

Lineare Algebra I

Vorlesung bei Prof. Dr. W. Decker

Skript zur Vorlesung Lineare Algebra I im Wintersemester 2000 an der UdS.
Für Hinweise auf Tipp- sowie Kontextfehler bedanken wir uns im Voraus.
gesetzt mit $\text{\LaTeX}$ 2 ϵ

email:

cyberoli@studcs.uni-sb.de
mkaiser@studcs.uni-sb.de
mjung@studcs.uni-sb.de
seki0001@stud.uni-saarland.de
decker@math.uni-sb.de

13. Februar 2001, Oliver Barth, Martin Kaiser, Marko Jung, Sebastian Kirsch
Korrektur und Ergänzungen Prof. Dr. W. Decker
Die Autoren übernehmen keine Haftung für den Inhalt.

Inhaltsverzeichnis

0	Motivation	5
1	Mengen, Abbildungen und Relationen	13
	Aufgaben	22
2	Gruppen, Ringe, Körper	27
	Aufgaben	29
	Aufgaben	38
	Aufgaben	47
	Aufgaben	53
	Aufgaben	62
3	Vektorräume, Basis, Dimension	65
	Aufgaben	72
	Aufgaben	79
	Aufgaben	89
4	Lineare Abbildungen und Matrizen, lineare Gleichungssysteme	91
5	Determinanten	135

Kapitel 0

Motivation

Das Wort Algebra entstand aus dem Titel eines arabischen Werkes von Muhammed ibn Mûsâ Alchwarizmî aus dem ersten Viertel des 9. Jahrhunderts nach Christus. Naiv können wir sagen:

Algebra ist die mathematische Wissenschaft, die sich mit dem Lösen von algebraischen Gleichungen beschäftigt.

Eine typische algebraische Gleichung ist etwa

$$x^3 - 6x^2 + 11x - 6 = 0.$$

Sie hat die drei Lösungen

$$x = 1, x = 2 \quad \text{und} \quad x = 3.$$

Diese Lösungen sind wie die *Koeffizienten* 1, -6, 11, -6 ganze Zahlen. Hingegen hat

$$x^3 - 6x^2 + 11x - 5 = 0$$

auch ganzzahlige Koeffizienten, aber keine ganzzahlige Lösungen. Sucht man Lösungen in größeren Zahlbereichen, so erhält man zunächst die irrationale Lösung

$$x = 2 - \frac{1}{6} \sqrt[3]{108 - 12\sqrt{69}} - \frac{1}{6} \sqrt[3]{108 + 12\sqrt{69}}.$$

Zwei weitere Lösungen ergeben sich, wenn man nicht nur reelle, sondern auch komplexe Zahlen als Lösungen zulässt.

Allgemeiner kann man Gleichungen der Form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1}$$

betrachten. Dabei sind die *Koeffizienten* a_i Zahlen aus einem bestimmten Zahlbereich, etwa ganze oder rationale oder reelle oder komplexe Zahlen, und x ist eine *Unbestimmte* (oder *Variable*). Eine *Lösung* von (1) ist eine Zahl, die die Gleichung erfüllt, wenn man sie an Stelle von x einsetzt. Eine Gleichung wie (1) heißt auch *algebraische Gleichung in einer Unbestimmten* x . Ist $a_n \neq 0$ so nennt man n den *Grad der Gleichung*.

Ein Ausdruck $p(x)$ der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,$$

heißt *Polynom vom Grade n* in der *Unbestimmten x* mit *Koeffizienten a_i* in einem gegebenen Zahlbereich. Die Lösungen von $p(x) = 0$ nennt man die *Nullstellen* von p .

Noch allgemeiner betrachtet man *Polynome in mehreren Variablen*, etwa in den zwei Variablen x und y :

$$p(x,y) = \sum_{i=0}^n \sum_{j=0}^m c_{ij} x^i y^j.$$

Die Nullstellen von p sind Lösungen der Gleichung

$$p(x,y) = 0.$$

Wir setzen im folgenden einmal voraus, daß die Koeffizienten c_{ij} reelle Zahlen sind, und lassen als Lösungen auch nur Paare reeller Zahlen zu. Dann können wir die Lösungen als Punkte in der Ebene mit den cartesischen Koordinaten (x,y) deuten.

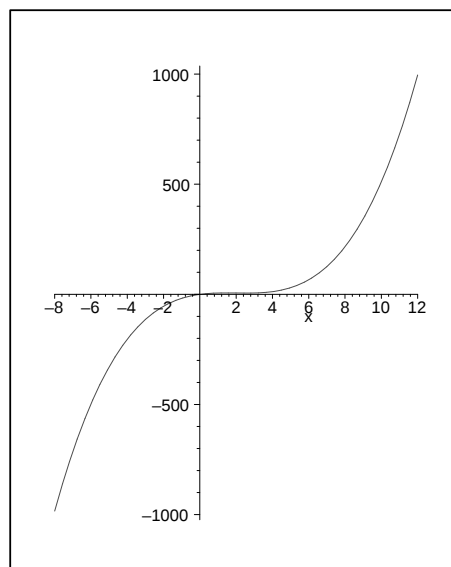
Beispiel 0.1. Wir betrachten die Gleichung

$$x^3 - 6x^2 + 11x - y = 0.$$

Diese können wir in die folgende Form bringen:

$$y = x^3 - 6x^2 + 11x.$$

Die Lösungen stellen dann eine *algebraische Kurve* dar.



□

Eine Gleichung $p(x,y) = 0$ hat im Allgemeinen also unendlich viele Lösungen, nämlich alle Punkte der entsprechenden ebenen Kurve. Anders sieht die Sache aus, wenn wir ein System von zwei algebraischen Gleichungen in zwei Unbekannten betrachten:

$$\begin{aligned} p(x,y) &= 0 \\ q(x,y) &= 0 \end{aligned} \quad (2)$$

Zu diesen Gleichungen gehören die zwei Kurven der Nullstellenmengen

$$\begin{aligned} C &= \{(x,y) \mid p(x,y) = 0\} , \\ D &= \{(x,y) \mid q(x,y) = 0\} . \end{aligned}$$

Lösungen von (2) entsprechen genau den Punkten im Durchschnitt der Kurven

$$C \cap D.$$

Wenn diese Kurven nicht ganze “Stücke” gemeinsam haben, so kann man erwarten, daß $C \cap D$ nur aus endlich vielen Punkten besteht. Beliebige algebraische Gleichungen $p(x,y) = 0$, d.h. beliebige ebene algebraische Kurven, studiert man in der *algebraischen Geometrie*. Im Rahmen unserer Vorlesung hier beschäftigen wir uns nur mit den allereinfachsten Kurven, den Geraden (lateinisch: *linea*):

$$ax + by = \alpha.$$

Wir sprechen auch von einer *linearen Gleichung*. Betrachten wir wie oben zwei solche Gleichungen, so erhalten wir ein *System von zwei linearen Gleichungen in zwei Variablen*:

$$\begin{aligned} ax + by &= \alpha \\ cx + dy &= \beta \end{aligned} \quad (3)$$

Geometrisch lassen sich die Lösungen durch Betrachten von

$$\begin{aligned} L &= \{(x,y) \mid ax + by = \alpha\} , \\ L' &= \{(x,y) \mid cx + dy = \beta\} \end{aligned}$$

beschreiben. Setzen wir für den Augenblick voraus, daß $(a,b) \neq (0,0)$ und $(c,d) \neq (0,0)$, so sind L und L' Geraden in der (x,y) -Ebene, und für den Durchschnitt $L \cap L'$ sind drei Fälle möglich:

- (i) L und L' sind nicht parallel, d.h. $L \cap L'$ besteht aus genau einem Punkt.
- (ii) L und L' sind parallel und verschieden, d.h. $L \cap L' = \emptyset$.
- (iii) L und L' sind gleich, d.h. $L \cap L' = L = L'$ ist eine Gerade.

Für (3) bedeutet dies:

- (i) Es gibt genau eine Lösung.

(ii) Es gibt keine Lösung.

(iii) Es gibt unendlich viele Lösungen.

Um herauszufinden, unter welchen algebraischen Bedingungen die Fälle (i), (ii) und (iii) eintreten, formen wir (3) um: Multiplikation mit d , b , c und a liefert

$$\begin{aligned}adx + bdy &= d\alpha \\bcx + bdy &= b\beta \\acx + bcy &= c\alpha \\acx + ady &= a\beta \quad .\end{aligned}$$

Durch Subtraktion ergibt sich

$$\begin{aligned}(ad - bc)x &= (\alpha d - b\beta) \\(ad - bc)y &= (a\beta - \alpha c).\end{aligned}\tag{4}$$

Fall A. $(ad - bc) \neq 0$.

Dann hat (4) und damit auch (3) genau eine Lösung, es liegt also der Fall (i) vor. Die Zahl $ad - bc$ ist offensichtlich eine wichtige Größe, die dem Schema der Koeffizienten a, b, c, d des Gleichungssystems zugeordnet ist. Wir schreiben das Koeffizientenschema auch in Form einer *Matrix*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Die Zahl $ad - bc$ heißt die *Determinante* des Koeffizienten-Schemas bzw. der Matrix, wir schreiben

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Für die eindeutig bestimmte Lösung (x, y) von (3) hat man

$$x = \frac{\begin{vmatrix} \alpha & b \\ \beta & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, \quad y = \frac{\begin{vmatrix} a & \alpha \\ c & \beta \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}$$

(*Cramersche Regel*, 1750). □

Wenn die Determinante verschwindet, gibt es zwei mögliche Fälle.

Fall B. $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 0$ und $\begin{vmatrix} \alpha & b \\ \beta & d \end{vmatrix} \neq 0$ oder $\begin{vmatrix} a & \alpha \\ c & \beta \end{vmatrix} \neq 0$.

Hier hat (4) und somit auch (3) keine Lösung, es liegt also der Fall (ii) vor. □

Fall C. $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} \alpha & b \\ \beta & d \end{vmatrix} = \begin{vmatrix} a & \alpha \\ c & \beta \end{vmatrix} = 0.$

Nach Voraussetzung gilt $(a, b) \neq (0, 0)$ und $(c, d) \neq (0, 0)$. Sei ohne Beschränkung der Allgemeinheit $a \neq 0$. Dann ist auch $c \neq 0$, denn sonst wäre wegen $ad - bc = 0$ auch $d = 0$ im Widerspruch zu $(c, d) \neq (0, 0)$. Also sind a und c ungleich 0. Deswegen hat (3) dieselben Lösungen wie

$$\begin{aligned} acx + bcy &= c\alpha \\ acx + ady &= a\beta \end{aligned} \quad .$$

Diese Gleichungen sind aber im Falle C identisch, wir erhalten als Lösungen alle Punkte auf der Geraden

$$ax + by = \alpha. \quad \square$$

Fall A entspricht also (i), Fall B entspricht (ii) und Fall C entspricht (iii). Wir haben die verschiedenen Möglichkeiten für die Lösungen unseres linearen Gleichungssystems eindeutig durch Determinantenbedingungen charakterisiert, und damit die Theorie von zwei linearen Gleichungen mit zwei Unbekannten im Wesentlichen erledigt.

In der Praxis hat man es häufig mit sehr viel größeren Gleichungssystemen zu tun (mehrere hundert Unbekannte). Es ist deswegen wichtig, systematische Schreibweisen einzuführen. Für die Variablen benutzen wir indizierte Buchstaben, etwa $x_1, \dots, x_n$, für die Koeffizienten benutzen wir doppelt indizierte Buchstaben, etwa $a_{11}, \dots, a_{1n}, \dots, a_{mn}$. Ein System von m linearen Gleichungen in n Unbestimmten geben wir meist in der folgenden Form an:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

Dabei sind die Koeffizienten a_{ij} bestimmte "Zahlen" aus einem im Kontext festgelegten Zahlbereich K , meist aus einem bestimmten Körper (z.B. aus dem Körper der reellen Zahlen). Ebenso sind die b_i bestimmte Zahlen aus diesem Zahlbereich. Eine Lösung des Gleichungssystems ist ein System von n Zahlen $c_1, \dots, c_n$ aus K , so daß beim Einsetzen von $c_1, \dots, c_n$ statt der Unbestimmten $x_1, \dots, x_n$ die Gleichungen des Systems identisch erfüllt sind. Beim Betrachten von Gleichungen in zwei Variablen haben wir zwei Zahlen (Variable) zu einem Paar (x_1, x_2) zusammengefasst. Analog bildet man Tripel (x_1, x_2, x_3) und allgemeiner n -Tupel $(x_1, \dots, x_n)$ von Zahlen (Variablen). Ebenso fassen wir die Koeffizienten a_{ij} zu einer Matrix (a_{ij}) zusammen. Diese stellt man sich als rechteckige Anordnung von Elementen a_{ij} vor:

$$A = (a_{ij}) = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

Die a_{ij} heißen die Koeffizienten der Matrix. Liegen diese alle in einem Zahlbereich K , so sprechen wir von einer Matrix mit Koeffizienten in K . Die Zahlen $a_{i1}, a_{i2}, \dots, a_{in}$ bilden die i -te Zeile von (a_{ij}) , die Zahlen $a_{1j}, \dots, a_{mj}$ die j -te Spalte von (a_{ij}) :

$$\begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{m1} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix} \leftarrow \begin{matrix} \text{i-te Zeile} \\ \uparrow \\ \text{j-te Spalte} \end{matrix}$$

Eine Matrix $(a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ heißt $m \times n$ -Matrix. Die Menge aller $m \times n$ -Matrizen mit Koeffizienten in K bezeichnen wir mit $M(m \times n, K)$. Die Menge aller n -Tupel $(c_1, \dots, c_n)$ von Zahlen $c_1, \dots, c_n$ aus K wird mit K^n bezeichnet.

Zusammenfassung 0.2. Ein System von m linearen Gleichungen in n Unbekannten mit Koeffizienten in K wird durch zwei Daten gegeben. Eine Koeffizientenmatrix $a_{ij} \in M(m \times n, K)$ und ein m -Tupel $(b_1, \dots, b_m) \in K^m$. Die Lösungen des Gleichungssystems sind n -Tupel $(x_1, \dots, x_n) \in K^n$. $\square$

Ist ein lineares Gleichungssystem gegeben, so stellen wir uns folgende Fragen:

- Hat das Gleichungssystem Lösungen?
- Wie viele Lösungen hat das System?
- Wie findet man die Lösungen?

Diese Fragen haben wir für 2×2 -Matrizen mit Hilfe von Determinantenbedingungen beantwortet. Später werden wir unter anderem allgemein für $n \times n$ -Matrizen Determinanten definieren und damit eine mögliche Antwort auf obige Fragen geben. Allgemein kann man sagen: Die *Aufgabe der linearen Algebra* ist es, eine systematische Theorie der Lösung linearer Gleichungssysteme zu entwickeln. In diesem Zusammenhang stößt man automatisch auf eine bestimmte Struktur, nämlich die *Vektorraumstruktur*. Betrachten wir einmal ein *homogenes lineares Gleichungssystem*, d.h. ein solches, bei dem die rechte Seite verschwindet:

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ \vdots & \\ a_{m1}x_1 + \dots + a_{mn}x_n &= 0 \end{aligned} \tag{5}$$

Eine einzelne Gleichung

$$a_{i1}x_1 + \dots + a_{in}x_n = 0$$

können wir mit einem beliebigen $a \in K$ multiplizieren und erhalten die Gleichung

$$a_{i1}ax_1 + \dots + a_{in}ax_n = 0.$$

Also ist mit $x_1, \dots, x_n$ auch $ax_1, \dots, ax_n$ eine Lösung von (5). Für n -Tupel definieren wir deswegen auch

$$a(x_1, \dots, x_n) := (ax_1, \dots, ax_n).$$

Analog erhalten wir durch addieren der Gleichungen: Mit $(x_1, \dots, x_n)$ und $(y_1, \dots, y_n)$ ist auch

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n)$$

eine Lösung von (5). Diese *Skalarmultiplikation* und *Addition* erfüllen gewisse Rechenregeln (in Abhängigkeit von Rechenregeln für unseren Zahlbereich K). Schreiben wir abkürzend $x = (x_1, \dots, x_n)$ sowie $\Rightarrow$ für “daraus folgt”, so gilt also:

$$\begin{array}{llll} x \text{ Lösung, } a \text{ Zahl in } K & \Rightarrow & ax & \text{Lösung} \\ x, y \text{ Lösungen} & \Rightarrow & x + y & \text{Lösung.} \end{array}$$

Daraus folgt auch:

$$x, y \text{ Lösungen, } a, b \text{ Zahlen in } K \Rightarrow ax + by \text{ Lösung.}$$

Wir nennen $ax + by$ eine *Linearkombination* von x und y .

Zusammenfassung 0.3. Linearkombinationen von Lösungen von (5) sind also wieder Lösungen. Durch oben definierte Skalarmultiplikation und Addition erhalten wir eine Struktur auf der Menge V aller Lösungen. Die Eigenschaften dieser Struktur hängen von denen von K ab. Wir werden später sehen: Ist z.B. K ein *Körper*, so ist V ein *K -Vektorraum*. $\square$

Wir wollen nun die Motivation beenden und darangehen, uns die angesprochenen Begriffe mathematisch exakt zu erarbeiten. Dabei verwenden wir:

Definition 0.4 (Logische Schreibweisen).

$\forall$: für alle

$\exists$: es existiert

$\Rightarrow$: daraus folgt

$\Leftrightarrow$: genau dann wenn

$\square$

Aufgaben

Aufgabe 0. Bestimmen Sie sowohl geometrisch, d.h. durch Zeichnen der entsprechenden Geraden, als auch algebraisch, d.h. mit Hilfe von Determinantenbedingungen, alle Lösungen der folgenden linearen Gleichungssysteme:

(i)

$$2x + 3y = 4$$

$$5x + 6y = 7$$

(ii)

$$2x + 3y = 4$$

$$4x + 6y = 7$$

(iii)

$$2x + 3y = 4$$

$$4x + 6y = 8$$

Kapitel 1

Mengen, Abbildungen und Relationen

Wir wollen hier nicht auf die schwierige Frage eingehen, wie der Begriff “Menge” erklärt werden kann. Das ist Gegenstand der mathematischen Grundlagenforschung. Naiv könnte man sagen: Eine wohlbestimmte Gesamtheit von Objekten heißt eine *Menge*, die Objekte selbst heißen die *Elemente* oder gelegentlich auch die *Punkte* dieser Menge. Zwei Mengen heißen *gleich*, wenn sie dieselben Elemente haben.

Natürlich ist dies keine exakte mathematische Definition, da Begriffe wie wohlbestimmt oder Gesamtheit nicht näher erläutert wurden. Mit Problemen dieser Art wollen wir uns hier nicht beschäftigen. Für die lineare Algebra genügt es, einige elementare Regeln und Bezeichnungen zu erläutern.

Endliche Mengen kann man im Prinzip durch eine vollständige Liste ihrer Elemente angeben. Wir schreiben

$$X = \{x_1, \dots, x_n\},$$

wenn die Menge X aus den Elementen $x_1, \dots, x_n$ besteht. Dabei müssen die Elemente nicht notwendig verschieden sein und die Reihenfolge ist gleichgültig. Es ist etwa

$$\{1, 2, 3, 1\} = \{1, 2, 3\} = \{2, 1, 3\}.$$

$x_1, \dots, x_n$ heißen *paarweise verschieden*, wenn $x_i \neq x_j$ für $i \neq j$. In diesem Fall ist X eine *n-elementige* Menge. Ein erstes Beispiel einer unendlichen Menge ist die Menge

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}$$

der *natürlichen Zahlen* einschließlich der Null. Weitere Beispiele sind die Menge

$$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

der *ganzen Zahlen*, die Menge

$$\mathbb{Q} := \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$$

der *rationalen Zahlen*, und die Menge $\mathbb{R}$ der *reellen Zahlen*. Zur Konstruktion dieser Zahlen verweisen wir auf die Analysis.

Definition 1.1. (i) Die Schreibweise $x \in X$ bedeutet, daß x ein Element der Menge X ist. Ist dies nicht der Fall, so schreiben wir $x \notin X$.

(ii) Eine Menge A heißt *Teilmenge* der Menge X , wenn gilt $x \in A \Rightarrow x \in X$. Mit anderen Worten : Jedes Element von A liegt auch in X . In diesem Fall schreiben wir $A \subset X$, andernfalls $A \not\subset X$.

□

Bemerkung 1.2. Aus gegebenen Mengen kann man Teilmengen auswählen, die durch gewisse Eigenschaften charakterisiert sind, etwa

$$\begin{aligned} X &= \{n \in \mathbb{N} \mid n \text{ ist gerade}\} \\ &= \{0, 2, 4, 6, 8, \dots\}. \end{aligned}$$

□

Beispiel 1.3. (i) $3 \in \mathbb{N}$, $\frac{2}{3} \notin \mathbb{N}$.

(ii) $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

□

Definition 1.4. (i) Mit $\emptyset$ bezeichnet man die *leere Menge*, die kein Element enthält.

(ii) Ist X eine Menge so bezeichnen wir mit $\mathfrak{P}(X)$ die Menge aller Teilmengen von X und nennen $\mathfrak{P}(X)$ die *Potenzmenge* von X . Diese enthält die leere Menge und X selbst.

□

Beispiel 1.5. $\mathfrak{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

□

Wir kommen zu einigen mengentheoretischen Operationen. Wenden wir diese Operationen auf Elemente einer Potenzmenge $\mathfrak{P}(X)$ an, so ergeben sich wieder Elemente von $\mathfrak{P}(X)$.

Definition 1.6. Seien A und B beliebige Mengen.

(i)

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$$

heißt die *Vereinigung* von A und B .

(ii)

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\}$$

heißt der *Durchschnitt* von A und B .

(iii)

$$B \setminus A := \{x \mid x \in B \text{ und } x \notin A\}$$

heißt die *Differenz* von B und A .

(iv) Ist A eine Teilmenge von B , so schreiben wir

$$\complement_B A := B \setminus A$$

und nennen $\complement_B A$ das *Komplement* von A in B .

(v) A und B heißen *disjunkt*, wenn gilt $A \cap B = \emptyset$.

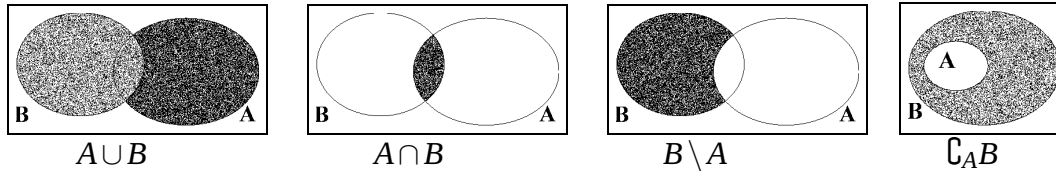


Abbildung 1.1: Mengenoperationen

□

Beispiel 1.7. Jede rationale Zahl lässt sich als abbrechende oder periodische Dezimalzahl darstellen, etwa $\frac{3}{5} = 0,6$ oder $\frac{1}{3} = 0,\overline{3}$. Diejenigen Dezimalzahlen, die weder abbrechend, noch periodisch sind, nennt man auch *irrationale Zahlen*. Die Menge der rationalen Zahlen und die Menge der irrationalen Zahlen sind disjunkt, ihre Vereinigung ist gerade $\mathbb{R}$ (siehe Analysis). □

1

Rechenregeln 1.8. Sind A, B, C Mengen, so gilt:

(i)

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \end{aligned} \quad (\text{Kommutativität})$$

(ii)

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap C \\ A \cap (B \cup C) &= (A \cap B) \cup C \end{aligned} \quad (\text{Assoziativität})$$

Sind A, B Teilmengen der Menge X , so gilt:

(iii)

$$\begin{aligned} \complement_X(A \cup B) &= \complement_X A \cap \complement_X B \\ \complement_X(A \cap B) &= \complement_X A \cup \complement_X B \end{aligned} \quad (\text{Distributivität})$$

Beweis. Wir zeigen nur

$$\complement_X(A \cup B) = \complement_X A \cap \complement_X B,$$

die anderen Aussagen behandeln wir in den Aufgaben.

$$\begin{aligned}
 x \in \complement_X(A \cup B) &\Leftrightarrow x \in X \text{ und } x \notin A \cup B \\
 &\Leftrightarrow x \in X \text{ und } x \notin A \text{ und } x \notin B \\
 &\Leftrightarrow (x \in X \text{ und } x \notin A) \text{ und } (x \in X \text{ und } x \notin B) \\
 &\Leftrightarrow x \in \complement_X A \text{ und } x \in \complement_X B \\
 &\Leftrightarrow x \in \complement_X A \cap \complement_X B
 \end{aligned}$$

□

Von großer Bedeutung ist das

Beweisprinzip durch vollständige Induktion 1.9. Jeder natürlichen Zahl n sei eine Aussage $A(n)$ zugeordnet, so daß gilt:

- (i) Die Aussage $A(0)$ ist wahr.
- (ii) $\forall n \in \mathbb{N}$ gilt: Ist $A(n)$ wahr, so auch $A(n+1)$.

Dann ist $A(n)$ wahr $\forall n \in \mathbb{N}$.

□

Bemerkung und Definition 1.10. Benutzt man 1.9 um zu zeigen, daß die Aussage $A(n)$ wahr ist $\forall n \in \mathbb{N}$, so spricht man von einem *Beweis durch vollständige Induktion*. Der Nachweis von $A(0)$ heißt *Induktionsanfang*, der Schluß von $A(n)$ (der *Induktionsannahme*) auf $A(n+1)$ (der *Induktionsbehauptung*) heißt *Induktionsschluß*.

Mit demselben Prinzip beweist man die Gültigkeit von Aussagen $A(n)$ für alle $n \in \mathbb{N}$ die größer oder gleich einem gegebenen $n_0 \in \mathbb{N}$ sind. Dazu muß man in (i) dann $A(n_0)$ nachweisen. Manchmal formuliert man den Induktionsschluß auch so, daß man von $A(n-1)$ auf $A(n)$ schließt.

□

Satz 1.11. Ist X eine Menge mit genau n Elementen, so besteht die Potenzmenge $\mathfrak{P}(X)$ aus 2^n Elementen.

Beweis. Durch vollständige Induktion.

Induktionsanfang. $n = 0$

Hat X keine Elemente, so ist $X = \emptyset$ und somit $\mathfrak{P}(X) = \mathfrak{P}(\emptyset) = \{\emptyset\}$. Also hat $\mathfrak{P}(X)$ genau $1 = 2^0$ Elemente.

Induktionsschluß. Sei $n \in \mathbb{N}$.

Induktionsannahme. Jede n -elementige Menge hat genau 2^n Teilmengen.

Induktionsbehauptung. Jede $(n+1)$ -elementige Menge hat genau 2^{n+1} Teilmengen.

Sei also $X = \{x_1, \dots, x_{n+1}\}$ eine Menge mit $n+1$ Elementen. Wir betrachten $X' = \{x_1, \dots, x_n\}$. Dann hat $\mathfrak{P}(X')$ nach Induktionsannahme 2^n Elemente. Ist $A \in \mathfrak{P}(X')$, so sind A und $A \cup \{x_{n+1}\}$ Elemente von $\mathfrak{P}(X)$. Auf diese Weise erhält man alle Teilmengen von X . Also hat $\mathfrak{P}(X)$ genau $2 \cdot 2^n = 2^{n+1}$ Elemente.

□

Als weitere Anwendung zeigen wir:

Satz 1.12. Sei $A \subset \mathbb{N}$, $A \neq \emptyset$. Dann besitzt A ein kleinstes Element :

$$\exists a_0 \in A \text{ mit } a \in A \Rightarrow a \geq a_0.$$

Beweis. *Annahme.* Die Aussage ist falsch.

Dann gibt es eine Teilmenge $A \subset \mathbb{N}$, $A \neq \emptyset$, ohne kleinstes Element. Sei

$$B = \{n \in \mathbb{N} \mid \{0, 1, 2, \dots, n\} \cap A \neq \emptyset\}.$$

Wir zeigen durch vollständige Induktion: $B = \mathbb{N}$.

Induktionsanfang. $0 \in B$, denn sonst wäre $0 \in A$ und 0 wäre kleinstes Element von A .

Induktionsschluss. Sei $n \in \mathbb{N}$.

Induktionsannahme. $n \in B$.

Induktionsbehauptung. $n+1 \in B$.

Wegen $n \in B$ sind $0, 1, 2, \dots, n \notin A$. Wäre $n+1 \in A$, so folgte $n+1 \leq a \forall a \in A$, d. h. $n+1$ wäre kleinstes Element. Also ist $n+1 \notin A$, es folgt $n+1 \in B$.

Somit gilt $B = \mathbb{N}$ im Widerspruch zu $A \neq \emptyset$. Also war unsere Annahme falsch und somit ist der Satz bewiesen. $\square$

Definition 1.13. Seien X und Y Mengen. Eine Vorschrift, die jedem Element $x \in X$ genau ein Element $y = f(x) \in Y$ zuordnet heißt *Abbildung* von X nach Y . Man schreibt dafür auch

$$f : X \rightarrow Y \quad \text{oder} \quad X \xrightarrow{f} Y$$

bzw.

$$f : X \rightarrow Y, x \mapsto f(x),$$

und nennt $f(x)$ das *Bild* von x unter f . X heißt *Definitionsbereich* und Y *Werte-* oder *Bildbereich* von $f : X \rightarrow Y$.

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

Bemerkung und Definition 1.14. (i) Ist X eine Menge, so ist

$$\text{id}_X : X \rightarrow X, x \mapsto x,$$

eine Abbildung, die *identische Abbildung* (von X).

(ii) Sind $f : X \rightarrow Y$ und $g : Y \rightarrow Z$ zwei Abbildungen, so erhält man eine neue Abbildung durch die Vorschrift

$$g \circ f : X \rightarrow Z, x \mapsto g(f(x)).$$

Diese heißt *Komposition* von f und g . $\square$

Definition 1.15. Eine Abbildung $f : X \rightarrow Y$ heißt

(i) *injektiv*, falls $\forall x, x' \in X$ gilt

$$f(x) = f(x') \Rightarrow x = x',$$

(ii) *surjektiv*, falls

$$\forall y \in Y \exists x \in X \text{ mit } f(x) = y,$$

(iii) *bijektiv*, falls f injektiv und surjektiv ist.

□

Satz und Definition 1.16. Für eine Abbildung $f : X \rightarrow Y$ sind äquivalent:

(i) f ist bijektiv

(ii) $\exists$ Abbildung $g : Y \rightarrow X$ mit

$$g \circ f = \text{id}_X \text{ und } f \circ g = \text{id}_Y$$

Eine Abbildung g wie in (ii) ist durch f eindeutig bestimmt und wird mit f^{-1} bezeichnet. f^{-1} heißt Umkehrabbildung zu f oder die zu f inverse Abbildung.

Beweis. '(i) $\Rightarrow$ (ii)'. Sei f bijektiv. Wir definieren g wie folgt. Sei $y \in Y$. Da f surjektiv ist $\exists x \in X$ mit $f(x) = y$. Das Element x ist durch y und f eindeutig bestimmt, da f auch injektiv ist. Wir setzen $g(y) := x$. Dann folgt mit $y = f(x)$:

$$(g \circ f)(x) = g(f(x)) = g(y) = x = \text{id}_X, \text{ und}$$

$$(f \circ g)(y) = f(g(y)) = f(x) = y = \text{id}_Y.$$

Da im ersten Fall x und im zweiten Fall y beliebig sind folgt

$$g \circ f = \text{id}_X \text{ und } f \circ g = \text{id}_Y.$$

'(ii) $\Rightarrow$ (i)'. Sei $g : Y \rightarrow X$ eine Abbildung mit $g \circ f = \text{id}_X$, $f \circ g = \text{id}_Y$. Dann ist f injektiv: Sind $x, x' \in X$ mit $f(x) = f(x')$, so gilt

$$x = g(f(x)) = g(f(x')) = x'.$$

f ist auch surjektiv: Ist $y \in Y$, so gilt für $x = g(y)$:

$$f(x) = f(g(y)) = y.$$

Insgesamt folgt, daß f bijektiv ist.

Sind g und g' zwei Abbildungen, die (ii) erfüllen, so gilt $\forall y \in Y: f(g(y)) = y = f(g'(y))$. Also ist $g = g'$, d. h. g ist eindeutig bestimmt. □

Bemerkung und Definition 1.17. Sei $f : X \rightarrow Y$ eine Abbildung.

(i) Ist $A \subset X$ eine Teilmenge, so ist

$$f(A) := \{y \in Y \mid \exists x \in A \text{ mit } f(x) = y\}$$

eine Teilmenge von Y , die *Bildmenge* von A unter f . Insbesondere heit

$$\text{Bild } f := f(X)$$

das *Bild* von f .

(ii) Ist $B \subset Y$ eine Teilmenge, so ist

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}$$

eine Teilmenge von X , die Urbildmenge von B unter f .

(iii) Ist $y \in Y$, so heit

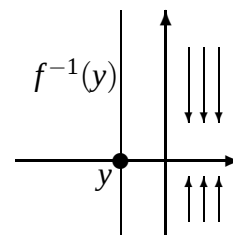
$$f^{-1}(y) := f^{-1}(\{y\})$$

die *Faser* von f ber y .

(iv) Ist $A \subset X$, so ist

$$f|_A : A \rightarrow Y, x \mapsto f(x)$$

eine Abbildung, die *Einschrnkung* von f auf A .



□

Beispiel 1.18. (i) Sicher ist

$$f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2,$$

eine Abbildung. f ist nicht injektiv, da z.B. ± 1 dasselbe Bild $+1$ haben. f ist auch nicht surjektiv, da etwa -1 kein Urbild hat. Definieren wir

$$\mathbb{R}_+ := \{x \in \mathbb{R} \mid x \geq 0\},$$

so ist

$$\mathbb{R} \rightarrow \mathbb{R}_+, x \mapsto x^2,$$

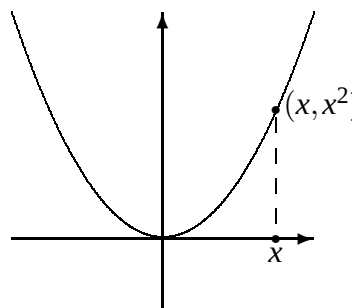
surjektiv,

$$\mathbb{R}_+ \rightarrow \mathbb{R}, x \mapsto x^2,$$

injektiv und

$$\mathbb{R}_+ \rightarrow \mathbb{R}_+, x \mapsto x^2,$$

bijektiv.



(ii) Die Vorschrift

$$\mathbb{R}_+ \rightarrow \mathbb{R}, x \rightarrow \pm\sqrt{x},$$

ist keine Abbildung, da dadurch jedem $x > 0$ zwei Punkte zugeordnet werden. Dagegen ist

$$\mathbb{R}_+ \rightarrow \mathbb{R}_+, x \rightarrow +\sqrt{x},$$

eine Abbildung, und zwar die Umkehrabbildung von

$$\mathbb{R}_+ \rightarrow \mathbb{R}_+, x \rightarrow x^2.$$

□

Jedes n -Tupel $(x_1, \dots, x_n)$ von Elementen in einem Zahlbereich K wie in der Motivation entspricht einer Abbildung

$$\{1, \dots, n\} \rightarrow K, i \rightarrow x_i,$$

die jeder Zahl $i \in \{1, \dots, n\}$ das Element x_i zuordnet. Allgemeiner erklären wir:

Definition 1.19. Ist

$$\varphi : I \rightarrow X$$

eine Abbildung zwischen zwei Mengen, so schreiben wir auch

$$(x_i)_{i \in I} \text{ mit } x_i = \varphi(i)$$

für φ und sprechen von einer *Familie* (oder einem I -Tupel) von Elementen in X mit *Indexmenge* I . Wir schreiben

$$X^I := \text{Abb}(I, X)$$

für die Menge aller I -Tupel in X .

Ist $I = \mathbb{N}$, so heißt $(x_n)_{n \in \mathbb{N}}$ eine *Folge* in X .

Ist $I = \{1, \dots, n\}$, so bezeichnen wir mit

$$X \times \dots \times X := X^n := X^{\{1, \dots, n\}}$$

die Menge aller n -Tupel von Elementen in X . Wir sprechen auch von *geordneten n -Tupeln* $(x_1, \dots, x_n)$ und betonen damit, daß durch die Abbildung $\{1, \dots, n\} \rightarrow X, i \rightarrow x_i$, eine Reihenfolge festgelegt ist. □

Beispiel 1.20. In $\mathbb{N}^2$ gilt etwa

$$(1, 2) \neq (2, 1)$$

□

Bemerkung und Definition 1.21. Betrachten wir in 1.19 Abbildungen von einer Indexmenge $I \neq \emptyset$ in eine Menge von Mengen, so ergibt sich der Begriff der *Familie von Mengen*. Ist $(X_i)_{i \in I}$ eine solche, so erhalten wir analog zu 1.6 die *Vereinigung* der $X_i, i \in I$, durch

$$\bigcup_{i \in I} X_i := \{x \mid \exists i \in I \text{ mit } x \in X_i\},$$

und den Durchschnitt der $X_i, i \in I$, durch

$$\bigcap_{i \in I} X_i := \{x \mid x \in X_i \ \forall i \in I\}.$$

Weiter heit

$$\prod_{i \in I} X_i := \{\varphi \in \text{Abb}(I, \bigcup_{i \in I} X_i \mid \varphi(i) \in X_i \ \forall i \in I\}$$

das *kartesische* oder *direkte Produkt* der $X_i, i \in I$. Man schreibt dafr auch

$$\prod_{i \in I} X_i = \{(x_i)_{i \in I} \mid x_i \in X_i \ \forall i \in I\}.$$

und nennt x_i die *i-te Komponente* von $(x_i)_{i \in I}$.

Ist speziell $X_i = X \ \forall i \in I$, so ist

$$\prod_{i \in I} X_i = X^I.$$

□

Bemerkung 1.22. Durch ein Element $(x_i)_{i \in I} \in \prod_{i \in I} X_i$ wird $\forall i \in I$ aus X ein Element x_i ausgewhlt. Damit dies berhaupt mglich ist, mu jedes X_i mindestens ein Element enthalten, es mu $X_i \neq \emptyset$ gelten. Da man auch im Falle unendlicher Indexmengen stets eine Auswahl treffen kann, besagt das sogenannte

Auswahlaxiom. Ist $(X_i)_{i \in I}$ eine Familie von Mengen, so gilt

$$X_i \neq \emptyset \ \forall i \in I \Rightarrow \prod_{i \in I} X_i \neq \emptyset.$$

Darauf wollen wir hier nicht weiter eingehen.

□

Bemerkung und Definition 1.23. Ist $(X_i)_{i \in I}$ eine Familie von Mengen, so ist

$$p_i : \prod_{i \in I} X_i \rightarrow X_i, (x_i)_{i \in I} \rightarrow x_i,$$

eine Abbildung, die *i-te kanonische Projektion* (oder auch *Projektion auf die i-te Komponente*). Ist allgemeiner $J \subset I$ eine Teilmenge der Indexmenge, so haben wir eine *Projektion*

$$\prod_{i \in I} X_i \rightarrow \prod_{j \in J} X_j, (x_i)_{i \in I} \rightarrow (x_j)_{j \in J}.$$

□

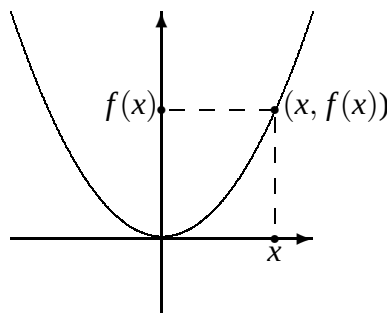
Definition 1.24. Ist $f : X \rightarrow Y$ eine beliebige Abbildung zwischen zwei Mengen, so heißt

$$\Gamma_f := \{(x, y) \in X \times Y \mid f(x) = y\}$$

der Graph von f . □

Mit Hilfe des Graphen kann man sich, wie bereits in 1.18 gesehen, Abbildungen veranschaulichen.

Beispiel 1.25. Der Graph von $f : \mathbb{R} \rightarrow \mathbb{R}, x \rightarrow x^2$, sieht wie folgt aus:



□

1

Aufgaben

Aufgabe 1. Beweisen Sie die Rechenregeln 1.8 aus der Vorlesung.

Aufgabe 2. Leiten Sie aus Satz 1.12 der Vorlesung folgende Eigenschaft von $\mathbb{Z}$ ab:
Sind $a, b \in \mathbb{Z}$, und ist $b > 0$, so gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$a = bq + r \text{ und } 0 \leq r < b.$$

Aufgabe 3. Zeigen Sie durch vollständige Induktion:

- (i) Ist $a \in \mathbb{N}$, so gilt $(1+a)^n \geq 1+na$ für alle $n \in \mathbb{N}$.
- (ii) Es gilt $n^2 \geq 3n$ für alle $n \in \mathbb{N}, n \geq 3$.

Aufgabe 4. Seien $f : X \rightarrow Y, g : Y \rightarrow Z$ Abbildungen und $g \circ f : X \rightarrow Z$ die Komposition von f und g . Zeigen Sie, daß gilt:

- (i) Sind f und g injektiv (surjektiv), so ist auch $g \circ f$ injektiv (surjektiv).

(ii) Ist $g \circ f$ injektiv (surjektiv), so ist auch f injektiv (g surjektiv).

Wir kommen nun zu Äquivalenzrelationen. Diese dienen sowohl zur Konstruktion von Mengen als auch zur ‘Injektivisierung’ von Abbildungen.

Definition 1.26. Sei X eine Menge. Eine *Relation* in X ist eine Aussage für geordnete Paare $(x, y) \in X \times X$, d. h. in $X \times X$ ist eine Teilmenge R gegeben durch die Paare (x, y) , die diese Aussage erfüllen. Wir schreiben auch

$$xRy \text{ für } (x, y) \in R.$$

Eine Relation $R \subset X \times X$ heißt

(i) *reflexiv*, falls $\forall x \in X$ gilt

$$xRx,$$

(ii) *symmetrisch*, falls $\forall x, y \in X$ gilt:

$$xRy \Rightarrow yRx,$$

(iii) *antisymmetrisch*, falls $\forall x, y \in X$ gilt

$$xRy \text{ und } yRx \Rightarrow x = y,$$

(iv) *transitiv*, falls $\forall x, y, z \in X$ gilt:

$$xRy \text{ und } yRz \Rightarrow xRz.$$

□

Definition 1.27. Eine Relation R in einer Menge X heißt *Äquivalenzrelation*, wenn R reflexiv, symmetrisch und transitiv ist. In diesem Fall schreibt man oft auch $\sim$ für R und somit auch

$$x \sim y \text{ für } xRy.$$

Für $x \in X$ heißt

$$[x] := [x]_{\sim} := \{y \in X \mid y \sim x\}$$

die *Äquivalenzklasse* von x .

