(e_i) = c_i$ für $i = 1, \ldots, m$, $\pi_{\vec{D}}(e_k) = d_k$ für $k = 1, \ldots, \ell$. Diese bestimmen Isomorphismen $\pi_{\vec{B}} \colon K^n \xrightarrow{\cong} U$, $\pi_{\vec{C}} \colon K^m \xrightarrow{\cong} V$, $\pi_{\vec{D}} \colon K^\ell \xrightarrow{\cong} W$.

Dann kommutiert folgendes Diagramm

$$\begin{array}{ccccc} U & \xrightarrow{h} & V & \xrightarrow{g} & W \\ \uparrow{\scriptstyle \pi_{\vec{B}}} & & \uparrow{\scriptstyle \pi_{\vec{C}}} & & \uparrow{\scriptstyle \pi_{\vec{D}}} \\ K^n & \xrightarrow{\varphi_{A_h}} & K^m & \xrightarrow{\varphi_{A_g}} & K^\ell \end{array} \tag{3.2}$$

Somit ist nach Satz 3.21 und Beispiel 3.25

$$\begin{aligned} A_h &= \mathrm{Mat}_{\vec{B}}^{\vec{C}}(h) \quad \text{und} \quad \varphi_{A_h} = \pi_{\vec{C}}^{-1} \circ h \circ \pi_{\vec{B}} \\ A_g &= \mathrm{Mat}_{\vec{C}}^{\vec{D}}(g) \quad \text{und} \quad \varphi_{A_g} = \pi_{\vec{D}}^{-1} \circ g \circ \pi_{\vec{C}}. \end{aligned}$$

Nach Satz 3.24 ist $A_{h \circ g} = A_h A_g$.

Nun setzen wir $V = W$ und $i(c_i) = d_i$. Dadurch wird ein Isomorphismus $i \colon V \to V$ bestimmt, ein sogenannter Basiswechsel. Dann ist $\mathrm{Mat}_{\vec{D}}^{\vec{C}}(i)$ die Einheitsmatix. Wie setzen $g = \mathrm{id}$ und erhalten aus der Multiplikationsformel

$$\mathrm{Mat}_{\vec{B}}^{\vec{D}}(h) = \mathrm{Mat}_{\vec{C}}^{\vec{D}}(\mathrm{id}) \cdot \mathrm{Mat}_{\vec{B}}^{\vec{C}}(h)$$

Im folgenden Lemma lernen wir, wie man $\mathrm{Mat}_{\vec{C}}^{\vec{D}}(\mathrm{id}) = M$ aus $\vec{D}$ und $\vec{C}$ berechnet. Nun setzen wir $U = V$ und $i(b_j) = c_j$ und $h = \mathrm{id}$ und erhalten aus der Multiplikationsformel

$$\mathrm{Mat}_{\vec{B}}^{\vec{D}}(g) = \mathrm{Mat}_{\vec{C}}^{\vec{D}}(g) \cdot \mathrm{Mat}_{\vec{B}}^{\vec{C}}(\mathrm{id})$$

Außerdem ist $\mathrm{Mat}_{\vec{B}}^{\vec{C}}(\mathrm{id})$ wieder aus $\vec{C}$ und $\vec{B}$ zu bestimmen.

Nach diesen Vorbetrachtungen wechseln wir die Basen auf beiden Seiten und erhalten:

Satz 3.31. *Satz von der Transformation bei Basiswechsel. Sei f bezüglich der Basen $\vec{B}$ und $\vec{C}$ gegeben durch $A_f = \mathrm{Mat}_{\vec{B}}^{\vec{C}}(f)$. Sei $h\colon \vec{B}' \to \vec{B}$ und sei $g\colon \vec{C} \to \vec{C}'$ Basiswechsel, d.h. $h(b_j) = b'_j$, $j = 1, \ldots, n$, und $g(c_j) = c'_j$, $i = 1, \ldots, m$. Hierbei schreiben wir die Matrizen zu den Basiswechseln als $\hat{B}$ mit*

