LINEARE ALGEBRA I

Ernst Bönecke

Universität Hamburg

2015

V O R W O R T

Dieser Text ist entstanden aus mehreren Vorlesungen über Lineare Algebra, insbesondere den drei Kursen aus den Jahren 2000 - 2004, und anderen Vorlesungen,die ich als Dozent an der Universität Hamburg gehalten habe. Er ist kein reines Vorlesungsskript, denn er enthält mehr als man in 14 Semesterwochen schaffen kann, insbesondere mehr Beispiele.

Der Aufbau richtet sich nicht nach didaktischen, sondern allein nach mathematischen Gesichtspunkten. So werden bereits in §2 Faktorgruppen behandelt - ein Thema, das Anfänger häufig als abstrakt empfinden. Ich hoffe aber, den Text so ausführlich aufgeschrieben zu haben, dass man danach die Lineare Algebra auch vor Beginn eines Mathematik- oder Physikstudiums lernen kann.

Kenntnisse in Analysis werden nicht vorausgesetzt, außer der Existenz von Quadratwurzeln nichtnegativer reeller Zahlen. Auch das Induktionsaxiom, das eher in die Analysis gehört, und die Konstruktion des Körpers der komplexen Zahlen werden nicht vorausgesetzt, sondern ausführlich behandelt.

Der Text knüpft an Schulkenntnisse an, z.B. wird die analytische Geometrie im $\mathbb{R}^2$ und im $\mathbb{R}^3$ in §1 wiederholt. Er richtet sich also an alle Anfänger mit Studienfach Mathematik oder Physik und eignet sich gut dafür, sich zwischen Schule und Hochschule auf das Studium vorzubereiten.

Hamburg, im November 2015

Inhaltsverzeichnis

§1 Grundbegriffe

1.1 Einiges über Aussagen und Mengen

Mengenlehre und Logik sind für uns nicht Selbstzweck, sondern man braucht sie, um mathematische Sachverhalte kurz und unmissverständlich zu formulieren. Wir werden uns auf das Notwendigste beschränken.

Definition 1.1.1 : Unter einer **Aussage** A verstehen wir ein sprachliches oder schriftliches Gebilde, das entweder **wahr** (w) ist oder **falsch** (f) . Man sagt auch, die Aussage A hat den **Wahrheitswert** w oder f .

Beispiel 1.1.2

Aussage	Wahrheitswert
Es gibt keinen Studierenden in diesem Hörsaal	f
$1 \cdot 2 = 2$	w
$1 \cdot 2 = 2$ und $3 \cdot 4 = 4$	f
$1 \cdot 2 = 2$ oder $3 \cdot 4 = 4$	w
Wenn Ptolemäus Recht hat , dann ist die Erde eine Scheibe	w

□

Wichtig ist für uns die **Verknüpfung von Aussagen** : Mathematische Sätze sind logisch verknüpfte Aussagen. Man definiert so eine Verknüpfung, indem man den Wahrheitswert der verknüpften Aussage in Abhängigkeit von den Wahrheitswerten der gegebenen Aussage festlegt:

Definition 1.1.3 : Seien A und B zwei gegebene Aussagen. Dann definieren wir die Wahrheitswerte von
a) A **und** B , in Zeichen: $A \wedge B$, durch folgende Tabelle:

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

$A \wedge B$ ist also genau dann wahr, wenn sowohl A als auch B wahr sind.

b) A **oder** B , in Zeichen: $A \vee B$, durch folgende Tabelle:

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

$A \vee B$ ist also auch dann wahr, wenn beide Aussagen wahr sind. Man sieht

hier, wie sinnvoll es ist, solche Verabredungen am Anfang zu treffen, um Missverständnisse oder sprachlich unschöne Formulierungen wie "und/oder", die man in juristischen Texten häufig findet, zu vermeiden.

c)**Aus A folgt B** , in Zeichen: $A \implies B$, man sagt auch: **A impliziert B** oder : **Wenn A gilt, dann gilt B** , durch folgenden Tabelle:

A	B	$A \implies B$
w	w	w
w	f	f
f	w	w
f	f	w

Man beachte: $A \implies B$ ist stets wahr, wenn A falsch ist. Das mag manchen erstaunen, ist aber eine sinnvolle Definition, die sich sogar mit dem umgangssprachlichen Gebrauch deckt, wie das Beispiel "Wenn Ptolemäus Recht hat, dann ist die Erde eine Scheibe" zeigt, das wahr ist , obwohl beide Teilaussagen falsch sind.

d) **A gleichbedeutend mit B** , in Zeichen : $A \iff B$, man sagt auch: **A gilt genau dann, wenn B gilt** , durch folgende Tabelle:

A	B	$A \iff B$
w	w	w
w	f	f
f	w	f
f	f	w

e) **nicht A** , in Zeichen : $\neg A$, auch non A , durch die Tabelle

A	$\neg A$
w	f
f	w

Solche Tabellen mit Wahrheitswerten wie diese fünf hier nennt man auch **Wahrheitstafeln**. □

Wahrheitstafeln verwendet man auch, um die Wahrheitswerte von weiteren verknüpften Aussagen wie

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

auszurechnen. Dabei muss man sämtliche möglichen Wahrheitswerte von A, B und C berücksichtigen, z.B. für $(\neg A) \vee B$:

A	B	$\neg A$	$(\neg A) \vee B$
w	w	f	w
w	f	f	f
f	w	w	w
f	f	w	w

Wir sehen an diesem Beispiel, dass $(\neg A) \vee B$ dieselbe Wahrheitstafel hat wie $A \implies B$. Man wird die Aussagen "$A \implies B$ " und "$(\neg A) \vee B$" deshalb "logisch gleichwertig" nennen:

Definition 1.1.4 : Gegeben seien mehrere Aussagen $A, B, C, \ldots$ und zwei Aussagen X und Y , die beide durch Verknüpfung dieser Aussagen $A, B, C, \ldots$ entstanden sind. Wenn die Aussage

$$X \iff Y$$

für alle möglichen Wahrheitswerte der Aussagen $A, B, C, \ldots$ den Wahrheitswert w annimmt, so sagt man: X und Y sind **(logisch) gleichwertig** . Die Aussage "$X \iff Y$ " bezeichnet man dann als eine **Tautologie** .

Satz 1.1.5 : Wenn A, B, C Aussagen sind, dann gelten folgende Tautologien:

a) $\neg(\neg A) \iff A$
b) $A \wedge B \iff B \wedge A$
c) $(A \wedge B) \wedge C \iff A \wedge (B \wedge C)$
d) $A \vee B \iff B \vee A$
e) $(A \vee B) \vee C \iff A \vee (B \vee C)$
f) $A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$
g) $A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$
h) $\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$
i) $\neg(A \vee B) \iff (\neg A) \wedge (\neg B)$
j) $(A \implies B) \iff ((\neg B) \implies (\neg A))$

Man **beweist** diesen Satz durch Wahrheitstafeln, z.B. für h) :

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$(\neg A) \vee (\neg B)$	h)
w	w	w	f	f	f	f	w
w	f	f	w	f	w	w	w
f	w	f	w	w	f	w	w
f	f	f	w	w	w	w	w

□

Zur Schreibweise : Bei den Formeln in Satz 1.1.5 haben wir Klammern weggelassen: Statt d) hätten wir genauer

$$(A \vee B) \iff (B \vee A)$$

schreiben müssen. Man kann die Klammern weglassen, wenn man vereinbart: Die Verknüpfungen sind in der Reihenfolge

erst $\neg$, dann $\wedge$, dann $\vee$, dann $\Longrightarrow$ und dann $\Longleftrightarrow$

auszuführen, soweit Klammern nichts Anderes festlegen.

Neben Aussagen hat man es in der Mathematik zu tun mit Zahlen oder Buchstaben, die man zusammenfassen möchte zu einer Menge. Es bereitet nun erhebliche Schwierigkeiten, exakt zu definieren, was eine Menge ist. Da wir uns hier nicht mit Grundlagen der Mathematik beschäftigen wollen, reicht für uns die folgende

Definition 1.1.6 : Unter einer **Menge** M verstehen wir eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche die **Elemente** der Menge M genannt werden, zu einem Ganzen. Ist x ein Element von M , so schreiben wir

$$x \in M \quad ;$$

ist diese Aussage falsch, so schreiben wir

$$x \notin M \quad .$$

Definition 1.1.7 (Schreibweise von Mengen) : Man kann eine Menge auf zwei Arten angeben: Entweder, man schreibt in geschweiften Klammern alle Elemente der Menge hin, etwa

$$\{1, 2, 5, x\} \quad ,$$

das soll bedeuten, dass die Menge aus den Elementen $1, 2, 5$ und x besteht, oder man schreibt in den geschweiften Klammern ein Symbol für die Elemente, einen senkrechten Strich und dann die Eigenschaft, die die Elemente haben sollen. Z.B. ist

$$\{\ x\ \mid\ x \,\text{ist ganze Zahl und}\, 2 \,\text{teilt}\, x\ \}$$

die Menge der geraden ganzen Zahlen.

Definition und Beispiel 1.1.8 : Mengen, die bei uns immer wieder vorkommen, sind

$$\mathbb{N}_0 \quad = \quad \{0, 1, 2, \ldots\}$$

(Pünktchen setzt man, wenn man nicht alle Elemente hinschreiben will oder kann, aber sich denken kann, wie es weitergeht), die Menge der **natürlichen Zahlen mit Null** ,

$$\mathbb{N} \quad = \quad \{1, 2, 3, \ldots\}$$

die Menge der **natürlichen Zahlen**, (es ist Definitionssache, ob man 0 zu den natürlichen Zahlen rechnet; wir wollen das hier nicht tun),

$$\mathbb{Z} \quad = \quad \{0, 1, -1, 2, -2, 3, -3, \ldots\}$$

die Menge der **ganzen Zahlen** ,

$$\mathbb{Q} \quad = \quad \left\{ \frac{r}{s} \;\middle|\; r \in \mathbb{Z} \wedge s \in \mathbb{Z} \wedge s \neq 0 \right\}$$

die Menge der **rationalen Zahlen** , schließlich die Mengen $\mathbb{R}$ der **reellen** und $\mathbb{C}$ der **komplexen Zahlen** , die in 3.5 eingeführt werden. Wir wollen noch vereinbaren, dass es eine Menge gibt, die gar kein Element enthält, die **leere Menge** $\emptyset$.

Definition 1.1.9 (Gleichheit zweier Mengen) : Zwei Mengen M und N heißen **gleich** , man schreibt $M \quad = \quad N$, wenn jedes Element von M auch Element von N , und jedes Element von N auch Element von M ist. Wir wollen diese Definition etwas formaler aufschreiben und dabei auch gleich zwei neue Symbole kennenlernen :

$$M \quad = \quad N \quad :\Longleftrightarrow \quad \forall\, x \,:\, (x \in M \quad \Longleftrightarrow \quad x \in N) \quad ,$$

das Zeichen $:\Longleftrightarrow$ bedeutet, dass die linke Aussage durch die rechte definiert wird, man liest es : "**nach Definition gleichbedeutend**". Das Zeichen $\forall$ heißt: "**für alle**" .

Definition 1.1.10 (Teilmenge): Seien M und N Mengen. Man sagt, M ist **Teilmenge** von N , wenn jedes Element von M auch Element von N ist. Formal :

$$M \subset N \quad :\Longleftrightarrow \quad \forall\, x \,:\, (x \in M \quad \Longrightarrow \quad x \in N).$$

Beispiel 1.1.11 : a) Es gilt $\mathbb{N} \subset \mathbb{Z}$ und $\mathbb{Z} \subset \mathbb{Q}$.
b) Es gilt für jede Menge M : $\emptyset \subset M$.
Beweis: Es gilt $\forall\, x \,:\, (x \in \emptyset \quad \Longrightarrow \quad x \in M)$, denn die Aussage "$x \in \emptyset$ " ist für alle x falsch, nach Definition der leeren Menge. □

Wir definieren drei Operationen zwischen Mengen:
Definition 1.1.12 : Seien M und N Mengen.
a) Den **Durchschnitt** der Mengen M und N definieren wir als

$$M \cap N \quad := \quad \{\; x \mid x \in M \wedge x \in N \;\} \,.$$

Dabei bedeutet das Zeichen " $:=$ ", dass die linke Menge durch die rechte Menge definiert wird. Man liest es: "**nach Definition gleich**".
b) Als **Vereinigung** der Mengen M und N definieren wir

$$M \cup N \quad := \quad \{\; x \mid x \in M \vee x \in N \;\} \,.$$

c) Als **Differenz** von M und N definieren wir

$$M \setminus N \quad := \quad \{\ x \mid x \in M \wedge x \notin N\ \}\ .$$

Bemerkung 1.1.13 : Wir haben inzwischen einige Zeichen kennengelernt:

$$\wedge \quad , \quad \vee \quad , \quad \neg \quad , \quad \Longrightarrow \quad , \quad \Longleftrightarrow \quad , \quad :\Longleftrightarrow$$

stehen zwischen zwei **Aussagen** . Die Zeichen

$$\cap \quad , \quad \cup \quad , \quad \setminus \quad , \quad \subset \quad , \quad = \quad , \quad :=$$

stehen zwischen zwei **Mengen** . Das ist klar, wird aber von Anfängern häufig falsch gemacht. - In der Mathematik geht man davon aus , dass die Elemente von Mengen selbst wieder Mengen sind. Deshalb können die Zeichen

$$= \quad , \quad :=$$

auch zwischen Elementen einer Menge stehen.

Falls $N \subset M$ ist, hat man für $M \setminus N$ eine besondere Bezeichnung:
Definition 1.1.14 : Seien M und N Mengen, $N \subset M$. Dann heißt

$$\complement N \quad := \quad M \setminus N$$

das **Komplement** von N (bezüglich M , genauer kann man auch $\complement_M N$ schreiben).

Aus Satz 1.1.5 folgen einige Rechenregeln für $\cap, \cup, \complement$:

Satz 1.1.15 : Seien R, S, T Mengen, dann gilt
a) $R \cap S = S \cap R$
b) $(R \cap S) \cap T = R \cap (S \cap T)$
c) $R \cup S = S \cup R$
d) $(R \cup S) \cup T = R \cup (S \cup T)$
e) $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$
f) $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$
Sind S und T Teilmengen einer Menge M , so gilt für das Komplement bezüglich M :

g) $\complement(\complement S) = S$

h) $\complement(S \cup T) = \complement S \cap \complement T$

i) $\complement(S \cap T) = \complement S \cup \complement T$

Beweis mit den Regeln aus Satz 1.1.5 ; wir wollen das an einem Beispiel

vorführen, etwa:
e) Nach Definition 1.1.9 muss man zeigen, dass jedes Element von $R \cap (S \cup T)$ auch Element von $(R \cap S) \cup (R \cap T)$ ist, und umgekehrt: Nun gilt für jedes Element x :

$$
\begin{aligned}
& x \in R \cap (S \cup T) \quad \overset{1.1.12}{\Longleftrightarrow} \\
& x \in R \wedge x \in S \cup T \quad \overset{1.1.12}{\Longleftrightarrow} \\
& x \in R \wedge (x \in S \vee x \in T) \quad \overset{1.1.5}{\Longleftrightarrow} \\
& (x \in R \wedge x \in S) \vee (x \in R \wedge x \in T) \quad \overset{1.1.12}{\Longleftrightarrow} \\
& x \in R \cap S \vee x \in R \cap T \quad \overset{1.1.12}{\Longleftrightarrow} \\
& x \in (R \cap S) \cup (R \cap T) \quad .
\end{aligned}
$$

□

Definition 1.1.16 : Seien M und N Mengen, dann heißt

$$M \times N \quad := \quad \{ \ (x, y) \mid x \in M \wedge y \in N \ \}$$

das **cartesische Produkt** der Mengen M und N . Die Elemente von $M \times N$ heißen **geordnete Paare** von Elementen von M und N . Wir wollen nicht definieren, was ein geordnetes Paar ist, man muss nur wissen, wann zwei geordnete Paare gleich sind: Seien $(x_1, y_1), (x_2, y_2) \in M \times N$, dann gilt

$$(x_1, y_1) \quad = \quad (x_2, y_2) \quad \Longleftrightarrow \quad x_1 = x_2 \wedge y_1 = y_2 \quad .$$

Es kommt also auf die Reihenfolge an : $(2, 3) \neq (3, 2)$!

1.2 Relationen, Induktion

Definition 1.2.1 : Sei M eine Menge. Eine **Relation in M** ist eine Teilmenge

$$R \quad \text{von} \quad M \times M \ .$$

Statt $(x, y) \in R$ sagt man dann: " x steht in Relation R zu y ".
(1.2.2) Beispiele für Relationen sind
a) $\emptyset$,
b) $D \quad := \quad \{ \ (x, y) \in M \mid x = y \ \}$, die **Gleichheitsrelation** in M .
c) Ein weiteres Beispiel ist die
(1.2.3) Anordnung $\leq$ in $\mathbb{Z}$: Man setzt

$$\leq \quad := \quad \{ \ (x, y) \in \mathbb{Z} \mid \text{es gibt ein } z \in \mathbb{N}_0 : \ x + z = y \ \} \ ,$$

und wir schreiben im Folgenden $x \leq y$ statt $(x,y) \in \leq$. Statt $a \leq b$ schreibt man auch : $b \geq a$ für $a, b \in \mathbb{Z}$, und man schreibt

$a < b$ statt $a \leq b \wedge a \neq b$,

$b > a$ statt $a < b$. Es gilt dann

(O1) $\forall\, x \in \mathbb{Z} \;:\; x \leq x$,

(O2) $\forall\, x, y \in \mathbb{Z} \;:\; (x \leq y \wedge y \leq x \implies x = y)$,

(O3) $\forall\, x, y, z \in \mathbb{Z} \;:\; (x \leq y \wedge y \leq z \implies x \leq z)$.

□

Für "es gibt ein" führt man eine Abkürzung ein:

Definition 1.2.4 : Statt "es existiert ein" schreiben wir : "$\exists$". Sei also M eine Menge und $A(x)$ ein sprachliches Gebilde, in das man für x ein Element aus M einsetzen kann und dann eine Aussage erhält. In der Logik nennt man das ein **einstelliges Prädikat** . Dann ist

$$\exists\, x \in M \;:\; A(x)$$

eine Aussage.

(1.2.5) Beachten Sie: a) "$\exists\, x \in M \;:\; A(x)$" heißt, dass es **mindestens** ein Element x mit der Eigenschaft $A(x)$ gibt, es kann auch mehrere solche Elemente geben ! Will man ausdrücken, dass es **genau ein** Element x mit der Eigenschaft $A(x)$ gibt, so schreibt man:

$$\exists_1\, x \in M \;:\; A(x) \quad .$$

b) Es gibt einige logische Regeln für " $\exists$ " und "$\forall$ ": Seien M und N Mengen, $A(x), B(x)$ einstellige Prädikate und $C(x,y)$ ein zweistelliges Prädikat (d.h. hier muss man für x und y Elemente einsetzen, um eine Aussage zu erhalten). Dann gelten die Regeln:

(1) $\neg(\forall\, x \in M \;:\; A(x)) \iff \exists\, x \in M \;:\; (\neg A(x))$

(2) $\neg(\exists\, x \in M \;:\; A(x)) \iff \forall\, x \in M \;:\; (\neg A(x))$

(3) $\forall\, x \in M \;:\; A(x) \wedge \forall\, x \in M \;:\; B(x) \iff \forall\, x \in M \;:\; (A(x) \wedge B(x))$

(4) $\forall\, x \in M \;:\; A(x) \vee \forall\, x \in M \;:\; B(x) \implies \forall\, x \in M \;:\; (A(x) \vee B(x))$

(5) $\exists\, x \in M \;:\; (A(x) \vee B(x)) \iff \exists\, x \in M \;:\; A(x) \vee \exists\, x \in M \;:\; B(x)$

(6) $\exists\, x \in M \;:\; (A(x) \wedge B(x)) \implies \exists\, x \in M \;:\; A(x) \wedge \exists\, x \in M \;:\; B(x)$

(7) $\forall\, x \in M\, \forall\, y \in N \;:\; C(x,y) \iff \forall\, y \in N\, \forall\, x \in M \;:\; C(x,y)$

(8) $\exists\, x \in M\, \exists\, y \in N \;:\; C(x,y) \iff \exists\, y \in N\, \exists\, x \in M \;:\; C(x,y)$

(9) $\exists\, x \in M\, \forall\, y \in N \;:\; C(x,y) \implies \forall\, y \in N\, \exists\, x \in M \;:\; C(x,y)$.

Man mache sich an Beispielen klar, dass bei (4),(6) und (9) nicht "$\iff$" steht!

Definition 1.2.6 : Sei M eine Menge und R eine Relation in M, die die drei Eigenschaften
(Ä1) $\forall\, x \in M \,:\; (x,x) \in R$ ("Reflexivität"),
(Ä2) $\forall\, x,y \in M \,:\; ((x,y) \in R \implies (y,x) \in R)$ ("Symmetrie")
(Ä3) $\forall\, x,y,z \in M \,:\; ((x,y) \in R \wedge (y,z) \in R \implies (x,z) \in R)$
("Transitivität")
hat, dann heißt R eine **Äquivalenzrelation** auf M. Man schreibt dann meist

$$\sim \quad \text{statt} \quad R \quad \text{und} \quad x \sim y \quad \text{statt} \quad (x,y) \in R.$$

Definition und Satz 1.2.7 : Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M . Für $x \in M$ nennt man

$$\overline{x} \quad := \quad \{\; y \in M \;\mid\; y \sim x \;\}$$

die **Äquivalenzklasse** von x . Es gilt

(1) $\quad \forall\, x \in M \,:\; x \in \overline{x},$

(2) $\quad \forall\, x,y \in M : (\overline{x} = \overline{y} \quad \vee \quad \overline{x} \cap \overline{y} = \emptyset),$

(3) $\quad \bigcup_{x \in M} \overline{x} = M.$

Der **Beweis** ist eine leichte Übungsaufgabe.

□

Eine Eigenschaft der Menge $\mathbb{N}$ der natürlichen Zahlen ist das
(1.2.8) Induktionsaxiom (IP) : Sei $P(n)$ ein einstelliges Prädikat, das für natürliche Zahlen n definiert ist. Dann gilt

$$(P(1) \;\wedge\; \forall\, m \in \mathbb{N} \,:\, (P(m) \implies P(m+1))) \quad \implies \quad \forall\, n \in \mathbb{N} \,:\, P(n)\,.$$

□

Man kann damit **Induktionsbeweise** führen, um eine Aussage der Form

$$\forall\, n \in \mathbb{N} \,:\, P(n)$$

zu beweisen. Entsprechend dem Induktionsaxiom besteht so ein Induktionsbeweis aus zwei (!) Schritten:
Induktionsanfang : Man zeigt, dass $P(1)$ wahr ist.
Induktionsschluss : Man zeigt für jedes $m \in \mathbb{N}$: **Wenn** $P(m)$ wahr ist (Induktionsvoraussetzung), **dann** gilt auch $P(m+1)$.

Aus diesen beiden Aussagen folgt dann, dass die Aussage $\forall\, n \in \mathbb{N} \,:\, P(n)$ wahr ist.

□

Bemerkung 1.2.9 : In der Schule lernt man häufig folgendes Schema für Induktionsbeweise:

Induktionsanfang : Man zeigt, dass $P(1)$ wahr ist.
Induktionsvoraussetzung: Sei $m \in \mathbb{N}$, und $P(m)$ sei wahr.
Induktionsschluss: Man zeigt, dass dann auch $P(m+1)$ wahr ist.
Wenn man das Induktionsaxiom verstanden hat, mag diese Schreibweise angehen. Aber man darf dieses Schema nicht lesen als

$$P(1) \quad \wedge \quad \forall\, m \in \mathbb{N} \,:\, P(m) \quad \Longrightarrow \quad \forall\, m \in \mathbb{N} : P(m+1)$$

dann hat man das Induktionsaxiom nicht verstanden. Die obige, zweiteilige, Form des Induktionsbeweises, bei der die Induktionsvoraussetzung (I.V.) Teil des Induktionsschlusses ist, ist logisch durchsichtiger.

□

Man kann auch den Induktionsanfang bei einer Zahl $k \in \mathbb{Z}$ und den Induktionsschluss für alle $m \in \mathbb{Z}$ mit $m \geq k$ machen, dann gilt $P(n)$ für alle $n \in \mathbb{Z}$ mit $n \geq k$.

Bemerkung 1.2.10 : Man kann das Induktionsaxiom auch für **rekursive Definitionen** verwenden: Wenn man für alle $n \in \mathbb{N}$ ein Element $x(n)$ definieren will, definiert man
(1.) $x(1)$, und
(2.) für jedes $m \in \mathbb{N} \,:\, x(m+1)$ mit Hilfe von $x(m)$,
dann ist nach dem Induktionaxiom $x(n)$ für jedes $n \in \mathbb{N}$ definiert.
Ein Beispiel ist die Definition des **Summenzeichens**:
Definition 1.2.11: Sei M eine Menge, in der eine Addition $+$ definiert ist. Seien $m, n \in \mathbb{Z}$, $m \leq n$. Für jede Zahl k in $\mathbb{Z}$ mit $m \leq k \leq n$ sei $a_k \in M$ gegeben. Dann setzen wir

(I) für $n = m$: $\displaystyle\sum_{k=m}^{m} a_k \quad := \quad a_m$

(II) für $n \geq m$: $\displaystyle\sum_{k=m}^{n+1} a_k \quad := \quad \sum_{k=m}^{n} a_k \,+\, a_{n+1}$,

wenn auch $a_{n+1} \in M$ ist.

Übrigens: wenn M genau ein Element 0 mit der Eigenschaft

$$\forall\, a \in M \,:\; a \,+\, 0 \quad = \quad a$$

besitzt, definiert man noch die **leere Summe**

$$\sum_{k=m}^{n} a_k := 0 \quad \text{für} \quad n < m \quad .$$

Wir brauchen das Summenzeichen häufig etwas allgemeiner: Bei der in M definierten Addition $+$ komme es auf die Reihenfolge der Summanden nicht an, es sei $a + b = b + a$ für alle a, b. Sei

$$I = \{j_1, \ldots, j_n\} \quad \text{mit} \quad n \in \mathbb{N}_0$$

eine Menge und seien $a_{j_1}, \ldots, a_{j_n} \in M$. Dann setzen wir

$$\sum_{k \in I} a_k := \sum_{k=1}^{n} a_{j_k} \quad .$$

□

Es gibt noch zwei Aussagen über natürliche Zahlen, die zum Induktionsaxiom (IP) gleichbedeutend sind. Das wollen wir aber hier nicht beweisen:

(1.2.12) Prinzip der Ordnungsinduktion (OI): Sei $P(n)$ ein einstelliges Prädikat, das für natürliche Zahlen n definiert ist. Dann gilt

$$P(1) \wedge \forall\, m \in \mathbb{N} : ((\forall\, k \in \mathbb{N} : (k < m \Longrightarrow P(k))) \Longrightarrow P(m)) \Longrightarrow \forall\, n \in \mathbb{N} : P(n)$$

Das liest sich etwas kompliziert, sagt aber nur: Man macht den Induktionsschluss nicht vom m auf $m + 1$, sondern von allen Zahlen $k < m$ auf m.

(1.2.13) Wohlordnung der natürlichen Zahlen (WO) : Jede nichtleere Teilmenge M von $\mathbb{N}$ besitzt ein kleinstes Element, d.h.

$$\exists\, a \in M \forall\, x \in M \ : \ a \leq x \quad .$$

So ein Element (das dann eindeutig bestimmt ist) nennen wir **min(M)** .

1.3 Funktionen

Definition 1.3.1 : Seien M und N Mengen, dann heißt eine Vorschrift f, die **jedem** Element $x \in M$ **genau ein** Element aus N zuordnet, das man mit $f(x)$ bezeichnet, eine **Funktion** (**Abbildung**) von M in N. Man schreibt zur Abkürzung

$$\begin{aligned} f \ : \ M &\longrightarrow N \\ x &\longmapsto f(x) \quad . \end{aligned}$$

Die Menge M heißt der **Definitionsbereich** von f , die Menge N der **Wertebereich** von f , das Element $f(x)$ der **Funktionswert** von x . Für die Menge aller Funktionen von M in N schreiben wir: $\mathcal{F}(M,N)$.

Bemerkung 1.3.2 : Falls Sie die Begriffe "Vorschrift" und "Zuordnung" unpräzis finden, machen Sie es formaler (aber weniger einprägsam): Seien M und N Mengen und F eine Teilmenge von $M \times N$ mit den beiden Eigenschaften:
(1) $\forall\, x \in M\, \exists y \in N\, :\, (x,y) \in F$,
(2) $\forall\, x \in M\, \forall y_1, y_2 \in N\, :\, ((x,y_1) \in F \,\wedge\, (x,y_2) \in F \implies y_1 = y_2)$.
Dann heißt das Paar $f := (F,N)$ eine Funktion von M in N .

Mit dieser etwas formaleren Definition kann man beweisen:

Satz 1.3.3 : Seien M_1, M_2, N_1, N_2 Mengen. Zwei Funktionen

$$f\, :\, M_1 \longrightarrow N_1 \quad \text{und} \quad g\, :\, M_2 \longrightarrow N_2$$

sind gleich , wenn gilt

$$M_1 = M_2 \;\wedge\; N_1 = N_2 \;\wedge\; \forall\, x \in M_1\, :\, f(x) = g(x) \quad ,$$

also wenn Definitions- und Wertebereiche und für alle $x \in M_1$ die Funktionswerte übereinstimmen.

Definition 1.3.4 : Sei $f\, :\, M \longrightarrow N$ eine Abbildung. Sei $A \subset M$ und $B \subset N$. Dann heißt

$$f(A) := \{\; y \in N \mid \exists\, x \in A\, :\, y = f(x) \;\}$$

das **Bild** von A unter f und

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

das **Urbild** von B unter f . □

Definition 1.3.5 : Sei $f\, :\, M \longrightarrow N$ eine Abbildung und $A \subset M$. Dann heißt die durch

$$f|_A\, :\, A \longrightarrow N \quad , \quad f|_A(x) \quad := \quad f(x)$$

definierte Abbildung die **Restriktion (Einschränkung)** von f auf A . $f|_A$ hat also einen kleineren Definitionsbereich als f ; die Funktionswerte $f|_A(x)$ sind für $x \in A$ aber die gleichen wie die Funktionswerte $f(x)$. □

Zusätzliche Eigenschaften von Funktionen haben besondere Namen:

Definition 1.3.6 : Sei $f : M \longrightarrow N$ eine Abbildung. f heißt

a) **surjektiv** (Abbildung von M **auf** N) , wenn $f(M) = N$ ist, oder, was nach Definition 1.3.4 gleichbedeutend ist:

$$\forall\, y \in N\, \exists\, x \in M : \; f(x) = y \quad ,$$

b) **injektiv** (**eineindeutig**), wenn verschiedene Elemente von M verschiedene Funktionswerte haben, oder, was gleichbedeutend ist:

$$\forall\, x, x' \in M : \; (\, f(x) = f(x') \implies x = x'\,) \quad ,$$

c) **bijektiv** , wenn f surjektiv und injektiv ist.

Definition 1.3.7 : Sei $f : M \longrightarrow N$ bijektiv. Sei $y \in N$, dann gibt es dazu, da f surjektiv ist, ein, und da f injektiv ist, genau ein Element aus M , dessen Funktionswert gleich y ist, wir nennen es $f^{-1}(y)$. Die Funktion

$$f^{-1} : N \longrightarrow M \quad , \quad y \longmapsto f^{-1}(y)$$

heißt die **Umkehrfunktion** von f .

(1.3.8) Beachten Sie : Sei $f : M \longrightarrow N$, dann ist für $B \subset N$ das

Urbild $\overset{-1}{f}(B)$

definiert. Nur, wenn f bijektiv ist, ist die

Umkehrfunktion f^{-1}

definiert. Für $B \subset N$ ist dann allerdings

$$f^{-1}(B) = \overset{-1}{f}(B) \ ,$$

so dass es keine Missverständnisse gibt.

(1.3.9) Beispiele : 1) Ist M eine Menge, so heißt

$$\begin{aligned} \mathrm{id}_M : M &\longrightarrow M \\ x &\longmapsto x \end{aligned}$$

die **identische Abbildung** von M . Sie bildet jedes Element auf sich selbst ab und ist bijektiv.

2) Sei $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) := x^2$, so ist f nicht surjektiv, denn zu -1 gibt es kein $x \in \mathbb{R}$ mit $f(x) = -1$. f ist auch nicht injektiv, denn

$$f(2) = f(-2) = 4 \quad , \quad \text{aber} \quad 2 \neq -2 \quad .$$

Setzt man aber $\mathbb{R}_+^* := \{\, x \in \mathbb{R} \mid x > 0 \,\}$ und betrachtet

$$g : \mathbb{R}_+^* \longrightarrow \mathbb{R}_+^* \quad , \quad g(x) := x^2 \quad ,$$

so ist g bijektiv. Um das zu beweisen, muss man zeigen, dass es zu jedem $y \in \mathbb{R}_+^*$ ein $x \in \mathbb{R}_+^*$ mit $y = x^2$ gibt, also dass man aus positiven reellen

Zahlen Quadratwurzeln ziehen kann. Man lernt das in der Analysis.

Definition 1.3.10 : Seien $f : L \longrightarrow M$ und $g : M \longrightarrow N$ Abbildungen, dann kann man die **Hintereinanderausführung** von f und g bilden :

$$g \circ f : L \longrightarrow N \quad ,$$
$$x \longmapsto g(f(x)) \quad .$$

Beachten Sie, dass man $(g \circ f)(x)$ erhält, indem man **zuerst** f auf x und **dann** g auf $f(x)$ anwendet. □

Bildet man die Hintereinanderausführung von drei oder mehr Funktionen, so kommt es nicht auf die Reihenfolge der Klammern an:
Satz 1.3.11 (Assoziativität der Hintereinanderausführung) : Seien

$$f : K \longrightarrow L \quad , \quad g : L \longrightarrow M \quad , \quad h : M \longrightarrow N$$

Abbildungen, dann gilt

$$(h \circ g) \circ f \quad = \quad h \circ (g \circ f) \quad .$$

Beweis : $(h \circ g) \circ f$ und $h \circ (g \circ f)$ sind beides Abbildungen von K in N, und für alle $x \in K$ gilt

$$((h \circ g) \circ f)(x) \quad = \quad (h \circ g)(f(x)) \quad = \quad h(g(f(x))) \quad ,$$

$$(h \circ (g \circ f))(x) \quad = \quad h((g \circ f)(x)) \quad = \quad h(g(f(x))) \quad .$$

Nach Satz 1.3.3 gilt $h \circ (g \circ f) \quad = \quad (h \circ g) \circ f \quad .$ □

Wir wollen noch ein Kriterium dafür beweisen, wann eine Funktion injektiv, surjektiv oder bijektiv ist:
Satz 1.3.12 : Sei $f : M \longrightarrow N$ eine Funktion und seien $M, N \neq \emptyset$. Dann gilt:
a) f ist injektiv genau dann, wenn es eine Abbildung

$$g : N \longrightarrow M \quad \text{mit} \quad g \circ f \quad = \quad \mathrm{id}_M \quad \text{gibt.}$$

b) f ist surjektiv genau dann, wenn es eine Abbildung

$$g : N \longrightarrow M \quad \text{mit} \quad f \circ g \quad = \quad \mathrm{id}_N \quad \text{gibt.}$$

c) f ist bijektiv genau dann, wenn es eine Abbildung

$$g : N \longrightarrow M \quad \text{mit} \quad f \circ g \quad = \quad \mathrm{id}_N \quad \text{und} \quad g \circ f \quad = \quad \mathrm{id}_M \quad \text{gibt.}$$

In diesem Fall ist $g = f^{-1}$ die Umkehrfunktion von f .

Beweis : a) 1.) Sei f injektiv. Sei $y \in N$, dann gibt es zwei Möglichkeiten: Entweder ist $y \in f(M)$, dann gibt es, da f injektiv ist, genau ein x mit $y = f(x)$. Wir setzen $g(y) := x$. Oder es ist $y \notin f(M)$. Wegen $M \neq \emptyset$ gibt es ein Element $x_0 \in M$. Wir setzen dann $g(y) := x_0$. Dann ist

$$g \circ f \quad = \quad \mathrm{id}_M \quad ,$$

denn für alle $x \in M$ gilt $(g \circ f)(x) = x$.
2.) Es gebe ein $g : N \longrightarrow M$ mit $g \circ f = \mathrm{id}_M$. Seien $x, x' \in M$, dann gilt

$$f(x) = f(x') \quad \Longrightarrow \quad g(f(x)) = g(f(x')) \quad \Longrightarrow \quad \mathrm{id}_M(x) = \mathrm{id}_M(x')$$

$$\Longrightarrow \quad x = x' \quad , \quad \text{also ist } f \text{ injektiv.}$$

b) 1.) Sei f surjektiv. Sei $y \in N$, dann gibt es mindestens ein $x \in M$ mit $y = f(x)$, es ist $\overset{-1}{f}(\{y\}) \neq \emptyset$.
$(*)$ Wir wählen ein $x \in \overset{-1}{f}(\{y\})$
und setzen

$$g(y) \quad := \quad x \quad ,$$

dann gilt

$$f \circ g \quad = \quad \mathrm{id}_N \quad ,$$

denn für $y \in N$ gilt $g(y) = x$, wobei $f(x) = y$ ist, also $f(g(y)) = y$.
2.) Es gebe ein $g : N \longrightarrow M$ mit $f \circ g = \mathrm{id}_N$. Sei $y \in N$,dann ist $y = (f \circ g)(y) = f(g(y))$, also gibt es ein $x \in M$ mit $y = f(x)$, nämlich $x := g(y)$. Also ist f surjektiv.
c) 1.) Wenn es ein $g : N \longrightarrow M$ mit

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

gibt, folgt aus a) und b) , dass f bijektiv ist.
2.) Wenn f bijektiv ist, haben wir die Umkehrfunktion $f^{-1} : N \longrightarrow M$, die die beiden Gleichungen

$$f \circ f^{-1} = \mathrm{id}_N \quad , \quad f^{-1} \circ f = \mathrm{id}_M$$

erfüllt.
3.) Sei f bijektiv und es gebe $g : N \longrightarrow M$ mit

$$f \circ g = \mathrm{id}_N \quad , \quad g \circ f = \mathrm{id}_M \quad ,$$

dann folgt

$$f^{-1} \quad = \quad f^{-1} \circ (f \circ g) \quad = \quad (f^{-1} \circ f) \circ g \quad = \quad \mathrm{id}_N \circ g \quad = \quad g \quad .$$

Bei $(*)$ haben wir gebraucht, dass man aus (möglicherweise unendlich vielen) Mengen je ein Element auswählen kann; das "Auswahlaxiom" der Mengenlehre besagt, dass das geht. Wir wollen auf solche Fragen der Grundlagen der Mathematik hier nicht eingehen. □

Definition 1.3.13 : a) Für $n \in \mathbb{N}$ setzen wir

$$\underline{n} \quad := \quad \{ \; m \in \mathbb{N} \mid \; m \leq n \; \} \quad , \qquad \text{also}$$

$$\underline{n} \quad := \quad \{1, 2, \ldots, n\} \quad , \quad \text{und zusätzlich}$$

$$\underline{0} \quad := \quad \emptyset \quad .$$

b) Sei M eine Menge. M heißt **endlich** , wenn es ein $n \in \mathbb{N}_0$ und eine bijektive Abbildung

$$f \; : \; \underline{n} \; \longrightarrow \; M$$

gibt. Man kann dann (mit Induktion) beweisen, dass das n eindeutig bestimmt ist. Es ist daher sinnvoll,

$$\#(M) \quad := \quad n$$

die **Mächtigkeit** von M zu nennen.
c) Ist die Menge M nicht endlich, so heißt M eine **unendliche** Menge.

1.4 Etwas analytische Geometrie im $\mathbb{R}^n$

Wir wollen dieses Kapitel voranstellen, auch wenn wir hinterher Vieles allgemeiner machen. Aber Sie sollen zunächst mal etwas lernen, das an die "Vektorrechnung" anknüpft, die Sie von der Schule kennen:
Bemerkung 1.4.1 : Mit der Einführung der reellen Zahlen beschäftigen Sie sich in der Analysis. Hier brauchen Sie zunächst nur zu wissen, dass man für $a, b \in \mathbb{R}$

die Summe $a + b \in \mathbb{R}$ und
das Produkt $a \cdot b \in \mathbb{R}$ hat,

die Rechenregeln setzen wir auch mal als bekannt voraus, auch, dass man die reellen Zahlen anordnen kann, so dass

$$a < b \; , \; a \leq b \; , b > a \; , b \geq a$$

für $a, b \in \mathbb{R}$ definierte Aussagen sind. Wir brauchen noch: Für $a \in \mathbb{R}, a \geq 0$, ist

$$\sqrt{a} \in \mathbb{R} \quad \text{definiert} \quad , (\sqrt{a})^2 = a \, , \, \sqrt{a} \geq 0.$$

Definition 1.4.2 : Sei $n \in \mathbb{N}$. Dann definieren wir mit Def.1.1.16 $\mathbb{R}^n$ rekursiv durch

$$\mathbb{R}^1 := \mathbb{R} \quad , \quad \mathbb{R}^{n+1} := \mathbb{R}^n \times \mathbb{R} \quad \text{für} \quad n \in \mathbb{N}, \quad \text{also}$$

$$\mathbb{R}^n = \{ \ (x_1, \ldots, x_n) \ | \ \forall\, j \in \underline{n} : x_j \in \mathbb{R} \ \} \ ,$$

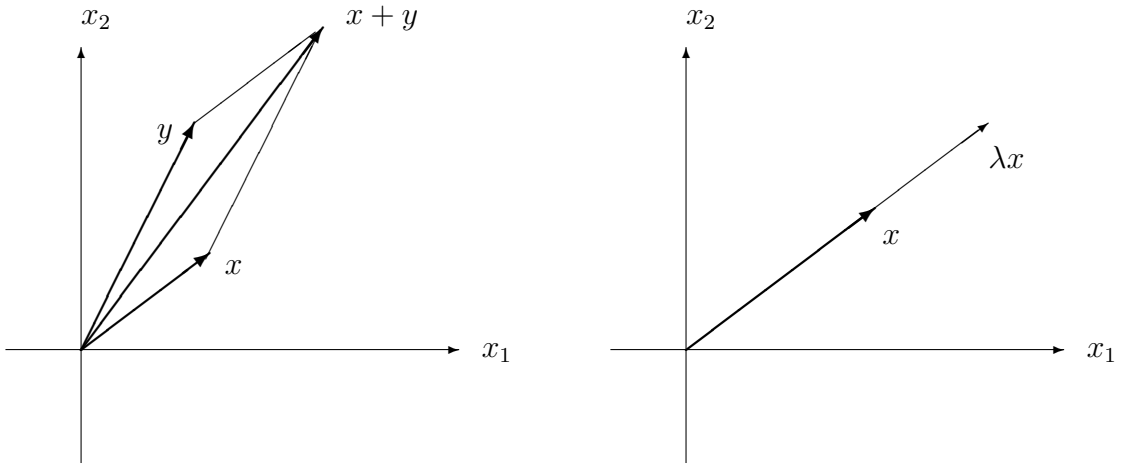
also ist $\mathbb{R}^n$ die Menge der geordneten $n-$tupel reeller Zahlen.
Man kann Elemente aus $\mathbb{R}^n$ addieren,

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

und mit einem $\lambda \in \mathbb{R}$ multiplizieren:

$$\lambda(x_1, \ldots, x_n) := (\lambda \cdot x_1, \ldots, \lambda \cdot x_n),$$

für $x_1, \ldots, x_n, y_1, \ldots y_n \in \mathbb{R}$. Für $n = 2$ und $n = 3$ kann man diese Addition von "Vektoren" und die Multiplikation mit reellen Zahlen geometrisch veranschaulichen (etwa für $n = 2$):



Noch zur Schreibweise: Man hat die reelle Zahl 0 , und

$$0 := (0, \ldots, 0) \in \mathbb{R}^n,$$

wir schreiben für beide Elemente dasselbe Zeichen. Zu

$$x = (x_1, \ldots, x_n) \in \mathbb{R}^n \quad \text{hat man}$$

$$-x := (-x_1, \ldots, -x_n) \in \mathbb{R}^n, \quad \text{dafür gilt}$$

$$x + (-x) = 0.$$

Für $x, y \in \mathbb{R}^n$ schreiben wir auch

$$x - y := x + (-y).$$

Definition 1.4.3 : Seien

$$x = (x_1, \ldots, x_n)\,,\; y = (y_1, \ldots, y_n) \in \mathbb{R}^n.$$

Dann nennen wir

$$\langle x, y\rangle := \sum_{j=1}^{n} x_j y_j$$

das **kanonische Skalarprodukt** von x und y. Man hat also die Abbildung

$$\langle \quad , \quad \rangle \quad : \quad \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}\,,$$

$$(x, y) \longmapsto \langle x, y\rangle\,,$$

d,h. zwei "Vektoren" $x, y \in \mathbb{R}^n$ wird ein "Skalar" $\langle x, y\rangle \in \mathbb{R}$ zugeordnet.
Behauptung 1.4.4 : Für alle $x, x', y \in \mathbb{R}^n, \lambda \in \mathbb{R}$ gilt

(H1) $\langle x{+}x', y\rangle = \langle x, y\rangle{+}\langle x' y\rangle \quad ,$

$$\langle \lambda x, y\rangle = \lambda \langle x, y\rangle \quad ,$$

(H2) $\langle x, y\rangle = \langle y, x\rangle \quad ,$

(H4) $\langle x, x\rangle \geq 0 \quad \text{und} \quad (x \neq 0 \quad \Longrightarrow \quad \langle x, x\rangle > 0\,).$

Beweisen kann man diese Aussagen direkt mit der Definition. Bei (H4) braucht man noch, was man in der Analysis lernt :

$$\forall\, a \in \mathbb{R} \;:\; (a \neq 0 \quad \Longrightarrow \quad a^2 > 0)\,, \quad \text{und}$$

$$\forall a, b \in \mathbb{R} \;:\; (a, b \geq 0 \quad \Longrightarrow \quad a + b \geq 0).$$

□

Wegen (H4) ist die folgende Definition sinnvoll:
Definition 1.4.5 : Für $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ nennen wir

$$\| x \| \quad := \quad \sqrt{\langle x, x\rangle} \quad = \quad \sqrt{x_1^2 + \ldots + x_n^2}$$

die **Norm** (**Länge**) von x .

Den Winkel zwischen zwei "Vektoren" wollen wir jetzt nicht definieren, dazu fehlen uns Kenntnisse aus der Analysis. Aber wir können "senkrecht stehen" von Vektoren definieren:
Definition 1.4.6 : Seien $x, y \in \mathbb{R}^n$. Wir sagen, x und y sind zueinander

orthogonal , oder: x und y **stehen senkrecht** aufeinander, in Zeichen : $x \perp y$, wenn

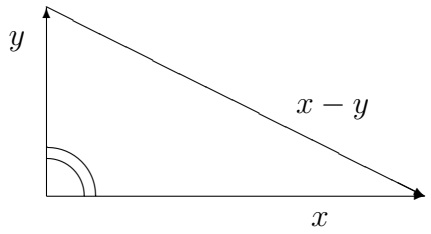
$$\langle x, y \rangle \quad = \quad 0 \quad \text{ist.}$$

□

Ganz einfach zu beweisen (aber letztlich nur eine Folge davon, dass wir unsere Definitionen passend gewählt haben) ist

Satz 1.4.7 (Pythagoras) Seien $x, y \in \mathbb{R}^n, x \perp y$, dann gilt

$$\| x \|^2 + \| y \|^2 = \| x - y \|^2 .$$



Beweis :

$$\| x - y \|^2 \overset{1.4.5}{=} \langle x - y, x - y \rangle \overset{(H1)}{=} \langle x, x - y \rangle - \langle y, x - y \rangle$$

$$\overset{(H1),(H2)}{=} \langle x, x \rangle - \langle x, y \rangle - \langle y, x \rangle + \langle y, y \rangle \overset{(*)}{=} \| x \|^2 + \| y \|^2,$$

wobei wir bei (*) verwendet haben, dass $x \perp y$ gilt.

□

Definition 1.4.8 : Sei $n \in \mathbb{N}$ und seien $p, a \in \mathbb{R}^n$, $a \neq 0$. Dann heißt die Menge

$$G_{p,a} := \{ \; p + \lambda a \mid \lambda \in \mathbb{R} \; \} \quad , \quad \text{kurz geschrieben:}$$

$$G_{p,a} = p + \mathbb{R} \cdot a$$

die **Gerade** durch p mit **Richtung** a . Die Schreibweise

$$G_{p,a} = p + \mathbb{R} \cdot a$$

heißt eine **Parameterdarstellung** von $G_{p,a}$.