□

Satz und Definition 1.28. Sei $\sim$ eine Äquivalenzrelation in der Menge X . Dann ist X die Vereinigung der Äquivalenzklassen bezüglich $\sim$. Diese Äquivalenzklassen sind paarweise disjunkte, nichtleere Teilmengen von X . Genauer gilt:

$$[x] \cap [y] \neq \emptyset \Leftrightarrow x \sim y \Leftrightarrow [x] = [y].$$

Jedes $y \in [x]$ heißt *Repräsentant* der Äquivalenzklasse $[x]$.

Beweis. Sei $x \in X$. Dann ist $[x] \neq \emptyset$, da $x \in [x]$ wegen $x \sim x$. Daraus folgt auch, daß X Vereinigung der Äquivalenzklassen bezüglich $\sim$ ist.

Ist $[x] \cap [y] \neq \emptyset$, so $\exists z \in [x] \cap [y]$. Also gilt $z \sim x$ und $z \sim y$. Wegen der Symmetrie und der Transitivität folgt $x \sim y$. Daraus wiederum ergibt sich $[x] = [y]$: Ist nämlich $u \in [x]$, so ist $u \sim x$ und wegen $x \sim y$ auch $u \sim y$, d. h. $u \in [y]$. Es folgt $[x] \subset [y]$. Analog ergibt sich $[y] \subset [x]$.

Ist andererseits $[x] = [y]$, so ist $x \in [x] = [y]$ und somit ist $[x] \cap [y] \neq \emptyset$. $\square$

Bemerkung und Definition 1.29. Sei $\sim$ eine Äquivalenzrelation in der Menge X . Dann wird die Menge der Äquivalenzklassen von $\sim$ mit

$$X/\sim$$

bezeichnet. Die Vorschrift

$$p : X \rightarrow X/\sim, x \mapsto [x],$$

definiert eine surjektive Abbildung, die *kanonische Projektion* von X auf $X/\sim$. $\square$

Satz und Definition 1.30. Seien $f : X \rightarrow Y$ eine Abbildung und $\sim$ eine Äquivalenzrelation in X mit

$$x \sim x' \Rightarrow f(x) = f(x').$$

Dann existiert genau eine Abbildung

$$\bar{f} : X/\sim \rightarrow Y,$$

so daß das Diagramm

$$\begin{array}{ccc} X & \xrightarrow{p} & X/\sim \\ f \searrow & & \swarrow \bar{f} \\ & Y & \end{array}$$

kommutiert, d. h. so daß gilt

$$\bar{f} \circ p = f.$$

Beweis. Wir definieren $\bar{f}$ durch die Vorschrift

$$\bar{f} : X/\sim \rightarrow Y, [x] \mapsto f(x).$$

Um zu zeigen, daß $\bar{f}$ eine Abbildung ist, muß man zeigen, daß $\bar{f}$ wohldefiniert ist, d. h. nicht von der Wahl des Repräsentanten x abhängt. Dies ergibt sich wie folgt:

$$[x] = [x'] \Rightarrow x \sim x' \Rightarrow f(x) = f(x').$$

Also ist $\bar{f}$ eine Abbildung und per Definition gilt

$$(\bar{f} \circ p)(x) = \bar{f}(p(x)) = \bar{f}([x]) = f(x) \quad \forall x \in X.$$

Durch diese Eigenschaft ist $\bar{f}$ eindeutig bestimmt. $\square$

Bemerkung 1.31. Ist $f : X \rightarrow Y$ eine Abbildung, so ist durch

$$x \sim_f x' \Leftrightarrow f(x) = f(x')$$

eine Äquivalenzrelation in X definiert. Die zugehörige Abbildung

$$\bar{f} : X / \sim_f \rightarrow Y$$

ist injektiv (und somit bijektiv als Abbildung $X / \sim_f \rightarrow \text{Bild } \bar{f}$):

$$\bar{f}([x]) = \bar{f}([x']) \Rightarrow f(x) = f(x') \Rightarrow x \sim_f x' \Rightarrow [x]_{\sim_f} = [x']_{\sim_f}$$

□

Beispiel 1.32. In $\mathbb{Z}$ ist durch

$$a \sim b \Leftrightarrow a - b \text{ ist gerade}$$

offensichtlich eine Äquivalenzrelation definiert. Es gibt genau zwei Äquivalenzklassen:

$$\begin{aligned} [0] &= \{a \in \mathbb{Z} \mid a \text{ gerade}\}, \\ [1] &= \{a \in \mathbb{Z} \mid a \text{ ungerade}\}. \end{aligned}$$

□

Im letzten Teil dieses Abschnittes besprechen wir mit dem Lemma von Zorn ein wichtiges beweistechnisches Hilfsmittel.

Definition 1.33. Eine Relation R in der Menge X heißt *Ordnung(srelation)*, wenn sie reflexiv, antisymmetrisch und transitiv ist. In diesem Fall schreiben wir oft auch $\leq$ für R und nennen X eine durch $\leq$ *geordnete Menge*. Weiter schreiben wir abkürzend

$$x < y \text{ für } (x \leq y \text{ und } x \neq y).$$

□

Bemerkung und Definition 1.34. Seien $\leq$ eine Ordnung in X und $A \subset X$. Dann erhält man durch Beschränkung von $\leq$ auf die Elemente von A eine Ordnung in A , die *induzierte Ordnung*. Wenn nicht anders erwähnt, sind Teilmengen von geordneten Mengen immer mit der induzierten Ordnung versehen. □

Beispiel 1.35. Die natürliche Ordnung $\leq$ in $\mathbb{R}$ und die dadurch induzierten Ordnungen in

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

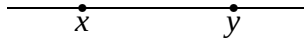
(vergleiche wieder Analysis). □

Definition 1.36. Eine Ordnung $\leq$ in X heißt *total* (X heißt durch $\leq$ *total geordnet* oder eine *Kette*), wenn gilt:

$$x, y \in X \Rightarrow x \leq y \text{ oder } y \leq x$$

(je zwei Elemente sind bezüglich $\leq$ *vergleichbar*). □

Beispiel 1.37. (i) $\leq$ in $\mathbb{R}$ ist total.



(ii) Sei X eine Menge. Dann ist durch

$$A \leq B \Leftrightarrow A \subset B$$

eine Ordnung in $\mathfrak{P}(X)$ definiert. Hat X mehr als ein Element, so ist $\leq$ nicht total: Sind $x, y \in X$ mit $x \neq y$, so sind $\{x\}$ und $\{y\}$ nicht vergleichbar. □

Definition 1.38. Sei $\leq$ eine Ordnung in X .

(i) $z \in X$ heißt *maximales Element* von X , wenn gilt:

$$x \in X, x \geq z \Rightarrow x = z.$$

(ii) Sind $A \subset X$ und $z \in X$, so heißt z *obere Schranke* von A , wenn gilt:

$$x \in A \Rightarrow x \leq z.$$

Analog definiert man die Begriffe *minimales Element* und *untere Schranke*. □

Definition 1.39. Eine Ordnung $\leq$ in X heißt *induktiv* bzw. X heißt durch $\leq$ *induktiv geordnet*, wenn jede total geordnete Teilmenge von X eine obere Schranke in X besitzt. □

Beispiel 1.40. (i) $\leq$ in $\mathbb{R}$ ist nicht induktiv.

(ii) $\leq$ in $\mathfrak{P}(X)$ wie oben ist trivialerweise induktiv, da X ein (eindeutig bestimmtes) maximales Element ist. □

In Beweisen benutzt man die folgende Aussage, um die Existenz von maximalen Elementen zu zeigen.

Lemma von Zorn 1.41. Sei X eine induktiv geordnete Menge. Dann gibt es in X (mindestens) ein maximales Element.

Bemerkung 1.42. Das Lemma von Zorn ist äquivalent zum Auswahlaxiom. Auf einen Beweis dieser Tatsache wollen wir hier nicht eingehen. □

Kapitel 2

Gruppen, Ringe, Körper

Motivation 2.1. Die Addition in $\mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$ bzw. die Multiplikation in $\mathbb{Q} \setminus \{0\}$ oder $\mathbb{R} \setminus \{0\}$ sind Rechenoperationen, die weitgehend übereinstimmenden Rechengesetzen unterliegen (vergleiche wieder Analysis). So gilt z. B.

$$(a + b) + c = a + (b + c) \text{ bzw. } (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Weiter gibt es ausgezeichnete Zahlen, nämlich 0 bzw. 1, die sich bei diesen Operationen neutral verhalten:

$$0 + a = a + 0 = a \text{ bzw. } 1 \cdot a = a \cdot 1 = a.$$

Schließlich gilt

$$(-a) + a = a + (-a) = 0 \text{ bzw. } \frac{1}{a} \cdot a = a \cdot \frac{1}{a} = 1,$$

d. h. es gibt zu jedem a eine Zahl a' (nämlich $-a$ bzw. $\frac{1}{a}$), so daß die Summe bzw. das Produkt dieser Zahlen gerade die jeweilige neutrale Zahl ergibt (im Falle der Multiplikation haben wir, wie oben gesagt, $a \neq 0$ vorausgesetzt).

Da diese Rechenregeln das Zahlenrechnen weitgehend beherrschen und auch in vielen anderen Fällen auftreten, ist es naheliegend, sie unabhängig von der speziellen Natur der Rechengrößen und der jeweiligen Operationen zu untersuchen. Das hat insbesondere den Vorteil, daß mathematische Aussagen, die auf den grundlegenden Rechenregeln beruhen, nicht in jeder Situation wieder neu bewiesen werden müssen.

Bei dieser abstrakten Betrachtungsweise stehen also die Rechengesetze im Vordergrund: Nicht womit man rechnet, ist wesentlich, sondern wie man rechnet. Man setzt lediglich voraus, daß für die Elemente einer gegebenen Menge eine Operation (Verknüpfung) definiert ist, die jedem geordneten Paar (a, b) von Elementen der Menge wieder ein Element der Menge zuordnet, und die den oben genannten Rechenregeln genügt. Die Verknüpfung selbst bezeichnen wir mit dem Symbol $\circ$. $\square$

Definition 2.2. Eine Verknüpfung $\circ$ auf einer Menge X ist eine Abbildung

$$X \times X \rightarrow X, (x, y) \rightarrow x \circ y.$$

Ist $A \subset X$ eine Teilmenge, und gilt

$$a, b \in A \Rightarrow a \circ b \in A,$$

so heißt A bzgl. $\circ$ abgeschlossen. Ist dies der Fall, so erhält man durch das Beschränken von $\circ$ auf die Elemente von A eine Verknüpfung auf A , die *induzierte Verknüpfung*. $\square$

Bemerkung und Definition 2.3. Sei $\circ$ eine Verknüpfung auf der Menge X .

(i) $\circ$ heißt *assoziativ*, wenn gilt

$$(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in X.$$

In diesem Fall nennen wir das Paar $(X, \circ)$ auch eine *Halbgruppe*.

(ii) Ein Element $e \in X$ heißt *neutrales Element* bezüglich $\circ$, wenn gilt

$$e \circ a = a = a \circ e \quad \forall a \in X.$$

Dieses ist im Falle der Existenz eindeutig bestimmt: Sind e, f zwei neutrale Elemente, so gilt

$$e \underset{f \text{ neutral}}{=} e \circ f \underset{e \text{ neutral}}{=} f.$$

Jede Halbgruppe, die ein neutrales Element besitzt, heißt *Monoid*.

(iii) Ist $(X, \circ)$ ein Monoid mit neutralem Element e , so heißt $a \in X$ *invertierbar* in X , wenn es ein zu a *inverses Element* in X gibt, d. h. wenn $\exists a' \in X$ mit

$$a' \circ a = e = a \circ a'.$$

Ein zu a inverses Element ist im Falle der Existenz eindeutig bestimmt und wird auch mit a^{-1} bezeichnet: Sind a' und a'' zu a invers, so gilt

$$a' = e \circ a' = (a'' \circ a) \circ a' = a'' \circ (a \circ a') = a'' \circ e = a''.$$

(iv) $\circ$ heißt *kommutativ*, wenn gilt

$$a \circ b = b \circ a \quad \forall a, b \in X.$$

Eine Halbgruppe mit kommutativer Verknüpfung heißt eine *kommutative* oder *abelsche* Halbgruppe. $\square$

Definition 2.4. Eine *Gruppe* ist ein Monoid, in dem jedes Element invertierbar ist. Mit anderen Worten: Ein Paar $(G, \circ)$, bestehend aus einer Menge G und einer Verknüpfung $\circ$ heißt *Gruppe*, falls gilt:

- (i) $\circ$ ist assoziativ,
- (ii) es gibt ein neutrales Element bezüglich $\circ$ in G ,
- (iii) jedes Element in G besitzt ein inverses Element in G .

Gilt zusätzlich

- (iv) $\circ$ ist kommutativ,

so heißt $(G, \circ)$ eine *kommutative* oder *abelsche Gruppe*. $\square$

Beispiel 2.5. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ bzw. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen. $\square$

Aufgaben

Aufgabe 5. Zeigen Sie, daß für eine Menge $X \neq \emptyset$ die folgenden Aussagen äquivalent sind:

- (i) X ist endlich.
- (ii) Jede injektive Abbildung $X \rightarrow X$ ist bijektiv.
- (iii) Jede surjektive Abbildung $X \rightarrow X$ ist bijektiv.

Aufgabe 6. Sei $f : X \rightarrow Y$ eine Abbildung zwischen zwei Mengen. Zeigen Sie:

- (i)

$$\begin{aligned} f^{-1}(f(A)) &\supset A \text{ für } A \subset X, \\ f(f^{-1}(B)) &\subset B \text{ für } B \subset Y. \end{aligned}$$

- (ii)

$$\begin{aligned} f^{-1}\left(\bigcap_{i \in I} B_i\right) &= \bigcap_{i \in I} f^{-1}(B_i) \\ f^{-1}\left(\bigcup_{i \in I} B_i\right) &= \bigcup_{i \in I} f^{-1}(B_i) \end{aligned} \quad \text{für } (B_i)_{i \in I} \subset \mathfrak{P}(Y).$$

- (iii)

$$\begin{aligned} f\left(\bigcap_{i \in I} A_i\right) &\subset \bigcap_{i \in I} f(A_i) \\ f\left(\bigcup_{i \in I} A_i\right) &= \bigcup_{i \in I} f(A_i) \end{aligned} \quad \text{für } (A_i)_{i \in I} \subset \mathfrak{P}(X).$$

Zeigen Sie an Hand von Beispielen, daß in (i) und im ersten Fall von (iii) die Gleichheit im Allgemeinen nicht gilt.

Aufgabe 7. Sei X eine Menge mit genau n Elementen. Zeigen Sie: Die Anzahl der Paare $(A, B) \in \mathfrak{P}(X) \times \mathfrak{P}(X)$ mit $A \cap B = \emptyset$ beträgt 3^n .

Aufgabe 8. (a) Sei $\emptyset \neq X$ eine endliche geordnete Menge. Zeigen Sie: X besitzt ein minimales und ein maximales Element.

(b) Sei X eine induktiv geordnete Menge mit $x \in X$. Zeigen Sie: Es gibt ein maximales Element $z \in X$ mit $x \leq z$.

Hier ist ein weiteres Beispiel:

Bemerkung und Definition 2.6. (i) Ist X eine Menge, so heißen die Elemente von

$$S(X) := \{f : X \rightarrow X \mid f \text{ ist bijektiv}\}$$

auch *Permutationen* von X . Nach Aufgabe 4 ist die Komposition von zwei Permutationen wieder eine solche. Also ist $\circ$ eine Verknüpfung auf $S(X)$. Diese ist assoziativ:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x) \\ \forall f, g, h \in S(X), \forall x \in X.$$

Weiter ist id_X ein neutrales Element:

$$(\text{id}_X \circ f)(x) = \text{id}_X(f(x)) = f(x) = f(\text{id}_X(x)) = (f \circ \text{id}_X)(x) \quad \forall f \in S(X), \forall x \in X.$$

Ist schließlich $f \in S(X)$, so ist die Umkehrabbildung f^{-1} ein zu f inverses Element:

$$f^{-1} \circ f = \text{id}_X = f \circ f^{-1}.$$

Also ist $(S(X), \circ)$ eine Gruppe, die *Permutationsgruppe* von X .

(ii) Im Falle der endlichen Menge $\{1, \dots, n\} \subset \mathbb{N}$ schreibt man auch

$$S_n := S(\{1, \dots, n\}).$$

Für $\sigma \in S_n$ schreiben wir auch

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} \text{ mit } \sigma_i = \sigma(i).$$

(iii) $\tau \in S_n$ heißt *Transposition*, wenn $\exists k, l \in \{1, \dots, n\}, k \neq l$, mit

$$\tau(i) = \begin{cases} l & i = k \\ k & i = l \\ i & \text{sonst} \end{cases}, \quad 1 \leq i \leq n.$$

Wir sprechen auch von der *Vertauschung* von k und l . Für jedes solche τ gilt $\tau \circ \tau = \text{id}$, d.h. $\tau^{-1} = \tau$.

- (iv) Wie man leicht nachrechnet, ist S_n kommutativ für $n = 1, 2$. Für $n = 3$ gilt dies nicht mehr: Sind etwa τ_{12} die Vertauschung von 1 und 2 sowie τ_{23} die Vertauschung von 2 und 3, so gilt

$$\tau_{23} \circ \tau_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} = \tau_{12} \circ \tau_{23}.$$

□

Wir wollen einige Regeln für das Rechnen in Gruppen herleiten. Dazu benötigen wir eine andere Version des Beweisprinzips durch vollständige Induktion. Diese ist offensichtlich zu 1.9 bzw. 1.10 äquivalent.

Beweisprinzip durch vollständige Induktion 2.7. Sei $n_0 \in \mathbb{N}$. Jeder natürlichen Zahl $n \geq n_0$ sei eine Aussage $A(n)$ zugeordnet, so daß gilt:

- (i) Die Aussage $A(n)$ ist wahr.
- (ii) $\forall n \in \mathbb{N}, n \geq n_0$, gilt: Ist $A(n)$ wahr für alle $m \in \mathbb{N}$ mit $n_0 \leq m \leq n$, so auch $A(n+1)$.

Dann ist $A(n)$ wahr $\forall n \in \mathbb{N}, n \geq n_0$.

□

Sei nun $(H, \circ)$ eine Menge H mit einer Verknüpfung $\circ$. Sind $a, b \in H$, so heißt $a \circ b$ auch das *Produkt* von a und b . Ist $\circ$ zusätzlich assoziativ, d. h. ist $(H, \circ)$ eine Halbgruppe, so können wir das Produkt von drei Elementen $a, b, c \in H$ durch

$$a \circ b \circ c = (a \circ b) \circ c = a \circ (b \circ c)$$

definieren. Das Assoziativgesetz besagt, daß das Produkt von a, b, c unabhängig davon ist, in welcher Weise (die durch die Klammersetzung beschrieben wird) es ausgerechnet wird. Dies überträgt sich auf beliebige endliche Produkte.

Allgemeine Klammerregel 2.8. Ist $(H, \circ)$ eine Halbgruppe, so ist das *Produkt*

$$a_1 \circ \dots \circ a_n := (\dots ((a_1 \circ a_2) \circ a_3) \circ \dots \circ a_{n-1}) \circ a_n$$

unabhängig von der Klammerung definiert.

Beweis. Durch vollständige Induktion wie in 2.7.

Induktionsanfang. Die Aussage ist trivialerweise richtig für $n = 1, 2$. Daß sie für $n = 3$ gilt, besagt das Assoziativgesetz.

Induktionsschluß. Sei $n \in \mathbb{N}, n \geq 3$.

Induktionsannahme. Ist $3 \leq m \leq n$, sind $b_1, \dots, b_m \in H$ beliebig, und ist $P(b_1, \dots, b_m)$ ein durch beliebige Klammerung gewonnenes Produkt von $b_1, \dots, b_m$, so gilt

$$P(b_1, \dots, b_m) = b_1 \circ \dots \circ b_m.$$

Induktionsbehauptung. Sind $a_1, \dots, a_{n+1} \in H$ beliebig, und ist $P(a_1, \dots, a_{n+1})$ ein durch beliebige Klammerung gewonnenes Produkt von $a_1, \dots, a_{n+1} \in H$, so gilt

$$P(a_1, \dots, a_{n+1}) = a_1 \circ \dots \circ a_{n+1}.$$

Seien also $a_1, \dots, a_{n+1} \in H$ und $P(a_1, \dots, a_{n+1})$ ein solches Produkt. Seien weiter a_i und a_{i+1} zwei aufeinanderfolgende Elemente, die bei der Ausrechnung von $P(a_1, \dots, a_{n+1})$ miteinander verknüpft werden. Dann gilt

$$\begin{aligned}
 P(a_1, \dots, a_{n+1}) &= (a_1 \circ \dots \circ a_{i-1}) \circ (a_i \circ a_{i+1}) \circ (a_{i+2} \circ \dots \circ a_{n+1}) \\
 &\stackrel{(*)}{=} (((a_1 \circ \dots \circ a_{i-1}) \circ a_i) \circ a_{i+1}) \circ (a_{i+2} \circ \dots \circ a_{n+1}) \\
 &= (a_1 \circ \dots \circ a_{i+1}) \circ (a_{i+2} \circ \dots \circ a_{n+1}) \\
 &= (a_1 \circ \dots \circ a_{i+1}) \circ ((a_{i+2} \circ \dots \circ a_n) \circ a_{n+1}) \\
 &\stackrel{(*)}{=} ((a_1 \circ \dots \circ a_{i+1}) \circ (a_{i+2} \circ \dots \circ a_n)) \circ a_{n+1} \\
 &= (a_1 \circ \dots \circ a_n) \circ a_{n+1} \\
 &= a_1 \circ \dots \circ a_{n+1}.
 \end{aligned}$$

Dabei haben wir jeweils die Induktionsannahme angewandt (in den mit $(*)$ gekennzeichneten Fällen ist dies direkt das Assoziativgesetz). Für $i = 1$ und $i \geq n - 1$ muß man die Gleichungen richtig interpretieren. □

Definition 2.9. Seien $(H, \circ)$ eine Halbgruppe mit neutralem Element e , $a \in H$ und $n \in \mathbb{Z}$. Dann setzen wir

$$\begin{aligned}
 a^n &= \underbrace{a \circ \dots \circ a}_{n\text{-mal}} \text{ falls } n \geq 0, \\
 a^0 &= e,
 \end{aligned}$$

sowie, falls a invertierbar,

$$a^n = (a^{-1})^{-n} \text{ falls } n < 0.$$

a^n heißt die n -te Potenz von a . □

2

Rechenregeln 2.10. Sei $(G, \circ)$ eine Gruppe mit neutralem Element e . Dann gilt

- (i) $e^{-1} = e$.
- (ii) $(a^{-1})^{-1} = a \quad \forall a \in G$.
- (iii) $(a_1 \circ \dots \circ a_n)^{-1} = a_n^{-1} \circ \dots \circ a_1^{-1} \quad \forall a_1, \dots, a_n \in G$.
- (iv) $a^m \circ a^n = a^{m+n}$, $(a^m)^n = a^{m \cdot n} \quad \forall a \in G \quad \forall m, n \in \mathbb{Z}$.
- (v) $a^m \circ b^n = b^n \circ a^m$, $(a \circ b)^m = a^m \circ b^m \quad \forall n, m \in \mathbb{Z} \quad \forall a, b \in G \text{ mit } a \circ b = b \circ a$.
- (vi) Kürzungsregeln: $\forall a, x, y \in G$ gilt

$$a \circ x = a \circ y \Rightarrow x = y \text{ und } x \circ a = y \circ a \Rightarrow x = y.$$

Beweis. Aufgaben. □

Für den Fall, daß man nachweisen will, daß eine gegebene Halbgruppe eine Gruppe ist, ist es nützlich zu wissen, daß man die Bedingungen (ii), (iii) in Definition 2.4 abschwächen bzw. auch ganz anders ausdrücken kann. In den nächsten drei Sätzen stellen wir entsprechende Kriterien vor:

Satz 2.11. Für eine Halbgruppe $(G, \circ)$ sind äquivalent:

(i) $(G, \circ)$ ist eine Gruppe.

(ii) Es gilt

a) $\exists e \in G$ mit $a \circ e = a \quad \forall a \in G$ (e ist rechtsneutral),

b) $\forall a \in G \exists a' \in G$ mit $a \circ a' = e$ (a' ist zu a rechtsinvers).

(iii) Es gilt

a) $\exists e \in G$ mit $e \circ a = a \quad \forall a \in G$ (e ist linksneutral),

b) $\forall a \in G \exists a' \in G$ mit $a' \circ a = e$ (a' ist zu a linksinvers).

Beweis. ‘(i)⇒(ii)’ und ‘(i)⇒(iii)’ sind klar. Wir zeigen ‘(ii)⇒(i)’ (‘(iii)⇒(i)’ ergibt sich analog).

Sei e ein rechtsneutrales Element. Dann ist e auch linksneutral: Denn ist $a \in G$, so

$$\exists a', a'' \in G \text{ mit } a \circ a' = e, a' \circ a'' = e$$

wegen (ii), b). Es folgt

$$a = a \circ e = a \circ (a' \circ a'') = (a \circ a') \circ a'' = e \circ a''.$$

Setzt man nun a für $e \circ a''$ in

$$e \circ a'' = (e \circ e) \circ a'' = e \circ (e \circ a'')$$

ein, so ergibt sich

$$a = e \circ a.$$

Ist andererseits a' zu $a \in G$ rechtsinvers, so existiert wie eben ein $a'' \in G$ mit $a' \circ a'' = e$, und es folgt wie eben, daß

$$a = e \circ a'' = a'',$$

da wir jetzt bereits wissen, daß e linksneutral ist. Insgesamt erhalten wir

$$a' \circ a = e.$$

□

Satz 2.12. Für eine nichtleere Halbgruppe $(G, \circ)$ sind äquivalent:

(i) $(G, \circ)$ ist eine Gruppe.

(ii) Für beliebige $a, b \in G$ sind die Gleichungen

$$a \circ x = b \text{ und } y \circ a = b$$

eindeutig in G lösbar.

(iii) Für beliebige $a, b \in G$ sind die Gleichungen

$$a \circ x = b \text{ und } y \circ a = b$$

in G lösbar.

Beweis. ‘(i) $\Rightarrow$ (ii)’. Es ist $x := a^{-1} \circ b$ eine Lösung von $a \circ x = b$, denn es gilt

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

Sind x_1, x_2 zwei Lösungen, d. h. gilt

$$a \circ x_1 = b = a \circ x_2,$$

so folgt aus der Kürzungsregel $x_1 = x_2$. Analog behandelt man die zweite Gleichung.

‘(ii) $\Rightarrow$ (iii)’ ist trivialerweise richtig.

‘(iii) $\Rightarrow$ (i)’. Nach Voraussetzung ist $G \neq \emptyset$. Also $\exists a_0 \in G$. Dann

$$\exists e \in G \text{ mit } a_0 \circ e = a_0.$$

Wir zeigen: e ist rechtsneutral. Sei dazu $a \in G$ beliebig. Dann

$$\exists y \in G \text{ mit } y \circ a_0 = a.$$

Es folgt

$$a \circ e = (y \circ a_0) \circ e = y \circ (a_0 \circ e) = y \circ a_0 = a.$$

Zu $a \in G$ können wir die Gleichung

$$a \circ x = e$$

lösen, also ein rechtsinverses Element finden. Mit 2.11 sind wir fertig. □

Satz 2.13. Für eine nichtleere Halbgruppe $(G, \circ)$ sind äquivalent:

(i) $(G, \circ)$ ist eine Gruppe.

(ii) $\forall a \in G$ sind die Linkstranslation

$$G \rightarrow G, x \rightarrow a \circ x,$$

und die Rechtstranslation

$$G \rightarrow G, y \rightarrow y \circ a,$$

bijektiv.

(iii) $\forall a \in G$ sind Links- und Rechtstranslation surjektiv.

Beweis. Offensichtlich sind (ii) bzw. (iii) äquivalent zu (ii) bzw. (iii) in 2.12. $\square$

Bemerkung 2.14. Eine Verknüpfung auf einer endlichen Menge $G = \{a_1, \dots, a_n\}$ kann man im Prinzip dadurch angeben, daß man alle $a_i \circ a_j$ in einem quadratischen Schema ähnlich einer Matrix aufschreibt. Dabei steht $a_i \circ a_j$ in der i-ten Zeile und der j-ten Spalte der *Verknüpfungstafel* (oder im Falle einer Gruppe der *Gruppentafel*):

$\circ$	...	a_j	...
$\vdots$			
a_i		$a_i \circ a_j$	
$\vdots$			

Weiß man bereits, daß $\circ$ assoziativ ist (dies muß man für alle Tripel a_i, a_j, a_k nachprüfen), so kann man aus der Verknüpfungstafel ablesen, ob $(G, \circ)$ eine Gruppe ist: Nach obigen Kriterien bedeutet dies, daß in jeder Zeile und in jeder Spalte der Tafel jedes a_i genau einmal vorkommt.

Daraus folgt sofort, daß es nur eine Möglichkeit gibt, eine zweielementige Menge zu einer Gruppe zu machen: Ein Element, etwa e , muss neutral sein. Bezeichnen wir mit a das andere Element, so ergibt sich die einzig mögliche Gruppentafel wie folgt:

$\circ$	e	a
e	e	a
a	a	e

Für $n = 3$ und $G = \{e, a, b\}$ erhält man ebenfalls nur eine mögliche Gruppentafel, nämlich die folgende:

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

In beiden Fällen ergibt sich aus der Tafel, daß die Gruppe kommutativ ist. $\square$

Betrachtet man in der Mathematik Strukturen auf Mengen, so stellt sich immer auch die Frage, wie diese Strukturen mit mengentheoretischen Operationen und mit Abbildungen verträglich sind. Wir wollen einige Antworten auf diese Frage im Fall der Gruppenstruktur geben.

Definition 2.15. Seien $(G, \circ)$ eine Gruppe und $U \subset G$ eine Teilmenge. Dann heißt U *Untergruppe* von G , wenn folgendes gilt:

- (i) U ist bzgl. $\circ$ abgeschlossen.
- (ii) U zusammen mit der induzierten Verknüpfung ist eine Gruppe.

□

Satz 2.16. Seien $(G, \circ)$ eine Gruppe und $U \subset G$. Dann sind die folgenden Bedingungen äquivalent:

- (i) U ist eine Untergruppe von G .
- (ii) $U \neq \emptyset$ und es gilt:

$$\begin{aligned} a, b \in U &\Rightarrow a \circ b \in U, \\ a \in U &\Rightarrow a^{-1} \in U. \end{aligned}$$

- (iii) $U \neq \emptyset$ und es gilt:

$$a, b \in U \Rightarrow a \circ b^{-1} \in U.$$

Beweis. ‘(i)⇒(ii)’. Daß U bzgl. $\circ$ abgeschlossen ist, bedeutet gerade, daß gilt $a, b \in U \Rightarrow a \circ b \in U$. Ist e das neutrale Element von G und e' dasjenige von U , so gilt

$$e \circ e' = e' = e' \circ e'$$

und die Kürzungsregel in G liefert $e = e'$. Also ist das neutrale Element von G auch dasjenige von U . $U \neq \emptyset$, da es mindestens das neutrale Element enthalten muß. Ist $a \in U$, so

$$\exists a' \in U \text{ mit } a' \circ a = e = a \circ a'.$$

Wegen der Eindeutigkeit des Inversen in G folgt

$$a^{-1} = a' \in U.$$

‘(ii)⇒(iii)’. $a, b \in U \Rightarrow a, b^{-1} \in U \Rightarrow a \circ b^{-1} \in U$

‘(iii)⇒(i)’. $U \neq \emptyset \Rightarrow \exists a_0 \in U$. Also ist

$$e = a_0 \circ a_0^{-1} \in U.$$

Ist $a \in U$, so ist auch

$$a^{-1} = e \circ a^{-1} \in U.$$

Sind schließlich $a, b \in U$, so auch

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

Also ist U bzgl. $\circ$ abgeschlossen, besitzt ein neutrales Element und zu jedem Element das inverse Element. □

Beispiel 2.17. (i) $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$ sind Untergruppen. Ebenso $(\mathbb{Q} \setminus \{0\}, \cdot) \subset (\mathbb{R} \setminus \{0\}, \cdot)$.

(ii) Wir betrachten die Permutationsgruppe S_4 und die durch

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

gegebene Teilmenge

$$U = \{e, a, b, c\} \subset S_4.$$

Aus der Verknüpfungstafel können wir ablesen, daß $(U, \circ)$ eine kommutative Untergruppe von $(S_4, \circ)$ ist (*Kleinsche Vierergruppe*):

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

□

Bemerkung und Definition 2.18. Sei $(G, \circ)$ eine Gruppe.

(i) Ist $(U_i)_{i \in I}$ eine Familie von Untergruppen, so folgt aus 2.16, daß auch

$$\bigcap_{i \in I} U_i \subset G$$

eine Untergruppe ist.

(ii) Sei $A \subset G$ eine Teilmenge. Dann ist

$$U(A) := \bigcap_{\substack{U \subset G \\ \text{Untergruppe} \\ A \subset U}} U$$

die kleinste Untergruppe von G , die A enthält. Wir nennen $U(A)$ die von A erzeugte Untergruppe. Sie besteht aus allen endlichen Produkten, die aus den Elementen von A und deren Inversen gebildet werden können.

Ist speziell $A = \{a_1, \dots, a_n\}$ endlich, so schreiben wir auch

$$U(a_1, \dots, a_n) = U(\{a_1, \dots, a_n\}).$$

Im Falle eines Elementes a besteht $U(a)$ aus allen Potenzen $a^n, n \in \mathbb{Z}$. Insbesondere ist $U(a)$ kommutativ.

- (iii) Ist $A \subset G$ mit $U(A) = G$, so nennen wir die Elemente von A auch ein *Erzeugendensystem* von G . Eine Gruppe, die ein endliches Erzeugendensystem besitzt, heißt *endlich erzeugte Gruppe*. Gibt es ein $a \in G$ mit $U(a) = G$, so heißt G *zyklisch*. Zyklische Gruppe sind kommutativ.

□

Beispiel 2.19. (i) Für $n \in \mathbb{N}$ ist

$$n \cdot \mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$$

eine zyklische Untergruppe von $(\mathbb{Z}, +)$. Umgekehrt ist jede Untergruppe von $(\mathbb{Z}, +)$ von dieser Form (Aufgaben).

- (ii) Wir betrachten

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3.$$

Wie sieht $U(\sigma, \tau) \subset S_3$ aus? $U(\sigma, \tau)$ ist abgeschlossen bzgl. $\circ$, enthält also die folgenden Elemente:

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \\ \tau &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & \sigma^2 \circ \tau &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

Es folgt $U(\sigma, \tau) = S_3$, d.h. σ und τ erzeugen S_3 .

□

2

Aufgaben

Aufgabe 9. Sei S_n die Permutationsgruppe von $\{1, \dots, n\}$. Zeigen Sie durch vollständige Induktion nach n :

- (i) S_n hat genau $n!$ Elemente. Dabei ist $n!$ induktiv definiert durch

$$0! = 1 \text{ und } n! = n(n-1)!.$$

- (ii) Jedes $\sigma \in S_n$, $n \geq 2$, läßt sich als Produkt von endlich vielen Transpositionen schreiben.

Aufgabe 10. Zeigen Sie die Rechenregeln 2.10 aus der Vorlesung.

Aufgabe 11. Bestimmen Sie alle Untergruppen

- (i) der Kleinschen Vierergruppe,
- (ii) der Permutationsgruppe S_3 .

Aufgabe 12. Zeigen Sie: Ist U eine Untergruppe von $(\mathbb{Z}, +)$, so existiert $n \in \mathbb{N}$ mit

$$U = n\mathbb{Z}.$$

Insbesondere ist jede Untergruppe von $(\mathbb{Z}, +)$ zyklisch.

Hinweis: Verwenden Sie Satz 1.12 und Aufgabe 2.

Bemerkung und Definition 2.20. Seien $(G, \circ)$ eine Gruppe und $H \subset G$ eine Untergruppe. Dann ist durch

$$a \underset{l}{\overset{H}{\sim}} b \Leftrightarrow \exists h \in H \text{ mit } a = b \circ h$$

eine Äquivalenzrelation in G definiert. Denn:

$\underset{l}{\overset{H}{\sim}}$ ist reflexiv: $a \underset{l}{\overset{H}{\sim}} a$, da $e \in H$ und $a = a \circ e$.

$\underset{l}{\overset{H}{\sim}}$ ist symmetrisch: $a \underset{l}{\overset{H}{\sim}} b \Rightarrow \exists h \in H \text{ mit } a = b \circ h \Rightarrow b = a \circ h^{-1} \text{ mit } h^{-1} \in H \Rightarrow b \underset{l}{\overset{H}{\sim}} a$.

$\underset{l}{\overset{H}{\sim}}$ ist transitiv: $a \underset{l}{\overset{H}{\sim}} b, b \underset{l}{\overset{H}{\sim}} c \Rightarrow \exists h_1, h_2 \in H \text{ mit } a = b \circ h_1, b = c \circ h_2 \Rightarrow a = c \circ (h_2 \circ h_1) \text{ mit } h_2 \circ h_1 \in H \Rightarrow a \underset{l}{\overset{H}{\sim}} c$.

Wir schreiben

$$aH := \{a \circ h \mid h \in H\}$$

für die von a repräsentierte Äquivalenzklasse. Jede solche heißt auch *Linksnebenklasse* von H .

Analog erhält man durch

$$a \underset{r}{\overset{H}{\sim}} b \Leftrightarrow \exists h \in H \text{ mit } a = h \circ b$$

eine Äquivalenzrelation. Jede Äquivalenzklasse

$$Ha = \{h \circ a \mid h \in H\}$$

heißt *Rechtsnebenklasse* von H . Durch

$$G/\underset{l}{\overset{H}{\sim}} \rightarrow G/\underset{r}{\overset{H}{\sim}}, aH \rightarrow Ha^{-1},$$

ist eine bijektive Abbildung mit der Umkehrabbildung

$$G/\underset{r}{\overset{H}{\sim}} \rightarrow G/\underset{l}{\overset{H}{\sim}}, Ha \rightarrow a^{-1}H,$$

definiert. □

Bemerkung und Definition 2.21. Sei $(G, \circ)$ eine endliche Gruppe. Wir bezeichnen mit $|G|$ die Anzahl der Elemente von G . $|G|$ heißt auch die *Ordnung* von G . Ist $H \subset G$ eine Untergruppe, so bezeichnet $[G : H]$ die Anzahl der Linksnebenklassen und somit auch die Anzahl der Rechtsnebenklassen von H . $[G : H]$ heißt der *Index* von H in G . $\square$

Indexsatz 2.22. Ist $(G, \circ)$ eine endliche Gruppe und $H \subset G$ eine Untergruppe, so gilt

$$|G| = [G : H] \cdot |H|.$$

Beweis. Nach 1.28 ist G die Vereinigung seiner Linksnebenklassen und diese sind paarweise disjunkt und nicht leer. Ist also $n := [G : H]$, so können wir $a_1, \dots, a_n \in G$ finden mit $G = \bigcup_{i=1}^n a_i H$ und $a_i H \cap a_j H = \emptyset$ für $i \neq j$.

Daraus ergibt sich, daß die Abbildung

$$\{1, \dots, n\} \times H \rightarrow G, (i, h) \rightarrow a_i \circ h,$$

bijektiv ist, woraus die Behauptung folgt. $\square$

Satz von Lagrange 2.23. Sind $(G, \circ)$ eine endliche Gruppe und $H \subset G$ eine Untergruppe, so ist $|H|$ ein Teiler von $|G|$.

Beweis. Klar nach 2.22. $\square$

Bemerkung und Definition 2.24. Sei $(G, \circ)$ eine Gruppe. Eine Untergruppe $N \subset G$ heißt *normal* oder ein *Normalteiler* (in G), wenn gilt:

$$aN = Na \quad \forall a \in G.$$

In diesem Fall brauchen wir also nicht zwischen Links- und Rechtsnebenklassen zu unterscheiden und sprechen dann einfach von Nebenklassen. Die Menge aller *Nebenklassen* von N wird mit G/N bezeichnet. $\square$

Satz und Definition 2.25. Sei $(G, \circ)$ eine Gruppe mit Neutralelement e und $N \subset G$ ein Normalteiler. Dann wird durch

$$G/N \times G/N \rightarrow G/N, (aN, bN) \rightarrow (a \circ b)N,$$

eine Verknüpfung $\circ$ auf G/N definiert, so daß $(G/N, \circ)$ eine Gruppe mit Neutralelement $N = eN$ ist. Diese Gruppe heißt *Quotientengruppe* oder *Faktorgruppe* von G nach N .

Beweis. Wir müssen zunächst zeigen, daß $\circ$ wohldefiniert ist, d. h. nicht von der Wahl der Repräsentanten abhängt. Seien also

$$a_1 N = a_2 N \text{ und } b_1 N = b_2 N, a_i, b_i \in G.$$

Dann $\exists n, m \in N$ mit

$$a_1 = a_2 \circ n \text{ und } b_1 = b_2 \circ m.$$

Es folgt

$$a_1 \circ b_1 = a_2 \circ n \circ b_2 \circ m.$$

Nach Voraussetzung an N ist

$$Nb_2 = b_2N.$$

Also $\exists p \in N$ mit

$$n \circ b_2 = b_2 \circ p.$$

Insgesamt folgt

$$a_1 \circ b_1 = a_2 \circ (n \circ b_2) \circ m = a_2 \circ b_2 \circ (p \circ m)$$

mit $p \circ m \in N$, und somit

$$(a_1 \circ b_1)N = (a_2 \circ b_2)N.$$

Also ist $\circ$ eine wohldefinierte Verknüpfung auf G/N .

Diese ist assoziativ:

$$\begin{aligned} (aN \circ bN) \circ cN &= ((a \circ b)N) \circ cN = ((a \circ b) \circ c)N = (a \circ (b \circ c))N \\ &= aN \circ ((b \circ c)N) = aN \circ (bN \circ cN). \end{aligned}$$

Weiter ist $N = eN$, e das Neutralelement von G , ein Neutralelement in G/N :

$$eN \circ aN = (e \circ a)N = aN = (a \circ e)N = aN \circ eN.$$

Schließlich ist $a^{-1}N$ zu aN invers:

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

Insgesamt ist $(G/N, \circ)$ eine Gruppe. □

Beispiel 2.26. (i) Ist $(G, \circ)$ eine abelsche Gruppe, so ist jede Untergruppe N von G ein Normalteiler. Die Faktorgruppe G/N ist dann abelsch:

$$aN \circ bN = (a \circ b)N = (b \circ a)N = bN \circ aN.$$

- (ii) Insbesondere ist für jedes $n \in \mathbb{N}$ die Untergruppe $n\mathbb{Z}$ von $(\mathbb{Z}, +)$ aus Beispiel 2.19 ein Normalteiler und somit

$$(\mathbb{Z}/n\mathbb{Z}, +)$$

eine abelsche Gruppe. Ist $a \in \mathbb{Z}$, so schreiben wir auch $\bar{a}$ für die Nebenklasse von a . Es gilt dann

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

$a, a' \in \mathbb{Z}$ liegen genau dann in derselben Nebenklasse, wenn $a - a'$ durch n teilbar ist. Man schreibt dann auch

$$a \equiv a' \pmod{n}$$

und sagt, a ist kongruent zu a' modulo n . Ist z. B. $n = 5$, so ist etwa 7 kongruent zu 2, und für die Addition in $\mathbb{Z}/5\mathbb{Z}$ gilt z. B.

$$\bar{3} + \bar{4} = \overline{3+4} = \bar{7} = \bar{2}.$$

□

Satz 2.27. Seien $(G, \circ)$ eine Gruppe und $N \subset G$ eine Untergruppe. Dann sind äquivalent:

- (i) N ist normal, d. h. $aN = Na \ \forall a \in G$.
- (ii) $aNa^{-1} := \{a \circ n \circ a^{-1} \mid n \in N\} = N \ \forall a \in G$.
- (iii) $aNa^{-1} \subset N \ \forall a \in G$.