$$\sum_{i=1}^{m} \xi_i b_i = \sum \xi'_i b'_i \ \textit{gdw}\ x' = \hat{B}x,$$

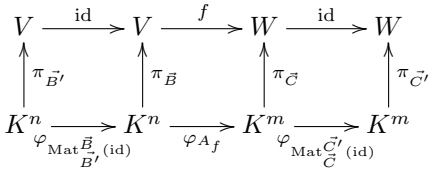
wobei x der Spaltenvektor aus $(\xi_1, \ldots, \xi_n)$ ist, und als $\hat{C}$ mit

$$\sum_{j=1}^{n} \zeta_j c_j = \sum_{j=1}^{n} \zeta'_j c'_j \ \textit{gdw}\ y' = \hat{C}y,$$

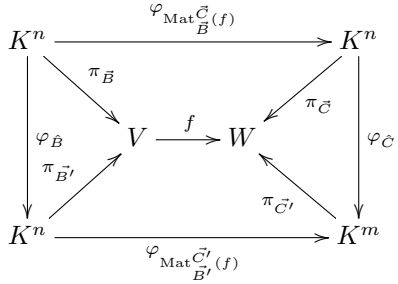
wobei y der Spaltenvektor aus $(\zeta_1, \ldots, \zeta_n)$ ist. Dann gilt

$$\begin{aligned} \mathrm{Mat}_{\vec{B}'}^{\vec{C}'}(f) &= \mathrm{Mat}_{\vec{C}}^{\vec{C}'}(\mathrm{id}) \cdot \mathrm{Mat}_{\vec{B}}^{\vec{C}}(f) \cdot \mathrm{Mat}_{\vec{B}'}^{\vec{B}}(\mathrm{id}) \\ &= \hat{C} \cdot \mathrm{Mat}_{\vec{B}}^{\vec{C}}(f) \cdot \hat{B}^{-1}. \end{aligned} \tag{3.3}$$

Beweis: Das Diagramm



oder auch das Diagramm



beschreibt die Voraussetzungen des Satzes. Nun folgt Gleichung (3.3) aus Satz 3.24

Wir geben noch einen alternativen Beweis, der mit den Rechenregeln in den Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{GL}_n(K)$ und der Assoziativität der Matrizenmultiplikation arbeitet (die ihrerseits wiederum auf Satz 3.24 bauen): Seien $\mathrm{Mat}_{\vec{B}}^{\vec{C}}(f) = A$ und $\mathrm{Mat}_{\vec{B}'}^{\vec{C}'}(f) = A'$. Seien x die Koordinaten von v bzgl. $\vec{B}$ und x' die Koordinaten von v bzgl. $\vec{B}'$. Seien y die Koordinaten von $f(v)$ bzgl. $\vec{C}$ und y' die Koordinaten von $f(v)$ bzgl. $\vec{C}'$. Dann ist $y = Ax$ und $y' = A'x'$. Nun ist $y' = \hat{C}y$ und $x' = \hat{B}x$, also $x = \hat{B}^{-1}x$. Also

$$y' = \hat{C}Ax = \hat{C}A\hat{B}^{-1}x'$$

und

$$A' = \hat{C}A\hat{B}^{-1}$$

□

Lemma 3.32. *über die zu einer Basistransformation gehörende Koordinatentransformation. Seien V ein n-dimensionaler Vektorraum und $\vec{B}$ und $\vec{B}'$ Basen von V. Sei*

$$\text{für } j = 1, \ldots, n \quad b'_j = \sum_{i=1}^{n} \alpha_{i,j} b_i. \tag{3.4}$$

Sei zu $x' = (\xi'_1, \ldots, \xi'_n)$ als Spaltenvektor der Spaltenvektor x gewählt, so dass

$$\sum_{j=1}^{n} \xi_j b_j = \sum_{j=1}^{n} \xi'_j b'_j. \tag{3.5}$$

Dann berechnet sich $x = (\xi_1, \ldots, \xi_n)$ aus $x' = (\xi'_1, \ldots, \xi'_n)$ wie folgt:

$$\xi_j = \sum_{i=1}^{n} \alpha_{j,i} \xi'_i. \tag{3.6}$$

Beweis: Der Koeffizient von b_j ist auf beiden Seiten von (3.5): $\xi_j = \sum_{i=1}^{n} \alpha_{i,j} \xi'_i$. Beachten Sie, dass in (3.6) alte Koordinaten durch neue ausgedrückt werden und dass die Matrix aus der Gleichung (3.4) transponiert verwendet wird: Es wird über den Zeilenindex summiert. □