Bemerkung 1.4.9 (1.5) : Zu einer Geraden $G \subset \mathbb{R}^n$ sind p, a mit $G = G_{p,a}$ nicht eindeutig bestimmt. Bitte überlegen Sie sich: Für $p, q, a, b \in \mathbb{R}^n$ mit $a, b \neq 0$ gilt

$$G_{p,a} = G_{q,b} \iff q \in G_{p,a} \wedge \exists\, \mu \in \mathbb{R} \setminus \{0\} : \; b = \mu a \quad .$$

□

Man kann mit der Parameterdarstellung durchaus rechnen, z.B. kann man Schnittpunkte ausrechnen, wenn sie existieren. Im $\mathbb{R}^2$ kann man Geraden auch anders, als Lösungsmenge **einer** linearen Gleichung, angeben:

1.5 Geraden im $\mathbb{R}^2$

Bemerkung 1.5.1 : Sei $G \subset \mathbb{R}^2$ eine Gerade, dann gibt es $p, a \in \mathbb{R}^2$ mit $a \neq 0$ und

$$G = G_{p,a} = \{\; p + \lambda a \mid \lambda \in \mathbb{R} \;\} \quad , \quad \text{also gilt :}$$

$$x = (x_1, x_2) \in G \iff$$
$$\exists\, \lambda \in \mathbb{R} : \; (x_1 = p_1 + \lambda a_1 \wedge x_2 = p_2 + \lambda a_2) \quad .$$

Wir multiplizieren die erste Gleichung mit a_2, die zweite mit a_1 und subtrahieren die beiden Gleichungen voneinander :

$$a_2 x_1 - a_1 x_2 = a_2 p_1 - a_1 p_2 \quad , \quad \text{dann wird}$$

$$G \subset \{\; x \in \mathbb{R}^2 \mid \langle x, (-a_2, a_1) \rangle = \langle p, (-a_2, a_1) \rangle \;\} \quad ,$$

wir werden gleich sehen, dass hier nicht nur "$\subset$", sondern sogar "$=$" steht. Zunächst

Definition und Satz 1.5.2 : Für $a = (a_1, a_2) \in \mathbb{R}^2$ definieren wir

$$a^\perp := (-a_2, a_1) \quad .$$

Dann gilt für alle $a, b \in \mathbb{R}^2$, $\lambda \in \mathbb{R}$:

(1) $(a+b)^\perp = a^\perp + b^\perp$, $(\lambda a)^\perp = \lambda a^\perp$

(2) $\langle a, a^\perp \rangle = 0$, $\langle a, b^\perp \rangle = -\langle a^\perp, b \rangle$,
$\|a^\perp\| = \|a\|$, $(a^\perp)^\perp = -a$.

Beweis als Übungsaufgabe (1.5).

□

Definition und Satz 1.5.3 : Sei $c \in \mathbb{R}^2 \setminus \{0\}$ und $\alpha \in \mathbb{R}$, dann ist

$$H_{c,\alpha} := \left\{ x \in \mathbb{R}^2 \;\middle|\; \langle x, c \rangle = \alpha \right\}$$
$$= \left\{ x \in \mathbb{R}^2 \;\middle|\; c_1 x_1 + c_2 x_2 = \alpha \right\}$$

eine Gerade im $\mathbb{R}^2$, und zwar

$$(*) \qquad H_{c,\alpha} = G_{\frac{\alpha}{\|c\|^2} \cdot c, c^\perp} \quad .$$

$H_{c,\alpha}$ heißt die **Gleichungsdarstellung** der Geraden $G := G_{\frac{\alpha}{\|c\|^2} \cdot c, c^\perp}$, denn $H_{c,\alpha}$ ist die Menge der Lösungen x der linearen Gleichung

$$c_1 x_1 + c_2 x_2 = \alpha \quad .$$

Beweis : Wenn wir die Gleichheit $(*)$ zeigen, ist bewiesen, dass $H_{c,\alpha}$ eine Gerade ist :
1.) Sei $x \in G_{\frac{\alpha}{\|c\|^2} \cdot c, c^\perp}$, dann gibt es ein $\lambda \in \mathbb{R}$ mit

$$x = \frac{\alpha}{\|c\|^2} c + \lambda c^\perp \quad ,$$

$$\text{also} \quad \langle x, c \rangle = \frac{\alpha}{\|c\|^2} \langle c, c \rangle + \lambda \langle c^\perp, c \rangle \quad ,$$

$$\langle x, c \rangle = \frac{\alpha}{\|c\|^2} \|c\|^2 = \alpha \quad , \qquad \text{also} \quad x \in H_{c,\alpha} \quad .$$

2.) Sei $x \in H_{c,\alpha}$, also $\langle x, c \rangle = \alpha$, dann folgt

$$\langle x - \frac{\alpha}{\|c\|^2} c, c \rangle = \langle x, c \rangle - \frac{\alpha}{\|c\|^2} \langle c, c \rangle = \alpha - \alpha = 0 \quad .$$

Für $y := x - \frac{\alpha}{\|c\|^2} c$ gilt also $\langle y, c \rangle = 0$, und es ist $c \neq 0$. Ist $c_1 \neq 0$, so folgt aus $0 = \langle y, c \rangle = y_1 c_1 + y_2 c_2$:

$$y_1 = \frac{y_2}{c_1} \cdot (-c_2) \quad , \quad \text{und sowieso :} \quad y_2 = \frac{y_2}{c_1} c_1 \quad ,$$

$$\text{also} \quad y = \frac{y_2}{c_1} \cdot c^\perp \quad .$$

Ist $c_2 \neq 0$, so folgt

$$y_2 = -\frac{y_1}{c_2} \cdot c_1 \quad , \quad \text{und sowieso :} \quad y_1 = -\frac{y_1}{c_2} \cdot (-c_2) \quad ,$$

$$\text{also} \quad y = -\frac{y_1}{c_2} \cdot c^\perp \quad ,$$

auf jeden Fall: $\exists\,\lambda \in \mathbb{R} : \; y = \lambda c^{\perp} \quad ,$

$$x - \frac{\alpha}{\|c\|^2} c = \lambda c^{\perp} \quad , \quad x = \frac{\alpha}{\|c\|^2} c + \lambda c^{\perp} \quad ,$$

also $x \in G_{\frac{\alpha}{\|c\|^2} \cdot c, c^{\perp}}$.

□

Bemerkung 1.5.4 : Mit der Formel

$$(*) \qquad H_{c,\alpha} \quad = \quad G_{\frac{\alpha}{\|c\|^2} \cdot c, c^{\perp}}$$

erhält man zu einer Geraden in Gleichungsdarstellung leicht eine Parameterdarstellung. Umgekehrt geht das auch: Für $p, a \in \mathbb{R}^2$ mit $a \neq 0$ gilt

$$(**) \qquad G_{p,a} \quad = \quad H_{a^{\perp}, \langle a^{\perp}, p \rangle} \quad .$$

Beweis als Übung.

□

(1.5.5) Schnittpunkt zwischen Geraden im $\mathbb{R}^2$: Hat man zwei Geraden im $\mathbb{R}^2$, etwa in Parameterform

$$G_{p,a} \quad \text{und} \quad G_{q,b} \quad \text{mit} \quad p, q, a, b \in \mathbb{R}^2, a, b \neq 0 \quad ,$$

so kann man fragen, ob sie einen eindeutig bestimmten Schnittpunkt s besitzen. Ist $s \in G_{p,a} \cap G_{q,b}$, so gibt es $\lambda, \mu \in \mathbb{R}$ mit

$$s = p + \lambda\, a \quad = \quad q + \mu b \quad ,$$

und wenn wir das Skalarprodukt mit $a^{\perp}$ bilden :

$$(0) \qquad \langle\, p, a^{\perp} \,\rangle \quad = \quad \langle\, q, a^{\perp} \,\rangle + \mu \langle\, b, a^{\perp} \,\rangle \quad ,$$

und es gibt genau dann eine eindeutig bestimmte Lösung für μ , wenn $\langle\, b, a^{\perp} \,\rangle \neq 0$ ist :

$$(1) \qquad G_{p,a} \cap G_{q,b} \quad = \quad \left\{ q + \frac{\langle\, p - q, a^{\perp} \,\rangle}{\langle\, b, a^{\perp} \,\rangle}\, b \right\} \quad \text{für} \quad \langle\, b, a^{\perp} \,\rangle \neq 0 \quad .$$

Ist $\langle\, b, a^{\perp} \,\rangle = 0$, so sieht man:
Für $\langle\, p - q, a^{\perp} \,\rangle \neq 0$ gibt es keinen Schnittpunkt,
für $\langle\, p - q, a^{\perp} \,\rangle = 0$ ist jedes $\mu \in \mathbb{R}$ Lösung von (0) .

Man sieht, dass $\langle b, a^\perp \rangle = 0$ bedeutet, dass die Geraden $G_{p,a}$ und $G_{q,b}$ parallel sind. Wir halten es schon einmal fest: Eine lineare Gleichung mit einer Unbekannten, wie (0) , besitzt durchaus nicht immer eine eindeutig bestimmte Lösung; es kann auch sein, dass sie keine Lösung besitzt oder dass alle reellen Zahlen Lösungen sind !

Der Vollständigkeit halber geben wir noch Formeln für den Schnittpunkt an, wenn mindestens eine der Geraden in Gleichungsdarstellung gegeben ist: Für $a, b, c, p \in \mathbb{R}^2 \quad , \quad a, b, c \neq 0 \quad$ und $\quad \alpha, \beta \in \mathbb{R}$ gilt

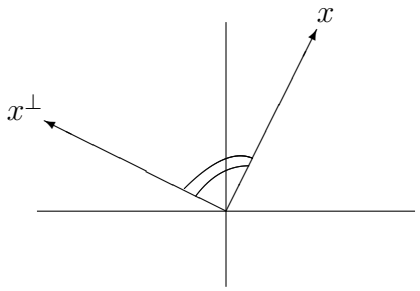
$$(2) \qquad H_{a,\alpha} \cap H_{b,\beta} \quad = \quad \left\{ \frac{1}{\langle a^\perp, b \rangle} (\beta a^\perp - \alpha b^\perp) \right\} \quad \text{für} \quad \langle a^\perp, b \rangle \neq 0 \quad ,$$

$$(3) \qquad G_{p,a} \cap H_{c,\alpha} \quad = \quad \left\{ p + \frac{\alpha - \langle p, c \rangle}{\langle a, c \rangle} a \right\} \quad \text{für} \quad \langle a, c \rangle \neq 0 \quad .$$

Beweisen können Sie diese Formeln leicht. Auswendig lernen sollten Sie sie keineswegs !

□

Es liegt nahe, dass man so etwas wie den Vektor $x^\perp$, der "die" zu x senkrechte Richtung angibt, falls $x \neq 0$ ist, im $\mathbb{R}^n$ für $n \geq 3$ nicht definieren kann.



1.6 Geraden und Ebenen im $\mathbb{R}^3$

Zuvor die

Definition 1.6.1 : Seien $a, b \in \mathbb{R}^n$, $n \in \mathbb{N}$. Dann heißt das Paar (a, b) **linear unabhängig**, wenn für alle $\lambda, \mu \in \mathbb{R}$ gilt

$$\lambda a + \mu b = 0 \quad \Longrightarrow \quad \lambda = \mu = 0 \quad .$$

Bemerkung 1.6.2 : Seien $p, a \in \mathbb{R}^3$, $a \neq 0$, so ist

$$G_{p,a} \quad = \quad \{\ p + \lambda\, a \ \mid\ \lambda \in \mathbb{R}\ \}$$

die Gerade durch p mit Richtung a , in Parameterdarstellung. Aber: Ist $c \in \mathbb{R}^3$, $c \neq 0$, und $\alpha \in \mathbb{R}$, so ist

$$H_{c,\alpha} \quad = \quad \left\{\ x \in \mathbb{R}^3 \ \middle|\ \langle\, x, c\,\rangle \,=\, \alpha\ \right\} \quad ,$$

also die Menge der Lösungen (x_1, x_2, x_3) der linearen Gleichung

$$c_1 x_1 + c_2 x_2 + c_3 x_3 \,=\, \alpha$$

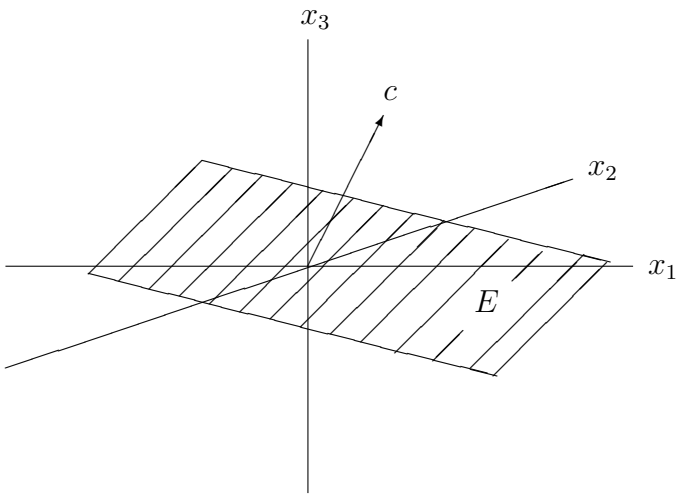
keine Gerade: Sei $p \in H_{c,\alpha}$, also p eine feste Lösung dieser Gleichung (die wegen $c \neq 0$ existiert: Ist etwa $c_1 \neq 0$, so ist

$$p \quad = \quad \left(\frac{\alpha}{c_1}, 0, 0\right) \quad \text{eine Lösung),}$$

dann gilt für beliebiges $x \in H_{c,\alpha}$:

$$(1) \qquad \langle\, x - p, c\,\rangle \quad = \quad \langle\, x, c\,\rangle - \langle\, p, c\,\rangle \quad = \quad \alpha - \alpha \quad = \quad 0 \quad ,$$

$H_{c,\alpha}$ ist die Menge der $x \in \mathbb{R}^3$, für die $x - p$ auf c senkrecht steht : Anschaulich gesehen, ist das eine Ebene:



Sei $\qquad E \quad := \quad \{\ y \in \mathbb{R}^3 \ \mid\ \langle\, y, c\,\rangle \,=\, 0\ \} \quad ,$
dann gibt es wegen $c \neq 0$ stets zwei Lösungen a, b von $\langle\, y, c\,\rangle \,=\, 0$, also zwei Elemente aus E , die verschiedene "Richtungen" haben: Ist etwa $c_1 \neq 0$, so kann man

$$a \quad := \quad \left(-\frac{c_2}{c_1}, 1, 0\right) \quad , \quad b \quad := \quad \left(-\frac{c_3}{c_1}, 0, 1\right)$$

wählen, entsprechend für die Fälle $c_2 \neq 0$ bzw. $c_3 \neq 0$. Dass a und b verschiedene "Richtungen" haben, kann man mit Definition 1.6.1 so ausdrücken: Das Paar (a, b) ist linear unabhängig. Es gilt dann

(2) $\quad E \;=\; \{\; \lambda\, a + \mu\, b \;\mid\; \alpha, \mu \in \mathbb{R} \;\}$.

Beweis von (2): 1.) Aus $\langle\, a, c \,\rangle \;=\; \langle\, b, c \,\rangle \;=\; 0$ folgt

$$\langle\, \lambda\, a + \mu\, b\,,\, c \,\rangle \;\;=\;\; \lambda\, \langle\, a, c \,\rangle + \mu\, \langle\, b, c \,\rangle \;\;=\;\; 0$$

für alle $\lambda, \mu \in \mathbb{R}$, also $\{\; \lambda\, a + \mu\, b \;\mid\; \lambda, \mu \in \mathbb{R} \;\} \;\subset\; E$.

2.) Wir zeigen $E \subset \{\; \lambda a + \mu b \;\mid\; \lambda, \mu \in \mathbb{R} \;\}$ für den Fall $c_1 \neq 0$ und obiges a, b: Sei $y \;=\; (y_1, y_2, y_3) \in E$, dann setzen wir $\lambda \;:=\; y_2$ und $\mu \;:=\; y_3$. Wegen

$$\langle\, y, c \,\rangle \;=\; 0 \quad \text{gilt dann} \quad y_1 \;=\; -\frac{c_2}{c_1} y_2 - \frac{c_3}{c_1} y_3 \quad , \quad \text{also}$$

$$\begin{aligned} y_1 \;&=\; \lambda a_1 + \mu b_1 \quad , \\ y_2 \;&=\; \lambda a_2 + \mu b_2 \quad \text{wegen} \quad a_2 \;=\; 1 \quad , \quad b_2 \;=\; 0 \quad , \\ y_3 \;&=\; \lambda a_3 + \mu b_3 \quad \text{wegen} \quad a_3 \;=\; 0 \quad , \quad b_3 \;=\; 1 \quad , \quad \text{also} \\ y \;&=\; \lambda a + \mu b \end{aligned}$$

Aus (1) und (2) folgt dann

$$H_{c,\alpha} \;\;=\;\; \{\; p + \lambda a + \mu b \;\mid\; \lambda, \mu \in \mathbb{R} \;\} \quad ,$$

wobei p eine feste Lösung von $\langle\, x, c \,\rangle \;=\; \alpha$ ist, und a, b Lösungen von $\langle\, y, c \,\rangle \;=\; 0$ sind, noch so, dass das Paar (a, b) linear unabhängig ist.

□

Wir haben gesehen: **Eine** lineare Gleichung

$$\langle\, x, c \,\rangle \;=\; \alpha \quad , \quad c \in \mathbb{R}^3 \setminus \{0\}\,,\; \alpha \in \mathbb{R}$$

beschreibt eine Ebene im $\mathbb{R}^3$. Kann man eine Gerade im $\mathbb{R}^3$ vielleicht durch mehrere lineare Gleichungen beschreiben ?

Definition und Satz 1.6.3 : Seien $b \;=\; (b_1, b_2, b_3)\,,\; c \;=\; (c_1, c_2, c_3) \in \mathbb{R}^3$, dann nennen wir

$$b \;\times\; c \quad :=\quad (b_2 c_3 - b_3 c_2\,,\; -b_1 c_3 + b_3 c_1\,,\; b_1 c_2 - b_2 c_1)$$

das **Vektorprodukt** von b und c . Es gilt

$$(0) \qquad \langle\, b, b \times c \,\rangle \;=\; \langle\, c, b \times c \,\rangle \;=\; 0 \quad ,$$

d.h. b und c stehen auf $b \times c$ senkrecht.
Beweis : Die Gleichung (0) ist Aufgabe (1.9) e).

□

Bemerkung 1.6.4 : 1.) Sei

$$G_{p,a} \quad = \quad \{\ p + \lambda a \mid \lambda \in \mathbb{R}\ \} \quad \text{mit} \quad a, p \in \mathbb{R}^3\,,\ a \neq 0$$

eine Gerade im $\mathbb{R}^3$ Dann gilt für $x \in G_{p,a}\,,\ x = (x_1, x_2, x_3)$:

$$x_j = p_j + \lambda a_j \quad \text{für} \quad j \in \underline{3} \quad .$$

Man kann eine dieser Gleichungen nach λ auflösen und auf diese Weise λ eliminieren: Wegen $a \neq 0$ ist eins der a_j ungleich 0. Sei etwa $a_1 \neq 0$, dann haben wir $\lambda = \frac{1}{a_1}x_1 - \frac{1}{a_1}p_1$ und $x_2 = p_2 + \frac{a_2}{a_1}x_1 - \frac{a_2}{a_1}p_1$, also

$$a_1x_2 - a_2x_1 = a_1p_2 - a_2p_1 \quad , \quad \text{entsprechend :}$$

$$a_1x_3 - a_3x_1 = a_1p_3 - a_3p_1 \quad .$$

Setzen wir

$$b := (-a_2, a_1, 0) \quad , \quad c := (-a_3, 0, a_1) \quad ,$$

$$\beta := a_1p_2 - a_2p_1 \quad , \quad \gamma := a_1p_3 - a_3p_1 \quad , \quad \text{so ist}$$

$$(*) \qquad G_{p,a} \subset \{\ x \in \mathbb{R}^3 \mid \langle b, x\rangle = \beta \wedge \langle c, x\rangle = \gamma\ \} \quad ,$$

wobei die Familie (b, c) wegen $a_1 \neq 0$ linear unabhängig ist, und b und c stehen auf dem Richtungsvektor a von $G_{p,a}$ senkrecht:

$$b \perp a \quad \text{wegen} \quad \langle (-a_2, a_1, 0), (a_1, a_2, a_3)\rangle = 0 \quad , \quad \text{ebenso :}$$

$$c \perp a \quad .$$

2.) Wir zeigen nun : Für eine linear unabhängige Familie (b, c) mit $b, c \in \mathbb{R}^3$ und $\beta, \gamma \in \mathbb{R}$ ist

$$\{\ x \in \mathbb{R}^3 \mid \langle b, x\rangle = \beta \wedge \langle c, x\rangle = \gamma\ \}$$

eine Gerade im $\mathbb{R}^3$, deren Richtungsvektor auf b und c senkrecht steht. Damit ist dann auch gezeigt, dass in $(*)$ das Gleichheitszeichen steht: Aus der linearen Unabhängigkeit von (b, c) folgt, dass b und c ungleich 0 sind.

Sei etwa $b_1 \neq 0$. Wir multiplizieren die Gleichung $\langle b, x \rangle = \beta$ mit c_1 und die Gleichung $\langle c, x \rangle = \gamma$ mit b_1 ,

$$b_1c_1x_1 + b_2c_1x_2 + b_3c_1x_3 \quad = \quad c_1\beta \quad ,$$

$$b_1c_1x_1 + b_1c_2x_2 + b_1c_3x_3 \quad = \quad b_1\gamma \quad ,$$

und subtrahieren:

$$(b_2c_1 - b_1c_2)x_2 \; + \; (b_3c_1 - b_1c_3)\, x_3 \; = \; c_1\beta - b_1\gamma \quad .$$

Angenommen, $b_2c_1 - b_1c_2 \; = \; 0 \; \wedge b_3c_1 - b_1c_3 \; = \; 0 \quad ,$ dann folgt

$$c_2 \; = \; \frac{c_1}{b_1}b_2 \; \wedge c_3 \; = \; \frac{c_1}{b_1}b_3 \, , \text{ sowieso: } c_1 \; = \; \frac{c_1}{b_1}b_1 \quad ,$$

also $c \; = \; \frac{c_1}{b_1}\, b \, ,$ also (b, c) nicht linear unabhängig, Widerspruch. Also ist $b_2c_1 - b_1c_2 \neq 0 \; \vee \, b_3c_1 - b_1c_3 \neq 0 \quad .$ Sei etwa

$$b_2c_1 - b_1c_2 \neq 0 \quad , \quad \text{dann können wir}$$

$$p_3 \; := \; 1 \quad , \quad p_2 \; := \; \frac{c_1\beta - b_1\gamma - b_3c_1 + b_1c_3}{b_2c_1 - b_1c_2} \quad \text{und}$$

$$p_1 \; := \; \frac{1}{b_1}(\beta - b_2p_2 - b_3p_3)$$

wählen, dann ist p eine Lösung von

$$\langle b, p \rangle \; = \; \beta \quad \wedge \quad \langle c, p \rangle \; = \; \gamma \quad .$$

Für jede weitere Lösung x von $\langle b, x \rangle \; = \; \beta \; \wedge \; \langle c, x \rangle \; = \; \gamma$ gilt dann

$$\langle b, x - p \rangle \; = \; 0 \quad \wedge \quad \langle c, x - p \rangle \; = \; 0 \quad ,$$

also ist $y \; := \; x - p$ eine Lösung von

$$(**) \qquad \langle b, y \rangle \quad = \quad \langle c, y \rangle \quad = \quad 0 \quad .$$

Mit derselben Rechnung wie oben folgt

$$(b_2c_1 - b_1c_2)y_2 + (b_3c_1 - b_1c_3)y_3 \quad = \quad 0 \quad .$$

Wenn wir $y_3 \; := \; b_1c_2 - b_2c_1$ setzen, folgt

$$y_2 \; = \; -b_1c_3 + b_3c_1 \quad , \quad \text{und aus} \quad \langle b, y \rangle \; = \; 0 \; :$$

$$b_1y_1 + b_2(-b_1c_3 + b_3c_1) + b_3(b_1c_2 - b_2c_1) \;=\; 0 \quad ,$$

$$b_1y_1 + b_1(c_2b_3 - c_3b_2) \quad = \quad 0 \quad ,$$

$$y_1 \quad = \quad -c_2b_3 + c_3b_2 \quad , \qquad \text{also}$$

$$y \quad = \quad (b_2c_3 - b_3c_2\,,\, -b_1c_3 + b_3c_1\,,\, b_1c_2 - b_2c_1) \quad = \quad b \times c \quad ,$$

und jede andere Lösung von $(**)$ ist ein $\lambda-$faches dieses Vektors, $\lambda \in \mathbb{R}$. Für jede Lösung x von $\langle\, b, x\,\rangle = \beta \wedge \langle\, c, x\,\rangle = \gamma$ gilt

$$x \quad = \quad p + \lambda\,(\,b \times c) \quad , \qquad \text{also}$$

$$\left\{\; x \in \mathbb{R}^3 \;\middle|\; \langle\, b, x\rangle = \beta \wedge \langle\, c, x\,\rangle = \gamma \;\right\} \quad = \quad G_{p,b\times c} \quad .$$

□

Bemerkung 1.6.5 : Sie sehen: Es ist gar nicht von vornherein klar, wie die Lösungsmenge von m Gleichungen mit n Unbekannten im $\mathbb{R}^n$ geometrisch aussieht. Wir werden im Laufe dieses Semesters eine Theorie dafür entwickeln. Das ist auch deshalb sinnvoll, weil wir bei unseren bisherigen Überlegungen oft nur Spezialfälle betrachtet haben, wenn wir gesagt haben:

Sei $b \in \mathbb{R}^3$, $b \neq 0$, dann ist eine der drei Komponenten $\neq 0$.
Sei **etwa** $b_1 \neq 0$, dann folgt $\ldots$.

1.7 Aufgaben

(1.1) Sei $f : M \longrightarrow N$ eine Abbildung. Zeigen Sie:

a) Für alle $A \subset M$ gilt $A \subset \overset{-1}{f}(f(A))$.

b) f ist genau dann injektiv, wenn für alle $A \subset M$ gilt

$$A \quad = \quad \overset{-1}{f}(f(A)) \quad .$$

c) Für alle $B \subset N$ gilt $f(\overset{-1}{f}(B)) \subset B$.

d) f ist genau dann surjektiv, wenn für alle $B \subset N$ gilt

$$B \quad = \quad f(\overset{-1}{f}(B)) \quad .$$

e) Ist f bijektiv, so ist für alle $B \subset N$ das Bild von B unter f^{-1} gleich dem Urbild von B unter f :

$$f^{-1}(B) \quad = \quad \overset{-1}{f}(B) \quad .$$

(1.2) Sei $f : M \longrightarrow N$ eine Abbildung und seien $A, B \subset M$, $C, D \subset N$. Zeigen Sie :

a) $\overset{-1}{f}(C \cup D) = \overset{-1}{f}(C) \cup \overset{-1}{f}(D)$

b) $\overset{-1}{f}(C \cap D) = \overset{-1}{f}(C) \cap \overset{-1}{f}(D)$

c) $f(A \cup B) = f(A) \cup f(B)$

d) $f(A \cap B) \subset f(A) \cap f(B)$

e) Es gilt $\forall\, A, B \subset M : \; f(A \cap B) = f(A) \cap f(B)$
genau dann, wenn f injektiv ist.

f) Geben Sie eine Funktion $f : M \longrightarrow N$ und Teilmengen A, B von M an mit $f(A) \cap f(B) \neq f(A \cap B)$.

(1.3.) Seien L, M, N nichtleere Mengen,

$f : L \longrightarrow M$, $g : M \longrightarrow N$ Funktionen. Zeigen Sie :

a) Sind f und g surjektiv, so ist $g \circ f$ surjektiv.

b) Sind f und g injektiv, so ist $g \circ f$ injektiv.

c) Ist $g \circ f$ surjektiv, so ist g surjektiv .

d) Ist $g \circ f$ injektiv, so ist f injektiv.

(1.4) Seien $c \in \mathbb{R}^2 \setminus \{0\}$, $\alpha \in \mathbb{R}$ und $p \in \mathbb{R}^2$.
Sei $G := \{\; x \in \mathbb{R}^2 \mid < c, x >= \alpha \;\}$.

a) Berechnen Sie den "Fußpunkt f des Lots von p auf G", d.h. den Schnittpunkt der auf G senkrechten Geraden durch p mit G, und damit den "Abstand von p und G", d.h. $\|p - f\|$.

b) Zeigen Sie: Ist G in der Form

$$G = \left\{\; x \in \mathbb{R}^2 \;\middle|\; \langle c, x\rangle = \alpha \;\right\} \quad \text{mit} \quad \|c\| = 1$$

("HESSEsche Normalform")

gegeben, so ist der Abstand von p und G gleich

$$|\, \langle c, p\rangle - \alpha \,| \quad .$$

(1.5) Beweisen Sie, dass für alle $a, b \in \mathbb{R}^2$, $\lambda \in \mathbb{R}$ gilt:

a) $(a+b)^\perp = a^\perp + b^\perp$, $(\lambda a)^\perp = \lambda \cdot a^\perp$,

b) $\langle a, a^\perp\rangle = 0$, $\langle a, b^\perp\rangle = -\langle a^\perp, b\rangle$,

c) $\|a^\perp\| = \|a\|$, d) $(a^\perp)^\perp = -a$.

(1.6) Seien $a, b, c\,\mathbb{R}^2$ mit $a \neq b$, $c \notin G_{a,b-a}$ gegeben. Als "Höhen im Dreieck (a, b, c)" bezeichnet man die Geraden durch die Punkte $a, b, c,$ die auf den Geraden durch die anderen beiden Punkte senkrecht stehen. Zeigen Sie, dass sich die drei Höhen in genau einem Punkt h schneiden, und geben Sie eine Formel zur Berechnung dieses "Höhenschnittpunkts" an.

(1.7) Sei $m \in \mathbb{R}^2$ und $r \in \mathbb{R}$, $r > 0$, dann heißt

$$K \quad := \quad \{\ x \in \mathbb{R}^2 \mid \|x - m\| = r\ \}$$

der "Kreis mit Mittelpunkt m und Radius r". Zeigen Sie:

a) Sei $p \in \mathbb{R}^2$ mit $\|p - m\| < r$. Sei S eine Gerade durch p. Dann gibt es genau zwei Schnittpunkte a_S, b_S von S mit K, und das Produkt

$$\|a_S - p\| \cdot \|b_S - p\|$$

hängt nicht von S ab. ("Zwei-Sehnen-Satz").

b) Sei $p \in \mathbb{R}^2$ mit $\|p - m\| > r$. Sei S eine Gerade durch p, die zwei Schnittpunkte a_S, b_S mit K hat, und T eine Gerade durch p, die K in genau einem Punkt q schneidet. Dann gilt

$$\|a_S - p\| \cdot \|b_S - p\| \quad = \quad \|q - p\|^2 .$$

("Sehnen-Tangenten-Satz").

(1.8) Seien $p, q, a, b \in \mathbb{R}^3$ und (a, b) linear unabhängig. Berechnen Sie, analog zu Aufgabe (1.4), den Abstand d des Punktes q von der Ebene $E_{p,a,b}$.

(1.9) Sei $P(x, y)$ das für ganze Zahlen x, y definierte zweistellige Prädikat

$$x \leq y \quad .$$

Zeigen Sie an diesem Beispiel, dass in Regel 1.2.5 (9) in der Mitte kein $\Longleftrightarrow$ stehen kann.

§2 Gruppen

2.1 Allgemeines

Definition 2.1.1 : Sei H eine nichtleere Menge und τ eine **Verknüpfung** auf H , d.h. eine Abbildung

$$\tau \; : \; H \times H \; \longrightarrow \; H \quad , \quad (x,y) \longmapsto x\tau y \quad .$$

Wenn die Aussage
(G1) $\forall\, x,y,z \in H \; : \; x\tau(y\tau z) = (x\tau y)\tau z$ (Assoziativgesetz)
gilt, dann heißt H (genauer: das Paar (H,τ)) eine **Halbgruppe** .

Definition 2.1.2 : Sei G eine nichtleere Menge und τ eine Verknüpfung auf G , d.h. eine Abbildung

$$\tau \; : \; G \times G \; \longrightarrow \; G \quad , \quad (x,y) \longmapsto x\tau y \quad .$$

Wenn die Aussagen
(G1) $\forall\, x,y,z \in G \; : \; x\tau(y\tau z) = (x\tau y)\tau z$ (Assoziativgesetz)
(G2) $\exists\, e \in G \forall\, x \in G \; : \; e\tau x = x$ (Existenz eines linksneutralen Elements)
(G3) $\forall\, x \in G \exists\, x^* \in G \; : \; x^*\tau x = e$ (Existenz eines Linksinversen)
richtig sind, dann heißt G (genauer: das Paar (G,τ)) eine **Gruppe** .
Wenn zusätzlich
(G4) $\forall\, x,y \in G \; : \; x\tau y = y\tau x$ (Kommutativgesetz)
gilt, heißt (G,τ) eine **abelsche (kommutative) Gruppe** .

□

Jede Gruppe ist also auch eine Halbgruppe.

Bemerkung 2.1.3 : In Def. 2.1.1 steht mit Absicht möglichst Wenig, damit man wenig Arbeit hat, wenn man nachweisen will, dass eine gegebene Menge G mit einer Verknüpfung τ eine Gruppe ist. Tatsächlich folgt aus (G1) - (G3) mehr:

Folgerung 2.1.4 : Sei (G,τ) eine Gruppe, e ein linksneutrales Element. Dann gilt für alle $x,y \in G$:
(a) Wenn $x^* \in G$ ist mit $x^*\tau x = e$, dann ist auch $x\tau x^* = e$.
(b) $x\tau e = x$.
(c) Sei $f \in G$ mit $\forall\, a \in G : f\tau a = a$, dann ist $f = e$.
Das linksneutrale Elementist also eindeutig bestimmt, und wegen (b) es ist auch rechtsneutral. Man spricht daher von **dem neutralen Element** von

(G, τ) .
(d) $\exists_1 x^* \in G : \; x^* \tau x = e$, und es gilt auch

$$x \tau x^* = e \quad . \quad x^* \text{ heißt daher } \underline{\textbf{das Inverse}} \text{ von } x,$$

und wir schreiben meist x^{-1} statt x^*.
(e) $e^* = e$.
(f) Es gelten die **Kürzungsregeln** :

$$\forall\, a \in G : (a\tau x = a\tau y \Longrightarrow x = y \quad \wedge \quad x\tau a = y\tau a \Longrightarrow x = y) .$$

(g) $\exists_1 a \in G : \; x\tau a = y \quad \wedge \quad \exists_1 b \in G : \; b\tau x = y$.
(h) $\forall\, x, y \in G : ((x^{-1})^{-1} = x \quad \wedge \quad (x\tau y)^{-1} = y^{-1}\tau x^{-1})$.
Beweis : (a) Wegen (G3) hat man $(x^*)^* \in G$ mit $(x^*)^* \tau x^* = e$, also

$$x\tau x^* \overset{(G2)}{=} e\tau(x\tau x^*) = ((x^*)^*\tau x^*)\tau(x\tau x^*) = (x^*)^*\tau(x^*\tau(x\tau x^*))$$

$$= (x^*)^*\tau((x^*\tau x)\tau x^*) = (x^*)^*\tau(e\tau x^*) = (x^*)^*\tau x^* = e \; .$$

(b) $x\tau e \overset{(G3)}{=} x\tau(x^*\tau x) \overset{(G1)}{=} (x\tau x^*)\tau x \overset{(a)}{=} e\tau x = x.$

(c) $e = f\tau e \overset{(b)}{=} f.$

(d) Seien x^* und x' Linksinverse von x , dann gilt

$$x^* = e\tau x^* = (x'\tau x)\tau x^* = x'\tau(x\tau x^*) \overset{(a)}{=} x'\tau e \overset{(b)}{=} x' \; ,$$

das Linksinverse x^* zu x ist also eindeutig bestimmt, und nach (a) auch rechtsneutral.
(e) $e\tau e \overset{(G2)}{=} e$ und $e^*\tau e \overset{(G3)}{=} e$. Nach (d) folgt $e = e^*$.
(f) Aus $a\tau x = a\tau y$ folgt

$$a^*\tau(a\tau x) = a^*\tau(a\tau y), \quad \text{und mit (G1) :}$$

$$(a^*\tau a)\tau x = (a^*\tau a)\tau y; \quad \text{und mit (G3) :}$$

$$e\tau x = e\tau y, \quad \text{also mit (G2) :} \quad x = y.$$

Entsprechend zeigt man die zweite Implikation, wobei man noch (d) braucht.
(g) Setzen wir $a := x^*\tau y$, so folgt

$$x\tau a = x\tau(x^*\tau y) = (x\tau x^*)\tau y = e\tau y = y.$$

Zum Beweis der zweiten Aussage setzt man $b := y\tau x^*$. Dass a und b eindeutig bestimmt sind, folgt aus (f).
(h) Wegen (d) haben wir

$$x^{-1}\tau x = x\tau x^{-1} = e \quad ,$$

und da das Inverse eindeutig bestimmt ist, ist x das Inverse von x^{-1}, also $(x^{-1})^{-1} = x$. Für $x, y \in G$ gilt

$$(y^{-1}\tau x^{-1})\tau(x\tau y) = (y^{-1}\tau(x^{-1}\tau x))\tau y = (y^{-1}\tau e)\tau y = y^{-1}\tau y = e\,,$$

also folgt (wieder mit (d)) : $(x\tau y)^{-1} = y^{-1}\tau x^{-1}$.

□

In Halbgruppen kann man Potenzen mit Exponenten aus $\mathbb{N}$ definieren, in Gruppen sogar mit Exponenten aus $\mathbb{Z}$:

Definition 2.1.5 : Sei (G, τ) eine Halbgruppe und $x \in G$. Dann definieren wir **Potenzen** von x rekursiv durch

$$x^1 := x\,,$$
$$(*) \quad x^{n+1} := x^n \tau x \quad \text{für} \quad n \in \mathbb{N}\,.$$

Ist (G, τ) eine Gruppe, e ihr neutrales Element, so setzen wir zusätzlich $x^0 := x$ und für $n \in \mathbb{N}$:

$$(**) \quad x^{-n} := (x^{-1})^n\,.$$

Bemerkung 2.1.6 : Beim Beweis von Folgerung 2.1.7 setzen wir die folgende Eigenschaft der ganzen Zahlen als bekannt voraus: Es ist $\mathbb{N}_0 \subset \mathbb{Z}$, und wenn $m \in \mathbb{Z}, m \notin \mathbb{N}_0$ ist, dann ist $-m \in \mathbb{N}$. Also ist

$$\mathbb{Z} = \mathbb{N}_0 \cup \{\ -k \mid k \in \mathbb{N}\ \}\,.$$

Folgerung 2.1.7 : Sei (G, τ) eine Halbgruppe und seien $x, y \in G$, $n, m \in \mathbb{N}$. Dann gilt

(1) $x^n \tau x^m = x^{n+m}$

(2) $(x^n)^m = x^{n \cdot m}$

(3) Wenn $x\tau y = y\tau x$ ist: $(x\tau y)^n = x^n \tau y^n$.

Ist (G, τ) eine Gruppe , so gelten diese Regeln für alle $n, m \in \mathbb{Z}$.

Beweis : (1) a) Sei (G, τ) eine Halbgruppe. Dann beweisen wir (1) durch Induktion nach m :

Induktionsanfang: Sei $n \in \mathbb{N}$ beliebig und $m = 1$: Dann gilt

$$x^n \tau x^1 = x^{n+1} \quad \text{nach Definition } (*).$$

Induktionsschluss: Sei $n \in \mathbb{N}$ beliebig und für m sei (1) richtig (I.V.), dann folgt

$$x^n \tau x^{m+1} \overset{(*)}{=} x^n \tau (x^m \tau x) = (x^n \tau x^m)\tau x \overset{\text{(I.V.)}}{=} x^{n+m}\tau x \overset{(*)}{=} x^{n+m+1}\,.$$

b) Sei nun (G, τ) eine Gruppe und $x \in G$.
b_1) Wir zeigen zunächst

$$\forall\, m \in \mathbb{Z} : \;\; x^{m+1} = x^m \tau x.$$

Beweis von b_1) : Für $m \in \mathbb{N}$ ist das die Definition $(*)$. Für $m = -1$ oder $m = 0$ gilt das nach Definition von x^0. Sei $m \in \mathbb{Z}$, $m \leq -2$, dann ist $m = -k$ mit $k \geq 2$, also $k - 1 \in \mathbb{N}$. Nach Def. $(**)$ folgt

$$x^m \tau x = (x^{-1})^{-m} \tau x = (x^{-1})^{-m-1} \tau x^{-1} \tau x = (x^{-1})^{-m-1} = x^{m+1} \quad .$$

b_2) Wir zeigen nun $\forall\, n \in \mathbb{Z} \forall\, m \in \mathbb{N}_0 : \;\; x^n \tau x^m = x^{n+m}$ durch Induktion nach m :
Induktionsanfang: Für $m = 0$ gilt

$$x^n \tau x^0 = x^n \tau e = x^n = x^{n+0} \quad .$$

Induktionsschluss: Sei $m \in \mathbb{N}_0$, und für alle $n \in \mathbb{Z}$ sei $x^n \tau x^m = x^{n+m}$ richtig. Dann folgt

$$x^n \tau x^{m+1} = x^n \tau x^m \tau x = x^{n+m} \tau x \overset{b_1)}{=} x^{n+m+1} \quad .$$

b_3) Wir verwenden b_2) für x^{-1} statt x. Dann haben wir

$$\forall\, n \in \mathbb{Z} \forall\, m \in \mathbb{N}_0 : \;\; (x^{-1})^n \tau (x^{-1})^m = (x^{-1})^{n+m}$$

und nach $(**)$.

$$\forall\, n \in \mathbb{Z} \forall\, m \in \mathbb{N}_0 : \;\; x^{-n} \tau x^{-m} = x^{-(n+m)} \quad .$$

Mit $n \in \mathbb{Z}$ ist auch $-n \in \mathbb{Z}$, und mit $m \in \mathbb{N}_0$ ist $-m \in \mathbb{Z} \setminus \mathbb{N}$, also gilt

$$\forall\, n \in \mathbb{Z} \forall\, m \in \mathbb{Z} \setminus \mathbb{N} : \;\; x^n \tau x^m = x^{-(-(n+m))} = x^{n+m} \quad .$$

c) Mit b_2) und b_3) haben wir gezeigt:

$$\forall\, n \in \mathbb{Z} \forall\, m \in \mathbb{Z} : \;\; x^n \tau x^m = x^{n+m} \quad .$$

(2) und (3) zeigt man ähnlich.

□

(2.1.8) Additive und multiplikative Schreibweise : Häufig haben wir in einer Menge G zwei Verknüpfungen. Dafür kann man dann nicht immer

"τ " schreiben:
a) Schreibt man die Verknüpfung als Addition + , so schreibt man, falls vorhanden,
• für das neutrale Element : 0 , und spricht vom **Nullelement**,
• für das inverse Element eines $x \in M$: $-x$, und spricht vom **Negativen** von x,
• für die $n-$te Potenz von x , $n \in \mathbb{N}$ bzw. $\mathbb{Z}$: nx , und spricht vom $n-$**fachen** von x.
b) Schreibt man die Verknüpfung als Multiplikation $\cdot$, so schreibt man, falls vorhanden,
• für das neutrale Element : 1_G oder einfach 1 , und spricht vom **Einselement**.
• für das Inverse eines $x \in M$: wie bisher, x^{-1} ,
• und für Potenzen von x wie bisher: x^n.

2.2 Untergruppen und Normalteiler

Definition 2.2.1 : Sei $(G, \cdot)$ eine Gruppe. Eine Menge U heißt eine **Untergruppe** von G, wenn gilt
(U1) $U \neq \emptyset$ und $U \subset G$,
(U2) $\forall\, a, b \in U \;:\; a^{-1} \cdot b \in U$.
- Die Definition ist sinnvoll, denn es gilt die
Behauptung 2.2.2 : Sei U eine Untergruppe von $(G, \cdot)$, dann ist U mit der auf U eingeschränkten Verknüpfung $\cdot$ selbst eine Gruppe, mit dem neutralen Element e von G als neutralem Element von U.
Beweis : (1) Wegen $U \neq \emptyset$ gibt es ein Element $a \in U$. Dafür ist nach (U2)

$$a^{-1} \cdot a \in U \quad , \quad \text{also } e \in U \ .$$

Für $a, b \in U$ ist dann nach (U2) auch

$$a^{-1} \;=\; a^{-1} \cdot e \in U \quad , \quad \text{und damit}$$

$$a \cdot b \;=\; (a^{-1})^{-1} \cdot b \in U \ ,$$

also ist die Restriktion von $\cdot$ auf $U \times U$ eine Abbildung von $U \times U$ **nach** U **!** Und die Gruppenaxiome (G1)-(G3) gelten für U .

□

Beispiel (2.2.3) : Sei $(G, \cdot)$ eine Gruppe und $a \in G$ fest. Dann ist

$$< a >:= \{ \;\; a^n \;\; | \;\; n \in \mathbb{Z} \;\; \}$$

eine Untergruppe. $< a >$ heißt die **von a erzeugte zyklische Untergruppe** von G.
Dass $\{ \ a^n \mid n \in \mathbb{Z} \ \}$ eine Untergruppe ist, sieht man leicht mit der Potenzregel (1) aus 2.1.6. Andererseits: Jede Untergruppe U mit $a \in U$ enthält auch $< a >$, denn sie enthält a, a^{-1}, und mit Induktion folgt dann, dass auch alle Potenzen von a in U liegen.