Beweis. Sicher ist (i) äquivalent zu (ii). ‘(ii) $\Rightarrow$ (iii)’ ist klar.

Wir zeigen ‘(iii) $\Rightarrow$ (ii)’. Seien $a \in G, n \in N$. Dann gilt

$$n = a \circ (a^{-1} \circ n \circ a) \circ a^{-1} \in aNa^{-1},$$

da $a^{-1} \circ n \circ a \in N$ nach (iii). Also ist $N \subset aNa^{-1}$ und somit gilt $N = aNa^{-1}$. □

Bemerkung und Definition 2.28. Sei $(G_i, \circ_i)_{i \in I}$ eine Familie von Gruppen und sei $e_i, i \in I$, das jeweilige neutrale Element. Dann ist durch

$$\prod_{i \in I} G_i \times \prod_{i \in I} G_i \rightarrow \prod_{i \in I} G_i, ((a_i)_{i \in I}, (b_i)_{i \in I}) \rightarrow (a_i \circ_i b_i)_{i \in I},$$

eine Verknüpfung auf $\prod_{i \in I} G_i$ definiert. Diese macht $\prod_{i \in I} G_i$ zu einer Gruppe. Wir sprechen vom *direkten Produkt* der Gruppen $(G_i)_{i \in I}$. Das neutrale Element ist $(e_i)_{i \in I}$ und zu $(a_i)_{i \in I}$ ist $(a_i^{-1})_{i \in I}$ invers.

Durch

$$\bigoplus_{i \in I} G_i := \{(a_i)_{i \in I} \in \prod_{i \in I} G_i \mid a_i = e_i \text{ bis auf endlich viele } i\}$$

ist eine Untergruppe von $\prod_{i \in I} G_i$ definiert. Diese heißt die *direkte Summe* der $(G_i, \circ_i)_{i \in I}$. Ist I endlich, so stimmen $\prod_{i \in I} G_i$ und $\bigoplus_{i \in I} G_i$ überein. □

Beispiel 2.29. Ist $I = \{1, \dots, n\}$ und $(G_i, \circ_i) = (\mathbb{R}, +)$ für $i = 1, \dots, n$, so ergibt sich als direktes Produkt $\mathbb{R}^n$ mit der bereits in der Motivation betrachteten komponentenweise Addition

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n).$$

□

Wir kommen nun zu den Abbildungen, die mit den bisher behandelten Strukturen auf Mengen verträglich sind.

Definition 2.30. Seien $(G, \circ)$ und $(H, *)$ Gruppen bzw. Monoide bzw. Halbgruppen. Eine Abbildung $\varphi : G \rightarrow H$ heißt *Homomorphismus* (von Gruppen bzw. Monoiden bzw. Halbgruppen), wenn gilt

$$\varphi(a \circ b) = \varphi(a) * \varphi(b) \quad \forall a, b \in G.$$

Wir schreiben

$$\text{Hom}(G, H) := \{\varphi : G \rightarrow H \mid \varphi \text{ ist Homomorphismus}\}.$$

$\varphi \in \text{Hom}(G, H)$ heißt

- *Monomorphismus*, falls φ injektiv,
- *Epimorphismus*, falls φ surjektiv,
- *Isomorphismus*, falls φ bijektiv.

Wir sagen G und H sind *isomorph*, in Zeichen $G \cong H$, falls es einen Isomorphismus $\varphi : G \rightarrow H$ gibt.

Ist speziell $G = H$, so heißt jeder Homomorphismus auch *Endomorphismus* von G und jeder Isomorphismus auch *Automorphismus* von G . $\text{End}(G)$ bzw. $\text{Aut}(G)$ bezeichnet die Menge aller Endo- bzw. Automorphismen von G . □

Bemerkung 2.31. (i) Sind

$$\varphi : G \rightarrow H \text{ und } \psi : H \rightarrow K$$

Homomorphismen, so auch

$$\psi \circ \varphi : G \rightarrow K.$$

Gleiches gilt für Mono-, Epi- und Isomorphismen.

(ii) Ist $\varphi : G \rightarrow H$ ein Isomorphismus, so auch φ^{-1} . In der Tat ist φ^{-1} bijektiv, und sind $f, g \in H$, so existieren $a, b \in G$ mit $\varphi(a) = f$, $\varphi(b) = g$, da φ surjektiv, also gilt

$$\varphi^{-1}(f * g) = \varphi^{-1}(\varphi(a) * \varphi(b)) = \varphi^{-1}(\varphi(a \circ b)) = a \circ b = \varphi^{-1}(f) \circ \varphi^{-1}(g).$$

(iii) Ist $(G, \circ)$ eine Gruppe, so ist

$$\text{Aut}(G) \subset S(G)$$

eine Untergruppe.

□

Satz und Definition 2.32. Seien $(G, \circ)$ und $(H, *)$ Gruppen mit neutralem Element e_G bzw. e_H . Sei weiter $\varphi : G \rightarrow H$ ein Homomorphismus. Dann gilt:

- (i) $\varphi(a^n) = \varphi(a)^n \quad \forall a \in G \quad \forall n \in \mathbb{Z}$. Insbesondere ist $\varphi(e_G) = e_H$.
- (ii) $\text{Bild } \varphi = \varphi(G)$ ist eine Untergruppe von H , das Bild von φ .
- (iii) $\text{Kern } \varphi := \{a \in G \mid \varphi(a) = e_H\}$ ist ein Normalteiler in G , der Kern von φ .
- (iv) φ ist ein Monomorphismus $\Leftrightarrow \text{Kern } \varphi = \{e_G\}$.

Beweis. (i) $n = 0$: Aus

$$e_H * \varphi(e_G) = \varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G)$$

folgt mit der Kürzungsregel

$$e_H = \varphi(e_G).$$

$n > 0$: Es gilt

$$\varphi(a^n) = \varphi(a^{n-1} \circ a) = \varphi(a^{n-1}) \circ \varphi(a) \quad \forall a \in G$$

und die Aussage folgt mit Induktion.

$n < 0$: Sei $a \in G$. Dann gilt

$$e_H = \varphi(e_G) = \varphi(a \circ a^{-1}) = \varphi(a) * \varphi(a^{-1})$$

und somit

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

Es folgt

$$\varphi(a^n) = \varphi((a^{-1})^{-n}) = (\varphi(a^{-1}))^{-n} = ((\varphi(a))^{-1})^{-n} = \varphi(a)^n.$$

- (ii) $\text{Bild } \varphi \neq \emptyset$, wegen $e_H = \varphi(e_G) \in \text{Bild } \varphi$. Sind weiter $f, g \in \text{Bild } \varphi$, so $\exists a, b \in G$ mit $f = \varphi(a)$, $g = \varphi(b)$. Es folgt

$$f * g^{-1} = \varphi(a) * \varphi(b)^{-1} = \varphi(a) * \varphi(b^{-1}) = \varphi(a \circ b^{-1}) \in \text{Bild } \varphi$$

(iii) $\text{Kern } \varphi \neq \emptyset$, da $e_G \in \text{Kern } \varphi$. Sind $a, b \in \text{Kern } \varphi$, so gilt

$$\varphi(a \circ b^{-1}) = \varphi(a) * \varphi(b)^{-1} = e_H * e_H = e_H,$$

d. h. $a \circ b^{-1} \in \text{Kern } \varphi$. $\text{Kern } \varphi$ ist also eine Untergruppe.

Sind $a \in G$ und $n \in \text{Kern } \varphi$, so gilt

$$\varphi(a \circ n \circ a^{-1}) = \varphi(a) * \varphi(n) * \varphi(a^{-1}) = \varphi(a) * e_H * \varphi(a)^{-1} = e_H,$$

d. h. $a \circ n \circ a^{-1} \in \text{Kern } \varphi$. Nach 2.27 ist $\text{Kern } \varphi$ ein Normalteiler.

(iv) ' $\Rightarrow$ '. $a \in \text{Kern } \varphi \Rightarrow \varphi(a) = e_H = \varphi(e_G) \Rightarrow a = e_G$. Andererseits liegt e_G immer im Kern.

' $\Leftarrow$ '. $a, b \in G$ mit $\varphi(a) = \varphi(b) \Rightarrow \varphi(a \circ b^{-1}) = e_H \Rightarrow a \circ b^{-1} = e_G \Rightarrow a = b$

□

Bemerkung 2.33. (i) Ist $(G, \circ)$ eine Gruppe und $N \subset G$ ein Normalteiler, so ist die kanonische Projektion

$$\pi : G \rightarrow G/N, a \rightarrow aN,$$

ein Epimorphismus, denn π ist surjektiv mit

$$\pi(a \circ b) = (a \circ b)N = aN \circ bN \quad \forall a, b \in G.$$

Weiter gilt

$$\text{Kern } \pi = N :$$

$$a \in \text{Kern } \pi \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N.$$

z. B. ist

$$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \rightarrow \bar{a},$$

ein Epimorphismus mit $n\mathbb{Z}$ als Kern.

2

(ii) Sind $(G, \circ)$, $(H, *)$ Gruppen und $\varphi : G \rightarrow H$ ein Homomorphismus, so existiert nach 1.30 eine Abbildung $\bar{\varphi} : G/\text{Kern } \varphi \rightarrow H$, so daß

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/\text{Kern } \varphi \\ \varphi \searrow & & \swarrow \bar{\varphi} \\ & H & \end{array}$$

kommutiert. Nach 1.31 ist $\bar{\varphi}$ injektiv, also ein Monomorphismus, denn per Definition gilt

$$\bar{\varphi}((a \text{ Kern } \varphi) \circ (b \text{ Kern } \varphi)) = \varphi(a \circ b) = \varphi(a) * \varphi(b) = \bar{\varphi}(a \text{ Kern } \varphi) * \bar{\varphi}(b \text{ Kern } \varphi).$$

Ist φ ein Epimorphismus, so ist $\bar{\varphi}$ ein Isomorphismus. In jedem Fall ist $\bar{\varphi}$ ein Isomorphismus als Abbildung

$$\bar{\varphi} : G/\text{Kern } \varphi \rightarrow \text{Bild } \varphi.$$

(iii) Ist $(G_i, \circ_i)$ eine Familie von Gruppen und ist $J \subset I$, so ist die Projektion

$$\prod_{i \in I} G_i \rightarrow \prod_{j \in J} G_j, (g_i)_{i \in I} \rightarrow (g_j)_{j \in J},$$

ein Epimorphismus. □

Notation 2.34. Benutzt man statt des neutralen Zeichens $\circ$ das Zeichen $+$ bzw. $\cdot$, so sprechen wir von einer *additiven* bzw. *multiplikativen Gruppe* (Halbgruppe, ...) und schreiben 0 bzw. 1 für das Neutralelement sowie $-a$ bzw. $\frac{1}{a}$ für ein zu a inverses Element. Sind $a_1, \dots, a_n$ Gruppenelemente, so schreiben wir auch abkürzend

$$\sum_{i=1}^n a_i = a_1 + \dots + a_n \quad \text{bzw.} \quad \prod_{i=1}^n a_i = a_1 \cdot \dots \cdot a_n$$

(im letzteren Fall lässt man das Zeichen $\cdot$ auch einfach weg.) □

Bei Gruppen haben wir nur eine Verknüpfung betrachtet. Andererseits sind z. B. auf den ganzen Zahlen $\mathbb{Z}$ zwei Verknüpfungen erklärt, nämlich Addition und Multiplikation, die in geregelter Beziehung zueinander stehen. Abstrahiert man die dort gültigen Rechenregeln, so erhält man wie bei Gruppen neue algebraische Strukturen auf Mengen.

Definition 2.35. Eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ auf R heißt *Ring*, falls folgendes gilt:

- (i) $(R, +)$ ist eine abelsche Gruppe.
- (ii) $(R, \cdot)$ ist eine Halbgruppe.
- (iii) Es gelten die *Distributivgesetze*

$$a(b + c) = ab + ac, (b + c)a = ba + ca \quad \forall a, b, c \in R$$

(Multiplikation bindet stärker als Addition.)

In diesem Fall schreiben wir 0 für das Neutralelement von $(R, +)$ (*'Nullelement'*).

Ein Ring R heißt

- *kommutativ*, falls $(R, \cdot)$ kommutativ ist,
- *Ring mit 1*, falls $(R, \cdot)$ ein neutrales Element besitzt, das dann mit 1 bezeichnet wird (*'Einselement'*). □

Rechenregeln 2.36. Sei $(R, +, \cdot)$ ein Ring. Dann gilt:

- (i) $a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in R$.
- (ii) $a(-b) = (-a)b = -(ab), \quad (-a)(-b) = ab \quad \forall a, b \in R$.
- (iii) Ist $R \neq \{0\}$ ein Ring mit 1, so gilt $0 \neq 1$.
- (iv) Allgemeines Distributivgesetz: Sind $a_1, \dots, a_n, b_1, \dots, b_m \in R$, so gilt

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

Beweis. Übung. □

Aufgaben

Aufgabe 13. (i) Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Zeigen Sie:

- a) $U \subset G$ Untergruppe $\Rightarrow \varphi(U) \subset H$ Untergruppe.
 b) $V \subset H$ Untergruppe $\Rightarrow \varphi^{-1}(V) \subset G$ Untergruppe.

(ii) Welche der folgenden Abbildungen sind Gruppenhomomorphismen von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$?

$$\text{a) } \mathbb{Z} \rightarrow \mathbb{Z}, \quad a \rightarrow 2a \qquad \text{b) } \mathbb{Z} \rightarrow \mathbb{Z}, \quad a \rightarrow a + 1.$$

Begründen Sie Ihre Aussage.

Aufgabe 14. (i) Sei $(G, \circ)$ eine Gruppe. Zeigen Sie: Das **Zentrum von G** ,

$$Z(G) := \{z \in G \mid a \circ z = z \circ a \quad \forall a \in G\}$$

ist ein Normalteiler in G .

(ii) Bestimmen Sie $Z(S_3)$.

Aufgabe 15. Konstruieren Sie eine Gruppe mit 4 Elementen, die nicht isomorph zur Kleinschen Vierergruppe ist. Begründen Sie, daß es sich tatsächlich um eine Gruppe handelt, und daß diese nicht isomorph zur Kleinschen Vierergruppe ist.

Aufgabe 16. (i) Sei X eine Menge. Zeigen Sie: Durch

$$A \sim B \Leftrightarrow \exists \text{ bijektive Abbildung } A \rightarrow B$$

ist eine Äquivalenzrelation in $\mathcal{P}(X)$ definiert.

- (ii) Sei X eine endliche Menge mit n Elementen. Wieviele Äquivalenzklassen gibt es bzgl. $\sim$ wie in (i)?

Beispiel 2.37. (i) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1. Gleiches gilt für $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$.

- (ii) Ist $I \subset \mathbb{R}$ ein Intervall (vergleiche Analysis) und

$$R := \{f : I \rightarrow \mathbb{R} \mid f \text{ Abbildung}\},$$

so erklären wir die Addition $f + g$ bzw. die Multiplikation $f \cdot g$ durch

$$(f + g)(x) := f(x) + g(x), \text{ bzw.}$$

$$(f \cdot g)(x) := f(x) \cdot g(x) \quad \forall x \in I.$$

Aus den Ringeigenschaften von $\mathbb{R}$ ergibt sich sofort, daß dadurch $(R, +, \cdot)$ zu einem kommutativen Ring mit 1 wird.

- (iii) In $\mathbb{Z}/n\mathbb{Z}$ können wir zusätzlich zur Addition eine Multiplikation erklären, und zwar durch folgende Vorschrift:

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b} \quad \forall a, b \in \mathbb{Z}.$$

Diese Definition ist unabhängig von der Repräsentantenwahl:

Gilt $\bar{a} = \bar{a'}$ und $\bar{b} = \bar{b'}$, so $\exists k, l \in \mathbb{Z}$ mit $a - a' = nk$ und $b - b' = nl$, es folgt

$$a \cdot b = (a' + nk) \cdot (b' + nl) = a'b' + n(b'k + a'l + kln).$$

Also gilt $\bar{a} \cdot \bar{b} = \overline{a' \cdot b'}$. Aus den Ringeigenschaften von $\mathbb{Z}$ ergibt sich sofort, daß $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1 ist. Wir schreiben die Multiplikationstabellen für $n = 2, 3, 4$ auf (dabei lassen wir die Multiplikation mit $\bar{0}$ weg).

$$n=2: \begin{array}{c|c} \cdot & \bar{1} \\ \hline \bar{1} & \bar{1} \end{array} \quad n=3: \begin{array}{c|cc} \cdot & \bar{1} & \bar{2} \\ \hline \bar{1} & \bar{1} & \bar{2} \\ \bar{2} & \bar{2} & \bar{1} \end{array} \quad n=4: \begin{array}{c|ccc} \cdot & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{1} & \bar{1} & \bar{2} & \bar{3} \\ \bar{2} & \bar{2} & \bar{0} & \bar{2} \\ \bar{3} & \bar{3} & \bar{2} & \bar{1} \end{array}$$

Wir sehen, daß $(\mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ für $n = 2$ und 3 eine Gruppe ist, für $n = 4$ jedoch nicht:

$$\bar{2} \cdot \bar{2} = \bar{0} \notin \mathbb{Z}/4\mathbb{Z} \setminus \{\bar{0}\}.$$

□

Obiges Beispiel motiviert die

Definition 2.38. Ein Ring R heißt *nullteilerfrei*, wenn gilt:

$$a, b \in R, a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0$$

□

Beispiel 2.39. (i) $\mathbb{Z}$ ist nullteilerfrei.

(ii) Für $n \in \mathbb{Z}, n \geq 2$ gilt:

$$\mathbb{Z}/n\mathbb{Z} \text{ nullteilerfrei} \Leftrightarrow n \text{ ist Primzahl,}$$

d. h. n ist nur durch 1 und sich selbst teilbar:

‘ $\Rightarrow$ ’. Sei n keine Primzahl. Dann

$$\exists k, l \in \mathbb{Z}, 1 < k, l < n, \text{ mit } n = kl.$$

Es folgt

$$\bar{k} \neq 0 \neq \bar{l}, \text{ aber } \bar{k} \cdot \bar{l} = \overline{k \cdot l} = \bar{n} = \bar{0},$$

d. h. $\mathbb{Z}/n\mathbb{Z}$ ist nicht nullteilerfrei.

‘ $\Leftarrow$ ’. Sei umgekehrt n eine Primzahl. Sei weiter

$$k, l \in \mathbb{Z} \text{ mit } \bar{k} \cdot \bar{l} = \bar{0}.$$

Dann

$$\exists r \in \mathbb{Z} \text{ mit } k \cdot l = n \cdot r.$$

Somit ist k oder l ein Vielfaches von n , also ist entweder $\bar{k} = \bar{0}$ oder $\bar{l} = \bar{0}$.

□

Viele der bei Gruppen behandelten Begriffe und Aussagen lassen sich analog für Ringe definieren und formulieren. Hier sind einige Beispiele:

Bemerkung und Definition 2.40. Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $R' \subset R$ heißt *Unterring* von R , falls gilt:

(i) R' ist eine Untergruppe von R bzgl. $+$.

(ii) R' ist abgeschlossen bzgl. $\cdot$.

In diesem Fall ist R' zusammen mit den induzierten Verknüpfungen $+$ und $\cdot$ wieder ein Ring.

Wie in 2.18 ergibt sich, daß der Durchschnitt einer beliebigen Familie von Unterringen von R wieder ein Unterring von R ist. □

Bemerkung und Definition 2.41. Seien $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe. Eine Abbildung

$$\varphi : R \rightarrow S$$

heißt *Homomorphismus* (von Ringen), wenn gilt:

$$(i) \quad \varphi(a + b) = \varphi(a) + \varphi(b) \quad \forall a, b \in R,$$

$$(ii) \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in R.$$

Mit anderen Worten: φ ist ein Gruppenhomomorphismus von $(R, +)$ in $(S, +)$ und ein Halbgruppenhomomorphismus von $(R, \cdot)$ in $(S, \cdot)$.

Die weiteren Begriffe bzw. Aussagen aus 2.30 und 2.31, (i), (ii) übertragen sich wortwörtlich. $\square$

Beispiel 2.42. (i) $n\mathbb{Z}$ ist ein Unterring von $\mathbb{Z}$.

(ii) Die Projektion

$$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad a \rightarrow \bar{a},$$

ist ein Homomorphismus von Ringen. $\square$

Wie $(\mathbb{Z}, +, \cdot)$ ist auch $(\mathbb{Q}, +, \cdot)$ ein kommutativer Ring mit 1. Tatsächlich gilt aber mehr: $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist sogar eine abelsche Gruppe. Dies wollen wir nun abstrahieren:

Definition 2.43. Ein kommutativer Ring $(K, +, \cdot)$ mit 1 heißt *Körper*, wenn zusätzlich folgendes gilt:

$$K^* := (K \setminus \{0\}, \cdot) \text{ ist eine abelsche Gruppe.}$$

Mit anderen Worten: Eine Menge K zusammen mit zwei Verknüpfungen $+$ und $\cdot$ auf K heißt Körper, falls gilt:

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

(ii) $(K^*, \cdot)$ ist eine abelsche Gruppe.

(iii) Es gelten die Distributivgesetze

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca \quad \forall a, b, c \in K.$$

$\square$

Rechenregeln 2.44. Sei $(K, +, \cdot)$ ein Körper. Dann gilt:

(i) $1 \neq 0$, ein Körper hat also mindestens zwei Elemente.

(ii) K ist nullteilerfrei.

(iii) Kürzungsregel: $\forall a, x, y \in K$ gilt:

$$xa = ya, a \neq 0 \Rightarrow x = y$$

Bemerkung und Definition 2.45. Sei $(K, +, \cdot)$ ein Körper. Eine Teilmenge $K' \subset K$ heißt *Unterkörper* von K , falls gilt:

(i) K' ist eine Untergruppe von K bzgl. $+$.

(ii) K'^* ist eine Untergruppe von K^* bzgl. $\cdot$.

In diesem Fall ist K' zusammen mit den induzierten Verknüpfungen $+$ und $\cdot$ wieder ein Körper.

Aus 2.18 folgt, daß der Durchschnitt einer beliebigen Familie von Unterkörpern von K wieder ein Unterkörper von K ist. $\square$

Beispiel 2.46. $(\mathbb{R}, +, \cdot)$ ist ein Körper und $(\mathbb{Q}, +, \cdot)$ ist ein Unterkörper von $\mathbb{R}$ (siehe Analysis). $\square$

Aus dem folgenden Satz ergeben sich weitere Beispiele.

Satz 2.47. Sei R ein nullteilerfreier, kommutativer Ring mit $1 \neq 0$, der endlich viele Elemente hat. Dann ist R ein Körper.

Beweis. Wir müssen zeigen: $(R^*, \cdot)$ ist eine Gruppe. Wir wenden das Kriterium aus 2.13 an. Wegen der Kommutativität von $\cdot$ genügt es zu zeigen, daß $\forall a \in R^*$ die Linkstranslation

$$R^* \rightarrow R^*, x \mapsto a \cdot x,$$

surjektiv ist. Da R und damit auch R^* endlich ist, ist es äquivalent zu zeigen, daß die Linkstranslation injektiv ist. Letzteres ist aber klar:

$$x, y \in R^*, a \cdot x = a \cdot y \Rightarrow a(x - y) = 0,$$

und da $a \neq 0$ folgt aus der Nullteilerfreiheit $x - y = 0$, d. h. $x = y$. $\square$

Beispiel 2.48. Aus 2.47 und 2.39 folgt, daß $\mathbb{Z}/n\mathbb{Z}$, $n \geq 2$, genau dann ein Körper ist, wenn n eine Primzahl ist. $\square$

Bemerkung und Definition 2.49. Seien $(K, +, \cdot)$ und $(L, +, \cdot)$ zwei Körper. Dann heißt jeder Homomorphismus (von Ringen)

$$\varphi : K \rightarrow L$$

auch *Homomorphismus* von Körpern. Die weiteren Begriffe bzw. Aussagen aus 2.30 und 2.31, (i), (ii) übertragen sich wortwörtlich. $\square$

Wir kommen nun zu einem weiteren wichtigen Beispiel für einen Körper:

Satz und Definition 2.50. *Die Menge*

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$$

zusammen mit der durch

$$(a, b) + (a', b') = (a + a', b + b')$$

definierten Addition und der durch

$$(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b)$$

definierten Multiplikation ist ein Körper. Dieser Körper heißt der Körper der komplexen Zahlen und wird mit $\mathbb{C}$ bezeichnet.

$(0, 0)$ ist das Neutralelement bzgl. $+$, $-(a, b) := (-a, -b)$ ist zu (a, b) invers bzgl. $+$.

$(1, 0)$ ist das neutrale Element bzgl. $\cdot$,

$$(a, b)^{-1} := \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

ist zu (a, b) invers bzgl. $\cdot$.

Beweis. Daß $(\mathbb{C} = \mathbb{R}^2, +)$ eine Gruppe ist, ist ein Spezialfall von 2.29. Die übrigen Körpergesetze rechnet man nach, z. B. gilt $\forall (a, b) \in \mathbb{C} \setminus \{(0, 0)\}$:

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \left(\frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2}, \frac{-ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2} \right) = (1, 0)$$

□

Bemerkung 2.51. Die Abbildung

$$\varphi: \mathbb{R} \rightarrow \mathbb{R}^2 = \mathbb{C}, a \rightarrow (a, 0),$$

ist injektiv und somit wegen

$$\begin{aligned} \varphi(a + a') &= (a + a', 0) = (a, 0) + (a', 0) = \varphi(a) + \varphi(a'), \\ \varphi(a \cdot a') &= (a \cdot a', 0) = (a, 0) \cdot (a', 0) = \varphi(a) \cdot \varphi(a'), \end{aligned}$$

ein Körpermonomorphismus.

Bild φ ist dann also ein zu $\mathbb{R}$ isomorpher Unterkörper von $\mathbb{C}$. Vermöge φ können wir $\mathbb{R}$ mit diesem Unterkörper identifizieren und somit $\mathbb{R}$ als Unterkörper von $\mathbb{C}$ auffassen. Ist $a \in \mathbb{R}$, so schreiben wir auch

$$a = (a, 0) \in \mathbb{C}$$

für a aufgefaßt als komplexe Zahl.

□

Aufgaben

Aufgabe 17. (i) Zeigen Sie durch vollständige Induktion nach n : Für alle $n \in \mathbb{N}$ gilt:

$$3 \text{ teilt } n^3 + 2n.$$

(ii) Für $n \in \mathbb{N}$ ist die n -te Fibonacci-Zahl $\mathcal{F}_n$ definiert durch

$$\begin{aligned} \mathcal{F}_0 &:= 0, \mathcal{F}_1 := 1, \\ \mathcal{F}_n &:= \mathcal{F}_{n-1} + \mathcal{F}_{n-2} \text{ für } n \geq 2. \end{aligned}$$

Zeigen Sie durch vollständige Induktion nach n : Für alle $n \in \mathbb{N}$ gilt:

$$\mathcal{F}_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Aufgabe 18. Für eine natürliche Zahl $n \geq 3$ sei $d \in S(\mathbb{R}^2)$ die Drehung um den Winkel $\frac{2\pi}{n}$ und $s \in S(\mathbb{R}^2)$ die Spiegelung an der x -Achse. Die **Diedergruppe** D_n ist definiert durch

$$D_n := U(s, d) \subset S(\mathbb{R}^2).$$

(i) Wie viele Elemente hat D_n ?

(ii) Geben Sie eine Gruppentafel von D_3 an.

Aufgabe 19. Seien $\varphi : G \rightarrow H$ ein Gruppenepimorphismus und $\psi : G \rightarrow F$ ein Gruppenhomomorphismus mit

$$\text{Kern } \varphi \subset \text{Kern } \psi.$$

Zeigen Sie: Es existiert ein eindeutig bestimmter Gruppenhomomorphismus $\eta : H \rightarrow F$, so daß folgendes Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \psi \searrow & & \swarrow \eta \\ & F & \end{array}$$

Aufgabe 20. (i) Sei $G = U(a)$ eine zyklische Gruppe. Zeigen Sie:

$$\varphi : \mathbb{Z} \rightarrow G, n \mapsto a^n,$$

ist ein Epimorphismus.

(ii) **Klassifikation zyklischer Gruppen:** Zeigen Sie: Jede zyklische Gruppe ist isomorph entweder zu $(\mathbb{Z}, +)$ oder zu $(\mathbb{Z}/n\mathbb{Z}, +)$ für ein $n \in \mathbb{N} \setminus \{0\}$.

Diese Idee wird noch einleuchtender durch die folgende Konvention:

Bemerkung und Definition 2.52. Die komplexe Zahl

$$i = (0, 1)$$

heißt *imaginäre Einheit*. Mit ihrer Hilfe läßt sich jede komplexe Zahl (a, b) in der Form

$$\begin{aligned}(a, b) &= (a, 0) + (0, b) = (a, 0) + (0, 1)(b, 0) \\ &= a + ib\end{aligned}$$

schreiben. Beachte, daß gilt:

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

Für

$$z = a + ib \in \mathbb{C}$$

sei

$$\begin{aligned}\operatorname{Re} z &:= a \in \mathbb{R} && (\text{Realteil}) \\ \operatorname{Im} z &:= b \in \mathbb{R} && (\text{Imaginärteil}) \\ \bar{z} &:= a - ib \in \mathbb{C} && (\text{konjugiert komplexe Zahl})\end{aligned}$$

und

$$|z| := \sqrt{a^2 + b^2} \in \mathbb{R} \quad (\text{Absolutbetrag}).$$

Jede komplexe Zahl der Form $z = ib$ heißt *imaginär*. □

2

Für weitere Rechenregeln siehe Aufgaben.

Bemerkung und Definition 2.53. Sei $0 \neq z \in \mathbb{C}$. Setzen wir $z' = \frac{1}{|z|}z$, so gilt $|z'| = 1$. Also gibt es ein eindeutig bestimmtes $\alpha \in [0, 2\pi)$ mit

$$z' = \cos \alpha + i \sin \alpha = e^{i\alpha}$$

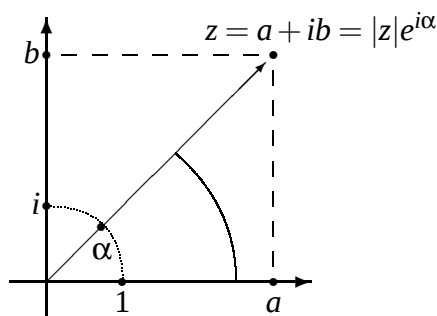
(vergleiche Analysis). Wir nennen

$$\arg z := \alpha$$

das Argument von z . Dann läßt sich z in der Form

$$z = |z| \cdot e^{i \arg z}$$

schreiben.



Ist

$$w = |w| \cdot e^{i \arg w}$$

eine weitere komplexe Zahl, so gilt

$$zw = |z||w|e^{i(\arg z + \arg w)}.$$

□

Wir kommen noch einmal zurück auf die Ringe $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$, $n > 1$.

In $\mathbb{Z}$ gilt für jedes $m \in \mathbb{N}$, $m > 1$ folgendes:

$$m \cdot 1 = \underbrace{1 + \dots + 1}_{m\text{-mal}} = m \neq 0.$$

In $\mathbb{Z}/n\mathbb{Z}$, $n > 1$ gilt hingegen

$$n \cdot \bar{1} = \underbrace{\bar{1} + \dots + \bar{1}}_{n\text{-mal}} = \bar{n} = \bar{0}.$$

2

Definition 2.54. Sei R ein Ring mit 1. Dann heißt

$$\text{char}(R) := \begin{cases} 0 & \text{falls } m1 \neq 0 \ \forall m \geq 1, \\ \min\{m \in \mathbb{N} \setminus \{0\} \mid m1 = 0\} & \text{sonst,} \end{cases}$$

die Charakteristik von R .

□

Bemerkung 2.55. Die Charakteristik eines Rings R mit Einselement 1_R ist genau dann 1, wenn $1_R = 0_R$, d. h. wenn R nur ein Element enthält.

□

Satz 2.56. Sei R ein nullteilerfreier Ring mit $1_R \neq 0_R$. Dann ist $\text{char}(R)$ entweder 0 oder eine Primzahl.

Beweis. Sei $m = \text{char}(R)$. Ist $m = 0$, so sind wir fertig. Sei also $m \neq 0$. Dann ist $m > 1$.

Annahme. m ist keine Primzahl. Dann $\exists k, l \in \mathbb{N}, 1 < k, l < m$ mit $m = kl$. Es folgt

$$0_R = m1_R = kl1_R = (k1_R)(l1_R)$$

und somit $k1_R = 0_R$ oder $l1_R = 0_R$, da R nullteilerfrei. Dies ist ein Widerspruch zur Minimalität von m . $\square$

Wir kommen nun auf den Begriff des Polynoms aus der Motivation zurück. In der linearen Algebra werden Polynome bei der Suche nach sogenannten Eigenwerten eine wichtige Rolle spielen.

Definition 2.57. Sei R ein kommutativer Ring mit 1. Ein Ausdruck der Form

$$p = p(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \cdots + a_n x^n, \quad a_0, \dots, a_n \in R,$$

heißt *Polynom* in der *Unbestimmten* x mit *Koeffizienten* a_i in R . Sind alle $a_i = 0$, so spricht man vom *Nullpolynom* und schreibt entsprechend $p = 0$. Der *Grad* von p ist definiert als

$$\deg(p) := \begin{cases} -\infty & \text{falls } p = 0, \\ \max\{i \mid i \in \mathbb{N}, a_i \neq 0\} & \text{sonst.} \end{cases}$$

$\text{lc}(p) := a_{\deg(p)}$ heißt der *Leitkoeffizient* von p . p heißt *normiert*, wenn $\text{lc}(p) = 1$. Jedes Polynom der Form $p = a_0, a_0 \in R$ heißt *konstantes Polynom*. Mit $R[x]$ bezeichnen wir die Menge aller Polynome in x mit Koeffizienten in R . $\square$

Satz 2.58. Ist R ein kommutativer Ring mit 1, so können wir $R[x]$ wie folgt zu einem kommutativen Ring mit $1 = 1_R$ und $0 = 0_R$ machen: Seien

$$p = \sum_{i=0}^n a_i x^i, q = \sum_{i=0}^m b_i x^i \in R[x].$$

Zur Definition der Addition können wir $m = n$ annehmen (ist etwa $m < n$, so setzt man $b_{m+1} = \cdots = b_n = 0$). Dann sei

$$p + q = \sum_{i=0}^n (a_i + b_i) x^i.$$

Die Multiplikation ist so erklärt, daß man formal ausmultipliziert:

$$pq = \sum_{k=0}^{m+n} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k$$

Beweis. Daß $(R[x], +)$ eine abelsche Gruppe ist, sieht man sofort. Das Nullpolynom 0 ist offensichtlich ein Neutralelement von $R[x]$ bezüglich $+$, und zu $p = \sum_{i=0}^n a_i x^i$ ist $-p = \sum_{i=0}^n (-a_i) x^i$ invers bezüglich $+$. Auch die anderen Ringgesetze ergeben sich aus denen von R durch Nachrechnen. $\square$

Bemerkung 2.59. Ist R ein nullteilerfreier, kommutativer Ring mit 1, so gilt

$$\deg(pq) = \deg(p) + \deg(q) \quad \forall p, q \in R[x].$$

Dabei soll formal

$$n + (-\infty) = (-\infty) + n = (-\infty) + (-\infty) = -\infty$$

sein. Die Gradformel folgt wegen $a_n, b_m \neq 0 \Rightarrow a_n b_m \neq 0$. □

Bemerkung 2.60. Ist R ein kommutativer Ring mit 1, so hat man die *Auswertungsabbildung*

$$R[x] \rightarrow \text{Abb}(R, R), p \rightarrow \tilde{p},$$

wobei für $p = \sum_{i=0}^n a_i x^i \in R[x]$ die Abbildung $\tilde{p}$ durch

$$\tilde{p} : R \rightarrow R, \lambda \rightarrow p(\lambda) = \sum_{i=0}^n a_i \lambda^i,$$

definiert ist. □

Beispiel 2.61. (i) Sind etwa

$$p = x^2 - 2x + 1, q = x^3 - 5x^2 - 3 \in \mathbb{Z}[x],$$

so gilt

$$p + q = x^3 - 4x^2 - 2x - 2$$

und

$$pq = (x^2 - 2x + 1)(x^3 - 5x^2 - 3) = x^5 - 7x^4 + 11x^3 - 8x^2 + 6x - 3.$$

2

(ii) Ist

$$p = x^2 + x \in \mathbb{Z}/2\mathbb{Z}[x],$$

so gilt

$$p(0) = 0, p(1) = 1 + 1 = 0.$$

Also ist $\tilde{p}$ die Nullabbildung, obwohl $p \neq 0$ ist. □

Selbst wenn $R = K$ ein Körper ist, ist der Polynomring $K[x]$ nur ein Ring, man kann im Allgemeinen nicht dividieren. Bei ganzen Zahlen hat man als ‘Ersatz’ eine Division mit Rest, die ganz analog auch für Polynomringe über Körpern erklärt werden kann. Wir wiederholen zunächst den Fall der ganzen Zahlen.

Bemerkung 2.62 (Division mit Rest in $\mathbb{Z}$). Aus Aufgabe 2 ergibt sich: $\forall a, b \in \mathbb{Z}, b \neq 0$, gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$a = bq + \underbrace{r}_{\text{Rest}} \text{ und } 0 \leq r < |b|.$$

□

Satz 2.63 (Division mit Rest in $K[x]$). Sie K ein Körper. Dann gilt: $\forall f, g \in K[x], g \neq 0$, gibt es eindeutig bestimmte $q, r \in K[x]$ mit

$$f = gq + \underbrace{r}_{\text{Rest}} \text{ und } \deg(r) < \deg(g). \quad (*)$$

Beweis. Die Eindeutigkeit ergibt sich wie folgt: Sind $gq_1 + r_2 = f = gq_2 + r_2$ zwei Darstellungen von f wie in $(*)$, so gilt:

$$g(q_1 - q_2) = r_2 - r_1$$

mit $\deg(r_2 - r_1) < \deg(g)$. Wäre $q_1 - q_2 \neq 0$, so folgte aus der Gradformel in 2.59, daß

$$\deg(r_2 - r_1) = \deg(g(q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g).$$

Dies kann nicht sein, also ist

$$q_1 - q_2 = 0 \text{ und somit } r_2 - r_1 = 0.$$

Nun zur Existenz. Sei

$$d := \deg(f), e := \deg(g).$$

Ist $d < e$, so ist

$$f = g \cdot 0 + f$$

eine Darstellung wie in $(*)$. Wir nehmen nun $d \geq e$ an und führen Induktion nach d . Der Induktionsanfang $d = e = 0$ ist klar mit $r = 0$ und $q = \frac{f}{g}$ konstant. Sei nun also $d > 0$. Im Induktionsschritt nehmen wir an, daß die Aussage des Satzes für alle Polynome vom Grad $< d$ richtig ist. Diese Induktionsvoraussetzung können wir auf

$$f_1 := f - \frac{\text{lc}(f)}{\text{lc}(g)} x^{d-e} g$$

anwenden und erhalten eine Darstellung

$$f_1 = gq_1 + r_1 \text{ mit } \deg(r_1) < \deg(g).$$

Daraus ergibt sich eine Darstellung $(*)$ für f :

$$f = f_1 + \frac{\text{lc}(f)}{\text{lc}(g)} x^{d-e} g = gq_1 + r_1 + \frac{\text{lc}(f)}{\text{lc}(g)} x^{d-e} g = g \left(q_1 + \frac{\text{lc}(f)}{\text{lc}(g)} x^{d-e} \right) + r_1 =: gq + r.$$

□

Der Beweis ergibt einen Algorithmus zur Durchführung von Division mit Rest. Im Prinzip kennen wir diesen schon aus der Schule:

Beispiel 2.64. In $\mathbb{Q}[x]$ gilt etwa

$$(x^3 + 3x^2 - 3) : (x^2 - 2) = x + 3 \text{ Rest } 2x + 3.$$

Also:

$$(x^3 + 3x^2 - 3) = (x^2 - 2)(x + 3) + (2x + 3).$$

□

Die eigentliche Frage, mit der wir uns hier beschäftigen wollen, ist die Frage nach der Existenz von Nullstellen von Polynomen. Darauf kann man nämlich viele andere Fragen zurückführen, etwa in der linearen Algebra die nach der Existenz von Eigenwerten. Neben der reinen Existenzfrage ist es für die Praxis wichtig, Verfahren für die näherungsweise Berechnung von Nullstellen zu haben (siehe numerische Mathematik).

Definition 2.65. Seien R ein kommutativer Ring mit 1 und $p = \sum_{i=0}^n a_i x^i \in R[x]$. Dann heißt $\lambda \in R$ *Nullstelle* von p , wenn gilt

$$p(\lambda) = \sum_{i=0}^n a_i \lambda^i = 0.$$

□

Beispiel 2.66. (i) $p = x^2 + 1 \in \mathbb{R}[x]$ hat keine reelle Nullstelle wegen

$$p(\lambda) \geq 1 \quad \forall \lambda \in \mathbb{R}.$$

(ii) Ist $K = \{a_1, \dots, a_n\}$ ein endlicher Körper und

$$p = \prod_{i=1}^n (x - a_i) + 1,$$

so ist $p(\lambda) = 1 \quad \forall \lambda \in K$, also hat p keine Nullstelle in K .

□

Ist K ein Körper, so hat also nicht notwendig jedes Polynom $p \in K[x]$ eine Nullstelle in K . Deswegen betrachtet man auch größere Körper L , die K als Unterkörper enthalten, und sucht nach Nullstellen von p in L . In der Körpertheorie konstruiert man zu jedem Körper K einen eventuell größeren Körper $\overline{K}$, der jede Nullstelle von jedem Polynom in $K[x]$ enthält. Mit dem Fundamentalsatz der Algebra wollen wir einen Satz aus der Körpertheorie ohne Beweis vorwegnehmen. Dieser Satz besagt, daß $\overline{\mathbb{R}} = \mathbb{C}$. Zunächst ein Hilfssatz:

Lemma und Definition 2.67. Sei K ein Körper. Dann gilt:

(i) Ist $p \in K[x]$ und $\lambda \in K$ eine Nullstelle von p , so gibt es ein eindeutig bestimmtest $q \in K[x]$ mit

$$a) \quad p = (x - \lambda)q,$$

$$b) \quad \deg(q) = \deg(p) - 1.$$

$x - \lambda$ heißt auch Linearfaktor von p .