Definition 3.33. (1) Seien $A, B \in M_{m,n}(K)$. A und B heißen äquivalent, wenn es ein reguläres $C \in M_{n,n}(K)$ und ein reguläres $D \in M_{m,m}(K)$ gibt, so dass

$$B = DAC^{-1}.$$

(2) Seien $f, g \in \mathrm{Hom}(V, W)$. f und g heißen äquivalent, wenn es ein invertierbares $h \in \mathrm{Hom}(V, V)$ und ein invertierbares $i \in \mathrm{Hom}(W, W)$ gibt, so dass

$$g = i \circ f \circ h^{-1}.$$

(3) Seien $A, B \in M_{m,m}(K)$. A und B heißen ähnlich oder konjugiert, wenn es ein reguläres $C \in M_{m,m}(K)$ gibt, so dass

$$B = CAC^{-1}.$$

(4) Seien $f, g \in \mathrm{End}(V)$. f und g heißen ähnlich oder konjugiert, wenn es ein invertierbares $h \in \mathrm{End}(V)$ gibt, so dass

$$g = h \circ f \circ h^{-1}.$$

Beobachtung 3.34. *(1) Seien $\vec{B}$ und $\vec{C}$ endliche geordnete Basen von V bzw. W. Dann sind f und $g \in \mathrm{Hom}(V, W)$ äquivalent gdw $\mathrm{Mat}_{\vec{B}}^{\vec{C}}(f)$ und $\mathrm{Mat}_{\vec{B}}^{\vec{C}}(g)$ äquivalent sind.*

(2) Sei $\vec{B}$ eine endliche geordnete Basis von V. Dann sind f und $g \in \mathrm{End}(V)$ ähnlich gdw $\mathrm{Mat}_{\vec{B}}^{\vec{B}}(f)$ und $\mathrm{Mat}_{\vec{B}}^{\vec{B}}(g)$ ähnlich sind.

(3) Die Äquivalenz von Matrizen, von Homomorphismen, und die Ähnlichkeit von quadratischen Matrizen, von Endomorphismen sind auf ihren jeweiligen Räumen Äquivalenzrelationen.

Satz 3.35. *von der Normalform modulo Äquivalenz, auch Normalform für lineare Abbildungen genannt. Sei $A \in M_{m,n}(K)$. Dann gibt es zu A eine äquivalente Matrix B der Form*

$$B = \begin{pmatrix} 1_{M_{k,k}(K)} & 0_{M_{k,n-k}(K)} \\ 0_{M_{m-k,k}(K)} & 0_{M_{m-k,n-k}(K)} \end{pmatrix} \tag{3.7}$$

Beweis: Wir nehmen eine Basis $b_{k+1}, \ldots, b_n$ von $\ker(f)$ und ergänzen sie um $b_1, \ldots, b_k$ zu einer Basis von V. Es sei $\vec{B} = (b_1, \ldots, b_n)$. Wir wählen $f(b_i) = c_i$ für $i = 1 \ldots, k$ und wählen einen komplementären Unterraum in W zu $\mathrm{Im}(f) = \mathrm{span}(\{c_1, \ldots, c_k\})$. Wir nehmen eine Basis $\{c_{k+1}, \ldots, c_m\}$ von W und setzen $\vec{C} = (c_1, \ldots, c_m)$. Dann ist $\mathrm{Mat}_{\vec{B}}^{\vec{C}}(f)$ in der Form (3.7). □

Korollar 3.36. *Eine m-n-Matrix A hat genau dann Rang k, wenn es eine reguläre n-n-Matrix B und eine eine reguläre m-m-Matrix C gibt, so dass CAB die Gestalt* (3.7) *hat*