Bemerkung 2.2.4 : Sei U eine Untergruppe von $(G, \cdot)$, dann wird durch

$$a \sim b \quad :\Longleftrightarrow \quad a^{-1} \cdot b \in U$$

eine Äquivalenzrelation in G definiert. Die Äquivalenzklassen sind die Mengen

$$a \cdot U \ := \ \{ \ a \cdot u \ \mid \ u \in U \ \} \ .$$

Die Mengen $a \cdot U$ heißen die **Linksnebenklassen** von G bezüglich U.
Beweis : Es gilt für alle $a, b, c \in G$:
(Ä1) $a \sim a$ wegen $a^{-1} \cdot a \ = \ e \in U$.
(Ä2) Aus $a \sim b$ folgt $a^{-1} \cdot b \in U$, also $(a^{-1} \cdot b)^{-1} \in U$, $b^{-1} \cdot a \in U$, also $b \sim a$.
(Ä3) Aus $a \sim b$ und $b \sim c$ folgt

$a^{-1} \cdot b \in U \quad$ und $\quad b^{-1} \cdot c \in U$, also $a^{-1} \cdot c \ = \ a^{-1} \cdot b \cdot b^{-1} \cdot c \in U \quad$ also $\quad a \sim c \quad .$

Beachten Sie, dass wir hier die (wegen des Assoziativgesetzes (G1) überflüssigen) Klammern weggelassen haben. Sei $\overline{a}$ die Äquivalenzlasse von a , also

$$\overline{a} \ = \ \{ \ b \in G \ \mid \ b \sim a \ \} \ ,$$

und $u \in U$, dann ist $a \cdot u \in \overline{a}$ wegen $a^{-1} \cdot (a \cdot u) \ = \ u \in U$, also $a \cdot U \subset \overline{a}$, und wenn $b \in \overline{a}$ ist, gilt $a \sim b, \quad$ also $\quad u \ := \ a^{-1} \cdot b \in U$, $b \ = \ a \cdot u \in a \cdot U \quad .$

□

(2.2.5) Satz von Lagrange : Sei $(G, \cdot)$ eine endliche Gruppe, d.h die Menge G sei endlich, und U eine Untergruppe von G. Sei $[G : U]$ die Anzahl der Linksnebenklassen von G bezüglich U, dann gilt

$$\#(G) \ = \ [G : U] \cdot \#(U).$$

Beweis : Nach Bemerkung 2.2.4 wird durch

$$a \sim b \quad :\Longleftrightarrow \quad a^{-1} \cdot b \in U \quad \text{für} \quad a, b \in G$$

eine Äquivalenzrelation auf G definiert, wobei die Äquivalenzklassen die Linksnebenklassen $a \cdot U$, $a \in G$ sind, also gilt nach Satz 1.2.7(3) :

$$(*) \qquad G \ = \ \bigcup_{a \in G} a \cdot U \quad .$$

Die Nebenklassen sind endliche Mengen, da sie Teilmengen der endlichen Menge G sind.
(1) Alle Nebenklassen haben die gleiche Mächtigkeit.
Beweis: Wegen $U \subset G$ gibt es ein $m \in \mathbb{N}$ mit $\#(U) = m$. Sei $a \in G$ und

$$f : U \longrightarrow a \cdot U\,,\ f(x) := a \cdot x\,,$$

dann ist f surjektiv nach Definition von $a \cdot U$, und injektiv nach der Kürzungsregel 2.1.4(f), also bijektiv. Also ist auch $\#(a \cdot U) = m$, und zwar für alle $a \in G$ dasselbe m . Alle Nebenklassen haben also die Mächtigkeit $\#(U)$.
(2) Zwei verschiedene Linksnebenklassen haben nach Satz 1.2.7(2) kein Element gemeinsam, und es gilt $(*)$. Es gibt also insgesamt $[G : U]$ Linksnebenklassen, die je $\#(U)$ Elemente enthalten. Also ist

$$\#(G) = [G : U] \cdot \#(U) \quad .$$

□

Anwendung 2.2.6 : Sei $(G, \cdot)$ eine Gruppe. Wenn man die Teilmengen U von G sucht, die Untergruppen von G sind, so kann man sich also auf die Teilmengen U beschränken, für die gilt

$$\exists\, n \in \mathbb{N} : \ \#(G) = n \cdot \#(U) \quad ,$$

man sagt: "Die Mächtigkeit von U ist ein Teiler von $\#(G)$".
Bemerkung 2.2.7 : Sei $(G, \cdot)$ eine Gruppe und U eine Untergruppe, so hat man die Menge

$$G/_U := \{\ a \cdot U \mid a \in G\ \} \quad .$$

Wir fragen uns, ob diese **Menge** $G/_U$ durch die Definition

$$(**) \quad (a \cdot U) \circ (b \cdot U) := (a \cdot b) \cdot U\,, \quad \text{also}$$

$$\overline{a} \circ \overline{b} := \overline{a \cdot b} \quad \text{für} \quad \overline{a} = a \cdot U\,,\ a, b \in G$$

eine Gruppe $(G/_U, \circ)$ wird. Die Frage dabei ist, ob durch

$$\overline{a} \circ \overline{b} := \overline{a \cdot b}$$

überhaupt eindeutig eine Abbildung

$$\circ : \ G/_U \times G/_U \longrightarrow G/_U$$

definiert ist, ob also aus

$$a \cdot U \;=\; a' \cdot U \;\wedge b \cdot U \;=\; b' \cdot U \quad \text{immer}$$

$$(a \cdot b) \cdot U \quad = \quad (a' \cdot b') \cdot U \quad \text{folgt.}$$

Wenn ja, dann sagt man: $\circ$ ist **wohldefiniert** . Wenn die Gruppe $(G, \cdot)$ nicht kommutativ ist, ist das nicht immer der Fall. Man muss von U etwas mehr fordern als nur die Untergruppen-Eigenschaft:
Definition 2.2.8 : Sei $(G, \cdot)$ eine Gruppe und N eine Untergruppe von G. Wenn auch noch

$$\text{(N)} \qquad \forall\, x \in G \,\forall\, u \in N \;:\; \; x \cdot u \cdot x^{-1} \;\in\; N$$

gilt, dann heißt N ein **Normalteiler** in G.
Bemerkung 2.2.9 : Man sieht, dass in einer kommutativen Gruppe jede Untergruppe ein Normalteiler ist!
- Es wird Zeit, einige Beispiele anzugeben:

(2.2.10) Die symmetrische Gruppe

Sei M eine nichtleere Menge. Wir setzen

$$S_M := \{\; f : M \;\longrightarrow\; M \;\mid\; f \text{ ist bijektiv } \} \quad ,$$

Man rechnet nach, dass für $f, g \in S_M$ auch
die Hintereinanderausführung $f \circ g$ und die Umkehrfunktion f^{-1} bijektiv, also Elemente von S_M, sind. Dass die Hintereinanderausführung $\circ$ assoziativ ist, wissen wir aus Satz 1.3.11, und für die in 1.3.9 definierte identische Abbildung id_M gilt

$$\forall\, f \in S_M \;:\; \; f \circ \mathrm{id}_M \;=\; \mathrm{id}_M \circ f \;=\; f \quad .$$

Also ist $(S_M, \circ)$ eine Gruppe, mit id_M als neutralem Element. Sie heißt die **symmetrische Gruppe** von M. Für $\#(M) \geq 3$ ist sie nicht abelsch: Seien a, b, c drei verschiedene Elemente von M und seien

$$f, g \;:\; \; M \;\longrightarrow\; M,$$

$$f(a) \;:=\; b\,,\; f(b) \;:=\; c\,,\; f(c) \;:=\; a \quad , \quad g(a) \;:=\; b\,,\; g(b) \;:=\; a\,,\; g(c) \;:=\; c$$

und $f(x) \;:=\; g(x) \;:=\; x \quad$ für $\quad x \notin \{a, b, c\}$, dann gilt

$$(f \circ g)(c) \;=\; f(c) \;=\; a \quad , \quad (g \circ f)(c) \;=\; g(a) \;=\; b \quad ,$$

also $f \circ g \neq g \circ f$.
Wenn M eine unendliche Menge ist, ist auch S_M unendlich. Uns interessieren mehr die endlichen Gruppen, die man bekommt, wenn man

$$M := \underline{n} \quad \text{für} \quad n \in \mathbb{N}$$

nimmt. Wir schreiben dann S_n statt $S_{\underline{n}}$ und nennen die Elemente dieser Gruppe **Permutationen der Menge $\underline{n}$** . Im Zusammenhang mit Determinanten werden wir uns noch ausführlich mit diesen Gruppen beschäftigen. Wir beginnen mit

Beispiel (2.2.11) : Die Gruppe S_3

Wie gesagt, ist sie nicht kommutativ. Wir werden gleich Bezeichnungen für ihre Elemente einführen, deren Sinn sich in (2.2.13) erschließen wird. Wir definieren hier mal die Permutationen $(1,2,3)$, $(1,3,2)$, $(1,2)$, $(1,3)$, $(2,3)$ (das sollen jetzt keine Tripel bzw. Paare ganzer Zahlen, sondern Bezeichnungen für Permutationen sein) durch

$$(1,2,3) : \; 1 \mapsto 2\,,\; 2 \mapsto 3\,,\; 3 \mapsto 1\,,$$

$$(1,3,2) : \; 1 \mapsto 3\,,\; 2 \mapsto 1\,,\; 3 \mapsto 2\,,$$

$$(1,2) : \; 1 \mapsto 2\,,\; 2 \mapsto 1\,,\; 3 \mapsto 3\,,$$

$$(1,3) : \; 1 \mapsto 3\,,\; 2 \mapsto 2\,,\; 3 \mapsto 1\,,$$

$$(2,3) : \; 1 \mapsto 1\,,\; 2 \mapsto 3\,,\; 3 \mapsto 2 \quad .$$

Zusammen mit $\mathrm{id}_{\underline{3}}$ sind das alle Permutationen von $\underline{3}$. Die Verknüpfung $\circ$ schreibt man sich am besten in einer **Gruppentafel** auf: Seien $a, b \in S_3$. In die linke Spalte schreibt man das a von $a \circ b$, in die obere Zeile das b, und in die Kreuzung der Zeile von a und der Spalte von b die Hintereinanderausführung $a \circ b$:

$\circ$	$\mathrm{id}_{\underline{3}}$	(1,2,3)	(1,3,2)	(1,2)	(1,3)	(2,3)
$\mathrm{id}_{\underline{3}}$	$\mathrm{id}_{\underline{3}}$	(1,2,3)	(1,3,2)	(1,2)	(1,3)	(2,3)
(1,2,3)	(1,2,3)	(1,3,2)	$\mathrm{id}_{\underline{3}}$	(1,3)	(2,3)	(1,2)
(1,3,2)	(1,3,2)	$\mathrm{id}_{\underline{3}}$	(1,2,3)	(2,3)	(1,2)	(1,3)
(1,2)	(1,2)	(2,3)	(1,3)	$\mathrm{id}_{\underline{3}}$	(1,3,2)	(1,2,3)
(1,3)	(1,3)	(1,2)	(2, 3)	(1,2, 3)	$\mathrm{id}_{\underline{3}}$	(1,3,2)
(2,3)	(2,3)	(1,3)	(1,2)	(1,3,2)	(1,2,3)	$\mathrm{id}_{\underline{3}}$

(a) Wegen Anwendung (2.2.6) wissen wir, dass eine Untergruppe U von $(S_3, \circ)$ nur

$$1, 2, 3 \quad \text{oder} \quad 6$$

Elemente enthalten kann. Mit 1 bzw. 6 Elementen haben wir die
trivialen Untergruppen

$$\{\,\mathrm{id}_{\underline{3}}\} \quad \text{bzw.} \quad S_3 \quad .$$

Aus der Gruppentafel sehen wir, dass

$$U_3 := \{\,\mathrm{id}_{\underline{3}}, (1,2)\} \quad , \quad U_2 := \{\,\mathrm{id}_{\underline{3}}, (1,3)\} \quad , \quad U_1 := \{\,\mathrm{id}_{\underline{3}}, (2,3)\}$$

Untergruppen mit zwei Elementen sind, und zwar die einzigen. Und

$$V := \{\,\mathrm{id}_{\underline{3}}, (1,2,3), (1,3,2)\}$$

ist die einzige Untergruppe mit drei Elementen.
(b) Nehmen wir mal die Untergruppe U_3 und bilden einige Linksnebenklassen:

$$(1,2,3) \circ U_3 \;=\; (1,3) \circ U_3 \;=\; \{(1,2,3), (1,3)\} \quad ,$$
$$(1,3,2) \circ U_3 \;=\; (2,3) \circ U_3 \;=\; \{(1,3,2), (2,3\} \quad .$$

Aber: Es ist

$$((1,2,3) \circ (1,3,2)) \circ U_3 \;=\; \mathrm{id}_{\underline{3}} \circ U_3 \;=\; \{(1,2),\, \mathrm{id}_{\underline{3}}\} \quad ,$$

$$((1,3) \circ (2,3)) \circ U_3 \;=\; (1,3,2) \circ U_3 \;=\; \{(1,3,2), (2,3)\} \quad ,$$

man sieht, dass durch $(**)$ in (2.2.7) keine eindeutige Verknüpfung in S_3/U_3 definiert ist!

(c) Für die Untergruppe V kann man anhand der Gruppentafel nachrechnen:

$$\forall\, x \in S_3\, \forall\, v \in V \;:\; \; x \circ v \circ x^{-1} \in V \quad ,$$

V ist also ein Normalteiler in S_3 . Man hat zwei verschiedene Linksnebenklassen

$$\mathrm{id}_{\underline{3}} \circ V \;=\; V \quad \text{und} \quad (1,2) \circ V \;=\; \{(1,2), (2,3), (1,3)\} \quad .$$

Satz und Definition 2.2.12: Sei $(G, \cdot)$ eine Gruppe und N ein Normalteiler in G. Dann wird die Menge der Linksnebenklassen

$$G/_N \;=\; \{\;\; a \cdot N \;\mid\; a \in G \;\;\} \qquad \text{mit der durch}$$

$(**)$ $\qquad (a{\cdot}N) \circ (b{\cdot}N) \quad := \quad (a{\cdot}b){\cdot}N \quad \text{für} \quad a, b \in G$

definierten Verknüpfung $\circ$ eine Gruppe, genannt die
Faktorgruppe von G modulo N . Die Nebenklasse N $(= e \cdot N$, wenn e

das neutrale Element von G ist,) ist das neutrale Element von $(G/_N, \circ)$
Bemerkung : Das Zeichen $\circ$ bedeutet hier nicht, wie in (2.2.10)und (2.2.11), die Hintereinanderausführung von Funktionen, sondern ist nur ein Zeichen für eine von $\cdot$ verschiedene Verknüpfung (und wir werden später auch dafür wieder $\cdot$ schreiben, wenn keine Verwechslungen zu befürchten sind).

Beweis : (1) Wir zeigen, dass durch $(**)$ eindeutig eine Verknüpfung $\circ$ auf $G/_N$ definiert ist: Seien $a, a', b, b' \in G$ und

$$a \cdot N = a' \cdot N \quad \text{und} \quad b \cdot N = b' \cdot N \quad , \quad \text{dann gilt}$$

$$a \in a' \cdot N \quad \text{und} \quad b \in b' \cdot N \quad , \qquad \text{also}$$

$$\exists\, u \in N : a = a' \cdot u \quad \wedge \quad \exists\, v \in N : b = b' \cdot v \quad , \qquad \text{also} \quad \forall\, w \in N :$$

$$a \cdot b \cdot w = (a' \cdot u) \cdot (b' \cdot v) \cdot w = a' \cdot u \cdot b' \cdot v \cdot w \quad .$$

$$= a' \cdot b' \cdot (b')^{-1} \cdot u \cdot b' \cdot v \cdot w \quad .$$

Nach Definition des Normalteilers (angewendet auf $(b')^{-1} \in G$ und $u \in N$) gibt es ein $u' \in U$ mit

$$(b')^{-1} \cdot u \cdot b' = u' \quad , \qquad \text{also}$$

$$a \cdot b \cdot w = a' \cdot b' \cdot u' \cdot v \cdot w \quad , \qquad \text{mit} \quad u' \cdot v \cdot w \in U \quad , \qquad \text{also}$$

$$a \cdot b \cdot w \in a' \cdot b' \cdot N \quad .$$

Also ist $(a \cdot b) \cdot N \subset (a' \cdot b') \cdot N$, und ebenso zeigt man $(a' \cdot b') \cdot N \subset (a \cdot b) \cdot N$, die beiden Nebenklassen sind also gleich. Durch $(**)$ ist also eindeutig eine Verknüpfung $\circ$ auf $G/_N$ definiert.
(2) Die Gültigkeit des Assoziativgesetzes in $(G/_N, \circ)$ folgt aus der Def. $(**)$ und dem Assoziativgesetz in $(G, \cdot)$. Ist e das neutrale Element von $(G, \cdot)$, so ist

$$e \cdot N \quad = \quad N$$

das neutrale Element von $(G/_N, \circ)$, und zu $x \cdot N \in G/_N$ ist $x^{-1} \cdot N$ das Inverse.

□

- Wir wollen uns noch einmal mit der in Beispiel (2.2.11) verwendeten Schreibweise beschäftigen, damit Sie sehen, was es mit Bezeichnungen wie "(1,3,2)" oder "(2,3)" auf sich hat, und um weitere Beispiele angeben zu können:
(2.2.13) Schreibweise von Permutationen : Sei $n \in \mathbb{N}$, $n \geq 2$. Ein

$\sigma \in S_n$ kann man dadurch angeben, dass man für $1, \ldots, n$ die Funktionswerte hinschreibt, wie in (2.2.11) :

$$\sigma \; : \; 1 \mapsto \sigma(1), \ldots, n \mapsto \sigma(n) \quad .$$

Das ist ziemlich viel Schreibarbeit. Einfacher ist es, man schreibt nur eine Zeile hin, beginnend mit einer runden Klammer, schreibt eine Zahl $j \in \underline{n}$ hin, dahinter ihren Funktionswert $k := \sigma(j)$, also

$(j, k, \ldots \quad ,$

danach $\sigma(k)$ usw. Irgendwann wird ein l mit $\sigma(l) = j$ auftreten, dann schließt man die Klammer :

$(j, k, \ldots, l) \quad .$

Z.B. ist $(1, 3, 4)$ eine Abkürzung für

$$\sigma : 1 \mapsto 3 \, , \, 3 \mapsto 4 \, , \, 4 \mapsto 1 \quad , \quad \sigma \in S_4 \quad ,$$

wenn man vereinbart, dass Zahlen, die nicht in der Klammer auftauchen, auf sich selbst abgebildet werden. Wir formulieren das etwas genauer:

Definition 2.2.14 : Eine Permutation $\sigma \in S_n$ heißt ein **Zyklus**, wenn es eine Teilmenge $\{a_1, \ldots, a_r\} \subset \underline{n}$, $r \geq 1$, gibt, so dass

$\forall \, j \in \underline{r-1} \; : \; \sigma(a_j) = a_{j+1}$,

für $j = r \; : \; \sigma(a_r) = a_1$ und

$\forall \, j \in \underline{n} \setminus \{a_1, \ldots, a_r\} \; : \; \sigma(j) = j$

gilt . Ist $r = 1$, so ist $\sigma = \mathrm{id}_{\underline{n}}$ und man schreibt

$(1) \quad := \quad \mathrm{id}_{\underline{n}} \quad .$

Ist $r > 1$, so schreibt man für σ kurz

$(a_1, a_2, \ldots, a_r) \quad .$

Bemerkungen 2.2.15 : 1) Nicht jedes $\sigma \in S_n$ ist ein Zyklus, sondern i.A. ein Produkt mehrerer Zyklen, z.B. ist

$$\sigma \quad = \quad (1, 2) \circ (3, 4) \in S_4$$

kein Zyklus.

2) Die Zyklenschreibweise ist nicht eindeutig, z.B. ist

$(1, 2, 3) \; = \; (2, 3, 1) \in S_3 \quad .$

3) Mit der Zyklenschreibweise kann man gut rechnen: Etwa in S_3 rechnet man $\sigma := (1, 3, 2) \circ (2, 3)$ so aus: Man nimmt eine Zahl aus $\underline{3}$, etwa 1 , wendet darauf den hinten stehenden Zyklus an, das ergibt in diesem Fall wieder 1 , darauf dan den vorderen Zyklus, das ergibt hier 3, man schreibt

$(1, 3$

hin und wiederholt das Spiel mit 3 : Der hintere Zyklus,angewendet auf 3 , ergibt 2 , der vordere, angewendet auf 2 , ergibt 1 . Das hatten wir schon, man schließt die Klammer:

$$(1,3)$$

Zur Probe kann man noch nachrechnen, dass $\sigma(2) = 2$ ist. Also ist $\sigma = (1,3)$. Es kann sein, dass weitere Zyklen hinzukommen (bei S_n mit $n \geq 4$).

Beispiel (2.2.16) : Die Gruppe V_4

In der Gruppe $(S_4, \circ)$ sei $V_4 := \{e, a, b, c\}$ mit

$$e := \mathrm{id}_{\underline{4}}\,,\ a := (1,2) \circ (3,4)\,,\ b := (1,3) \circ (2,4)\,,\ c := (1,4) \circ (2,3)\,,$$

dann rechnen wir folgende Produkte aus:

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

Man sieht aus dieser Tabelle: Für alle $x, y \in V_4$ gilt

$$x^{-1} = x \quad \text{und} \quad x \cdot y \in V_4 \quad .$$

Also ist V_4 eine Untergruppe von S_4, also $(V_4, \circ)$ eine Gruppe und obige Tabellle die Gruppentafel von $(V_4, \circ)$. $(V_4, \circ)$ heißt die
Kleinsche Vierergruppe .

Beispiel (2.2.17) : Die zyklischen Gruppen Z_n

Sei $n \in \mathbb{N}$, $n \geq 2$. Wir nehmen die Gruppe $(S_n, \circ)$ und darin die Permutation

$$\alpha := (1, 2, \ldots, n) \quad ,$$

jede Zahl aus $\underline{n}$ wird also auf die folgende abgebildet, und n auf 1 . Führt man die Permutation α genau n mal aus, so erhält man die identische Abbildung $\mathrm{id}_{\underline{n}}$, und n ist die kleinste Zahl $k \in \mathbb{N}$ mit $\alpha^k = \mathrm{id}_{\underline{n}}$. Die von α erzeugte zyklische Untergruppe

$$< \alpha >= \left\{ \ \alpha^j \ \middle| \ j \in \underline{n} \ \right\}$$

bezeichnen wir mit Z_n und nennen $(Z_n, \circ)$ die
zyklische Gruppe mit n Elementen .

- Um das etwas deutlicher zu machen, nehmen wir $n := 4$:

Beispiel (2.2.18): Die zyklische Gruppe Z_4

In S_4 nehmen wir

$$\alpha := (1,2,3,4) \quad , \quad \text{dann ist}$$

$$\alpha^2 = (1,3) \circ (2,4) \quad , \quad \alpha^3 = (1,4,3,2) \quad , \quad \alpha^4 = \mathrm{id}_{\underline{4}} \quad .$$

Wir schreiben uns die Gruppentafel von $(Z_4, \circ)$ auf:

$\circ$	$\mathrm{id}_{\underline{4}}$	α	α^2	α^3
$\mathrm{id}_{\underline{4}}$	$\mathrm{id}_{\underline{4}}$	α	α^2	α^3
α	α	α^2	α^3	$\mathrm{id}_{\underline{4}}$
α^2	α^2	α^3	$\mathrm{id}_{\underline{4}}$	α
α^3	α^3	$\mathrm{id}_{\underline{4}}$	α	α^2

Wir sehen einen wesentlichen Unterschied zur Gruppentafel von V_4 in (2.2.16): Beide Gruppen bestehen aus 4 Elementen. In V_4 ist das Quadrat jedes Elements gleich dem neutralen Element, in Z_4 gilt das nur für zwei Elemente. Und in V_4 gilt

$$\forall\, x \in V_4 \,:\, < x > \neq V_4 \quad ,$$

wir sagen: V_4 ist keine **zyklische Gruppe** . Solche Unterschiede werden im nächsten Abschnitt deutlicher:

2.3 Homomorphismen von Gruppen

Definition 2.3.1 : Seien $(G, \cdot)$ und $(H, \circ)$ Halbgruppen. Eine Abbildung

$$\varphi \,:\, G \longrightarrow H$$

heißt ein **Homomorphismus** von $(G, \cdot)$ in $(H, \circ)$ wenn gilt

$$\forall\, x, y \in G \,:\, \varphi(x \cdot y) = \varphi(x) \circ \varphi(y) \quad .$$

Zusatz 2.3.2 : Ein Homomorphismus der Halbgruppe $(G, \cdot)$ in die Halbgruppe $(H, \circ)$ heißt ein

Endomorphismus , wenn $(G, \cdot) = (H, \circ)$,
Monomorphismus , wenn φ injektiv,
Epimorphismus, wenn φ surjektiv,
Isomorphismus, wenn φ bijektiv,
Automorphismus, wenn φ bijektiv und $(G, \cdot) = (H, \circ)$ ist.

□

(2.3.3) Beispiele :(1) Seien $(G,\cdot)$ und $(H,\circ)$ Gruppen, e_H das neutrale Element von H , dann ist

$$\varphi : \ G \ \longrightarrow \ H \quad , \quad x \mapsto e_H$$

ein Homomorphismus.
(2) Sei $(G,\cdot)$ eine Gruppe, $a \in G$ ein festes Element, dann ist

$$\varphi_a : \ G \ \longrightarrow \ G \quad , \quad x \mapsto a \cdot x \cdot a^{-1}$$

ein Automorphismus von $(G,\cdot)$. Falls $(G,\cdot)$ abelsch oder a das neutrale Element von $(G,\cdot)$ ist, ist $\varphi_a = \mathrm{id}_G$. - Das ist Übungsaufgabe (2.5 b)!
(3) Ein Beispiel aus der Analysis: Sei $(\mathbb{R},+)$ die additive Gruppe der reellen Zahlen und $(\mathbb{R}_+^*,\cdot)$ mit

$$\mathbb{R}_+^* := \ \{ \ x \in \mathbb{R} \ \mid \ x > 0 \ \}$$

die multiplikative Gruppe der positiven reellen Zahlen, dann ist die Exponentialfunktion

$$\exp : \ \mathbb{R} \ \longrightarrow \ \mathbb{R}_+^*$$

ein Isomorphismus der Gruppe $(\mathbb{R},+)$ in $(\mathbb{R}_+^*,\cdot)$.
(4) Sei $(G,\cdot)$ eine Gruppe, N ein Normalteiler in $(G,\cdot)$ und $(G/_N,\circ)$ die Faktorgruppe von G modulo N. Da wir

$$(a \cdot N) \circ (b \cdot N) \quad := \quad (a \cdot b) \cdot N \quad \text{für} \quad a,b \in G$$

definiert hatten, ist die surjektive Abbildung

$$\kappa_N : \ G \ \longrightarrow \ G/_N \quad , \quad a \mapsto a \cdot N$$

ein Epimorphismus von Gruppen. κ_N heißt der
kanonische Nebenklassenepimorphismus von G auf $G/_N$. ("kanonisch" bedeutet: "naheliegend").

□

Satz 2.3.4 : Seien $(G,\cdot)$ und $(H,\circ)$ Gruppen, mit neutralen Elementen e_G bzw. e_H , und

$$\varphi : \ G \ \longrightarrow \ H$$

ein Homomorphismus von $(G,\cdot)$ in $(H,\circ)$. Dann gilt
(1) $\varphi(e_G) = e_H$,
(2) $\forall\, x \in G : \ \varphi(x^{-1}) = (\varphi(x))^{-1}$,

(3) $\forall\, x \in G \forall\, n \in \mathbb{Z} :\ \varphi(x^n) = (\varphi(x))^n \quad .$
Beweis : (1) Es ist $e_G \circ e_G = e_G$, also

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

Mit der Kürzungsregel (2.1.4)(f) folgt

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

(2) $\varphi(x) \circ \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(e_G) \overset{(1)}{=} e_H$, also ist $\varphi(x^{-1})$ das (eindeutig bestimmte) Inverse von $\varphi(x)$ in der Gruppe $(H, \circ)$, also

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

(3) Für $n = 0$ ist das Regel (1).
(a) Sei $n \in \mathbb{N}$, dann machen wir Induktion nach n : Für $n = 1$ gilt

$$\varphi(x^1) = \varphi(x) = (\varphi(x))^1 \quad .$$

Sei $n \in \mathbb{N}$ und für n sei (3) richtig, dann folgt

$$\varphi(x^{n+1}) = \varphi(x^n \cdot x) = \varphi(x^n) \circ \varphi(x) = (\varphi(x))^n \circ \varphi(x) = (\varphi(x))^{n+1} \quad ,$$

wobei wir die Definition 2.1.5$(*)$ der Potenzen in den Gruppen $(G, \cdot)$ und $(H, \circ)$ verwendet haben.
(b) Für negative Exponenten $-n$, $n \in \mathbb{N}$ erhalten wir nach (2.1.5)$(**)$ und (a) :

$$\varphi(x^{-n}) \overset{(**)}{=} \varphi((x^{-1})^n) \overset{(a)}{=} (\varphi(x^{-1}))^n \overset{(2)}{=} ((\varphi(x))^{-1})^n \overset{(**)}{=} \varphi(x)^{-n} .$$

□

(2.3.5) Sprechweise : Seien $(G, \cdot)$ und $(H, \circ)$ Gruppen. Es gebe einen Isomophismus der beiden Gruppen

$$\varphi :\ G \longrightarrow H \quad ,$$

dann haben wir wegen der Bijektivität von φ die Umkehrfunktion

$$\varphi^{-1} :\ H \longrightarrow G \quad .$$

Sie ist auch ein Gruppen-Homomorphismus, denn seien $x, y \in H$, dann gibt es $a, b \in G$ mit $\varphi(a) = x$, $\varphi(b) = y$, also $a = \varphi^{-1}(x)$, $b = \varphi^{-1}(y)$, und wir erhalten

$$\varphi^{-1}(x \circ y) = \varphi^{-1}(\varphi(a) \circ \varphi(b)) = \varphi^{-1}(\varphi(a \cdot b)) = a \cdot b = \varphi^{-1}(x) \cdot \varphi^{-1}(y) .$$

Man kann daher sagen : $(G,\cdot)$ **ist isomorph zu** $(H,\circ)$ und schreiben : $G \cong H$. Für Gruppen $(G,\cdot),(H,\circ)$ und (L,τ) hat man dann die Aussagen
(Ä1) $G \cong G$,
(Ä2) $G \cong H \implies H \cong G$,
(Ä3) $G \cong H \ \wedge \ H \cong L \implies G \cong L$,
wie bei einer Äquivalenzrelation, aber man kann nicht sagen, dass $\cong$ eine Äquivalenzrelation ist, da die "Menge aller Gruppen" nicht existiert! Man kann nicht beliebige Objekte zu einer Menge zusammenfassen, das führt zu logischen Widersprüchen.

□

(2.3.6) Beispiel : Die Gruppen $(V_4,\circ)$ und $(Z_4,\circ)$ sind nicht isomorph!
Die beiden Mengen V_4 und Z_4 haben jeweils vier Elemente, es gibt also eine bijektive Abbildung von V_4 auf Z_4. Aber angenommen,

$$\varphi : \ Z_4 \ \longrightarrow \ V_4$$

ist ein Isomorphismus der **Gruppen** $(Z_4,\circ)$ und $(V_4,\circ)$, dann gilt nach Satz 2.3.4 (1) :

$$\forall\, x \in V_4 : \ \varphi(x^2) \ \overset{(2.1.6)}{=} \ \varphi(\,\mathrm{id}_{\underline{4}}) \ = \ \mathrm{id}_{\underline{4}} \quad ,$$

also für das in (2.2.17) definierte $\alpha \in Z_4$:

$$\exists\, y \in V_4 : \ \alpha \ = \ \varphi(y) \quad \text{und damit} \quad \alpha^2 \ = \ (\varphi(y))^2 \ = \ \varphi(y^2) \ = \ \varphi(\,\mathrm{id}_{\underline{4}}) \ = \ \mathrm{id}_{\underline{4}}\,,$$

was nach der Tabelle in (2.2.18) falsch ist.

Definition und Satz 2.3.7 : Seien $(G,\cdot)$ und $(H,\circ)$ Gruppen, mit neutralen Elementen e_G bzw. e_H , und $\varphi : \ G \ \longrightarrow \ H$ ein Homomorphismus von G nach H. Dann heißt

$$\ker\,\varphi \quad := \quad \{ \ x \in G \ \mid \ \varphi(x) \ = \ e_H \ \}$$

der **Kern** des Homomorphismus φ . $\ker\,\varphi$ ist ein Normalteiler in $(G,\cdot)$.
Beweis : Es ist $\ker\,\varphi \subset G$ nach Definition und $e_G \in \ker\,\varphi$ nach 2.3.4 (1), also $\ker\,\varphi \neq \emptyset$. Seien $a,b \in \ker\,\varphi$, dann gilt nach (2.3.4) (2) :

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

also ist $\ker\,\varphi$ eine Untergruppe von G. Sei $x \in G$ und $a \in \ker\,\varphi$, dann gilt

$$\varphi(x{\cdot}a{\cdot}x^{-1}) = \varphi(x){\circ}\varphi(a){\circ}\varphi(x^{-1}) = \varphi(x){\circ}e_H{\circ}(\varphi(x))^{-1} = \varphi(x){\circ}(\varphi(x))^{-1} = e_H\,,$$

also $x \cdot a \cdot x^{-1} \in \ker \varphi$. Also ist $\ker \varphi$ ein Normalteiler in G .

□

Bemerkung (2.3.8) : Seien M und N **Mengen** und $f : M \longrightarrow N$, und will man zeigen, dass f injektiv ist, so muss man

$$\forall\, a, b \in M : \ (f(a) = f(b) \quad \Longrightarrow \quad a = b)$$

zeigen. Hat man einen **Gruppenhomomorphismus** $\varphi : G \longrightarrow H$ von zwei Gruppen $(G, \cdot)$ und $(H, \circ)$, mit neutralen Elementen e_G bzw. e_H, so muss man nur

$$\forall\, a \in G : \ (\varphi(a) = e_H \quad \Longrightarrow \quad a = e_G)$$

zeigen, wegen $\varphi(e_G) = e_H$ und des folgenden Satzes:

Satz 2.3.9 : Seien $(G, \cdot)$ und $(H, \circ)$ Gruppen, mit neutralen Elementen e_G bzw. e_H , und $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gilt

$$\varphi \quad \text{ist ein Monomorphismus} \quad \Longleftrightarrow \quad \ker \varphi = \{e_G\} \quad .$$

Beweis : a) Sei φ ein Monomorphismus, also ein injektiver Homomorphismus, und

$$x \in \ker \varphi \quad , \qquad \text{also} \quad \varphi(x) = e_H \overset{(2.3.4)(1)}{=} \varphi(e_G) \quad ,$$

dann folgt $x = e_G$. Also: $\ker \varphi \subset \{e_G\}$, und "$\supset$" folgt aus (2.3.4)(1).
b) Sei $\ker \varphi = \{e_G\}$ und seien $a, b \in G$ mit $\varphi(a) = \varphi(b)$. Dann folgt

$$\varphi(a) \circ (\varphi(b))^{-1} = e_H \quad , \qquad \text{also} \quad \varphi(a \cdot b^{-1}) = e_H \quad , \quad a \cdot b^{-1} \in \ker \varphi \quad ,$$

also $a \cdot b^{-1} = e_G \quad , \quad$ also $a = b$. Also ist φ injektiv.

□

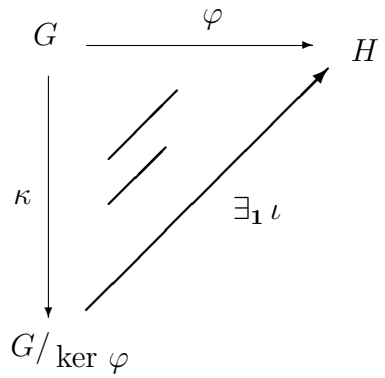
(2.3.10) Homomorphiesatz für Gruppen : Seien $(G, \cdot)$ und (H, τ) Gruppen ,

$$\varphi : G \longrightarrow H \quad \text{ein Epimorphismus von Gruppen.}$$

Sei $\kappa : G \longrightarrow G/_{\ker \varphi} \quad , \quad x \mapsto x \cdot (\ker \varphi)$
der kanonische Nebenklassenepimorphismus von G auf die Faktorgruppe $G/_{\ker \varphi}$, dann gibt es genau einen Gruppen-Isomorphismus

$$\iota : G/_{\ker \varphi} \longrightarrow H \quad \text{mit} \quad \iota \circ \kappa \quad = \quad \varphi \quad .$$

(" $\circ$ " ist hier die Hintereinanderausführung von Abbildungen.) Man sagt, dass das folgende "Diagramm kommutativ" wird:



Beweis : a) Wir zeigen zunächst: Wenn ein Homomorphismus ι mit $\iota \circ \kappa = \varphi$ existiert, so ist ι eindeutig bestimmt: Es gilt dann nämlich für $x \in G$:

$$\iota(x \cdot \ker \varphi) = \iota(\kappa(x)) = (\iota \circ \kappa)(x) = \varphi(x) \quad ,$$

man kann also ι nicht anders als durch

$$(*) \qquad \iota(x \cdot \ker \varphi) \quad := \quad \varphi(x)$$

definieren:
b) Wir definieren ι durch $(*)$. Dann ist ι eindeutig definiert, denn seien $x, x' \in G$ mit $x \cdot \ker \varphi = x' \cdot \ker \varphi$, dann ist $x^{-1} \cdot x' \in \ker \varphi$, also $\varphi(x^{-1} \cdot x') = e_G$, also $\varphi(x) = \varphi(x')$. ι ist ein Gruppenhomomorphismus, denn für

$$x \cdot \ker \varphi \,,\, y \cdot \ker \varphi \in G/_{\ker \varphi} \quad \text{gilt}$$

$$\begin{aligned} \iota((x \cdot \ker \varphi) * (y \cdot \ker \varphi)) &= \iota((x \cdot y) \cdot \ker \varphi) \\ &= \varphi(x \cdot y) = \varphi(x) \tau \varphi(y) = \iota(x \cdot \ker \varphi) \tau\, \iota(y \cdot \ker \varphi) \,. \end{aligned}$$

Hier haben wir mit $*$ die Verknüpfung in der Faktorgruppe $G/_{\ker \varphi}$ bezeichnet. ι ist injektiv nach Satz 2.3.9, denn aus

$$\iota(x \cdot \ker \varphi) = e_H \quad \text{folgt} \quad \varphi(x) = e_H \quad , \qquad \text{also} \quad x \in \ker \varphi \quad ,$$

und damit ist $x \cdot \ker \varphi = \ker \varphi = e_G \cdot \ker \varphi$ das neutrale Element in $(G/_{\ker \varphi}, *)$. Und ι ist surjektiv, weil φ surjektiv ist: Sei $z \in H$, dann gibt es ein $x \in G$ mit $z = \varphi(x)$, also $z = \iota(x \cdot \ker \varphi)$. Die Gleichung $\iota \circ \kappa = \varphi$ folgt aus der Def. $(*)$ von ι .

□

2.4 Aufgaben

(2.1) Sei $(G, \cdot)$ eine Gruppe. Zeigen Sie: Sei $a \in G$, dann ist

$$l_a : G \longrightarrow G \,,\, l_a(x) := a \cdot x$$

bijektiv. Die Abbildung

$$l : G \longrightarrow S_G \quad , \quad a \mapsto l_a$$

ist ein Monomorphismus der Gruppe $(G, \cdot)$ in die symmetrische Gruppe $(S_G, \circ)$. (Interpretation: Wegen $G \cong l(G)$ ist also jede Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe.)

(2.2) (Regeln für das Rechnen mit Zyklen :) Sei $n \in \mathbb{N}$ und seien $a_1, \ldots, a_k$ paarweise verschiedene Elemente aus $\underline{n}$. Zeigen Sie :

a) $(a_1, \ldots, a_k)^{-1} \quad = \quad (a_k, a_{k-1}, \ldots, a_1)$,

b) $(a_1, a_2)^{-1} \quad = \quad (a_1, a_2)$,

c) $\forall\, \tau \in S_n \,:\; \tau \circ (a_1, \ldots, a_k) \circ \tau^{-1} \quad = \quad (\tau(a_1), \ldots, \tau(a_k))$,

d) seien auch $b_1, \ldots, b_l$ paarweise verschiedene Elemente aus $\underline{n}$ und $\{b_1, \ldots, b_l\} \cap \{a_1, \ldots, a_k\} = \emptyset$, so gilt
$(a_1, \ldots, a_k) \circ (b_1, \ldots, b_l) = (b_1, \ldots b_l) \circ (a_1, \ldots, a_k)$.

(2.3) In der symmetrischen Gruppe $(S_4, \circ)$ sei

$$\gamma := (1, 2, 3, 4) \quad \text{und} \quad \delta := (2, 4) \quad .$$

a) Berechnen Sie γ^m für $m \in \underline{4}$, δ^n für $n \in \underline{2}$.

b) Zeigen Sie $\gamma \circ \delta = \delta \circ \gamma^3$.

c) Zeigen Sie, dass

$$D_4 := \{\; \delta^n \circ \gamma^m \;\mid\; m \in \{0, 1, 2, 3\} \wedge n \in \{0, 1\} \;\}$$

eine Untergruppe von $(S_4, \circ)$ mit 8 Elementen ist.
$(D_4, \circ)$ heißt die **Diedergruppe** (gesprochen: Di-edergruppe) mit 8 Elementen.

(2.4) In der symmetrischen Gruppe $(S_8, \circ)$ sei $e := \mathrm{id}_{\underline{8}}$,
$n := (1, 5) \circ (2, 6) \circ (3, 7) \circ (4, 8)$, $i := (1, 2, 5, 6) \circ (3, 4, 7, 8)$,
$j := (1, 3, 5, 7) \circ (2, 8, 6, 4)$, $k := (1, 4, 5, 8) \circ (2, 3, 6, 7)$.
Zeigen Sie, dass $Q := \{e, n, i, j, k, i^{-1}, j^{-1}, k^{-1}\}$ eine nicht kommutative Untergruppe von $(S_8, \circ)$ ist. Rechnen Sie dazu möglichst nur

$$n^2, i^2, j^2, k^2, i \circ j, j \circ k, k \circ i$$

aus und berechnen Sie die übrigen Produkte mit den Regeln aus (2.1.4) h) . Q heißt die **Quaternionengruppe** .

(2.5) Sei $(G, \cdot)$ eine Gruppe. Zeigen Sie :

a) $\mathrm{Aut}(G) := \{ \ \psi : G \longrightarrow G \mid \psi \text{ ist ein Automorphismus von } G \ \}$ ist eine Untergruppe von $(S_G, \circ)$.
$\mathrm{Aut}(G)$ heißt die **Automorphismengruppe** von G.

b) Für jedes $a \in G$ ist

$$\varphi_a : G \longrightarrow G \, , \, \varphi_a(x) := a \cdot x \cdot a^{-1}$$

ein Automorphismus von G (siehe auch 2.3.3 (2)) . φ_a heißt ein **innerer Automorphismus** von G.

c) Sei $\mathrm{Inn}(G) := \{ \ \varphi_a \mid a \in G \ \}$ die Menge der inneren Automorphismen von G, dann ist $\mathrm{Inn}(G)$ ein Normalteiler in $(\mathrm{Aut}(G), \circ)$.

d) Zählen Sie nach, dass

$$\#(\mathrm{Inn}(S_3)) = \#(\mathrm{Aut}(S_3)) = 6$$

ist, und damit $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$.
(Hinweis: Überlegen Sie sich, dass ein $\psi \in \mathrm{Aut}(S_3)$ bereits durch

$$\psi((1,2)) \quad \text{und} \quad \psi((1,2,3))$$

bestimmt ist, und dass es für diese Funktionswerte nur 3 bzw.2 Möglichkeiten gibt.)

e) Sei $(Z_4, \circ)$ die in (2.2.18) definierte zyklische Gruppe

$$Z_4 = \left\{ \ \alpha^k \ \middle| \ k \in \{0,1,2,3\} \ \right\} \quad \text{mit} \quad \alpha = (1,2,3,4) \quad .$$

Zeige, dass durch

$$\psi : Z_4 \longrightarrow Z_4 \quad , \quad \psi(\alpha^j) := \alpha^{3j} \quad \text{für} \quad j \in \mathbb{N}_0$$

ein Automorphismus von Z_4 definiert ist, der kein innerer Automorphismus von Z_4 ist .

(2.6) Zeigen Sie: Die in (2.2.16) definierte Gruppe V_4 ist ein Normalteiler in $(S_4, \circ)$, und es gilt

$$S_4/_{V_4} \cong S_3 \quad .$$

§3 Ringe und Körper

3.1 Etwas Ringtheorie

Definition 3.1.1 : Sei R eine Menge. Es gebe zwei Verknüpfungen

$$+ : R \times R \longrightarrow R \quad , \quad (x,y) \mapsto x+y \quad ,$$

$$\cdot : R \times R \longrightarrow R \quad , \quad (x,y) \mapsto x \cdot y \quad ,$$

die wir **Addition** und **Multiplikation** nennen, so dass gilt:

(R1) $(R,+)$ ist eine abelsche Gruppe.
Das neutrale Element dieser Gruppe bezeichnen wir mit 0, und statt vom "Inversen" eines Elements x sprechen wir vom **Negativen** und schreiben: $-x$, siehe auch (2.1.7),

(R2) $(R,\cdot)$ ist eine Halbgruppe. Nach Def.2.1.1 bedeutet das:

$$\forall\, x,y,z \in R : \; x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad .$$

(R3) $\exists\, 1 \in R : (1 \neq 0 \wedge \forall\, x \in R : \; 1 \cdot x = x \cdot 1 = x)$,
es gibt also ein neutrales Element bezüglich $\cdot$. Wir nennen 1 das **Einselement** von $(R,+,\cdot)$,

(R4) $\forall\, x,y,z \in R : (x\cdot(y+z) = (x\cdot y)+(x\cdot z) \wedge (x+y)\cdot z = (x\cdot z)+(y\cdot z))$
(Distributivgesetz) ,

dann heißt R , genauer: Das Tripel $(R,+,\cdot)$, ein **Ring** .

(3.1.2) Bemerkungen : (1) Das, was wir hier als "Ring" definiert haben, heißt in der Literatur genauer "assoziativer Ring mit Eins", aber das ist uns zu lang. Man kann aber auch eine Theorie ohne die Axiome (R2) und (R3) entwickeln.

(2) Das neutrale Element 1 mit der Eigenschaft aus (R3) ist eindeutig bestimmt, denn sei auch $1' \in R$ mit

$$\forall\, x \in R : \; 1' \cdot x = x \cdot 1' = x \quad , \quad \text{dann folgt}$$

$$1' = 1' \cdot 1 = 1 \quad .$$

(3) Auf die Klammern auf der rechten Seite der Regeln im Distributivgesetz werden wir verzichten: Wir definieren: "Punktrechnung geht vor Strichrechnung", dann bedeutet also

$$x \cdot y + x \cdot z \quad \text{dasselbe wie} \quad (x \cdot y) + (x \cdot z) \quad .$$

Definition 3.1.3 : Sei $(R,+,\cdot)$ ein Ring. Gilt zusätzlich zu den Axiomen (R1) - (R4) noch

(R5) $\forall\, x, y \in R : \; x \cdot y = y \cdot x$ (Kommutativgesetz der Multiplikation) ,
so heißt $(R, +, \cdot)$ ein **kommutativer Ring** . Gilt
(R6) $\forall\, x, y \in R \setminus \{0\} : x \cdot y \neq 0$,
so heißt $(R, +, \cdot)$ ein **nullteilerfreier Ring** .

Folgerung 3.1.4 : Sei $(R, +, \cdot)$ ein Ring, 0 das Nullelement und 1 das Einselement von $(R, +, \cdot)$, dann gilt für alle $x, y \in R$:
(1) $x \cdot 0 = 0$,
(2) $0 \cdot x = 0$,
(3) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$,
(4) $(-1) \cdot x = -x$,
(5) $(-x) \cdot (-y) = x \cdot y$.

Beweis : (1) Aus $0 + 0 = 0$ folgt $x \cdot 0 = x \cdot (0 + 0) \overset{(R4)}{=} x \cdot 0 + x \cdot 0$, andererseits gilt auch $x \cdot 0 + 0 = x \cdot 0$, also nach der Kürzungsregel in der Gruppe $(R, +)$:
$x \cdot 0 = 0$.
(2) zeigt man analog zu (1) mit (R4).
(3) $x \cdot y + (-x) \cdot y \overset{(R4)}{=} (x + (-x)) \cdot y = 0 \cdot y \overset{(2)}{=} 0$,
also ist $(-x) \cdot y$ das eindeutig bestimmte Negative von $x \cdot y$,
$(-x) \cdot y = -(x \cdot y)$, und ebenso
$x \cdot (-y) + x \cdot y \overset{(R4)}{=} x \cdot ((-y) + y) = x \cdot 0 \overset{(1)}{=} 0$, also $x \cdot (-y) = -(x \cdot y)$.
(4) $(-1) \cdot x \overset{(3)}{=} -(1 \cdot x) = -x$,
(5) $(-x) \cdot (-y) \overset{(3)}{=} -(x \cdot (-y)) \overset{(3)}{=} -(-(x \cdot y)) \overset{(2.1.4)(h)}{=} x \cdot y$.

□

Bemerkung 3.1.5 : Alles, was wir für Gruppen gelernt haben, gilt auch für die abelsche Gruppe $(R, +)$ eines Ringes $(R, +, \cdot)$. Statt Potenzen in $(R, +)$ spricht man nach (2.1.8) von Vielfachen

$$na \quad \text{für} \quad a \in R\,,\, n \in \mathbb{Z} \quad ,$$

und da $(R, \cdot)$ eine Halbgruppe ist, hat man auch Potenzen

$$a^n \quad \text{für} \quad a \in R\,,\, n \in \mathbb{N} \quad .$$

Wegen (R3) können wir noch definieren:

$$a^0 := 1 \quad \text{für} \quad a \in R \quad ,$$

dann sind also Potenzen a^n für $n \in \mathbb{N}_0$ definiert und alle $a \in R$, auch

$$0^0 \;=\; 1 \quad .$$

(Die untere 0 ist die 0 aus R, die obere die aus $\mathbb{N}_0$.)
Definition 3.1.6 : Sei $(R, +, \cdot)$ ein Ring, mit Einselement 1 und $U \subset R$. Es gelte

(I1) U ist eine Untergruppe von $(R, +)$, d.h.
$U \neq \emptyset \;\wedge\; \forall\, a, b \in U \,:\, b - a \in U \quad ,$ und
(UR) $1 \in U \;\wedge\; \forall\, a, b \in U \,:\; a \cdot b \in U \quad ,$
dann heißt U ein **Unterring** von $(R, +, \cdot)$.

□

Bemerkungen 3.1.7 (1) Die Definition ergibt Sinn: Ist U Unterring von $(R, +, \cdot)$, so ist $(U, +, \cdot)$ selbst wieder ein Ring, mit demselben Nullelement und Einselement wie in $(R, +, \cdot)$.
(2) Da $(R, +)$ abelsch ist, ist eine Teilmenge U von R, die (I1) erfüllt, ein Normalteiler in $(R, +)$. Man kann daher die Faktor**gruppe**

$$(R/_U, \oplus) \qquad \text{mit} \qquad (a + U) \oplus (b + U) \;=\; (a + b) + U$$

bilden, aber man möchte diese Linksnebenklassen nun auch multiplizieren. Damit das "wohldefiniert" wird, und nicht nur Triviales ergibt, nimmt man statt Unterringen "Ideale":

Definition 3.1.8 : Sei $(R, +, \cdot)$ ein Ring und $I \subset R$. Es gelte

(I1) I ist eine Untergruppe von $(R, +)$, d.h.
$I \neq \emptyset \;\wedge\; \forall\, a, b \in I \,:\, b - a \in I \quad ,$ und
(I2) $\forall r \in R \forall a \in I \,:\; (r \cdot a \in I \;\wedge\; a \cdot r \in I) \quad , \quad ,$
dann heißt I ein **Ideal** in $(R, +, \cdot)$.
- Man beachte, dass wir hier keineswegs gefordert haben, dass $1 \in I$ ist. Ist nämlich $1 \in I$, so ist wegen (I2) :

$$\forall\, r \in R \,:\; r \cdot 1 \in I \quad ,$$

dann ist also $R \subset I$, also $I = R$. Wir wollen aber auch "nichttriviale" Ideale haben !