(ii) Sei $0 \neq p \in K[x]$ und k die Anzahl der Nullstellen von p in K . Dann ist

$$k \leq \deg(p).$$

(iii) Ist K unendlich, so ist die Abbildung

$$K[x] \rightarrow \text{Abb}(K, K), \quad p \rightarrow \tilde{p},$$

injektiv.

Beweis. (i) Wir dividieren p durch $(x - \lambda)$ mit Rest:

$$p = (x - \lambda)q + r \quad \text{mit} \quad \deg(r) < \deg(x - \lambda) = 1.$$

Dann ist $r \in K$ ein konstantes Polynom. Aus $p(\lambda) = 0$ folgt durch Einsetzen

$$0 = p(\lambda) = (\lambda - \lambda)q + r = r,$$

und somit a). b) ergibt sich aus der Gradformel:

$$\deg(p) = \deg(x - \lambda) + \deg(q) = 1 + \deg(q).$$

(ii) Wir führen Induktion nach $d := \deg(p)$. Der Induktionsanfang ergibt sich wie folgt: Ist $d = 0$, so ist $p = a_0 \neq 0$ ein konstantes Polynom. Dieses hat keine Nullstelle, also ist die Behauptung für $d = 0$ richtig. Sei also nun $d > 0$. Im Induktionsschritt nehmen wir an, daß die Aussage für Polynome vom Grad $< d$ richtig ist. Wenn p keine Nullstelle in K hat, so ist die Behauptung richtig. Ist $\lambda \in K$ eine Nullstelle, so existiert nach (i) ein $q \in K[x]$ mit

$$p = (x - \lambda)q \quad \text{und} \quad \deg(q) = d - 1.$$

Jede weitere Nullstelle von p in K ist eine solche von q . Ist l die Anzahl der Nullstellen von q , so ist nach Induktionsannahme

$$l \leq d - 1, \quad \text{also} \quad k \leq l + 1 \leq d.$$

(iii) Seien $p_1, p_2 \in K[x]$ mit $\tilde{p}_1 = \tilde{p}_2$. Setzen wir $q = p_1 - p_2$, so folgt $\tilde{q} = 0$, d. h. $q(\lambda) = 0 \quad \forall \lambda \in K$. Da K unendlich ist, hat q unendlich viele Nullstellen. Mit (ii) folgt $q = 0$, d. h. $p_1 = p_2$.

□

Bemerkung 2.68. Sei K ein Körper. Sind $f, g \in K[x]$, so sagt man auch g teilt f , in Zeichen $g|f$, wenn $\exists q \in K[x]$ mit $f = gq$. Ist $(x - \lambda)$ ein Linearfaktor von $p \in K[x]$, so gilt $(x - \lambda)|p$. Ist $p = (x - \lambda)q$, so kann λ natürlich auch Nullstelle von q sein. In diesem Fall gilt $(x - \lambda)^2|p$, wir sprechen auch von einer *mehrfachen Nullstelle*. Sind $0 \neq p \in K[x]$ und $\lambda \in K$, so sei

$$\mu(p, \lambda)$$

die größte Zahl $r \in \mathbb{N}$ mit $(x - \lambda)^r|p$. Dann gilt:

$$\mu(p, \lambda) = 0 \Leftrightarrow \lambda \text{ ist keine Nullstelle von } p.$$

Ist $\mu(p, \lambda) > 0$, so heißt $\mu(p, \lambda)$ die *Vielfachheit der Nullstelle* λ von p . □

Beispiel 2.69. Sei

$$p = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \mathbb{R}[x].$$

Durch Probieren findet man, daß $\lambda_1 = 1$ eine Nullstelle von p ist. Division durch $(x - 1)$ liefert

$$p = (x - 1)(x^3 - x^2 + x - 1) =: (x - 1)q.$$

1 ist aber auch Nullstelle von q . Division ergibt

$$p = (x - 1)^2(x^2 + 1).$$

1 ist also eine zweifache Nullstelle, weitere reelle Nullstellen gibt es nicht. Läßt man auch komplexe Zahlen zur Konkurrenz zu, so ergibt sich

$$p = (x - 1)^2(x + i)(x - i).$$

i und $-i$ sind jeweils einfache Nullstellen. □

Fundamentalsatz der Algebra 2.70. Sei $p \in \mathbb{C}[x]$ ein nicht konstantes Polynom. Dann hat p mindestens eine Nullstelle.

Korollar und Definition 2.71. Jedes Polynom $p \in \mathbb{C}[x]$ zerfällt in Linearfaktoren, d. h.

$$\exists a, \lambda_1, \dots, \lambda_d \in \mathbb{C} \text{ mit } p = a(x - \lambda_1) \dots (x - \lambda_d).$$

Beweis. Die Behauptung folgt aus 2.70 durch sukzessives Herausdividieren von Linearfaktoren, bis man bei einem Polynom von Grad 0 angelangt ist. □

Aufgaben

Aufgabe 21. Für $n, m \in \mathbb{N}$ sei der Binomialkoeffizient $\binom{n}{m}$ definiert durch:

$$\binom{n}{m} := \begin{cases} \frac{n!}{m!(n-m)!} & \text{falls } n \geq m \geq 0, \\ 0 & \text{sonst.} \end{cases}$$

(i) Zeigen Sie: Es gilt

$$\binom{n}{m} + \binom{n}{m-1} = \binom{n+1}{m} \quad \forall n, m \in \mathbb{N}.$$

(ii) Sei R ein kommutativer Ring mit 1. Zeigen Sie die *binomische Formel*:

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i} \quad \forall a, b \in R, n \in \mathbb{N}.$$

Aufgabe 22. Betrachten Sie den Ring $R = (\mathbb{Z}/10\mathbb{Z}, +, \cdot)$ wie in der Vorlesung definiert und die Teilmenge

$$S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}.$$

Zeigen Sie:

- (i) S ist ein Unterring von R . Bestimmen Sie die Verknüpfungstabelle bzgl. $+$ und $\cdot$.
- (ii) S ist ein Körper. Bestimmen Sie 1_S .
- (iii) Bestimmen Sie die Charakteristik von S .

Aufgabe 23. Bestimmen Sie Real-, Imaginärteil und Betrag der folgenden komplexen Zahlen:

- a) $\frac{3+5i}{7i+1}$
- b) $\frac{1}{(3-i)^2}$
- c) $\left[\frac{-1+i\sqrt{3}}{2}\right]^3$
- d) i^n für $n \in \mathbb{N}$.

Aufgabe 24. Seien $z, w \in \mathbb{C}$. Zeigen Sie:

- (i) $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$, $\overline{\bar{z}} = z$, $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$.
- (ii) $\operatorname{Re} z = \frac{1}{2}(z + \bar{z})$, $\operatorname{Im} z = \frac{1}{2i}(z - \bar{z})$.

$$(iii) \quad |\bar{z}| = |z|, \quad z\bar{z} = |z|^2, \quad z^{-1} = \frac{\bar{z}}{|z|^2} \quad \text{falls } z \neq 0.$$

Bisher haben wir kein Verfahren zur praktischen Bestimmung von Nullstellen angegeben.
Für ein Polynom

$$ax^2 + bx + c \in \mathbb{C}[x]$$

vom Grad 2 ergeben sich die Nullstellen aus der Formel

$$\lambda_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Etwas kompliziertere Formeln diese Art gibt es auch für Polynome von Grad 3 und 4. Abel hat 1826 gezeigt, daß es solche allgemeinen Formeln für Polynome vom Grad ≥ 5 nicht geben kann. Deswegen benutzt man in der Praxis, wie bereits gesagt, numerische Näherungsverfahren zur Nullstellenbestimmung.

–pWyIEgJYm5f9v55/–

Kapitel 3

Vektorräume, Basis, Dimension

In der Motivation haben wir für n -Tupel mit Elementen in einem Körper K eine Addition und eine Skalarmultiplikation eingeführt. Abstrahiert man diese, so erhält man den Begriff des K -Vektorraums.

Definition 3.1. Sei K ein Körper. Eine Menge V zusammen mit einer Verknüpfung

$$+ : V \times V \rightarrow V, (v, w) \rightarrow v + w,$$

(Addition) und einer Abbildung

$$\cdot : K \times V \rightarrow V, (\lambda, v) \rightarrow \lambda \cdot v,$$

(Skalarmultiplikation) heißt K -Vektorraum (Vektorraum über K), wenn gilt:

- (i) $(V, +)$ ist eine abelsche Gruppe.
- (ii) Es gelten die *Distributivgesetze*

$$(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v, \lambda(v + w) = \lambda \cdot v + \lambda \cdot w \quad \forall \lambda, \mu \in K \quad \forall v, w \in V,$$

das *Assoziativgesetz*

$$\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v \quad \forall \lambda, \mu \in K \quad \forall v \in V,$$

sowie

$$1 \cdot v = v \quad \forall v \in V.$$

In diesem Fall nennen wir $+$ auch eine *innere Verknüpfung* und $\cdot$ eine *äussere Verknüpfung*. Die Elemente von V heißen *Vektoren*, das neutrale Element 0 der Addition heißt *Nullvektor*. Wir schreiben oft abkürzend

$$\lambda v := \lambda \cdot v \quad \text{für } \lambda \in K, v \in V.$$

Ist $K = \mathbb{R}$ bzw. $K = \mathbb{C}$, so sprechen wir auch von *reellen* bzw. *komplexen Vektorräumen*.

□

Rechenregeln 3.2. Sei V ein K -Vektorraum. Dann gilt:

- (i) $0 \cdot v = 0$.
- (ii) $\lambda \cdot 0 = 0$.
- (iii) $\lambda \cdot v = 0 \Rightarrow \lambda = 0$ oder $v = 0$.
- (iv) $(-1) \cdot v = -v$.

Beweis. (i) $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$ und wir können die Kürzungsregel in der Gruppe $(V, +)$ anwenden.

(ii) $\lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 + \lambda \cdot 0$ sowie Kürzungsregel.

(iii) Sei $\lambda \cdot v = 0$ aber $\lambda \neq 0$. Dann gilt

$$v = 1 \cdot v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v) = \lambda^{-1}0 = 0.$$

(iv) $v + (-1)v = 1v + (-1)v = (1 - 1)v = 0v = 0$.

□

Beispiel 3.3. Sei K ein Körper.

(i) Sei $n \in \mathbb{N} \setminus \{0\}$. In der Menge

$$K^n = \{x = (x_1, \dots, x_n) \mid x_i \in K\}$$

der n -Tupel in K erklären wir eine Addition

$$+ : K^n \times K^n \rightarrow K^n, (x, y) \rightarrow x + y,$$

durch

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

sowie eine Skalarmultiplikation

$$\cdot : K \times K^n \rightarrow K^n, (\lambda, x) \rightarrow \lambda \cdot x,$$

durch

$$\lambda \cdot (x_1, \dots, x_n) = (\lambda \cdot x_1, \dots, \lambda \cdot x_n).$$

Dadurch wird K^n zu einem K -Vektorraum mit Nullvektor $0 = (0, \dots, 0)$.

In diesem Fall können wir Addition und Skalarmultiplikation geometrisch deuten, indem wir jeden Vektor $x = (x_1, \dots, x_n)$ als Pfeil vom Nullvektor mit Spitze in x ansehen. Für $n = 2$ kann man das einfach zeichnen.

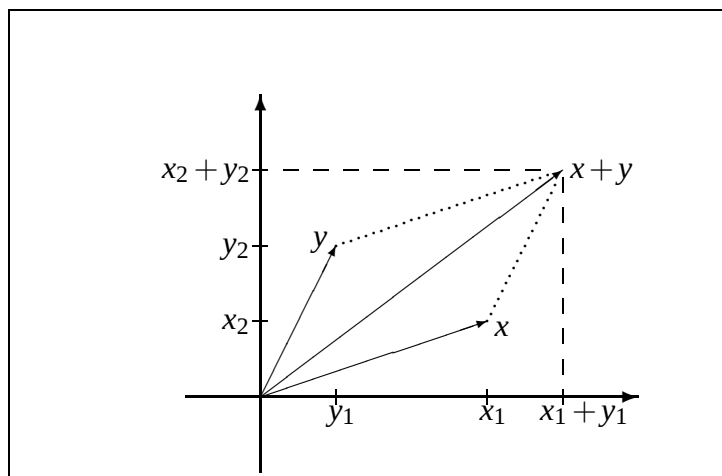


Abbildung 3.1: Vektoraddition

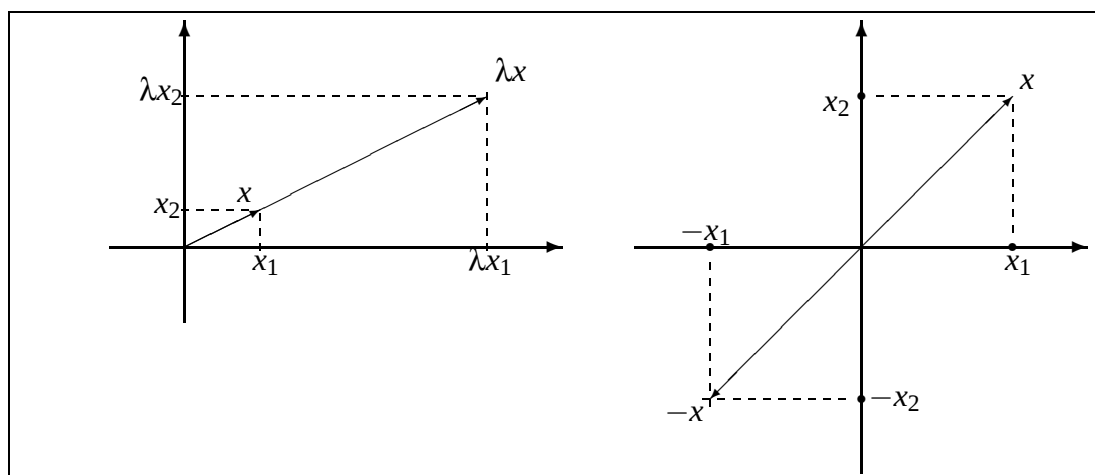


Abbildung 3.2: Skalarmultiplikation

- (ii) Seien $m, n \in \mathbb{N} \setminus \{0\}$. Auch $m \times n$ -Matrizen mit Koeffizienten in K kann man addieren und mit Skalaren multiplizieren: Sind

$$A = (a_{ij}) \text{ und } B = (b_{ij}) \in M(m \times n, K) \text{ und } \lambda \in K,$$

so sind

$$A + B = (a_{ij} + b_{ij}) \text{ und } \lambda \cdot A = (\lambda \cdot a_{ij})$$

wieder in $M(m \times n, K)$. Mit dieser Addition und Skalarmultiplikation wird $M(m \times n, K)$ zu einem K -Vektorraum, dessen Nullvektor die Nullmatrix mit m Zeilen und n Spalten ist:

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

Schreibt man die Zeilen einer Matrix a_{ij} hintereinander als Vektor

$$(a_{11}, \dots, a_{1n}, a_{21}, \dots, a_{2n}, \dots, a_{m1}, \dots, a_{mn}),$$

so sieht man, daß $M(m \times n, K)$ als K -Vektorraum eigentlich nichts anderes ist als $K^{m \cdot n}$.

- (iii) Im Polynomring $K[x]$, in dem ja schon eine Addition erklärt ist, definieren wir eine Skalarmultiplikation

$$K \times K[x] \rightarrow K[x], (\lambda, p) \rightarrow \lambda \cdot p,$$

durch

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

Dadurch wird $K[x]$ auch zu einem K -Vektorraum. Der Nullvektor ist das Nullpolynom. □

Im Polynomring $K[x]$ hat man also zwei innere Verknüpfungen $+$ und $\cdot$ und eine äußere Verknüpfung. Durch Abstraktion der geltenden Rechenregeln gelangt man zur folgenden Definition:

Definition 3.4. Sei K ein Körper. Eine Menge A zusammen mit zwei inneren Verknüpfungen

$$\begin{aligned} + : A \times A &\rightarrow A, (a, b) \rightarrow a + b, \\ \cdot : A \times A &\rightarrow A, (a, b) \rightarrow a \cdot b, \end{aligned}$$

(Addition und Multiplikation) sowie einer äußeren Verknüpfung

$$\bullet : A \times A \rightarrow A, (a, b) \rightarrow a \bullet b,$$

(Skalarmultiplikation) heißt K -Algebra, wenn gilt:

- (i) $(A, +, \cdot)$ ist ein Ring.
- (ii) $(A, +, \bullet)$ ist ein K -Vektorraum.
- (iii) Es gilt das Assoziativgesetz

$$\lambda \bullet (a \cdot b) = (\lambda \bullet a) \cdot b = a \cdot (\lambda \bullet b).$$

Wir sprechen von einer *kommutativen K -Algebra* bzw. einer *K -Algebra mit 1*, wenn der Ring $(A, +, \cdot)$ diese Eigenschaften hat. $\square$

Beispiel 3.5. (i) Ist K ein Körper, so ist $K[x]$ eine kommutative K -Algebra mit 1.

- (ii) Seien $I \subset \mathbb{R}$ ein Intervall und

$$R := \{f : I \rightarrow \mathbb{R} \text{ Abbildung}\}$$

der Ring aus Beispiel 2.37, (ii) mit der durch

$$\begin{aligned}(f + g)(x) &= f(x) + g(x), \\ (f \cdot g)(x) &= f(x) \cdot g(x),\end{aligned}$$

definierten Addition bzw. Multiplikation. Dann wird $(R, +, \cdot)$ zusammen mit der Skalarmultiplikation

$$(\lambda \bullet f)(x) = \lambda \cdot f(x) \quad \forall \lambda \in \mathbb{R}, f \in R, x \in I$$

zu einer $\mathbb{R}$ -Algebra. $\square$

Bemerkung und Definition 3.6. Sei V ein K -Vektorraum und $U \subset V$ eine Teilmenge. Dann heißt U ein *Untervektorraum* von V , wenn gilt:

- (i) U ist eine Untergruppe von V bzgl. $+$.
- (ii) U ist abgeschlossen bzgl. der Multiplikation mit Skalaren:

$$\lambda \in K, v \in U \Rightarrow \lambda \cdot v \in U.$$

In diesem Fall wird in U eine Multiplikation mit Skalaren induziert, so daß U zusammen mit der induzierten Addition wieder ein K -Vektorraum ist.

Ist $(U_i)_{i \in I}$ eine beliebige Familie von Untervektorräumen von V , so ist auch

$$U := \bigcap_{i \in I} U_i$$

ein Untervektorraum: Aus 2.18 folgt, daß U eine Untergruppe bzgl. $+$ ist. Sind andererseits alle U_i abgeschlossen bzgl. der Multiplikation mit Skalaren, so sicher auch U . $\square$

Hier ist ein Kriterium, das das Nachrechnen der Unterraumeigenschaften erleichtert:

Satz 3.7. Seien V ein K -Vektorraum und $U \subset V$. Dann sind äquivalent:

(i) U ist ein Untervektorraum von V .

(ii) $U \neq \emptyset$ und es gilt

$$u, v \in U \Rightarrow u + v \in U, \lambda \in K, u \in U \Rightarrow \lambda \cdot u \in U.$$

Beweis. Dies folgt aus dem entsprechenden Kriterium 2.16 für Untergruppen:

$$u, v \in U \Rightarrow u, -v \in U \Rightarrow u - v \in U.$$

□

Beispiel 3.8. (i) $U := \{(x, y, 0) \mid x, y \in \mathbb{R}\}$ ist ein $\mathbb{R}$ -Untervektorraum von $\mathbb{R}^3$.

(ii) $U := \{(x, y, 1) \mid x, y \in \mathbb{R}\}$ ist kein Untervektorraum von $\mathbb{R}^3$, denn $(0, 0, 0) \notin U$.

□

Wir kommen nun zum Begriff der Linearkombination, dem wir schon in der Motivation begegnet sind. Gleichzeitig übertragen wir 2.18, (ii), (iii) auf Vektorräume.

Bemerkung und Definition 3.9. Sei V ein K -Vektorraum.

(i) Sei $(v_i)_{i \in I}$ eine Familie von Vektoren in V . Ein Vektor $v \in V$ heißt *Linearkombination* der $(v_i)_{i \in I}$, wenn es Indizes $i_1, \dots, i_n$ und Skalare $\lambda_1, \dots, \lambda_n \in K$ gibt mit

$$v = \sum_{v=1}^n \lambda_v v_{i_v}.$$

Wir bezeichnen mit

$$\text{span}(v_i)_{i \in I} = \text{span}_K(v_i)_{i \in I}$$

die Menge aller Linearkombinationen der $(v_i)_{i \in I}$. $\text{span}(v_i)_{i \in I}$ ist der kleinste Untervektorraum von V , der alle $v_i, i \in I$, enthält. Dieser heißt der von der Familie *aufgespannte* (oder *erzeugte*) Unterraum. Schreiben wir

$$A = \{v_i \mid i \in I\} \subset V,$$

so gilt

$$\text{span}(A) = \bigcap_{\substack{U \subset V \\ \text{Untervektorraum} \\ A \subset U}} U.$$

Wir setzen

$$\text{span}(\emptyset) := \{0\}.$$

Ist speziell $I = \{1, \dots, n\}$ und sind $v_1, \dots, v_n \in V$, so schreiben wir auch

$$\text{span}(v_1, \dots, v_n) = \text{span}_K(v_1, \dots, v_n) = \{v \in V \mid \exists \lambda_1, \dots, \lambda_n \in K \text{ mit } v = \sum_{i=1}^n \lambda_i v_i\}$$

für den von $v_1, \dots, v_n$ aufgespannten Untervektorraum.

(ii) Ist $(v_i)_{i \in I}$ eine Familie von Vektoren in V mit

$$\text{span}(v_i)_{i \in I} = V,$$

so nennen wir die Familie *Erzeugendensystem* von V . In diesem Fall ist also jeder Vektor in V eine Linearkombination von endlich vielen der v_i . V heißt *endlich erzeugt*, falls es ein endliches Erzeugendensystem gibt.

□

Beispiel 3.10. (i) Ist K ein Körper, so betrachten wir in K^n die Vektoren

$$e_i := (0, \dots, 0, \underbrace{1}_{i\text{-te Stelle}}, 0, \dots, 0), \quad i = 1, \dots, n.$$

Dann gilt

$$\text{span}(e_1, \dots, e_n) = K^n.$$

(ii) Der Polynomring $K[x]$ über einem Körper K wird erzeugt von $1, x, x^2, x^3, \dots$:

$$K[x] = \text{span}(x^i)_{i \in \mathbb{N}}$$

(iii) Sei $0 \neq v_1 \in \mathbb{R}^3$. Dann ist $\text{span}(v_1)$ die Gerade durch 0 und v_1 . Ist $v_2 \in \mathbb{R}^3$ ein weiterer Vektor, $v_2 \notin \text{span}(v_1)$, so ist $\text{span}(v_1, v_2)$ die Ebene durch 0, v_1, v_2 .

(iv) Seien

$$v_1 = (1, 2, 3, 4), v_2 = (6, 6, 10, 10), v_3 = (1, 0, 1, 0), v_4 = (1, 1, 1, 1) \in \mathbb{R}^4.$$

Dann ergibt sich z. B. für den Vektor $v = (4, 2, 4, 2) \in \mathbb{R}^4$:

$$v = v_2 - 2 \cdot v_1 = 2 \cdot (v_3 + v_4).$$

Die Darstellung von v als Linearkombination von $v_1, \dots, v_4$ ist also nicht eindeutig.

□

Daß im obigen Beispiel die Darstellung nicht eindeutig ist, liegt daran, daß z. B. v_2 bereits im span der anderen drei Vektoren enthalten ist:

$$v_2 = 2v_1 + 2v_3 + 2v_4.$$

Daraus folgt dann

$$\text{span}(v_1, \dots, v_4) = \text{span}(v_1, v_3, v_4).$$

Natürlich ist es sinnvoll, mit der geringstmöglichen Anzahl von Vektoren zu arbeiten, die einen Untervektorraum aufspannen. Wie kann man aber überprüfen, ob ein gegebenes Erzeugendensystem verkleinert werden kann?

Aufgaben

Aufgabe 25. Sei R ein nullteilerfreier, kommutativer Ring mit $1 \neq 0$ (**Integritätsring**). Zeigen Sie:

- (i) In der Menge $R \times (R \setminus \{0\})$ ist durch

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$$

eine Äquivalenzrelation definiert. Wir schreiben $\frac{a}{b}$ für die durch (a, b) repräsentierte Äquivalenzklasse sowie

$$Q(R) := \left\{ \frac{a}{b} \mid (a, b) \in R \times (R \setminus \{0\}) \right\}$$

für die Menge aller Äquivalenzklassen.

- (ii) Durch

$$\frac{a}{b} + \frac{a'}{b'} := \frac{ab' + ba'}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}$$

erhalten wir wohldefinierte Verknüpfungen $+$ und $\cdot$ auf $Q(R)$.

- (iii) $(Q(R), +, \cdot)$ ist ein Körper (**Quotientenkörper von R**).

Aufgabe 26. Seien $u, v \in \mathbb{Z}$. Wir sagen: u **teilt** v , in Zeichen $u|v$, falls ein $k \in \mathbb{Z}$ existiert mit $u \cdot k = v$. Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Definieren Sie induktiv eine Folge $c_0, c_1, c_2, \dots$ ganzer Zahlen durch

$$\begin{aligned} c_0 &= a, \\ c_1 &= b, \\ c_{i+1} &= \begin{cases} \text{der Rest von } c_{i-1} \text{ bei der Division durch } c_i, & \text{falls } c_i \neq 0, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

Zeigen Sie: Es gibt einen kleinsten Index n mit $c_{n+1} = 0$. Für dieses n gilt:

(i) $c_n|a$ und $c_n|b$.

(ii) c_n ist ein **größter gemeinsamer Teiler** von a und b , d.h. es gilt:

$$d|a \text{ und } d|b \Rightarrow d|c_n.$$

Aufgabe 27. Bestimmen Sie bis auf Isomorphie alle Körper mit 4 Elementen.

Aufgabe 28. Seien K ein Körper und $a_0, \dots, a_n, b_0, \dots, b_n \in K$ mit $a_i \neq a_j$ für alle $i \neq j$. Zeigen Sie: Es gibt genau ein Polynom $f \in K[x]$ vom Grad $\leq n$, so daß $f(a_i) = b_i$ für $i = 1, \dots, n$.

Hinweis: Konstruieren Sie zuerst Polynome $g_k \in K[x]$ vom Grad $\leq n$ mit

$$g_k(a_i) = \begin{cases} 1 & \text{für } i = k, \\ 0 & \text{für } i \neq k. \end{cases}$$

Was man leicht testen kann ist, ob der Nullvektor nur eine Darstellung aus dem gegebenen Vektor zuläßt. Das führt zur

Definition 3.11. Sei V ein K -Vektorraum. Eine endliche Familie $(v_1, \dots, v_n)$ von Vektoren aus V heißt *linear unabhängig*, wenn gilt

$$\sum_{i=1}^n \lambda_i v_i = 0, \lambda_1, \dots, \lambda_n \in K \Rightarrow \lambda_1 = \dots = \lambda_n = 0.$$

Eine beliebige Familie $(v_i)_{i \in I}$ von Vektoren aus V heißt *linear unabhängig*, wenn je endlich viele Vektoren aus der Familie linear unabhängig sind. Eine Familie von Vektoren heißt *linear abhängig*, wenn sie nicht linear unabhängig ist. $\square$

Tatsächlich reicht es, den Nullvektor auf eindeutige Darstellbarkeit zu testen:

Lemma 3.12. Für eine Familie $(v_i)_{i \in I}$ von Vektoren eines K -Vektorraums sind äquivalent:

(i) $(v_i)_{i \in I}$ ist linear unabhängig.

(ii) Jeder Vektor $v \in \text{span}(v_i)_{i \in I}$ läßt sich in eindeutiger Weise aus Vektoren der Familie $(v_i)_{i \in I}$ linear kombinieren.

Beweis. '(ii) $\Rightarrow$ (i)' ist klar.

'(i) $\Rightarrow$ (ii)'. Sei

$$v = \sum_{i \in I} \lambda_i v_i = \sum_{i \in I} \mu_i v_i \in \text{span}(v_i)_{i \in I}$$

auf zwei Arten linear kombiniert. Dabei sind die Summen so zu verstehen, daß nur endlich viele λ_i bzw. μ_i von Null verschieden sind, und tatsächlich nur über die entsprechenden Indizes summiert wird. Dann gilt

$$\sum_{i \in I} (\lambda_i - \mu_i) v_i = 0,$$

wobei jetzt tatsächlich nur über die endlich vielen Indizes mit $\lambda_i \neq 0$ oder $\mu_i \neq 0$ summiert wird. Es folgt $\lambda_i = \mu_i \forall i \in I$ nach (i). $\square$

Ist $(v_1, \dots, v_n)$ eine linear unabhängige (abhängige) Familie von Vektoren, so sagen wir auch einfach $v_1, \dots, v_n$ sind linear unabhängig (abhängig).

Beispiel 3.13. (i) Die Vektoren $e_1, \dots, e_n$ des K^n sind linear unabhängig.

(ii) Die Polynome $1, x, x^2, x^3 \dots$ des Polynomrings $K[x]$ sind linear unabhängig. □

Lemma 3.14. Sei V ein K -Vektorraum. Dann gilt:

(i) $v \in V$ linear unabhängig $\Leftrightarrow v \neq 0$.

(ii) Ist $n \geq 2$, so sind $v_1, \dots, v_n \in V$ genau dann linear abhängig, wenn einer der Vektoren Linearkombination der anderen ist.

Beweis. (i) ' $\Leftarrow$ '. v linear abhängig $\Rightarrow \exists \lambda \neq 0$ mit $\lambda \cdot v = 0 \Rightarrow v = 0$.

' $\Rightarrow$ '. 0 ist linear abhängig wegen $1 \cdot 0 = 0$.

(ii) ' $\Rightarrow$ '. Sind $v_1, \dots, v_n$ linear abhängig, so $\exists \lambda_1, \dots, \lambda_n \in K$ mit $\sum_{i=1}^n \lambda_i v_i = 0$ und für mindestens ein k gilt $\lambda_k \neq 0$. Es folgt

$$v_k = \frac{-\lambda_1}{\lambda_k} v_1 - \dots - \frac{-\lambda_{k-1}}{\lambda_k} v_{k-1} - \frac{-\lambda_{k+1}}{\lambda_k} v_{k+1} - \dots - \frac{-\lambda_n}{\lambda_k} v_n.$$

' $\Leftarrow$ '. Ist umgekehrt etwa

$$v_k = \mu_1 v_1 + \dots + \mu_{k-1} v_{k-1} + \mu_{k+1} v_{k+1} + \dots + \mu_n v_n,$$

so folgt

$$\mu_1 v_1 + \dots + \mu_{k-1} v_{k-1} + (-1) v_k + \mu_{k+1} v_{k+1} + \dots + \mu_n v_n = 0.$$

□

Beispiel 3.15. Die Vektoren $v_1, \dots, v_4 \in \mathbb{R}^4$ in Beispiel 3.10, (iii) sind linear abhängig. □

Definition 3.16. Sei V ein K -Vektorraum. Eine Familie $\mathcal{B} = (v_i)_{i \in I}$ in V heißt *Basis* von V , wenn gilt:

(i) $\mathcal{B}$ ist ein Erzeugendensystem von V .

(ii) $\mathcal{B}$ ist linear unabhängig.

Ist $I = \{1, \dots, n\}$ endlich, also $\mathcal{B} = (v_1, \dots, v_n)$, so heißt n *Länge des Basis*. Ist I unendlich, so sprechen wir von einer *Basis unendlicher Länge*. □

Beispiel 3.17. (i) $\mathcal{K} := (e_1, \dots, e_n)$ ist eine Basis des K^n , sie heißt die *kanonische Basis* oder *Standardbasis*.

(ii) Die Matrizen

$$E_i^j := \begin{pmatrix} & \begin{matrix} j\text{-te Spalte} \\ \downarrow \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{matrix} & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ & & & \leftarrow i\text{-te Zeile} & & & \end{pmatrix},$$

$1 \leq i \leq m, 1 \leq j \leq n$ bilden eine Basis von $M(m \times n, K)$. Dies ist wieder nur eine Variante von (i).

(iii) $1, x, x^2, x^3, \dots$ ist eine Basis unendlicher Länge von $K[x]$.

□

Satz 3.18. Für eine Familie $\mathcal{B} = (v_1, \dots, v_n)$ von Vektoren eines K -Vektorraums $V \neq \{0\}$ sind äquivalent

(i) $\mathcal{B}$ ist eine Basis.

(ii) $\mathcal{B}$ ist ein unverkürzbares Erzeugendensystem, d. h. $\mathcal{B}$ ist ein Erzeugendensystem, aber

$$(v_1, \dots, v_{r-1}, v_{r+1}, \dots, v_n)$$

ist für jedes $r \in \{1, \dots, n\}$ kein Erzeugendensystem mehr.

(iii) Für jedes $v \in V$ gibt es eindeutig bestimmte $\lambda_1, \dots, \lambda_n \in K$ mit

$$v = \sum_{i=1}^n \lambda_i v_i,$$

d. h. $\mathcal{B}$ ist ein Erzeugendensystem mit der zusätzlichen Eindeutigkeitseigenschaft.

(iv) $\mathcal{B}$ ist linear unabhängig und $\forall v \in V$ ist $(v_1, \dots, v_n, v)$ linear abhängig.

Beweis. ‘(i) $\Rightarrow$ (ii)’. Ist $\mathcal{B}$ eine Basis, so ist $\mathcal{B}$ ein Erzeugendensystem. Wäre $\mathcal{B}$ verkürzbar, so könnte man ein v_r als Linearkombination der anderen v_i schreiben und $\mathcal{B}$ wäre linear abhängig.

‘(ii) $\Rightarrow$ (iii)’. $\mathcal{B}$ ist ein Erzeugendensystem. Gäbe es ein $v \in V$ mit

$$\sum_{i=1}^n \lambda_i v_i = v = \sum_{i=1}^n \mu_i v_i$$

und $\lambda_r \neq \mu_r$ für ein r , so folgte

$$v_r = \frac{\mu_1 - \lambda_1}{\lambda_r - \mu_r} v_1 + \cdots + \frac{\mu_{r-1} - \lambda_{r-1}}{\lambda_r - \mu_r} v_{r-1} + \frac{\mu_{r+1} - \lambda_{r+1}}{\lambda_r - \mu_r} v_{r+1} + \cdots + \frac{\mu_n - \lambda_n}{\lambda_r - \mu_r} v_n,$$

und $\mathcal{B}$ wäre verkürzbar.

‘(iii) $\Rightarrow$ (iv)’. Aus 3.12 folgt: $\mathcal{B}$ ist linear unabhängig. Ist $v \in V$, so ist v von der Form $v = \sum_{i=1}^n \lambda_i v_i$, es folgt

$$\lambda_1 v_1 + \cdots + \lambda_n v_n + (-1)v = 0,$$

d. h. $(v_1, \dots, v_n, v)$ ist linear abhängig.

‘(iv) $\Rightarrow$ (i)’. $\mathcal{B}$ ist linear unabhängig. Sei $v \in V$. Da $(v_1, \dots, v_n, v)$ linear abhängig ist $\exists \lambda_1, \dots, \lambda_n, \lambda \in K, \lambda \neq 0$, mit $\lambda_1 v_1 + \cdots + \lambda_n v_n + \lambda v = 0$, es folgt

$$v = -\frac{\lambda_n}{\lambda} v_1 - \cdots - \frac{\lambda_1}{\lambda} v_n.$$

Also ist $\mathcal{B}$ auch ein Erzeugendensystem von V . □

Korollar 3.19. *Ist V ein K -Vektorraum, der nicht endlich erzeugt ist, so gibt es eine linear unabhängige Familie von Vektoren in V mit unendlich vielen Elementen.*

Beweis. Wir zeigen durch vollständige Induktion nach n : $\forall n \geq 1$ gibt es linear unabhängige Vektoren $v_1, \dots, v_n \in V$.

Induktionsanfang. $n = 1$ Es gibt einen Vektor $0 \neq v_1 \in V$, denn sonst wäre $V = \{0\}$ endlich erzeugt.

Induktionsschluß. Sei $n \in \mathbb{N}, n \geq 1$.

Induktionsannahme. $\exists v_1, \dots, v_n \in V$ linear unabhängig.

Induktionsbehauptung. $\exists v_{n+1} \in V$, so daß $v_1, \dots, v_{n+1}$ linear unabhängig sind.

Wären $v_1, \dots, v_n, v$ für jedes $v \in V$ linear abhängig wäre, dann wäre nach 3.18 $v_1, \dots, v_n$ auch ein Erzeugendensystem von V im Widerspruch zur Voraussetzung. □

Satz 3.20 (Basisauswahlsatz). *Aus jedem endlichen Erzeugendensystem eines K -Vektorraums kann man Vektoren auswählen, die eine Basis bilden. Insbesondere hat jeder endlich erzeugte K -Vektorraum eine Basis endlicher Länge.*

Beweis. Aus dem endlichen Erzeugendensystem nehme man so lange Vektoren weg, bis es unverkürzbar geworden ist. □

Bemerkung 3.21. Allgemeiner kann man zeigen, daß jeder K -Vektorraum eine Basis hat. Der Beweis ist wesentlich komplizierter und benutzt das Lemma von Zorn. Darauf wollen wir nicht weiter eingehen. □

Wir wollen nun die Länge verschiedener Basen eines endlich erzeugten K -Vektorraums vergleichen. Dazu muß man systematisch Vektoren austauschen.

Satz 3.22 (Austauschlemma von Steinitz). Sei V ein K -Vektorraum, $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V und $w = \sum_{i=1}^n \lambda_i v_i \in V$. Dann ist für jedes $k \in \{1, \dots, n\}$ mit $\lambda_k \neq 0$ auch

$$\mathcal{B}' = (v_1, \dots, v_{k-1}, w, v_{k+1}, \dots, v_n)$$

eine Basis von V . Man kann also v_k gegen w austauschen.

Beweis. Ohne Einschränkung nehmen wir $k = 1$ an (dies kann man durch umnummerieren stets erreichen). Es ist also zu zeigen, daß $\mathcal{B}' = (w, v_2, \dots, v_n)$ eine Basis ist.

$\mathcal{B}'$ ist ein Erzeugendensystem. Sei $v \in V$. Dann $\exists \mu_1, \dots, \mu_n \in K$ mit $v = \sum_{i=1}^n \mu_i v_i$. Andererseits folgt wegen $\lambda_1 \neq 0$:

$$v_1 = \frac{1}{\lambda_1} w - \sum_{i=2}^n \frac{\lambda_i}{\lambda_1} v_i,$$

also

$$v = \frac{\mu_1}{\lambda_1} w + \left(\mu_2 - \frac{\mu_1 \lambda_2}{\lambda_1}\right) v_2 + \dots + \left(\mu_n - \frac{\mu_1 \lambda_n}{\lambda_1}\right) v_n.$$

$\mathcal{B}'$ ist linear unabhängig. Seien $\mu_1, \dots, \mu_n \in K$ mit

$$\mu w + \mu_2 v_2 + \dots + \mu_n v_n = 0.$$

Dann folgt durch Einsetzen

$$\mu \lambda_1 v_1 + (\mu \lambda_2 + \mu_2) v_2 + \dots + (\mu \lambda_n + \mu_n) v_n = 0,$$

also

$$\mu \lambda_1 = \mu \lambda_2 + \mu_2 = \dots = \mu \lambda_n + \mu_n = 0,$$

da $\mathcal{B}$ linear unabhängig. Da $\lambda_1 \neq 0$ folgt $\mu = 0$ und somit auch $\mu_2 = \dots = \mu_n = 0$. $\square$

Durch Iteration erhält man den

Satz 3.23 (Austauschsatz von Steinitz). Seien V ein K -Vektorraum, $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V und $(w_1, \dots, w_r)$ eine Familie linear unabhängiger Vektoren in V . Dann gilt

(i) $r \leq n$

(ii) Es gibt Indizes $i_1, \dots, i_r \in \{1, \dots, n\}$, so daß man nach Austausch von v_{i_1} durch $w_1, \dots, v_{i_r}$ durch w_r wieder eine Basis von V erhält. Numeriert man so um, daß $i_1 = 1, \dots, i_r = r$, so bedeutet das, daß

$$\mathcal{B}' = (w_1, \dots, w_r, v_{r+1}, \dots, v_n)$$

eine Basis von V ist.

Beweis. Wir führen vollständige Induktion nach r .

Induktionsanfang. Der Fall $r = 1$ ist das gerade bewiesene Austauschlemma.

Induktionsschluß. Sei $r \in \mathbb{N}, r \geq 1$.

Induktionsannahme. Die Aussage sei richtig für r .

Induktionsbehauptung. Die Aussage ist richtig für $r + 1$.
Seien $(w_1, \dots, w_{r+1})$ eine Familie linear unabhängiger Vektoren in V . Dann ist auch $(w_1, \dots, w_r)$ linear unabhängig. Also ergibt sich aus der Induktionsannahme, daß (evtl. nach Umnummerierung)

$$(w_1, \dots, w_r, v_{r+1}, \dots, v_n)$$

eine Basis von V ist. Ebenfalls gilt $r \leq n$ nach Induktionsannahme. Wäre $r = n$, so wäre $(w_1, \dots, w_r)$ bereits eine Basis von V im Widerspruch zu 3.18, (iv). Also gilt $r + 1 \leq n$. Nun schreiben wir

$$w_{r+1} = \lambda_1 w_1 + \dots + \lambda_r w_r + \lambda_{r+1} v_{r+1} + \dots + \lambda_n v_n$$

mit $\lambda_1, \dots, \lambda_n \in K$. Wäre $(\lambda_{r+1} = \dots = \lambda_n = 0)$, so hätte man einen Widerspruch zur linearen Unabhängigkeit von $(w_1, \dots, w_{r+1})$. Bei geeigneter Numerierung können wir also $\lambda_{r+1} \neq 0$ annehmen und nach dem Austauschlemma v_{r+1} gegen w_{r+1} austauschen. □

Korollar 3.24. *Hat ein K -Vektorraum V eine endliche Basis, so ist jede Basis von V endlich.*

Beweis. Seien $(v_1, \dots, v_n)$ eine endliche Basis und $(w_i)_{i \in I}$ eine beliebige Basis von V . Wäre I unendlich, so gäbe es Indizes $i_1, \dots, i_{n+1} \in I$, so daß $w_{i_1}, \dots, w_{i_{n+1}}$ linear unabhängig sind. Dies widerspricht 3.23, (i). □

Korollar 3.25. *Je zwei endliche Basen eines K -Vektorraums V haben gleiche Länge.*

Beweis. Sind $(w_1, \dots, v_n)$ und $(w_1, \dots, w_m)$ zwei Basen von V , so kann man 3.23, (i) zweimal anwenden und erhält $m \leq n$, aber auch $n \leq m$. □

Definition 3.26. Ist V ein K -Vektorraum, so heißt

$$\dim V := \dim_K V := \begin{cases} \infty, & \text{falls } V \text{ keine endliche Basis hat,} \\ n, & \text{falls } V \text{ eine Basis der Länge } n \text{ hat,} \end{cases}$$

die *Dimension* von V über K . □

Korollar 3.27. *Seien V ein endlich erzeugter K -Vektorraum und $W \subset V$ ein Unterraum. Dann gilt:*

- (i) W ist endlich erzeugt und $\dim W \leq \dim V$.
- (ii) Ist $\dim W = \dim V$, so folgt $W = V$.