Definition 3.37. Die n-n-Elementarmatrizen $E_{i,j}^{\lambda}$: Für $i, j = 1, \ldots, n$, $i \neq j$ und $\lambda \in K$ definieren wir $E_{i,j}^{\lambda} = (\alpha_{i',j'})_{i',j'=1,\ldots,n}$ wie folgt:

$$\alpha_{i',j'} = \begin{cases} \delta_{i',j'}, & \text{für } (i',j') \neq (i,j); \\ \lambda, & \text{für } (i',j') = (i,j). \end{cases}$$

Für $i = 1, \ldots, n$, $\lambda \in K \setminus \{0\}$ definieren wir $E_{i,i}^{\lambda} = E_i^{\lambda} = (\alpha_{i',j'})_{i',j'=1,\ldots,n}$ wie folgt:

$$\alpha_{i',j'} = \begin{cases} \delta_{i',j'}, & \text{für } (i',j') \neq (i,i); \\ \lambda, & \text{für } (i',j') = (i,i). \end{cases}$$

Lemma 3.38. *Sei $A \in M_{m,n}(K)$. Die Rechtsmultiplikation mit einer Elementarmarix aus $M_{n,n}(K)$ entspricht einer Spaltenumformung Die Bildung von $AE_{i,j}^{\lambda}$ für $i \neq j$ addiert das λ-fache der i-ten Spalte von A zur j-ten Spalte. Die Bildung von AE_i^{λ} bildet das λ-fache der i-ten Spalte. Die Linksmultiplikation $E_{i,j}^{\lambda}A$ für $i \neq j$ addiert das λ-fache der j-ten Zeile zur i-ten Zeile von A. Die Bildung von $E_i^{\lambda}A$ bildet das λ-fache der i-ten Zeile.*

Beweis: Wir rechnen die Linksmultiplikation für $i \neq j$ nach: Seien $B = (\beta_{i',j'})$ eine m-n-Matrix, $E_{i,j}^{\lambda} = (\alpha_{k,i'})$ eine m-m-Matrix und

$$(\gamma_{k,j'})_{k=1,\ldots,m,j'=1,\ldots,n} = E_{i,j}^{\lambda} \cdot B.$$

Dann ist für $k = 1, \ldots, m$ mit $k \neq i$, $j' = 1, \ldots, n$, $\gamma_{k,j'} = \sum_{i'=1}^{m} \alpha_{k,i'}\beta_{i',j'} = \beta_{k,j'}$. Alle Zeilen außer eventuell der i-ten Zeile von B bleiben also unverändert durch die Multiplikation von links mit $E_{i,j}^{\lambda}$.

Sei nun $k = i$. Dann ist für $j' = 1, \ldots, n$, $\gamma_{i,j'} = \sum_{i'=1}^{m} \alpha_{i,i'}\beta_{i',j'} = \beta_{i,j'} + \lambda\beta_{j,j'}$ Das λ-fache der $j$ten Zeile wurde zur i-ten Zeile von B addiert.

Wir rechnen nun die Rechtsmultiplikation für $i \neq j$ nach: Seien $B = (\beta_{i',j'})$ eine m-n-Matrix, $E_{i,j}^{\lambda} = (\alpha_{k,i'})$ eine n-n-Matrix und

$$(\gamma_{k,j'})_{k=1,\ldots,m,j'=1,\ldots,n} = B \cdot E_{i,j}^{\lambda}.$$

Dann ist für $k = 1, \ldots, m$, $j' = 1, \ldots, n$, $j' \neq j$, $\gamma_{k,j'} = \sum_{i'=1}^{m} \beta_{k,i'}\alpha_{i',j'} = \beta_{k,j'}$. Alle Spalten außer eventuell der j-ten Spalte von B bleiben also unverändert durch die Multiplikation von rechts mit $E_{i,j}^{\lambda}$.