Definition und Satz 3.1.9 : Sei $(R, +, \cdot)$ ein Ring, mit Nullelement 0 und Einselement 1 . Sei I ein Ideal in R. Dann hat man die durch

$$(a + I) \oplus (b + I) \quad := \quad (a + b) + I \quad \text{für} \quad a, b \in R$$

gemäß (2.2.12) definierte Faktorgruppe $(R/_I, \oplus)$, mit dem Nullelement $0 + I = I$. Durch

$$(*) \quad (a+I) \odot (b+I) \quad := \quad (a \cdot b) + I$$

wird eindeutig eine Verknüpfung $\odot$ auf $R/_I$ definiert. $(R/_I, \oplus, \odot)$ ist dann ein Ring, mit Nullelement $0 + I$ und Einselement $1 + I$. $(R/_I, \oplus, \odot)$ heißt der **Faktorring** von R modulo I .
Beweis : (1) Wir zeigen, dass durch $(*)$ eindeutig eine Abbildung

$$\odot \; : \; R/_I \times R/_I \;\longrightarrow\; R/_I$$

definiert ist: Seien $a, a', b, b' \in R$ mit

$$a + I \;=\; a' + I \quad \text{und} \quad b + I \;=\; b' + I \quad ,$$

dann gilt $a - a' \in I$ und $b - b' \in I$, also

$$a \cdot b - a' \cdot b' \;=\; a \cdot b - a \cdot b' + a \cdot b' - a' \cdot b' \;=\; a \cdot (b - b') + (a - a') \cdot b' \quad ,$$

und das liegt in I , denn $b - b' \in I$ und $a - a' \in I$, nach (I2) also $a \cdot (b - b') \in I$ und $(a - a') \cdot b' \in I$, und nach (I1) liegt auch die Summe in I . Also gilt

$$a \cdot b + I \quad = \quad a' \cdot b' + I \quad .$$

(2) Die anderen Ringaxiome gelten in $(R/_I, \oplus, \odot)$, da sie in $(R, +, \cdot)$ gelten.

□

Um Homomorphismen von Ringen zu definieren, müssen wir zwei evtl. verschiedene Mengen R und S nehmen, mit verschiedener Addtion und Multiplikation. Um die Formeln aber nicht zu unübersichtlich werden zu lassen, schreiben wir die Zeichen $+$ und $\cdot$ für die Verknüpfungen in beiden Ringen. Für die Einselemente schreiben wir aber 1_R bzw. 1_S :
Definition 3.1.9 : Seien $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe, mit Einselementen 1_R bzw. 1_S . Eine Abbildung

$$\psi \; : \; R \;\longrightarrow\; S$$

heßt ein **Ringhomomorphismus**, wenn gilt
(RH1) $\quad \forall\, a, b \in R \; : \; \psi(a + b) \;=\; \psi(a) + \psi(b)$,
(RH2) $\quad \forall\, a, b \in R \; : \; \psi(a \cdot b) \;=\; \psi(a) \cdot \psi(b)$,
(RH3) $\quad \psi(1_R) \;=\; 1_S \quad .$

□

Man beachte, dass (RH3) nicht aus Satz 2.3.4(1) folgt, denn $(R, \cdot)$ und $(S, \cdot)$ sind keine Gruppen!

Wie bei Gruppen-Homomorphismen definiert man den Kern :
Definition und Satz 3.1.10 : Seien $(R, +, \cdot)$ und $(S, +\cdot)$ Ringe,
$\psi : R \longrightarrow S$ ein Homomorphismus. Dann heißt

$$\ker \psi \quad := \quad \{ \ x \in R \mid \psi(x) = 0 \ \}$$

der **Kern des Ringhomomorphismus** ψ . (Die 0 hier ist natürlich die 0 in S .)
$\ker \psi$ ist ein Ideal in R .
Beweis : (I1) $\ker \psi$ ist ein Normalteiler, also eine Untergruppe, von $(R, +)$ nach Satz 2.3.7 .
(I2) Für $r \in R$ und $a \in \ker \psi$ gilt

$$\psi(r \cdot a) = \psi(r) \cdot \psi(a) = \psi(r) \cdot 0 = 0 \quad \text{und}$$

$$\psi(a \cdot r) = \psi(a) \cdot \psi(r) = 0 \cdot \psi(r) = 0 \quad ,$$

also $r \cdot a, a \cdot r \in \ker \psi$.

□

Man hat also den Faktorring $R/_{\ker \psi}$, und kann damit den Homomorphiesatz für Ringe formulieren:
(3.1.11) Homomorphiesatz für Ringe : Seien $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe ,

$$\psi : R \longrightarrow S \quad \text{ein Epimorphismus von Ringen.}$$

Sei $\kappa : R \longrightarrow R/_{\ker \psi}$, $x \mapsto x + (\ker \psi)$ der kanonische Nebenklassenepimorphismus von R auf den Faktorring $R/_{\ker \psi}$, dann gibt es genau einen Ring-Isomorphismus

$$\iota : R/_{\ker \psi} \longrightarrow S \quad \text{mit} \quad \iota \circ \kappa = \psi \quad .$$

(" $\circ$ " ist hier die Hintereinanderausführung von Abbildungen.)
Beweis : Da Satz 2.3.9 schon bewiesen ist, muss man nur noch nachrechnen, dass κ und ι die Bedingungen (RH2) und (RH3) für einen Ringhomomorphismus erfüllt. Das ist eine leichte Übungsaufgabe.

□

3.2 Der Ring der ganzen Zahlen

Das Rechnen mit ganzen Zahlen sollte aus der Schule bekannt sein, d.h. wir wissen, dass $(\mathbb{Z}, +, \cdot)$ mit der gewöhnlichen Addition + und der gewöhnlichen

Multiplikation $\cdot$ ein kommutativer, nullteilerfreier Ring ist, mit der Zahl 0 als Nullelement und der Zahl 1 als Einselement.
Bemerkung 3.2.1 : Mit der Anordnung der ganzen Zahlen, dem Induktionsaxiom und gleichbedeutenden Aussagen hatten wir uns schon in Abschnitt 1.2 beschäftigt. Wir setzen als bekannt voraus, dass außer den Axiomen (O1) - (O3) auch noch
(O4) $\quad \forall\, x, y \in \mathbb{Z} : \ (x \leq y \ \vee \ y \leq x)$,
(O5) $\quad \forall\, x, y, z \in \mathbb{Z} : \ (x \leq y \quad \Longrightarrow \quad x + z \leq y + z)$,
(O6) $\quad \forall\, x, y, z \in \mathbb{Z} : \ (x \leq y \ \wedge \ z \geq 0 \quad \Longrightarrow \quad x \cdot z \leq y \cdot z)$
gilt.

Satz 3.2.2 : Sei m eine feste ganze Zahl. Dann ist die Menge

$$(m) \quad := \quad \{ \ km \mid k \in \mathbb{Z} \ \} \quad \text{ein Ideal in} \quad (\mathbb{Z}, +, \cdot) \quad .$$

Dabei bezeichnet km für $k \in \mathbb{Z}$ das $k-$fache von m - das aber gleich dem Produkt $k \cdot m$ in $\mathbb{Z}$ ist.
Beweis : (I1) $(m) \subset \mathbb{Z}$ sieht man, und $(m) \neq \emptyset$ wegen $0 = 0 \cdot m \in (m)$.
Seien $a, b \in (m)$, dann gibt es $k, l \in Z$ mit $a = km$, $b = lm$, also
$b - a = (l - k)m \in (m)$.
(I2) Sei $r \in \mathbb{Z}$ und $a \in (m)$, dann gibt es ein $k \in \mathbb{Z}$ mit $a = km$, also

$$a \cdot r = r \cdot a = r \cdot (km) = r \cdot (k \cdot m) = (r \cdot k) \cdot m = (r \cdot k)m \in (m) \quad .$$

□

Wir wollen zeigen, dass die Ideale (m) , $m \in \mathbb{N}_0$, sogar alle Ideale von $(\mathbb{Z}, +, \cdot)$ sind. Dazu brauchen wir den

Satz 3.2.3 (Division mit Rest in $\mathbb{Z}$): Sei $n \in \mathbb{Z}, a \in \mathbb{N}$, dann gibt es eindeutig bestimmte Zahlen $v \in \mathbb{Z}, r \in \mathbb{N}_0$ mit

$$n = v \cdot a + r \quad \text{und} \quad 0 \leq r < a \quad .$$

Beweis : a) Wir zeigen die Existenz von v und r:
a_1) Sei zunächst $n \in \mathbb{N}_0$. Dann zeigen wir die Aussage

$$\underbrace{\forall\, a \in \mathbb{N}\, \exists\, v \in \mathbb{N}_0 \exists\, r \in \mathbb{N}_0 : (n = v \cdot a + r \ \wedge \ r < a)}_{\Longleftrightarrow \ : \ P(n)}$$

durch Induktion nach n:
Induktionsanfang: Für $n = 0$ gilt

$$0 = 0 \cdot a + 0 \ \wedge \ 0 < a \quad ,$$

für beliebiges $a \in \mathbb{N}$. Die Aussage ist also für $n = 0$ richtig.
Induktionsschluss: Sei $n \in \mathbb{N}_0$, und für n sei $P(n)$ richtig. Dann folgt

$$n+1 = (v \cdot a + r) + 1 = v \cdot a + (r+1) \quad ,$$

mit $0 \leq r < a$, also $0 \leq r+1 \leq a$. Wenn $r+1 < a$ ist, sind wir fertig, es gilt dann auch $P(n+1)$. Anderenfalls gilt $r+1 = a$ und wir haben

$$n+1 = v \cdot a + a = (v+1) \cdot a + 0 \quad ,$$

und auch in diesem Fall gilt $P(n+1)$.
a_2) Sei nun $n \in \mathbb{Z} \setminus \mathbb{N}$ und $a \in \mathbb{N}$ gegeben. Dann ist $-n \in \mathbb{N}$, also nach a_1) :

$$\exists\, v \in \mathbb{N}_0\, \exists\, r \in \mathbb{N}_0 : (-n = v \cdot a + r \wedge r < a) \quad , \qquad \text{also}$$

$$n = (-v) \cdot a - r \quad \text{mit} \quad 0 \leq r < a \quad .$$

Ist hier $r = 0$, so haben wir die Behauptung gezeigt, mit $-v \in \mathbb{Z}$. Ist $0 < r < a$, so ist $0 < a - r < a$, wir haben

$$n = (-v-1) \cdot a + (a - r)$$

mit $-v - 1 \in \mathbb{Z}$, also gilt die Behauptung auch in diesem Fall.
b) Wir zeigen nun die Eindeutigkeit von v und r: Sei auch

$$n = v' \cdot a + r' \quad \text{mit} \quad v' \in \mathbb{Z}\,,\, 0 \leq r' < a \quad , \quad \text{dann folgt}$$

$$v \cdot a + r = v' \cdot a + r' \quad .$$

Ist hier $v = v'$, so folgt auch $r = r'$ und wir haben die Eindeutigkeit. Angenommen, $v \neq v'$, so ist eine der beiden Zahlen die kleinere, etwa $v < v'$, also existiert ein $w \in \mathbb{N}$ mit $v + w = v'$,

$$v \cdot a + r = (v+w) \cdot a + r' \quad ,$$

$$r = w \cdot a + r' \quad ,$$

mit $r < a$, aber $w \cdot a + r' \geq w \cdot a > a$, was ein Widerspruch ist.

□

Satz 3.2.4 : Sei I ein Ideal von $(\mathbb{Z}, +, \cdot)$, dann gibt es genau ein $m \in \mathbb{N}_0$ mit $I = (m)$.
Beweis : Sei I ein Ideal von $(\mathbb{Z}, +, \cdot)$, dann kann

$$I \quad = \quad \{0\} \quad \text{sein, dann ist} \quad I \quad = \quad (0) \quad .$$

Sei $I \neq \{0\}$, dann gibt es ein $c \in I, c \neq 0$. Es kann $c \in \mathbb{N}$ sein, sonst ist $-c \in \mathbb{N}$, aber auch $-c \in I$, da I Untergruppe von $(\mathbb{Z}, +)$ ist. Jedenfalls ist

$$M \quad := \quad I \cap \mathbb{N} \quad \neq \quad \emptyset \quad ,$$

und nach (1.2.13) existiert

$$m \quad := \quad \min(M) \quad ,$$

also ist $m \in I$, und da I Untergruppe ist, auch

$$\forall\, v \in \mathbb{Z} : \quad vm \in I \quad , \qquad \text{also} \quad (m) \subset I \quad .$$

Sei nun $n \in I$, dann dividieren wir n mit Rest durch m : Nach Satz 3.2.3 haben wir ein $r \in \mathbb{N}_0$ und ein $v \in \mathbb{Z}$ mit

$$n \,=\, v \cdot m + r \quad \text{und} \quad 0 \leq r < m \quad ,$$

also $r \,=\, n - v \cdot m$. Da die rechte Seite in I liegt, ist auch $r \in I$. Aus $0 < r < m$ würde folgen, dass in $I \cap \mathbb{N}$ noch ein kleineres Element als m liegt, Widerspruch zur Definition von m , also $r \,=\, 0$,

$$n \,=\, v \cdot m \;\in\; (m).$$

□

Definition 3.2.5 : Seien $a, b \in Z$. Wir sagen:

$$a \,\big|\, b \quad , \quad \text{gesprochen: } a \text{ teilt } b \quad :\Longleftrightarrow \quad \exists\, c \in \mathbb{Z} \;:\; a \cdot c \,=\, b \quad .$$

Definition 3.2.6 : Sei $p \in \mathbb{N}$, $p \neq 1$. p heißt eine **Primzahl**, wenn gilt

$$\forall\, a, b \in \mathbb{Z} : \quad (\, p \,\big|\, a \cdot b \quad \Longrightarrow \quad p \,\big|\, a \,\vee\, p \,\big|\, b\,) \quad .$$

Satz 3.2.7 : Eine Zahl $p \in \mathbb{N}$ ist genau dann eine Primzahl, wenn gilt

$$(*) \quad \forall\, k, l \in \mathbb{N} : \quad (p \,=\, k \cdot l \quad \Longrightarrow \quad k = 1 \,\vee\, l = 1) \quad .$$

Beweis : 1) p sei eine Primzahl und seien $k, l \in \mathbb{N}$ mit

$$p \quad = \quad k \cdot l \quad , \quad \text{dann gilt} \quad p \cdot 1 \quad = \quad k \cdot l \quad , \quad \text{also}$$

$$p \,|k \cdot l \quad ,$$

nach Definition 3.2.6 also $p \,|\, k$ oder $p \,|\, l$. Aus $p \,|\, k$ folgt

$$\exists t \in \mathbb{Z} : \quad p \cdot t \quad = \quad k \quad ,$$

sogar $t \in \mathbb{N}$ wegen $p, k \in \mathbb{N}$, also

$$k \quad = \quad p \cdot t \quad \geq \quad p \cdot 1 \quad = \quad p \quad .$$

Aus $k > p$ oder $l > 1$ würde dann

$$k \cdot l \; > \; p \cdot 1 \quad = \quad p \quad \text{folgen, Widerspruch, also}$$

$k = p$ und $l = 1$. Analog: Aus $p \,|\, l$ folgt $k = 1$.

2) Für p gelte $(*)$. Seien a, b in $\mathbb{Z}$; es gelte

$$p \,|\, a \cdot b \quad , \quad \text{aber nicht} \quad p \,|\, a \quad .$$

Dann ist

$$I \quad := \quad \{ \; n \cdot p + m \cdot a \; \mid \; n, m \in \mathbb{Z} \; \}$$

ein Ideal von $(\mathbb{Z}, +, \cdot)$, was man leicht nachrechnet. Nach Satz 3.2.4 gibt es genau ein $d \in \mathbb{N}_0$ mit

$$I \; = \; (d) \quad , \quad \text{sogar} \quad d \in \mathbb{N} \quad ,$$

denn $p \; = \; 1 \cdot p + 0 \cdot a \; \in \; I$, also $I \neq \{0\}$. Es ist $p \in (d)$, also gibt es ein $s \in \mathbb{Z}$ mit

$$p \; = \; s \cdot d \quad , \quad \text{sogar} \quad s \in \mathbb{N} \quad \text{wegen} \quad p, d \in \mathbb{N} \quad .$$

Nach $(*)$ folgt $s \; = \; 1$ oder $d \; = \; 1$. Aus $s \; = \; 1$ würde folgen: $p \; = \; d$,

$$a \; = \; 0 \cdot p + 1 \cdot a \in I \in (d) \; = \; (p) \quad , \qquad \text{also}$$

$$\exists \, t \in \mathbb{Z} : \;\; a \; = \; t \cdot p \quad , \quad p \,|\, a \quad , \quad \text{Widerspruch.}$$

Also ist $d = 1$, also $1 \in I$, also

$$\exists \, u, v \in \mathbb{Z} : \;\; 1 \quad = \quad u \cdot p + v \cdot a \quad , \qquad \text{also}$$

$$b \quad = \quad u \cdot p \cdot b + v \cdot a \cdot b \quad ,$$

und wegen $p \,|\, p$, $p \,|\, a \cdot b$ folgt: $p \,|\, b$. Also ist p eine Primzahl.

□

Bemerkung 3.2.8 : Wir kennen nun alle Ideale von $(\mathbb{Z}, +, \cdot)$, es sind die Ideale (m) mit $m \in \mathbb{N}_0$, und wollen uns nun die zugehörigen Faktorringe

$\mathbb{Z}/_{(m)}$ ansehen:
Ist $m = 0$, so haben wir

$$(0) = \{ \ k \cdot 0 \mid k \in \mathbb{Z} \ \} = \{0\} \quad ,$$

und der Faktorring $\mathbb{Z}/_{(0)}$ ist isomorph zu $\mathbb{Z}$: Die Abbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/_{(0)} \quad , \quad z \mapsto z + (0)$$

ist ein Ring-Isomorphismus. Auch für $m = 1$ erhalten wir nichts Neues: Es ist

$$(1) = \{ \ k \cdot 1 \mid k \in \mathbb{Z} \ \} = \mathbb{Z} \quad ,$$

und $\mathbb{Z}/_{\mathbb{Z}} \cong (0)$.
Wir nehmen daher im Folgenden $m \in \mathbb{N}$, $m \geq 2$.

Folgerung 3.2.9 : Sei $m \in \mathbb{N}$, $m \geq 2$. Wenn wir die Nebenklassen $a + (n)$ für $a \in \mathbb{Z}$ mit $\overline{a}$ bezeichnen, so ist

$$\mathbb{Z}/_{(m)} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

und Summe und Produkt von $\overline{a}, \overline{b} \in \mathbb{Z}/_{(m)}$ erhält man, indem man die ganzen Zahlen a, b addiert bzw. multipliziert und vom Ergebnis c den nach Satz 3.2.3 existierenden Divisionsrest c' modulo m nimmt, d.h. man sucht sich die Zahl $c' \in \mathbb{N}_0$ mit

$$0 \leq c' < n \quad \text{und} \quad c - c' \in (n),$$

und bildet dazu $\overline{c'}$. Sei nämlich $c - c' \in (n)$, dann gilt $c + (n) = c' + (n)$, also $\overline{c} = \overline{c'}$.
a) Die additive Gruppe $(\mathbb{Z}/_{(n)}, +)$ ist für uns nichts Neues: Sei $(Z_n, \circ)$ die aus Beispiel (2.1.16) bekannte Gruppe, dann ist

$$Z_n = <\alpha> = \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\} \quad \text{mit} \quad \alpha = (1, 2, \cdots, n)$$

und die Abbildung

$$\varphi : \ Z_n \longrightarrow \mathbb{Z}/_{(n)} \quad , \quad \alpha^k \mapsto \overline{k} \quad \text{für} \quad k \in \{0, \ldots, n-1\}$$

ist ein Isomorphismus der Gruppe $(Z_n, \circ)$ auf die Gruppe $(\mathbb{Z}/_{(n)}, +)$. Wir sehen uns als Beispiel die Gruppentafeln für $(\mathbb{Z}/_{(5)}, +)$ und $(\mathbb{Z}/_{(6)}, +)$ an, wobei wir zur Unterscheidung $\tilde{a}$ für die Elemente aus $\mathbb{Z}/_{(6)}$ schreiben:

$(\mathbb{Z}/_{(5)}, +)$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$(\mathbb{Z}/_{(6)}, +)$

$+$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{0}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{1}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{0}$
$\tilde{2}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{0}$	$\tilde{1}$
$\tilde{3}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{4}$	$\tilde{4}$	$\tilde{5}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$
$\tilde{5}$	$\tilde{5}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$

Deutliche Unterschiede in der Struktur haben die multiplikativen Halbgruppen $(\mathbb{Z}/_{(5)}, \cdot)$ und $(\mathbb{Z}/_{(6)}, \cdot)$:

$(\mathbb{Z}/_{(5)}, \cdot)$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$(\mathbb{Z}/_{(6)}, \cdot)$:

$\cdot$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$
$\tilde{1}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{2}$	$\tilde{0}$	$\tilde{2}$	$\tilde{4}$	$\tilde{0}$	$\tilde{2}$	$\tilde{4}$
$\tilde{3}$	$\tilde{0}$	$\tilde{3}$	$\tilde{0}$	$\tilde{3}$	$\tilde{0}$	$\tilde{3}$
$\tilde{4}$	$\tilde{0}$	$\tilde{4}$	$\tilde{2}$	$\tilde{0}$	$\tilde{4}$	$\tilde{2}$
$\tilde{5}$	$\tilde{0}$	$\tilde{5}$	$\tilde{4}$	$\tilde{3}$	$\tilde{2}$	$\tilde{1}$

Dass in den Tabellen jeweils in der ersten Zeile und Spalte, also bei den Produkten mit dem Nullelement, nur das Nullelement steht, ist nach Folgerung 3.1.4 klar. Aber wir sehen: In $\mathbb{Z}/_{(5)} \setminus \{\overline{0}\}$ besitzt jedes Element ein Inverses bezüglich $\cdot$:

$$\overline{1}^{-1} = \overline{1} \quad , \quad \overline{2}^{-1} = \overline{3} \quad , \quad \overline{3}^{-1} = \overline{2} \quad , \quad \overline{4}^{-1} = \overline{4} \quad .$$

In $\mathbb{Z}/_{(6)} \setminus \{\tilde{0}\}$ gilt das nicht, schlimmer noch: Es gibt Produkte von Elementen ungleich $\tilde{0}$, die $\tilde{0}$ sind. Wir haben hier ein Beispiel für einen Ring, der nicht nullteilerfrei ist. Das liegt daran, dass 5 eine Primzahl ist, 6 aber nicht. Allgemein: Sei $n \in \mathbb{N}$, $n \geq 2$ und n keine Primzahl,

$$\mathbb{Z}/_{(n)} = \{ \ \tilde{a} \mid \ a \in \{0, 1, \ldots, n-1\} \ \} \quad \text{mit} \quad \tilde{a} := a + (n) \quad ,$$

dann gibt es nach Satz 3.2.7 zwei Zahlen

$$k, l \in \mathbb{N} \quad \text{mit} \quad 1 < k < n \, , \, 1 < l < n \quad \text{und} \quad n = k \cdot l \quad , \qquad \text{also}$$

$$\tilde{k} \cdot \tilde{l} = \tilde{0} \quad \text{und} \quad \tilde{k}, \tilde{l} \neq \tilde{0} \quad .$$

Satz und Definition 3.2.11 : Sei $(R, +, \cdot)$ ein Ring, 1 das Einselement von R. Dann ist die Menge der Elemente, die ein Inverses bezüglich $\cdot$ besitzen, also

$$R^\times := \{\ a \in R \mid \exists\, a^* \in R : a \cdot a^* = a^* \cdot a = 1\ \}$$

mit $\cdot$ eine Gruppe, genannt die **Einheitengruppe** von R .
Beweis : Sind $a, b \in R^\times$, so haben wir

$$(a \cdot b) \cdot (b^* \cdot a^*) = (a \cdot (b \cdot b^*)) \cdot a^* = (a \cdot 1) \cdot a^* = a \cdot a^* = 1\,,$$

ebenso: $(b^* \cdot a^*) \cdot (a \cdot b) = 1$. Also ist $a \cdot b \in R^\times$, $\cdot$ ist eine Verknpfung auf $R^\times$.
(G1) Das Assoziativgesetz für $\cdot$ gilt in $R^\times$, da es in R gilt.
(G2) Wegen $1 \cdot 1 = 1$ ist $1 \in R^\times$ und
$\forall\, a \in R^\times : 1 \cdot a = a\,.$
(G3) Sei $a \in R^\times$, dann haben wir nach Def. von $R^\times$ ein $a^* \in R$ mit $a^* \cdot a = 1$.
Dieses a^* gehört aber sogar zu $R^\times$ wegen $a \cdot a^* = 1$, wir können also $(a^*)^* := a$ nehmen.
$(R^\times, \cdot)$ erfüllt also die Gruppenaxiome.

□

Beisiele 3.2.12 : 1) Es ist $\mathbb{Z}^\times = \{1, -1\}$.
2) Ist n eine Primzahl, so ist

$$(\mathbb{Z}/_{(n)})^\times = \mathbb{Z}/_{(n)} \setminus \{\overline{0}\} \quad \text{für} \quad \overline{0} = 0 + (n) \quad .$$

3) Es gilt

$$(\mathbb{Z}/_{(8)})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \quad , \quad (\mathbb{Z}/_{(10)})^\times = \{\tilde{1}, \tilde{3}, \tilde{7}, \tilde{9}\}$$

$$\text{mit} \quad \overline{a} := a + (8) \quad , \quad \tilde{a} := a + (10) \quad \text{für} \quad a \in \mathbb{Z}$$

und wir haben folgende Gruppentafeln:

$((\mathbb{Z}/_{(8)})^\times, \cdot)$

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

$((\mathbb{Z}/_{(10)})^\times, \cdot)$

$\cdot$	$\tilde{1}$	$\tilde{3}$	$\tilde{7}$	$\tilde{9}$
$\tilde{1}$	$\tilde{1}$	$\tilde{3}$	$\tilde{7}$	$\tilde{9}$
$\tilde{3}$	$\tilde{3}$	$\tilde{9}$	$\tilde{1}$	$\tilde{7}$
$\tilde{7}$	$\tilde{7}$	$\tilde{1}$	$\tilde{9}$	$\tilde{3}$
$\tilde{9}$	$\tilde{9}$	$\tilde{7}$	$\tilde{3}$	$\tilde{1}$

Wir sehen: $(\mathbb{Z}/_{(8)})^\times \cong V_4 \quad , \quad (\mathbb{Z}/_{(10)})^\times \cong Z_4\,.$

Ist jedenfalls n eine Primzahl p, so ist $\mathbb{Z}/_{(p)} \setminus \{0+(p)\}$ mit der auf diese Menge eingeschränkten Multiplikation eine kommutative Gruppe. Bevor wir das beweisen, noch ein neuer Begriff:

Definition 3.2.13 : Sei $(K,+,\cdot)$ ein kommutativer Ring, mit Nullelement 0 und Einselement 1. Wenn dann (zusätzlich zu den Axiomen (R1) - (R5)) noch gilt

(KK) $\quad \forall\, x \in K\setminus\{0\}\ \exists\, x^{-1} \in K\ :\ x^{-1}\cdot x = 1 \quad ,$

dann nennen wir $(K,+,\cdot)$ einen **Körper** .

□

Folgerung 3.2.14 : Ist $(K,+,\cdot)$ ein Körper, mit Nullelement 0 und Einselement 1, so ist $K \setminus \{0\}$ mit der darauf eingeschränkten Multiplikation $\cdot$ eine kommutative Gruppe.

Beweis : Wegen der Kommutativität von $(K,\cdot)$ und nach Axiom (KK) ist

$$K \setminus \{0\} \quad = \quad K^{\times}$$

die Einheitengruppe von $(K,+,\cdot)$, also nach Satz 3.2.11 eine Gruppe. Wegen (R5) ist diese Gruppe kommutativ.

□

Sie kennen aus der Schule Beispiele für Körper:

$(\mathbb{Q},+,\cdot)$, den Körper der rationalen Zahlen,

$(\mathbb{R},+,\cdot)$, den Körper der reellen Zahlen,
dessen genaue Charakterisierung in die Analysis gehört,

und vielleicht noch

$(\mathbb{C},+,\cdot)$, den Körper der komplexen Zahlen,
den wir hier (sicherheitshalber) noch einführen werden.

Aber nun eben auch:

Satz 3.2.15 : Sei p eine Primzahl, dann ist $(\mathbb{Z}/_{(p)},+,\cdot)$ ein Körper.
$\mathbb{Z}/_{(p)}$ enthält genau p Elemente.

Beweis : Für $a \in \mathbb{Z}$ setzen wir wieder

$$\overline{a} \ = \ a+(p) \quad ,$$

dann wissen wir:

$$\mathbb{Z}/_{(p)} \ = \ \{\overline{0},\ldots,\overline{p-1}\} \quad ,$$

und die angegebenen p Elemente sind verschieden. Dass $(\mathbb{Z}/_{(p)}, +, \cdot)$ ein Ring ist, gilt nach Satz 3.1.9 , und kommutativ ist er, da $(\mathbb{Z}, +, \cdot)$ ein kommutativer Ring ist. $\overline{1}$ ist das Einselement von $(\mathbb{Z}/_{(p)}, +, \cdot)$. Sei $\overline{a} \in \mathbb{Z}/_{(p)}$ mit

$$(*) \qquad \overline{a} \neq \overline{0} \quad , \qquad \text{also} \quad 0 < a < p \quad .$$

Sei $I := \{ \; r \cdot a + s \cdot p \mid r, s \in \mathbb{Z} \; \}$, dann ist I ein Ideal im Ring $(\mathbb{Z}, +, \cdot)$, mit $a = 1 \cdot a + 0 \cdot p \in I$ und $p = 0 \cdot a + 1 \cdot p \in I$. Nach Satz 3.2.5 gibt es ein $d \in \mathbb{N}_0$ mit

$$I = (d) \quad , \quad \text{sogar} \quad d \in \mathbb{N} \quad \text{wegen} \quad p \in I \, , \quad \text{also} \quad I \neq (0) \quad .$$

Es ist dann $p \in (d)$, also

$$\exists t \in \mathbb{Z} : \; p = t \cdot d \quad ,$$

sogar $t \in \mathbb{N}$ wegen $p, d \in \mathbb{N}$. Nun ist $p \in \mathbb{P}$, also folgt aus $p = t \cdot d$ nach Satz 3.2.8 : $d = 1$ oder $t = 1$. Angenommen, $t = 1$, dann würde $d = p$ und $a \in I = (d) = (p)$ folgen, also

$$\overline{a} = a + (p) = 0 + (p) = \overline{0}$$

folgen, Widerspruch zu $(*)$. Also ist $t = 1$ falsch und es gilt $d = 1$,

$$I = (d) = (1) = \mathbb{Z} \quad , \qquad \text{also}$$

$$\{ \; r \cdot a + s \cdot p \mid r, s \in \mathbb{Z} \; \} \quad = \quad \mathbb{Z} \quad ,$$

und das heißt, zu jedem $z \in \mathbb{Z}$ gibt es $r, s \in \mathbb{Z}$ mit $z = r \cdot a + s \cdot p$, insbesondere

$$\exists r \in \mathbb{Z} \; \exists s \in \mathbb{Z} : \; 1 = r \cdot a + s \cdot p \quad ,$$

und mit diesem r folgt

$$1 - r \cdot a = s \cdot p \in (p) \quad ,$$

$$\overline{1} = \overline{r} \cdot \overline{a} \quad .$$

Wir haben also ein Inverses zu $\overline{a}$ gefunden: Es gilt (KK) .

□

-Zwischen den Körpern $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ einerseits und den Körpern $\mathbb{Z}/_{(p)}$ andererseits gibt es einen wesentlichen Unterschied: Nimmt man die 1 dieser Körper und bildet die Vielfachen

$$n\,1 \quad \text{für} \quad n \in \mathbb{N} \quad ,$$

so sind diese in $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ niemals 0. In $Z/_{(5)} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ mit dem Einselement $\overline{1}$ gilt aber

$$5\,\overline{1} = \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{0} \quad .$$

Definition und Satz 3.2.16 : Sei $(R, +, \cdot)$ ein kommutativer, nullteilerfreier Ring, mit Nullelement 0 und Einselement 1. Wenn alle Vielfachen

$$n\,1 \quad \text{für} \quad n \in \mathbb{N}$$

ungleich dem Nullement 0 sind, dann sagen wir:
R **hat die Charakteristik 0** und schreiben : **char** $R = 0$.
Anderenfalls ist

$$\{\ n \in \mathbb{N} \mid n\,1 = 0\ \} \quad \text{eine nichtleere Teilmenge von } \mathbb{N}\,, \quad \text{und}$$

$$\operatorname{char} R := p := \min\{\ n \in \mathbb{N} \mid n\,1 = 0\ \}$$

ist eine natürliche Zahl, sogar eine Primzahl. Wir sagen dann:
R **hat die Charakteristik** p .
Beweisen müssen wir nur, dass p eine Primzahl ist: Angenommen, p ist keine Primzahl, dann haben wir nach Satz 3.2.8 zwei Zahlen

$$k, l \in \mathbb{N} \quad \text{mit} \quad p = k \cdot l \quad \text{und} \quad (1 < k < p) \ \wedge\ (1 < l < p) \quad .$$

Aus $p\,1 = 0$ folgt dann

$$(k\,1) \cdot (l\,1) \overset{(*)}{=} (k \cdot l)\,1 = p\,1 = 0$$

und da $(R, +, \cdot)$ nullteilerfrei ist:

$$k\,1 = 0 \quad \vee \quad l\,1 = 0\,,$$

aber $k, l < p$, Widerspruch zur Minimalität von p. Die Formel

$$(*) \qquad \forall\, m, n \in \mathbb{N}_0 : \ (n\,1) \cdot (m\,1) = (n \cdot m)\,1$$

folgt mit Induktion aus dem Distributivgesetz und der Potenzregel 2.1.7(1).

□

Wir haben also : $\operatorname{char} \mathbb{Q} = 0$, $\operatorname{char} \mathbb{Z}/_{(p)} = p$ für alle $p \in \mathbb{P}$.

3.3 Der Polynomring in einer Unbestimmten

(3.3.1) Zur Motivation : Sei $(R, +, \cdot)$ ein kommutativer, nullteilerfreier Ring, dann heißt eine Funktion

$$f \; : \; R \; \longrightarrow \; R$$

eine **Polynomfunktion** , wenn es ein $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in R$ gibt, so dass

$$f(t) \quad = \quad \sum_{k=0}^{n} a_k \cdot t^k \quad \text{für alle} \quad t \in R \quad \text{gilt.}$$

Ist $R = \mathbb{Q}$ oder $\mathbb{R}$, so haben diese Polynomfunktionen die angenehme Eigenschaft, dass ihre Koeffizienten eindeutig bestimmt sind: Seien $n, m \in \mathbb{N}_0, a_0, \ldots a_n, b_0, \ldots, b_m \in \mathbb{R}$ und

$$\forall\, t \in \mathbb{R} \; : \; \sum_{k=0}^{n} a_k \cdot t^k \; = \; \sum_{k=0}^{m} b_k \cdot t^k \quad , \quad \text{etwa} \quad n \leq m \quad ,$$

dann folgt $a_k = b_k$ für $k \in \{0, \ldots, n\}$ und $b_k = 0$ für $k > n$. Für andere Ringe oder Körper gilt das nicht: Sei etwa

$$K := \mathbb{Z}/_{(3)} \quad \text{und} \quad f, g \; : \; K \; \longrightarrow \; K \quad ,$$

$$f(t) := t \quad \text{und} \quad g(t) := t^3 \quad ,$$

dann gilt

$$\begin{aligned} f(\overline{0}) \; = \; \overline{0} \; = \; g(\overline{0}) \quad , \quad f(\overline{1}) \; = \; \overline{1} \; = \; g(\overline{1}) \quad , \\ f(\overline{2}) \; = \; \overline{2} \; = \; g(\overline{2}) \quad , \quad \text{also} \quad f \; = \; g \quad , \quad \text{aber} \\ f(t) \; = \; \overline{0} + \overline{1} \cdot t + \overline{0} \cdot t^2 + \overline{0} \cdot t^3 \quad , \\ g(t) \; = \; \overline{0} + \overline{0} \cdot t + \overline{0} \cdot t^2 + \overline{1} \cdot t^3 \quad , \end{aligned}$$

die Koeffizienten sind also nicht eindeutig bestimmt und es ist daher nicht möglich, den Grad einer solchen Polynomfunktion zu definieren. (Soll der Grad von f nun 1 oder 3 sein ?) Man führt daher statt Polynomfunktionen

$$\text{Polynome} \quad \sum_{k=0}^{n} a_k \cdot X^k$$

mit einem Element $X \notin K$ ein. In manchen Büchern werden nun Polynome als "formale Ausdrücke $\sum_{k=0}^{n} a_k X^k$ " eingeführt, das ist im Grunde genau so

unverständlich, wie wenn man versucht, die komplexen Zahlen dadurch einzuführen, dass man sagt: "$\sqrt{-1}$ existiert nicht. Wir setzen daher $i := \sqrt{-1}$". Wie bei der Einführung von $\mathbb{C}$ muss man sich die Mühe machen, die Menge K zu erweitern. Das geht natürlich nicht ganz schnell, aber das Ergebnis ist so, wie man es haben will. Dazu zunächst eine Abkürzung:

Definition 3.3.2 : Sei M eine Menge und $P(y)$ ein einstelliges Prädikat, in das man Elemente $y \in M$ einsetzen kann. Dann sagen wir:
Für **fast alle** $y \in M$ gilt $P(y)$, in Zeichen : $\forall' y \in M : P(y)$, wenn die Menge

$$\{ \ z \in M \mid \neg P(z) \ \} \quad \text{endlich ist.}$$

□

Was Folgen in M sind, wissen Sie vielleicht aus der Analysis, nämlich Funktionen a von $\mathbb{N}_0$ in M , die wir aber etwas anders schreiben, nämlich

$$(a_j)_{j\in\mathbb{N}_0} \quad \text{statt} \quad a \quad \text{und} \quad a_j \quad \text{statt} \quad a(j) \ :$$

Definition 3.3.3 : Sei R ein kommutativer Ring und $\mathcal{F}(\mathbb{N}_0, R)$ die Menge der Folgen $(a_j)_{j\in\mathbb{N}_0}$ mit $a_j \in R$.
Dann setzen wir

$$R[X] \quad := \quad \{ \ (a_j)_{j\in\mathbb{N}_0} \in \mathcal{F}(\mathbb{N}_0, R) \mid \forall' j \in \mathbb{N}_0 : \ a_j = 0 \ \} \quad .$$

Hilfssatz und Definition 3.3.4 : Sei M eine nichtleere, endliche Teilmenge von $\mathbb{N}_0$. Dann besitzt M ein **größtes Element**, also ein

$$m \in M \quad \text{mit} \quad \forall\, a \in M : \ a \leq m \quad .$$

Dieses Element bezeichnen wir mit $\max M$.
Beweis durch Induktion nach $n := \#(M)$:
Induktionsanfang: Ist $\#(M) = 1$, also $M = \{a_1\}$, so leistet $m := a_1$ das Gewünschte.
Induktionsschluss: Sei $n \in \mathbb{N}$, und für Mengen M' mit $\#(M') = n$ sei die Behauptung richtig. Sei M eine Teilmenge von $\mathbb{N}_0$ mit $n+1$ Elementen und $b \in M$, dann hat $M' := M \setminus \{b\}$ nur m Elemente, es gibt ein m' mit

$$m' \in M' \quad \text{und} \quad \forall\, a \in M' \ : \ a \leq m' \ .$$

Es kann $b \leq m'$ sein, dann setzen wir $m := m'$. Ist $b > m$, so setzen wir $m := b$.

□

Definition 3.3.5 : Sei $(a_j)_{j\in\mathbb{N}_0} \in R[X]$. Es kann

$$(a_j)_{j\in\mathbb{N}_0} \quad = \quad (0,0,\ldots)$$

sein. Anderenfalls ist $\{\ j\in\mathbb{N}_0 \mid a_j \neq 0\ \}$ nichtleer und endlich. Wir nennen

$$\deg(a_j)_{j\in\mathbb{N}_0} \quad := \quad \max\{\ j\in\mathbb{N}_0 \mid a_j\neq 0\ \}$$

den **Grad** von $(a_j)_{j\in\mathbb{N}_0}$. Für $(0,0,\ldots)$ definieren wir keinen Grad.

Satz 3.3.6 : Sei R ein kommutativer Ring. Setzt man für $(a_j)_{j\in\mathbb{N}_0}, (b_j)_{j\in\mathbb{N}_0} \in R[X]$:

$$(a_j)_{j\in\mathbb{N}_0} + (b_j)_{j\in\mathbb{N}_0} \quad := \quad (a_j+b_j)_{j\in\mathbb{N}_0} \quad ,$$

$$(a_j)_{j\in\mathbb{N}_0} \cdot (b_j)_{j\in\mathbb{N}_0} \quad := \quad \left(\sum_{k=0}^{j} a_k\cdot b_{j-k}\right)_{j\in\mathbb{N}_0} \quad ,$$

so wird $(R[X],+,\cdot)$ ein kommutativer Ring, mit
Nullelement $(0,0,0,\ldots)$ und
Einselement $(1,0,0,\ldots)$.
Den **Beweis** dafür wollen wir nicht im Einzelnen führen. Man muss sich zunächst überlegen, dass aus

$$\forall' j\in\mathbb{N}_0 : \ a_j = 0 \quad \text{und} \quad \forall' j\in\mathbb{N}_0 : \ b_j = 0 \quad \text{auch}$$

$$\forall' j\in\mathbb{N}_0 : \ a_j + b_j = 0 \quad \text{und} \quad \forall' j\in\mathbb{N}_0 : \ \sum_{k=0}^{j} a_k\cdot b_{j-k} = 0$$

folgt. Für letzteres und den Beweis der Assoziativität und Kommutativität von $\cdot$ ist es nützlich, zu verwenden, dass

$$\sum_{k=0}^{j} a_k\cdot b_{j-k} \quad = \quad \sum_{(k,l)\in\mathbb{N}_0\times\mathbb{N}_0 \text{ mit } k+l=j} a_k\cdot b_l$$

gilt.
Bemerkung 3.3.7 : Man möchte haben, dass $R\subset R[X]$ gilt. Das ist dasselbe Problem wie bei der Zahlbereichserweiterung von $\mathbb{Z}$ zu $\mathbb{Q}$. Dort sieht man zunächst nicht, dass ganze Zahlen $n\in\mathbb{Z}$ Brüche sind, aber man kann

$$n \quad \text{mit} \quad \frac{n}{1}\in\mathbb{Q} \quad \text{identifizieren.}$$

Hier wird man ein

$$a\in R \quad \text{mit dem Element} \quad (a,0,0,\ldots)$$

identifizieren; das geht wegen der

Beh. 3.3.8 : $\varphi : R \longrightarrow R[X] \quad , \quad a \longmapsto (a,0,0,\ldots)$ ist ein injektiver Ringhomomorphismus.

Der **Beweis** ist leicht.

□

Folgerung 3.3.9 : Wenn wir für $a \in R$

$a \quad$ statt $\quad (a,0,0,\ldots) \in R[X]$

schreiben, ist es egal, ob wir $a+b$ oder $a \cdot b$ in R oder in $R[X]$ bilden, und dann ist $R \subset R[X]$. Wir setzen noch

$$X \quad := \quad (0,1,0,0,\ldots) \quad , \quad \text{dann gilt}$$

$$X \notin R\,, \quad \text{und} \quad \forall\, k \in \mathbb{N}_0 : \; X^k \quad = \quad (\underbrace{0}_{0\text{-te Stelle}}, \ldots, 0, \underbrace{1}_{k\text{-te Stelle}}, 0, \ldots)\,.$$

Sei nun $(a_j)_{j\in\mathbb{N}_0} \in R[X] \quad , \quad$ dann gibt es ein $n \in \mathbb{N}_0$ mit

$$a_j \quad = \quad 0 \quad \text{für} \quad j > n\,, \quad \text{also}$$

$$\begin{aligned} (a_j)_{j\in\mathbb{N}_0} \quad &= \quad (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \\ &= \quad \sum_{k=0}^{n} (0, \ldots, 0, a_k, 0, \ldots) \\ &= \quad \sum_{k=0}^{n} (a_k, 0, 0, \ldots) \cdot (0, \ldots, 0, \underbrace{1}_{k\text{-te Stelle}}, 0, \ldots) \\ &= \quad \sum_{k=0}^{n} a_k \cdot X^k \quad . \end{aligned}$$

Zwischen Folgen $(a_j)_{j\in\mathbb{N}_0}$ und $(b_j)_{j\in\mathbb{N}_0}$, also Funktionen von $\mathbb{N}_0$ nach R, hat man

$$(a_j)_{j\in\mathbb{N}_0} = (b_j)_{j\in\mathbb{N}_0} \quad \Longleftrightarrow \quad \forall\, j \in \mathbb{N}_0 : \; a_j = b_j\,.$$

Mit dem oben definierten X und der Schreibweise
$\sum\limits_{k=0}^{\infty} a_k \cdot X^k$ statt $(a_0, a_1, \ldots, a_n, 0, \ldots)$ erhält man

Satz und Definition 3.3.10 : Sei $(R, +, \cdot)$ ein kommutativer Ring.

Dann ist

$$R[X] \quad = \quad \left\{ \; \sum_{k=0}^{\infty} a_k \cdot X^k \;\middle|\; \forall\, k \in \mathbb{N}_0 : \, a_k \in R \;\wedge\; \forall' \, k \in \mathbb{N}_0 : \, a_k = 0 \; \right\} \quad ,$$

und $(R[X],+,\cdot)$ ist ein kommutativer Ring, wenn man

$$\sum_{k=0}^{\infty} a_k \cdot X^k + \sum_{k=0}^{\infty} b_k \cdot X^k \quad := \quad \sum_{k=0}^{\infty} (a_k + b_k) \cdot X^k \quad ,$$

$$\left(\sum_{k=0}^{\infty} a_k \cdot X^k \right) \cdot \left(\sum_{k=0}^{\infty} b_k \cdot X^k \right) \quad := \quad \sum_{j=0}^{\infty} \left(\sum_{k=0}^{j} a_k \cdot b_{j-k} \right) \cdot X^j$$

setzt. Es ist

$$X \in R[X] \, , \, X \notin R \quad .$$

$(R[X],+,\cdot)$ heißt der **Polynomring in der Unbestimmten X** über R . Es gilt in $R[X]$:

$$\sum_{k=0}^{\infty} a_k \cdot X^k \, = \, \sum_{k=0}^{\infty} b_k \cdot X^k \quad \Longleftrightarrow \quad \forall \, k \in \mathbb{N}_0 \, : \, a_k \, = \, b_k \, .$$

Damit ist dann für $f(X) \, = \, \sum\limits_{k=0}^{\infty} a_k \cdot X^k \, \neq \, 0$

$$\deg \, f(X) \quad = \quad \max \, \{ \;\; k \in \mathbb{N}_0 \;\; | \;\; a_k \neq 0 \;\; \}$$

definiert. Die Elemente von $R[X]$ heißen **Polynome** in X .

Definition 3.3.11 : Sei R ein kommutativer Ring, mit Einselement 1 , und

$$f(X) \, \in \, R[X] \quad , \quad f(X) \neq 0 \quad ,$$

dann ist also $n \, = \, \deg f(X)$ definiert, und man hat $a_0, \ldots, a_n \in R$ mit

$$f(X) \, = \, \sum_{k=0}^{n} a_k \cdot X^k \quad \text{und} \quad a_n \neq 0 \quad .$$

Das Element

$$\ell(f) \quad := \quad a_n$$

heißt der **Leitkoeffizient** des Polynoms $f(X)$. Ist $f(X) \neq 0$ und

$$\ell(f) \quad = \quad 1 \quad ,$$

so heißt das Polynom $f(X)$ **normiert** .