Beweis. (i) Wäre W nicht endlich erzeugt, so gäbe es nach 3.19 eine linear unabhängige Familie von Vektoren in W und damit auch in V mit unendlich vielen Elementen. Dies widerspricht dem Austauschsatz. Also hat W eine endliche Basis, und wieder nach 3.23 ist ihre Länge höchstens gleich $\dim V$.

(ii) Sei $\dim V = \dim W = n$. Dann $\exists$ Basis $w_1, \dots, w_n$ von W mit n . Wäre $W \neq V$, so gäbe es $v \in V \setminus W$, und $w_1, \dots, w_n, v$ wären linear unabhängig im Widerspruch zu 3.23. □

Satz 3.28 (Basisergänzungssatz). Seien V ein endlich erzeugter K -Vektorraum und $w_1, \dots, w_r \in V$ linear unabhängig. Dann gibt es $v_{r+1}, \dots, v_n \in V$, so daß

$$\mathcal{B} = (w_1, \dots, w_r, v_{r+1}, \dots, v_n)$$

eine Basis von V ist.

Beweis. Wähle eine Basis $(v_1, \dots, v_n)$ von V . und wende 3.23 an. □

Beispiel 3.29. (i) $\dim_K K^n = n$, denn K^n hat die kanonische Basis $(e_1, \dots, e_n)$.

(ii) $\dim_K \text{Mat}(m \times n, K) = m \cdot n$.

(iii) $\dim_K K[x] = \infty$. □

Aufgaben

Aufgabe 29. Seien G eine endliche Gruppe mit Neutralelement e und $a \in G$. Dann heißt

$$\text{ord}(a) := |U(a)|$$

die **Ordnung** von a . Zeigen Sie:

(i) Für $n \in \mathbb{Z}$ ist $a^n = e \Leftrightarrow \text{ord}(a)$ ist ein Teiler von n .

(ii) (**Kleiner Fermatscher Satz**) Es gilt $a^{|G|} = e$.

(iii) Ist $m \in \mathbb{Z}$ und $d \in \mathbb{N}$ größter gemeinsamer Teiler von m und $\text{ord}(a)$, so gilt

$$\text{ord}(a^m) = \frac{\text{ord}(a)}{d}.$$

Aufgabe 30. Seien $(R, +, \cdot)$ ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt **Ideal** von R , wenn gilt:

(a) $\mathfrak{a}$ ist eine Untergruppe von R bzgl. $+$.

(b) $a \in \mathfrak{a}, r \in R \Rightarrow a \cdot r \in \mathfrak{a}$ und $r \cdot a \in \mathfrak{a}$.

Zeigen Sie:

(i) Der Durchschnitt einer beliebigen Familie von Idealen in R ist wieder ein Ideal in R .

(ii) Die Faktorgruppe

$$(R/\mathfrak{a}, +)$$

wird durch

$$R/\mathfrak{a} \times R/\mathfrak{a} \longrightarrow R/\mathfrak{a}, (r + \mathfrak{a}, s + \mathfrak{a}) \mapsto (r \cdot s) + \mathfrak{a},$$

zu einem Ring (**Faktorring** von R nach $\mathfrak{a}$).

(iii) Ist $\varphi : R \rightarrow S$ ein Homomorphismus von Ringen, so ist Kern φ ein Ideal in R .

Aufgabe 31. (i) Für welche $t \in \mathbb{R}$ sind die drei Vektoren

$$(1, 3, 4), (3, t, 11), (-1, -4, 0) \in \mathbb{R}^3$$

linear abhängig? Begründen Sie Ihre Aussage.

(ii) Zeigen Sie:

$$U = \{(x, y, z) \in \mathbb{R}^3 \mid x = z\}$$

ist ein Untervektorraum des $\mathbb{R}^3$. Bestimmen Sie eine Basis von U .

Aufgabe 32. Sei $\mathbb{F}_q$ ein Körper mit q Elementen.

Ein $[n, k]$ -Code über $\mathbb{F}_q$ ist ein Untervektorraum $C \subset \mathbb{F}_q^n$ der Dimension k .

Eine **Erzeuger-Matrix** für C ist eine $k \times n$ -Matrix mit Koeffizienten in $\mathbb{F}_q$, deren Zeilen eine Basis von C bilden.

Bestimmen Sie eine Erzeuger-Matrix für die von den Zeilen der folgenden Matrizen aufgespannten Codes:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \in M(3 \times 4, \mathbb{F}_2),$$

$$\begin{pmatrix} 2 & 0 & 2 & 0 & 0 & 2 \\ 2 & 2 & 0 & 1 & 2 & 2 \\ 2 & 1 & 2 & 1 & 1 & 2 \\ 2 & 1 & 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 2 & 1 & 2 \end{pmatrix} \in M(5 \times 6, \mathbb{F}_3),$$

wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

In 3.23 haben wir bewiesen, daß man aus jedem endlichen Erzeugendensystem eines K -Vektorraums eine Basis auswählen kann. Für die Praxis ist das Verfahren des Weglassens (und die Kontrolle, ob ein Erzeugendensystem übrigbleibt) nicht ökonomisch. Wir geben nun einen Algorithmus an, wie man aus einem Erzeugendensystem eine Basis linear kombinieren kann. Dabei behandeln wir den Spezialfall eines Untervektorraums W von K^n . Später werden wir sehen, daß sich der allgemeine Fall darauf zurückführen läßt.

Seien also Vektoren $a_1, \dots, a_m \in K^n$ gegeben, und sei $W = \text{span}(a_1, \dots, a_m)$. Sind $a_{i1}, \dots, a_{in}$ die Komponenten von a_i , d. h. ist $a_i = (a_{i1}, \dots, a_{in})$, so ergeben die Vektoren untereinander geschrieben eine Matrix

$$A := \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in M(m \times n, K).$$

Bemerkung 3.33. Ist $A \in M(m \times n, K)$ in Zeilenstufenform, so gibt es eine Zahl r , $0 \leq r \leq m$, so daß in jeder der ersten r Zeilen mindestens ein von Null verschiedener Eintrag steht, und in den anderen Zeilen nur Nullen stehen. Ist $r \geq 1$, so sind die ersten r Zeilen linear unabhängig, bilden also eine Basis von $\text{ZR}(A)$. Es gilt $\dim_K \text{ZR}(A) = r$. $\square$

Beispiel 3.34. Für

$$A = \begin{pmatrix} 0 & 2 & 0 & 4 & 6 & 0 & 5 \\ 0 & 0 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

ist $\dim_K \text{ZR}(A) = 3$. $\square$

Ist nun A beliebig, so können wir A durch elementare Zeilenumformungen auf Zeilenstufenform bringen, ohne den Zeilenraum zu verändern.

Definition 3.35. Unter einer *elementaren Zeilenumformung* von $A \in M(m \times n, K)$ verstehen wir eine der folgenden Operationen:

I. Multiplikation der i -ten Zeilen mit $\lambda \in K^*$:

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} \rightarrow \begin{pmatrix} \vdots \\ \lambda a_i \\ \vdots \end{pmatrix}$$

II. Addition der j -ten Zeilen zur i -ten Zeile:

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \rightarrow \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

III. Addition der λ -fachen j -ten Zeilen zur i -ten Zeile, $\lambda \in K$:

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \rightarrow \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

IV. Vertauschen der i -ten Zeilen mit der j -ten Zeile:

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \rightarrow \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$

Dabei bezeichnen $a_1, \dots, a_m$ die Zeilen von A , es ist stets $i \neq j$ vorausgesetzt, und an den mit Punkten gekennzeichneten Zeilen ändert sich nichts. $\square$

Bemerkung 3.36. Elementare Zeilenumformungen von Typ III bzw. IV kann man aus denen vom Typ I und II kombinieren:

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{I}} \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{II}} \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{I}} \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

bzw.

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{I}} \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ -a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{II}} \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_i - a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{III}} \begin{pmatrix} \vdots \\ a_i - (a_i - a_j) \\ \vdots \\ a_i - a_j \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i - a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{II}} \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$

$\square$

Lemma 3.37. Ist B aus A durch elementare Zeilenumformungen entstanden, so gilt $\text{ZR}(B) = \text{ZR}(A)$.

Beweis. Nach 3.36 genügt es, Zeilenumformungen vom Typ I bzw. II zu betrachten. Dafür ist die Behauptung wahr. $\square$

Satz 3.38. Jede Matrix $A \in M(m \times n, K)$ kann durch elementare Zeilenumformungen auf Zeilenstufenform gebracht werden.

Beweis. Wir formen A so lange um, bis wir eine Matrix B in Zeilenstufenform erhalten.

Ist $A = 0$, so ist $B = A$ bereits in Zeilenstufenform.

Ist $A \neq 0$, so gibt es mindestens eine Spalte von A , deren Einträge nicht alle Null sind. Wir wählen diejenige Spalte mit dem kleinsten Index j_1 :

$$j_1 := \min\{j \mid \exists i \text{ mit } a_{ij} \neq 0\}.$$

Ist $a_{1j_1} \neq 0$, so können wir a_{1j_1} als Pivot wählen. Andernfalls suchen wir uns ein $a_{i_1j_1} \neq 0$ und vertauschen die Zeile 1 mit der Zeile i_1 . Die neue erste Zeile ist schon die erste Zeile von B . Also gilt für den ersten Pivot

$$b_{1j_1} = a_{i_1j_1}.$$

Durch Umformungen vom Typ III kann man alle unterhalb von b_{1j_1} stehenden Einträge zu Null machen. Ist a einer davon, so soll

$$a + \lambda b_{1j_1} = 0$$

werden, also hat man

$$\lambda = \frac{-a}{b_{1j_1}}$$

zu wählen. Als Ergebnis dieser Umformungen erhalten wir eine Matrix der Gestalt

$$\tilde{A}_1 = \left(\begin{array}{cccc|cccc} 0 & \dots & 0 & b_{1j_1} & * & \dots & * \\ \vdots & & \vdots & 0 & & & \\ \vdots & & \vdots & \vdots & & & \\ 0 & \dots & 0 & 0 & & & \end{array} \begin{array}{c} A_2 \end{array} \right).$$

Im nächsten Schritt macht man mit A_2 das gleiche wie im ersten Schritt mit $A = A_1$. Die dazu nötigen Zeilenumformungen von A_2 kann man auf die Zeilen 2 bis m von $\tilde{A}_1$ ausdehnen, ohne daß sich in den Spalten 1 bis j_1 etwas ändert, denn dort stehen Nullen. Ist A_2 umgeformt, so erhält man A_3 usw. Das Verfahren muß abbrechen, weil die Zeilen- und Spaltenzahlen der Matrizen A_k abnehmen. Als Ergebnis erhält man eine Matrix B in Zeilenstufenform. $\square$

Beispiel 3.39. Wir bestimmen eine Basis des von

$$\begin{aligned} a_1 &= (0, 0, 0, 2, -1) \\ a_2 &= (0, 1, -2, 1, 0) \\ a_3 &= (0, -1, 2, 1, -1) \\ a_4 &= (0, 0, 0, 1, 2) \end{aligned}$$

aufgespannten Untervektorraums U des $\mathbb{R}^5$. Dazu führen wir die entsprechende Matrix A in Zeilenstufenform über:

$$\begin{aligned} A &= \begin{pmatrix} 0 & 0 & 0 & 2 & -1 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & -1 & 2 & 1 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 2 & -1 \\ 0 & -1 & 2 & 1 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \\ &\rightarrow \begin{pmatrix} 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 2 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & -5 \\ 0 & 0 & 0 & 0 & -5 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & -5 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} =: B. \end{aligned}$$

□

Bemerkung 3.40. Der Beweis von 3.38 liefert einen Algorithmus zur Überführung einer Matrix in Zeilenstufenform. Im Zusammenhang mit dem Lösen linearer Gleichungssysteme werden wir auf diesen Algorithmus zurückkommen. Wir sprechen dann auch vom *Eliminationsverfahren von Gauss*. □

Ob man Vektoren als Zeilen oder als Spalten schreibt, ist eine Frage der Konvention. Für die zugehörige Matrix A bedeutet der Übergang vom Zeilen- zum Spaltenraum, daß man A transponiert.

Definition 3.41. Sei $A = (a_{ij}) \in M(m \times n, K)$. Dann heißt

$${}^tA := (a'_{ij}) \in M(m \times n, K) \text{ mit } a'_{ij} := a_{ji}$$

die zu A transponierte Matrix. □

Beispiel 3.42. Es gilt

$${}^t \begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 3 & 1 \end{pmatrix}.$$

□

Unmittelbar aus der Definition ergibt sich

Rechenregeln 3.43. Für $A, B \in M(m \times n, K)$ gilt:

$$(i) \quad {}^t(A + B) = {}^tA + {}^tB.$$

$$(ii) \quad {}^t({}^tA) = A.$$

$$(iii) \quad {}^t(\lambda A) = \lambda {}^tA.$$

Zum Schluß dieses Paragraphen wollen wir – analog zur Vorgehensweise bei Gruppen und Ringen – weitere Möglichkeiten studieren, wie wir aus bereits bekannten Vektorräumen weitere Beispiele ableiten können.

Satz und Definition 3.44. Seien V ein K -Vektorraum und $W \subset V$ ein Unterraum. Dann wird durch

$$K \times V/W \rightarrow V/W, (\lambda, v + W) \rightarrow \lambda \cdot v + W,$$

eine Skalarmultiplikation erklärt, so daß die Faktorgruppe $(V/W, +)$ zusammen mit dieser Skalarmultiplikation zu einem K -Vektorraum wird. Dieser heißt Quotientenvektorraum oder Faktorraum von V nach W .

Beweis. Wir müssen zeigen, daß die Skalarmultiplikation wohldefiniert ist. Seien $v_1, v_2 \in V$ mit $v_1 + W = v_2 + W$ und $\lambda \in K$. Dann $\exists w \in W$ mit $v_1 - v_2 = w$. Es folgt

$$\lambda v_1 - \lambda v_2 = \lambda(v_1 - v_2) = \lambda w \in W$$

und somit

$$\lambda v_1 + W = \lambda v_2 + W.$$

Die Vektorraumgesetze übertragen sich von V auf V/W . □

Satz 3.45. Ist V endlich erzeugt, so auch V/W , und es ist

$$\dim V = \dim W + \dim V/W.$$

Genauer gilt: Ist $(w_1, \dots, w_r)$ eine Basis von W und $(w_1, \dots, w_r, v_{r+1}, \dots, v_n)$ eine Basis von V , so ist

$$(v_{r+1} + W, \dots, v_n + W) =: \mathcal{B}$$

eine Basis von V/W .

Beweis. Ist V endlich erzeugt, so gilt dies auch für W nach 3.27, (i). Sei $(w_1, \dots, w_r)$ eine Basis von W . Nach 3.28 (Basisergänzungssatz) können wir diese zu einer Basis

$$(w_1, \dots, w_r, v_{r+1}, \dots, v_n)$$

von V ergänzen. Es gilt

$$w_i + W = W = 0_{V/W}, \quad i = 1, \dots, r.$$

$\mathcal{B}$ erzeugt V/W . Sei $v + W \in V/W, v \in V$. Dann gibt es $\lambda_1, \dots, \lambda_n \in K$ mit

$$v = \sum_{i=1}^r \lambda_i w_i + \sum_{i=r+1}^n \lambda_i v_i.$$

Es folgt

$$v + W = \sum_{i=r+1}^n \lambda_i (v_i + W).$$

$\mathcal{B}$ ist linear unabhängig. Seien $\lambda_{r+1}, \dots, \lambda_n \in K$ mit

$$0_{V/W} = \sum_{i=r+1}^n \lambda_i (v_i + W) = \left(\sum_{i=r+1}^n \lambda_i v_i \right) + W.$$

Dann ist $\sum_{i=r+1}^n \lambda_i v_i \in W$, d. h. $\exists \lambda_1, \dots, \lambda_r \in K$ mit

$$\sum_{i=r+1}^n \lambda_i v_i = \sum_{i=1}^r \lambda_i w_i.$$

Da aber $(w_1, \dots, w_r, v_{r+1}, \dots, v_n)$ linear unabhängig sind, folgt $\lambda_1 = \dots = \lambda_r = \lambda_{r+1} = \dots = \lambda_n = 0$. □

Im Gegensatz zu Durchschnitten ist die Vereinigung von Untervektorräumen im Allgemeinen kein Untervektorraum, man betrachte etwa zwei verschiedene Nullpunktsgersten im $\mathbb{R}^2$. Man kann aber natürlich den von den Untervektorräumen aufgespannten Untervektorraum (in unserem Beispiel ist dies der ganze $\mathbb{R}^2$) betrachten.

Bemerkung und Definition 3.46. Seien V ein K -Vektorraum und $W, W' \subset V$ Untervektorräume. Dann ist

$$W + W' = \text{span}(W \cup W') = \{v \in V \mid \exists w \in W, w' \in W' \text{ mit } v = w + w'\}$$

ein Untervektorraum. Dieser heißt die *Summe* von W und W' . □

Satz 3.47 (Dimensionsformel für Summen). Sind V ein K -Vektorraum und $W, W' \subset V$ endlichdimensionale Untervektorräume, so gilt

$$\dim(W + W') = \dim W + \dim W' - \dim(W \cap W').$$

Beweis. Nach 3.27, (i) ist auch $W \cap W'$ endlichdimensional. Sei $w_1, \dots, w_r$ eine Basis von $W \cap W'$. Diese können wir nach 3.28 zu Basen

$$(w_1, \dots, w_r, v_{r+1}, \dots, v_n) \text{ bzw. } (w_1, \dots, w_r, v'_{r+1}, \dots, v'_m)$$

von W bzw. W' ergänzen. Die Behauptung ist bewiesen, wenn wir gezeigt haben, daß

$$\mathcal{B} := (w_1, \dots, w_r, v_{r+1}, \dots, v_n, v'_{r+1}, \dots, v'_m)$$

eine Basis von $W + W'$ ist. Daß $W + W'$ von $\mathcal{B}$ erzeugt wird, ist klar.

$\mathcal{B}$ ist linear unabhängig. Seien $\lambda_1, \dots, \lambda_r, \mu_{r+1}, \dots, \mu_n, \mu'_{r+1}, \dots, \mu'_m \in K$ mit

$$\sum_{i=1}^r \lambda_i w_i + \sum_{i=r+1}^n \mu_i v_i + \sum_{i=r+1}^m \mu'_i v'_i = 0. \quad (*)$$

Wir setzen

$$v := \sum_{i=1}^r \lambda_i w_i + \sum_{i=r+1}^n \mu_i v_i.$$

Dann ist $v \in W$ und $-v = \sum_{i=r+1}^m \mu'_i v'_i \in W'$, also $v \in W \cap W'$. Somit gibt es $\alpha_1, \dots, \alpha_r \in K$ mit

$$v = \sum_{i=1}^r \alpha_i w_i.$$

Wegen der Eindeutigkeit der Linearkombinationen folgt dann insbesondere $\mu_{r+1} = \dots = \mu_n = 0$. Einsetzen in (*) liefert $\lambda_1 = \dots = \lambda_r = \mu'_{r+1} = \dots = \mu'_m = 0$, da $(w_1, \dots, w_r, v'_{r+1}, \dots, v'_m)$ eine Basis von W' ist. □

Will man den "Korrekturterm" $\dim(W \cap W')$ loswerden, so muß man $W \cap W' = \{0\}$ fordern.

Definition 3.48. Ein K -Vektorraum V heißt *direkte Summe* von zwei Untervektorräumen W und W' , in Zeichen

$$V = W \oplus W',$$

wenn gilt:

- (i) $V = W + W'$,
- (ii) $W \cap W' = \{0\}$.

□

Satz 3.49. Für einen K -Vektorraum V und Unterräume W' mit

$$V = W + W'$$

sind äquivalent:

- (i) $V = W \oplus W'$.
- (ii) $\forall v \in V$ gibt es eindeutig bestimmte $w \in W, w' \in W'$ mit $v = w + w'$.
- (iii) Sind $0 \neq w \in W$ und $0 \neq w' \in W'$, so sind w und w' linear unabhängig.

Beweis. '(i) $\Rightarrow$ (ii)'. Ist $v = w + w' = \tilde{w} + \tilde{w}'$, so folgt

$$w - \tilde{w} = \tilde{w}' - w' \in W \cap W' = \{0\}.$$

'(ii) $\Rightarrow$ (iii)'. Wären w, w' linear abhängig, so erhielte man verschiedene Darstellungen des Nullvektors.

'(iii) $\Rightarrow$ (i)'. Wäre $0 \neq v \in W \cap W'$, so ergäbe

$$1v + (-1)v = 0$$

einen Widerspruch zu (iii). □

Satz 3.50. Ist V ein endlichdimensionaler K -Vektorraum mit Untervektorräumen W und W' , so sind äquivalent:

- (i) $V = W \oplus W'$.
- (ii) Es gibt Basen $(w_1, \dots, w_r)$ von W und $(w'_1, \dots, w'_s)$ von W' , so daß

$$(w_1, \dots, w_r, w'_1, \dots, w'_s)$$

eine Basis von V ist.

- (iii) $V = W + W'$ und $\dim V = \dim W + \dim W'$.

Beweis. Alle Implikationen (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) ergeben sich unmittelbar aus der Dimensionsformel 3.47. $\square$

Korollar und Definition 3.51. Ist V endlichdimensional und $W \subset V$ ein Untervektorraum, so gibt es einen Untervektorraum $W' \subset V$ mit

$$W \oplus W' = V$$

W' heißt ein direkter Summand von V zu W .

Beweis. Man nehme eine Basis $(w_1, \dots, w_s)$ von W , ergänze sie zu einer Basis von $(w_1, \dots, w_s, v_{s+1}, \dots, v_n)$ von V und setze

$$W' := \text{span}(v_{s+1}, \dots, v_n).$$

$\square$

Beispiel 3.52. Ist $V = \mathbb{R}^2$ und $W = \text{span}(1, 0)$, so gilt etwa

$$V = W \oplus \text{span}(0, 1),$$

aber auch

$$V = W \oplus \text{span}(1, 1).$$

Ein direkter Summand ist also im Allgemeinen nicht eindeutig bestimmt. $\square$

Analog zu 3.40 definiert man die Summe endlich vieler Untervektorräume $W_1, \dots, W_k$ von V durch

$$W_1 + \dots + W_k = \text{span}(W_1 \cup \dots \cup W_k) = \{v \in V \mid \exists w_1 \in W_1, \dots, w_k \in W_k \text{ mit } v = \sum_{i=1}^k w_i\}.$$

Zur Verallgemeinerung der Definition der direkten Summe siehe Literatur.

Aufgaben

Aufgabe 33. Gegeben seien folgende Teilmengen des $\mathbb{Q}$ -Vektorraums $V = \mathbb{Q}^4$:

$$\begin{aligned} U_1 &= \{(x, x+1, x+2, x+4) \mid x \in \mathbb{Q}\} \\ U_2 &= \{(x, 2x, 3x, 4x) \mid x \in \mathbb{Q}\} \\ U_3 &= \{(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{Q}, x_3 = x_1 + x_2, x_4 = x_2 + x_3\} \\ U_4 &= \{(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{Q}, x_2 \geq 0\} \\ U_5 &= \{(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{Z}\} \end{aligned}$$

Welche dieser Mengen sind Untervektorräume von V ? Begründen Sie Ihre Aussage.

Aufgabe 34. (i) Berechnen Sie die Linearkombination $\sum \lambda_i v_i$ der Vektoren $v_i \in V$ für:

a) $K = \mathbb{R}, V = \mathbb{R}^4$

$$v_1 = (3, -1, 2, 0), v_2 = (1, 3, -1, 6), v_3 = (8, 0, -2, 6)$$

$$\lambda_1 = -\frac{1}{3}, \lambda_2 = 2, \lambda_3 = \frac{1}{5}$$

b) $K = \mathbb{C}, V = \mathbb{C}^3$

$$v_1 = (1+i, 1, -i), v_2 = (2, 0, i), v_3 = (-3+i, -i, 1)$$

$$\lambda_1 = 1+i, \lambda_2 = -i, \lambda_3 = i$$

(ii) Sei $\mathbb{F}_2 = (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ der Körper mit zwei Elementen und $V = \mathbb{F}_2^4$. Zeigen Sie, daß die Vektoren

$$v_1 = (1, 0, 0, 0), v_2 = (1, 0, 1, 0), v_3 = (1, 1, 0, 1), v_4 = (0, 1, 0, 1)$$

linear abhängig sind, und untersuchen Sie, welche von ihnen sich als Linearkombination der restlichen drei Vektoren darstellen lassen.

Aufgabe 35. Sei $U \subset \mathbb{R}^5$ der von den Vektoren

$$v_1 = (4, 1, 1, 0, -2), v_2 = (0, 1, 4, -1, 2), v_3 = (4, 3, 9, -2, 2),$$

$$v_4 = (1, 1, 1, 1, 1), v_5 = (0, -2, -8, 2, -4)$$

aufgespannte Untervektorraum. Bestimmen Sie eine Basis von U und ergänzen Sie diese zu einer Basis von $\mathbb{R}^5$.

Aufgabe 36. Lösen Sie Aufgabe 32 mit Hilfe des Eliminationsverfahrens von Gauß.

Kapitel 4

Lineare Abbildungen und Matrizen, lineare Gleichungssysteme

Wir studieren mit der Vektorraumstruktur verträgliche Abbildungen.

Bemerkung und Definition 4.1. Eine Abbildung

$$\varphi : V \rightarrow W$$

zwischen K -Vektorräumen V und W heißt *linear* (genauer K -linear oder *Homomorphismus* von K -Vektorräumen), wenn gilt:

- (i) $\varphi(v + w) = \varphi(v) + \varphi(w) \quad \forall v, w \in V,$
- (ii) $\varphi(\lambda v) = \lambda \varphi(v) \quad \forall \lambda \in K, v \in V.$

Mit anderen Worten: φ ist ein Gruppenhomomorphismus von $(V, +)$ nach $(W, +)$ und φ ist verträglich mit der Skalarmultiplikation. Äquivalent:

$$(iii) \quad \varphi(\lambda v + \mu w) = \lambda \varphi(v) + \mu \varphi(w) \quad \forall \lambda, \mu \in K, v, w \in V.$$

Die weiteren Begriffe aus 2.30 (Monomorphismus, Epimorphismus, Isomorphismus, isomorph, Endomorphismus, Automorphismus) sowie die Aussagen aus 2.31, (i), (ii) (Hintereinanderausführung von linearen Abbildungen, Umkehrabbildungen von Isomorphismen) übertragen sich wortwörtlich.

Ebenso hat man die Begriffe

$$\text{Bild } \varphi = \varphi(V)$$

(Bild von φ) und

$$\text{Kern } \varphi = \{v \in V \mid \varphi(v) = 0\}$$

(Kern von φ) wie in 2.3.2. □

Wir notieren einige einfache Folgerungen aus den Definitionen.

Satz 4.2. Sei $f : V \rightarrow W$ eine lineare Abbildung zwischen K -Vektorräumen. Dann gilt:

- (i) $\varphi(0) = 0$.
- (ii) $\varphi\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i \varphi(v_i)$.
- (iii) $(v_i)_{i \in I}$ linear abhängig in $V \Rightarrow (\varphi(v_i))_{i \in I}$ linear abhängig in W .
- (iv) Sind $V' \subset V$ bzw. $W' \subset W$ Untervektorräume, so auch $\varphi(V') \subset W$ und $\varphi^{-1}(W') \subset V$. Insbesondere sind
- Bild $\varphi \subset W$ und Kern $\varphi \subset V$
- Untervektorräume.
- (v) φ surjektiv $\iff$ Bild $\varphi = W$.
- (vi) φ injektiv $\iff$ Kern $\varphi = \{0\}$.
- (vii) φ injektiv, $v_1, \dots, v_n \in V$ linear unabhängig $\implies \varphi(v_1), \dots, \varphi(v_n) \in W$ linear unabhängig.

Beweis. (i) Ist klar nach 2.32, (i).

(ii) Folgt durch wiederholte Anwendung von 4.1, (iii).

(iii) Ergibt sich aus (i) und (ii).

(iv) Wegen $0 \in V'$ ist $0 = \varphi(0) \in \varphi(V')$, also ist $\varphi(V') \neq \emptyset$.

Sind $w, w' \in \varphi(V')$, so gibt es $v, v' \in V'$ mit $\varphi(v) = w$ und $\varphi(v') = w'$. Also ist

$$w + w' = \varphi(v) + \varphi(v') = \varphi(v + v') \in \varphi(V'),$$

denn $v + v' \in V'$. Für alle $\lambda \in K$ gilt wegen $\lambda v \in V'$:

$$\lambda w = \lambda \varphi(v) = \varphi(\lambda v) \in \varphi(V').$$

Sind $v, v' \in \varphi^{-1}(W')$, so sind $\varphi(v), \varphi(v') \in W'$. Also ist

$$\varphi(v + v') = \varphi(v) + \varphi(v') \in W'$$

und somit $v + v' \in \varphi^{-1}(W')$. Analog sieht man $\lambda v \in \varphi^{-1}(W')$ für $\lambda \in K$ und $v \in \varphi^{-1}(W')$.

(v) Ist klar per Definition.

(vi) Gilt nach 2.32, (iv).

(vii) Seien $\lambda_1, \dots, \lambda_n \in K$ mit $\sum_{i=1}^n \lambda_i \varphi(v_i) = 0$. Dann gilt

$$\varphi\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i \varphi(v_i) = 0.$$

Da φ injektiv ist folgt $\sum_{i=1}^n \lambda_i v_i = 0$, also $\lambda_1 = \dots = \lambda_n = 0$, da $v_1, \dots, v_n$ linear unabhängig.

□

Bemerkung und Definition 4.3. (i) Sind V, W K -Vektorräume, so sei

$$\text{Hom}(V, W) := \text{Hom}_K(V, W) := \{\varphi : V \rightarrow W \mid \varphi \text{ linear}\} .$$

Definiert man $\varphi + \psi$ bzw. $\lambda \cdot \varphi$ durch

$$(\varphi + \psi)(v) := \varphi(v) + \psi(v) \quad \text{bzw.} \quad (\lambda \cdot \psi)(v) := \lambda \cdot \varphi(v) ,$$

so wird dadurch, wie man sofort nachrechnet, $\text{Hom}_K(V, W)$ zu einem K -Vektorraum. Der Nullvektor ist die *Nullabbildung*

$$V \rightarrow W, v \rightarrow 0 .$$

(ii) Im Spezialfall $V = W$ schreibt man

$$\text{End}(V) := \text{End}_K(V) := \text{Hom}_K(V, V)$$

für den K -Vektorraum aller Endomorphismen von V . $\text{End}_K(V)$ zusammen mit der durch Hintereinanderausführung definierten Multiplikation ist sogar eine K -Algebra. $\square$

Beispiel 4.4. (i) Die Abbildung

$$\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^3, \quad (x, y) \rightarrow (x, y, x + y + 1)$$

ist nicht linear, denn

$$\varphi(0, 0) = (0, 0, 1) \neq (0, 0, 0) .$$

(ii) Die Abbildung

$$\varphi : \mathbb{R}^4 \rightarrow \mathbb{R}^2, \quad (w, x, y, z) \rightarrow (w + 2x, 3y - z)$$

ist linear, denn es gilt

$$\begin{aligned} \varphi((w, x, y, z) + (w', x', y', z')) &= (w + w' + 2(x + x'), 3(y + y') - (z + z')) \\ &= \varphi(w, x, y, z) + \varphi(w', x', y', z') \end{aligned}$$

sowie

$$\begin{aligned} \varphi(\lambda(w, x, y, z)) &= (\lambda w + 2\lambda x, 3\lambda y - \lambda z) \\ &= \lambda \varphi(w, x, y, z) . \end{aligned}$$

(iii) Allgemeiner rechnet man leicht nach: Ist

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in M(m \times n, K) ,$$

so ist durch

$$\varphi_A : K^n \rightarrow K^m, \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rightarrow \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} =: A \cdot x$$

eine lineare Abbildung definiert. Dabei schreiben wir die Elemente von K^n bzw. K^m als Spaltenvektoren. Setzt man für x den j -ten kanonischen Basisvektor des K^n ein, so erhält man als Bild die j -te Spalte von A . Die Spalten von A sind also die Bilder der kanonischen Basisvektoren !

Die Vektoren in $\text{Kern } \varphi_A$ sind gerade die Lösungen des homogenen linearen Gleichungssystems

$$\begin{array}{ccccccc} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & 0, \end{array}$$

das wir jetzt auch in der Kurzform

$$A \cdot x = 0$$

schreiben können.

Wir werden später sehen, daß jede lineare Abbildung $\varphi : K^n \rightarrow K^m$ von der Form φ_A für ein $A \in M(m \times n, K)$ ist. $\square$

Ein beliebiges lineares Gleichungssystem wie in der Motivation läßt sich also in der Kurzform

$$A \cdot x = b, \quad A \in M(m \times n, K), \quad b \in K^m$$

schreiben. Die Lösungen sind dann gerade die Vektoren in der Faser $\varphi_A^{-1}(b)$, Insbesondere gibt es genau dann mindestens eine Lösung wenn gilt

$$b \in \text{Bild } \varphi_A.$$

Beispiel 4.5. Sei

$$A = \begin{pmatrix} -2 & 2 \\ -1 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{R}).$$

Dann ist φ_A die Abbildung

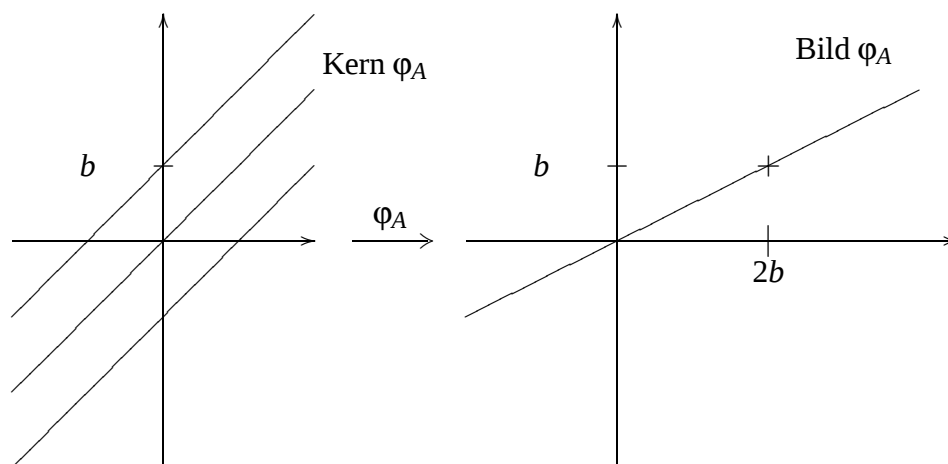
$$\varphi_A : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rightarrow \begin{pmatrix} -2x_1 + 2x_2 \\ -x_1 + x_2 \end{pmatrix}.$$

Es gilt

$$\text{Bild } \varphi_A = \text{span}\left(\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right), \quad \text{Kern } \varphi_A = \text{span}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right),$$

und für $\begin{pmatrix} 2b \\ 2 \end{pmatrix} \in \text{Bild } \varphi_A$ ist die Faser die Gerade mit der Gleichung $x_2 = x_1 + b$, also

$$\varphi_A^{-1}\left(\begin{pmatrix} 2b \\ 2 \end{pmatrix}\right) = \{(\lambda, b+1) \mid \lambda \in \mathbb{R}\} = \begin{pmatrix} 0 \\ b \end{pmatrix} + \text{span}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right).$$



Die Fasern sind also parallele Geraden, der Kern ist die einzige Faser durch den Nullpunkt. Die Lösungen von $A \cdot x = \begin{pmatrix} 2b \\ 2 \end{pmatrix}$ erhält man durch Parallelverschieben der Lösungen von $A \cdot x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ durch einen beliebigen Punkt der Faser

$$\varphi_A^{-1}\left(\begin{pmatrix} 2b \\ b \end{pmatrix}\right).$$

□

Allgemein gilt:

Lemma 4.6. Ist $\varphi : V \rightarrow W$ linear, $w \in \text{Bild } \varphi$ und $v \in \varphi^{-1}(w)$ beliebig, so ist

$$\varphi^{-1}(w) = v + \text{Kern } \varphi = \{v + u \mid u \in \text{Kern } \varphi\}.$$

Beweis. "⊂" Ist $v' \in \varphi^{-1}(w)$, so gilt

$$\begin{aligned} \varphi(v') = \varphi(v) &\Rightarrow \varphi(v' - v) = 0 \Rightarrow u := v' - v \in \text{Kern } \varphi \\ &\Rightarrow v' = v + u \in v + \text{Kern } \varphi \end{aligned}$$

"⊃" Ist umgekehrt $v' = v + u \in v + \text{Kern } \varphi$, so ist $\varphi(v') = \varphi(v) = w$, also $v' \in \varphi^{-1}(w)$ □

Teilmengen, die durch "Parallelverschiebung" eines Untervektorraums entstehen, erhalten einen eigenen Namen.

Definition 4.7. Eine Teilmenge X eines K -Vektorraums V heißt ein *affiner Unterraum*, falls $\exists v \in V$ und Untervektorraum $U \subset V$ mit

$$X = v + U := \{v + u \mid u \in U\}.$$

Auch die leere Menge wird affiner Unterraum genannt. □

Lemma 4.8. Sei $X = v + U$ ein affiner Unterraum. Dann gilt:

$$(i) \quad v' \in X \Rightarrow X = v' + U$$

(ii) Sind $v' \in V$ und $U' \subset V$ ein Untervektorraum mit

$$v + U = v' + U'$$

so folgt

$$U = U' \quad \text{und} \quad v' - v \in U.$$

Beweis. Übung. □

Zu einem affinen Unterraum $X = v + U$ ist also der Untervektorraum U eindeutig bestimmt, während der "Aufhängepunkt" v beliebig in X gewählt werden kann.

Definition 4.9. Ist $X = v + U$ ein affiner Unterraum, so heißt

$$\dim X := \dim U$$

die Dimension von X □

Wir zeigen nun, wie man Basen wählen kann, die maßgeschneidert sind für eine lineare Abbildung.

Satz 4.10. Sei $\varphi : V \rightarrow W$ eine lineare Abbildung zwischen K -Vektorräumen V und W mit $\dim_K V < \infty$. Dann ist auch $\dim_K(\text{Bild } \varphi) < \infty$ und es gilt: Sind Basen

$$(v_1, \dots, v_k) \text{ von } \text{Kern } \varphi \text{ und } (w_1, \dots, w_r) \text{ von } \text{Bild } \varphi$$

sowie beliebige Vektoren $u_1 \in \varphi^{-1}(w_1), \dots, u_r \in \varphi^{-1}(w_r)$ gegeben, so ist

$$\mathcal{A} := (u_1, \dots, u_r, v_1, \dots, v_k)$$

eine Basis von V . Insbesondere gilt die Dimensionsformel

$$\dim V = \dim(\text{Bild } \varphi) + \dim(\text{Kern } \varphi).$$

Beweis. Es gilt

$$\dim(\text{Bild } \varphi) \leq \dim(\text{Kern } \varphi) < \infty,$$

denn sind $y_1 = \varphi(x_1), \dots, y_s = \varphi(x_s) \in \text{Bild } \varphi$ linear unabhängig, so auch $x_1, \dots, x_s \in V$ nach 4.2, (iii). Weiter ist nach 3.27

$$\dim(\text{Kern } \varphi) \leq \dim V < \infty.$$

Wir können also Basen wie angegeben wählen.

$\mathcal{A}$ ist ein Erzeugendensystem von V . Sei $v \in V$. Dann

$$\exists \mu_1, \dots, \mu_r \in K \quad \text{mit} \quad \varphi(v) = \sum_{i=1}^r \mu_i w_i.$$

Wir setzen

$$v' := \sum_{i=1}^r \mu_i u_i .$$

Wegen $\varphi(v) = \varphi(v')$ folgt $v - v' \in \text{Kern } \varphi$, also

$$\exists \lambda_1, \dots, \lambda_k \in K \quad \text{mit} \quad v - v' = \sum_{i=1}^k \lambda_i v_i .$$

Insgesamt gilt

$$v = \sum_{i=1}^r \mu_i u_i + \sum_{i=1}^k \lambda_i v_i .$$

$\mathcal{B}$ ist linear unabhängig. Seien

$$(*) \quad \mu_1, \dots, \mu_r, \lambda_1, \dots, \lambda_k \in K \quad \text{mit} \quad \sum_{i=1}^r \mu_i u_i + \sum_{i=1}^k \lambda_i v_i = 0 .$$

Dann folgt durch Anwendung von φ

$$0 = \sum_{i=1}^r \mu_i \varphi(v_i) = \sum_{i=1}^r \mu_i w_i ,$$

also $\mu_1 = \dots = \mu_r = 0$. Einsetzen in $(*)$ liefert

$$\sum_{i=1}^k \lambda_i v_i = 0 ,$$

also auch $\lambda_1 = \dots = \lambda_k = 0$. □

Unmittelbar aus der Dimensionsformel ergeben sich zwei Folgerungen:

Korollar 4.11. Ist $\dim_K V < \infty$ und $\varphi : V \rightarrow W$ K -linear, so gilt für alle nichtleeren Fasern

$$\dim \varphi^{-1}(W) = \dim V - \dim(\text{Bild } \varphi) .$$

Korollar 4.12. Ist $\dim_K V = \dim_K W < \infty$ und $\varphi : V \rightarrow W$ K -linear, so sind äquivalent:

- (i) φ injektiv.
- (ii) φ surjektiv.
- (iii) φ bijektiv.

Bemerkung 4.13. Wie in 2.33 zeigt man: Ist V ein K -Vektorraum und U ein Unterraum, so ist die kanonische Projektion

$$\pi : V \rightarrow V/U$$

ein Epimorphismus mit

$$\text{Kern } \pi = U.$$

4.10 ist also eine Verallgemeinerung von 3.45. □

Weiter ergibt sich mit den Basen aus 4.10:

Satz 4.14 (Faktorisierungssatz). Seien $\phi : V \rightarrow W$ linear und

$$\mathcal{A} = (u_1, \dots, u_r, v_1, \dots, v_k)$$

eine Basis von V , so daß $(v_1, \dots, v_k)$ eine Basis von $\text{Kern } \phi$ ist. Definieren wir

$$U = \text{span}(u_1, \dots, u_r),$$

so gilt:

(i) $V = U \oplus \text{Kern } \phi.$

(ii) Die Einschränkung $\phi|_U : U \rightarrow \text{Bild } \phi$ ist ein Isomorphismus.