Sei nun $j' = j$. Dann ist für $k = 1, \ldots, m$, $\gamma_{k,j} = \sum_{i'=1}^{m} \beta_{k,i'}\alpha_{i',j} = \beta_{k,j} + \lambda\beta_{k,i}$ Das λ-fache der i-ten Spalte wurde zur j-ten Spalte von B addiert. □

Lemma 3.39. $(E_{i,j}^{\lambda})^{-1} = E_{i,j}^{-\lambda}$ *für $i \neq j$ und* $(E_i^{\lambda})^{-1} = E_i^{\frac{1}{\lambda}}$. *Die Umkehrungen von Elementarmatrizen sind also wieder Elementarmatrizen.*

Induktiv über die Dimension n zeigt man:

Lemma 3.40. *Jede reguläre n-n-Matrix lässt sich als Produkt von endlich vielen Elementarmatrizen schreiben.*

Beweis: Für $n = 1$ ist $A = (\lambda)$ und $\lambda \neq 0$, also ist $A = E^{\lambda}_{1,1}$. Sei $A \in M_{n+1,n+1}(K)$ regulär. Die Vertauschung zweier Zeilen lässt sich durch Heranmultiplizieren geeigneter Elementarmatrizen von links durchführen. Wir bilden wir mit geeigneten ζ_k, i_k, $k = 1, \ldots, n+1$,

$$A' = E^{\zeta_1}_{n+1,i_1} \cdot \cdots \cdot E^{\zeta_{n+1}}_{n+1,i_{n+1}} \cdot A,$$

so dass die letzte Zeile von A' wie $(0, \ldots, 0, 1)$ als Spalte geschrieben aussieht. Hierbei sind gegebenfalls zwischen die $E^{\zeta_{i_k}}_{n+1,i_k}$ Zeilenvertauschungen einzuschalten, wenn in allen Zeilen außer der letzten in der entsprechenden Spalte eine 0 steht. Danach bilden wir mit geeigneten ξ_i, $i = 1, \ldots, n$,

$$B = E^{\xi_1}_{1,n+1} \cdot \cdots \cdot E^{\xi_n}_{n,n+1} \cdot A',$$

so dass die letzte Spalte von B wie $(0, \ldots, 0, 1)$ als Spalte aussieht. Außerdem bleibt die letzte Zeile von B gleich wie die letzte Zeite von A'. Nun wenden wir die Induktionsvoraussetzung auf $B_{\text{kurz}} = B \restriction \{1, \ldots, n\} \times \{1, \ldots, n\}$ an. Diese liefert: B_{kurz} ist ein Produkt von (endlich vielen) n-n-Elementarmatizen. Wir fügen zu jeder dieser Elementarmatrizen als letzte Zeile $(0, \ldots, 0)$ der Länge n an und dann als $n+1$-te Spalte $(0, \ldots, 0, 1)$ der Länge $n+1$ als Spalte. So erhalten wir $n+1$-$n+1$-Elementarmatrizen, deren Produkt gerade B ist. Da das Inversen einer Elementarmatrix wieder eine Elementarmatrix ist, erhalten wir aus der Darstellung von B eine Darstellung von A. □

Korollar 3.41. *Jede m-n-Matrix lässt sich durch Zeilen- und Spaltenumformungen in die Gestalt 3.7 bringen.*

Satz 3.42. *Seien U, V K-Vektorräume der Dimension m und n und, sei $f\colon V \to W$ eine lineare Abbildung vom Rang k. In V sei eine angeordnete Basis $\vec{B}$ fixiert. Dann kann man $\vec{B}$ zu einer angeordneten Basis $\vec{B}'$ umordnen und eine angeordnete Basis $\vec{C}$ von W wählen, so dass f bezüglich der neuen angeordneten Basen durch eine Matrix in Form*

$$B = \begin{pmatrix} 1_{M_{k,k}(K)} & *_{M_{k,n-k}(K)} \\ 0_{M_{m-k,k}(K)} & 0_{M_{m-k,n-k}(K)} \end{pmatrix} \tag{3.8}$$

dargestellt wird. Hierbei ist $*_{M_{k,n-k}(K)}$ eine beliebige Matrix in $M_{k,n-k}(K)$.