Behauptung 3.3.12 : Sei R ein kommutativer, nullteilerfreier Ring . Seien $f(X) \, , \, g(X) \, \in \, R[X] \setminus \{0\}$, dann gilt

$$\deg(f(X) \cdot g(X)) \quad = \quad \deg f(X) + \deg g(X) \quad ,$$

$$\ell(f \cdot g) \quad = \quad \ell(f) \cdot \ell(g) \quad ,$$

und der Polynomring ist auch nullteilerfrei.
Beweis : Sei $n := \deg f(X)$, $m := \deg g(X)$, dann ist

$$f(X) = \sum_{k=0}^{n} a_k \cdot X^k \quad \text{mit} \quad \ell(f) = a_n \neq 0 \quad ,$$

$$g(X) = \sum_{k=0}^{m} b_k \cdot X^k \quad \text{mit} \quad \ell(g) = b_m \neq 0 \,, \quad \text{und}$$

$$f(X) \cdot g(X) = \sum_{j=0}^{\infty} \left(\sum_{k=0}^{j} a_k \cdot b_{j-k} \right) \cdot X^j \quad .$$

Ist $j > n + m$ und $k \in \{0, \ldots, j\}$, so kann
(1) $k \leq n$ sein, dann ist $j - k > n + m - n = m$, also $b_{j-k} = 0$,
oder es kann
(2) $k > n$ sein, dann ist $a_k = 0$, auf jeden Fall :

$$a_k \cdot b_{j-k} = 0 \quad . \quad \text{Also ist}$$

$$f(X) \cdot g(X) \quad = \quad \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k \cdot b_{j-k} \right) \cdot X^j \quad ,$$

und für $j = n + m$ gilt $a_k b_{j-k} \neq 0$ höchstens für $k = n$ und $j - k = m$. Also ist

$$\sum_{k=0}^{n+m} a_k \cdot b_{n+m-k} \quad = \quad a_n \cdot b_m \quad = \quad \ell(f) \cdot \ell(g) \quad .$$

Also ist $f(X) \cdot g(X) \neq 0$, $R[X]$ ist nullteilerfrei und wir haben die angegebenen Formeln.

□

Definition 3.3.13 (Einsetzen in Polynome) : Sei R ein kommutativer, nullteilerfreier Ring und

$$f(X) \quad = \quad \sum_{k=0}^{n} a_k \cdot X^k \in R[X]$$

ein Polynom, dann kann man für X jedes Element aus $R[X]$ einsetzen, man kann etwa

$$f(X^2) \quad := \quad \sum_{k=0}^{n} a_k \cdot X^{2k}$$

bilden. Insbesondere kann man jedes $\lambda \in R$ einsetzen, man kann

$$f(\lambda) \quad := \quad \sum_{k=0}^{n} a_k \cdot \lambda^k \ \in \ R$$

bilden und erhält so zu $f(X) \in R[X]$ eine Polynomfunktion

$$\tilde{f} \in \mathcal{F}(R,R) \quad , \quad \tilde{f}(\lambda) := f(\lambda) \quad .$$

Macht man nun die Menge $\mathcal{F}(R,R)$ zu einem Ring $(\mathcal{F}(R,R),+,\cdot)$, indem man für $g, h \in \mathcal{F}(R,R)$

$$g+h : \ R \ \longrightarrow \ R \quad \text{durch} \quad (g+h)(\lambda) := g(\lambda)+h(\lambda) \quad ,$$

$$g \cdot h : \ R \ \longrightarrow \ R \quad \text{durch} \quad (g \cdot h)(\lambda) := g(\lambda) \cdot h(\lambda)$$

für $\lambda \in R$ definiert, so wird die Abbildung

$$\widetilde{\ } \ : \ R[X] \ \longrightarrow \ \mathcal{F}(R,R) \quad , \quad f(X) \longmapsto \tilde{f}$$

ein Ring-Homomorphismus (wozu man

$$\widetilde{f_1+f_2} = \tilde{f}_1+\tilde{f}_2 \quad , \quad \widetilde{f_1 \cdot f_2} = \tilde{f}_1 \cdot \tilde{f}_2 \quad \text{für} \quad f_1 \, , \, f_2 \in R[X]$$

im Einzelnen nachrechnen müsste). $\widetilde{\ }$ ist i.A. nicht surjektiv; man sieht, etwa für $R := \mathbb{R}$, leicht, dass es Funktionen gibt, die keine Polynomfunktionen sind. Z.B. ist

$$\sin : \ \mathbb{R} \ \longrightarrow \ \mathbb{R}$$

ungleich 0 und hat unendlich viele "Nullstellen". Nach dem nächsten Satz haben Polynomfunktionen $\neq 0$ aber nur endlich viele Nullstellen. Die Abbildung $\widetilde{\ }$ ist i.A. aber auch nicht injektiv, wie wir in (3.3.1) gesehen haben:

$$f(X) := X \quad \text{und} \quad g(X) := X^3 \in \mathbb{Z}/_{(3)}[X]$$

sind verschiedene Polynome, aber für die Polynomfunktionen gilt

$$\tilde{f}(\lambda) = \lambda = \lambda^3 = \tilde{g}(\lambda) \quad \text{für alle} \quad \lambda \in \mathbb{Z}/_{(3)} \quad , \quad \text{also}$$

$$\tilde{f} \quad = \quad \tilde{g} \quad .$$

$\widetilde{\ }$ ist aber injektiv, wenn R unendlich viele Elemente hat, das ist Satz 3.3.15 . Zunächst

Definition und Satz 3.3.14 : Sei R ein kommutativer, nullteilerfreier Ring. Für $f(X) \in R[X]$ heißt

$$N(f(X)) \quad := \quad \{\ \alpha \in R \mid f(\alpha) = 0\ \}$$

die Menge der **Nullstellen** von $f(X)$. Es gilt dann für $f(X) \neq 0$:

$$\#(N(f(X))) \leq \deg f(X) \quad .$$

Beweis durch Induktion nach $\deg f(X)$:
Induktionsanfang: Ist $\deg f(X) = 0$, so ist

$$f(X) \quad = \quad a_0 \in R \quad , \quad a_0 \neq 0 \quad ,$$

es gibt kein $\alpha \in R$ mit $f(\alpha) = 0$, also

$$\#(N(f(X))) \quad = \quad 0 \quad = \quad \deg f(X) \quad .$$

Induktionsschluss: Sei $n \in \mathbb{N}$, und für Polynome vom Grad $n-1$ sei die Beh. richtig. Sei nun $f(X) \in R[X] \setminus \{0\}$ und $\deg f(X) = n$. Es kann sein, dass es keine Nullstelle von $f(X)$ gibt, dann ist

$$\#(N(f(X))) \quad = \quad 0 \quad < \quad n \quad = \quad \deg f(X) \quad ,$$

die Behauptung ist also für $f(X)$ richtig. Sonst: Sei α eine Nullstelle von $f(X)$,

$$f(X) \quad = \quad \sum_{k=0}^{n} a_k \cdot X^k \quad \text{mit} \quad a_n \neq 0 \quad ,$$

dann ist $f(\alpha) = 0$, also

$$f(X) = f(X) - f(\alpha) = \sum_{k=0}^{n} a_k \cdot X^k - \sum_{k=0}^{n} a_k \cdot \alpha^k = \sum_{k=1}^{n} a_k \cdot (X^k - \alpha^k) \quad .$$

Wie Sie durch Ausmultiplizieren (ohne Induktion) beweisen können, ist für alle $j \in \mathbb{N}$:

$$X^j - \alpha^j \quad = \quad (X - \alpha) \cdot \sum_{l=0}^{j-1} X^l \cdot \alpha^{j-1-l} \quad , \quad \text{also}$$

$$f(X) \quad = \quad (X - \alpha) \cdot \sum_{k=1}^{n} a_k \cdot \left(\sum_{j=0}^{k-1} X^j \cdot \alpha^{k-1-j} \right) \quad .$$

Nun ist $g(X) := \sum_{k=1}^{n} a_k \cdot \left(\sum_{j=0}^{k-1} X^j \cdot \alpha^{k-1-j} \right)$ ein Polynom vom Grad $n-1$, denn die höchste Potenz von X , die darin vorkommt, ist X^{n-1}, mit dem Koeffizienten $a_n \neq 0$. Also ist

$$f(X) \quad = \quad (X-\alpha) \cdot g(X) \quad \text{mit} \quad \deg g(X) \quad = \quad n-1 \quad ,$$

und da R nullteilerfrei ist, ist eine Nullstelle von $f(X)$ eine Nullstelle von $X-\alpha$ oder von $g(X)$, und $g(X)$ hat höchstens $n-1$ Nullstellen. Also ist

$$\#(N(f(X))) \leq 1+(n-1) = n \quad . \qquad \square$$

Man erhält damit den

Satz 3.3.15: Sei R ein kommutativer, nullteilerfreier Ring und unendlich vielen Elementen, dann ist die Abbildung

$$\tilde{} : \; R[X] \longrightarrow \mathcal{F}(R,R) \quad ,$$

die dem Polynom

$$f(X) \quad = \quad \sum_{k=0}^{n} a_k \cdot X^k \quad \in \quad R[X]$$

die Polynomfunktion $\tilde{f} : \; R \longrightarrow R \quad , \quad \tilde{f}(\lambda) \quad := \quad \sum_{k=0}^{n} a_k \cdot \lambda^k$

zuordnet, injektiv.
Beweis : Seien $f_1(X)$, $f_2(X) \in R[X]$ und

$$\tilde{f_1} \quad = \quad \tilde{f_2} \quad ,$$

dann hat das Polynom

$$f_1(X) - f_2(X)$$

unendlich viele Nullstellen, nämlich alle $\lambda \in R$. Nach Satz 3.3.14 geht das nur, wenn $f_1(X) - f_2(X)$ das Nullpolynom ist, also:

$$f_1(X) \quad = \quad f_2(X) \quad . \qquad \square$$

Für den folgenden Satz braucht man nun einen Körper K. Für die Elemente aus $K[X]$werden wir im Rest dieses Abschnitts, wie schon in 3.3.13, einfach

$$f \, , \, g \, , \, , \ldots \quad \text{statt} \quad f(X) \, , \, g(X) \, , \ldots$$

schreiben:
Satz 3.3.16 : Sei K ein Körper, $f, g \in K[X]$ und $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ mit

$$f \quad = \quad q \cdot g + r \wedge (r \, = \, 0 \vee \deg r < \deg g) \quad .$$

Beweis : 1) der Eindeutigkeit von q und r : Seien auch $q', r' \in K[X]$ mit

$$f \quad = \quad q' \cdot g + r' \wedge (r' \, = \, 0 \vee \deg r' < \deg g \,) \quad , \quad \text{dann folgt}$$

$$0 \quad = \quad (q - q') \cdot g + (r - r') \quad , \quad \text{also}$$

$$(q - q') \cdot g \quad = \quad r' - r \quad .$$

Aus $q - q' \neq 0$ würde folgen: $\deg(q - q') \geq 0$, also nach Behauptung 3.3.12:

$$\deg(r' - r) \quad = \quad \deg((q - q') \cdot g) \quad = \quad \deg(q - q') + \deg g \geq \deg g \quad ,$$

aber $(r = 0 \vee \deg r < \deg g) \wedge (r' = 0 \vee \deg r' < \deg g)$, also
$r - r' \, = \, 0 \, \vee \deg(r - r') \, < \, \deg g$, Widerspruch.
Also ist $q - q' = 0$, $q = q'$, und damit

$$r - r' \quad = \quad 0 \quad , \quad r = r' \, .$$

2) der Existenz von q, r :
a) Ist $f = 0 \quad , \quad$ so kann man $q := r := 0$ nehmen.
b) Ist $f \neq 0 \quad , \quad$ so beweisen wir die Existenz von q, r durch Induktion nach $\deg f$:
Induktionsanfang : Ist $\deg f \, = \, 0$, so ist $f(X) = a \in K \setminus \{0\}$. Ist $\deg g = 0$, also $g(X) = b \in K \setminus \{0\}$, so ist
$a \, = \, a \cdot b^{-1} \cdot b + 0 \quad , \quad$ wir können also $q := a \cdot b^{-1}$ und $r := 0$ nehmen.
Ist $\deg g \geq 1$, so haben wir
$a \quad = \quad 0 \cdot g + a$, wir können also $q := 0$ und $r := a$ nehmen.
Induktionsschluss : Sei $\deg f = m \in \mathbb{N}$, und für Polynome $u \in K[X]$ mit $\deg u < m$ sei die Behauptung richtig. Trivial ist der Fall
$\deg g > m$: Dann können wir
$r := f \quad , \quad q := 0$ nehmen, dann ist
$f = 0 \cdot g + f \, \wedge \deg f < \deg g \quad .$ Sei nun
$\deg g \leq m \quad , \quad$ also

$$f(X) \quad = \quad \sum_{k=0}^{m} a_k \cdot X^k \quad , \quad g(X) \quad = \quad \sum_{k=0}^{n} b_k \cdot X^k \quad \text{mit} \quad a_m, b_n \neq 0$$

und $n \leq m$, so ist

$$u(X) \quad := \quad f(X) - a_m \cdot {b_n}^{-1} \cdot g(X) \cdot X^{m-n}$$

ein Polynom, bei dem X^m den Koeffizienten

$$a_m - a_m \cdot {b_n}^{-1} \cdot b_n \quad = \quad 0$$

hat, also ist $\deg u < m$ oder $u = 0$. Ist $u = 0$, so haben wir

$$f(X) \quad = \quad q(X) \cdot g(X) + 0 \quad \text{mit} \quad q(x) \quad := \quad a_m \cdot {b_n}^{-1} \cdot X^{m-n} .$$

Ist $\deg u < m$, so können wir die Induktionsvoraussetzung anwenden: Es gibt $q_1, r \in K[X]$ mit

$$u \quad = \quad q_1 \cdot g + r \ \wedge \ (r = 0 \vee \deg r < \deg g) \quad , \quad \text{also}$$

$$f(X) \quad = \quad (q_1(X) + a_m \cdot {b_n}^{-1} \cdot X^{m-n}) \cdot g(X) + r(X) \quad ,$$

und mit $q(X) \quad := \quad q_1(X) + a_m \cdot {b_n}^{-1} \cdot X^{m-n}$ folgt die Behauptung.

□

Man kann also im Polynomring $K[X]$, wenn K ein Körper ist, "mit Rest dividieren", so wie wir es in Satz 3.2.3 für $\mathbb{Z}$ bewiesen haben. Man definiert daher allgemein:

Definition 3.3.17 : Sei $(R, +, \cdot)$ ein kommutativer, nullteilerfreier Ring. R heißt ein **euklidischer Ring** , wenn es eine Funktion

$$\delta \ : \ R \setminus \{0\} \ \longrightarrow \ \mathbb{N}_0$$

gibt mit folgender Eigenschaft: Zu $a, b \in R$ mit $b \neq 0$ gibt es Elemente $q, r \in R$ mit

$$a \ = \ q \cdot b + r \quad \text{und entweder } r \ = \ 0 \text{ oder } \delta(r) < \delta(b) \ .$$

Die Abbildung δ heißt dann eine **Gradfunktion** .

□

(3.3.18) Beispiele: (1) Setzt man für $c \in \mathbb{Z} \setminus \{0\}$:

$$|\, c \,| \quad := \quad \begin{cases} c & \text{für} \quad 0 < c \\ -c & \text{für} \quad c < 0 \end{cases} \quad ,$$

so kann man $\delta(c) := |\, c \,|$ für $c \neq 0$ setzen. $\mathbb{Z}$ mit δ wird dann ein euklidischer Ring.
(2) Sei K ein Körper, dann wird der Polynomring $K[X]$ mit $\delta := \deg$ ein euklidischer Ring.

Der Vorteil dieser allgemeinen Definition ist, dass man damit sehr übersichtlich folgenden Satz beweisen kann - den wir für $\mathbb{Z}$ schon als Satz 3.2.5 bewiesen haben:

Satz 3.3.19 : Sei $(R, +, \cdot)$ ein euklidischer Ring, und I ein Ideal von R. Dann gibt es ein $d \in R$ mit

$$I = (d) := \{ \ x \cdot d \mid x \in R \ \} \quad .$$

Beweis : Sei δ die Gradfunktion von R. Ist $I = \{0\}$, so können wir $d := 0$ nehmen. Sonst ist

$$M \quad := \quad \{ \ \delta(x) \mid x \in I \setminus \{0\} \ \}$$

eine nichtleere Teilmenge von $\mathbb{N}_0$, es existiert also $\min M$, und dazu ein $d \in M$ mit $\delta(d) = \min M$. Sei nun $y \in I$ beliebig. Dann gibt es $q, r \in R$ mit

$$y = q \cdot d + r \quad \text{und} \quad (r = 0 \vee \delta(r) < \delta(d)) \quad .$$

Wegen $d, y \in I$ folgt $r \in I$, und aus $r \neq 0$ würde $\delta(r) < \delta(d) = \min M$ folgen, Widerspruch zur Definition von M . Also ist $r = 0$ und damit

$$y = q \cdot d \in (d) \quad ,$$

und damit $I \subset (d)$. $(d) \subset I$ gilt wegen $d \in I$.

□

Wie in $\mathbb{Z}$ kann man in $K[X]$ Teilbarkeit und Primelemente definieren:

Definition 3.3.20 : Sei K ein Körper und seien $f, g \in K[X]$. Wir sagen:

$$f \,|\, g \quad , \quad \text{gesprochen: } f \ \underline{\text{teilt}} \ g \quad :\Longleftrightarrow \quad \exists\, h \in K[X] \ : \ f \cdot h = g \quad .$$

Definition 3.3.21 : Sei $p \in K[X] \setminus \{0\}$, $\deg(p) \neq 0$.
p heißt ein **Primpolynom**, wenn gilt

$$\forall\, f, g \in K[X] \ : \ (\, p \,|\, f \cdot g \quad \Longrightarrow \quad p \,|\, f \ \vee \ p \,|\, g \,) \quad .$$

Mit einem Beweis, den man fast wörtlich bei Satz 3.2.8 abschreiben kann (und den wir besser gleich allgemeiner für euklidische Ringe bewiesen hätten) zeigt man, dass man Primpolynome nicht in ein Produkt von Polynomen mit kleinerem Grad zerlegen kann - außer einer der Faktoren hat den Grad 0 :

Satz 3.3.22 : Sei K ein Körper. Ein Polynom $p \in K[X] \setminus \{0\}$ ist genau dann ein Primpolynom, wenn gilt

$$\forall\, f, g \in K[X] \ : \ (p = f \cdot g \quad \Longrightarrow \quad \deg f = 0 \ \vee \ \deg g = 0)$$

□

Bemerkung 3.3.23 : Ist R ein kommutativer, nullteilerfreier Ring, so haben wir in 3.3.10 und 3.3.12 gesehen, dass auch $R[X]$ ein kommutativer, nullteilerfreier Ring ist. Wir können daher den Polynomring in einer Unbestimmten über $R[X]$ bilden, mit einer Unbestimmten, die nicht in $R[X]$ liegt und die wir daher nicht X nennen können. Nennen wir sie Y, so haben wir

$$R[X,Y] \quad := \quad (R[X])[Y]$$

und nennen $(R[X,Y],+,\cdot)$ den **Polynomring in zwei Unbestimmten** über R . Als Menge ist

$$R[X,Y] = \left\{ \sum_{j,k=0}^{\infty} a_{jk} \cdot X^j \cdot Y^k \;\middle|\; a_{jk} \in R \wedge a_{jk} = 0 \,\text{für fast alle}\, j,k \in \mathbb{N}_0 \right\} .$$

Man muss aber vorsichtig sein, nicht alle Eigenschaften des Polynomrings in einer Unbestimmten hat auch der Polynomring in zwei Unbestimmten, z.B.: Hat man einen Körper K , so ist $K[X]$ nach Satz 3.3.16 und Def. 3.3.17 ein euklidischer Ring. $K[X,Y]$ ist es aber nicht !

□

3.4 Der Körper der Brüche

Aus der Schule wissen Sie, dass man den Ring $(\mathbb{Z},+,\cdot)$ der ganzen Zahlen erweitern kann zum Körper der rationalen Zahlen. Das geht allgemein für kommutative, nullteilerfreie Ringe :

Satz und Definition 3.4.1 : Sei $(R,+,\cdot)$ ein kommutativer, nullteilerfreier Ring, mit Nullelement 0 und Einselement 1. Wir setzen

$$R^* := R \setminus \{0\} \quad .$$

Dann wird durch

$$(a,f) \sim (b,g) \quad :\Longleftrightarrow \quad a \cdot g = b \cdot f \quad \text{für} \quad a,b \in R\,,\; f,g \in R^*$$

eine Äquivalenzrelation auf der Menge $R \times R^*$ definiert. Für die Äquivalenzklasse von (a,f) schreiben wir: $\dfrac{a}{f}$. Dann wird

$$Q(R) := \left\{ \frac{a}{f} \;\middle|\; a \in R, f \in R^* \right\}$$

ein Körper $(Q(R), \oplus, \odot)$, mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$, wenn man definiert:

$$\frac{a}{f} \oplus \frac{b}{g} := \frac{a \cdot g + b \cdot f}{f \cdot g},$$

$$\frac{a}{f} \odot \frac{b}{g} := \frac{a \cdot b}{f \cdot g} \quad ,$$

für $a, b \in R, f, g \in R^*$. $(Q(R), \oplus, \odot)$ heißt der **Körper der Brüche** oder auch der **Quotientenkörper** von R . In $Q(R)$ können wir "kürzen": Es gilt

(Kü) $$\frac{a \cdot g}{f \cdot g} = \frac{a}{f} \quad \text{für alle} \quad a \in R\,,\ f, g \in R^* \quad .$$

Beweis : Im Folgenden seien stets $a, b, c, a', b' \in R\,,\ f, g, h, f', g' \in R^*$.

(1) Wir zeigen zunächst, dass $\sim$ eine Äquivalenzrelation auf $R \times R^*$ ist: Es gilt

(Ä1) $(a, f) \sim (a, f)$ wegen $a \cdot f = a \cdot f$,

(Ä2) $(\ (a, f) \sim (b, g) \implies (b, g) \sim (a, f)\ )$ wegen

$$a \cdot g = b \cdot f \implies b \cdot f = a \cdot g \quad .$$

(Ä3) $(\ (a, f) \sim (b, g) \ \wedge\ (b, g) \sim (c, h)\ )$

$$\implies (a \cdot g = b \cdot f \ \wedge\ b \cdot h = c \cdot g)$$

$$\implies (a \cdot g \cdot h = b \cdot f \cdot h \ \wedge b \cdot h \cdot f = c \cdot g \cdot f) \quad .$$

Wegen der Kommutativität des Ringes R folgt daraus

$$a \cdot h \cdot g = c \cdot f \cdot g \quad , \qquad \text{also} \quad (a \cdot h - c \cdot f) \cdot g = 0 \quad .$$

Wegen der Nullteilerfreiheit von R, und wegen $g \in R^*$, also $g \neq 0$, folgt daraus

$$a \cdot h - c \cdot f = 0 \quad , \qquad \text{also} \quad a \cdot h = c \cdot f \quad , \qquad \text{also} \quad (a, f) \sim (c, h) \quad .$$

(Kü) folgt sofort aus der Definition von $\sim$.

(2) Wir zeigen nun, dass Addition $\oplus$ und Multiplikation $\odot$ in $Q(R)$ eindeutig definiert (also "wohldefiniert") sind : Es gelte

$$\frac{a}{f} = \frac{a'}{b'} \quad \text{und} \quad \frac{b}{g} = \frac{b'}{g'} \quad , \quad \text{dann gilt}$$

$$(a, f) \sim (a', f') \ \wedge\ (b, g) \sim (b', g')\,, \quad \text{also}$$

$$(*) \qquad a \cdot f' = a' \cdot f \ \wedge b \cdot g' = b' \cdot g \quad .$$

Aus $(*)$ erhalten wir :

$$a \cdot f' \cdot g \cdot g' = a' \cdot f \cdot g \cdot g' \quad \wedge \quad b \cdot g' \cdot f \cdot f' = b' \cdot g \cdot f \cdot f' \quad .$$

Wir addieren die beiden Gleichungen. Unter Verwendung der Kommutativität der Multiplikation und des Distributivgesetzes in R folgt :

$$(a \cdot g + b \cdot f) \cdot g' \cdot f' = (a' \cdot g' + b' \cdot f') \cdot g \cdot f \quad , \qquad \text{also}$$

$$(a \cdot g + b \cdot f, f \cdot g) \sim (a' \cdot g' + b' \cdot f', f' \cdot g') \quad , \qquad \text{also}$$

$$\frac{a \cdot g + b \cdot f}{f \cdot g} = \frac{a' \cdot g' + b' \cdot f'}{f' \cdot g'} \quad .$$

$\oplus$ ist also wohldefiniert. Und aus $(*)$ folgt durch Multiplikation der beiden Gleichungen:

$$a \cdot b \cdot f' \cdot g' = a' \cdot b' \cdot f \cdot g \quad , \qquad \text{also}$$

$$(a \cdot b, f \cdot g) \sim (a' \cdot b', f' \cdot g') \quad , \qquad \text{also} \quad \frac{a \cdot b}{f \cdot g} = \frac{a' \cdot b'}{f' \cdot g'} \quad .$$

Also ist auch $\odot$ wohldefiniert.

(3) Ohne Probleme, aber mühsam, können wir nun zeigen, dass $(Q(R), \oplus)$ eine abelsche Gruppe ist. Wir verwenden dabei die Rechenregeln im Ring $(R, +, \cdot)$, ohne sie jedesmal zu erwähnen:

$$\left(\frac{a}{f} \oplus \frac{b}{g}\right) \oplus \frac{c}{h} = \frac{a \cdot g + b \cdot f}{f \cdot g} \oplus \frac{c}{h} = \frac{(a \cdot g + b \cdot f) \cdot h + c \cdot (f \cdot g)}{(f \cdot g) \cdot h}$$

$$= \frac{a \cdot g \cdot h + b \cdot f \cdot h + c \cdot f \cdot g}{f \cdot g \cdot h} \quad ,$$

und das erhält man auch , wenn man

$$\frac{a}{f} \oplus \left(\frac{b}{g} \oplus \frac{c}{h}\right)$$

ausrechnet, also gilt das Assoziativgesetz für $\oplus$. Und

$$\frac{a}{f} \oplus \frac{b}{g} = \frac{a \cdot g + b \cdot f}{f \cdot g} = \frac{b \cdot f + a \cdot g}{g \cdot f} = \frac{b}{g} \oplus \frac{a}{f} \quad ,$$

es gilt also auch das Kommutativgesetz für $\oplus$. Wegen

$$\frac{a}{f} \oplus \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot f}{f \cdot 1} = \frac{a}{f}$$

ist $\frac{0}{1}$ das neutrale Element in $(Q(R), \oplus)$. Zu $\frac{a}{f}$ haben wir das Negative $\frac{-a}{f}$, denn

$$\begin{aligned} \frac{a}{f} \oplus \frac{-a}{f} &= \frac{a \cdot f + (-a) \cdot f}{f \cdot f} = \frac{(a + (-a)) \cdot f}{f \cdot f} \\ &\overset{\text{(Kü)}}{=} \frac{a + (-a)}{f} = \frac{0}{f} = \frac{0 \cdot f}{1 \cdot f} \overset{\text{(Kü)}}{=} \frac{0}{1} . \end{aligned}$$

Bezüglich $\oplus$ haben wir also

$$-\frac{a}{f} = \frac{-a}{f} .$$

(4) Einfacher ist es, nachzurechnen, dass $(Q(R), \odot)$ eine Halbgruppe ist: Es gilt

$$\begin{aligned} \left(\frac{a}{f} \odot \frac{b}{g}\right) \odot \frac{c}{h} &= \frac{a \cdot b}{f \cdot g} \odot \frac{c}{h} = \\ \frac{(a \cdot b) \cdot c}{(f \cdot g) \cdot h} &= \frac{a \cdot (b \cdot c)}{f \cdot (g \cdot h)} = \frac{a}{f} \odot \left(\frac{b}{g} \odot \frac{c}{h}\right) . \end{aligned}$$

Es gilt auch das Kommutativgesetz für $\odot$:

$$\frac{a}{f} \odot \frac{b}{g} = \frac{a \cdot b}{f \cdot g} = \frac{b \cdot a}{g \cdot f} = \frac{b}{g} \odot \frac{a}{f} .$$

(5) $\frac{1}{1}$ ist das Einselement in $(Q(R), \cdot)$ wegen

$$\frac{a}{f} \odot \frac{1}{1} = \frac{a \cdot 1}{f \cdot 1} = \frac{a}{f} .$$

(6) Nun zum Distributivgesetz: Da $\odot$ kommutativ ist, brauchen wir nur eine Gleichung nachzurechnen. Es gilt

$$\begin{aligned} \left(\frac{a}{f} \oplus \frac{b}{g}\right) \odot \frac{c}{h} &= \frac{a \cdot g + b \cdot f}{f \cdot g} \odot \frac{c}{h} = \frac{(a \cdot g + b \cdot f) \cdot c}{(f \cdot g) \cdot h} \\ &= \frac{a \cdot c \cdot g + b \cdot c \cdot f}{f \cdot g \cdot h} \overset{\text{(Kü)}}{=} \frac{a \cdot c \cdot g \cdot h + b \cdot c \cdot f \cdot h}{(f \cdot h) \cdot (g \cdot h)} \\ &= \frac{a \cdot c}{f \cdot h} \oplus \frac{b \cdot c}{g \cdot h} = \left(\frac{a}{f} \odot \frac{c}{h}\right) \oplus \left(\frac{b}{g} \odot \frac{c}{h}\right) . \end{aligned}$$

(5) Um den Beweis, dass $(Q(R), \oplus, \odot)$ ein Körper ist, zu vervollständigen, müssen wir nur noch die Eigenschaft (KK) nachweisen: Sei

$$\frac{a}{f} \in Q(R) \quad , \quad \frac{a}{f} \neq \frac{0}{1} \quad ,$$

dann ist $a \in R^*$, denn aus $a = 0$ würde

$$\frac{a}{f} = \frac{0}{f} = \frac{0 \cdot f}{f} \quad \overset{(\text{Kü})}{=} \quad \frac{0}{1}$$

folgen. Zu $\frac{a}{f}$ mit $a \in R^*$ haben wir aber

$$\frac{f}{a} \in Q(R) \quad , \qquad \text{und} \quad \frac{f}{a} \odot \frac{a}{f} \quad = \quad \frac{f \cdot a}{a \cdot f} \quad \overset{(\text{Kü})}{=} \quad \frac{1}{1} \quad .$$

In $(Q(R), \odot)$ haben wir also

$$\left(\frac{a}{f}\right)^{-1} \quad = \quad \frac{f}{a} \quad \text{für} \quad a, f \in R^* \quad .$$

□

Folgerung 3.4.2 : Sei $(R, +, \cdot)$ ein kommutativer, nullteilerfreier Ring und $Q(R)$ der in 3.4.1 definierte Körper der Brüche von R. Dann ist durch

$$j \; : \; R \; \longrightarrow \; Q(R) \quad , \quad a \mapsto \frac{a}{1}$$

ein injektiver Ringhomomorphismus von $(R, +, \cdot)$ in $(Q(R), \oplus, \odot)$ definiert. Wenn wir nun

$$a \quad \text{statt} \quad \frac{a}{1} \quad \text{für} \quad a \in R$$

und $+$ statt $\oplus$, $\cdot$ statt $\odot$ in $Q(R)$ schreiben, ist $(R, +, \cdot)$ ein Unterring von $(Q(R), +, \cdot)$.

□

(3.4.3) Beispiele für Körper der Brüche:
(1) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring. Der Körper der Brüche ist der Körper

$$Q(\mathbb{Z}) \quad = \quad \mathbb{Q}$$

der rationalen Zahlen. Das wissen Sie aus der Schule, aber es ist zu bezweifeln, dass Sie das dort so ausführlich wie in Satz 3.4.1 bewiesen haben !
(2) Sei K ein Körper. Nach (3.3.10) und (3.3.12) ist dann der Polynomring $K[X]$ ein kommutativer, nullteilerfreier Ring , und daher können wir

$$K(X) \; := \; Q(K[X]) \; = \; \left\{ \; \frac{f(X)}{g(X)} \; \middle| \; f(X), g(X) \in K[X] \; \wedge \; g(X) \neq 0 \; \right\}$$

bilden. $K(X)$ heißt der **Körper der rationalen Funktionen** mit Koeffizienten in K .

3.5 Der Körper der komplexen Zahlen

Die Einführung der komplexen Zahlen ist eigentlich Schulstoff. Da aber erfahrungsgemäß nicht jeder Abiturient die komplexen Zahlen kennt, und wir sie von §4 an ständig brauchen, geben wir hier eine kurze Einführung.

(3.5.1) Die Anordnung der reellen Zahlen : Wir wollen hier nicht auch noch die reellen Zahlen definieren, und nicht mal alle Axiome angeben, durch die der Körper $(\mathbb{R}, +, \cdot)$ charakterisiert ist. Was wir brauchen, ist die Anordnung der reellen Zahlen. Man muss wissen:
$(\mathbb{R}, +, \cdot)$ ist ein Körper, mit Nullelement 0 und Einselement 1. In $\mathbb{R}$ gibt es eine Teilmenge $\mathbb{R}_+^*$ von Zahlen, die man als **positive reelle Zahlen** bezeichnet, mit den Eigenschaften:
(AK1) Für alle $a \in \mathbb{R}$ gilt genau eine der drei Aussagen:

$$a \in \mathbb{R}_+^* \,,\; a = 0 \,,\; -a \in \mathbb{R}_+^* .$$

(AK2) $\forall\, a, b \in \mathbb{R}_+^* \;:\; a + b \in \mathbb{R}_+^*$,
(AK3) $\forall\, a, b \in \mathbb{R}_+^* \;:\; a \cdot b \in \mathbb{R}_+^*$.
Der Vollständigkeit halber, aber man braucht es nur in der Analysis: Es gilt noch
(AK4) $\forall\, a \in \mathbb{R}\, \exists\, n \in \mathbb{N} \;:\; n\,1 - a \in \mathbb{R}_+^*$.
Man kann damit für $a, b \in R$ definieren:

$$a < b \quad :\Longleftrightarrow \quad b - a \in \mathbb{R}_+^*, \quad \text{und}: \quad a \leq b \quad :\Longleftrightarrow \quad (a < b \vee a = b) \quad .$$

Wir schreiben gelegentlich noch $b > a$ statt $a < b$ und $b \geq a$ statt $a \leq b$. Für reelle Zahlen gelten dann die Anordnungsaxiome (O1) - (O6) , wie wir sie aus 1.2.3 und 3.2.1 für die ganzen Zahlen kennen.

Folgerung 3.5.2 : (i) Für alle reellen Zahlen a gilt $0 \leq a^2$,
(ii) $-1 < 0$.
Beweis : (i) Ist $a = 0$, so gilt nach Folgerung 3.1.4(1) : $a^2 = 0 \cdot 0 = 0$.
Ist $a \in \mathbb{R}_+^*$, so ist $a^2 = a \cdot a \in \mathbb{R}_+^*$ nach (AK3) .
Ist $a \notin \mathbb{R}_+^*$ und $a \neq 0$, so ist $-a \in \mathbb{R}_+^*$ nach (AK1) , und nach Folgerung 3.1.4(5):

$$a^2 = a \cdot a = (-a) \cdot (-a) \in \mathbb{R}_+^* \quad \text{nach (AK3)} \quad ,$$

in jedem Fall also $0 \leq a^2$.
(ii) Nach (i) und wegen $1 \neq 0$ ist $0 < 1 \cdot 1 = 1$, also $1 \in \mathbb{R}_+^*$, also

$0-(-1) \in \mathbb{R}_+^*$, also $-1 < 0$.

□

Man entnimmt dieser Folgerung: -1 ist nicht Quadrat einer reellen Zahl. Wir wollen nun $\mathbb{R}$ so zu einem Körper $\mathbb{C}$ erweitern, dass es in $\mathbb{C}$ ein Element mit -1 als Quadrat gibt. Das wird dann aber kein Körper sein, in dem es eine Teilmenge mit den Eigenschaften (AK1)- (AK3) gibt.

Definition 3.5.3 : In der Menge

$$\mathbb{C} \quad := \quad \{ \ (x,y) \ \mid \ x,y \in \mathbb{R} \ \}$$

definieren wir eine Addition $\oplus$ und eine Multiplikation $\odot$ durch

$$(a,b) \oplus (u,v) \ := \ (a+u, b+v) \quad ,$$

$$(a,b) \odot (u,v) \ := \ (a \cdot u - b \cdot v, a \cdot v + b \cdot u)$$

für $a, b, u, v \in \mathbb{R}$.

Satz und Definition 3.5.4 : Mit der in 3.5.3 definierten Addition $\oplus$ und Multiplikation $\odot$ erhalten wir einen Körper $(\mathbb{C}, \oplus, \odot)$, mit Nullelement $(0,0)$ und Einselement $(1,0)$,den wir den **Körper der komplexen Zahlen** nennen.

Beweis : Man sieht, dass $\oplus$ und $\odot$ Abbildungen von $\mathbb{C} \times \mathbb{C}$ nach $\mathbb{C}$, also Verknüpfungen auf $\mathbb{C}$, sind.
Seien im Folgenden $(a,b), (u,v), (s,t) \in \mathbb{C}$.
(1) Wir zeigen, dass $(\mathbb{C}, \oplus)$, eine abelsche Gruppe ist: Es gilt

$$((a,b) \oplus (u,v)) \oplus (s,t) \ = \ (a+u, b+v) \oplus (s,t) \ = \ ((a+u)+s, (b+v)+t)$$

$$= \ (a+(u+s), b+(v+t)) \ = \ (a,b) \oplus (u+s, v+t) \ = \ (a,b) \oplus ((u,v) \oplus (s,t)) \quad ,$$

$$(a,b) \oplus (u,v) \ = \ (a+u, b+v) \ = \ (u+a, v+b) \ = \ (u,v) \oplus (a,b) \quad ,$$

$$(a,b) \oplus (0,0) \quad = \quad (a+0, b+0) \quad = \quad (a,b) \quad ,$$

also ist $(0,0)$ das Nullelement, und

$$(a,b) \oplus (-a,-b) \quad = \quad (a+(-a), b+(-b)) \quad = \quad (0,0) \quad ,$$

also ist $(-a,-b)$ das Negative von $(a,b) \in \mathbb{C}$,

$$-(a,b) \quad = \quad (-a,-b) \quad .$$

(2) Wir zeigen nun, dass $(\mathbb{C}, \oplus, \odot)$ ein kommutativer Ring ist: Es gilt

$$((a,b) \odot (u,v)) \odot (s,t) \ = \ (a \cdot u - b \cdot v, a \cdot v + b \cdot u) \odot (s,t)$$

$$= ((a\cdot u - b\cdot v)\cdot s - (a\cdot v + b\cdot u)\cdot t, (a\cdot u - b\cdot v)\cdot t + (a\cdot v + b\cdot u)\cdot s)$$
$$= (a\cdot u\cdot s - b\cdot v\cdot s - a\cdot v\cdot t - b\cdot u\cdot t, a\cdot u\cdot t - b\cdot v\cdot t + a\cdot v\cdot s + b\cdot u\cdot s)$$
$$= (a\cdot(u\cdot s - v\cdot t) - b\cdot(u\cdot t + v\cdot s), a\cdot(u\cdot t + v\cdot s) + b\cdot(u\cdot s - v\cdot t))$$
$$= (a,b)\odot(u\cdot s - v\cdot t, u\cdot t + v\cdot s) = (a,b)\odot((u,v)\odot(s,t)) \quad ,$$

$$(a,b)\odot(u,v) = (a\cdot u - b\cdot v, a\cdot v + b\cdot u) = (u\cdot a - v\cdot b, v\cdot a + u\cdot b) = (u,v)\odot(a,b)\,,$$

$$(a,b)\odot(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b) \quad ,$$

also ist $(1,0)$ das Einselement, und es gilt das Distributivgesetz:

$$(a,b)\odot((u,v)\oplus(s,t)) = (a,b)\odot(u+s, v+t)$$
$$= (a\cdot(u+s) - b\cdot(v+t), a\cdot(v+t) + b\cdot(u+s))$$
$$= (a\cdot u + a\cdot s - b\cdot v - b\cdot t, a\cdot v + a\cdot t + b\cdot u + b\cdot s)$$
$$= (a\cdot u - b\cdot v, a\cdot v + b\cdot u)\oplus(a\cdot s - b\cdot t, a\cdot t + b\cdot s)$$
$$= ((a,b)\odot(u,v))\oplus((a,b)\odot(s,t)) \quad .$$

(3) Nun zum Axiom (KK) : Sei $(a,b)\in\mathbb{C}$, $(a,b)\neq(0,0)$. Dann gilt nach Folgerung 3.5.2 :

$$0\leq a^2 \quad \text{und} \quad 0\leq b^2 \quad ,$$

und wegen $(a,b)\neq(0,0)$ gilt nicht $a^2 = b^2 = 0$, eine der beiden Zahlen ist also nicht Null, und für die Summe gilt daher

$$0 < a^2 + b^2 \quad \text{nach (AK2)} \quad .$$

Daher haben wir $t := (a^2+b^2)^{-1}\in\mathbb{R}$. Es folgt

$$(a,b)\odot(a\cdot t, -b\cdot t) = (a\cdot(a\cdot t) - b\cdot(-b\cdot t), a\cdot(-b\cdot t) + b\cdot(a\cdot t))$$
$$= (a^2\cdot t + b^2\cdot t, -a\cdot(b\cdot t) + a\cdot(b\cdot t)) = ((a^2+b^2)\cdot t, 0) = (1,0)\,.$$

Wir haben also ein Inverses zu $(a,b)\neq(0,0)$,

$$(a,b)^{-1} = (a\cdot((a^2+b^2)^{-1}), -b\cdot((a^2+b^2)^{-1})) \quad .$$

Insgesamt: $(\mathbb{C},\oplus,\odot)$ ist ein Körper.

□

So ähnlich, wie wir in 3.3.9 gesehen haben, dass man R als Unterring von $R[X]$, und in 3.4.2, dass man R als Unterring von $Q(R)$ auffassen kann, sehen wir, dass man $\mathbb{R}$ als Unterring (in diesem Fall muss man besser sagen: als

Unterkörper) von $\mathbb{C}$ auffassen kann:
Folgerung 3.5.5 : Die Abbildung

$$\iota \ : \ \mathbb{R} \ \longrightarrow \ \mathbb{C} \quad , \quad a \mapsto (a,0)$$

ist ein injektiver Ringhomomorphismus von $(\mathbb{R},+,\cdot)$in $(\mathbb{C},\oplus,\odot)$.
Wir schreiben daher

$$a \quad \text{statt} \quad (a,0) \quad ,$$

dann wird $\mathbb{R} \subset \mathbb{C}$. Wenn wir nun auch noch

$$+ \quad \text{statt} \quad \oplus \quad , \quad \cdot \quad \text{statt} \quad \odot$$

für die Verknüpfungen in $\mathbb{C}$ schreiben, wird $(\mathbb{R},+,\cdot)$ ein Unterring von $(\mathbb{C},+,\cdot)$. Da beide Körper sind, sagen wir: $(\mathbb{R},+,\cdot)$ ist ein **Unterkörper** von $(\mathbb{C},+,\cdot)$. Wenn wir diese Schreibweisen verwenden, also a statt $(a,0)$ schreiben, gilt für beliebiges $(a,b) \in \mathbb{C}$:

$$(a,b) \ = \ (a,0) + (0,b) \ = \ (a,0) + (0,1) \cdot (b,0) \ = \ a + (0,1) \cdot b \quad .$$

Das Element $(0,1)$ gehört zu $\mathbb{C}$, aber nicht zu $\mathbb{R}$. Wir nennen

$$i \quad := \quad (0,1)$$

die **imaginäre Einheit** . Dann gilt für jedes $(a,b) \in \mathbb{C}$:

$$(a,b) \ = \ a + i \cdot b \quad , \quad \text{und damit}$$

$$(*) \qquad \mathbb{C} \ = \ \{ \ a + i \cdot b \ \mid \ a,b \in \mathbb{R} \ \} \quad .$$

Es gilt

$$i^2 \ = \ (0,1) \cdot (0,1) \ = \ (-1,0) \ = \ -1 \quad ,$$

aber i ist nicht die einzige Zahl mit Quadrat -1, denn es gilt auch

$$(-i)^2 \ = \ (-i) \cdot (-i) \ = \ i \cdot i \ = \ -1 \quad .$$

Die Schreibweise $i \ = \ \sqrt{-1}$ sollte man deshalb besser nicht verwenden ! Mit der Schreibweise $(*)$ für $\mathbb{C}$ - und mit $i^2 \ = \ -1$ - kann man auch die Definition von Addition und Multiplikation in $\mathbb{C}$ übersichtlicher schreiben als

$$(a+ib) + (u+iv) \ = \ (a+u) + i(b+v) \quad ,$$

$$(a+ib) \cdot (u+iv) \ = \ (a \cdot u - b \cdot v) + i(a \cdot v + b \cdot u) \quad .$$

Definition 3.5.6: Sei $z \in \mathbb{C}$, $z = x + iy = (x, y)$ mit $x, y \in \mathbb{R}$. Aus der Definition des cartesischen Produkts folgt

$$(x, y) = (x'y') \iff (x = x' \wedge y = y') \quad \text{für} \quad x, x', y, y' \in \mathbb{R} \quad .$$

Hat man also $z = x + i \cdot y$ mit $x, y \in \mathbb{R}$, so sind x und y eindeutig bestimmt. Man nennt

x den **Realteil** von z, und schreibt $\operatorname{Re} z := x$, und

y den **Imaginärteil** von z, und schreibt $\operatorname{Im} z := y$.

Und man nennt noch

$\overline{z} := x - i \cdot y$ das **Konjugiert-Komplexe** von z.

Folgerung 3.5.7 : Die Abbildung

$$\overline{} : \mathbb{C} \longrightarrow \mathbb{C}, z \mapsto \overline{z}$$

ist ein Automorphismus des Körpers $(\mathbb{C}, +, \cdot)$, d.h. $\overline{}$ ist bijektiv, und es gilt

$$(*) \qquad \forall z, w \in \mathbb{C} : (\overline{z + w} = \overline{z} + \overline{w} \wedge \overline{z \cdot w} = \overline{z} \cdot \overline{w}) \quad .$$

Und es gilt

$$(**) \qquad \forall z \in \mathbb{C} : \overline{\overline{z}} = z \quad .$$

Beweis : Die Regeln $(*)$ und $(**)$ kann man leicht nachrechnen. Aus $(**)$ folgt, dass die Abbildung $\overline{}$ sich selbst als Umkehrfunktion hat und daher bijektiv ist.

□

Bemerkung 3.5.8 : In der Analysis lernt man: Zu jedem $a \in \mathbb{R}$ mit $a \geq 0$ gibt es genau ein $y \in \mathbb{R}$ mit $y^2 = a$ und $y \geq 0$. Wir setzen $\sqrt{a} := y$ und haben damit die **Wurzelfunktion**

$$\sqrt{} : \{ a \in \mathbb{R} \mid a \geq 0 \} \longrightarrow \{ a \in \mathbb{R} \mid a \geq 0 \} \quad , \quad a \mapsto \sqrt{a} \quad .$$

Es gilt $\forall a, b \in \mathbb{R} : \sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b}$. Damit ist $\sqrt{}$ ein Endomorphismus der Gruppe $(\mathbb{R}_+^*, \cdot)$ (aber keineswegs ein Homomorphismus bezüglich $+$) .
Die Wurzelfunktion ist **streng monoton wachsend**: Es gilt

$$(\mathrm{M}) \qquad \forall a, b \in \mathbb{R} : (0 \leq a < b \implies \sqrt{a} < \sqrt{b}) \quad .$$

Beweis : von (M) : Es gelte $0 \leq a < b$. Dann ist

$$\sqrt{a} + \sqrt{b} > 0 \quad ,$$

denn aus $\sqrt{a}+\sqrt{b}=0$ würde $a=b=0$ folgen. Aus $\sqrt{b}-\sqrt{a}\leq 0$ und der Gleichung

$$(\sqrt{b}+\sqrt{a})\cdot(\sqrt{b}-\sqrt{a}) \quad = \quad b-a$$

würde $b-a\leq 0$ folgen, Widerspruch zu $a<b$. Also : $\sqrt{b}-\sqrt{a}>0$.