(iii) Bezeichnet

$$P : V = U \oplus \text{Kern } \phi \rightarrow U, v = u + v' \rightarrow u,$$

die Projektion auf den ersten Summanden, so gilt

$$\phi = (\phi|_U) \circ P,$$

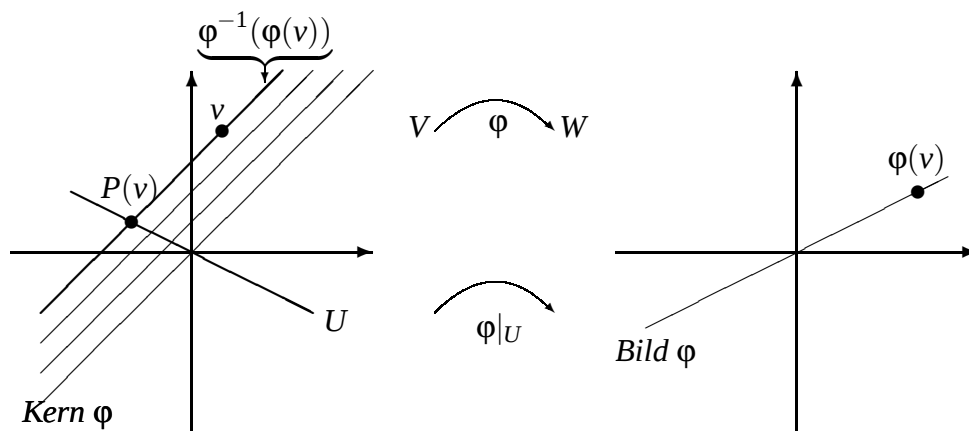
d.h., das Diagramm

$$\begin{array}{ccc} V & & \\ \downarrow P & \searrow \phi & \\ U & \xrightarrow{\phi|_U} & \text{Bild } \phi \subset W \end{array}$$

ist kommutativ.

Insbesondere hat jede nichtleere Faser $\phi^{-1}(w)$ mit U genau einen Schnittpunkt und es gilt

$$P(v) = \phi^{-1}(\phi(v)) \cap U.$$



Beweis. (i) ist klar nach 3.50.

(ii) Mit φ ist auch $\varphi|_U$ linear. Wegen

$$\text{Bild } \varphi|_U = \text{Bild } \varphi$$

und

$$\text{Kern } \varphi|_U = (\text{Kern } \varphi) \cap U = \{0\}$$

ist φ ein Isomorphismus.

(iii) ist klar nach der Definition von P .

Nun zum Zusatz: Ist

$$v = \sum_{i=1}^r \mu_i u_i \in \varphi^{-1}(w) \cap U,$$

so folgt

$$w = \sum_{i=1}^r \mu_i \varphi(u_i).$$

Nach 4.10 ist aber $\varphi(u_1), \dots, \varphi(u_r)$ eine Basis von $\text{Bild } \varphi$. Also sind $\mu_1, \dots, \mu_r$ und damit auch v eindeutig bestimmt. $\square$

Bemerkung 4.15. Man kann also φ zerlegen (oder *faktorisieren*) in eine "Parallelprojektion" P , den Isomorphismus $\varphi|_U$ und die Inklusion $\text{Bild } \varphi \subset U$. $\square$

Will man eine Abbildung $\varphi : X \rightarrow Y$ zwischen Mengen definieren, so kann man die Bilder verschiedener Elemente des Definitionsbereichs völlig unabhängig voneinander wählen.

Ganz anders ist die Situation für eine lineare Abbildung $\varphi : V \rightarrow W$ zwischen Vektorräumen. Kennt man einen Wert $\varphi(v)$, $v \neq 0$ so ist φ auf der ganzen Geraden $K \cdot v = \{\lambda \cdot v \mid \lambda \in K\}$ festgelegt. Will man für einen weiteren Vektor $v' \in V$ den Wert beliebig vorschreiben, so darf also v' nicht auf der Geraden $K \cdot v$ liegen. Durch $\varphi(v)$ und $\varphi(v')$ ist dann φ auf der ganzen Ebene $Kv + Kv'$ festgelegt usw.

Die Frage, durch wieviele Vorgaben eine lineare Abbildung festgelegt ist, hat eine einfache Antwort.

Satz 4.16 (über die Erzeugung von linearen Abbildungen). Gegeben seien Vektorräume V und W mit $\dim_K V < \infty$ sowie Vektoren $v_1, \dots, v_r \in V$ und $w_1, \dots, w_r \in W$. Dann gilt:

(i) $v_1, \dots, v_r$ linear unabhängig $\Rightarrow$ es gibt mindestens eine lineare Abbildung

$$\varphi : V \rightarrow W \quad \text{mit} \quad \varphi(v_i) = w_i, \quad i = 1, \dots, r.$$

(ii) Ist $v_1, \dots, v_r$ sogar eine Basis, so gibt es genau eine solche Abbildung φ . Für diese gilt:

a) $\text{Bild } \varphi = \text{span}(w_1, \dots, w_r)$.

b) φ ist injektiv $\Leftrightarrow w_1, \dots, w_r$ sind linear unabhängig.

Beweis. (ii) Jedes $v \in V$ hat eine eindeutige Darstellung

$$v = \sum_{i=1}^r \lambda_i v_i, \quad \lambda_1, \dots, \lambda_r \in K,$$

da $(v_1, \dots, v_r)$ eine Basis ist. Wegen $\varphi(v_i) = w_i$ und der Linearität von φ ist also $\varphi(v)$ durch

$$\varphi(v) = \sum_{i=1}^r \lambda_i \varphi(v_i)$$

eindeutig bestimmt. Definiert man umgekehrt φ durch diese Vorschrift, so ist φ linear.

a) " $\subset$ " ist klar.

" $\supset$ " Ist $w = \sum_{i=1}^r \mu_i w_i \in \text{span}(w_1, \dots, w_r)$, so gilt $w = \varphi(\sum_{i=1}^r \mu_i v_i) \in \text{Bild } \varphi$.

b) " $\Rightarrow$ ". Seien $w_1, \dots, w_r$ linear abhängig. Dann

$$\exists (\mu_1, \dots, \mu_r) \neq (0, \dots, 0) \quad \text{mit} \quad \sum_{i=1}^r \mu_i w_i = 0.$$

Dann ist $\varphi(\sum_{i=1}^r \mu_i v_i) = 0$, also ist φ nicht injektiv.

" $\Leftarrow$ ". Sei $\varphi(v) = 0$. Schreiben wir $v = \sum_{i=1}^r \lambda_i v_i$, so ist $\sum_{i=1}^r \lambda_i w_i = 0$. Wegen der linearen Unabhängigkeit von $w_1, \dots, w_r$ folgt $\lambda_1 = \dots = \lambda_r = 0$, also $v = 0$.

(i) Wir ergänzen $(v_1, \dots, v_r)$ zu einer Basis

$$(v_1, \dots, v_r, v_{r+1}, \dots, v_n)$$

von V und wählen $w_{r+1}, \dots, w_n \in W$ beliebig. Dann definieren wir φ wie in (ii) bzgl. dieser Basis. □

Korollar 4.17. Zwei endlichdimensionale K -Vektorräume V und W sind genau dann isomorph, $V \cong W$, wenn gilt $\dim_K V = \dim_K W$.

Korollar 4.18. Ist V ein Vektorraum mit einer Basis $\mathcal{B} = (v_1, \dots, v_n)$, so gibt es genau einen Isomorphismus

$$\Phi_{\mathcal{B}} : K^n \rightarrow V \quad \text{mit} \quad \Phi_{\mathcal{B}}(e_j) = v_j, \quad j = 1, \dots, n,$$

wobei $(e_1, \dots, e_n)$ die kanonische Basis des K^n bezeichnet.

Korollar 4.19. Zu jeder linearen Abbildung $\varphi : K^n \rightarrow K^m$ gibt es genau eine Matrix $A \in M(m \times n, K)$, so daß gilt

$$\varphi = \varphi_A, \quad \text{d.h.} \quad \varphi(x) = A \cdot x$$

für alle Spaltenvektoren $x \in K^n$.

Beweis. Man schreibe $\varphi(e_1), \dots, \varphi(e_n)$ als Spaltenvektoren nebeneinander, dies ergibt A . $\square$

Einen solchen Zusammenhang zwischen linearen Abbildungen und Matrizen gibt es nicht nur für Vektorräume vom Typ K^n .

Satz 4.20. Gegeben seien K -Vektorräume

$$V \text{ mit Basis } \mathcal{A} = (v_1, \dots, v_n)$$

und

$$W \text{ mit Basis } B = (w_1, \dots, w_m).$$

Dann gibt es zu jeder linearen Abbildung $\varphi : V \rightarrow W$ genau eine Matrix $A = (a_{ij}) \in M(m \times n, K)$ mit

$$\varphi(v_j) = \sum_{i=1}^m a_{ij} w_i, \quad j = 1, \dots, n. \quad (*)$$

Die durch diese Zuordnung definierte Abbildung

$$M_B^{\mathcal{A}} : \text{Hom}(V, W) \rightarrow M(m \times n, K), \quad \varphi \rightarrow A = M_B^{\mathcal{A}}(\varphi),$$

ist ein Isomorphismus von K -Vektorräumen.

Beweis. Die a_{ij} in (*) existieren, da B eine Basis ist. Aus demselben Grund sind die a_{ij} eindeutig bestimmt. Da auch $\mathcal{A}$ eine Basis ist, gibt es nach 4.16 genau ein φ , das die durch (*) festgelegten Werte annimmt. Also ist $M_B^{\mathcal{A}}$ bijektiv.

$M_B^{\mathcal{A}}$ ist auch linear: Gehört zur linearen Abbildung ψ die Matrix $B = (b_{ij})$, so gilt

$$\begin{aligned} (\varphi + \psi)(v_j) &= \varphi(v_j) + \psi(v_j) = \sum_{i=1}^m a_{ij} w_i + \sum_{i=1}^m b_{ij} w_i \\ &= \sum_{i=1}^m (a_{ij} + b_{ij}) w_i, \end{aligned}$$

und für $\lambda \in K$ ist

$$(\lambda\varphi)(v_j) = \lambda \cdot \varphi(v_j) = \lambda \sum_{i=1}^m a_{ij} w_i = \sum_{i=1}^m (\lambda a_{ij}) w_i$$

$\square$

Bemerkung und Definition 4.21. (i) 4.20 bedeutet: Nach Wahl fester Basen kann man lineare Abbildungen durch Matrizen (d.h. relativ abstrakte durch konkrete Objekte) ersetzen. Man nennt $M_B^{\mathcal{A}}(\varphi)$ auch die *Matrix, die φ bezüglich den Basen $\mathcal{A}$ und B darstellt*.

(ii) Im Spezialfall $V = K^n$ bzw. $W = K^m$ mit den kanonischen Basen $\mathcal{K}$ bzw. $\mathcal{K}'$ ist der kanonische Isomorphismus

$$M_{\mathcal{K}'}^{\mathcal{K}} = \text{Hom}(K^n, K^m) \rightarrow M(m \times n, K), \quad \varphi \leftrightarrow A,$$

die in Korollar 4.19 und 4.4,(iii) beschriebene Beziehung.

- (iii) Den in 3.17 beschriebenen Basisvektoren E_i^j von $M(m \times n, K)$ entsprechen bzgl. $M_B^{\mathcal{A}}$ die durch

$$F_i^j(v_k) := \begin{cases} w_j & k = i, \\ 0 & \text{sonst,} \end{cases}$$

definierten Basisvektoren F_i^j von $\text{Hom}(V, W)$.

□

Als Folgerung aus 4.10 erhält man, daß bei Benutzung der dort konstruierten Basen die darstellende Matrix besonders einfach wird.

Korollar 4.22. Seien $\varphi : V \rightarrow W$ linear, $n = \dim V$, $m = \dim W$ und $r = \dim \text{Bild } \varphi$. Dann $\exists$ Basen $\mathcal{A}$ von V und $\mathcal{B}$ von W mit

$$M_B^{\mathcal{A}}(\varphi) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Dabei ist E_r die in 3.30 eingeführte r -reihige Einheitsmatrix.

Beweis. Wir wählen eine Basis $\mathcal{A}$ von V wie in 4.10 und ergänzen die dort gewählte Basis von $\text{Bild } \varphi$ zu einer Basis $\mathcal{B}$ von W . Bezüglich dieser Basen hat $M_B^{\mathcal{A}}(\varphi)$ die angegebene Form. □

Aufgabe 37. Bringen Sie folgende Matrix auf Zeilenstufenform:

$$\begin{pmatrix} 4+i & -6 & 1 & 0 & 2-i & 5+i \\ -6 & 12 & 0 & 1 & -1 & 3i \\ 10+i & -18 & 1 & -1 & 3-i & 5-2i \\ -2+i & 6 & 1 & 1 & 1-i & 5-i \end{pmatrix} \in M(4 \times 6, \mathbb{C})$$

Aufgabe 38. Für ein Polynom $f \in \mathbb{F}_2[x]$ ist

$$(f) := \{g \cdot f \mid g \in \mathbb{F}_2[x]\}$$

ein Ideal in $\mathbb{F}_2[x]$. Betrachten Sie den Faktorring

$$R := \mathbb{F}_2[x]/(f)$$

für

(a) $f = x^2 + x + 1$,

(b) $f = x^2 + 1$.

Beantworten Sie für (a) und (b) folgende Fragen (mit Begründung!):

- (i) Welche Charakteristik hat R ?
- (ii) Wie viele Elemente enthält R ?
- (iii) Ist R ein Körper?

Bestimmen Sie für beide Fälle die Verknüpfungstabellen von R bzgl. $+$ und $\cdot$.

Aufgabe 39. Sei $U \subset \mathbb{R}^4$ der durch die Vektoren

$$\begin{aligned} w_1 &= (8, -12, 2, 0) \\ w_2 &= (-18, 36, 0, 3) \\ w_3 &= (-2, 6, 1, 1) \end{aligned}$$

aufgespannte Untervektorraum. Bestimmen Sie Basen von U und $\mathbb{R}^4/U$.

Aufgabe 40. Eine Matrix $A \in M(n \times n, K)$ heißt **symmetrisch**, falls ${}^tA = A$.

- (i) Zeigen Sie, daß die symmetrischen Matrizen einen Untervektorraum $\text{Sym}(n, K)$ von $M(n \times n, K)$ bilden. Geben Sie die Dimension und eine Basis von $\text{Sym}(n, K)$ an.

Ist $\text{char}(K) \neq 2$, so heißt $A \in M(n \times n, K)$ **schiefsymmetrisch** (oder **alternierend**), falls ${}^tA = -A$. Im folgenden sei stets $\text{char}(K) \neq 2$.

- (ii) Zeigen Sie, daß die alternierenden Matrizen einen Untervektorraum $\text{Alt}(n, K)$ von $M(n \times n, K)$ bilden. Bestimmen Sie auch für $\text{Alt}(n, K)$ die Dimension und eine Basis.
- (iii) Für $A \in M(n \times n, K)$ sei $A_s := \frac{1}{2}(A + {}^tA)$ und $A_a := \frac{1}{2}(A - {}^tA)$. Zeigen Sie: A_s ist symmetrisch, A_a ist alternierend, und es gilt $A = A_s + A_a$.
- (iv) Zeigen Sie: $M(n \times n, K) = \text{Sym}(n, K) \oplus \text{Alt}(n, K)$.

Maple-Aufgabe M2:

- (i) Studieren Sie die Hilfe der Maple-Funktionen `array`, `linalg[rowdim]`, `linalg[coldim]`.
- (ii) Schreiben Sie eine Prozedur in Maple, die bei Eingabe einer $m \times n$ -Matrix diese auf Zeilenstufenform bringt und ausgibt.

Zwei naheliegende Fragen sind, wie sich die Beziehung zwischen linearen Abbildungen und Matrizen im Zusammenhang mit der Komposition von Abbildungen verhält, und wie sich die Matrix A verändert, wenn man andere Basen einführt. Zunächst zur ersten Frage.

Wir betrachten zuerst den Spezialfall

$$K^r \xrightarrow{\Phi_B} K^n \xrightarrow{\Phi_A} K^m,$$

also

$$B \in M(n \times r, K), \quad A \in M(m \times n, K),$$

und

$$\varphi_B : K^r \longrightarrow K^n, y \longrightarrow B \cdot y,$$

sowie

$$\varphi_A : K^n \longrightarrow K^m, x \longrightarrow A \cdot x.$$

Insbesondere stimmen die Spaltenzahl von A und die Zeilenzahl von B überein.

$\varphi_A \circ \varphi_B$ ist dann die Abbildung

$$\begin{aligned} \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} &\xrightarrow{\varphi_B} \begin{pmatrix} b_{11} \dots b_{1r} \\ \vdots \\ b_{n1} \dots b_{nr} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^r b_{1k} y_k \\ \vdots \\ \sum_{k=1}^r b_{nk} y_k \end{pmatrix} =: \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\ &\xrightarrow{\varphi_A} \begin{pmatrix} a_{11} \dots a_{1r} \\ \vdots \\ a_{m1} \dots a_{mr} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1j} x_j \\ \vdots \\ \sum_{j=1}^n a_{mj} x_j \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^n a_{1j} \sum_{k=1}^r b_{jk} y_k \\ \vdots \\ \sum_{j=1}^n a_{mj} \sum_{k=1}^r b_{jk} y_k \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^r \left(\sum_{j=1}^n a_{1j} b_{jk} \right) y_k \\ \vdots \\ \sum_{k=1}^r \left(\sum_{j=1}^n a_{mj} b_{jk} \right) y_k \end{pmatrix} \\ &=: \begin{pmatrix} c_{11} \dots c_{1r} \\ \vdots \\ c_{m1} \dots c_{mr} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}, \end{aligned}$$

d.h. es gilt

$$\varphi_A \circ \varphi_B = \varphi_C$$

mit

$$C := (c_{ik}) = \left(\sum_{j=1}^n a_{ij} b_{jk} \right).$$

Definition 4.23. Sind

$$A = (a_{ij}) \in M(m \times n, K), \quad B = (b_{jk}) \in M(n \times r, K),$$

so ist das *Produkt* von A und B definiert durch

$$A \cdot B := (c_{ik}) \in M(m \times r, K) \quad \text{mit} \quad c_{ik} = \sum_{j=1}^n a_{ij} b_{jk}$$

□

Bemerkung 4.24. Damit $A \cdot B$ gebildet werden kann, muß also die Spaltenzahl von A mit der Zeilenzahl von B übereinstimmen. $A \cdot B$ hat so viele Zeilen wie A und so viele Spalten wie B . Für die Abbildungen

$$K^r \xrightarrow{\Phi_B} K^n \xrightarrow{\Phi_A} K^m$$

gilt

$$\Phi_A \circ \Phi_B = \Phi_{A \cdot B}.$$

□

Auf den Fall der Komposition von linearen Abbildungen zwischen beliebigen Vektorräumen gehen wir etwas später ein.

Beispiel 4.25. (i)

$$\begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 2 & -2 \\ 2 & -1 & 0 & -3 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & -1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -5 \\ 0 & 1 \\ -1 & -3 \end{pmatrix}$$

(ii) Ist speziell $m = r = 1$ und n beliebig, so gilt

$$(a_1, \dots, a_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + \dots + a_n b_n \in K = M(1 \times 1, K).$$

(iii) Andererseits ist

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot (b_1, \dots, b_n) = \begin{pmatrix} a_1 b_1 & \dots & a_1 b_n \\ \vdots & & \vdots \\ a_n b_1 & \dots & a_n b_n \end{pmatrix} \in M(n \times n, K).$$

(iv) Ist speziell $m = n = r$, so kann man sowohl $A \cdot B$ als auch $B \cdot A$ bilden. Im allgemeinen ist $A \cdot B \neq B \cdot A$: Es gilt etwa

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

aber

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

□

Rechenregeln 4.26. Seien Matrizen $A, A' \in M(m \times n, K)$, $B, B' \in M(n \times r, K)$, $C \in M(r \times s, K)$, sowie $\lambda \in K$ gegeben. Dann gilt:

$$(i) \quad A \cdot (B \cdot C) = (A \cdot B) \cdot C \quad (\text{Assoziativgesetz})$$

$$(ii) \quad E_m \cdot A = A \cdot E_n = A \quad (\text{Neutralität der Einheitsmatrix})$$

$$(iii) \quad \begin{aligned} A \cdot (B + B') &= A \cdot B + A \cdot B' \\ (A + A') \cdot B &= A \cdot B + A' \cdot B \end{aligned} \quad (\text{Distributivgesetze})$$

$$(iv) \quad A \cdot (\lambda \cdot B) = (\lambda A) \cdot B = \lambda(A \cdot B) \quad (\text{Assoziativgesetz})$$

$$(v) \quad {}^t(A \cdot B) = {}^t B \cdot {}^t A.$$

Beweis. Aufgaben. □

Im Spezialfall *quadratischer Matrizen* ($m = n$) folgt aus diesen Regeln (vergleiche auch 4.3,(ii)):

Korollar 4.27. $M(n \times n, K)$ ist eine K -Algebra.

Wir betrachten nun diejenigen Matrizen $A \in M(n \times n, K)$, die ein inverses Element bzgl. der Multiplikation besitzen. Dieses ist nach 2.3,(iii) im Falle der Existenz eindeutig bestimmt.

Definition 4.28. $A \in M(n \times n, K)$ heißt *invertierbar*, wenn $\exists A' \in M(n \times n, K)$ mit

$$A \cdot A' = A' \cdot A = E_n.$$

In diesem Fall schreiben wir auch

$$A^{-1} = A'$$

und nennen A^{-1} die zu A *inverse Matrix*. □

Läßt man nur invertierbare $n \times n$ -Matrizen zur Konkurrenz zu, so erhält man eine Gruppe:

Satz und Definition 4.29. Die Menge

$$\text{GL}(n, K) := \{A \in M(n \times n, K) \mid A \text{ invertierbar}\}$$

mit der Multiplikation von Matrizen als Verknüpfung ist eine Gruppe mit neutralem Element E_n . Sie heißt die allgemeine lineare Gruppe.

Beweis. Zunächst zeigen wir, daß $\text{GL}(n, K)$ bzgl. der Matrizenmultiplikation abgeschlossen ist.:

Sind A, B invertierbar, so auch $A \cdot B$ mit inverser Matrix $B^{-1} \cdot A^{-1}$:

$$\begin{aligned} (AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} = AE_nA^{-1} = E_n, \\ (B^{-1}A^{-1})AB &= B^{-1}(A^{-1}A)B = B^{-1}E_nB = E_n. \end{aligned}$$

Dabei haben wir das Assoziativgesetz benutzt, das sogar in $M(n \times n, K)$ gilt, und wir haben benutzt, daß sich E_n neutral verhält. □

Bemerkung 4.30. Sind die folgenden Größen definiert, so gilt:

$$(A^{-1})^{-1} = A \quad \text{und} \quad (AB)^{-1} = B^{-1}A^{-1}.$$

□

Bemerkung 4.31. Sei $A \in M(n \times n, K)$. Daß A invertierbar ist bedeutet für die lineare Abbildung

$$\varphi_A : K^n \rightarrow K^n,$$

daß φ_A ein Isomorphismus ist. In der Tat gilt

$$\varphi_A \circ \varphi_{A^{-1}} = \varphi_{A \cdot A^{-1}} = \varphi_{E_n} = \text{id}_{K^n}$$

und

$$\varphi_{A^{-1}} \circ \varphi_A = \varphi_{A^{-1} \cdot A} = \varphi_{E_n} = \text{id}_{K^n},$$

d.h. $\varphi_{A^{-1}}$ ist die Umkehrabbildung zu φ_A .

□

Beispiel 4.32. Die Matrix

$$A = \begin{pmatrix} 5 & 10 & 20 \\ 1 & 1 & 1 \\ 12 & 12 & 20 \end{pmatrix} \in M(3 \times 3, \mathbb{Q})$$

ist invertierbar mit

$$A^{-1} = \begin{pmatrix} -1/5 & -1 & 1/4 \\ 1/5 & 7/2 & -3/8 \\ 0 & -3/2 & 1/8 \end{pmatrix}.$$

□

Hat man bereits einen Kandidaten für A^{-1} , so kann man durch Nachrechnen wie eben überprüfen, ob es sich um die inverse Matrix handelt. Wie aber findet man tatsächlich A^{-1} ? Wir werden später sehen, daß das Eliminationsverfahren von Gauss einen Algorithmus liefert, mit dem man entscheiden kann, ob eine gegebene quadratische Matrix invertierbar ist, und mit dem man gleichzeitig die inverse Matrix berechnen kann, falls existent. Im nächsten Kapitel werden wir sehen, daß eine quadratische Matrix genau dann invertierbar ist, wenn ihre Determinante ungleich Null ist.

Bemerkung 4.33. Für $A \in M(n \times n, K)$ sind äquivalent:

- (i) A invertierbar.
- (ii) ${}^t A$ invertierbar.
- (iii) Spaltenrang $A = n$.
- (iv) Zeilenrang $A = n$.

Sind diese Bedingungen erfüllt, so gilt

$$({}^tA)^{-1} = {}^t(A^{-1}) .$$

□

Beweis. '(i) $\Rightarrow$ (ii)' sowie der Zusatz folgt aus

$${}^t(A^{-1}) \cdot {}^tA = {}^t(A \cdot A^{-1}) = {}^tE_n = E_n$$

und

$${}^tA {}^t(A^{-1}) = {}^t(A^{-1} \cdot A) = {}^tE_n = E_n .$$

'(ii) $\Rightarrow$ (i)' ergibt sich daraus durch Transposition.

'(i) $\Leftrightarrow$ (iii)' gilt wegen

$$\begin{aligned} A \text{ invertierbar} &\Leftrightarrow \varphi_A \text{ Isomorphismus} \\ &\Leftrightarrow \text{Spaltenrang } A = n , \end{aligned}$$

denn die Spaltenvektoren von A bilden ja eine Basis von $\text{Bild } \varphi_A$.

'(ii) $\Leftrightarrow$ (iv)' ergibt sich analog oder durch Transposition. □

Wir kommen nun auf die Frage zu sprechen, wie sich die Matrix A verändert, wenn man andere Basen einführt. Dies erlaubt uns dann auch die Frage nach Matrizen und Komposition von linearen Abbildungen zwischen beliebigen Vektorräumen zu beantworten. Außerdem werden wir beweisen, daß Zeilen- und Spaltenrang einer Matrix übereinstimmen.

Bemerkung und Definition 4.34. Sei V ein Vektorraum mit einer Basis $\mathcal{B} = (v_1, \dots, v_n)$. Dann gibt es nach 4.18 genau einen Isomorphismus

$$\Phi_{\mathcal{B}} : K^n \rightarrow V \quad \text{mit} \quad \Phi_{\mathcal{B}}(e_j) = v_j, \quad j = 1, \dots, n,$$

wobei $(e_1, \dots, e_n)$ die kanonische Basis des K^n ist. Es gilt dann

$$\Phi_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{i=1}^n x_i v_i .$$

Man nennt $\Phi_{\mathcal{B}}$ das durch $\mathcal{B}$ bestimmte *Koordinatensystem* in V und

$$x = (x_1, \dots, x_n) = \Phi_{\mathcal{B}}^{-1}(v) \in K^n$$

die *Koordinaten* von $x = \sum_{i=1}^n x_i v_i$. □

Für die Anwendungen ist es wichtig, verschiedene Koordinaten ineinander umzurechnen. Seien also zwei Basen $\mathcal{A} = (v_1, \dots, v_n)$ und $\mathcal{B} = (w_1, \dots, w_n)$ von V gegeben. Dann hat man ein kommutatives Diagramm von Isomorphismen

$$\begin{array}{ccc} K^n & & \\ & \searrow \Phi_{\mathcal{A}} & \\ & & V \\ & \nearrow \Phi_{\mathcal{B}} & \\ K^n & & \end{array} \quad \begin{array}{c} \downarrow \Phi_{\mathcal{B}}^{-1} \circ \Phi_{\mathcal{A}} \\ \\ \downarrow \end{array}$$

Da $\Phi_{\mathcal{B}}^{-1} \circ \Phi_{\mathcal{A}}$ ein Isomorphismus von K^n auf K^n ist, gibt es eine Matrix $T_{\mathcal{B}}^{\mathcal{A}} \in \text{GL}(n, K)$ mit

$$\Phi_{\mathcal{B}}^{-1} \circ \Phi_{\mathcal{A}} = \varphi_{T_{\mathcal{B}}^{\mathcal{A}}} ,$$

d.h. eine invertierbare Matrix $T_{\mathcal{B}}^{\mathcal{A}}$, die $\Phi_{\mathcal{B}} \circ \Phi_{\mathcal{A}}^{-1}$ bzgl. der kanonischen Basis des K^n darstellt.

Definition 4.35. $T_{\mathcal{B}}^{\mathcal{A}}$ heißt die *Transformationsmatrix des Basiswechsels* von $\mathcal{A}$ nach $\mathcal{B}$. $\square$

Bemerkung 4.36. $T_{\mathcal{B}}^{\mathcal{A}}$ hat per Definition die folgende Eigenschaft: Ist

$$v = x_1 v_1 + \dots + x_n v_n = y_1 w_1 + \dots + y_n w_n \in V ,$$

so ist

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = T_{\mathcal{B}}^{\mathcal{A}} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

$\square$

Kennt man also $T_{\mathcal{B}}^{\mathcal{A}}$, so kann man die neuen aus den alten Koordinaten berechnen.

Wie bestimmt man $T_{\mathcal{B}}^{\mathcal{A}}$?

Bemerkung 4.37. (i) Wir betrachten zunächst den Spezialfall $V = K^n$. Sind A bzw. B die Matrizen mit den Vektoren aus $\mathcal{A}$ bzw. $\mathcal{B}$ als Spalten, so gilt $\Phi_A = \varphi_A$ und $\Phi_B = \varphi_B$, also sieht obiges kommutative Diagramm wie folgt aus:

$$\begin{array}{ccc} K^n & & \\ \downarrow \varphi_{T_{\mathcal{B}}^{\mathcal{A}}} & \searrow \varphi_A & \\ & K^n & \\ \uparrow \varphi_B & & \\ K^n & & \end{array}$$

Somit gilt

$$\varphi_{T_{\mathcal{B}}^{\mathcal{A}}} = \varphi_B^{-1} \circ \varphi_A = \varphi_{B^{-1} \cdot A} ,$$

d.h. $T_{\mathcal{B}}^{\mathcal{A}}$ ist das Produkt

$$T_{\mathcal{B}}^{\mathcal{A}} = B^{-1} \cdot A .$$

(ii) Sei nun wieder V beliebig. Schreibt man die Vektoren aus $\mathcal{B} = (w_1, \dots, w_n)$ als Linearkombination der Vektoren aus $\mathcal{A} = (v_1, \dots, v_n)$,

$$w_j = \sum_{i=1}^n s_{ij} v_j \quad \text{mit} \quad s_{ij} \in K ,$$

so gilt für die Matrix $S = (s_{ij})$:

$$(\Phi_{\mathcal{A}} \circ \varphi_S)(e_j) = \Phi_{\mathcal{A}}(s_{1j}, \dots, s_{nj}) = \sum_{i=1}^n s_{ij} v_i = w_j = \Phi_{\mathcal{B}}(e_j) .$$

Da eine lineare Abbildung durch die Bilder einer gegebenen Basis eindeutig bestimmt ist, folgt

$$\Phi_{\mathcal{A}} \circ \varphi_S = \Phi_{\mathcal{B}} ,$$

also

$$\varphi_{T_{\mathcal{B}}^{\mathcal{A}}} = \Phi_{\mathcal{B}}^{-1} \circ \Phi_{\mathcal{A}} = \varphi_{S^{-1}}$$

und somit

$$T_{\mathcal{B}}^{\mathcal{A}} = S^{-1} .$$

□

Beispiel 4.38. Im $\mathbb{R}^2$ seien $\mathcal{A} = \mathcal{K} = (e_1, e_2)$ die kanonische Basis und

$$\mathcal{B} = (w_1, w_2) = \left(\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right) .$$

Dann gilt in 4.37,(i):

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} .$$

Durch Lösen des linearen Gleichungssystems

$$\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

erhält man

$$B^{-1} = \frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} .$$

Also folgt

$$T_{\mathcal{B}}^{\mathcal{A}} = B^{-1} \cdot A = B^{-1} = \frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} .$$

Nun kann man Koordinaten ineinander umrechnen. Betrachtet man etwa den Vektor mit den Koordinaten $x = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$ bzgl. $\mathcal{A} = (e_1, e_2)$, d.h. den Vektor $v = -e_1 - e_2$, so hat v bzgl. $\mathcal{B}$ die Koordinaten

$$y = B^{-1} \cdot x = \begin{pmatrix} -2/5 \\ -1/5 \end{pmatrix} ,$$

d.h. es gilt

$$v = -2/5 w_1 - 1/5 w_2 .$$

□

Den Zusammenhang zwischen Koordinatensystemen und Matrizen liefert

Lemma 4.39. Seien $\varphi: V \rightarrow W$ eine lineare Abbildung und $\mathcal{A} = (v_1, \dots, v_n)$ bzw. $\mathcal{B} = (w_1, \dots, w_m)$ Basen von V bzw. W . Dann ist das Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{\Phi_{\mathcal{A}}} & V \\ \varphi_{M_{\mathcal{B}}^{\mathcal{A}}(\varphi)} \downarrow & & \downarrow \varphi \\ K^m & \xrightarrow{\Phi_{\mathcal{B}}} & W \end{array}$$

kommutativ.

Beweis. Sei $\mathcal{K} = (e_1, \dots, e_n)$ die kanonische Basis des K^n und sei

$$\Phi_{\mathcal{B}}^{\mathcal{A}}(\varphi) =: A = (a_{ij}) .$$

Wir müssen zeigen:

$$\Phi_{\mathcal{B}} \circ \varphi_{M_{\mathcal{B}}^{\mathcal{A}}(\varphi)} = \varphi \circ \Phi_{\mathcal{A}} .$$

Es genügt, die Bilder der Basisvektoren zu vergleichen. Für diese gilt

$$\begin{aligned} \Phi_{\mathcal{B}} \circ \varphi_{M_{\mathcal{B}}^{\mathcal{A}}(\varphi)} &= \Phi_{\mathcal{B}}(a_{1j}, \dots, a_{mj}) = \sum_{i=1}^m a_{ij} w_i \\ &= \varphi(v_j) = \varphi(\Phi_{\mathcal{A}}(e_j)) . \end{aligned}$$

□

Nun zur Komposition von linearen Abbildungen:

Satz 4.40. Gegeben seien Vektorräume U, V, W der Dimension r, m, n mit Basen $\mathcal{A}, \mathcal{B}, \mathcal{C}$ sowie lineare Abbildungen

$$U \xrightarrow{\psi} V \xrightarrow{\varphi} W .$$

Dann gilt

$$M_{\mathcal{C}}^{\mathcal{A}}(\varphi \circ \psi) = M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \circ M_{\mathcal{B}}^{\mathcal{C}}(\psi) .$$

Beweis. Nach Bemerkung 4.24 und 4.21,(ii) ist die Aussage richtig für Vektorräume vom Typ K^n zusammen mit den kanonischen Basen. Daraus folgt nun die allgemeine Behauptung durch Betrachten des kommutativen Diagramms (!)

$$\begin{array}{ccccc} K^r & & \xrightarrow{\Phi_{\mathcal{A}}} & & U \\ & \searrow \varphi_{\mathcal{B}} & & \searrow \psi & \\ & & K^n & \xrightarrow{\Phi_{\mathcal{B}}} & V \\ & \nearrow \varphi_{\mathcal{A}} & & \nearrow \varphi & \\ K^m & & \xrightarrow{\Phi_{\mathcal{C}}} & & W \end{array}$$

$\varphi_{\mathcal{A} \cdot \mathcal{B}}$ (links), $\varphi \circ \psi$ (rechts)

wobei $A = M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ und $B = M_{\mathcal{B}}^{\mathcal{C}}(\psi)$.

□

Beispiel 4.41. Durch

$$\psi(x_1, x_2) = (2x_1, x_1 + x_2, 0)$$

und

$$\varphi(y_1, y_2, y_3) = (y_1 + y_2, y_1 + y_3, y_2 + y_3, y_1 + y_2 + y_3)$$

sind lineare Abbildungen

$$\mathbb{R}^2 \xrightarrow{\psi} \mathbb{R}^3 \xrightarrow{\varphi} \mathbb{R}^4$$

definiert. Wie wählen die Basen

$$\mathcal{A} = (u_1, u_2) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) \quad \text{von } \mathbb{R}^2,$$

$$\mathcal{B} = \mathcal{K} = (e_1, e_2, e_3) \quad \text{von } \mathbb{R}^3,$$

$$\mathcal{C} = (w_1, w_2, w_3, w_4) = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right) \quad \text{von } \mathbb{R}^4.$$

Da $\mathcal{B}$ die kanonische Basis des $\mathbb{R}^3$ ist, sind die Spalten der Matrix

$$B := M_{\mathcal{B}}^{\mathcal{A}}(\psi)$$

die Bilder der Basisvektoren u_1, u_2 . Wegen

$$\varphi(u_1) = \varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \quad \text{und} \quad \varphi(u_2) = \varphi\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}$$

gilt also

$$B = \begin{pmatrix} 2 & 2 \\ 1 & 2 \\ 0 & 0 \end{pmatrix}.$$

Wir berechnen

$$A := M_{\mathcal{C}}^{\mathcal{B}}(\psi):$$

Es ist

$$\varphi(e_1) = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 0 \cdot w_1 + 1 \cdot w_2 - 1 \cdot w_3 + 1 \cdot w_4,$$

$$\varphi(e_2) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 1 \cdot w_1 - 1 \cdot w_2 + 0 \cdot w_3 + 1 \cdot w_4,$$

$$\varphi(e_3) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 1 \cdot w_1 + 0 \cdot w_2 - 0 \cdot w_3 + 1 \cdot w_4,$$

also

$$A = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Analog erhält man

$$C := M_C^{\mathcal{A}}(\varphi \circ \psi) = \begin{pmatrix} 1 & 2 \\ 1 & 0 \\ -2 & -2 \\ 3 & 4 \end{pmatrix},$$

denn es gilt

$$\begin{aligned} (\varphi \circ \psi)(u_1) &= \begin{pmatrix} 3 \\ 2 \\ 1 \\ 3 \end{pmatrix} = 1 \cdot w_1 + 1 \cdot w_2 - 2 \cdot w_3 + 3 \cdot w_4, \\ (\varphi \circ \psi)(u_2) &= \begin{pmatrix} 4 \\ 2 \\ 2 \\ 4 \end{pmatrix} = 1 \cdot w_1 + 0 \cdot w_2 - 2 \cdot w_3 + 4 \cdot w_4. \end{aligned}$$

Tatsächlich gilt also

$$A \cdot B = C.$$

□

Nun kommen wir zur Antwort auf die Frage, wie sich die darstellende Matrix bei Einführung neuer Basen ändert.

Satz 4.42 (Transformationsformel). Ist $\varphi : V \rightarrow W$ eine lineare Abbildung zwischen endlich-dimensionalen Vektorräumen, und sind Basen $\mathcal{A}, \mathcal{A}'$ von V bzw. $\mathcal{B}, \mathcal{B}'$ von W gegeben, so ist das Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{\varphi_{M_{\mathcal{B}}^{\mathcal{A}}(\varphi)}} & K^m \\ \downarrow \varphi_{T_{\mathcal{A}'}^{\mathcal{A}}} & \searrow \Phi_{\mathcal{A}} & \swarrow \Phi_{\mathcal{B}} \\ & V & \xrightarrow{\varphi} W \\ & \nearrow \Phi_{\mathcal{A}'} & \searrow \Phi_{\mathcal{B}'} \\ K^n & \xrightarrow{\varphi_{M_{\mathcal{B}'}^{\mathcal{A}'}(\varphi)}} & K^m \\ & \downarrow \varphi_{T_{\mathcal{B}'}^{\mathcal{B}}} & \end{array}$$

kommutativ. Insbesondere gilt für die beteiligten Matrizen

$$M_{\mathcal{B}'}^{\mathcal{A}'}(\varphi) = T_{\mathcal{B}'}^{\mathcal{B}} \cdot M_{\mathcal{B}}^{\mathcal{A}}(\varphi) \cdot (T_{\mathcal{A}'}^{\mathcal{A}})^{-1}$$

Anders ausgedrückt: Sind

$$A = M_{\mathcal{B}}^{\mathcal{A}}(\varphi) \quad \text{und} \quad B = M_{\mathcal{B}'}^{\mathcal{A}'}(\varphi)$$

die beiden Matrizen die φ bzgl. der Basen $\mathcal{A}, \mathcal{B}$ bzw. $\mathcal{A}', \mathcal{B}'$ darstellen, und sind

$$T = T_{\mathcal{A}'}^{\mathcal{A}}, \quad S = T_{\mathcal{B}'}^{\mathcal{B}}$$

die entsprechenden Transformationsmatrizen zwischen den Basen, so gilt

$$B = S \cdot A \cdot T^{-1}.$$

Beweis. 4.39 und 4.40 . □

Nun können wir Zeilenrang und Spaltenrang einer Matrix vergleichen.

Satz 4.43. Für jede Matrix $A \in M(m \times n, K)$ gilt

$$\text{Zeilenrang } A = \text{Spaltenrang } A.$$

Beweis. Wir betrachten die lineare Abbildung

$$\varphi_A : K^n \rightarrow K^m, \quad x \mapsto A \cdot x,$$

und wählen Basen $\mathcal{A}$ von K^n und $\mathcal{B}$ von K^m wie in 4.22, d.h. mit

$$B := M_{\mathcal{B}}^{\mathcal{A}}(\varphi_A) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Für B gilt

$$\text{Zeilenrang } B = r = \text{Spaltenrang } B.$$

□

Um zu zeigen, daß sich diese Gleichheit auf A überträgt, wählen wir gemäß 4.41 invertierbare Matrizen S und T mit

$$B = S \cdot A \cdot T^{-1}$$

Die Behauptung ergibt sich dann aus dem folgenden Lemma.

Lemma 4.44. Für $A \in M(m \times n, K)$, $S \in GL(m, K)$ und $T \in GL(n, K)$ gilt

(i) $\text{Spaltenrang } SAT^{-1} = \text{Spaltenrang } A.$

(ii) $\text{Zeilenrang } SAT^{-1} = \text{Zeilenrang } A.$

Beweis. Zu den gegebenen Matrizen gehört ein kommutatives Diagramm linearer Abbildungen

$$\begin{array}{ccc} K^n & \xrightarrow{\varphi_A} & K^m \\ \varphi_{T^{-1}} \uparrow & & \downarrow \varphi_S \\ K^n & \xrightarrow{\varphi_{SAT^{-1}}} & K^m \end{array}.$$

Nach 4.31 sind φ_S und $\varphi_{T^{-1}}$ Isomorphismen, es folgt

$$\begin{aligned}\text{Spaltenrang } A &= \dim \text{Bild } \varphi_A = \dim \text{Bild } \varphi_S \circ \varphi_A \circ \varphi_{T^{-1}} \\ &= \text{Spaltenrang } \varphi_{SAT^{-1}},\end{aligned}$$

d.h. es gilt (i). (ii) ergibt sich aus (i) durch Transposition, denn

$$\text{Zeilenrang } A = \text{Spaltenrang } {}^t A$$

und

$${}^t(S \cdot A \cdot T^{-1}) = {}^t(T^{-1}) \cdot {}^t A \cdot {}^t S.$$

□

Wie man die Matrizen S und T im Beweis von 4.43 aus A berechnen kann, werden wir etwas später sehen.