Beweis: Sei B gegeben. Wir nehmen eine Basis $b'_{k+1}, \ldots, b'_n$ von $\ker(f)$ und ergänzen sie um $b_1 \in B$, …, $b_k \in B$ zu einer Basis von V. Danach ergänzen wir wiederum $\{b_1, \ldots, b_k\}$ mit Elementen $b_{k+1}, \ldots, b_n$ aus B zu einer Basis $\vec{B}$, die eine Anordnung von B ist. Die letzteren sind allerdings nicht mehr aus dem Kern. Wir wählen $f(b_i) = c_i$ für $i = 1 \ldots, k$ und wählen einen komplementären Unterraum W' in W zu $\mathrm{Im}(f) = \mathrm{span}(\{c_1, \ldots, c_k\})$. Wir nehmen eine Basis $\{c_{k+1}, \ldots, c_m\}$ von W'. Dann ist $\mathrm{Mat}^{\vec{C}}_{\vec{B}}(f)$ in der Form (3.8). □

Verzichtet man auf Multiplikation von rechts, d.h. auf Spaltenumformungen, und verzichtet man auch auf die eben noch gestatteten Spaltenvertauschungen, so erhält man wieder das Ergebnis des Gauß-Algorithmus: Die Stufenform vom Beginn des zweiten Kapitels:

Satz 3.43. *Seien U, V K-Vektorräume der Dimension m und n und, sei $f\colon V \to W$ eine lineare Abbildung vom Rang k. In V sei eine angeordnete Basis $\vec{B}$ fixiert. Dann kann man eine angeordnete Basis $\vec{C}$ von W wählen, so dass f bezüglich der neuen Basen durch eine Matrix in Stufenform hat.*

Beweis: Ändern der Basis $\vec{C}$ auf der Bildseite geschieht durch Heranmultiplizieren von links an $\mathrm{Mat}_{\vec{B}}^{\vec{C}}$. Heranmultiplizieren von links ist gleichwertig mit Zeilenumformungen. □

Je zwei ähnliche Matrizen sind äquivalent. Die Ähnlichkeit ist eine viel feinere Äquivalenzrelation als die Äquivalenz von Matrizen, d.h. viele Ähnlichkeitsklassen von Matrizen vereinigt ergeben eine Äquivalenzklasse bzgl. der „Äquivalenz" genannten Äquivalenzrelation von Matrizen. Besonders einfache Vertreter der Ähnlichkeitsklassen, die Normalformen (modulo Ähnlichkeit) genannt werden, untersuchen wir im Kapitel über die Jordan'sche Normalform.

Definition 3.44. Sei K ein Körper. Eine K-Algebra [mit Eins] ist eine Struktur

$$(A, K, +_K, \cdot_K, +, \cdot, \cdot_s),$$

so dass

(1) $(A, K, +_K, \cdot_K, +, \cdot_s)$ ein K-Vektorraum ist, und

(2) $(A, +, \cdot)$ ein Ring [mit Eins] ist, und

(3) $\forall \lambda \in K \forall a, b \in A (\lambda \cdot_s a) \cdot b = \lambda \cdot_s (a \cdot b) = a \cdot (\lambda \cdot_s b)$.

Lemma 3.45. *(1) Sei V ein K-Vektorraum. Dann ist $(\mathrm{End}(V), K, +_K, \cdot_K, +, \circ, \cdot_s)$ eine K-Algebra.*

(2) Sei $n \in \mathbb{N}$. Der Vektorraum $M_{n,n}(K)$ bildet mit der Matrizenmultiplikation als zusätzlichem Strukturmerkmal eine K-Algebra.

Definition 3.46. (Vektorraum-)Isomorphismen von V nach V heißen (Vektorraum-)Automorphismen. Mit $\mathrm{Aut}(V)$ bezeichnet man die Menge der Automorphismen oder auch die K-Algebra $(\mathrm{Aut}(V), K, +_k, \cdot_K, +, \circ, \cdot_s)$.

Satz 3.47. *Sei V n-dimensional, und sei $\vec{B}$ eine geordnete Basis von V. Dann ist*

$$\begin{aligned} \mathrm{Mat}_{\vec{B}}^{\vec{B}}\colon \mathrm{End}(V) &\to M_n(K), \\ f &\mapsto \mathrm{Mat}_{\vec{B}}^{\vec{B}}(f) \end{aligned}$$

ein K-Algebren-Isomorphismus, der $\mathrm{Aut}(V)$ auf $\mathrm{GL}_n(K)$ abbildet.