□

Definition 3.5.9 : Sei $z\in\mathbb{C}$, $z=x+i\cdot y$ mit $x,y\in\mathbb{R}$. Nach Folgerung 3.5.2(1) und nach (AK2) gilt dann $x^2+y^2\geq 0$. Wir können daher definieren:

$$|\,z\,| \quad := \quad \sqrt{x^2+y^2}$$

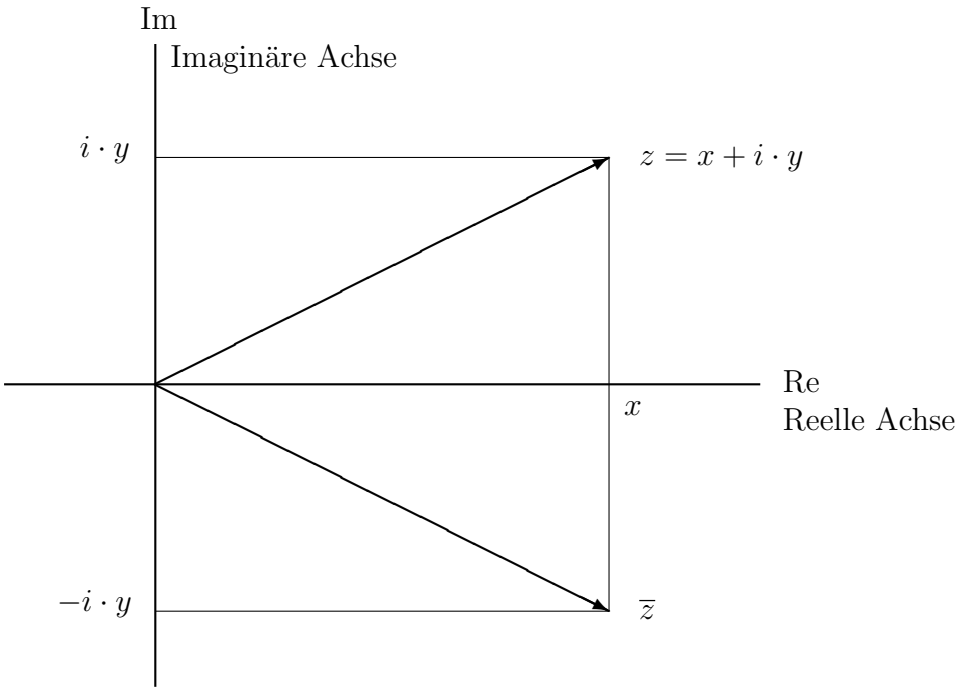
und nennen diese Zahl den **Betrag** von z . Auch für eine reelle Zahl x ist damit $|x|$ definiert, als $|x|=\sqrt{x^2}$.

Nachrechnen kann man die

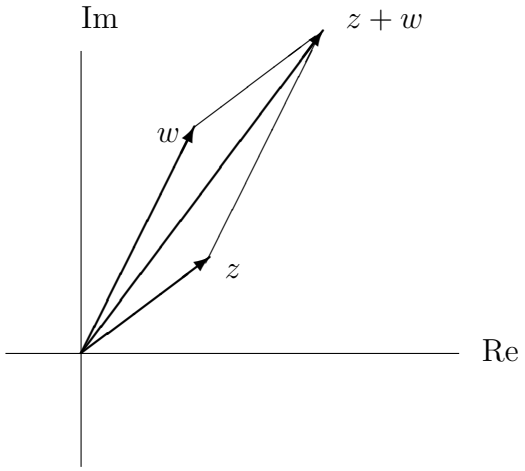
(3.5.10) Rechenregeln für den Betrag : Für alle $z,w\in\mathbb{C}$ gilt
(a) $|z|=\sqrt{z\cdot\overline{z}}$,
(b) $|\overline{z}|=|z|$,
(c) $|\mathrm{Re}\,z|\leq|z|$ und $|\mathrm{Im}\ z|\leq|z|$
und es gelten die folgenden, auch für den Betrag reeller Zahlen wichtigen, Regeln
(d) $|z|\geq 0$ und $(|z|=0 \iff z=0)$,
(e) $|z+w|\leq|z|+|w|$,
(f) $|z\cdot w|=|z|\cdot|w|$
und daher auch die aus (e) und (f) folgende Regel
(g) $|\,|z|-|w|\,|\leq|z-w|$.

□

(3.5.11) Die komplexe Zahlenebene: Man kann sich die komplexen Zahlen, das Konjugiert-Komplexe und die Summe komplexer Zahlen geometrisch veranschaulichen. Wir hatten $\mathbb{C}$ eingeführt als cartesisches Produkt $\mathbb{C}=\mathbb{R}\times\mathbb{R}$, daher kann man sich $\mathbb{C}$ vorstellen als die
Gaußsche Zahlenebene , in der die komplexen Zahlen in der Form
$z=x+i\cdot y$ mit $x,y\in\mathbb{R}$ eingetragen sind:



$|z|$ ist dann die Länge des "Vektors" $z = x + iy$, $\overline{z}$ der Vektor, den man durch Spiegelung von z an der reellen Achse bekommt, und die Summe ist die aus 1.2 bekannte Summe von Vektoren aus $\mathbb{R}^2$:



Zur Veranschaulichung des Produkts braucht man Winkel, das gehört in die

Analysis.

Für den nächsten Satz brauchen wir noch das **Produktzeichen**, das man ähnlich wie das Summenzeichen in 1.2.11 definiert:

Definition 3.5.12 : Sei $(R, +, \cdot)$ ein Ring. Seien $m, n \in \mathbb{Z}$. Dann definieren wir rekursiv

(i) für $n < m$:

$$\prod_{j=m}^{n} a_j \quad := \quad 1 \qquad (\text{“leeres Produkt”}),$$

(ii) für $m \leq n$ und $a_m, \ldots, a_n \in R$:

$$\prod_{j=m}^{n} a_j \quad := \quad \prod_{j=m}^{n-1} a_j \cdot a_n \quad .$$

(3.5.13) Fundamentalsatz der Algebra : Sei $f(X) \in \mathbb{C}[X]$ ein Polynom, $f(X) \neq 0$, so dass $n := \deg f(X)$ definiert ist, $n \in \mathbb{N}_0$. Dann gibt es (nicht notwendig verschiedene) Zahlen $a_1, \ldots, a_n \in \mathbb{C}$ und ein $c \in \mathbb{C} \setminus \{0\}$ mit

$$f(X) \quad = \quad c \cdot \prod_{j=1}^{n} (X - a_j) \quad .$$

Man sagt dazu: $f(X)$ zerfällt in ein Produkt von Linearfaktoren.

□

Was der Name des Satzes nicht vermuten lässt: Der Satz lässt sich nur mit Mitteln der Analysis beweisen, der Beweis gehört also nicht hierher. Der Beweis geht am Einfachsten mit Sätzen aus der Theorie der differenzierbaren Funktionen einer komplexen Variablen (“Funktionentheorie”). Wir werden ihn aber später bei der Theorie der Eigenwerte brauchen.

□

3.6 Aufgaben

(3.1) Sei K ein Körper. Zeigen Sie:

a) Sei I ein Ideal im Polynomring $K[X]$, dann gibt es ein Polynom $m(X)$ mit

$$I \; = \; (m(X)) \; := \; \{ \;\; f(X) \cdot m(X) \;\; | \;\; f(X) \in K(X) \;\; \} \quad .$$

b) In $K[X,Y]$ ist

$$I := \left\{ \sum_{(j,k)\in\mathbb{N}_0\times\mathbb{N}_0 \text{ mit } (j,k)\neq(0,0)} a_{jk}\cdot X^j\cdot Y^k \;\middle|\; a_{jk}\in K \right\}$$

ein Ideal, aber es gibt kein Polynom $m(X,Y)\in K[X,Y]$ mit

$$I = \{\; f(X,Y)\cdot m(X,Y) \mid f(X,Y)\in K[X,Y] \;\} \quad .$$

(3.2) Sei $(A,+)$ eine abelsche Gruppe, 0 ihr neutrales Element. Sei

$$\mathrm{End}(A) := \{\; \varphi : A \longrightarrow A \mid \varphi \text{ ist ein Gruppen-Endomorphismus von } A \;\} \; .$$

Für $\varphi,\psi\in\mathrm{End}(A)$ definiere $\varphi+\psi$ durch

$$(\varphi+\psi)(x) := \varphi(x)+\psi(x) \quad \text{für} \quad x\in A \quad .$$

Sei $\circ$ die Hintereinanderausführung von Abbildungen. Zeigen Sie, dass $(\,\mathrm{End}(A),+,\circ)$ ein Ring ist.

(3.3) Sei M eine nichtleere Menge und $(R,+,\cdot)$ ein Ring.
Für $f,g : M \longrightarrow R$ und $x\in M$ setze

$$(f+g)(x) := f(x)+g(x) \quad ,$$

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

Zeigen Sie, dass $(\mathcal{F}(M,R),+,\cdot)$ ein Ring ist, der für $\#(M)\geq 2$ nicht nullteilerfrei ist.

(3.4) Sei R ein kommutativer Ring, 1 das Einselement, $1\,,\,1\neq 0\,$. Für

$$u(X) = \sum_{j=0}^{\infty} a_j\,X^j \in K[X] \quad \text{sei} \quad D(u(X)) := \sum_{j=0}^{\infty}(j+1)\,a_{j+1}\,X^j \quad .$$

Zeigen Sie (ohne Benutzung von Regeln aus der Analysis), dass für $u(X),v(X)\in R[X]$ und $a\in R$ gilt

a) $D(a\cdot u(X)) = a\cdot D(u(X)) \quad ,$

b) $D(u(X)+v(X)) = D(u(X))+D(v(X)) \quad ,$

c) $D(u(X)\cdot v(X)) = D(u(X))\cdot v(X) + u(X)\cdot D(v(X)) \quad .$

Ist die Abbildung $D : R[X] \longrightarrow R[X] \quad , \quad u(X)\longmapsto D(u(X))$ ein Homomorphismus von Ringen ?

(3.5) Sei $(R,+,\cdot)$ ein kommutativer Ring und $\alpha \in R$. Sei

$$R_\alpha := R \times R \quad , \quad \text{und für} \quad (a,b),(c,d) \in R_\alpha \quad \text{sei}$$

$$(a,b) \oplus (c,d) := (a+b, c+d) \quad ,$$
$$(a,b) \circ (c,d) := (a \cdot c + \alpha \cdot b \cdot d, a \cdot d + b \cdot c) \quad . \quad \text{Zeigen Sie:}$$

a) $(R_\alpha, \oplus, \circ)$ ist ein kommutativer Ring mit Eins,
$\varphi : R \longrightarrow R_\alpha \quad , \quad \varphi(a) := (a,0)$
ist ein injektiver Ringhomomorphismus, und es gibt ein
$(x,y) \in R_\alpha \quad \text{mit} \quad (x,y)^2 = (\alpha, 0) \quad .$

b) Ist R ein Körper, und gibt es kein $x \in R$ mit $x^2 = \alpha$, so ist $(R_\alpha, \oplus, \circ)$ ein Körper.

(Hinweis: Mit $R := \mathbb{R}$ und $\alpha := -1$ ist $\mathbb{C} := \mathbb{R}_{-1}$ der Körper der komplexen Zahlen, wir haben hier also nur eine Verallgemeinerung von Satz 3.5.4 .)

(3.6) Zeigen Sie, etwa mit Aufgabe (3.5), dass es Körper mit 9 und mit 25 Elementen gibt.

(3.7) Sei $K := \mathbb{Z}/_{(3)}$. Geben Sie alle normierten Primpolynome vom Grad 3 aus $K[X]$ an. Hinweis: Für alle $\alpha \in K$ gilt $\alpha^3 = \alpha$.

Zu den folgenden Aufgaben: Sei $n \in \mathbb{Z} \setminus \{0,1\}$, und n sei **quadratfrei**, d.h. es gebe keine Quadratzahl in $\mathbb{N} \setminus \{1\}$, die Teiler von n ist. Für $n < 0$ setze $\sqrt{n} := i\sqrt{-n}$. Zeigen Sie:

(3.8) a)
$$\mathbb{Z}[\sqrt{n}] \quad := \quad \{ \ a + b\sqrt{n} \ \mid \ a,b \in \mathbb{Z} \ \} \quad ,$$
und für $n-1 \in (4)$(d.h. wenn 4 Teiler von $n-1$ ist) auch
$$\mathcal{O}_n \quad := \quad \left\{ \ a + b\frac{1+\sqrt{n}}{2} \ \middle| \ a,b \in \mathbb{Z} \ \right\}$$
sind Unterringe von $\mathbb{C}$.

b) Für $z = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ setze $\overline{z} := a - b\sqrt{n}$, und für
$z = a + b\frac{1+\sqrt{n}}{2} \in \mathcal{O}_n$ setze $\overline{z} := a + b\frac{1-\sqrt{n}}{2}$.
Dann gilt für alle $z,w \in \mathbb{Z}[\sqrt{n}]$ bzw. $\mathcal{O}_n$
$$N(z) := z \cdot \overline{z} \in \mathbb{Z} \quad , \quad N(z \cdot w) = N(z) \cdot N(w)$$

und damit: Zu z existiert genau dann ein $z^* \in \mathbb{Z}[\sqrt{n}]$ bzw. $\mathcal{O}_n$ mit $z \cdot z^* = 1$, wenn $N(z) \in \{\pm 1\}$ ist.

(3.9) Sei $(R, +, \cdot)$ ein Ring, 1 das Einselement von R. Nach Satz 3.2.11 ist die Menge $R^\times$ der invertierbaren Elemente von R, also

$$R^\times := \{\ a \in R \mid \exists\, a^* \in R :\ a \cdot a^* = a^* \cdot a = 1\ \}$$

mit $\cdot$ eine Gruppe, die Einheitengruppe von R.

a) Bestimmen Sie mit Aufgabe (3.4) b) die Einheitengruppen der in Aufgabe (3.4) a) definierten Ringe

$$\mathbb{Z}[\sqrt{-1}] \quad , \quad \mathbb{Z}[\sqrt{-2}] \quad , \quad \mathcal{O}_{-3} \quad .$$

b) Zeigen Sie, dass $\mathbb{Z}[\sqrt{3}]^\times$ unendlich viele Elemente hat. Tipp: Wenn Sie ein Element $z_1 \in \mathbb{Z}[\sqrt{3}]^\times$, $z_1 \neq \pm 1$, gefunden haben, dann sind alle z_1^n, $n \in \mathbb{N}_0$, verschieden und liegen auch in $\mathbb{Z}[\sqrt{3}]^\times$.

(3.10) Alle $\mathbb{Q}(\sqrt{n}) := \{\ a + b\sqrt{n} \mid a, b \in \mathbb{Q}\ \}$ sind Unterkörper von $\mathbb{C}$, im Falle von $n > 0$ auch von $\mathbb{R}$.

§4 Vektorräume

4.1 Definition und Beispiele

(4.1.1) Zur Motivation : Wenn man von "Vektoren" spricht , denkt man von der Schule her meistens an "Vektoren im dreidimensionalen Raum" , wie wir das in 1.6 gemacht haben. Wir wollen hier aber von der Vorstellung loskommen, dass Vektoren "Pfeile" sind. Gleich die ersten Beispiele werden zeigen, dass es auch etwas allgemeiner sein muss.

Definition 4.1.2 : V sei eine nichtleere Menge und K ein Körper, 1 das Einselement von K. Es gebe eine Verknüpfung

$$+ : V \times V \longrightarrow V \quad , \quad (a,b) \longmapsto a+b$$

und eine **äußere Operation**

$$\omega : K \times V \longrightarrow V \quad , \quad (\alpha, a) \longmapsto \alpha a \quad ,$$

so dass gilt :
(V1) $(V,+)$ ist eine abelsche Gruppe.
(V2) Für alle $\alpha, \beta \in K$ und alle $a, b \in V$ gilt
(a) $\alpha(a+b) = \alpha a + \alpha b$,
(b) $(\alpha+\beta)a = \alpha a + \beta a$,
(c) $(\alpha \cdot \beta)a = \alpha(\beta a)$,
(d) $1\,a = a$.
Dann heißt V (genauer: Das Tripel $(V,+,\omega)$) ein
K-(Links-)Vektorraum . Die Elemente von V heißen **Vektoren**,
die Elemente von K **Skalare** . □

Beispiel 4.1.3 : Sei L ein Körper und K ein Unterkörper von L, d.h. ein Unterring, der auch noch Körper ist. Dann ist $(L,+)$ eine abelsche Gruppe, es gilt also (V1) für $(L,+)$. Als äußere Operation von K auf L nehmen wir die Multiplikation in L , eingeschränkt auf $K \times L$; wir setzen also

$$\omega : K \times L \longrightarrow L \quad , \quad \omega(\alpha, a) := \alpha \underbrace{\cdot}_{\uparrow} a \quad ,$$

Multiplikation in L

also $\alpha a := \alpha \cdot a$. Auf diese Weise wird L ein $K-$Vektorraum, denn die Rechenregeln
(V2) (a) und (b) folgen dann aus dem Distributivgesetz in L ,
(c) aus dem Assoziativgesetz für $(L,\cdot)$, und

(d) daraus, dass 1 das Einselement von L ist .

Wir erhalten damit gleich weitere Beispiele:

a.) Sei $(K,+,\cdot)$ ein Körper, dann ist K ein Unterkörper von sich selbst. K selbst ist also ein $K-$Vektorraum.

b.) $\mathbb{Q},\mathbb{R},\mathbb{C}$ sind Körper mit $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$, $\mathbb{Q}$ ist Unterkörper von $\mathbb{R}$ und $\mathbb{R}$ ist Unterkörper von $\mathbb{C}$. Also sind

$\mathbb{Q},\mathbb{R},\mathbb{C}$ jeweils $\mathbb{Q}-$Vektorräume ,

$\mathbb{R}$ und $\mathbb{C}$ auch $\mathbb{R}-$Vektorräume , und

$\mathbb{C}$ ist ein $\mathbb{C}-$Vektorraum.

Beispiel 4.1.4 : Sei $(K,+,\cdot)$ ein Körper, A eine nichtleere Menge und V ein $K-$Vektorraum, den wir schon kennen (z.B. $V=K$). Dann wird $\mathcal{F}(A,V)$, die Menge der Funktionen von A nach V , wieder ein $K-$Vektorraum, wenn wir für $f,g\in\mathcal{F}(A,V)$ definieren:

$$(*)\qquad (f+g)(x) \;:=\; f(x)+g(x) \quad \text{für alle} \quad x\in A$$

$$\uparrow$$

Addition in V ,

dann ist also $f+g\in\mathcal{F}(A,V)$ für alle $f,g\in\mathcal{F}(A,V)$, und wir definieren die äußere Operation von K auf $\mathcal{F}(A,V)$ durch

$$(**)\qquad (\lambda f)(x) \;:=\; \lambda\, f(x) \quad \text{für alle} \quad \lambda\in K \quad \text{und} \quad f\in\mathcal{F}(A,V) \quad ,$$

$$\uparrow$$

äußere Operation von K auf V ,

dann ist also $\lambda f\in\mathcal{F}(A,V)$. Wir prüfen nach, ob die Axiome (V1) , (V2) gelten:

(V1) $+$ ist eine Verknüpfung auf $\mathcal{F}(A,V)$. Es gilt

(G1) $\forall\, f,g,h\in\mathcal{F}(A,V):\;\; (f+g)+h \;=\; f+(g+h)$,

denn $(V,+)$ ist eine Gruppe, und damit gilt nach $(*)$:

$$\begin{aligned}\forall\, x\in A:\;\; ((f+g)+h)(x) \;&=\; (f+g)(x)+h(x)\\ =\; (f(x)+g(x))+h(x) \;&=\; f(x)+(g(x)+h(x))\\ =\; f(x)+(g+h)(x) \;&=\; (f+(g+h))(x) \quad .\end{aligned}$$

(G4) $\forall\, f,g\in\mathcal{F}(A,V):\;\; f+g \;=\; g+f$,

denn $(V,+)$ ist eine abelsche Gruppe, also gilt

$$\forall\, x\in A:\; (f+g)(x) \;=\; f(x)+g(x) \;=\; g(x)+f(x) \;=\; (g+f)(x) \quad .$$

(G2) Sei $0: A \longrightarrow V$, $0(x):=0$, wobei die hintere 0 das Nullelement der abelschen Gruppe $(V,+)$ ist, dann gilt für alle $f\in\mathcal{F}(A,V)$:

$$0+f \;=\; f \quad \text{wegen} \quad (0+f)(x) \;=\; 0(x)+f(x) \;=\; 0+f(x) \;=\; f(x) \quad .$$

(G3) Zu $f \in \mathcal{F}(A,V)$ haben wir $-f$, definiert durch $(-f)(x) := -f(x)$ für $x \in A$. Dafür gilt

$$(-f)+f \;=\; 0 \quad \text{wegen} \quad ((-f)+f)(x) \;=\; (-f)(x)+f(x)$$

$$= -f(x)+f(x) \;=\; 0 \;=\; 0(x) \quad \text{für} \quad x \in A\ .$$

Also ist $(\mathcal{F}(A,V),+)$ eine abelsche Gruppe.
(V2) Für beliebige $\alpha,\beta \in K, f,g \in \mathcal{F}(A,V), x \in A$ gilt nun nach $(**)$:

$$((\alpha+\beta)f)(x) \quad = \quad (\alpha+\beta)f(x)$$

$$= \quad \alpha f(x)+\beta f(x) \quad \text{wegen (V2)(b) für}\, V$$

$$= \quad (\alpha f)(x)+(\beta f)(x) \quad = \quad (\alpha f+\beta f)(x), \quad \text{also}$$

$$(\alpha+\beta)f \quad = \quad \alpha f+\beta f \quad ,$$

also gilt (V2)(b) für $\mathcal{F}(A,V)$,

$$(\alpha(f+g))(x) \quad = \quad \alpha(f+g)(x) \quad = \quad \alpha(f(x)+g(x))$$

$$= \quad \alpha f(x)+\alpha g(x) \quad \text{wegen (V2)(a) für}\, V$$

$$= \quad (\alpha f)(x)+(\alpha g)(x) \quad = \quad (\alpha f+\alpha g)(x) \quad , \qquad \text{also}$$

$$\alpha(f+g) \quad = \quad \alpha f+\alpha g \quad ,$$

also gilt (V2)(a) für $\mathcal{F}(A,V)$,

$$(\alpha(\beta f))(x) \quad = \quad \alpha(\beta f)(x) \quad = \quad \alpha(\beta(f(x)))$$

$$= \quad (\alpha\cdot\beta)f(x) \quad \text{wegen (V2)(c) für } V \quad ,$$

$$= \quad ((\alpha\cdot\beta)f)(x) \quad , \qquad \text{also}$$

$$\alpha(\beta f) \quad = \quad (\alpha\cdot\beta)f \quad ,$$

also gilt (V2)(c) für $\mathcal{F}(A,V)$, und

$$(1f)(x) \quad = \quad 1f(x) \quad = \quad f(x) \quad \text{wegen (V2)(d) für}\, V \quad , \qquad \text{also}$$

$$1f \quad = \quad f \quad ,$$

also gilt (V2)(d) für $\mathcal{F}(A,V)$. Insgesamt haben wir gezeigt: $\mathcal{F}(A,V)$ ist ein $K-$Vektorraum. □

Beispiel 4.1.5 : Sei K ein Körper. Nach Beispiel 4.1.3 a.) ist K selbst ein $K-$Vektorraum, wenn man die Multiplikation von K als "äußere" Operation

von K auf K nimmt. Nach Beispiel 4.1.4 ist dann für eine beliebige nichtleere Menge A auch $\mathcal{F}(A,K)$ ein $K-$Vektorraum, wenn man für

$$f,g \in \mathcal{F}(A,K) \quad \text{und} \quad \alpha \in K$$

$$f+g \quad \text{und} \quad \alpha f \quad \text{definiert durch}$$

$(*)\,(f+g)(x) \quad := \quad f(x)+g(x) \quad$ und $\quad (**) \quad (\alpha f)(x) \quad := \quad \alpha \cdot f(x)$
für $x \in A$. Einen wichtigen Spezialfall betrachten wir gleich.

Definition 4.1.6 : Seien J und M Mengen. Für

$$a \,:\, J \;\longrightarrow\; M \quad , \quad j \longmapsto a(j)$$

schreiben wir auch

$$(a_j)_{j\in J} \quad \text{statt} \quad a \quad \text{und} \quad a_j \quad \text{statt} \quad a(j) \quad ,$$

und sprechen von der **Familie** $(a_j)_{j\in J}$ in M mit der **Indexmenge** J statt von der Funktion a . - Familien sind also einfach Funktionen, etwas anders geschrieben. Familien mit Indexmenge $\mathbb{N}$ bzw. $\mathbb{N}_0$ hatten wir in §3 , das waren Folgen.
Die Familie $(a_j)_{j\in J}$ heißt **endlich** , wenn J eine endliche Menge ist. Ist $I \subset J$, so heißt

$$a|_I \quad = \quad (a_j)_{j\in I}$$

eine **Teilfamilie** von $(a_j)_{j\in J}$. □

Beispiel 4.1.7: Der $K-$Vektorraum K^n

Sei K ein Körper und $n \in \mathbb{N}$. Wir hatten definiert:

$$\underline{n} \quad = \quad \{1,\ldots,n\} \quad .$$

Nach Beispiel 4.1.5 ist dann

$$\mathcal{F}(\underline{n},K) \quad = \quad \{ \;\; (a_j)_{j\in\underline{n}} \;\; | \;\; \forall\, j \in \underline{n} \,:\, a_j \in K \;\; \}$$

ein Vektorraum, mit den durch $(*)$ und $(**)$ definierten Rechenoperationen, die sich in der Schreibweise mit Familien schreiben lassen als

$(*) \quad (a_j)_{j\in\underline{n}} + (b_j)_{j\in\underline{n}} \quad := \quad (a_j+b_j)_{j\in\underline{n}} \quad ,$

$(**) \quad \lambda\,(a_j)_{j\in\underline{n}} \quad := \quad (\lambda\cdot a_j)_{j\in\underline{n}} \quad$ für $\quad (a_j)_{j\in\underline{n}}\,,\,(b_j)_{j\in\underline{n}} \in \mathcal{F}(\underline{n},K)\,,\,\lambda \in K \quad .$

Schreibt man nun

$$(a_1,\ldots,a_n) \quad := \quad (a_j)_{j\in\underline{n}} \quad ,$$

so sieht man , dass $\mathcal{F}(\underline{n}, K)$ die Menge der $\underline{n-\textbf{tupel}}$ von Elementen aus K ist. Man schreibt $K^n := \mathcal{F}(\underline{n}, K)$, und K^n wird also ein $K-$Vektorraum, wenn man

$$(*) \quad (a_1, \ldots, a_n) + (b_1, \ldots, b_n) \quad := \quad (a_1 + b_1, \ldots, a_n + b_n) \quad ,$$

$$(**) \quad \lambda(a_1, \ldots, a_n) \quad := \quad (\lambda a_1, \ldots, \lambda a_n)$$

definiert. Insbesondere erhalten wir damit für $K := \mathbb{R}$ die $\mathbb{R}-$Vektorräume $\mathbb{R}^2$ und $\mathbb{R}^3$ als Beispiele. □

Einige Rechenregeln für Vektorräume folgen direkt aus den Axiomen:

Satz 4.1.8 : Sei K ein Körper, 1 das Einselement von K, und V ein $K-$Vektorraum. Dann gilt für alle $a \in V$ und alle $\alpha \in K$:

(1) $0\,a = 0$, (2) $\alpha\,0 = 0$,

0 in K 0 in V 0 in V

(3) $(-\alpha)a = -(\alpha\,a) = \alpha(-a)$,
man kann daher für alle drei Elemente $-\alpha a$ schreiben,

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

Beweis : (1) $0\,a = (0+0)a \overset{(V2)(b)}{=} 0a + 0a$, also
$0a + (-(0a)) = 0a + 0a + (-0a)$, also
$0 = 0a$.

(2) $\alpha 0 \overset{(V1)}{=} \alpha\,(0+0) \overset{(V2)(a)}{=} \alpha 0 + \alpha 0$,
und Addition von $-(\alpha\,0)$ ergibt $0 = \alpha\,0$.

(3) $0 \overset{(1)}{=} 0\,a = (\alpha + (-\alpha))a \overset{(V2)(b)}{=} \alpha\,a + (-\alpha)a$, also
$(-\alpha)a = -(\alpha a)$, und
$0 \overset{(2)}{=} \alpha\,0 \overset{(V1)}{=} \alpha(a + (-a)) \overset{(V2)(a)}{=} \alpha a + \alpha(-a)$, also
$\alpha(-a) = -(\alpha a)$.

(4) $(-1)a \overset{(3)}{=} -(1\,a) \overset{(V2)(d)}{=} -a$. □

Satz 4.1.9 : Sei V ein $K-$Vektorraum. Dann gilt

$$\forall\,\alpha \in K\,\forall\,a \in V : \; (\,\alpha a = 0 \quad \Longleftrightarrow \quad \alpha = 0 \;\vee\; a = 0) \quad .$$

Beweis : " $\Longleftarrow$ " gilt nach Satz 4.1.8 (1) und (2) .
" $\Longrightarrow$ " : Sei $\alpha a = 0$. Es kann $\alpha = 0$ sein, dann sind wir fertig, oder $\alpha \neq 0$, also $\alpha \in K^*$. Dann existiert $\alpha^{-1} \in K^*$, und es folgt

$$0 = \alpha^{-1}\,0 = \alpha^{-1}(\alpha\,a) \overset{(V2)(c)}{=} (\alpha^{-1}\,\alpha)a = 1a \overset{(V2)(d)}{=} a \quad .$$

In jedem Fall gilt $\alpha = 0 \vee a = 0$. $\square$

Definition 4.1.10 : Sei K ein Körper und V ein $K-$Vektorraum. W heißt ein **Untervektorraum** (**Unterraum**, **Teilraum**) von V , falls gilt
(UV1) $W \subset V \quad \wedge \quad W \neq \emptyset$
(UV2) $\forall\, v, w \in W \,:\; v + w \in W$
(UV3) $\forall\, v \in W \,\forall\, \lambda \in K \,:\; \lambda\, v \in W$. $\square$

Die Definition des Untervektorraums ist sinnvoll wegen

Satz 4.1.11 : Ist V ein $K-$Vektorraum und W ein Untervektorraum von V , so ist W mit der auf $W \times W$ eingeschränkten Verknpfung $+$ und der auf $K \times W$ eingeschränkten äußeren Operation selbst ein $K-$Vektorraum.
Beweis : Die Axiome (UV2) und (UV3) sagen, dass die Restriktionen

$$+|_{W \times W} \,:\; W \times W \;\longrightarrow\; V \quad , \quad (v, w) \longmapsto v + w \quad , \quad \text{und}$$

$$\omega|_{K \times W} \,:\; K \times W \;\longrightarrow\; V \quad , \quad (\lambda, v) \longmapsto \lambda v$$

tatsächlich Abbildungen nach W sind. Man hat also eine Addition und eine äußere Operation auf W . Die Rechenregeln

$$\begin{aligned} u + (v + w) &= (u + v) + w \\ u + v &= v + u \\ \lambda(u + v) &= \lambda u + \lambda v \\ (\lambda + \mu)u &= \lambda u + \mu u \\ (\lambda \cdot \mu)u &= \lambda(\mu\, u) \\ 1\, u &= u \end{aligned}$$

für alle $u, v, w \in W$ und alle $\lambda, \mu \in K$ gelten, da sie sogar für alle $u, v, w \in V$ gelten. Damit hat man (V2), und einen Teil von (V1). Sei $v \in W$, dann ist nach (UV3) auch

$$-v \quad = \quad (-1)\, v \;\in\; W \quad .$$

Damit hat man zu $v, u \in W$ ein $x \in W$ mit $v + x = u$, nämlich $x := (-v) + u \in W$ nach (UV2) . Auch ist $W \neq \emptyset$. Also gilt auch (V1) für W . $\square$

Beispiele 4.1.12 : a.) Sei V ein beliebiger Vektorraum, dann sind $\{0\}$ und V Untervektorräume von V .
b.) Sei $v \in \mathbb{R}^2$, $v \neq 0$ und

$$\mathbb{R}\, v \quad := \quad \{\; \lambda\, v \;\mid\; \lambda \in \mathbb{R} \;\} \quad ,$$

dann ist $\mathbb{R}\, v$ ein Untervektorraum des $\mathbb{R}-$Vektorraums $\mathbb{R}^2$. Man kann sich $\mathbb{R}\, v$ vorstellen als Gerade durch den Nullpunkt, wobei v die "Richtung"

angibt.
(4.1.13) Sei K ein Körper. Dann haben wir nach 3.3.10 den Polynomring $(K[X], +, \cdot)$ mit

$$K[X] \;=\; \left\{ \;\; \sum_{k=0}^{\infty} a_k \cdot X^k \;\;\middle|\;\; a_k \in K \,,\, \forall' \, k \in \mathbb{N}_0 \,:\, a_k \,=\, 0 \;\right\} \quad .$$

Die Multiplikation $\cdot$ in $K[X]$ ist eine Abbildung

$$\cdot \,:\, K[X] \;\times\; K[X] \;\longrightarrow\; K[X] \quad ,$$

wir schränken sie ein auf $K \times K[X]$, dann haben wir eine äußere Operation

$$\omega :\; K \times K[X] \;\longrightarrow\; K[X] \quad , \quad (\alpha, \sum_{k=0}^{\infty} a_k \cdot X^k) \longmapsto \sum_{k=0}^{\infty} (\alpha \cdot a_k) \cdot X^k$$

und aus den Rechenregeln im Ring $K[X]$ folgt, dass $(K[X], +, \omega)$ ein $K-$Vektorraum ist.

4.2 Basis und Dimension

Grundlegend für die Lineare Algebra sind die Begriffe
"lineare Unabhängigkeit" und "Erzeugendensystem":
Definition und Satz 4.2.1 : Sei K ein Körper , V ein $K-$Vektorraum, $n \in \mathbb{N}$ und $(v_j)_{j \in \underline{n}}$ eine Familie von Vektoren aus V . Sei

$$\operatorname{span}(v_j)_{j \in \underline{n}} \quad := \quad \left\{ \;\; a \in V \;\mid\; \exists \, (\alpha_1, \ldots, \alpha_n) \in K^n \,:\; a \,=\, \sum_{j=1}^{n} \alpha_j v_j \;\right\} .$$

Dann ist $\operatorname{span}(v_j)_{j \in \underline{n}}$ ein Untervektorraum von V . Er heißt der von der Familie $(v_j)_{j \in \underline{n}}$ **aufgespannte Untervektorraum** von V . Die Elemente von $\operatorname{span}(v_j)_{j \in \underline{n}}$ heißen **Linearkombinationen** von $(v_j)_{j \in \underline{n}}$. Es gilt :
(1) $v_1, \ldots, v_n \in \operatorname{span}(v_j)_{j \in \underline{n}}$.
(2) Für jeden Untervektorraum U von V mit
$\{v_1, \ldots, v_n\} \subset U$ ist $\operatorname{span}(v_j)_{j \in \underline{n}} \subset U$,
d.h. $\operatorname{span}(v_j)_{j \in \underline{n}}$ ist der "kleinste" Untervektorraum von V , der die Vektoren $v_1, \ldots, v_n$ enthält. - Man setzt noch :

$$\operatorname{span}(v_j)_{j \in \underline{0}} \quad := \quad \{0\} \quad .$$

Beweis : Sei $n \in \mathbb{N}_0$ und $T := \operatorname{span}(v_j)_{j \in \underline{n}}$.
(0) Wir zeigen zunächst, dass T ein Untervektorraum von V ist:

Für $n = 0$ ist das klar. Sei nun $n \in \mathbb{N}$. Es gilt $T \subset V$ nach Definition, und

(UV1) $T \neq \emptyset$, da $0 = \sum_{j=1}^{n} 0\, v_j \in T$.

$\uparrow \quad \uparrow$

$\in V \quad \in K$

(UV2,3) Seien $a, b \in T$ und $\lambda \in K$, dann gibt es

$(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n) \in K^n$ mit

$$a = \sum_{j=1}^{n} \alpha_j v_j \quad \text{und} \quad b = \sum_{j=1}^{n} \beta_j v_j \quad , \qquad \text{also}$$

$$a + b = \sum_{j=1}^{n} (\alpha_j + \beta_j) v_j \quad , \quad \lambda\, a = \sum_{j=1}^{n} (\lambda\, \alpha_j) v_j \quad , \qquad \text{also}$$

$a + b \in T$, $\lambda\, a \in T$ wegen

$(\alpha_j + \beta_j)_{j \in \underline{n}}$, $(\lambda\, \alpha_j)_{j \in \underline{n}} \in K^n$.

(1) Für $n = 0$ ist bei (1) und (2) nichts zu zeigen. Sei $n \in \mathbb{N}$, dann gilt für alle $k \in \underline{n}$:

$$v_k = \sum_{j=1}^{n} \delta_{jk}\, v_j \quad \text{mit } \delta_{jk} = \begin{cases} 1 & \text{für } j = k \\ 0 & \text{für } j \neq k \end{cases} ,$$

also $v_k \in T$.

(2) Sei U ein Untervektorraum von V mit

$\{v_1, \ldots, v_n\} \subset U$,

dann sind alle $v_j \in U$ für $j \in \underline{n}$, und für beliebiges $\alpha_j \in K$ ist nach (UV3) auch $\alpha_j v_j \in U$. Nach (UV2), und mit Induktion nach n, folgt auch

$$\sum_{j=1}^{n} \alpha_j v_j \in U \quad .$$

Also gilt $T \subset U$. □

Definition 4.2.2 : Sei V ein $K-$Vektorraum. Gibt es ein $n \in \mathbb{N}_0$ und eine Familie $(v_j)_{j \in \underline{n}}$ mit $v_j \in V$ und

$$V \quad = \quad \text{span}(v_j)_{j \in \underline{n}} \quad ,$$

dann heißt V **endlich erzeugt** und die Familie $(v_j)_{j \in \underline{n}}$ ein **Erzeugendensystem** von V . □

Formal etwas komplizierter ist der Begriff "linear unabhängig":

Definition 4.2.3 : Sei K ein Körper und V ein $K-$Vektorraum. Sei $n \in \mathbb{N}$, und seien $a_1, \ldots, a_n \in V$. Die Familie

$(a_1, \ldots, a_n) \quad = \quad (a_j)_{j \in \underline{n}}$

heißt **linear unabhängig** , wenn gilt

$$\forall\,(\alpha_1,\ldots,\alpha_n)\in K^n\;:\;\left(\sum_{k=1}^{n}\alpha_k a_k\;=\;0\quad\Longrightarrow\quad\forall\,j\in\underline{n}\;:\;\alpha_j\;=\;0\right).$$

Die Familie $(v_1,\ldots,v_n)$ heißt **linear abhängig** , wenn sie nicht linear unabhängig ist, d.h. wenn gilt

$$\exists\,(\alpha_1,\ldots,\alpha_n)\in K^n\;:\;\left(\sum_{k=1}^{n}\alpha_k a_k\;=\;0\;\wedge\;\exists\,j\in\underline{n}\;:\;\alpha_j\neq 0\right).$$

Die "leere Familie" $(a_j)_{j\in\underline{0}}$ nennen wir linear unabhängig. □

Bemerkung 4.2.4 : Nach Definition 4.2.1 heißt der Vektor $\sum_{k=1}^{n}\alpha_k\,v_k$ eine Linearkombination von $(v_1,\ldots,v_n)$. Man nennt nun eine Linearkombination $\sum_{k=1}^{n}\alpha_k\,v_k$, in der nicht alle $\alpha_k\;=\;0$ sind, eine **nichttriviale Linearkombination** von $(v_1,\ldots,v_n)$, und die Linearkombination

$$\sum_{k=1}^{n}\alpha_k\,v_k\quad\text{mit}\quad\forall\,k\in\underline{n}\;:\;\alpha_k\;=\;0$$

die **triviale Linearkombination**. Also besagt Definition 4.2.3 :
Eine Familie $(v_1,\ldots,v_n)$ mit $n\in\mathbb{N}$ ist

- linear unabhängig genau dann, wenn nur die triviale Linearkombination von $(v_1,\ldots,v_n)$ Null ist, und
- linear abhängig, wenn es eine nichttriviale Linearkombination von $(v_1,\ldots,v_n)$ gibt, die Null ist. □

Beispiel 4.2.5 : Für eine beliebige Teilmenge A von $\mathbb{R}$, $A\neq\emptyset$, ist nach Beispiel 4.1.5

$$\mathcal{F}(A,\mathbb{R})\quad=\quad\{\,f\;:\;A\;\longrightarrow\;\mathbb{R}\,\}$$

ein $\mathbb{R}-$Vektorraum, mit den dort durch $(*)$ und $(**)$ definierten Rechenoperationen. Für $x\in A$ sei

$$f_1(x)\;:=\;|x|\quad,\quad f_2(x)\;:=\;x^2+x\quad,\quad f_3(x)\;:=\;x^2-x\quad.$$

a) Sei $A\;:=\;\mathbb{R}$ und $(\alpha_1,\alpha_2,\alpha_3)\in\mathbb{R}^3$ mit

$$\alpha_1\,f_1+\alpha_2\,f_2+\alpha_3\,f_3\;=\;0\in\mathcal{F}(A,\mathbb{R})\quad,$$

dann gilt für alle $x\in A\;=\;\mathbb{R}$:

$$\alpha_1\,f_1(x)+\alpha_2\,f_2(x)+\alpha_3\,f_3(x)\;=\;0(x)\;=\;0\in\mathbb{R}\quad,$$

$\alpha_1 |x| + \alpha_2 (x^2 + x) + \alpha_3 (x^2 - x) = 0$,
insbesondere für $x = 1, 2, -1$:

$$\alpha_1 + 2\alpha_2 = 0 \quad , \quad \text{also} \quad \alpha_2 = -\frac{1}{2}\alpha_1,$$

$$2\alpha_1 + 6\alpha_2 + 2\alpha_3 = 0 \quad , \quad \text{also} \quad \alpha_3 = \frac{1}{2}\alpha_1,$$

$$\alpha_1 + 2\alpha_3 = 0 \quad , \quad \text{also} \quad 2\alpha_1 = 0,$$

also $\alpha_1 = 0$ und damit auch $\alpha_2 = \alpha_3 = 0$. Also ist (f_1, f_2, f_3) im $\mathbb{R}-$Vektorraum $\mathcal{F}(\mathbb{R}, \mathbb{R})$ linear unabhängig.
b) Sei nun $A := \mathbb{R}_+^*$, dann gilt für alle $x \in A$:
$f_1(x) = x$,
$-2x + (x^2 + x) - (x^2 - x) = 0$, also
$-2f_1 + 1 \cdot f_2 + (-1)f_3 = 0$,
also ist (f_1, f_2, f_3) im $\mathbb{R}-$Vektorraum $\mathcal{F}(\mathbb{R}_+^*, \mathbb{R})$ linear abhängig. □

- Was bedeutet "lineare Unabhängigkeit" für zwei Vektoren ?

Bemerkung 4.2.6 : Seien $a_1, a_2 \in V$, und (a_1, a_2) sei linear abhängig, dann gibt es $\alpha_1, \alpha_2 \in K$ mit
$\alpha_1 a_1 + \alpha_2 a_2 = 0$
und α_1, α_2 sind nicht beide 0 . Ist $\alpha_1 \neq 0$, so folgt
$a_1 = -(\alpha_1^{-1} \cdot \alpha_2) a_2$,
ist $\alpha_1 = 0$, so folgt $\alpha_2 \neq 0$ und
$\alpha_2 a_2 = 0$, also $a_2 = 0$, also
$a_2 = 0\, a_1$.
Jedenfalls ist einer der beiden Vektoren (man weiß aber nicht, welcher) ein $\lambda-$ faches des anderen. Das gilt im Prinzip genau so für mehr als zwei Vektoren:

Satz 4.2.7 : Sei V ein $K-$Vektorraum . Sei $n \in \mathbb{N}$, $n \geq 2$ und $(a_1, \ldots, a_n)$ eine Familie von Vektoren aus V. Dann gilt:
$(a_1, \ldots, a_n)$ ist linear abhängig $\iff$ es gibt ein $k \in \underline{n}$, so dass a_k Linearkombination von $(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n)$ ist.

Beweis : " $\Longrightarrow$ " Sei $(a_1, \ldots, a_n)$ linear abhängig, dann gibt es
$(\alpha_1, \ldots, \alpha_n) \in K^n$, $(\alpha_1, \ldots, \alpha_n) \neq 0$, mit
$0 = \sum_{j=1}^{n} \alpha_j a_j$.
Es gibt ein $k \in \underline{n}$ mit $\alpha_k \neq 0$, also ist

$$a_k = -\alpha_k^{-1} \cdot \sum_{j \in \underline{n} \setminus \{k\}} \alpha_j a_j = \sum_{j \in \underline{n} \setminus \{k\}} (-\alpha_k^{-1} \cdot \alpha_j) a_j \quad .$$

" $\Longleftarrow$ ": Sei a_k Linearkombination von $(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n)$, dann gibt es eine Familie $(\beta_j)_{j \in \underline{n} \setminus \{k\}} \in K^{n-1}$ mit

$$a_k \quad = \quad \sum_{j \in \underline{n} \setminus \{k\}} \beta_j a_j \quad , \quad \text{also mit} \quad \beta_k := -1 :$$

$$\sum_{j=1}^{n} \beta_j a_j \; = \; 0 \quad \text{und} \quad (\beta_1, \ldots, \beta_k, \ldots, \beta_n) \neq 0 \quad ,$$

also ist $(a_1, \ldots, a_n)$ linear abhängig . □

Definition 4.2.8 : Sei V ein endlich erzeugter $K-$Vektorraum .
Sei $n \in \mathbb{N}_0$. Eine Familie $(v_j)_{j \in \underline{n}}$ von Elementen aus V heißt eine **Basis** von V, wenn gilt
(B1) $V = \text{span}(v_j)_{j \in \underline{n}}$, d.h. $(v_j)_{j \in \underline{n}}$ ist ein Erzeugendensystem von V , und
(B2) $(v_j)_{j \in \underline{n}}$ ist linear unabhängig.
Die Zahl n heißt die **Länge der Basis** $(v_j)_{j \in \underline{n}}$. □

Hier in diesem Paragraphen beschäftigen wir uns hauptsächlich mit endlich erzeugten Vektorräumen. Wir definieren aber auch, was eine Basis eines nicht endlich erzeugten Vektorraums ist:

Definition 4.2.9 : Sei V ein $K-$Vektorraum , $V \neq \{0\}$. Eine Familie $(v_j)_{j \in J}$ von Vektoren $v_j \in V$, wobei J eine beliebige Menge ist, heißt eine **Basis** von V, wenn gilt
(B1') $(v_j)_{j \in J}$ ist ein **Erzeugendensystem** von V , d.h. zu jedem $a \in V$ gibt es eine endliche Teilmenge $\{j_1, \ldots, j_n\}$ von J , so dass $a \in \text{span}(v_{j_1}, \ldots, v_{j_n})$ ist, und
(B2') $(v_j)_{j \in J}$ ist **linear unabhängig** , d.h. für jede endliche Teilmenge $\{j_1, \ldots, j_n\}$ von J ist $(v_{j_1}, \ldots, v_{j_n})$ linear unabhängig. □

Satz 4.2.10 : Sei V ein $K-$Vektorraum und $(v_j)_{j \in \underline{n}}$ mit $n \in \mathbb{N}$ eine Familie in V . Dann gilt:

$$(v_j)_{j \in \underline{n}} \text{ ist Basis von } V \iff \forall\, v \in V \exists_1 \, (\alpha_1, \ldots, \alpha_n) \in K^n \, : \, v \, = \, \sum_{j=1}^{n} \alpha_j v_j \, ,$$

d.h. $(v_j)_{j \in \underline{n}}$ ist genau dann eine Basis von V, wenn man jeden Vektor aus V eindeutig als Linearkombination von $(v_j)_{j \in \underline{n}}$ erhält.
Beweis : " $\Longrightarrow$ " : Sei $v \in V$, dann gilt wegen $V = \text{span}(v_j)_{j \in \underline{n}}$:

$$\exists \, (\alpha_1, \ldots, \alpha_n) \in K^n \, : \; v \, = \, \sum_{j=1}^{n} \alpha_j \, v_j \quad .$$

Sei auch $(\beta_1, \ldots, \beta_n) \in K^n$ mit $v = \sum_{j=1}^{n} \beta_j \, v_j$, dann ist

$$\sum_{j=1}^{n} (\alpha_j - \beta_j) \, v_j \quad = \quad v - v \quad = \quad 0 \quad ,$$

und da $(v_j)_{j\in\underline{n}}$ linear unabhängig ist : $\forall\, j \in \underline{n} : \alpha_j - \beta_j = 0$, also
$\forall\, j \in \underline{n} : \alpha_j = \beta_j$, also

$$\exists_1 (\alpha_1, \ldots, \alpha_n) \in K^n : \; v = \sum_{j=1}^{n} j\alpha_j v_j \quad .$$

" $\Longleftarrow$ " : Es gelte $\forall\, v \in V\, \exists_1 (\alpha_1, \ldots, \alpha_n) \in K^n : v = \sum_{j=1}^{n} \alpha_j v_j$, dann ist $(v_j)_{j\in\underline{n}}$ ein Erzeugendensystem von V . Sei

$$(\alpha_1, \ldots, \alpha_n) \in K^n \text{ mit } \sum_{j=1}^{n} \alpha_j v_j = 0 \quad ,$$

dann folgt wegen $0 = \sum_{j=1}^{n} 0\, v_j$, und da sich 0 eindeutig als Linearkombination von $(v_j)_{j\in\underline{n}}$ darstellen lässt,

$$\forall\, j \in \underline{n} : \; \alpha_j = 0 \quad .$$

Also ist $(v_j)_{j\in\underline{n}}$ linear unabhängig. □

Beispiel 4.2.11 : Sei $n \in \mathbb{N}$, dann ist K^n, die Menge der $n-$tupel von Elementen in K, mit den in 4.1.7 definierten Rechenoperationen ein $K-$Vektorraum . Setzen wir für $k \in \underline{n}$:

$$e_k := (0, \ldots, 0, 1, 0, \ldots, 0) = (\delta_{jk})_{j\in\underline{n}} \text{ mit } \delta_{jk} = \begin{cases} 1 & \text{für } j = k \\ 0 & \text{für } j \neq k \end{cases} ,$$

$$\uparrow$$

$k-$te Stelle

so ist $(e_k)_{k\in\underline{n}}$ eine Basis von K^n. Sie heißt die **kanonische** oder **Standard-Basis** von K^n.