Bemerkung und Definition 4.45. (i) Ist $A \in M(m \times n, K)$, so heißt

$$\text{rang } A := \text{Zeilenrang } A = \text{Spaltenrang } A$$

der *Rang* von A .

(ii) Ist $\varphi : V \rightarrow W$ eine lineare Abbildung zwischen K -Vektorräumen V und W , so heißt

$$\text{rang } \varphi := \dim \text{Bild } \varphi$$

der *Rang* von φ .

(iii) Sind $\mathcal{A}$ bzw. $\mathcal{B}$ Basen der endlichdimensionalen K -Vektorräume V bzw. W , so gilt

$$\text{rang } M_{\mathcal{B}}^{\mathcal{A}}(\varphi) = \text{rang } \varphi.$$

In der Tat, betrachte das kommutative Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{\Phi_{\mathcal{A}}} & V \\ \varphi_{M_{\mathcal{B}}^{\mathcal{A}}(\varphi)} \downarrow & & \downarrow \varphi \\ K^m & \xrightarrow{\Phi_{\mathcal{B}}} & W \end{array}$$

□

Bemerkung und Definition 4.46. $A, B \in M(m \times n, K)$ heißen *äquivalent*, in Zeichen $A \sim B$, wenn $\exists S \in \text{GL}(m, K), T \in \text{GL}(n, K)$ mit

$$B = S \cdot A \cdot T^{-1}.$$

Man rechnet sofort nach, daß es sich hierbei tatsächlich um eine Äquivalenzrelation handelt. Nach 4.41 sind zwei Matrizen genau dann äquivalent, wenn sie bzgl. geeigneter Paare von Basen die gleiche lineare Abbildung beschreiben. □

Satz 4.47. Zwei Matrizen $A, B \in M(m \times n, K)$ sind genau dann äquivalent, wenn gilt

$$\text{rang } A = \text{rang } B .$$

Insbesondere ist jede $m \times n$ -Matrix vom Rang r äquivalent zu

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} .$$

Beweis. Daß äquivalente Matrizen den gleichen Rang haben folgt aus 4.44. Ist A vom Rang r , so sieht man durch entsprechende Wahl der Basen von K^n und K^m , daß gilt

$$A \sim \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} .$$

Also ist A auch äquivalent zu jeder anderen Matrix B vom Rang r , da $\sim$ transitiv. $\square$

Die Matrizen $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$ repräsentieren also die Äquivalenzklassen bzgl. $\sim$, sie heißen auch *Normalformen*. Es gibt genau $1 + \min(m, n)$ verschiedene Äquivalenzklassen von $m \times n$ -Matrizen.

Wir betrachten noch einen wichtigen Spezialfall:

Bemerkung und Definition 4.48. Wir betrachten den Fall $V = W$, d.h. den Fall eines Endomorphismus $\varphi \in \text{End}(V)$.

(i) Sind $\mathcal{A}, \mathcal{B}$ zwei Basen von V , so folgt aus der Transformationsformel 4.42:

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) = T_{\mathcal{B}}^{\mathcal{A}} \cdot M_{\mathcal{A}}^{\mathcal{A}}(\varphi) \cdot (T_{\mathcal{B}}^{\mathcal{A}})^{-1} .$$

Anders ausgedrückt:

$$B = SAS^{-1} ,$$

wenn $A = M_{\mathcal{A}}^{\mathcal{A}}(\varphi)$, $B = M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ und $S = T_{\mathcal{B}}^{\mathcal{A}}$.

(ii) Zwei quadratische Matrizen $A, B \in M(n \times n, K)$ heißen *ähnlich*, wenn $\exists S \in \text{GL}(n, K)$ mit

$$B = S \cdot A \cdot S^{-1} ,$$

d.h. wenn sie bzgl. geeigneter Basen den gleichen Endomorphismus beschreiben. Auch hier handelt es sich wieder um eine Äquivalenzrelation. $\square$

Mit Normalformen für Klassen ähnlicher Matrizen werden wir uns im 2. Semester beschäftigen.

Aufgabe 41. Sei

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \in M(4 \times 5, \mathbb{R}).$$

Bestimmen Sie Basen von Kern φ_A und Bild φ_A .

Aufgabe 42. Sei $\varphi \in \text{End}_K(V)$ mit $\varphi \circ \varphi = \varphi$. Zeigen Sie, daß es Untervektorräume U, W von V gibt mit:

- (i) $V = U \oplus W$
- (ii) $\varphi(W) = 0$
- (iii) $\varphi(u) = u \quad \forall u \in U$

Aufgabe 43. Seien V und W endlichdimensionale Vektorräume mit $V = V_1 \oplus V_2, W = W_1 \oplus W_2$ sowie $\varphi : V \rightarrow W$ linear mit $\varphi(V_i) \subset W_i$ für $i = 1, 2$. Zeigen Sie, daß es Basen $\mathcal{A}$ von V und $\mathcal{B}$ von W gibt mit

$$M_{\mathcal{B}}^{\mathcal{A}}(\varphi) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

wobei $A \in M(\dim W_1 \times \dim V_1, K), B \in M(\dim W_2 \times \dim V_2, K)$.

Aufgabe 44.

- (i) Gegeben sei die Menge von Matrizen

$$\mathcal{M} = \left\{ \begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & 5 \\ 1 & 8 & -7 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 8 \\ -7 \end{pmatrix}, (-1 \ 2 \ 0 \ 8), \begin{pmatrix} 1 & 4 \\ 0 & 5 \\ 6 & 8 \end{pmatrix} \right\}.$$

Berechnen Sie für alle Paare $(A, B) \in \mathcal{M} \times \mathcal{M}$ das Produkt $A \cdot B$, falls dieses definiert ist.

- (ii) Gegeben sei

$$A = \begin{pmatrix} -2 & 3 & 2 & 3 \\ -3 & 5 & 0 & 1 \\ -1 & 2 & -2 & -2 \end{pmatrix}.$$

Bestimmen Sie Basen $\mathcal{A}$ von $\mathbb{R}^4$ und $\mathcal{B}$ von $\mathbb{R}^3$ mit

$$M_{\mathcal{B}}^{\mathcal{A}}(\varphi_A) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Maple-Aufgabe M3. Sie haben für Aufgabe M2 eine weitere Woche Zeit!

Wir wollen nun das Gauss'sche Eliminationsverfahren benutzen, um die Inverse einer invertierbaren Matrix zu berechnen, und um die Transformationsmatrizen zu bestimmen, die eine gegebene Matrix auf Normalform bringen. Zur theoretischen Begründung ist es dabei hilfreich, Matrizenumformungen zu interpretieren als Multiplikation mit speziellen invertierbaren Matrizen, den *Elementarmatrizen*. Genauer bewirkt die Multiplikation von links mit Elementarmatrizen elementare Zeilenumformungen, die Multiplikation von rechts elementare Spaltenumformungen.

Definition 4.49. Sind $m \in \mathbb{N}$, $1 \leq i, j \leq m$, und $\lambda \in K^*$, so nennt man die folgenden quadratischen Matrizen aus $M(m \times m, K)$ *Elementarmatrizen*:

$$S_i(\lambda) := \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ - & - & - & \lambda & - & - & - \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 \end{pmatrix} \begin{matrix} \leftarrow i\text{-te Zeile} \end{matrix}$$

$j\text{-te Spalte}$
 $\downarrow$

Im folgenden sei $i \neq j$.

$$Q_i^j := \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ - & - & 1 & - & - & 1 & - \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix} \begin{matrix} \leftarrow i\text{-te Zeile} \end{matrix}$$

$j\text{-te Spalte}$
 $\downarrow$

$$Q_i^j(\lambda) := \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix} \begin{matrix} \leftarrow i\text{-te Zeile} \\ \end{matrix}$$

$j\text{-te Spalte}$
↓

$$P_i^j := \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & & & & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \\ & & & 1 & & & 0 & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots & \\ & & & & & & & & & 1 \end{pmatrix} \begin{matrix} \leftarrow i\text{-te Zeile} \\ \leftarrow j\text{-te Zeile} \end{matrix}$$

Außer den eingetragenen oder durch Punkte angedeuteten sind dabei alle Koeffizienten gleich Null. $\square$

Bemerkung 4.50. Seien $A \in M(m \times n, K)$ und $\lambda \in K^*$ gegeben.

- (i) Durch elementare Zeilenumformungen wie in 3.35 erhält man aus A die folgenden Matrizen:

A_I durch Multiplikation der i -ten Zeile mit λ ,

A_{II} durch Addition der j -ten Zeile zur i -ten Zeile,

A_{III} durch Addition der λ -fachen j -ten Zeile zur i -ten Zeile,

A_{IV} durch Vertauschen der i -ten Zeile und der j -ten Zeile.

Offensichtlich gilt

$$A_I = S_i(\lambda) \cdot A,$$

$$A_{II} = Q_i^j \cdot A,$$

$$A_{III} = Q_i^j(\lambda) \cdot A,$$

$$A_{IV} = P_i^j \cdot A.$$

(ii) Für die analogen elementaren Spaltenumformungen von A ergibt sich

$$\begin{aligned} A^I &= A \cdot S_i(\lambda), \\ A^{II} &= A \cdot Q_j^i, \\ A^{III} &= A \cdot Q_j^i(\lambda), \\ A^{IV} &= A \cdot P_j^i. \end{aligned}$$

□

Bemerkung 4.51. (i) Entsprechend 3.36 sind die Elementarmatrizen $Q_i^j(\lambda)$ und P_i^j Produkte von Elementarmatrizen vom Typ $S_i(\lambda)$ und Q_i^j :

$$Q_i^j(\lambda) = S_j\left(\frac{1}{\lambda}\right) \cdot Q_i^j \cdot S_j(\lambda)$$

und

$$P_i^j = Q_j^i \cdot Q_i^j(-1) \cdot Q_j^i \cdot S_j(-1).$$

(ii) Die Elementarmatrizen sind invertierbar und ihre Inversen sind wieder Elementarmatrizen:

$$\begin{aligned} (S_i(\lambda))^{-1} &= S_i\left(\frac{1}{\lambda}\right), \\ (Q_i^j)^{-1} &= Q_i^j(-1), \\ (Q_i^j(\lambda))^{-1} &= Q_i^j(-\lambda), \\ (P_i^j)^{-1} &= P_i^j. \end{aligned}$$

Dies überprüft man durch Ausmultiplizieren.

□

Satz 4.52. Jede invertierbare Matrix $A \in M(n \times n, K)$ ist endliches Produkt von Elementarmatrizen, d.h. die Gruppe $GL(n, K)$ wird von den Elementarmatrizen erzeugt.

Beweis. Nach 4.33 gilt Zeilenrang $A = n$. Führt man also A mit Hilfe des Gauss'schen Verfahrens in 3.38 in eine Matrix B mit Zeilenstufenform über, so muß B eine obere Dreiecksmatrix mit von Null verschiedenen Diagonalelementen sein, d.h. B ist von der Form

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & \ddots & \vdots \\ 0 & & b_{nn} \end{pmatrix}$$

mit

$$b_{11} \cdot \dots \cdot b_{nn} \neq 0.$$

Nach 4.50 gibt es Elementarmatrizen $B_1, \dots, B_r$ mit

$$B = B_r \cdot \dots \cdot B_1 \cdot A.$$

Man kann nun B durch weitere Zeilenumformungen zur Einheitsmatrix E_n machen: Zunächst beseitige man $b_{1n}, \dots, b_{n-1,n}$ mit Hilfe der letzten Zeile, dann $b_{1,n-1}, \dots, b_{n-2,n-1}$ mit Hilfe der vorletzten Zeile usw. Schließlich normiere man die Koeffizienten in der Diagonale auf 1. Es gibt also weitere Elementarmatrizen $B_{r+1}, \dots, B_s$, so daß gilt

$$B_s \cdot \dots \cdot B_1 \cdot A = B_s \cdot \dots \cdot B_{r+1} \cdot B = E_n .$$

Mit 4.51, (ii) folgt, daß

$$A = B_1^{-1} \cdot \dots \cdot B_s^{-1}$$

ein Produkt von Elementarmatrizen ist. □

Aus dem Beweis ergibt sich auch

$$A^{-1} = B_s \cdot \dots \cdot B_1 = B_s \cdot \dots \cdot B_1 \cdot E_n ,$$

und somit ein einfaches Rechenverfahren zur Bestimmung der inversen Matrix.

Algorithmus 4.53 (Berechnung der inversen Matrix). Ist $A \in M(n \times n, K)$ gegeben, so schreibe man die Matrizen A und E_n nebeneinander. Alle Umformungen, die im folgenden an A vorgenommen werden, führe man gleichzeitig an E_n durch.

Zunächst bringt man A durch elementare Zeilenumformungen auf Zeilenstufenform. Dabei stellt sich heraus, ob gilt

$$\text{Zeilensrang } A = n ,$$

d.h. ob A invertierbar ist. Gilt $\text{Zeilensrang } A < n$, so kann man aufhören, A ist nicht invertierbar, und die Umformungen mit E_n waren dann umsonst. Andernfalls führt man weitere Zeilenumformungen durch, bis aus A die Matrix E_n geworden ist:

A	E_n
$B_1 \cdot A$	$B_1 \cdot E_n$
$\vdots$	$\vdots$
$B_s \cdot \dots \cdot B_1 \cdot A$	$B_s \cdot \dots \cdot B_1 \cdot E_n$

Ist links E_n entstanden, so steht rechts A^{-1} .

Beispiel 4.54. Sei $K = \mathbb{R}$.

(i)

$$A = \begin{array}{l} \\ Q_3^1(-1) \\ Q_3^2 \end{array} \begin{array}{|ccc|ccc|} \hline 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 1 \\ \hline \end{array}$$

A ist nicht invertierbar wegen

$$\text{Zeilenrang } A = 2.$$

(ii)

$$\begin{array}{l}
 A = \begin{array}{c|ccc}
 0 & 1 & -4 & 1 & 0 & 0 \\
 1 & 2 & -1 & 0 & 1 & 0 \\
 1 & 1 & 2 & 0 & 0 & 1
 \end{array} \\
 P_2^1 \begin{array}{c|ccc}
 1 & 2 & -1 & 0 & 1 & 0 \\
 0 & 1 & -4 & 1 & 0 & 0 \\
 1 & 1 & 2 & 0 & 0 & 1
 \end{array} \\
 Q_3^1(-1) \begin{array}{c|ccc}
 1 & 2 & -1 & 0 & 1 & 0 \\
 0 & 1 & -4 & 1 & 0 & 0 \\
 0 & 0 & 3 & 0 & -1 & 1
 \end{array} \\
 Q_3^2 \begin{array}{c|ccc}
 1 & 2 & -1 & 0 & 1 & 0 \\
 0 & 1 & -4 & 1 & 0 & 0 \\
 0 & 0 & -1 & 1 & -1 & 1
 \end{array} \\
 S_3(-1) \begin{array}{c|ccc}
 1 & 2 & -1 & 0 & 1 & 0 \\
 0 & 1 & -4 & 1 & 0 & 0 \\
 0 & 0 & 1 & -1 & 1 & -1
 \end{array} \\
 Q_1^2(-2) \begin{array}{c|ccc}
 1 & 0 & 7 & -2 & 1 & 0 \\
 0 & 1 & -4 & 1 & 0 & 0 \\
 0 & 0 & 1 & -1 & 1 & -1
 \end{array} \\
 Q_1^3(-7) \begin{array}{c|ccc}
 1 & 0 & 0 & 5 & -6 & 7 \\
 0 & 1 & -4 & 1 & 0 & 0 \\
 0 & 0 & 1 & -1 & 1 & -1
 \end{array} \\
 Q_2^3(4) \begin{array}{c|ccc}
 1 & 0 & 0 & 5 & -6 & 7 \\
 0 & 1 & 0 & -3 & 4 & -4 \\
 0 & 0 & 1 & -1 & 1 & -1
 \end{array} = A^{-1}.
 \end{array}$$

Man berechne zur Kontrolle $A \cdot A^{-1}$!

□

Ist $A \in M(m \times n, K)$, so gibt es nach 2.47 Transformationsmatrizen $S \in GL(m, K)$ und $T \in GL(n, K)$ mit

$$SAT^{-1} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix},$$

wobei $r = \text{rang } A$. Wir leiten nun ein Rechenverfahren zur Bestimmung von S und T ab.

Algorithmus 4.55 (Berechnung von Transformationsmatrizen). Sei $A \in M(m \times n, K)$. Wir betrachten folgendes Schema:

E_m	A	
$B_1 \cdot E_m$	$B_1 \cdot A$	
$\vdots$	$\vdots$	
$B_k \cdot \dots \cdot B_1 \cdot E_m$	$B_k \cdot \dots \cdot B_1 \cdot A$	E_n
	$B_k \cdot \dots \cdot B_1 \cdot A \cdot C_1$	$E_n \cdot C_1$
	$\vdots$	$\vdots$
	$B_k \cdot \dots \cdot B_1 \cdot A \cdot C_1 \cdot \dots \cdot C_l$	$E_n \cdot C_1 \cdot \dots \cdot C_l$

Zunächst wird A durch elementare Zeilenumformungen, die man gleichzeitig an E_m durchführt, auf Zeilenstufenform gebracht. Die Zeilenumformungen entsprechen der Multiplikation von links mit m -reihigen Elementarmatrizen $B_1, \dots, B_k$. Da die Matrix

$$B_k \cdot \dots \cdot B_1 \cdot A$$

Zeilenstufenform hat, kann man sie durch elementare Spaltenumformungen, die man gleichzeitig an E_n durchführt, auf die Form

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

mit $r = \text{rang } A$ bringen. Dies entspricht der Multiplikation von rechts mit n -reihigen Elementarmatrizen $C_1, \dots, C_l$. Wegen

$$B_k \cdot \dots \cdot B_1 \cdot A \cdot C_1 \cdot \dots \cdot C_l = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

sind durch

$$S = B_k \cdot \dots \cdot B_1 = B_k \cdot \dots \cdot B_1 \cdot E_m$$

und

$$T^{-1} = C_1 \cdot \dots \cdot C_l = E_n \cdot C_1 \cdot \dots \cdot C_l$$

die gewünschten Transformationsmatrizen gefunden.

Beispiel 4.56. Für $K = \mathbb{R}$ und $A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 2 & 1 \end{pmatrix}$ ergibt sich:

$$\begin{array}{c}
 \begin{array}{|cc|ccc|}
 \hline
 1 & 0 & 1 & 2 & 0 \\
 0 & 1 & 2 & 2 & 1 \\
 \hline
 \end{array} = A \\
 \\
 S = \begin{array}{|cc|ccc|ccc|}
 \hline
 1 & 0 & 1 & 2 & 0 & 1 & 0 & 0 \\
 -2 & 1 & 0 & -2 & 1 & 0 & 1 & 0 \\
 \hline
 \end{array} \\
 \\
 SAT^{-1} = \begin{array}{|ccc|ccc|}
 \hline
 1 & 0 & 2 & 1 & 0 & 0 \\
 0 & 1 & -2 & 0 & 0 & 1 \\
 \hline
 \end{array} \\
 \\
 \begin{array}{|ccc|ccc|}
 \hline
 1 & 0 & 0 & 1 & 0 & -2 \\
 0 & 1 & -2 & 0 & 0 & 1 \\
 & & & 0 & 1 & 0 \\
 \hline
 \end{array} \\
 \\
 SAT^{-1} = \begin{array}{|ccc|ccc|}
 \hline
 1 & 0 & 0 & 1 & 0 & -2 \\
 0 & 1 & 0 & 0 & 0 & 1 \\
 & & & 0 & 1 & 2 \\
 \hline
 \end{array} = T^{-1}
 \end{array}$$

□

Ist

$$D = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix},$$

so erhält man auch Basen $\mathcal{A}$ und $\mathcal{B}$ von K^n und K^m , bzgl. derer die Abbildung

$$\varphi_A : K^n \rightarrow K^m, \quad x \rightarrow A \cdot x$$

durch D beschrieben wird. Dazu betrachten wir das Diagramm

$$\begin{array}{ccc}
 K^n & \xrightarrow{\varphi_D} & K^m \\
 \varphi_T \uparrow & & \uparrow \varphi_S \\
 K^n & \xrightarrow{\varphi_A} & K^m
 \end{array},$$

das wegen

$$D = SAT^{-1}$$

kommutativ ist. $\mathcal{A}$ bzw. $\mathcal{B}$ sind die Bilder der kanonischen Basen $\mathcal{K}$ bzw. $\mathcal{K}'$ von K^n bzw. K^m unter den Isomorphismen $\varphi_{T^{-1}}$ und $\varphi_{S^{-1}}$. Also erhält man $\mathcal{A}$ und $\mathcal{B}$ als Spaltenvektoren von T^{-1} und S^{-1} . Dazu muß man S noch invertieren.

Beispiel 4.57. In 4.56 ist

$$S^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

also sind

$$\mathcal{A} = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \\ 2 \end{pmatrix} \right), \quad \mathcal{B} = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

die gesuchten Basen. Zur Kontrolle prüft man noch:

$$A \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad A \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad A \cdot \begin{pmatrix} -2 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

□

Nun wollen wir das Lösen von linearen Gleichungssystemen systematisch behandeln.

Satz und Definition 4.58. *Sei*

$$Ax = b, \quad A = (a_{ij}) \in M(m \times n, K), \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \quad (*)$$

ein lineares Gleichungssystem. Dann heißt

$$Ax = 0 \quad (**)$$

das zu () gehörige homogene System. Ist $b \neq 0$, so nennt man das System (*) inhomogen. Ist $r := \text{rang } A$ und setzt man*

$$\text{Lös}(A, b) := \{x \in K^n \mid Ax = b\} \subset K^n$$

so gilt:

- (i) $\text{Lös}(A, 0) \subset K^n$ ist ein Untervektorraum der Dimension $n - r$.
- (ii) $\text{Lös}(A, b) \subset K^n$ ist entweder leer oder ein affiner Raum der Dimension $n - r$.
Ist $v \in \text{Lös}(A, b)$ beliebig, so gilt

$$\text{Lös}(A, b) = v + \text{Lös}(A, 0).$$

Wir sprechen auch von den Lösungsräumen $\text{Lös}(A, b)$ bzw. $\text{Lös}(A, 0)$.

Beweis. Ist

$$\varphi_A : K^n \rightarrow K^m, x \mapsto Ax$$

so gilt

$$\text{Lös}(A, b) = \varphi_A^{-1}(b).$$

Die Behauptung ergibt sich aus 4.10, 4.11 und 4.45. $\square$

Man erhält also alle Lösungen des inhomogenen Systems (*), in dem man zu einer speziellen Lösung von (*) alle Lösungen des homogenen Systems (**) addiert.

Definition 4.59. Das lineare Gleichungssystem

$$Ax = b$$

heißt

- (i) lösbar, wenn es mindestens eine Lösung gibt,
- (ii) eindeutig lösbar, wenn es genau eine Lösung gibt.

Jedes homogene System ist lösbar, denn es gibt ja mindestens die *triviale Lösung* $x = 0$. Im allgemeinen Fall erhält man ein Kriterium für die Lösbarkeit bzw. eindeutige Lösbarkeit durch Betrachten der Matrix (A, b) , die aus A durch Hinzunahme des Spaltenvektors b entsteht. $\square$

Satz 4.60. Für das lineare Gleichungssystem

$$Ax = b, A = (a_{ij}) \in M(m \times n, K), b \in K^m \quad (*)$$

gilt:

- (i) (*) lösbar $\Leftrightarrow \text{rang } A = \text{rang}(A, b)$
- (ii) (*) eindeutig lösbar $\Leftrightarrow \text{rang } A = \text{rang}(A, b) = n$

Beweis. Wir schreiben $A' = (A, b)$ und betrachten die linearen Abbildungen

$$\varphi_A : K^n \rightarrow K^m, x \mapsto Ax$$

und

$$\varphi_{A'} : K^{n+1} \rightarrow K^m, x' \mapsto A'x'$$

mit

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, x' = \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ x_{n+1} \end{pmatrix}.$$

Dann gilt für die kanonischen Basen $(e_1, \dots, e_n)$ des K^n bzw. $(e'_1, \dots, e'_n, e'_{n+1})$ des K^{n+1} :

$$\varphi_A(e_1) = \varphi_{A'}(e'_1), \dots, \varphi_A(e_n) = \varphi_{A'}(e'_n) \text{ und } \varphi_{A'}(e'_{n+1}) = b.$$

Insbesondere ist stets $\text{Bild } \varphi_A \subset \text{Bild } \varphi_{A'}$ und somit

$$\text{rang } A \leq \text{rang } A'.$$

(i) folgt aus

$$\text{rang } A = \text{rang } A' \Leftrightarrow \text{Bild } \varphi_A = \text{Bild } \varphi_{A'} \Leftrightarrow b \in \text{Bild } \varphi_A \Leftrightarrow (*) \text{ lösbar}$$

Ist $(*)$ lösbar oder äquivalent $\text{rang } A = \text{rang}(A, b)$, so ist $(*)$ eindeutig lösbar $\Leftrightarrow$ das zugehörige homogene System hat nur die triviale Lösung $x = 0 \Leftrightarrow \varphi_A$ ist ein Monomorphismus $\Leftrightarrow \text{rang } A = \dim \text{Bild } \varphi_A = n$; dies ergibt (ii). $\square$

Bemerkung 4.61. Daß bei vorgegebenem $A \in M(m \times n, K)$ für jedes $b \in K^m$ mindestens eine Lösung von

$$Ax = b$$

existiert bedeutet, daß φ_A surjektiv ist, d.h. daß $\text{rang } A = m$ ist. $\square$

Bemerkung 4.62. Ist

$$(A, b) = \left(\begin{array}{ccc|ccc} \bullet & & & & & \\ \hline & \bullet & & & & \\ & & \bullet & & & \\ & & & \ddots & & \\ & & & & \bullet & \\ \hline & & & & & b_{r+1} \\ & & & & & \vdots \\ & & & & & b_m \end{array} \right)$$

mit A in Zeilenstufenform, so gilt

$$\text{rang } A = \text{rang}(A, b) \Leftrightarrow b_{r+1} = \dots = b_m = 0.$$

$\square$

Zum Lösen eines linearen Gleichungssystems $Ax = b$ kann man nun in zwei Schritten vorgehen: Im 1. Schritt bringe man A durch elementare Zeilenumformungen auf Zeilenstufenform, wobei man b entsprechend mit umformt. Dabei verändert sich der Lösungsraum nicht:

Lemma 4.63. Ist $S \in GL(m, K)$, so gilt

$$\text{Lös}(A, b) = \text{Lös}(SA, Sb)$$

Beweis.

$$x \in \text{Lös}(A, b) \Leftrightarrow Ax = b \Leftrightarrow S Ax = S b \Leftrightarrow x \in \text{Lös}(SA, Sb).$$

□

Satz 4.64. Geht (A, b) aus $(\tilde{A}, \tilde{b})$ durch elementare Zeilenumformungen hervor, so gilt

$$\text{Lös}(A, b) = \text{Lös}(\tilde{A}, \tilde{b}).$$

Beweis. Jede elementare Zeilenumformung entspricht der Multiplikation von links mit einer Elementarmatrix nach 4.50. Die Elementarmatrizen sind invertierbar nach 4.51(ii). □

Im 2. Schritt kann man nun von einem Gleichungssystem $Ax = b$ ausgehen, in dem (A, b) bereits in Zeilenstufenform ist.

Algorithmus 4.65. Sei

$$(A, b) = \left(\begin{array}{cccc|ccc} \bullet & & & & & & & \\ & \bullet & & & & & & \\ & & \bullet & & & & & \\ & & & \ddots & & & & \\ & & & & \bullet & & & \\ & & & & & b_{r+1} & & \\ & & & & & \vdots & & \\ & & & & & b_m & & \end{array} \right)$$

mit A in Zeilenstufenform. Gibt es ein i , $r+1 \leq i \leq m$, mit $b_i \neq 0$, so ist $Ax = b$ nicht lösbar. Andernfalls sei für jedes i , $1 \leq i \leq r$, j_i der Spaltenindex des Pivot-Elements in der i -ten Zeile. Das zu lösende lineare Gleichungssystem sieht dann wie folgt aus:

$$\begin{array}{ccccccc} x_{j_1} \overbrace{a_{1j_1}}^{\neq 0} & + & \dots & + & x_n a_{1n} & = & b_1 \\ & & \ddots & & & & \vdots \\ & & & x_{j_r} \underbrace{a_{rj_r}}_{\neq 0} & + \dots + x_n a_{rn} & = & b_r \end{array}$$

Wir schreiben $J = \{j_1, \dots, j_r\}$ und nennen jede Variable x_j , $j \in \{1, \dots, n\} \setminus J$, freie Variable und jede Variable x_j , $j \in J$, gebundene Variable.

Für jede der $n - r$ freien Variablen x_j kann man ein beliebiges Element aus K einsetzen. Man erhält dann einen Lösungsvektor, in dem man für jede der gebundenen Variablen x_j den nach den folgenden Rekursionsformeln berechneten Wert einsetzt:

$$x_{j_k} = \frac{1}{a_{kj_k}} (b_k - \sum_{j > j_k} a_{kj} x_j), \quad k = r, \dots, 1.$$

Durchläuft man beim Einsetzen für die $n - r$ freien Variablen den ganzen Vektorraum K^{n-r} , so durchlaufen die Lösungen den ganzen $(n - r)$ -dimensionalen affinen Lösungsraum des Systems.

Beispiel 4.66. Wir lösen das lineare Gleichungssystem

$$3x_1 + 4x_2 + 5x_3 = 9$$

$$6x_1 + 7x_2 + 8x_3 = 9$$

$$6x_1 + 6x_2 + 6x_3 = 0$$

Überführung in Zeilenstufenform liefert

$$\left(\begin{array}{ccc|c} 3 & 4 & 5 & 9 \\ 6 & 7 & 8 & 9 \\ 6 & 6 & 6 & 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 3 & 4 & 5 & 9 \\ 0 & -1 & -2 & -9 \\ 0 & -2 & -4 & -18 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 3 & 4 & 5 & 9 \\ 0 & -1 & -2 & -9 \\ 0 & 0 & 0 & 0 \end{array} \right),$$

d.h. das lineare Gleichungssystem

$$3x_1 + 4x_2 + 5x_3 = 9$$

$$-x_2 - 2x_3 = -9.$$

x_3 ist also freie Variable und kann beliebig gewählt werden. Die allgemeine Lösung ergibt sich rekursiv

$$\begin{aligned} x_2 &= 9 - 2x_3 \\ x_1 &= \frac{1}{3}(9 - 4x_2 - 5x_3) = \frac{1}{3}(9 - 36 + 8x_3 - 5x_3) = -9 + x_3 \end{aligned}$$

mit beliebigem x_3 . Diese Lösungen können wir auch in der Form

$$x = (x_1, x_2, x_3) = \underbrace{(-9, 9, 0)}_{\text{spez. Lösung}} + \underbrace{\lambda(1, -2, 1)}_{\text{Lösung des hom. System}}, \lambda \in K$$

schreiben.

Wir wollen nun noch einen Schritt weitergehen und eine systematische Methode angeben, wie man eine Basis des Lösungsraums $\text{Lös}(\tilde{A}, 0)$, sowie eine spezielle Lösung von $\tilde{A}x = \tilde{b}$ bekommt. Dazu muß man die erweiterte Matrix $(\tilde{A}, \tilde{b})$ durch elementare Zeilenumformungen auf *Zeilenstufennormalform* (A, b) bringen. Nach 4.24 gilt wieder

$$\text{Lös}(A, b) = \text{Lös}(\tilde{A}, \tilde{b}) \quad \text{bzw.} \quad \text{Lös}(A, 0) = \text{Lös}(\tilde{A}, 0).$$

□

Definition 4.67. Sei $B = (b_{ij})$ eine Matrix in Zeilenstufenform und seien $j_1, \dots, j_r$ die Spaltenindizes der Pivot-Elemente. Dann heißt B in Zeilenstufennormalform, wenn gilt:

(i) Alle Pivot-Elemente sind 1, d.h. es gilt

$$b_{ij_i} = 1, \quad i = 1, \dots, r.$$

(ii) Oberhalb der Pivot-Elemente stehen nur Nullen, d.h. es gilt

$$b_{kj_i} = 0, \quad i = 1, \dots, r, \quad k = 1, \dots, j_i - 1.$$

□

Bemerkung 4.68. Nach 3.38 kann jede Matrix durch elementare Zeilenumformungen in Zeilenstufenform übergeführt werden. Es ist aber auch klar, daß man jede Matrix in Zeilenstufenform durch elementare Zeilenumformungen in eine solche Zeilenstufennormalform überführen kann. Tatsächlich kann man sogar zeigen: Zu jeder Matrix A gibt es genau eine Matrix in Zeilenstufennormalform, in die sich A durch elementare Zeilenumformungen überführen läßt.

□

Beispiel 4.69.

$$\begin{pmatrix} 3 & 4 & 5 & 9 \\ 0 & -1 & -2 & -9 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 4/3 & 5/3 & 3 \\ 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & -1 & -9 \\ 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

□

Satz 4.70. Seien $(A, b) = (a_{ij}, b_i) \in M(m \times (n+1), K)$ eine Matrix mit A in Zeilenstufennormalform, $r = \text{rang } A$, j_i der Spaltenindex des Pivotelements in der i -ten Zeile, $i = 1, \dots, r$ und $J = \{j_1, \dots, j_r\}$. Dann gilt für das lineare Gleichungssystem

$$(*) \quad Ax = b$$

und das zugehörige homogene System

$$(**) \quad Ax = 0 :$$

(i) $(*)$ hat keine Lösung $\Leftrightarrow b_i \neq 0$ für ein $i \in \{r+1, \dots, m\}$.

(ii) Ist $b_i = 0$ für $i = r+1, \dots, m$, so ist $v = {}^t(v_1, \dots, v_n) \in K^n$ definiert durch

$$v_v := \begin{cases} b_i & \text{falls } v = j_i \\ 0 & \text{sonst} \end{cases}$$

eine spezielle Lösung von $(*)$.

(iii) $\forall k \in \{1, \dots, n\} \setminus J$ sei $u^k = {}^t(u_1^k, \dots, u_n^k) \in K^n$ definiert durch

$$u_v^k := \begin{cases} a_{ik} & \text{falls } v = j_i \\ -1 & \text{falls } v = k \\ 0 & \text{sonst.} \end{cases}$$

Dann ist

$$B := (u^k \mid k \in \{1, \dots, n\} \setminus J)$$

eine Basis von $\text{Lös}(A, 0)$.

Insgesamt gilt

$$\text{Lös}(A, b) = v + \text{span}(u^k \mid k \in \{1, \dots, n\} \setminus J).$$

Beweis. (i) ist wieder klar nach 4.60, (i)

(ii) $\forall i \in \{1, \dots, r\}$ gilt

$$\sum_{v=1}^n a_{iv} v_v = a_{ij_i} b_i = b_i.$$

Also ist v eine spezielle Lösung von (*).

(iii) $\forall k \in \{1, \dots, n\} \setminus J, \forall i \in \{1, \dots, r\}$ gilt

$$\sum_{v=1}^n a_{iv} u_v^k = -a_{ik} + a_{ij_i} a_{ik} = 0.$$

Also sind alle u^k Lösungen von $Ax = 0$. Die u^k sind auch linear unabhängig. Ist

$$\sum_{k \in \{1, \dots, n\} \setminus J} \lambda_k u^k = 0, \lambda_k \in K,$$

so gilt $\forall l \in \{1, \dots, n\} \setminus J$:

$$0 = \sum_{k \in \{1, \dots, n\} \setminus J} \lambda_k u_l^k = \lambda_l,$$

also sind alle $\lambda_k = 0$. Wegen $\text{rang } A = r$ gibt es genau $n - r$ linear unabhängige Lösungen von (**) nach 4.58(i). Also bilden die u^k eine Basis von $\text{Lös}(A, 0)$. □

Algorithmus 4.71. Seien (A, b) , r und $J = \{j_1, \dots, j_r\}$ wie in 4.70. Ist $b_i \neq 0$ für ein $i \in \{r + 1, \dots, m\}$, so hat $Ax = b$ keine Lösung. Andernfalls führe man in der Matrix (A, b) Nullzeilen ein, so daß die Pivot-Elemente in der neuen Matrix in der Diagonalen stehen, d.h. das Pivot-Element der i -ten Zeile steht an der Stelle (j_i, j_i) .

Durch weiteres Anhängen bzw. Streichen von Nullzeilen erhält man eine $n \times (n + 1)$ -Matrix. Dann ersetze man alle Nullen an den Stellen $(k, k), k \in \{1, \dots, n\} \setminus J$ durch eine -1 . Sei $C = (c^1, \dots, c^{n+1})$ die so entstandene Matrix. Dann ist c^{n+1} eine spezielle Lösung von $Ax = b$ und die Vektoren $c^k, k \in \{1, \dots, n\} \setminus J$, bilden eine Basis von $\text{Lös}(A, 0)$. Insgesamt gilt:

$$\text{Lös}(A, b) = c^{n+1} + \text{span}(c^k \mid k \in \{1, \dots, n\} \setminus J).$$

Beispiel 4.72. (i) Noch einmal 4.66 bzw. 4.69.

$$(A, b) = \begin{pmatrix} 1 & 0 & -1 & -9 \\ 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

ist in Zeilenstufennormalform. Die Pivot-Elemente stehen bereits in der Diagonalen und (A, b) ist eine 3×4 -Matrix. Wir müssen also lediglich die Null an der Stelle $(3, 3)$ durch eine -1 ersetzen:

$$(A, b) \rightarrow \begin{pmatrix} 1 & 0 & -1 & -9 \\ 0 & 1 & 2 & 9 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Es folgt

$$\text{Lös}(A, b) = \begin{pmatrix} -9 \\ 9 \\ 0 \end{pmatrix} + \text{span} \left(\begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} \right).$$

(ii)

$$(A, b) = \begin{pmatrix} 1 & 2 & 0 & -1 & 0 & 2 \\ 0 & 0 & 1 & 5 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

ist bereits in Zeilenstufennormalform. Unser Verfahren ergibt

$$(A, b) = \begin{pmatrix} 1 & 2 & 0 & -1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 0 & -1 & 0 & 2 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 & -2 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 7 \end{pmatrix}.$$

Es folgt

$$\text{Lös}(A, b) = \begin{pmatrix} 2 \\ 0 \\ -2 \\ 0 \\ 7 \end{pmatrix} + \text{span} \left(\begin{pmatrix} 2 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 5 \\ -1 \\ 0 \end{pmatrix} \right).$$

(iii)

$$(A, b) = \begin{pmatrix} 1 & 0 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 & 5 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

Es folgt

$$\text{Lös}(A, b) = \begin{pmatrix} 1 \\ 5 \\ 0 \\ 0 \end{pmatrix} + \text{span}\left(\begin{pmatrix} 0 \\ 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \\ -1 \end{pmatrix}\right).$$

□

Aufgabe 45.

(i) Sei

$$A = \begin{pmatrix} 2 & 4 & 2 \\ 2 & 12 & 7 \\ 1 & 10 & 6 \end{pmatrix} \in M(3 \times 3, \mathbb{R}).$$

Für welche $t \in \mathbb{R}$ ist das lineare Gleichungssystem

$$A \cdot x = b, \quad b = \begin{pmatrix} 12t \\ 12t + 7 \\ 7t + 8 \end{pmatrix}$$

lösbar? Geben Sie gegebenenfalls alle Lösungen an.

(ii) Seien

$$A = \begin{pmatrix} 2 & 5 & 10 & 8 & 8 \\ 1 & 3 & 7 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 0 & -2 \end{pmatrix} \in M(4 \times 5, \mathbb{R}), \quad b = \begin{pmatrix} -1 \\ -2 \\ 1 \\ -3 \end{pmatrix} \in \mathbb{R}^4.$$

Bestimmen Sie alle Lösungen von $A \cdot x = b$.

Aufgabe 46.

(i) Sind die folgenden Matrizen invertierbar? Wenn ja, dann geben Sie die inverse Matrix an.

$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix} \in M(3 \times 3, \mathbb{R}), \quad \begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix} \in M(3 \times 3, \mathbb{Z}/3\mathbb{Z}).$$

(ii) Zeigen Sie:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2 \times 2, K) \text{ ist invertierbar} \Leftrightarrow \det(A) \neq 0.$$

Berechnen Sie in diesem Fall die Inverse von A .

Aufgabe 47. Im $\mathbb{R}^3$ seien die Basen

$$\mathcal{A} = ((1, -1, 2), (2, 3, 7), (2, 3, 6)) \text{ und } \mathcal{B} = ((1, 2, 2), (-1, 3, 3), (-2, 7, 6))$$

gegeben.

(i) Berechnen Sie die Transformationsmatrix $T_{\mathcal{B}}^{\mathcal{A}}$.

(ii) Bestimmen Sie die Koordinaten des Vektors

$$v = 2 \cdot (1, -1, 2) + 9 \cdot (2, 3, 7) - 8 \cdot (2, 3, 6)$$

bezüglich der Basis $\mathcal{B}$.

Aufgabe 48:

Sei

$$A = \begin{pmatrix} 7 & 5 & 4 & 2 \\ 5 & -14 & -7 & -12 \\ 3 & 8 & 5 & 4 \end{pmatrix} \in M(3 \times 4, \mathbb{R}).$$

Führen Sie A in Normalform D über und bestimmen Sie Basen $\mathcal{A}$ bzw. $\mathcal{B}$ von $\mathbb{R}^4$ bzw. $\mathbb{R}^3$, bzgl. derer φ_A durch D beschrieben wird.

Maple-Aufgabe M4.

- (i) Schreiben Sie eine Prozedur in Maple, die als Eingabe eine $m \times n$ -Matrix A und einen Vektor b mit m Komponenten erhält und die Lösungsmenge des linearen Gleichungssystems $A \cdot x = b$ berechnet.
- (ii) Schreiben Sie eine Prozedur in Maple, die bei Eingabe einer $n \times n$ -Matrix A prüft, ob diese invertierbar ist, und gegebenenfalls die zu A inverse Matrix ausgibt.

Kapitel 5

Determinanten

Bereits in der Motivation zu Beginn der Vorlesung haben wir die Determinante einer 2×2 -Matrix eingeführt. Nun wollen wir erklären, was die Determinante einer beliebigen $n \times n$ -Matrix ist. Dazu gibt es mehrere Möglichkeiten. Zwei davon sind:

- Wir geben eine Formel für die Determinante an, die von den Einträgen der Matrix abhängt, also etwa

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc .$$

- Wir charakterisieren die Determinante als Abbildung

$$\det : M(n \times n, K) \rightarrow K, \quad A \rightarrow \det A,$$

durch ihre grundlegenden Eigenschaften. Dann muß man zeigen, daß es tatsächlich eine Abbildung mit diesen Eigenschaften gibt, und daß sie durch die Eigenschaften eindeutig bestimmt ist. Und man muß angeben, wie man Determinanten ausrechnet.