Beweis: Satz 3.21 und Satz 3.24 zusammen. □

Lemma 3.48. *Rechenregel. Sei $A \in M_{m,n}(K)$, $B \in M_{m,\ell}(K)$. Wir schreiben $(A \mid B) \in M_{m,n+\ell}(K)$ für die Hintereinanderschreibung von A und B. Sei $C \in M_{m,m}(K)$. Dann ist $C(A \mid B) = (CA \mid CB)$. Analoges gilt für die Untereinanderschreibung von Matrizen mit gleicher Spaltenzahl n und Heranmultiplizieren von n-n-Matrizen von rechts.*

Anwendung: $Ax = b$ gdw $(CA)x = Cb$. Man stellt C so aus Elementarmatrizen her, dass CA eine einfache Form hat.

Literaturverzeichnis

[1] E. Artin. *Geometric algebra*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1988. Reprint of the 1957 original, A Wiley-Interscience Publication.

[2] Victor Bangert. *Lineare Algebra 2006/2007, Vorlesungsskript*. http://home.mathematik.uni-freiburg.de/geometrie/bangert. Universität Freiburg, 2007.

[3] Andreas Blass. Existence of bases implies the axiom of choice. In *Axiomatic set theory (Boulder, Colo., 1983)*, volume 31 of *Contemp. Math.*, pages 31–33. Amer. Math. Soc., Providence, RI, 1984.

[4] Egbert Brieskorn. *Lineare Algebra und analytische Geometrie. I*. Friedr. Vieweg & Sohn, Braunschweig, 1983. With historical notes by Erhard Scholz.

[5] Theodor Bröcker. *Lineare Algebra und analytische Geometrie*. Grundstudium Mathematik. [Basic Study of Mathematics]. Birkhäuser Verlag, Basel, 2003. Ein Lehrbuch für Physiker und Mathematiker. [A textbook for physicists and mathematicians].

[6] H.-D. Ebbinghaus. *Einführung in die Mengenlehre*. Hochschultaschenbuch, 4 edition, 2003.

[7] Sebastian Goette. *Lineare Algebra 2012/2013, Vorlesungsskript*. http://home.mathematik.uni-freiburg.de/frank/index.de.html. Universität Freiburg, 2013.

[8] Werner Greub. *Linear algebra*. Springer-Verlag, New York, fourth edition, 1975. Graduate Texts in Mathematics, No. 23.

[9] Klaus Jänich. *Linear algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1994.

[10] Max Koecher. *Lineare Algebra und analytische Geometrie*, volume 2 of *Grundwissen Mathematik [Basic Knowledge in Mathematics]*. Springer-Verlag, Berlin, 1983.

[11] Hans-Joachim Kowalsky. *Lineare Algebra*. Walter de Gruyter, Berlin-New York, 1977. Achte Auflage, de Gruyter Lehrbuch.

[12] Kenneth Kunen. *Set theory*, volume 34 of *Studies in Logic (London)*. College Publications, London, 2011.

[13] Emmy Noether. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Math. Ann.*, 96(1):26–61, 1927.

[14] Ernst Steinitz. Zur Theorie der Moduln. *Math. Ann.*, 52(1):1–57, 1899.

[15] Ernst Zermelo. Beweis, daß jede Menge wohlgeordnet werden kann. *Math. Ann.*, 59:514–516, 1904.

[16] Martin Ziegler. *Mathematische Logik*. Mathematik kompakt. Birkhäuser, 2010.

[17] Martin Ziegler. *Lineare Algebra, Vorlesungsskript*. http://home.mathematik.uni-freiburg.de/ziegler. Universität Freiburg, 2012.

[18] Max Zorn. A remark on a method in transfinite algebra. *Bull. Amer. Math. Soc. N.S.*, 41:667–670, 1935.

Symbole

Begriffe und Namen