Beweis: Sei $\sum_{k=1}^{n} \alpha_k e_k = 0 \in K^n$ mit $(\alpha_1, \ldots, \alpha_n) \in K^n$, dann ist

$$(\alpha_1, \ldots, \alpha_n) = (0, \ldots, 0) \quad , \quad \text{also}$$

$$\forall\, k \in \underline{n} : \; \alpha_k = 0 \quad ,$$

nach Definition der Gleichheit zweier Funktionen bzw. Familien. Also ist $(e_k)_{k\in\underline{n}}$ linear unabhängig. Sei $(\alpha_1, \ldots, \alpha_n) \in K^n$ beliebig, dann gilt

$$(\alpha_1, \ldots, \alpha_n) = \sum_{k=1}^{n} \alpha_k e_k \quad ,$$

also ist $(e_k)_{k\in\underline{n}}$ ein Erzeugendensystem von K^n. □

Beispiel 4.2.12 : Sei K ein Körper. In dem in 4.1.13 definierten $K-$Vektorraum $K[X]$ der Polynome mit Koeffizienten aus K sei

$$f_j(X) := X^j \quad \text{für} \quad j \in \mathbb{N}_0 \quad .$$

Wir behaupten: $(f_j(X))_{j\in\mathbb{N}_0}$ ist eine Basis von $K[X]$.

Beweis: (B1') ist klar, denn sei $f(X) \in K[X]$, dann gibt es ein $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in K$, so dass

$f(X) = \sum_{j=0}^{n} a_j \cdot X^j = \sum_{j=0}^{n} a_j f_j(X)$ ist, also

$$f(X) = \sum_{j=0}^{n} a_j \, f_j(X) \quad .$$

$f(X)$ ist eine Linearkombination der endlichen Teilfamilie $(f_j(X))_{j \in \underline{n} \cup \{0\}}$.

(B2') Sei $J \subset \mathbb{N}_0$ endlich und $\sum_{j \in J} \alpha_j \, f_j(X) = 0$. Setzen wir noch

$$\alpha_j := 0 \quad \text{für} \quad j \in \mathbb{N}_0 \setminus J \quad , \quad \text{so haben wir}$$

$$\sum_{j=0}^{\infty} \alpha_j X^j = 0 \quad .$$

Nach Folgerung 3.3.9 sind die Koeffizienten eines Polynoms eindeutig bestimmt,

also $\forall \, j \in \mathbb{N}_0 : \alpha_j = 0$.

Also ist $(f_j(X))_{j \in \mathbb{N}_0}$ linear unabhängig. □

Bemerkung 4.2.13 : Unser Ziel ist es, zu zeigen:

(I) Jeder Vektorraum besitzt eine Basis. Für endlich erzeugte Vektorräume folgt der Beweis.

(II) Ist V endlich erzeugt, so haben zwei Basen von V die gleiche Länge.

Zum Beweis brauchen wir den Basisergänzungssatz und den Austauschsatz, die beide nicht wirklich schwierig zu beweisen sind :

Basisergänzungssatz 4.2.14 : Sei V ein endlich erzeugter $K-$Vektorraum . Sei

$(a_j)_{j \in \underline{r}}$ mit $r \in \mathbb{N}_0$ ein endliches Erzeugendensystem von V

und

$(b_k)_{k \in \underline{s}}$ mit $s \in \mathbb{N}_0$ eine linear unabhängige Familie in V .

Dann gibt es t Vektoren

$b_{s+1}, \ldots, b_{s+t} \in \{a_1, \ldots, a_r\}$, so dass

$(b_k)_{k \in \underline{s+t}}$ eine Basis von V ist.

Also: Man kann jede linear unabhängige Familie durch Hinzunahme geeigneter Vektoren aus V zu einer Basis von V ergänzen.

Beweis : Es kann sein, dass gilt :

(a) $(b_k)_{k \in \underline{s}}$ ist ein Erzeugendensystem von V ,

dann ist $(b_k)_{k \in \underline{s}}$ bereits eine Basis von V , wir brauchen also nichts hinzuzunehmen, können also $t := 0$ nehmen. Wenn (a) nicht gilt, ist jedenfalls

$(b_1, \ldots, b_s, a_1, \ldots, a_r)$

ein Erzeugendensystem von V , denn sei $v \in V$, dann gilt

$$\exists \, (\alpha_j)_{j \in \underline{r}} \in K^r : \; v = \sum_{j=1}^{r} \alpha_j \, a_j \quad , \quad \text{also}$$

$$v = \sum_{k=1}^{s} 0 \, b_k + \sum_{j=1}^{r} \alpha_j \, a_j \in \operatorname{span}(b_1, \ldots, b_s, a_1, \ldots, a_r) \quad .$$

Dabei kann es sein, dass man nicht alle der Vektoren $a_1, \ldots, a_r$ braucht , um - zusammen mit den $b_1, \ldots, b_s$ - V zu erzeugen. Sei

$$M \quad := \quad \{m \in \mathbb{N}_0 \mid \exists \{c_1, \ldots, c_m\} \subset \{a_1, \ldots, a_r\} : \\ V = \operatorname{span}(b_1, \ldots, b_s, c_1, \ldots, c_m)\} \quad ,$$

dann ist $0 \notin M$, da (a) nicht gilt, also $M \subset \mathbb{N}$. Es ist $r \in M$, also $M \neq \emptyset$, und nach Satz 1.2.13 existiert

$$t \quad := \quad \min M \in \mathbb{N} \quad .$$

Dann ist

$(b_1, \ldots, b_s, c_1, \ldots, c_t)$ mit $\{c_1, \ldots, c_t\} \subset \{a_1, \ldots, a_r\}$

ein Erzeugendensystem von V , und auch linear unabhängig, denn seien $\beta_1, \ldots, \beta_s, \gamma_1, \ldots, \gamma_t \in K$ mit

$$\sum_{k=1}^{s} \beta_k b_k + \sum_{l=1}^{t} \gamma_l c_l \quad = \quad 0 \quad ,$$

dann könnte gelten :

(1) $\exists j \in \underline{t} : \gamma_j \neq 0$, dann folgt für dieses j :

$$c_j \quad = \quad \sum_{k=1}^{s} (-\gamma_j^{-1}\beta_k) b_k + \sum_{l \in \underline{t} \setminus \{j\}} (-\gamma_j^{-1}\gamma_l) c_l \quad ,$$

also $c_j \in \operatorname{span}(b_1, \ldots, b_s, c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_t)$, also

$(*)$ $V \quad = \quad \operatorname{span}(b_1, \ldots, b_s, c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_t)$,

denn zu jedem $v \in V$ gibt es $\alpha_1, \ldots, \alpha_s, \delta_1, \ldots, \delta_t \in K$ mit

$$v \quad = \quad \sum_{k=1}^{s} \alpha_k b_k + \sum_{l=1}^{t} \delta_l c_l \, , \quad \text{also}$$

$$v \quad = \quad \sum_{k=1}^{s} (\alpha_k - \delta_j \gamma_j^{-1} \beta_k) b_k + \sum_{l \in \underline{t} \setminus \{j\}} (\delta_l - \delta_j \gamma_j^{-1} \gamma_l) c_l \quad .$$

Aus $(*)$ folgt aber : $t - 1 \in M$, Widerspruch zu $t = \min M$. Also gilt (1) nicht, sondern

(2) $\forall l \in \underline{t} : \gamma_l = 0$, und damit

$\sum_{k=1}^{s} \beta_k b_k = 0$, also, da $(b_k)_{k \in \underline{s}}$ linear unabhängig ist, auch

$\forall k \in \underline{s} : \beta_k = 0$,

und wir sind fertig. □

Folgerung 4.2.15 : Sei V ein $K-$Vektorraum und

$(a_j)_{j\in\underline{r}}$ mit $r \in \mathbb{N}_0$ ein Erzeugendensystem von V .
Dann gibt es ein $n \in \mathbb{N}_0$, $n \leq r$ und eine Teilfamilie
$(c_1, \ldots, c_n)$ von $(a_j)_{j\in\underline{r}}$, die Basis von V ist.
Beweis : Man wende Satz 4.2.14 mit $s := 0$ an. □
Folgerung 4.2.16 : Jeder endlich erzeugte $K-$Vektorraum V besitzt eine Basis. □

Bemerkung 4.2.17 : Auch Vektorräume, die nicht endlich erzeugt sind, besitzen eine Basis. Wir wollen das aber nicht beweisen.

Hilfssatz 4.2.18 : Sei V ein $K-$Vektorraum und $(b_1, \ldots, b_n)$ eine Basis von V . Seien $u, v \in V$ beliebig, dann ist
$(u, v, b_2, \ldots, b_n)$ linear abhängig.
Beweis : Wegen $u, v \in \operatorname{span}(b_j)_{j\in\underline{n}}$ gilt :

$$\exists\,(\beta_j)_{j\in\underline{n}} \in K^n \,:\, u = \sum_{j=1}^{n} \beta_j\, b_j \quad \wedge \quad \exists\,(\gamma_j)_{j\in\underline{n}} \in K^n \,:\, v = \sum_{j=1}^{n} \gamma_j\, b_j \quad ,$$

also

$$\gamma_1 u - \beta_1 v \quad = \quad \sum_{j=2}^{n} (\gamma_1\beta_j - \beta_1\gamma_j)\, b_j \,,$$

und wenn $\gamma_1 \neq 0$ oder $\beta_1 \neq 0$ ist, folgt die Beh. Für $\gamma_1 = 0$ haben wir

$$0\,u + (-1)v + \sum_{j=2}^{n} \gamma_j\, b_j \quad = \quad 0 \quad ,$$

und wegen $-1 \neq 0$ folgt die Behauptung. □

Austauschsatz 4.2.19 : Sei V ein $K-$Vektorraum , $(b_1, \ldots, b_n)$ eine Basis von V und $(a_1, \ldots, a_m)$ ein Erzeugendensystem von V . Dann gilt für alle $k \in \mathbb{N}_0$:
Wenn $k \leq n$ ist, gibt es k Vektoren $a_{i_1}, \ldots, a_{i_k} \in \{a_1, \ldots, a_m\}$, so dass
$(a_{i_1}, \ldots, a_{i_k}, b_{k+1}, \ldots, b_n)$
eine Basis von V ist.
Beweis durch Induktion nach k :
(I) Für $k = 0$ ist die Behauptung trivialerweise wahr.
(II) Sei $k \in \mathbb{N}_0$, und für k sei die Behauptung wahr. Ist $k \leq n$, so haben wir dann eine Basis
$(a_{i_1}, \ldots, a_{i_k}, b_{k+1}, \ldots, b_n)$ mit $a_{i_1}, \ldots, a_{i_k} \in \{a_1, \ldots, a_m\}$
von V . Ist nun $k + 1 > n$, so ist die Behauptung für $k + 1$ richtig.
Ist $k + 1 \leq n$, so ist $k < n$, und
$(a_{i_1}, \ldots, a_{i_k}, \quad b_{k+2} \ldots, b_n)$
ist eine aus $n - 1$ Vektoren bestehende, linear unabhängige, Familie in

V . Nach Satz 4.2.14 kann man sie durch Hinzunahme von Vektoren aus $\{a_1, \ldots, a_m\}$ ergänzen zu einer Basis von V . Zwei (oder mehr) Vektoren aus $\{a_1, \ldots, a_m\}$ können es nach Hilfssatz 4.2.18 nicht sein, denn dann wäre die entstehende Familie linear abhängig, da wir aus

$(a_{i_1}, \ldots, a_{i_k}, b_{k+1}, b_{k+2}, \ldots, b_n)$

nur den einen Vektor b_{k+1} herausgenommen haben. 0 Vektoren aus $\{a_1, \ldots, a_m\}$ können es auch nicht sein, denn dann wäre bereits $(a_{i_1}, \ldots, a_{i_k}, b_{k+2}, \ldots, b_n)$ eine Basis von V , also b_{k+1} eine Linearkombination dieser Basis und damit $(a_{i_1}, \ldots, a_{i_k}, b_{k+1}, \ldots, b_n)$ linear abhängig. Also können wir einen Vektor aus $\{a_1, \ldots, a_m\}$ finden, den wir $a_{i_{k+1}}$ nennen, so dass

$(a_{i_1}, \ldots, a_{i_{k+1}}, b_{k+2}, \ldots, b_n)$ eine Basis von V ist. □

Folgerung 4.2.20 : Sei V ein $K-$Vektorraum . Seien $m, n \in \mathbb{N}_0$, $(a_1, \ldots, a_m)$ ein Erzeugendensystem und $(b_1, \ldots, b_n)$ eine Basis von V . Dann gilt

$$n \leq m \quad .$$

Beweis : Wir wenden den Austauschsatz an mit $k := n$: Es gibt n Vektoren $a_{i_1}, \ldots, a_{i_n} \in \{a_1, \ldots, a_m\}$, so dass

$(a_{i_1}, \ldots, a_{i_n})$ eine Basis von V ist.

Die Vektoren $a_{i_1}, \ldots, a_{i_n}$ sind alle verschieden, denn gäbe es $j, k \in \underline{n}$ mit $j \neq k$ und $a_{i_j} = a_{i_k}$, dann hätten wir

$$1 \cdot a_{i_j} + (-1) a_{i_k} + \sum_{l \in \underline{n} \setminus \{j,k\}} 0 \cdot a_{i_l} \quad = \quad 0 \quad ,$$

im Widerspruch zur linearen Unabhängigkeit von $(a_{i_1}, \ldots, a_{i_n})$. Also liegen in $\{a_1, \ldots, a_m\}$ mindestens n verschiedene Elemente; es ist $n \leq m$.

□

Folgerung 4.2.21 : Sei V ein $K-$Vektorraum . Seien $n, m \in \mathbb{N}_0$, und seien $(a_1, \ldots, a_m)$ und $(b_1, \ldots, b_n)$ Basen von V . Dann gilt $n = m$, d.h. zwei Basen von V haben gleiche Länge.

Beweis : Jede Basis ist auch ein Erzeugendensystem von V , also gilt nach Folgerung 4.2.20 :

$$n \leq m \quad \text{und} \quad m \leq n \quad . \qquad \square$$

Definition 4.2.22 : Sei V ein $K-$Vektorraum .

a) Ist V endlich erzeugt, so gibt es nach Folgerung 4.2.15 eine Basis endlicher Länge. Sei n die Länge einer beliebigen endlichen Basis

von V . (Das n ist nach Folgerung 4.2.21 eindeutig bestimmt.) Dann setzen wir

$$\dim V \quad := \quad \dim_K V \quad := \quad n$$

und nennen n die **Dimension** von V (über K).

b) Ist V nicht endlich erzeugt, so schreiben wir :

$$\dim V \quad = \quad \dim_K V \quad = \quad \infty$$

und nennen V einen **unendlichdimensionalen** $K-$Vektorraum.

□

Beispiel 4.2.11 : Sei $n \in \mathbb{N}$. Im $K-$Vektorraum K^n war

$$(e_1, \ldots, e_n) \quad \text{mit} \quad e_k = (\delta_{jk})_{j \in \underline{n}}$$

eine Basis, also ist $\dim_K K^n = n$.

Beispiel 4.2.12 : Im $K-$Vektorraum $K[X]$ war

$$(f_j(X))_{j \in \mathbb{N}_0} \quad \text{mit} \quad f_j(X) = X^j$$

eine Basis. $K[X]$ ist nicht endlich erzeugt, denn wäre

$$\dim_K K[X] = n \in \mathbb{N}_0 \quad ,$$

dann könnte man die aus $n+1$ Elementen bestehende Familie $(f_j(X))_{j \in \underline{n} \cup \{0\}}$ zu einer Basis ergänzen, die dann mehr als n Elemente hätte, Widerspruch zu Folgerung 4.2.21. Also ist

$$\dim_K K[X] = \infty.$$

Beispiel 4.2.23 : Nach Beispiel 4.1.3 ist $\mathbb{C}$ ein $\mathbb{R}-$Vektorraum. Zu jedem $z \in \mathbb{C}$ gibt es eindeutig bestimmte $a, b \in \mathbb{R}$ mit

$$z = a \cdot 1 + b \cdot i \quad ,$$

also ist $(1, i)$ eine Basis des $\mathbb{R}-$Vektorraums $\mathbb{C}$, also ist

$$\dim_{\mathbb{R}} \mathbb{C} = 2 \quad .$$

Nach Beispiel 4.2.11 ist andererseits wegen $\mathbb{C} = \mathbb{C}^1$:

$$\dim_{\mathbb{C}} \mathbb{C} = 1 \quad .$$

Satz 4.2.24 : Sei V ein $K-$Vektorraum . V sei endlichdimensional, d.h. es gebe ein $n \in \mathbb{N}_0$ mit

$$\dim_K V = n \quad .$$

Dann gilt für jeden Untervektorraum U von V :

(1) Auch U ist endlich erzeugt, und $\dim_K U \leq \dim_K V$.

(2) Aus $\dim_K U = \dim_K V$ folgt $U = V$.

Beweis : (1) Es gibt eine Basis $(b_1, \ldots, b_n)$ von V . Angenommen, es ist $\dim_K U = \infty$ oder $\dim_K U = m > n$, dann gibt es in U eine linear unabhängige Familie

$$(u_1, \ldots, u_{n+1}) \quad ,$$

die dann auch in V linear unabhängig ist. Nach dem Basisergänzungssatz 4.2.14 lässt sie sich ergänzen zu einer Basis

$(u_1, \ldots, u_{n+1}, \ldots, u_r)$ von V ,

mit $r \geq n+1 > n$, Widerspruch zu Folgerung 4.2.21. Also ist $\dim U \leq n$.
(2) Sei $\dim_K U = \dim_K V = n$, dann gibt es eine Basis

$(a_1, \ldots, a_n)$ von U .

$(a_1, \ldots, a_n)$ ist linear unabhängig in V , lässt sich also nach 4.2.21 ergänzen zu einer Basis

$(a_1, \ldots, a_n, c_1, \ldots, c_t)$ mit $t \in \mathbb{N}_0$, $c_1, \ldots, c_t \in V$

von V , die dann die Länge $n+t$ hat. Nach 4.2.21 folgt $n+t = n$, also $t = 0$, also ist $(a_1, \ldots, a_n)$ Basis von V ,

$V = \operatorname{span}(a_1, \ldots, a_n) = U$.

□

4.3 Lineare Abbildungen

Definition 4.3.1 : Sei K ein Körper, V und W seien $K-$Vektorräume (also Vektorräume über demselben Körper). Eine Abbildung

$F : V \longrightarrow W$

heißt eine **$K-$lineare Abbildung** (oder ein **$K-$Vektorraum-Homomorphismus**), wenn gilt

(L1) $\forall\, a, b \in V : \underset{\uparrow}{F(a+b)} = \underset{\uparrow}{F(a)} + \underset{\uparrow}{F(b)}$, und

Addition in V , Addition in W

(L2) $\forall\, a \in V \,\forall\, \lambda \in K : \underset{\uparrow}{F(\lambda a)} = \underset{\uparrow}{\lambda F(a)}$.

äußere Operation auf V , auf W .

Die Begriffe Endo-, Mono-, Epi-, Iso- und Auto-morphismus von Vektorräumen definiert man wie in 2.3.2.

Bemerkung 4.3.2 : Seien V , W $K-$Vektorräume und

$F : V \longrightarrow W$ sei $K-$linear.

Dann ist F nach (L1) ein Gruppenhomomorphismus von $(V, +)$ in $(W, +)$. Aus Satz 2.3.4 folgt daher
$F(0) = 0$ und $\forall\, b \in V : F(-b) = -F(b)$ und damit
$\forall\, a, b \in V : F(a-b) = F(a) - F(b)$.

Satz 4.3.3 : (1) Sei $(v_1, \ldots, v_n)$ linear abhängig in V , dann ist

$(F(v_1), \ldots, F(v_n))$ linear abhängig in W .

(2) Ist V' ein Untervektorraum von V , so ist $F(V')$ ein

Untervektorraum von W .

(3) Ist W' ein Untervektorraum von W , so ist $\overset{-1}{F}(W')$ ein

Untervektorraum von V .

(4) $\dim F(V) \leq \dim V$, wenn man für $\in \mathbb{N}_0 \cup \{\infty\}$ setzt: $n \leq \infty$.

Beweis : (1),(2),(3) als Übungsaufgabe.

(4) Für $\dim V = \infty$ ist das sicher richtig. Sei $\dim V = n \in \mathbb{N}_0$, dann haben wir eine Basis $(v_1, \ldots, v_n)$ von V . Zu $y \in F(V)$ gibt es ein $v \in V$ mit $y = F(v)$, und

$$\exists\, (\alpha_j)_{j \in \underline{n}} \in K^n : \; v = \sum_{j=1}^{n} \alpha_j v_j \quad , \qquad \text{also}$$

$$F(v) = F(\sum_{j=1}^{n} \alpha_j\, v_j) \overset{(L1)}{=} \sum_{j=1}^{n} F(\alpha_j v_j) \overset{(L2)}{=} \sum_{j=1}^{n} \alpha_j F(v_j) \quad ,$$

also ist $(F(v_1), \ldots, F(v_n))$ ein Erzeugendensystem von $F(V)$, und nach Folgerung 4.2.20 :

$\dim_K F(V) \leq n$. □

Bemerkung 4.3.4 : Sei $F : V \longrightarrow W$ $K-$linear, dann definiert man den **Kern** von F als Kern des Gruppenhomorphismus F von $(V, +)$ in $(W, +)$, also

$$\ker F \quad := \quad \overset{-1}{F}(\{0\}) \quad = \quad \{\; v \in V \mid F(v) = 0 \;\} \quad .$$

Nach 4.3.3(3) ist $\ker F$ ein Untervektorraum von V . Nach Satz 2.3.9 gilt

F ist injektiv $\iff$ $\ker F = \{0\}$.

□

(4.3.5) Beispiele für lineare Abbildungen

Triviale Beispiele sind

$0 : V \longrightarrow W$, $0(v) := 0 \in W$ für alle $v \in V$, und

$\mathrm{id}_V : V \longrightarrow V$, $\mathrm{id}_V(x) := x$ für alle $x \in V$.

Ein weiteres Beispiel für lineare Abbildungen steht in

Satz und Definition 4.3.6 : Sei V ein $K-$Vektorraum mit $\dim_k V = n \in \mathbb{N}$ und

$\mathfrak{B} := (v_1, \ldots, v_n)$ eine Basis von V , dann ist

$$\Phi_{\mathfrak{B}} : K^n \longrightarrow V \quad , \quad \Phi_{\mathfrak{B}}(\beta_1, \ldots, \beta_n) := \sum_{j=1}^{n} \beta_j\, v_j$$

ein $K-$Vektorraum-Isomorphismus. .$\Phi_{\mathfrak{B}}$ heißt der durch $\mathfrak{B}$ gegebene **Basisisomorphismus** von K^n nach V.

Der **Beweis** ist eine sehr leichte Übungsaufgabe. □

Satz und Definition 4.3.7 : Seien V und W $K-$Vektorräume, dann ist

$$\mathrm{Hom}_K(V,W) \quad := \quad \{\ F \in \mathcal{F}(V,W) \mid F \text{ ist } K-\text{linear}\ \}$$

ein Untervektorraum von $\mathcal{F}(V,W)$. Für $V = W$ schreibt man

$$\mathrm{End}_K(V) \quad := \quad \mathrm{Hom}_K(V,V)\ ,$$

die Elemente von $\mathrm{End}_K(V)$ sind also die Endomorphismen von V . Für $W = K$ nennt man

$$V^* \quad := \quad \mathrm{Hom}_K(V,K)$$

den **Dualraum** von V und die Elemente von V^* **Linearformen** auf V.

Beweis : Nach Definition ist $\mathrm{Hom}_K(V,W) \subset \mathcal{F}(V,W)$ und $\mathrm{Hom}_K(V,W) \neq \emptyset$, da $0 : V \longrightarrow W$, $v \longmapsto 0$, $K-$ linear ist. Seien $F, G \in \mathrm{Hom}_K(V,W)$ und $\lambda \in K$, dann sind auch

$$F+G\,,\ \lambda F \in \mathrm{Hom}_K(V,W) \quad ,$$

denn für $a, b \in V$ und $\alpha \in K$ gilt

$$\begin{aligned}
(F+G)(a+b) &\overset{(*)}{=} F(a+b)+G(a+b) \overset{(1)}{=} F(a)+F(b)+G(a)+G(b)\\
&= F(a)+G(a)+F(b)+G(b) \overset{(*)}{=} (F+G)(a)+(F+G)(b) \quad ,\\
(F+G)(\alpha a) &\overset{(*)}{=} F(\alpha a)+G(\alpha a) \overset{(1)}{=} \alpha F(a)+\alpha G(a)\\
&= \alpha(F(a)+G(a)) \overset{(*)}{=} \alpha(F+G)(a) \quad ,\\
(\lambda F)(a+b) &\overset{(**)}{=} \lambda F(a+b) \overset{(1)}{=} \lambda(F(a)+F(b))\\
&= \lambda F(a)+\lambda F(b) \overset{(**)}{=} (\lambda F)(a)+(\lambda F)(b) \quad ,\\
(\lambda F)(\alpha a) &\overset{(**)}{=} \lambda F(\alpha a) \overset{(1)}{=} \lambda(\alpha F(a))) \ = \ (\lambda\cdot\alpha)F(a)\\
&= (\alpha\cdot\lambda)F(a) \ = \ \alpha(\lambda F(a)) \overset{(**)}{=} \alpha(\lambda F)(a) \quad .
\end{aligned}$$

Bei $(*)$ und $(**)$ haben wir die Definition der Rechenoperationen in $\mathcal{F}(V,W)$ benutzt, bei (1) die Linearität von F und G. □

Auch die Hintereinanderausführung linearer Abbildungen ist linear :

Satz 4.3.8 : Seien U, V, W $K-$Vektorräume,

$$G \in \mathrm{Hom}_K(U,V) \quad \text{und } F \in \mathrm{Hom}_K(V,W) \quad ,$$

dann ist $F \circ G \in \mathrm{Hom}_K(U,W)$.

Beweis : $F \circ G$ ist eine Abbildung von U in W . $F \circ G$ ist $K-$linear, denn für alle $a, b \in U$ und alle $\alpha \in K$ gilt

$$(F\circ G)(a+b) \ = \ F(G(a+b)) \overset{G \text{ linear}}{=} F(G(a)+G(b))$$

$$\overset{F \text{ linear}}{=} F(G(a)) + F(G(b)) \;=\; (F \circ G)(a) + (F \circ G)(b) \quad ,$$

$$(F \circ G)(\alpha a) \;=\; F(G(\alpha a)) \overset{G \text{ linear}}{=} F(\alpha G(a))$$

$$\overset{F \text{ linear}}{=} \alpha F(G(a)) \;=\; \alpha (F \circ G)(a) \quad . \qquad \square$$

Definition und Satz 4.3.9 : Sei K ein Körper, V ein $K-$Vektorraum und W ein Untervektorraum von V . Dann hat man nach 2.2.12 die Faktorgruppe

$$V/_W \;=\; \{\; v + W \;\mid\; v \in V \;\} \quad , \quad \text{wobei}$$

$$v + W \;=\; \{\; v + w \;\mid\; w \in W \;\} \quad \text{ist ,}$$

und es gilt für $u, v \in V$:

$$(u + W) + (v + W) \quad = \quad (u + v) + W \quad ,$$

$$u + W \;=\; v + W \quad \Longleftrightarrow \quad u - v \in W.$$

Wenn man für $v \in V$, $\lambda \in K$ definiert:

$$\omega(\lambda, v + W) \quad := \quad \lambda(v + W) \quad := \quad (\lambda v) + W \quad ,$$

dann wird $(V/_W, +, \omega)$ ein $K-$Vektorraum. $V/_W$ heißt der **Quotienten-Vektorraum** von V **modulo** W .

Beweis : Das Axiom (V2) für $V/_W$ gilt, da es für $(V, +, \omega)$ gilt.

$\square$

Beispiel 4.3.10 : Nehmen wir

$$V \quad := \quad \mathbb{R}^2 \quad \text{und} \quad W \quad := \quad \mathbb{R} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad ,$$

dann sind die Elemente von $V/_W$ Geraden, die zu $\mathbb{R} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ parallel sind.

- Der Homomorphiesatz für Gruppen gilt auch für Quotienten-Vektorräume:

(4.3.11) Homomorphiesatz für Vektorräume : Seien V und U $K-$Vektorräume,

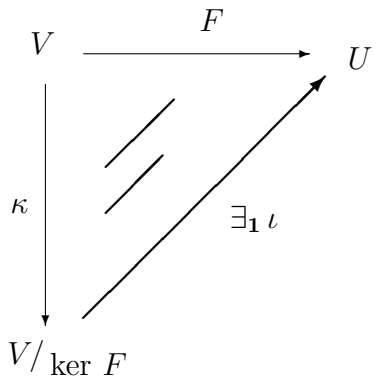
$$F \;:\; V \;\longrightarrow\; U \quad \text{eine surjektive lineare Abbildung . Sei}$$

$$\kappa \;:\; V \;\longrightarrow\; V/_{\ker F} \quad , \quad x \mapsto x + \ker F$$

der kanonische Nebenklassenepimorphismus von V auf den Quotienten-Vektorraum $V/_{\ker F}$, dann gibt es genau einen Vektorraum-Isomorphismus

$$\iota : V/_{\ker F} \longrightarrow U \quad \text{mit} \quad \iota \circ \kappa = F \quad .$$

Als Diagramm:



Beweis : Da Satz 2.3.9 gilt, müssen wir nur noch zeigen, dass κ und ι die Linearitätsbedingung (L2) erfüllen. Das ist aber leicht zu sehen.

□

Satz 4.3.12 : Sei V ein endlichdimensionaler $K-$Vektorraum und W ein Untervektorraum von V , dann ist

$$\dim V/_W \quad = \quad \dim V \; - \; \dim W \quad .$$

Es gilt:
(∗) Wenn $(w_1, \ldots, w_k)$ eine Basis von W ist,
und wir diese durch $v_1, \ldots, v_r$ zu einer Basis
$(w_1, \ldots, w_k, v_1, \ldots, v_r)$ von V ergänzen können, dann ist
$(v_1 + W, \ldots, v_r + W)$ eine Basis von $V/_W$.
Beweis : Nach Satz 4.2.24 ist auch W endlichdimensional. Sei

$$(w_1, \ldots, w_k) \quad \text{eine Basis von } W \quad ,$$

dann können wir diese Basis nach Satz 4.2.14 ergänzen zu einer Basis

$$(w_1, \ldots, w_k, v_1, \ldots, v_r) \quad \text{von} \quad V$$

und behaupten:

$$(*) \qquad (v_1 + W, \ldots, v_r + W) \quad \text{ist eine Basis von} \quad V/_W \quad .$$

Wenn wir das gezeigt haben, folgt

$$\dim V/_W \quad = \quad r \quad = \quad (r+k)-k \quad = \quad \dim V \; - \; \dim W \quad .$$

(4.3.13) Dimensionsformel für lineare Abbildungen : Seien V, U $K-$Vektorräume,

$$F \; : \; V \; \longrightarrow \; U \quad K-\text{linear und } \dim_k V < \infty \quad .$$

Dann gilt die Formel

$$\dim V \quad = \quad \dim \ker F + \dim F(V) \quad .$$

$(*)$ Nach 4.2.24 existiert eine endliche Basis

$$(w_1, \ldots, w_k) \text{ von } \ker F,$$

die wir durch $v_1, \ldots, v_r$ zu einer Basis $(w_1, \ldots, w_k, v_1, \ldots v_r)$ von V ergänzen können. Dann ist

$$(F(v_1), \ldots, F(v_r)) \quad \text{eine Basis von} \quad F(V) \quad .$$

Beweis : Wir schränken den Wertebereich von F ein, indem wir

$$G \; : \; V \; \longrightarrow \; F(V) \quad , \quad G(x) := F(x)$$

setzen, dann ist G linear und surjektiv, und es ist

$$\ker G \quad = \quad \ker F \quad .$$

Nach Satz 4.3.12 ist dann

$$\dim V \quad = \quad \dim \ker F + \dim V/_{\ker F} \quad .$$

Nach dem Homomorphiesatz 4.3.11 gibt es einen Isomorphismus

$$\iota \; : \; V/_{\ker F} \; \longrightarrow \; F(V) \quad ,$$

also $\dim V/_{\ker F} = \dim F(V)$, womit

$$\dim V \quad = \quad \dim \ker F + \dim F(V)$$

bewiesen ist. Der Rest folgt aus $(*)$ von Satz 4.3.12 : Wenn wir eine Basis $(w_1, \ldots, w_r)$ von $\ker F$ haben, und diese durch $(v_1, \ldots, v_r)$ zu einer Basis von V ergänzen, ist

$$(v_1 + \ker F, \ldots, v_r + \ker F) \quad \text{eine Basis von} \quad V/_{\ker F} \quad .$$

Die folgenden Aussagen (mit $\kappa(x) := x + \ker F$) sind gleichbedeutend:

$$(\kappa(v_1), \ldots, \kappa(v_r)) \quad \text{ist eine Basis von} \quad V/_{\ker F} \quad .$$

und da ι ein Isomorphismus ist:

$$(\iota(\kappa(v_1)), \ldots, \iota(\kappa(v_r))) \quad \text{ist eine Basis von} \quad F(V) \quad .$$

und wegen $\iota \circ \kappa = F$:

$$(F(v_1), \ldots, F(v_r)) \quad \text{ist eine Basis von} \quad F(V) \quad .$$

□

4.4 Matrizen

Unser Ziel ist es, einer linearen Abbildung

$$F : V \longrightarrow W ,$$

wobei V und W endlichdimensionale Vektorräume über einem Körper K sind, eine Matrix zuzuordnen. Matrizen sind aber auch für sich genommen interessante Objekte in der Algebra. Wir beschäftigen uns daher zunächst mit Matrizen und den Rechenoperationen zwischen ihnen:

Definition 4.4.1 : Seien $m, n \in \mathbb{N}$. Eine **$m \times n$ - Matrix** mit **Einträgen** aus einer Menge R ist eine Familie

$$A \quad = \quad (a_{kj})_{(k,j)\in \underline{m}\times\underline{n}} \quad \text{mit} \quad a_{kj} \in R \quad , \quad \text{kurz:} \quad A = (a_{kj}) ,$$

also eine Abbildung $A \in \mathcal{F}(\underline{m} \times \underline{n}, R)$, $A(k, j) := a_{kj}$. Man schreibt sich eine Matrix $A = (a_{kj})_{(k,j)\in \underline{m}\times\underline{n}}$ zumeist als "rechteckiges Schema" auf:

$$A \quad = \quad \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \quad .$$

Für die Menge aller $m \times n$ - Matrizen mit Einträgen aus R schreiben wir

$$M(m \times n, R) \quad ,$$

und für $A = (a_{kj}) \in M(m \times n, R)$ nennen wir die

$$a_k \quad := \quad (a_{k1}, \ldots, a_{kn}) \quad \text{für } k \in \underline{m} \text{ die } \textbf{Zeilenvektoren} \text{ von } A \ ,$$

und die

$$a^j \quad := \quad \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \quad \text{für } j \in \underline{n} \text{ die } \textbf{Spaltenvektoren} \text{ von } A .$$

Ist $m = n$, so heißt die Matrix A **quadratisch** .
Nach unserer Definition ist $M(m \times n, R) = \mathcal{F}(\underline{m} \times \underline{n}, R)$. Damit ist auch definiert, wann zwei Matrizen

$A = (a_{kj})$, $B = (b_{kj})$ gleich sind:

Es gilt $(a_{kj}) = (b_{kj}) \iff \forall\,(k,j) \in \underline{m} \times \underline{n} : a_{kj} = b_{kj}$.

Definition 4.4.2 : Sei $(R, +, \cdot)$ ein kommutativer Ring, $m, n \in \mathbb{N}$. Dann definieren wir für $(a_{kj}), (b_{kj}) \in M(m \times n, R)$ und $\lambda \in R$:

$$(*) \qquad \begin{cases} (a_{kj}) + (b_{kj}) & := & (a_{kj} + b_{kj})\,, \\ \\ \lambda(a_{kj}) & := & (\lambda \cdot a_{kj}) \end{cases}$$

Wenn 0 das Nullelement und 1 das Einselement von R bezeichnet, setzen wir für $(k,j) \in \underline{m} \times \underline{n}$:

$$E_{kj} \quad := \quad \begin{pmatrix} & & & 0 & & & \\ & & 0 & \vdots & 0 & & \\ & & & 0 & & & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ & & & 0 & & & \\ & & 0 & \vdots & 0 & & \\ & & & 0 & & & \end{pmatrix} \longleftarrow k-\text{te Zeile}$$

$$\uparrow$$

$$j-\text{te Spalte}$$

Folgerung 4.4.3 : Ist K ein Körper, so ist

$$M(m \times n, K) = \mathcal{F}(\underline{m} \times \underline{n}, K)$$

mit der in $(*)$ definierten Adition und äußeren Operation nach Beispiel 4.1.4 ein $K-$Vektorraum, und da für jedes $A = (a_{kj})) \in M(m \times n, K)$

$$A = \sum_{k=1}^{m} \sum_{j=1}^{n} a_{kj}\, E_{kj}$$

gilt, mit eindeutig bestimmten Koeffizienten a_{kj}, ist

$$(E_{kj})_{(k,j) \in \underline{m} \times \underline{n}}$$

eine Basis von $M(m \times n, K)$, und damit

$$\dim_K M(m \times n, K) = m \cdot n \quad .$$

□

Definition 4.4.4 : Seien $m, n, r \in \mathbb{N}$, R ein kommutativer Ring. Dann definiert man das **Produkt der Matrizen**

$$A = (a_{kj}) \in M(m \times n, R) \quad , \quad B = (b_{jl}) \in M(n \times r, R) \quad \text{als}$$

$$A \cdot B := (c_{kl}) \in M(m \times r, R) \quad \text{mit} \quad c_{kl} := \sum_{j=1}^{n} a_{kj} b_{jl} \quad .$$

(4.4.5) Bemerkungen : 1) Man kann also nicht beliebige Matrizen multiplizieren, $A \cdot B$ ist nur definiert, wenn

$$A \in M(m \times \underline{n}, R) \quad , \quad B \in M(\underline{n} \times r, R)$$

ist, d.h. wenn die Spaltenzahl der ersten gleich der Zeilenzahl der zweiten Matrix ist.
2) Man merkt sich die Definition des Matrizenprodukts

$$A \cdot B = \left(\sum_{j=1}^{n} a_{kj} b_{jl} \right)_{(k,l) \in \underline{m} \times \underline{r}} = (c_{kl})$$

am besten so: Um c_{kl} auszurechnen, bildet man das "Skalarprodukt" des $k-$ten Zeilenvektors von A mit dem $l-$ten Spaltenvektor von B.

Satz 4.4.6 : Seien $m, n, r, t \in \mathbb{N}$, R ein kommutativer Ring und

$$A \in M(m \times n, K) \quad , \quad B \in M(n \times r, K) \quad , \quad C \in M(r \times t, K) \quad ,$$

dann gilt $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.
Beweis : Sei $A = (a_{kj})$, $B = (b_{jl})$, $C = (c_{ls})$ mit
$k \in \underline{m}, j \in \underline{n}, l \in \underline{r}, s \in \underline{t}$, dann gilt

$$A \cdot (B \cdot C) = \left(\sum_{j=1}^{n} a_{kj} \cdot \left(\sum_{l=1}^{r} b_{jl}\, c_{ls} \right) \right)_{(k,s) \in \underline{m} \times \underline{t}}$$

$$= \left(\sum_{l=1}^{r} \left(\sum_{j=1}^{n} a_{kj}\, b_{jl} \right) \cdot c_{ls} \right)_{(k,s) \in \underline{m} \times \underline{t}} = (A \cdot B) \cdot C \quad .$$

□

Das Matrizenprodukt ist also assoziativ. Kommutativ ist es nicht, auch wenn der Ring $(R, +, \cdot)$ kommutativ ist:

Bemerkungen 4.4.7 : Sei $(R, +, \cdot)$ ein kommutativer Ring.

(1) Wir rechnen das Produkt der in 4.4.2 definierten Elemente

$$E_{kj} \;=\; (\delta_{ku}\cdot\delta_{jv})_{(u,v)\in\underline{m}\times\underline{n}} \in M(m\times n,R) \quad \text{mit}$$

$$E_{st} \;=\; (\delta_{sv}\cdot\delta_{tw})_{(v,w)\in\underline{n}\times\underline{r}} \in M(n\times r,R)$$

für $m,n,r\in\mathbb{N}$ aus. Am besten geht das, indem man sich ein Blatt Papier nimmt, die Matrizen E_{kj} und E_{st} hinschreibt und dann gemäß (4.4.5) 2) multipliziert (und es ist wichtig, dass Sie einen Blick dafür entwickeln, wie man einfache Matrizenprodukte schnell ausrechnet). Aber wenn Sie es formal mit der Definition in 4.4.4 ausrechnen wollen:

$$E_{kj}\cdot E_{st} \;=\; (\delta_{ku}\cdot\delta_{jv})_{(u,v)\in\underline{m}\times\underline{n}}\cdot(\delta_{sv}\cdot\delta_{tw})_{(v,w)\in\underline{n}\times\underline{r}}$$

$$= \left(\sum_{v=1}^{n}\delta_{ku}\cdot\delta_{jv}\cdot\delta_{sv}\cdot\delta_{tw}\right)_{(u,w)\in\underline{m}\times\underline{r}} ,$$

und da $\delta_{jv}\delta_{sv}$ nur für $v=j=s$ gleich 1 und sonst 0 ist:

$$E_{kj}\cdot E_{st} \;=\; (\delta_{ku}\cdot\delta_{js}\cdot\delta_{sw})_{(u,w)\in\underline{m}\times\underline{r}} \;=\; \delta_{js}\;(\delta_{ku}\cdot\delta_{sw})_{(u,w)\in\underline{m}\times\underline{r}}\,, \text{ also}$$

$$(**)\qquad E_{kj}\cdot E_{st} \;=\; \delta_{js}E_{kt} \quad \text{für} \quad k\in\underline{m}, j,s\in\underline{n}, t\in\underline{r} \quad .$$

Wir werden diese Formel noch brauchen, z.B. für

(2) Wir sehen uns quadratische Matrizen an, also $M(n\times n,R)$, und behaupten, dass die Multiplikation in $M(n\times n,R)$ für $n\geq 2$ nicht kommutativ ist. Für ein Gegenbeispiel setzen wir

$$C \;:=\; \sum_{k=3}^{n} E_{kk} \quad , \quad A \;:=\; E_{11}+E_{12}+E_{21}+C \quad , \quad B \;:=\; E_{12}+E_{21}+C \;,$$

dann folgt nach $(**)$ in (1) :

$$A\cdot B \;=\; (E_{11}+E_{12}+E_{21}+C)\cdot(E_{12}+E_{21}+C) \;=\; E_{11}+E_{12}+E_{22}+C \quad ,$$

$$B\cdot A \;=\; (E_{12}+E_{21}+C)\cdot(E_{11}+E_{12}+E_{21}+C) \;=\; E_{11}+E_{21}+E_{22}+C \quad ,$$

Sei $(d_{kj}) := A\cdot B$ und $(f_{kj}) := B\cdot A$, dann gilt also

$$d_{21} \;=\; 0\,, \text{ aber} \quad f_{21} \;=\; 1\,, \quad \text{also} \quad A\cdot B\neq B\cdot A \quad .$$

Übrigens: Zu A und B gibt es Metrizen A^{-1} und B^{-1} mit

$$A\cdot A^{-1} \;=\; A^{-1}\cdot A \;=\; E_n \quad \text{und} \quad B\cdot B^{-1} \;=\; B^{-1}\cdot B \;=\; E_n\,, \text{ nämlich}$$

$$A^{-1} := E_{12} + E_{21} - E_{22} + C \quad \text{und} \quad B^{-1} := B \quad .$$

Wir brauchen das in 4.4.9 .

Satz 4.4.8 : Sei $n \in \mathbb{N}, R$ ein kommutativer Ring. Dann ist die Menge $M(n \times n, R)$ mit der in Definition 4.4.2 definierten Addition $+$ und der in 4.4.4 definierten Multiplikation $\cdot$ ein Ring, mit dem Einselement

$$E_n \quad := \quad \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \quad = \quad (\delta_{kj}) \quad \text{mit} \quad \delta_{kj} = \begin{cases} 1 & \text{für } k = j \\ 0 & \text{für } k \neq j \end{cases} \quad .$$

E_n heißt die **Einsmatrix** in $M(n \times n, R)$. Für $n \geq 2$ ist dieser Ring weder kommutativ noch nullteilerfrei.

Beweis : Für $A, B \in M(n \times n, R)$ sind $A + B$, $A \cdot B \in M(n \times n, R)$ nach 4.4.2 bzw.4.4.4. $+$ und $\cdot$ sind also Verknüpfungen in $M(n \times n, R)$.
(R1) Dass $(M(n \times n, R), +)$ eine abelsche Gruppe ist, rechnet man leicht nach. Das Nullelement ist die Nullmatrix

$$0 := \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \quad ,$$

das Negative von (a_{kj}) ist $(-a_{kj})$.
(R2) Das Assoziativgesetz für $\cdot$ haben wir gerade als Satz 4.4.6 bewiesen.
(R3) Seien $(a_{kj}), (b_{kj}), (c_{kj}) \in M(n \times n, R)$, dann gilt

$$\begin{aligned} (((a_{kj}) + (b_{kj})) \cdot (c_{kj}) \quad &= \quad (a_{kj} + b_{kj}) \cdot (c_{kj}) \\ = \quad \left(\sum_{l=1}^{n} (a_{kl} + b_{kl}) \cdot c_{lj} \right) \quad &= \quad \left(\sum_{l=1}^{n} a_{kl} \cdot c_{lj} + \sum_{l=1}^{n} b_{kl} \cdot c_{lj} \right) \\ = \quad \left(\sum_{l=1}^{n} a_{kl} \cdot c_{lj} \right) + \left(\sum_{l=1}^{n} b_{kl} \cdot c_{lj} \right) \quad &= \quad (a_{kj}) \cdot (c_{kj}) + (b_{kj}) \cdot (c_{kj}) \,, \end{aligned}$$

entsprechend die zweite Gleichung des Distributivgesetzes.
(R4) Sei $A = (a_{kj}) \in M(n \times n, R)$, dann gilt

$$A \cdot E_n \quad = \quad \left(\sum_{l=1}^{n} a_{kl} \delta_{lj} \right) \quad .$$

In dieser Summe ist höchstens der Summand mit $l = j$ ungleich 0, also

$$A \cdot E_n \quad = \quad (a_{kj} \cdot 1) \quad = \quad A \quad .$$

entsprechend $E_n \cdot A = A$. E_n ist also das Einselement des Ringes $M(n \times n, R)$. Kommutativ ist $(M(n \times n, R), +, \cdot)$ nicht, das folgt aus Bemerkung (2) in (4.4.7). Es gilt

$$E_{12} \cdot E_{11} = 0 \quad ,$$

also ist $(M(n \times n, R), +, \cdot)$ nicht nullteilerfrei .

□

Bemerkung: $M(n \times n, R)$ ist mit $\cdot$ keine Gruppe, weil $(M(n \times n, R), +, \cdot)$ nicht nullteilerfrei ist. Aber man kann die Einheitengruppe $M(n \times n, R)^\times$ betrachten. Man nennt sie $\mathrm{GL}(n, R)$. Dass für einen beliebigen Ring $(S, +, \cdot)$, mit Einselement 1, die Menge

$$S^\times = \{ \ a \in R \mid \exists\, a^* \in R : a^* \cdot a = a \cdot a^* = 1 \ \}$$

eine Gruppe ist, hatten wir schon in 3.2.11 bewiesen. Dass $\mathrm{GL}(n, R)$ nicht kommutativ ist, folgt aus dem Gegenbeispiel in (4.4.7) 2) :

Satz und Definition 4.4.9 : Sei $n \in \mathbb{N}$, R ein kommutativer Ring und

$$\begin{aligned} \mathrm{GL}(n, R) \quad &:= \quad \{ A \in M(n \times n, R) \mid \\ &\quad\ \exists\, A^{-1} \in M(n \times n, R) : A^{-1} \cdot A = A \cdot A^{-1} = E_n \} \quad , \end{aligned}$$

dann ist $(\mathrm{GL}(n, R), \cdot)$ eine, für $n \geq 2$ nicht kommutative, Gruppe. Sie heißt die **allgemeine lineare Gruppe** vom Grad n über R .