Wir gehen hier nach der 2. Möglichkeit vor. Ist dabei $A \in M(n \times n, K)$, so bezeichnen wir stets mit $a_1, \dots, a_n$ die Zeilenvektoren von A und schreiben

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} .$$

Definition 5.1. Seien K ein Körper und $n \in \mathbb{N}$, $n > 0$. Dann heißt eine Abbildung

$$\det : M(n \times n, K) \rightarrow K, \quad A \rightarrow \det A,$$

Determinante, falls gilt:

D1) $\det$ ist *linear in jeder Zeile*, d.h. $\forall i \in \{1, \dots, n\}$ gilt:

a) Ist $a_i = a'_i + a''_i$, so ist

$$\det \begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} = \det \begin{pmatrix} \vdots \\ a'_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a''_i \\ \vdots \end{pmatrix}.$$

b) Ist $\lambda \in K$, so ist

$$\det \begin{pmatrix} \vdots \\ \lambda a_i \\ \vdots \end{pmatrix} = \lambda \cdot \det \begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix}.$$

An den mit Punkten bezeichneten Stellen stehen dabei jeweils unverändert die Zeilenvektoren $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$.

D2) $\det$ ist *alternierend*, d.h. hat A zwei gleiche Zeilen, so ist

$$\det A = 0.$$

D3) $\det$ ist *normiert*, d.h.

$$\det E_n = 1.$$

Ist

$$A = (a_{ij}) \in M(n \times n, K),$$

so schreiben wir auch

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} := \det \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

□

Bevor wir uns mit der Existenz und Eindeutigkeit der Determinante befassen, leiten wir aus D1, D2, D3 weitere Rechenregeln ab.

Satz 5.2 (Rechenregeln für Determinanten). *Eine Determinante*

$$\det : M(n \times n, K) \rightarrow K$$

hat die folgenden Eigenschaften:

$$D4) \quad \forall \lambda \in K \text{ ist } \det(\lambda \cdot A) = \lambda^n \cdot \det A.$$

$$D5) \quad \text{Ist eine Zeile von } A \text{ gleich Null, so ist } \det A = 0.$$

$$D6) \quad \text{Entsteht } B \text{ aus } A \text{ durch die Vertauschung von zwei Zeilen, so ist}$$

$$\det B = -\det A.$$

D7) Ist $\lambda \in K$, und entsteht B aus A durch Addition der λ -fachen j -ten Zeile zur i -ten Zeile, $i \neq j$, so ist

$$\det B = \det A .$$

D8) Ist A eine obere Dreiecksmatrix, also A von der Form

$$A = \begin{pmatrix} \lambda_1 & \cdots & \\ & \ddots & \vdots \\ 0 & & \lambda_n \end{pmatrix},$$

so ist

$$\det A = \lambda_1 \cdot \dots \cdot \lambda_n .$$

D9) Ist $n \geq 2$ und $A \in M(n \times n, K)$ von der Gestalt

$$A = \begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix}$$

mit quadratischen A_1 und A_2 , so gilt

$$\det A = (\det A_1) \cdot (\det A_2) .$$

D10) Es gilt

$$\det A \neq 0 \Leftrightarrow \text{rang } A = n \Leftrightarrow A \text{ ist invertierbar} .$$

D11) Es gilt

$$\det(A \cdot B) = \det A \cdot \det B \quad \forall A, B \in M(n \times n, K) .$$

Insbesondere gilt

$$\det A^{-1} = (\det A)^{-1} \quad \forall A \in \text{GL}(n, K) .$$

Beweis. D4 und D5 folgen sofort aus D1b.

Zum Beweis von D6 nehmen wir an, daß die Zeilen a_i und a_j , $i < j$, vertauscht werden.

Dann gilt

$$\begin{aligned}
 \det A + \det B &= \det \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix} \\
 &\stackrel{D2}{=} \det \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \\
 &\stackrel{D1a}{=} \det \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_i + a_j \\ \vdots \end{pmatrix} \stackrel{D2}{=} 0 .
 \end{aligned}$$

Dabei sind nur die Einträge der Zeilen i und j angegeben, sonst ändert sich nichts.

D7 gilt wegen

$$\det B = \det \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \stackrel{D1}{=} \det A + \lambda \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \stackrel{D2}{=} \det A .$$

D8: Sind alle $\lambda_i \neq 0$, so ergibt sich durch wiederholte Anwendung von D7:

$$\begin{aligned}
 \det A &\stackrel{D7}{=} \det \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \stackrel{D1b}{=} \lambda_1 \cdot \dots \cdot \lambda_n \cdot \det E_n \\
 &\stackrel{D3}{=} \lambda_1 \cdot \dots \cdot \lambda_n .
 \end{aligned}$$

Gibt es ein i mit $\lambda_i = 0$, so wählen wir i maximal mit dieser Eigenschaft, d.h. es gilt

$$\lambda_i = 0 \quad \text{aber} \quad \lambda_{i+1} \cdot \dots \cdot \lambda_n \neq 0 .$$

Mit Hilfe von $\lambda_{i+1}, \dots, \lambda_n$ macht man die restlichen Einträge der i -ten Zeile auch noch zu Null. Mit D7 und D5 folgt $\det A = 0$.

D9: Durch Zeilenumformungen vom Typ III und IV an A mache man A_1 zu einer oberen Dreiecksmatrix B_1 . Dabei bleibt A_2 unverändert, aus C werde C' . Ist k die Anzahl der ausgeführten Zeilenvertauschungen, so gilt

$$\det A_1 \stackrel{D6}{=} (-1)^k \cdot \det B_1 .$$

Dann mache man A_2 durch Zeilenumformungen vom Typ III und IV an A zu einer oberen Dreiecksmatrix. Dabei bleiben B_1 und C' unverändert. Ist l die Anzahl der ausgeführten Zeilenvertauschungen, so gilt

$$\det A_2 \stackrel{D6}{=} (-1)^l \cdot \det B_2 .$$

Schreiben wir

$$B = \begin{pmatrix} B_1 & C' \\ 0 & B_2 \end{pmatrix} ,$$

so ist mit B_1 und B_2 auch B eine obere Dreiecksmatrix. Aus D8 folgt

$$\det B = (\det B_1) \cdot (\det B_2) .$$

Wegen

$$\det A = (-1)^{k+l} \cdot \det B$$

folgt die Behauptung.

D10: Durch Zeilenumformungen vom Typ III und IV bringen wir A auf Zeilenstufenform B . Dann ist B insbesondere eine obere Dreiecksmatrix, also B von der Form

$$B = \begin{pmatrix} \lambda_1 & \dots & & \\ & \ddots & & \\ 0 & & \lambda_n & \end{pmatrix} ,$$

und nach D6 und D7 ist $\det B = \pm \det A$. Weiter ist $\text{rang } A = \text{rang } B$ und wegen D8

$$0 \neq \lambda_1 \cdot \dots \cdot \lambda_n = \det B \Leftrightarrow \text{rang } B = n .$$

Der zweite Teil der Behauptung ergibt sich aus 4.33.

D11: Es gilt $\text{rang } (A \cdot B) \leq \text{rang } A$ wegen $\text{Bild}(\varphi_A \circ \varphi_B) \subset \text{Bild } \varphi_A$ sowie $\text{rang } (A \cdot B) = \dim \text{Bild}(\varphi_A \circ \varphi_B)$ und $\text{rang } A = \dim \text{Bild } \varphi_A$. Ist also $\text{rang } A < n$, so ist $\text{rang } (A \cdot B) < n$, und die Gleichung lautet $0 = 0$ wegen D9.

Andernfalls ist $A \in \text{GL}(n, K)$. Nach 4.52 gibt es Elementarmatrizen $C_1, \dots, C_s$ mit

$$A = C_1 \cdot \dots \cdot C_s .$$

Es genügt also, vergleiche 4.51, zu zeigen, daß für jede Elementarmatrix C vom Typ $S_i(\lambda)$ oder Q_i^j gilt

$$\det(C \cdot B) = \det C \cdot \det B .$$

Nach Regel D8, die analog auch für untere Dreiecksmatrizen gilt, ist

$$\det S_i(\lambda) = \lambda \quad \text{und} \quad \det Q_i^j = 1 .$$

Multiplizieren von links mit $S_i(\lambda)$ multipliziert die i -te Zeile von B mit λ , also ist

$$\det(S_i(\lambda) \cdot B) \stackrel{D1}{=} \lambda \cdot \det B .$$

Multiplizieren von links mit Q_i^j bewirkt die Addition der j -ten zur i -ten Zeile, also ist

$$\det(Q_i^j \cdot B) \stackrel{D1}{=} 1 \cdot \det B .$$

□

Hiermit hat man eine erste Möglichkeit zur Berechnung von Determinanten: Man bringt A durch Zeilenumformungen vom Typ III und IV auf obere Dreiecksgestalt

$$B = \begin{pmatrix} \lambda_1 & \dots & 0 \\ & \ddots & \vdots \\ 0 & & \lambda_n \end{pmatrix} .$$

Ist k die Anzahl der dabei durchgeführten Zeilenvertauschungen, so gilt

$$\det A = (-1)^k \cdot \det B = (-1)^k \lambda_1 \cdot \dots \cdot \lambda_n .$$

Beispiel 5.3.

$$\begin{vmatrix} 0 & 1 & 2 \\ 3 & 2 & 1 \\ 1 & 1 & 0 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 0 \\ 3 & 2 & 1 \\ 0 & 1 & 2 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 2 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 3 \end{vmatrix} = 3$$

□

Um ein weiteres Verfahren zur Determinantenberechnung vorstellen zu können, benötigen wir ein paar technische Vorbereitungen.

Definition 5.4. Sei $A = (a_{ij}) \in M(n \times n, K)$ eine quadratische Matrix.

- (i) Für feste i, j sei A_{ij} die Matrix, die aus A entsteht, indem man a_{ij} durch 1 und alle anderen Komponenten in der i -ten Zeile oder j -ten Spalte durch 0 ersetzt:

$$A_{ij} := \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{pmatrix}$$

Wir setzen

$$a_{ij}^\sharp := \det A_{ji} ,$$

und nennen

$$A^\sharp = (a_{ij}^\sharp) \in M(n \times n, K)$$

die zu A komplementäre Matrix.

(ii) Wir bezeichnen mit

$$A'_{ij} := \begin{pmatrix} a_{11} & \dots & a_{i,j} & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \dots & a_{i,j} & \dots & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{n,j} & \dots & a_{n,n} \end{pmatrix} \in M((n-1) \times (n-1), K)$$

die Matrix, die man aus A durch *Streichen* der i -ten Zeile und der j -ten Spalte erhält.

□

Lemma 5.5. Für $A \in M(n \times n, K)$ gilt:

$$(i) \det A_{ij} = (-1)^{i+j} \det A'_{ij}.$$

$$(ii) \det A_{ij} = \det(a^1, \dots, a^{j-1}, e^i, a^{j+1}, \dots, a^n).$$

Dabei bezeichnen $a^1, \dots, a^n$ die Spaltenvektoren von A und

$$e^i = {}^t e_i = {}^t(0, \dots, 0, 1, 0, \dots, 0).$$

Beweis. (i) Durch $i-1$ Vertauschungen benachbarter Zeilen und $j-1$ Vertauschungen benachbarter Spalten kann man A_{ij} auf die Form

$$\begin{pmatrix} 1 & 0 \\ 0 & A'_{ij} \end{pmatrix}$$

bringen. Also folgt die Behauptung aus D6 und D9, die auch für Spalten gelten, wegen

$$(-1)^{(i-1)+(j-1)} = (-1)^{i+j}.$$

(ii) Durch Addition von Vielfachen der j -ten Spalte zu den anderen Spalten kann man

$$(a^1, \dots, a^{j-1}, e^i, a^{j+1}, \dots, a^n)$$

in A_{ij} überführen. Also folgt die Behauptung aus der Eigenschaft D7, die für Spalten gilt. □

Satz 5.6. Ist $A \in M(n \times n, K)$ und $A^\sharp$ die zu A komplementäre Matrix, so ist

$$A^\sharp \cdot A = A \cdot A^\sharp = (\det A) \cdot E_n.$$

Beweis. Wir berechnen die Komponenten c_{ik} von $A^\# \cdot A$:

$$\begin{aligned}
 c_{ik} &= \sum_{j=1}^n a_{ij}^\# a_{jk} = \sum_{j=1}^n a_{jk} \det A_{ji} \\
 &\stackrel{5.5,(ii)}{=} \sum_{j=1}^n a_{jk} \det(a^1, \dots, a^{i-1}, e^j, a^{i+1}, \dots, a^n) \\
 &\stackrel{D1}{=} \det(a^1, \dots, a^{i-1}, \sum_{j=1}^n a_{jk} e^j, a^{i+1}, \dots, a^n) \\
 &= \det(a^1, \dots, a^{i-1}, a^k, a^{i+1}, \dots, a^n) \\
 &\stackrel{D2}{=} \delta_{ik} \cdot \det A.
 \end{aligned}$$

Also ist $A^\# \cdot A = (\det A) \cdot E_n$. Analog berechnet man $A \cdot A^\#$. □

Satz 5.7 (Entwicklungssatz von Laplace). Ist $A \in M(n \times n, K)$, $n \geq 2$, so gilt $\forall i \in \{1, \dots, n\}$

$$\det A = \sum_{j=1}^n (-1)^{i+j} \cdot a_{ij} \cdot \det A'_{ij}$$

(Entwicklung nach der i -ten Zeile) und für $\forall j \in \{1, \dots, n\}$

$$\det A = \sum_{i=1}^n (-1)^{i+j} \cdot a_{ij} \cdot \det A'_{ij}$$

(Entwicklung nach der j -ten Spalte). Dabei bezeichnet A'_{ij} jeweils die in 5.4,(ii) definierte Streichungsmatrix.

Beweis. Nach 5.6 ist $\det A$ für jedes i gleich der i -ten Komponente in der Diagonale der Matrix $A \cdot A^\#$, also

$$\det A = \sum_{j=1}^n a_{ij} a_{ji}^\# = \sum_{j=1}^n a_{ij} \cdot \det A_{ij} \stackrel{5.5,(i)}{=} \sum_{j=1}^n (-1)^{i+j} a_{ij} \cdot \det A'_{ij}.$$

Indem man ebenso mit $A^\# \cdot A$ verfährt, erhält man die Formel für die Entwicklung nach der j -ten Spalte. □

Bemerkung 5.8. Die durch den Faktor $(-1)^{i+j}$ bewirkte Vorzeichenverteilung kann man sich als "Schachbrettmuster" vorstellen:

+	-	+	-
-	+	-	+
+	-	+	-
-	+	-	+

□

Beispiel 5.9. (i) Ist

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2 \times 2, K),$$

so ergibt die Entwicklung nach der 1. Zeile:

$$\det A = ad - bc.$$

(ii) Ist

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in M(3 \times 3, K),$$

so ergibt die Entwicklung nach der 1. Zeile:

$$\begin{aligned} \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} &= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} \\ &= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}. \end{aligned}$$

Dies kann man sich leicht merken durch die *Regel von Sarrus*. Man schreibt den ersten und zweiten Spaltenvektor noch einmal hinter die Matrix:

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

(iii) Zur Berechnung von

$$\begin{vmatrix} 1 & 2 & 5 & -1 \\ 3 & 1 & -2 & -2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 3 \end{vmatrix}$$

bietet sich die Entwicklung nach der 3-ten Zeile an.

$$\begin{aligned} \begin{vmatrix} 1 & 2 & 5 & -1 \\ 3 & 1 & -2 & -2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 3 \end{vmatrix} &= 1 \cdot \begin{vmatrix} 2 & 5 & -1 \\ 1 & -2 & -2 \\ 1 & 2 & 3 \end{vmatrix} - 1 \cdot \begin{vmatrix} 1 & 2 & 5 \\ 3 & 1 & -2 \\ 0 & 1 & 2 \end{vmatrix} \\ &= -33 - 7 = -40. \end{aligned}$$

□

Eine weitere Folgerung aus 5.6 ist:

Satz 5.10. Sei $A \in \text{GL}(n, K)$. Definiert man $C = (c_{ij}) \in M(n \times n, K)$ durch $(c_{ij}) := (-1)^{i+j} \det A'_{ij}$, so gilt

$$A^{-1} = \frac{1}{\det A} \cdot {}^t C.$$

Beweis. 5.6 und 5.5.(i). □

Beispiel 5.11. Ist $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, K)$, so gilt

$$A^{-1} = \frac{1}{ad - bc} \cdot {}^t \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

□

Für die praktische Berechnung bei größeren n ist dieses Verfahren zur Inversenrechnung wenig geeignet.

Nachdem wir nun wissen, wie man Determinanten ausrechnet, wollen wir zeigen, daß es sie auch tatsächlich gibt. Was ist dabei das Problem? Man könnte ja einfach sagen, man bringe eine gegebene Matrix A auf eine obere Dreiecksgestalt

$$B = \begin{pmatrix} \lambda_1 & \dots & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

und definiere

$$\det A := (-1)^k \det B := (-1)^k \lambda_1 \cdot \dots \cdot \lambda_n,$$

wobei k die Anzahl der durchgeführten Zeilenvertauschungen ist. Das Problem ist, daß diese Zeilenvertauschungen nicht eindeutig bestimmt sind, man hat Wahlmöglichkeiten. Aber das Ergebnis

$$(-1)^k \lambda_1 \cdot \dots \cdot \lambda_n$$

muß unabhängig von allen Auswahlen sein, insbesondere muß klar sein, ob die Zahl k für ein gegebenes A immer gerade oder immer ungerade ist.

Daß wir Zeilenvertauschungen vornehmen, bedeutet letztendlich, daß wir eine Permutation der Menge der Zeilenindizes $\{1, \dots, n\}$ vornehmen. Eine Transposition der Zeilenindizes entspricht dabei genau einer Zeilenvertauschung. Betrachten wir ein Beispiel: Ist $\sigma \in S_n$ eine Permutation, und sind $e_1, \dots, e_n$ die kanonischen Basisvektoren des K^n , so geht die Matrix

$$E_\sigma := \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$$

aus der Einheitsmatrix durch Zeilenvertauschungen hervor. In diesem Fall ist also die Frage: Ist $\det E_\sigma = +1$ oder ist $\det E_\sigma = -1$? Diese spezielle Frage, aber auch die Frage nach der Existenz von Determinanten läßt sich durch ein genaueres Studium von Permutationen lösen. Wir fassen zunächst zusammen was wir schon wissen:

Wiederholung 5.12. Sei $n \in \mathbb{N}$, $n \geq 1$.

- (i) Die Menge S_n der Permutationen von $\{1, \dots, n\}$, d.h. der bijektiven Abbildungen

$$\sigma: \{1, \dots, n\} \longrightarrow \{1, \dots, n\},$$

bildet bzgl. der Hintereinanderausführung $\circ$ eine Gruppe nach 2.5,(i),(ii). S_n hat $n!$ Elemente (Aufgabe 9,(i)). Für $\sigma \in S_n$ schreiben wir auch

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

- (ii) $\tau \in S_n$ heißt Transposition, wenn $\exists k, l \in \{1, \dots, n\}$, $k \neq l$, mit

$$\tau(i) = \begin{cases} l & i = k \\ k & i = l \\ i & \text{sonst} \end{cases}, \quad 1 \leq i \leq n.$$

Jedes $\sigma \in S_n$, $n \geq 2$, läßt sich als Produkt von endlich vielen Transpositionen schreiben (Aufgabe 9,(ii)):

$$\sigma = \tau_1 \circ \dots \circ \tau_k.$$

□

Die Zerlegung einer Permutation in Transpositionen ist keineswegs eindeutig. Um unser Vorzeichenproblem in den Griff zu bekommen, müssen wir beweisen, daß für gegebenes σ die Anzahl der benötigten Transpositionen immer gerade oder immer ungerade ist. Zu diesem Zweck ordnen wir jeder Permutation ein Vorzeichen zu.

Definition 5.13. Seien $n \in \mathbb{N}$, $n > 1$ und $\sigma \in S_n$. Dann heißt jedes Paar $i, j \in \{1, \dots, n\}$ mit

$$i < j \quad \text{aber} \quad \sigma(i) > \sigma(j)$$

ein *Fehlstand* von σ . Wir definieren das *Signum* von σ durch

$$\text{sign } \sigma := \begin{cases} +1 & \text{falls } \sigma \text{ eine gerade Anzahl von Fehlständen hat,} \\ -1 & \text{falls } \sigma \text{ eine ungerade Anzahl von Fehlständen hat.} \end{cases}$$

Weiter nennen wir σ

gerade, falls $\text{sign } \sigma = +1$,
bzw. *ungerade*, falls $\text{sign } \sigma = -1$.

□

Beispiel 5.14. $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ hat genau 2 Fehlstände, nämlich

$1 < 3$ aber $\sigma(1) = 2 > 1 = \sigma(3)$,
und $2 < 3$ aber $\sigma(2) = 3 > 2 = \sigma(3)$.

Es folgt

$$\text{sign } \sigma = +1$$

□

Satz 5.15 (Eigenschaften des Signums). Sei $n \in \mathbb{N}$, $n \geq 1$.

Dann gilt:

(i) $\forall \sigma \in S_n$ ist

$$\text{sign } \sigma = \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

(ii) $\forall \sigma', \sigma \in S_n$ gilt

$$\text{sign}(\sigma' \circ \sigma) = (\text{sign } \sigma') \cdot (\text{sign } \sigma).$$

Insbesondere gilt $\forall \sigma \in S_n$

$$\text{sign } \sigma^{-1} = \text{sign } \sigma.$$

(iii) Ist $n \geq 2$ und $\tau \in S_n$ eine Transposition, so gilt

$$\text{sign } \tau = -1.$$

(iv) Ist $n \geq 2$ und $\sigma = \tau_1 \circ \dots \circ \tau_k \in S_n$ mit Transpositionen $\tau_1, \dots, \tau_k$, so gilt

$$\text{sign } \sigma = (-1)^k.$$

(v) $\forall \sigma \in S_n$ ist

$$\det \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix} = \text{sign } \sigma.$$

Beweis. (i) Sei m die Anzahl der Fehlstände von σ . Dann gilt

$$\begin{aligned} \prod_{i < j} (\sigma(j) - \sigma(i)) &= \left(\prod_{\substack{i < j \\ \sigma(i) < \sigma(j)}} (\sigma(j) - \sigma(i)) \right) \cdot (-1)^m \prod_{\substack{i < j \\ \sigma(i) > \sigma(j)}} |\sigma(j) - \sigma(i)| \\ &= (-1)^m \prod_{i < j} |\sigma(j) - \sigma(i)| = (-1)^m \prod_{i < j} (j - i), \end{aligned}$$

da die letzten beiden Produkte die gleichen Faktoren bis auf Reihenfolge haben.

(ii) Es gilt

$$\begin{aligned} \text{sign}(\sigma' \circ \sigma) &= \prod_{i < j} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{j - i} \\ &= \prod_{i < j} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}. \end{aligned}$$

Da das zweite Produkt gleich $\text{sign } \sigma$ ist, genügt es zu zeigen, daß das erste Produkt gleich $\text{sign } \sigma'$ ist. Dies ergibt sich wie folgt:

$$\begin{aligned}
 & \prod_{i < j} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} \\
 &= \prod_{\substack{i < j \\ \sigma(i) < \sigma(j)}} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \prod_{\substack{i < j \\ \sigma(i) > \sigma(j)}} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} \\
 &= \prod_{\substack{i < j \\ \sigma(i) < \sigma(j)}} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \prod_{\substack{i > j \\ \sigma(i) < \sigma(j)}} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} \\
 &= \prod_{\sigma(i) < \sigma(j)} \frac{\sigma'(\sigma(j)) - \sigma'(\sigma(i))}{\sigma(j) - \sigma(i)} = \prod_{i < j} \frac{\sigma'(j) - \sigma'(i)}{j - i} \\
 &= \text{sign } \sigma'.
 \end{aligned}$$

Dabei schließt man beim vorletzten Gleichheitszeichen wie in (i).

(iii) Sei

$$\tau_0 := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$$

die Transposition, die 1 und 2 vertauscht. Wir zeigen:

(*) Ist $\tau \in S_n$ eine beliebige Transposition, so $\exists \sigma \in S_n$ mit

$$\tau = \sigma \circ \tau_0 \circ \sigma^{-1}.$$

Daraus folgt (iii): Es gilt $\text{sign } \tau_0 = -1$, denn τ_0 hat genau einen Fehlstand. Zu dem gegebenen τ wählen wir ein σ wie in (*). Mit (ii) folgt

$$\begin{aligned}
 \text{sign } \tau &= \text{sign } \sigma \cdot \text{sign } \tau_0 \cdot (\text{sign } \sigma)^{-1} = \\
 &= \text{sign } \tau_0 = -1.
 \end{aligned}$$

Nun zeigen wir (*): Seien k und l die von τ vertauschten Elemente. Wir behaupten, daß jedes $\sigma \in S_n$ mit

$$\sigma(1) = k \quad \text{und} \quad \sigma(2) = l$$

die verlangte Eigenschaft hat. Sei $\tau' := \sigma \circ \tau_0 \circ \sigma^{-1}$. Wegen $\sigma^{-1}(k) = 1$ und $\sigma^{-1}(l) = 2$ ist

$$\tau'(k) = \sigma(\tau_0(1)) = \sigma(2) = l$$

und

$$\tau'(l) = \sigma(\tau_0(2)) = \sigma(1) = k.$$

Für $i \notin \{k, l\}$ ist $\sigma^{-1}(i) \notin \{1, 2\}$, also gilt

$$\tau'(i) = \sigma(\tau_0(\sigma^{-1}(i))) = \sigma(\sigma^{-1}(i)) = i.$$

Daraus folgt $\tau' = \tau$.

(iv) ergibt sich aus (ii) und (iii).

(v) folgt aus (iv), denn man kann E_n durch k Zeilenvertauschungen in

$$\begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$$

überführen.

□

Bemerkung und Definition 5.16. Die Eigenschaft 5.15,(ii) besagt, daß die Abbildung

$$\text{sign} : S_n \rightarrow \{+1, -1\}$$

ein Gruppenepimorphismus auf die multiplikative Gruppe mit 2 Elementen ist. Insbesondere ist der Kern

$$A_n := \{\sigma \in S_n \mid \text{sign } \sigma = +1\} \subset S_n$$

ein Normalteiler in S_n . A_n heißt die *alternierende Gruppe*.

□

Für jedes $\sigma \in S_n$ können wir die Nebenklasse

$$A_n \sigma = \{\sigma' \circ \sigma \mid \sigma' \in A_n\}$$

betrachten.

Satz 5.17. Ist $\sigma \in S_n$ mit $\text{sign } \sigma = -1$, so gilt

$$S_n = A_n \cup A_n \sigma \quad \text{und} \quad A_n \cap A_n \sigma = \emptyset .$$

Insbesondere hat A_n genau $\frac{1}{2}n!$ Elemente.

Beweis. Sei $\sigma' \in S_n$ mit $\text{sign } \sigma' = -1$. Nach 5.15,(ii) gilt

$$\text{sign}(\sigma' \circ \sigma^{-1}) = +1 ,$$

also ist $\sigma' \in A_n \sigma$, denn

$$\sigma' = (\sigma' \circ \sigma^{-1}) \circ \sigma .$$

Für jedes $\sigma' \in A_n \sigma$ ist $\text{sign } \sigma' = -1$, also ist die Vereinigung auch disjunkt. Aus 2.13 ergibt sich, daß die Einschränkung der Linksstranslation auf A_n ,

$$A_n \rightarrow A_n \sigma, \quad \sigma' \rightarrow \sigma \circ \sigma' ,$$

bijektiv ist. Da S_n aus $n!$ Elementen besteht, enthalten A_n und $A_n \sigma$ je $\frac{1}{2}n!$ Elemente.

□

Nach diesen Vorbereitungen können wir nun zeigen:

Satz 5.18. Ist K ein Körper und $n \geq 1$, so gibt es genau eine Determinante

$$\det : M(n \times n, K) \rightarrow K ,$$

und zwar ist für $A = (a_{ij}) \in M(n \times n, K)$

$$(*) \quad \det A = \sum_{\sigma \in S_n} \text{sign } \sigma \cdot a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)} .$$

Beweis. Eindeutigkeit. Wir zeigen, daß sich die Formel (*) aus D1, D2, D3 und den Folgerungen daraus herleiten läßt. Seien

$$\det : M(n \times n, K) \rightarrow K$$

eine Determinante und $A \in M(n \times n, K)$. Wir bezeichnen mit a_i wieder die Zeilen von A und mit e_i die kanonischen Basisvektoren des K^n . Aus D1 ergibt sich die folgende Rechnung, die der sukzessiven Entwicklung nach Zeilen entspricht:

$$\begin{aligned} \det A &= \det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{j_1=1}^n a_{1j_1} \det \begin{pmatrix} e_{j_1} \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \\ &= \sum_{j_1=1}^n a_{1j_1} \sum_{j_2=1}^n a_{2j_2} \det \begin{pmatrix} e_{j_1} \\ e_{j_2} \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \dots = \\ &= \sum_{j_1=1}^n \sum_{j_2=1}^n \dots \sum_{j_n=1}^n a_{1j_1} \cdot a_{2j_2} \cdot \dots \cdot a_{nj_n} \cdot \det \begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_n} \end{pmatrix} . \end{aligned}$$

Wegen D2 und 5.15,(iv) gilt

$$\det \begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_n} \end{pmatrix} = \begin{cases} \text{sign } \sigma & \text{falls } \exists \sigma \in S_n \text{ mit } \sigma(v) = j_v \quad \forall v, \\ 0 & \text{sonst .} \end{cases}$$

Also bleiben nur $n!$ der n^n Summanden übrig und es gilt (*).

Existenz. Wir definieren nun

$$\det : M(n \times n, K) \rightarrow K$$

durch die Formel (*) für jedes $A \in M(n \times n, K)$, und müssen zeigen, daß D1, D2 und D3 gelten.

D1: Es gilt

$$\begin{aligned}
 \det \begin{pmatrix} \vdots \\ a'_i + a''_i \\ \vdots \end{pmatrix} &= \sum_{\sigma \in S_n} \text{sign } \sigma \cdot a_{1\sigma(1)} \cdots (a'_{i\sigma(i)} + a''_{i\sigma(i)}) \cdots a_{n\sigma(n)} \\
 &= \sum_{\sigma \in S_n} \text{sign } \sigma \cdot a_{1\sigma(1)} \cdots a'_{i\sigma(i)} \cdots a_{n\sigma(n)} \\
 &\quad + \sum_{\sigma \in S_n} \text{sign } \sigma \cdot a_{1\sigma(1)} \cdots a''_{i\sigma(i)} \cdots a_{n\sigma(n)} \\
 &= \det \begin{pmatrix} \vdots \\ a'_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a''_i \\ \vdots \end{pmatrix},
 \end{aligned}$$

und somit gilt D1,(i). Analog ergibt sich D1,(ii).

D2: Seien etwa die k -te und l -te Zeile von A gleich, $k < l$, und $\tau \in S_n$ die Transposition, die k und l vertauscht. Es gilt $\text{sign } \tau = -1$ nach 5.15,(iii), also erhält man aus 5.17 die disjunkte Vereinigung

$$S_n = A_n \cup A_n \tau.$$

Wenn σ die Gruppe A_n durchläuft, so durchläuft $\sigma \circ \tau$ die Menge $A_n \tau$. Es folgt

$$(**) \quad \det A = \sum_{\sigma \in A_n} a_{1\sigma(1)} \cdots a_{n\sigma(n)} - \sum_{\sigma \in A_n} a_{1\sigma(\tau(1))} \cdots a_{n\sigma(\tau(n))}.$$

Da die k -te und die l -te Zeile von A gleich sind, gilt nach Definition von τ

$$\begin{aligned}
 &a_{1\sigma(\tau(1))} \cdots a_{k\sigma(\tau(k))} \cdots a_{l\sigma(\tau(l))} \cdots a_{n\sigma(\tau(n))} \\
 &= a_{1\sigma(1)} \cdots a_{k\sigma(l)} \cdots a_{l\sigma(k)} \cdots a_{n\sigma(n)} \\
 &= a_{1\sigma(1)} \cdots a_{k\sigma(k)} \cdots a_{l\sigma(l)} \cdots a_{n\sigma(n)} \\
 &= a_{1\sigma(1)} \cdots a_{n\sigma(n)}.
 \end{aligned}$$

Also heben sich die Summanden in (**) gegenseitig auf, es folgt

$$\det A = 0.$$

D3: Ist δ_{ij} das Kronecker-Symbol und $\sigma \in S_n$, so ist

$$\delta_{1\sigma(1)} \cdots \delta_{n\sigma(n)} = \begin{cases} 0 & \text{für } \sigma \neq \text{id} \\ 1 & \text{für } \sigma = \text{id} \end{cases}.$$

Also gilt

$$\begin{aligned}
 \det E_n &= \det(\delta_{ij}) = \sum_{\sigma \in S_n} \text{sign } \sigma \cdot \delta_{1\sigma(1)} \cdots \delta_{n\sigma(n)} \\
 &= \text{sign}(\text{id}) = 1.
 \end{aligned}$$

□

Unmittelbar aus der Formel (*) ergibt sich eine weitere Eigenschaft von Determinanten:

Satz 5.19. $\forall A \in M(n \times n, K)$ gilt $\det {}^t A = \det A$.

Beweis. Ist $A = (a_{ij})$, so ist ${}^t A = (a'_{ij})$ mit $a'_{ij} = a_{ji}$. Also gilt

$$\begin{aligned} \det {}^t A &= \sum_{\sigma \in S_n} \text{sign } \sigma \cdot a'_{1\sigma(1)} \cdot \dots \cdot a'_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} \text{sign } \sigma \cdot a_{\sigma(1)1} \cdot \dots \cdot a_{\sigma(n)n} \\ &= \sum_{\sigma \in S_n} \text{sign } (\sigma^{-1}) \cdot a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)} \\ &= \det A. \end{aligned}$$

Bei der vorletzten Gleichung wurde benutzt, daß $\forall \sigma \in S_n$

$$a_{\sigma(1)1} \cdot \dots \cdot a_{\sigma(n)n} = a_{1\sigma^{-1}(1)} \cdot \dots \cdot a_{n\sigma^{-1}(n)}$$

gilt, denn bis auf die Reihenfolge enthalten beide Produkte die gleichen Faktoren. Außerdem wurde verwendet, daß

$$\text{sign } \sigma = \text{sign } \sigma^{-1}$$

ist wegen 5.15.(ii). Für die letzte Gleichung haben wir benutzt, daß mit σ auch σ^{-1} ganz S_n durchläuft. $\square$

5.19 unterstreicht noch einmal, daß es egal ist, ob wir $D1, \dots, D11$ oder andere Determinanten-Rechenregeln für Zeilen oder für Spalten formulieren. Wie nützlich es ist, wenn man abwechselnd mit Zeilen und Spalten operieren kann, zeigt das

Beispiel 5.20. Wir betrachten $X_1, \dots, X_n$ als Unbestimmte und definieren die *Vandermonde-Determinante* als

$$\Delta := \det \begin{pmatrix} 1 & X_1 & \dots & X_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & X_n & \dots & X_n^{n-1} \end{pmatrix}.$$

Offensichtlich ist $\Delta_1 = 1$, $\Delta_2 = X_2 - X_1$. Für $n = 3$ formt man zuerst Spalten um und zieht dann Faktoren aus den Zeilen:

$$\begin{aligned} \begin{vmatrix} 1 & X_1 & X_1^2 \\ 1 & X_2 & X_2^2 \\ 1 & X_3 & X_3^2 \end{vmatrix} &= \begin{vmatrix} 1 & X_1 & X_1^2 - X_1^2 \\ 1 & X_2 & X_2^2 - X_1 X_2 \\ 1 & X_3 & X_3^2 - X_1 X_3 \end{vmatrix} = \begin{vmatrix} 1 & X_1 - X_1 & 0 \\ 1 & X_2 - X_1 & X_2(X_2 - X_1) \\ 1 & X_3 - X_1 & X_3(X_3 - X_1) \end{vmatrix} \\ &= \begin{vmatrix} X_2 - X_1 & X_2(X_2 - X_1) \\ X_3 - X_1 & X_3(X_3 - X_1) \end{vmatrix} = (X_2 - X_1)(X_3 - X_1) \begin{vmatrix} 1 & X_2 \\ 1 & X_3 \end{vmatrix} \\ &= (X_2 - X_1)(X_3 - X_1)(X_3 - X_2). \end{aligned}$$

Induktiv ergibt sich mit demselben Prinzip

$$\Delta_n = \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

$\square$

Eine weitere Anwendung von Determinanten ergibt sich für die Lösung linearer Gleichungssysteme, und zwar im Fall

$$A \cdot x = b \quad \text{mit} \quad A \in \text{GL}(n, K) .$$

Dann gibt es genau eine Lösung nach 4.60,(ii), und zwar

$$x = A^{-1}b .$$

Mit Hilfe der komplementären Matrix kann man dies auch so formulieren:

Cramer'sche Regel 5.21. Seien $A \in \text{GL}(n, K)$, $b \in K^n$ und $x = {}^t(x_1, \dots, x_n) \in K^n$ die eindeutig bestimmte Lösung des Gleichungssystems

$$A \cdot x = b .$$

Bezeichnen $a^1, \dots, a^n$ die Spaltenvektoren von A , so gilt $\forall i \in \{1, \dots, n\}$:

$$x_i = \frac{\det(a^1, \dots, a^{i-1}, b, a^{i+1}, \dots, a^n)}{\det A} .$$

Beweis. Sind $a_1, \dots, a_n$ die Spaltenvektoren von A , so hat A^{-1} nach 5.10 in der i -ten Zeile und der j -ten Spalte die Komponente

$$\frac{\det A_{ji}}{\det A} = \frac{\det(a^1, \dots, a^{i-1}, e^j, a^{i+1}, \dots, a^n)}{\det A} .$$

Für die i -te Komponente von $x = A^{-1}b$ folgt nach D1 und 5.19

$$x_i = \sum_{j=1}^n b_j \frac{\det A_{ji}}{\det A} = \frac{\det(a^1, \dots, a^{i-1}, b, a^{i+1}, \dots, a^n)}{\det A} .$$

□

Beispiel 5.22. Seien

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 3 & 2 & 1 \end{pmatrix} \in M(3 \times 3, \mathbb{R}) \quad \text{und} \quad b = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3 .$$

Dann gilt etwa mit der Regel von Sarrus

$$\det A = 1 + 3 - 2 = 2$$

sowie

$$x_1 = \frac{1}{2} \begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 2 & 1 \end{vmatrix} = -1, \quad x_2 = \frac{1}{2} \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 3 & 0 & 1 \end{vmatrix} = 2, \quad x_3 = \frac{1}{2} \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 3 & 2 & 0 \end{vmatrix} = -1$$

□

Auch die Cramer'sche Regel ist für praktische Berechnungen wegen der vielen zu bestimmenden Determinanten nicht geeignet.

Zum Schluß beschäftigen wir uns noch mit der folgenden Frage: Nach D10 ist $\text{rang} A < n$ für $A \in M(n \times n, K)$ gleichbedeutend mit $\det A = 0$. Wie weit sinkt der Rang tatsächlich ab? Zur Beantwortung dieser Frage, muß man weitere Determinanten berechnen. Dies kann man sogar auf beliebige Matrizen ausdehnen.

Definition 5.23. Seien $A \in M(m \times n, K)$ und $k \leq \min\{m, n\}$. Dann heißt eine quadratische Matrix $A' \in M(k \times k, K)$ eine *k-reihige Teilmatrix* von A , wenn A durch Zeilen- und Spaltenvertauschungen auf die Form

$$\begin{pmatrix} A' & * \\ * & * \end{pmatrix}$$

gebracht werden kann. Man kann auch sagen, daß A' aus A durch Streichen von $m - k$ Zeilen und $n - k$ Spalten entstanden ist. Die Determinante $\det A'$ heißt dann auch ein *k-reihiger Minor* von A . $\square$

Satz 5.24. Für $A \in M(m \times n, K)$ und $r \in \mathbb{N}$ sind äquivalent:

- (i) $r = \text{rang} A$
- (ii) Es gibt einen r -reihigen Minor $\neq 0$, und für $k > r$ ist jeder k -reihige Minor gleich Null.

Beweis. Es genügt zu zeigen, daß $\forall k \in \mathbb{N}$ folgende Bedingungen äquivalent sind:

- a) $\text{rang} A \leq k$.
- b) Es gibt eine k -reihige Teilmatrix A' von A mit $\det A' \neq 0$.

'b) $\Rightarrow$ a)' $\det A' \neq 0 \Rightarrow \text{rang} A \geq \text{rang} A' = k$, weil sich der Rang einer Matrix bei Zeilen- und Spaltenvertauschungen nicht ändert.

'a) $\Rightarrow$ b)' $\text{rang} A \geq k \Rightarrow \exists k$ linear unabhängige Zeilenvektoren von A . Nach Zeilenvertauschungen können wir sie in die ersten k Zeilen bringen. Sei B die Matrix, die aus diesen Zeilen besteht. Wegen

$$k = \text{Zeilenrang } B = \text{Spaltenrang } B$$

gibt es k linear unabhängige Spaltenvektoren in B . Durch Spaltenvertauschungen können wir sie in die ersten k Spalten von B bringen. Sei $A' \in M(k \times k, K)$ die aus diesen Spalten bestehende Matrix. A' ist eine Teilmatrix von A , und wegen $\text{rang} A' = k$ ist $\det A' \neq 0$. $\square$

Aufgabe 49. Lösen Sie das Gleichungssystem

$$\begin{array}{rrcr} x_1 & & + & 2x_3 & = & 1 \\ x_1 & + & 2x_2 & + & x_3 & = & 1 \\ x_1 & + & 2x_2 & + & 2x_3 & = & 2 \end{array}$$

über dem Körper $\mathbb{F}_3$

- (i) mittels Gaußelimination,
- (ii) mit Hilfe der Cramerschen Regel.

Aufgabe 50. Berechnen Sie folgenden Determinanten:

$$\begin{vmatrix} 1 & 3 & 2 \\ 2 & 4 & 1 \\ 3 & 1 & 2 \end{vmatrix}, \begin{vmatrix} 3 & 0 & 7 & -4 \\ 5 & -7 & 2 & 1 \\ 4 & 0 & 0 & 3 \\ -7 & 2 & 1 & 0 \end{vmatrix}$$

Maple-Aufgabe M5.

- (i) Schreiben Sie eine Prozedur, die bei Eingabe einer $n \times n$ -Matrix deren Determinante berechnet.
- (ii) Probieren Sie die Funktionen aus dem Paket `plottools` aus.