□

Nun kommen wir zum Thema: Matrizen linearer Abbildungen von $K-$Vektorräumen. Dabei sei also stets K ein Körper.

Satz 4.4.10 : Sei V ein endlichdimensionaler $K-$Vektorraum,

$(v_1, \ldots, v_n)$ eine Basis von V ,

und seien $b_1, \ldots, b_n$ beliebige Vektoren aus einem $K-$Vektorraum W. Dann gibt es genau eine lineare Abbildung

$F : V \longrightarrow W$ mit $F(v_j) = b_j$ für alle $j \in \underline{n}$,

d.h. man kann eine lineare Abbildung dadurch definieren, dass man die Funktionswerte von Basiselementen festlegt.

Beweis : (1) Es gibt höchstens eine lineare Abbildung

$F : V \longrightarrow W$ mit $F(v_j) = b_j$ für alle $j \in \underline{n}$,

denn man kann jedes $v \in V$ eindeutig als Linearkombination

$$v \quad = \quad \sum_{j=1}^{n} \alpha_j \, v_j \quad \text{mit} \quad (\alpha_1, \ldots, \alpha_n) \in K^n$$

schreiben, und aus der Linearität von F folgt dann

$$(*) \quad F(v) = F\left(\sum_{j=1}^{n} \alpha_j v_j\right) = \sum_{j=1}^{n} \alpha_j F(v_j) = \sum_{j=1}^{n} \alpha_j b_j \quad .$$

Wir wissen also, wie $F(v)$ zu berechnen ist, wenn überhaupt so ein $F \in \mathrm{Hom}_K(V,W)$ existiert.
(2) Um die Existenz eines $F \in \mathrm{Hom}_K(V,W)$ mit $\forall j \in \underline{n} : F(v_j) = b_j$ zu zeigen, definieren wir F durch $(*)$:

$$F(v) \quad := \quad \sum_{j=1}^{n} \alpha_j b_j \quad \text{für} \quad v = \sum_{j=1}^{n} \alpha_j v_j \quad .$$

Da die α_j durch v eindeutig bestimmt sind, ist F auf diese Weise eindeutig festgelegt, also eine Abbildung. F ist linear, denn für
$v = \sum\limits_{j=1}^{n} \alpha_j v_j$, $v' = \sum\limits_{j=1}^{n} \beta_j v_j$, $\lambda \in K$ gilt

$$F(v+v') = F\left(\sum_{j=1}^{n} (\alpha_j + \beta_j) v_j\right) = \sum_{j=1}^{n} (\alpha_j + \beta_j) b_j = F(v) + F(v') \quad \text{und}$$

$$F(\lambda v) = F\left(\sum_{j=1}^{n} (\lambda \alpha_j) v_j\right) = \sum_{j=1}^{n} (\lambda \alpha_j) b_j = \lambda F(v) \quad .$$

Es gilt $\forall\, k \in \underline{n} : F(v_k) = b_k$, denn

$$v_k = \sum_{j=1}^{n} \delta_{jk} v_j \quad \text{mit} \quad \delta_{jk} = \begin{cases} 1 & \text{für } j = k \\ 0 & \text{für } j \neq k \end{cases} \quad , \text{ also}$$

$$F(v_k) = \sum_{j=1}^{n} \delta_{jk} b_j = b_k \quad . \qquad \square$$

Bemerkung : In Satz 4.4.10 ist $(v_j)_{j \in \underline{n}}$ eine Basis von V , aber $(b_j)_{j \in \underline{n}}$ i.A. keine Basis von W . Man kann aber die b_j als Linearkombinationen einer Basis von W schreiben, dann erhält man

(4.4.11) Die zu einer linearen Abbildung gehörige Matrix :

Seien V und W endlichdimensionale $K-$Vektorraume und sei
$F : V \longrightarrow W$ $K-$linear.
Gegeben seien feste Basen
$(v_1, \ldots, v_n)$ von V und $(w_1, \ldots, w_m)$ von W , mit $n, m \in \mathbb{N}$.
Dann hat man für alle $j \in \underline{n}$
$b_j := F(v_j)$,
die Vektoren b_j sind durch F eindeutig bestimmt, und umgekehrt ist nach

Satz 4.4.10 auch F durch $(F(v_1), \ldots, F(v_n))$ eindeutig festgelegt. Da $(w_1, \ldots, w_m)$ eine Basis von W ist, kann man die b_j eindeutig als Linearkombinationen von $(w_1, \ldots, w_m)$ schreiben :

$$\begin{array}{lcl} b_1 & = & a_{11}w_1 + \ldots + a_{m1}w_m \\ \vdots & & \vdots \\ b_n & = & a_{1n}w_1 + \ldots + a_{mn}w_m \end{array}$$

mit gewissen $m-$tupeln $(a_{1j}, \ldots, a_{mj}) \in K^m$, die natürlich von j abhängen. Kurz als Formel, die man sich **unbedingt** merken muss :

$$(4.4.12) \qquad \forall\, j \in \underline{n}\ \exists_1 \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^m \,:\, F(v_j) \,=\, \sum_{k=1}^{m} a_{kj}\, w_k$$

Auf diese Weise kann man bei gegebenem F **und festgelegten Basen** $(v_1, \ldots, v_n)$ von V und $(w_1, \ldots, w_m)$ von W die Elemente

a_{kj} für $j \in \underline{n}$ und $k \in \underline{m}$

berechnen, die zusammen eine Matrix $(a_{kj}) \in M(m \times n, K)$ bilden :

Definition und Satz 4.4.13 : Seien V und W $K-$Vektorräume, K ein Körper,

$\mathfrak{A} := (v_1, \ldots, v_n)$ sei Basis von V und

$\mathfrak{B} := (w_1, \ldots, w_m)$ sei Basis von W, mit $n, m \in \mathbb{N}$.

Sei

$$M_{\mathfrak{B}}^{\mathfrak{A}} \,:\, \mathrm{Hom}_K(V, W) \longrightarrow M(m \times n, K) \quad ,$$

$$M_{\mathfrak{B}}^{\mathfrak{A}}(F) \;:=\; (a_{kj}) \quad , \quad \text{wobei} \quad a_{kj} \quad \text{durch}$$

$$F(v_j) \;=\; \sum_{k=1}^{m} a_{kj}\, w_k \quad \text{für} \quad j \in \underline{n}$$

definiert ist, dann ist $M_{\mathfrak{B}}^{\mathfrak{A}}$ ein $K-$Vektorraum-Isomorphismus.

Beweis : (1) Nach (4.4.11) ist $M_{\mathfrak{B}}^{\mathfrak{A}}$ eine Abbildung.

(2) Seien $F, G \in \mathrm{Hom}_K(V, W)$ und $\lambda \in K$, dann gilt für $j \in \underline{n}$:

$$(F + G)(v_j) \,=\, F(v_j) + G(v_j) \,=\, \sum_{k=1}^{m} a_{kj}w_k + \sum_{k=1}^{m} b_{kj}w_k \quad ,$$

wenn $M_{\mathfrak{B}}^{\mathfrak{A}}(G) \,=\, (b_{kj})$ ist, also

$$(F + G)(v_j) \;=\; \sum_{k=1}^{m} (a_{kj} + b_{kj})w_k \quad ,$$

nach Formel (4.4.12) also

$$M_{\mathfrak{B}}^{\mathfrak{A}}(F+G) \;=\; (a_{kj}+b_{kj}) \overset{4.4.2}{=} (a_{kj})+(b_{kj}) \;=\; M_{\mathfrak{B}}^{\mathfrak{A}}(F) + M_{\mathfrak{B}}^{\mathfrak{A}}(G)\,,$$

ähnlich:

$$(\lambda F)(v_j) \;=\; \lambda\, F(v_j) \;=\; \lambda \sum_{k=1}^{m} a_{kj} w_k \quad = \quad \sum_{k=1}^{m} (\lambda a_{kj}) w_k \quad ,$$

also nach Formel (4.4.12) :

$$M_{\mathfrak{B}}^{\mathfrak{A}}(\lambda F) \;=\; (\lambda\, a_{kj}) \overset{4.4.5}{=} \lambda\,(a_{kj}) \;=\; \lambda\; M_{\mathfrak{B}}^{\mathfrak{A}}(F) \quad .$$

$M_{\mathfrak{B}}^{\mathfrak{A}}$ ist also $K-$linear.
(3) $M_{\mathfrak{B}}^{\mathfrak{A}}$ ist injektiv, denn sei $F \in \ker\, M_{\mathfrak{B}}^{\mathfrak{A}}$, also $M_{\mathfrak{B}}^{\mathfrak{A}}(F) = 0$ das Nullelement von $M(m \times n, K)$ also

$$M_{\mathfrak{B}}^{\mathfrak{A}}(F) \quad = \quad \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \quad \text{die Nullmatrix ,}$$

dann gilt nach Formel (4.4.12) :

$$\forall\, j \in \underline{n} : \;\; F(v_j) \;=\; \sum_{k=1}^{m} 0\, w_k \;=\; 0 \in W \quad ,$$

also ist F die Nullabbildung , $F \;=\; 0 \in \mathrm{Hom}_K(V,W)$. Nach Bemerkung 4.3.4 ist $M_{\mathfrak{B}}^{\mathfrak{A}}$ injektiv.
(4) $M_{\mathfrak{B}}^{\mathfrak{A}}$ ist surjektiv, denn sei $(a_{kj}) \in M(m \times n, K)$, dann ist durch

$$F \;:\; V \;\longrightarrow\; W \quad , \quad F(v_j) := \sum_{k=1}^{m} a_{kj}\, w_k$$

nach Satz 4.4.10 genau eine lineare Abbildung $F \in \mathrm{Hom}_K(V,W)$ definiert. Für dieses F gilt dann nach (4.4.12) wieder

$$M_{\mathfrak{B}}^{\mathfrak{A}}(F) \quad = \quad (a_{kj}) \quad .$$

Insgesamt : $M_{\mathfrak{B}}^{\mathfrak{A}}$ ist ein Vektorraum-Isomorphismus. □

Bemerkung 4.4.14 : In Satz 4.3.8 haben wir gesehen: Sind U, V, W $K-$ Vektorräume, und

$G : U \longrightarrow V$, $F : V \longrightarrow W$ $K-$linear ,
dann ist auch $F \circ G : U \longrightarrow W$ $K-$linear .

Sind nun U, V, W endlichdimensional, mit Basen

$\mathfrak{A} = (u_1, \ldots, u_r)$ von U ,
$\mathfrak{B} = (v_1, \ldots, v_n)$ von V ,
$\mathfrak{C} = (w_1, \ldots, w_m)$ von W ,

dann hat man Matrizen

$$A := M_{\mathfrak{C}}^{\mathfrak{B}}(F) = (a_{kj}) \in M(m \times n, K)\,,\ B := M_{\mathfrak{B}}^{\mathfrak{A}}(G) = (b_{jl}) \in M(n \times r, K)\,,$$

die gemäß Formel (4.4.12) definiert sind durch

$$F(v_j) = \sum_{k=1}^{m} a_{kj}\, w_k \quad \text{für} \quad j \in \underline{n} \quad ,$$

$$G(u_l) = \sum_{j=1}^{n} b_{jl}\, v_j \quad \text{für} \quad l \in \underline{r} \quad .$$

Aus diesen Gleichungen erhält man für $l \in \underline{r}$:

$$(F \circ G)(u_l) = F(G(u_l)) = \sum_{j=1}^{n} b_{jl} F(v_j)$$

$$= \sum_{j=1}^{n} b_{jl} \sum_{k=1}^{m} a_{kj} w_k = \sum_{k=1}^{m} \left(\sum_{j=1}^{n} a_{kj} b_{jl} \right) w_k \quad ,$$

also gilt für die − nach 4.4.13 eindeutig bestimmte − Matrix

$$C := (c_{kl}) = M_{\mathfrak{C}}^{\mathfrak{A}}(F \circ G) \in M(m \times r, K) \quad \text{mit}$$

$$(F \circ G)(u_l) = \sum_{k=1}^{m} c_{kl} w_k \ :$$

$$c_{kl} = \sum_{j=1}^{n} a_{kj} b_{jl} \quad \text{für} \quad k \in \underline{m} \quad , \quad l \in \underline{r} \quad .$$

C ist daher das Produkt der Matrizen

$$A = (a_{kj}) \in M(m \times n, K) \quad , \quad B = (b_{jl}) \in M(n \times r, K) \quad , \quad \text{also}$$

$$C = A \cdot B := (c_{kl}) \quad \text{mit} \quad c_{kl} := \sum_{j=1}^{n} a_{kj} b_{jl} \quad ,$$

es gilt also die Formel

$$\boxed{(4.4.15) \qquad M_{\mathfrak{C}}^{\mathfrak{A}}(F \circ G) \quad = \quad M_{\mathfrak{C}}^{\mathfrak{B}}(F) \cdot M_{\mathfrak{B}}^{\mathfrak{A}}(G) \quad ,}$$

d.h. bezüglich festgelegter Basen ist die Matrix der Hintereinanderausführung $F \circ G$ gleich dem Produkt der Matrizen von F und von G .

Bemerkung 4.4.16 : Seien V und W $K-$Vektorräume,

$$F : V \longrightarrow W \quad K-\text{linear},$$

$$\dim_k V = n \quad , \quad \dim_k W = m \quad ,$$

dann hatten wir in 4.4.11 die Matrix von F bezüglich gegebener Basen

$$\mathfrak{A} = (a_1, \ldots, a_n) \text{ von } V \quad , \quad \mathfrak{B} = (b_1, \ldots, b_m) \text{ von } W$$

definiert, also $A := M_{\mathfrak{B}}^{\mathfrak{A}}(F) \in M(m \times n, K)$, und zwar durch Formel (4.4.12) . Wählt man nun andere Basen von V bzw. W, so haben sie die gleiche Länge. Sei also auch

$$\mathfrak{A}' = (a'_1, \ldots, a'_n) \text{ eine Basis von } V \text{ und}$$

$$\mathfrak{B}' = (b'_1, \ldots, b'_m) \text{ eine Basis von } W,$$

so hat man $A' := M_{\mathfrak{B}'}^{\mathfrak{A}'}(F) \in M(m \times n, K)$. Wie kann man A' aus A berechnen ? Das geht ganz einfach (und ohne dass man viele Indizes hinschreiben muss) so: Sicher ist

$$F \quad = \quad \mathrm{id}_W \circ F \circ \mathrm{id}_V \quad ,$$

aber wir nehmen jetzt folgende Basen :

$$\begin{array}{ccccccc} V & \xrightarrow{\mathrm{id}_V} & V & \xrightarrow{F} & W & \xrightarrow{\mathrm{id}_W} & W \\ | & & | & & | & & | \\ \text{mit Basis } \mathfrak{A}' & & \text{mit Basis } \mathfrak{A} & & \text{mit Basis } \mathfrak{B} & & \text{mit Basis } \mathfrak{B}' \end{array} \quad ,$$

dann gilt nach Formel (4.4.15) :

$$(***) \quad M_{\mathfrak{B}'}^{\mathfrak{A}'}(F) \quad = \quad M_{\mathfrak{B}'}^{\mathfrak{A}'}(\mathrm{id}_W \circ F \circ \mathrm{id}_V) \quad = \quad M_{\mathfrak{B}'}^{\mathfrak{A}'}(\mathrm{id}_W \circ (F \circ \mathrm{id}_V))$$

$$= \quad M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}_W) \cdot M_{\mathfrak{B}}^{\mathfrak{A}'}(F \circ \mathrm{id}_V) \quad = \quad M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}_W) \cdot M_{\mathfrak{B}}^{\mathfrak{A}}(F) \cdot M_{\mathfrak{A}}^{\mathfrak{A}'}(\mathrm{id}_V) \quad .$$

Wir setzen $S := M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}_W)$, dann ist $S \in M(m \times m, K)$, und wegen

$$M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}_W) \cdot M_{\mathfrak{B}}^{\mathfrak{B}'}(\mathrm{id}_W) \overset{4.4.15}{=} M_{\mathfrak{B}'}^{\mathfrak{B}'}(\mathrm{id}_W) \overset{4.4.12}{=} E_m \quad ,$$

$$M_{\mathfrak{B}}^{\mathfrak{B}'}(\mathrm{id}_W) \cdot M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}_W) \overset{4.4.15}{=} M_{\mathfrak{B}}^{\mathfrak{B}}(\mathrm{id}_W) \overset{4.4.12}{=} E_m$$

ist sogar $S \in \mathrm{GL}(m, K)$, $S^{-1} = M_{\mathfrak{B}}^{\mathfrak{B}'}(\mathrm{id}_W)$. Ebenso gilt für $T := M_{\mathfrak{A}'}^{\mathfrak{A}}(\mathrm{id}_V)$: $T \in \mathrm{GL}(n, K)$ und $T^{-1} = M_{\mathfrak{A}}^{\mathfrak{A}'}(\mathrm{id}_V)$. Setzen wir das in $(*)$ ein, so erhalten

wir

(4.4.17)

$$A' \quad = \quad S \cdot A \cdot T^{-1} \qquad \text{für}$$

$$A \;=\; M^{\mathfrak{A}}_{\mathfrak{B}}(F) \quad , \quad A' \;=\; M^{\mathfrak{A}'}_{\mathfrak{B}'}(F)$$

mit den **Transformationsmatrizen**

$$T \;:=\; M^{\mathfrak{A}}_{\mathfrak{A}'}(\,\mathrm{id}_V) \quad , \quad S \;:=\; M^{\mathfrak{B}}_{\mathfrak{B}'}(\,\mathrm{id}_W)$$

Dabei haben wir (4.4.11) benutzt, um $M^{\mathfrak{B}}_{\mathfrak{B}}(\,\mathrm{id}_W) \;=\; E_m$ zu zeigen: Es gilt

$$\forall\, r \in \underline{m} : \quad \mathrm{id}_W(b_r) \;=\; b_r \;=\; \sum_{l=1}^{r} \delta_{lr} b_l \quad \text{und} \quad (\delta_{lr}) \;=\; E_m \quad .$$

Man braucht die Formel (4.4.11) auch, wenn man S und T konkret ausrechnen will: $T \;=\; (t_{kj}) \;\in\; M(n \times n, K)$ ist nach Formel (4.4.11) definiert durch

$$\forall\, j \in \underline{n} : \quad \mathrm{id}_V(a_j) \;=\; \sum_{k=1}^{n} t_{kj}\, a'_k \quad , \qquad \text{also}$$

$$\forall\, j \in \underline{n} : \quad a_j \quad = \quad \sum_{k=1}^{n} t_{kj}\, a'_k \quad ,$$

d.h. man erhält die Einträge t_{kj} der Transformationsmatrix T, indem man die Basisvektoren von $\mathfrak{A}$ als Linearkombinationen der Basisvektoren von $\mathfrak{A}'$ darstellt. Entsprechend ist

$$S \;=\; (s_{lr}) \;\in\; \mathrm{GL}(m, K) \quad \text{gegeben durch}$$

$$\forall\, r \in \underline{m} : \quad b_r \;=\; \sum_{l=1}^{r} s_{lr}\, b'_l \quad . \qquad \square$$

Wir brauchen die Transformationsformel (4.4.17) schon im nächsten Abschnitt. Den wiederum brauchen wir zur Lösung linearer Gleichungssysteme:

4.5 Der Rang einer Matrix

Definition 4.5.1 : Seien $m, n \in \mathbb{N}$, K ein Körper,

$$A \quad = \quad (a_{kj})_{(k,j)\in \underline{m}\times\underline{n}} \;\in\; M(m \times n, K) \quad ,$$

dann definieren wir die **transponierte Matrix** ${}^tA \in M(n \times m, K)$ als

$${}^tA \quad := \quad (b_{jk})_{(j,k)\in \underline{n}\times\underline{m}} \quad \text{mit} \quad b_{jk} \;:=\; a_{kj} \quad .$$

Rechenregeln 4.5.2 : Seien $n, m, r \in \mathbb{N}$, K ein Körper,

$$A, C \in M(m \times n, K) \quad , \quad B \in M(n \times r, K) \quad , \quad \lambda \in K \quad ,$$

dann gilt
(1) ${}^t(A + C) = {}^tA + {}^tC$, (2) ${}^t(\lambda A) = \lambda\, {}^tA$,
(3) ${}^t({}^tA) = A$, (4) ${}^t(A \cdot B) = {}^tB \cdot {}^tA$.
(5) Ist $m = n$ und $A \in \mathrm{GL}(n, K)$, so ist auch
${}^tA \in \mathrm{GL}(n, K)$, und es gilt $({}^tA)^{-1} = {}^t(A^{-1})$.
Beweis : (1) ,(2) und (3) sind leicht einzusehen.
(4) Es ist
${}^tA = (\alpha_{jk})_{(j,k)\in \underline{n}\times\underline{m}}$ mit $\alpha_{jk} := a_{kj}$,
${}^tB = (\beta_{lj})_{(l,j)\in \underline{r}\times\underline{n}}$ mit $\beta_{lj} := b_{jl}$
für $k \in \underline{m}$, $j \in \underline{n}$, $l \in \underline{r}$, also ist ${}^tB \cdot {}^tA \in M(r \times m, K)$ definiert,

$${}^tB \cdot {}^tA = \left(\sum_{j=1}^{n} \beta_{lj}\alpha_{jk} \right)_{(l,k)\in \underline{r}\times\underline{m}} =$$

$$\left(\sum_{j=1}^{n} b_{jl}a_{kj} \right)_{(l,k)\in \underline{r}\times\underline{m}} = \left(\sum_{j=1}^{n} a_{kj}b_{jl} \right)_{(l,k)\in \underline{r}\times\underline{m}} = {}^t(A \cdot B) \quad .$$

(5) Aus $A \cdot A^{-1} = A^{-1} \cdot A = E_n$ folgt nach (4) :

$${}^t(A^{-1}) \cdot {}^tA = {}^tA \cdot {}^t(A^{-1}) = {}^tE_n = E_n \quad ,$$

also ${}^tA \in \mathrm{GL}(n, K)$ und $({}^tA)^{-1} = {}^t(A^{-1})$.

Definition 4.5.3 : Seien $m, n \in \mathbb{N}$, K ein Körper,
$A = (a_{kj}) \in M(m \times n, K)$,
dann hatten wir in 4.4.1 die
$a_k = (a_{k1}, \ldots, a_{kn})$ für $k \in \underline{m}$ die Zeilenvektoren,
und die

$$a^j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^m \quad \text{für} \quad j \in \underline{n} \quad \text{die Spaltenvektoren von } A$$

genannt. Besser ist es übrigens, alle $n-$ und $m-$tupel als Spalten zu schreiben, dann sind also
${}^ta_1, \ldots, {}^ta_m \in K^n$ die Zeilenvektoren von A .
Wir nennen nun
$\mathrm{ZRg}(A) := \dim \mathrm{span}({}^ta_1, \ldots, {}^ta_m)$ den **Zeilenrang** von A und
$\mathrm{SRg}(A) := \dim \mathrm{span}(a^1, \ldots, a^n)$ den **Spaltenrang** von A .

Bemerkung 4.5.4 : Es ist

$$\text{span}({}^t a_1, \ldots, {}^t a_m) \subset K^n \quad ,$$
$$\text{span}(a^1, \ldots, a^n) \subset K^m \quad ,$$

wir haben also Untervektorräume verschiedener Vektorräume. Wir werden aber zeigen, dass sie gleiche Dimension haben, dass also

$$\text{ZRg}(A) \quad = \quad \text{SRg}(A) \quad \text{gilt.}$$

Dazu zunächst die

Schreibweise (4.5.5) : Seien $m, n \in \mathbb{N}$, K ein Körper und $A \in M(m \times n, K)$. Sei

$$f_A : \; K^n \; \longrightarrow \; K^m \quad , \quad f_A(x) \quad := \quad A \cdot x \quad ,$$

wobei unter $A \cdot x$ das Produkt der $m \times n-$Matrix A mit der $n \times 1-$Matrix $x \in K^n = M(n \times 1, K)$ verstanden wird, dann ist f_A eine lineare Abbildung.

Hilfssatz 4.5.6 : Sei K ein Körper, $n \in \mathbb{N}$, U ein Untervektorraum von K^n und $T \in \text{GL}(n, K)$. Dann gilt

$$\dim \, f_T(U) \quad = \quad \dim \, U \quad .$$

Beweis : Sei $F : \; U \; \longrightarrow \; f_T(U) \quad , \quad F(x) := f_T(x) \quad ,$
dann ist F linear, da f_T linear ist, und surjektiv, also

$$F(U) \quad = \quad f_T(U) \quad .$$

F ist auch injektiv, denn für $x, y \in U$ gilt

$$F(x) \, = \, F(y) \quad \Longrightarrow \quad f_T(x) \, = \, f_T(y) \quad \Longrightarrow \quad T \cdot x \, = \, T \cdot y \quad ,$$

und da $T^{-1} \in \text{GL}(n, K)$ existiert, folgt

$$T^{-1} \cdot (T \cdot x) \, = \, T^{-1} \cdot (T \cdot y) \, , \quad \text{also} \quad (T^{-1} \cdot T) \cdot x \, = \, (T^{-1} \cdot T) \cdot y \quad ,$$

also $x = y$. Nach Bemerkung 4.3.4 ist $\ker \, F = \{0\}$, und nach der Dimensionsformel (4.3.13) folgt

$$\dim U \, = \, \dim \, \ker \, F + \dim \, F(U) \, = \, 0 + \dim \, f_T(U) \quad . \qquad \square$$

Hilfssatz 4.5.7 : Sei $A \in M(m \times n, K)$, $S \in \text{GL}(m, K)$ und $T \in \text{GL}(n, K)$. Dann gilt

(1) $\text{SRg}(S \cdot A \cdot T) \quad = \quad \text{SRg}(A) \quad ,$
(2) $\text{ZRg}(S \cdot A \cdot T) \quad = \quad \text{ZRg}(A) \quad .$

Beweis : (1) a) Seien $a^1, \ldots, a^n$ die Spaltenvektoren von A und $e^1, \ldots, e^n$ die kanonischen Basisvektoren von K^n , als Spalten geschrieben, dann gilt

$$a^j \quad = \quad A \cdot e^j \quad \text{für} \quad j \in \underline{n} \quad ,$$

wie man mit scharfem Blick für die Matrizenmultiplikation sieht, also

$$\mathrm{SRg}(A) \quad = \quad \dim \mathrm{span}(f_A(e^1), \ldots, f_A(e^n)) \quad = \quad \dim f_A(K^n) \quad .$$

Nach Hilfssatz 4.5.6 ist

$$\dim f_T(K^n) \quad = \quad \dim K^n \quad = \quad n \quad ,$$

also wegen $f_T(K^n) \subset K^n$ nach Satz 4.2.24(2) :

$$f_T(K^n) \quad = \quad K^n \quad , \quad \text{also}$$

$$\mathrm{SRg}(A) \quad = \quad \dim f_A(f_T(K^n)) \quad = \quad \dim(f_A \circ f_T)(K^n)$$

$$= \quad \dim f_{A \cdot T}(K^n) \quad = \quad \mathrm{SRg}(A \cdot T) \quad .$$

b) Es ist

$$\mathrm{SRg}(S \cdot A) \quad = \quad \dim f_{S \cdot A}(K^n) \quad = \quad \dim f_S(f_A(K^n)) \quad ,$$

und Hilfssatz 4.5.6, angewendet auf den Untervektorraum $f_A(K^n)$ von K^m, ergibt

$$\dim f_S(f_A(K^n)) \quad = \quad \dim f_A(K^n) \quad , \quad \text{also}$$

$$\mathrm{SRg}(S \cdot A) \quad = \quad \dim f_A(K^n) \quad = \quad \mathrm{SRg}(A) \quad .$$

Insgesamt folgt aus b), angewendet auf $A \cdot T$ statt A, und aus a) :

$$\mathrm{SRg}(S \cdot A \cdot T) \quad = \quad \mathrm{SRg}(A \cdot T) \quad = \quad \mathrm{SRg}(A) \quad .$$

(2) Es ist

$$\mathrm{ZRg}(A) \quad = \quad \mathrm{SRg}({}^tA) \quad , \quad \text{und}$$

$${}^t(S \cdot A \cdot T) \quad = \quad {}^tT \cdot {}^t A \cdot {}^t S \quad \text{nach 4.5.2 (4)} \quad ,$$

und nach 4.5.2 (5) sind auch ${}^tT$ und ${}^tS$ invertierbar, also gilt nach (1) :

$$\mathrm{ZRg}(S \cdot A \cdot T) \quad = \quad \mathrm{SRg}({}^t(S \cdot A \cdot T)) \quad = \quad \mathrm{SRg}({}^tT \cdot {}^t A \cdot {}^t S)$$

$$\overset{(1)}{=} \quad \mathrm{SRg}({}^tA) \quad = \quad \mathrm{ZRg}(A) \quad . \qquad \square$$

Satz und Definition 4.5.8 : Seien $m, n \in \mathbb{N}$, K ein Körper und $A \in M(m \times n, K)$. Dann gilt

$$\mathrm{SRg}(A) \quad = \quad \mathrm{ZRg}(A) \quad ,$$

d. h. Zeilenrang und Spaltenrang von A sind gleich. Wir nennen diese Zahl den **Rang** von A , also

$$\mathrm{Rg}\, A \quad := \quad \mathrm{SRg}(A) \quad = \quad \mathrm{ZRg}(A) \quad .$$

Beweis : Sei

$\mathfrak{K} \quad := \quad (e^1, \ldots, e^n)$ die kanonische Basis von K^n und

$\mathfrak{L} \quad := \quad (f^1, \ldots, f^m)$ die kanonische Basis von K^m . Dann gilt

$$\forall\, j \in \underline{n} : \; f_A(e^j) \quad = \quad A \cdot e^j \quad = \quad a^j \quad = \quad \sum_{k=1}^{n} a_{kj} f^k \quad , \qquad \text{also}$$

$$M_{\mathfrak{L}}^{\mathfrak{K}}(f_A) \quad = \quad A \quad .$$

Nun haben wir in (4.3.13)(*) (bei der Dimensionsformel für lineare Abbildungen) bewiesen: Es gibt eine Basis

$\mathfrak{B} \quad := \quad (w_1, \ldots, w_r)$ von $f_A(K^n)$ und eine Basis

$\mathfrak{A} \quad := \quad (u_1, \ldots, u_r, v_1, \ldots, v_k)$ von K^n (also $r + k = n$), so dass

$f_A(u_j) = w_j$ für $j \in \underline{r}$ und $f_A(v_l) = 0$ für $l \in \underline{k}$

ist. Ergänzen wir $\mathfrak{B}$ zu einer Basis

$\mathfrak{C} \quad := \quad (w_1, \ldots, w_r, w_{r+1}, \ldots, w_m)$ von K^m , so wird nach (4.4.12):

$$B := M_{\mathfrak{C}}^{\mathfrak{A}}(f_A) =$$

$$\left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \\ \hline & 0 & & 0 \end{array}\right) \quad \begin{matrix} \\ \\ \\ \\ r \text{ Spalten} \end{matrix} \quad \begin{matrix} r \text{ Zeilen} \\ \\ \\ \\ \end{matrix} \quad = \left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right) \in M(m \times n, K) \quad .$$

Für die Matrix B gilt nun offensichtlich $\mathrm{SRg}(B) = \mathrm{ZRg}(B)$. Andererseits gilt nach der Formel für die Koordinatentransformation aus (4.4.17) :

$$M_{\mathfrak{L}}^{\mathfrak{K}}(f_A) \quad = \quad M_{\mathfrak{L}}^{\mathfrak{C}}(\mathrm{id}_{K^m}) \cdot M_{\mathfrak{C}}^{\mathfrak{A}}(f_A) \cdot M_{\mathfrak{A}}^{\mathfrak{K}}(\mathrm{id}_{K^n}) \quad ,$$

also mit $T := M_{\mathfrak{A}}^{\mathfrak{K}}(\mathrm{id}_{K^n}) \in \mathrm{GL}(n,K)$, $S := M_{\mathfrak{L}}^{\mathfrak{E}}(\mathrm{id}_{K^m}) \in \mathrm{GL}(m,K)$:

$$A \quad = \quad S \cdot B \cdot T \quad ,$$

und nach dem Hilfssatz 4.5.7 :

$$\mathrm{SRg}(A) \quad \overset{\downarrow}{=} \quad \mathrm{SRg}(B) \quad = \quad \mathrm{ZRg}(B) \quad \overset{\downarrow}{=} \quad \mathrm{ZRg}(A) \quad . \qquad \square$$

Wie kann man nun den Rang praktisch berechnen ? Es ist dazu nicht nötig, Basen von K^n bzw. K^m zu finden, so dass die Matrix von f_A bezüglich dieser Basen die Form

$$\begin{pmatrix} E_r & | & 0 \\ - & + & - \\ 0 & | & 0 \end{pmatrix} \quad \text{mit} \quad r = \mathrm{Rg}A$$

hat, es geht etwas einfacher. Man überlegt sich, dass gewisse Umformungen den Rang von A nicht ändern :

Definition 4.5.9 : Sei $A \in M(m \times n, K)$, mit Zeilenvektoren
$a_1, \ldots, a_m \in K^n$ (als Zeilen geschrieben).
Unter einer **elementaren Zeilenumformung** von A versteht man eine Umformung der folgenden Art:
(I) Multiplikation der $k-$ten Zeile mit $\lambda \in K \setminus \{0\}$: Aus

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_k \\ \vdots \\ a_m \end{pmatrix} \quad \text{wird} \quad A^I := \begin{pmatrix} a_1 \\ \vdots \\ \lambda a_k \\ \vdots \\ a_m \end{pmatrix} \quad .$$

(II) Addition der $j-$ten Zeile zur $k-$ten Zeile, $j \neq k$: Aus

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \\ a_m \end{pmatrix} \quad \text{wird} \quad A^{II} := \begin{pmatrix} a_1 \\ \vdots \\ a_k + a_j \\ \vdots \\ a_j \\ \vdots \\ a_m \end{pmatrix} \quad .$$

Durch Hintereinanderausführung mehrerer Umformungen
vom Typ (I) oder (II) erhält man noch folgende Umformungen:

(III) Addition des $\lambda-$fachen der $j-$ten Zeile zur $k-$ten Zeile, $k \neq j$, $\lambda \in K$: Aus

$$A = \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \quad \text{wird} \quad A^{III} := \begin{pmatrix} \vdots \\ a_k + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \quad ,$$

und zwar erhält man das folgendermaßen: Für $\lambda = 0$ macht man gar nichts. Für $\lambda \neq 0$ formt man so um :

$$\begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \xrightarrow{I} \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \xrightarrow{II} \begin{pmatrix} \vdots \\ a_k + \lambda a_j \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \xrightarrow{\text{I mit } \lambda^{-1}} \begin{pmatrix} \vdots \\ a_k + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

(IV) Vertauschen der $k-$ten Zeile mit der $j-$ten Zeile, $k \neq j$: Aus

$$A = \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \quad \text{wird} \quad A^{IV} := \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_k \\ \vdots \end{pmatrix} \quad ,$$

und zwar erhält man das folgendermaßen:

$$\begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \xrightarrow{I} \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ -a_j \\ \vdots \end{pmatrix} \xrightarrow{II} \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_k - a_j \\ \vdots \end{pmatrix}$$

$$\xrightarrow{III} \begin{pmatrix} \vdots \\ a_k - (a_k - a_j) \\ \vdots \\ a_k - a_j \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_k - a_j \\ \vdots \end{pmatrix} \xrightarrow{II} \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_k \\ \vdots \end{pmatrix} .$$

Entsprechend definiert man **elementare Spaltenumformungen** .

Hilfssatz 4.5.10 : Entsteht B aus A durch elementare Zeilen- bzw. Spaltenumformungen, so gilt

$$\mathrm{Rg}\, A \quad = \quad \mathrm{Rg}\, B \quad .$$

Beweis für Zeilenumformungen: Es reicht, den Satz für **eine** el. Umformung **vom Typ I oder II** zu beweisen. Durch Induktion nach der Anzahl solcher Umformungen folgt er dann auch für endlich viele Umformungen vom Typ I - IV :
I) Es ist $A^I = S_k(\lambda) \cdot A$ mit

$$S_k(\lambda) \quad := \quad \begin{pmatrix} 1 & & & 0 & & & \\ & \ddots & & \vdots & & 0 & \\ & & 1 & 0 & & & \\ 0 & \dots & 0 & \lambda & 0 & \dots & 0 \\ & & & 0 & 1 & & \\ & 0 & & \vdots & & \ddots & \\ & & & 0 & & & 1 \end{pmatrix} \longleftarrow k-\text{te Zeile} \quad ,$$

$$\uparrow$$

$k-$te Spalte,

$S_k(\lambda) \in M(m \times m, K)$, sogar $S_k(\lambda) \in \mathrm{GL}(m, K)$ wegen

$$S_k(\lambda) \cdot S_k(\lambda^{-1}) = S_k(\lambda^{-1}) \cdot S_k(\lambda) = E_m \quad .$$

Nach Hilfssatz 4.5.7 und Satz 4.5.8 folgt

$$\mathrm{Rg} A^I \quad = \quad \mathrm{Rg} A \quad .$$

II) Es ist $A^{II} = Q_k^j(1) \cdot A$ mit

$$Q_k^j(\lambda) \quad := \quad \begin{pmatrix} 1 & & & & & & & 0 & & & \\ & \ddots & & & & 0 & & \vdots & & 0 & \\ & & 1 & & & & & 0 & & & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 & \lambda & 0 & \dots & 0 \\ & & & & 1 & & & 0 & & & \\ & & & & & \ddots & & \vdots & & & \\ & & & & & & 1 & 0 & & & \\ & & & 0 & & & & 1 & & 0 & \\ & & & & & & & 0 & 1 & & \\ & & & & & & & \vdots & & \ddots & \\ & & & & & & & 0 & & & 1 \end{pmatrix} \longleftarrow k-\text{te Zeile} ,$$

$$\uparrow$$

$j-$te Spalte,

für $\lambda \in K$. Es ist

$$Q_k^j(\lambda) \in M(m \times m, K)\,, \text{ sogar } Q_k^j(\lambda) \in \mathrm{GL}(m, K) \quad ,$$

denn es existiert

$$Q_k^j(\lambda)^{-1} \quad = \quad Q_k^j(-\lambda) \quad .$$

Nach Hilfssatz 4.5.7 und Satz 4.5.8 folgt $\mathrm{Rg}A^{II} = \mathrm{Rg}A$.
Für Spaltenumformungen folgt die Behauptung daraus wegen

$$\mathrm{Rg}A \;=\; \mathrm{SRg}(A) \;=\; \mathrm{ZRg}({}^tA) \;=\; \mathrm{Rg}\,{}^tA \quad .$$

Definition und Satz 4.5.11 : Man sagt, eine Matrix $M \in M(m \times n, K)$ hat **Zeilenstufenform** , wenn es Zahlen $j_1, \ldots, j_r \in \underline{n}$ gibt mit

$$1 \leq j_1 < j_2 < \ldots < j_r \leq n \quad ,$$

so dass B die Form

$$\begin{pmatrix}
- & & & & & & & & & \\
 & | & b_{1j_1} & & & & & & & \\
 & |_ & - & - & & & & & & \\
 & & & & | & b_{2j_2} & & * & & \\
 & & & & |_ & - & - & & & \\
 & & & & & & & \ddots & & \\
 & & & 0 & & & & | & b_{rj_r} & \\
 & & & & & & & |_ & - & - \\
 & & & & & & & & &
\end{pmatrix}$$

hat, mit

$$b_{1j_1}\,, \ldots\,, b_{rj_r} \neq 0 \quad ,$$

Nullen unterhalb der "Stufenlinie" und irgendwelchen Einträgen oberhalb der b_{kj_k} . Es gilt dann

$$\mathrm{Rg}B \quad = \quad \mathrm{ZRg}(B) \quad = \quad r \quad .$$

Beweis : $(b_1, \ldots, b_r)$ ist eine Basis von

$$\mathrm{span}(b_1, \ldots, b_r, \ldots, b_m) \quad ,$$

denn $b_{r+1}, \ldots, b_m = 0$, und aus

$$\sum_{k=1}^{r} \beta_k\, b_k \quad = \quad 0$$

folgt zunächst, wenn man die j_1-te Komponente dieser Summe betrachtet :

$$\beta_1\, b_{1j_1} = 0 \quad , \quad \text{also wegen} \quad b_{1j_1} \neq 0 : \;\; \beta_1 = 0 \quad .$$

Mit der Gleichung $\sum_{k=2}^{r} \beta_k\, b_k = 0$ kann man so fortfahren und erhält

$0 = \beta_2 = \ldots = \beta_r \quad .$

Also ist $\mathrm{ZRg}(B) = r$. □

Bei einer Matrix in Zeilenstufenform kann man also den Rang leicht ablesen, es ist die "Anzahl der Stufen" dieser Matrix. Es gilt nun

Satz 4.5.12 : Jede Matrix $A \in M(m \times n, K)$ kann man durch endlich viele elementare Zeilenumformungen auf Zeilenstufenform bringen.

Beweis : Wir machen hier keinen exakten Induktionsbeweis, sondern geben die Schritte an, die man praktisch macht und auch so programmieren kann:

Ist $A = 0$, so sind wir fertig: A hat Zeilenstufenform, mit

0 Stufen.

$(*)$ Sei nun $A \neq 0$, so gibt es mindestens ein $a_{kj} \neq 0$. Die j_1-te Spalte sei diejenige mit dem kleinsten Index, in der nicht nur Nullen stehen, also

$a^1 = \ldots = a^{j_1-1} = 0 \quad , \quad$ und

$\exists\, k \in \underline{m} : \; a_{kj_1} \neq 0 \quad .$

Wenn nicht schon $a_{1j_1} \neq 0$ ist, vertauschen wir die 1. mit der $k-$ten Zeile (das ist eine Umformung vom Typ IV) und erhalten eine Matrix A' mit

$a'_{1j_1} \neq 0 \quad .$

In der Matrix A' addieren wir nun zur $k-$ten Zeile, $k = 2, \ldots, m$, jeweils das $-\dfrac{a'_{kj_1}}{a'_{1j_1}}-$fache der 1.Zeile, das sind $m-1$ Umformungen vom Typ III, und erhalten so eine Matrix A'' mit

$$a''_{kj_1} \quad = \quad a'_{kj_1} - \frac{a'_{kj_1}}{a'_{1j_1}} \cdot a'_{1j_1} \quad = \quad 0 \quad .$$

A'' hat also die Form

$$A'' \quad = \quad \begin{pmatrix} & & & \\ & a''_{1j_1} & & * \\ & & & \\ & 0 & & \\ & \vdots & & B_1 \\ & 0 & & \end{pmatrix} \quad .$$

Ist nun $B_1 = 0$ oder $j_1 = n$, so sind wir fertig, A'' hat Zeilenstufenform. Anderenfalls ist B_1 eine Matrix mit $m-1$ Zeilen, und wir fangen wieder bei $(*)$ an, mit B_1 statt A . Nach r solchen Schritten, $r \leq m \quad ,$ erhält

man eine Matrix der Form

$$B \;=\; \begin{pmatrix} - & & & & & & & & \\ & | & b_{1j_1} & & & & & & \\ & |\_ & - & - & & & & & \\ & & & & | & b_{2j_2} & & * & \\ & & & & |\_ & - & - & & \\ & & & & & & \ddots & & \\ & & & 0 & & & & | & b_{rj_r} \\ & & & & & & & |\_ & - \quad - \end{pmatrix} .$$

Bemerkung 4.5.13 : Unser Problem, den Rang einer Matrix zu bestimmen, ist damit gelöst: Man formt die Matrix durch elementare Zeilenumformungen so um, dass man auf eine Matrix in Zeilenstufenform kommt, die denselben Rang hat. Man kann zur Vereinfachung der Matrix auch elementare Spaltenumformungen verwenden; diese ändern den Rang auch nicht.

4.6 Lineare Gleichungssysteme

Definition 4.6.1 : Sei K ein Körper, $m, n \in \mathbb{N}$,

$$A = (a_{kj}) \in M(m \times n, K) \quad \text{und} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m$$

seien gegeben. Dann heißen die m Gleichungen

$$(1) \qquad \begin{cases} a_{11} & x_1 & + & \dots & + & a_{1n} & x_n & = & b_1 \\ \vdots & & & & & \vdots & & & \vdots \\ a_{m1} & x_1 & + & \dots & + & a_{mn} & x_n & = & b_m \end{cases} ,$$

wobei $x_1, \dots, x_n$ gesucht sind, ein **lineares Gleichungssystem** von m Gleichungen mit n **Unbekannten**. Fasst man den gesuchten Vektor

$$x \;=\; \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$$

als $n \times 1-$Matrix und b als $m \times 1-$Matrix auf, so kann man statt (1) kürzer schreiben:

(2) $\quad A \cdot x = b \quad .$

Das System (1) bzw. (2) heißt **homogen** , falls $b = 0$ ist, sonst **inhomogen**. Die Menge

$$\text{Lös}(A,b) \quad := \quad \{\ x \in K^n \mid A \cdot x = b\ \} \quad \subset \quad K^n$$

heißt die **Lösungsmenge** von (1) bzw.(2) . $A \cdot x = b$ heißt **lösbar** , wenn

$$\text{Lös}(A,b) \quad \neq \quad \emptyset \quad \text{ist.}$$

Bemerkung 4.6.2 : Zu $A \in M(m \times n, K)$ haben wir nach (4.5.5) die lineare Abbildung

$$f_A : \ K^n \ \longrightarrow \ K^m \quad , \quad f_A(x) := A \cdot x \quad .$$

Statt (2) kann man daher auch

(3) $\quad f_A(x) \quad = \quad b$

schreiben. Auf diese Weise können wir unsere Sätze über lineare Abbildungen auf lineare Gleichungssysteme anwenden.

Satz 4.6.3 : Das lineare Gleichungssystem $A \cdot x = b$ sei lösbar, und $a \in K^n$ sei eine Lösung. Dann ist die Lösungsmenge

$$\text{Lös}(A,b) \quad = \quad a + \ker f_A \quad := \quad \{\ a + y \mid y \in \ker f_A\ \} \quad ,$$

wobei $f_A(x) = A \cdot x$ ist. Man erhält also alle Lösungen von $A \cdot x = b$, indem man zu einer festen Lösung a alle Lösungen des "zugehörigen homogenen Systems" $A \cdot y = 0$ addiert.

Beweis : 1) Sei $x \in \text{Lös}(A,b)$, dann folgt wegen $a \in \text{Lös}(A,b)$:

$f_A(x) = b \quad$ und $\quad f_A(a) = b \quad , \quad$ also für $\quad y := x - a$:

$f_A(y) = f_A(x) - f_A(a) = 0 \quad , \quad y \in \ker f_A$, also

$x = a + y \quad$ mit $y \in \ker f_A \quad .$

2) Sei $x = a + y$ mit $y \in \ker f_A$, dann gilt

$f_A(x) = f_A(a) + f_A(y) = b + 0 = b$, $\quad$ also $\quad x \in \text{Lös}(A,b) \quad .$

Bemerkung 4.6.4 : Bei einem inhomogenen linearen Gleichungssystem

$f_A(x) = b \quad , \quad$ also mit $b \neq 0$,

ist $\text{Lös}(A,b)$ kein Untervektorraum von K^n , denn wegen

$f_A(0) = 0 \neq b \quad$ ist $\quad 0 \notin \text{Lös}(A,b) \quad .$

Bei einem homogenen linearen Gleichungssystem

$f_A(x) = 0$

ist $\text{Lös}(A,0) = \ker f_A$, also $\text{Lös}(A,0)$ ein Untervektorraum von K^n , also $0 \in \text{Lös}(A,0)$; das System hat also auf jeden Fall die **triviale Lösung**

$x = 0$, und es hat nichttriviale Lösungen, also Lösungen $\neq 0$, wenn

$\ker f_A \neq \{0\}$, also $\dim \ker f_A > 0$ ist.

Diese Dimension kann man mit der Dimensionsformel (4.3.13) berechnen:

Satz 4.6.5 : Sei $A \in M(m \times n, K)$, dann gilt für den Lösungsraum $\text{Lös}(A, 0)$ von $A \cdot x = 0$:

$$\boxed{\dim \text{Lös}(A,0) \quad = \quad n - \text{Rg}A \quad .}$$

Beachte: n ist die Anzahl der **Unbekannten** im System $A \cdot x = 0$.

Beweis : Es ist $\text{Lös}(A, 0) = \ker f_A$ für

$f_A : K^n \longrightarrow K^m \quad , \quad f_A(x) = A \cdot x \quad ,$

und nach der Dimensionsformel (4.3.13) gilt für f_A :

$\dim K^n \quad = \quad \dim \ker f_A + \dim f_A(K^n) \quad , \quad$ also

$n \quad = \quad \dim \text{Lös}(A, 0) + \dim f_A(K^n) \quad .$

Sei $(e^1, \ldots, e^n)$ die kanonische Basis des K^n , dann ist

$(f_A(e^1), \ldots, f_A(e^n))$

ein Erzeugendensystem von $f_A(K^n)$. Nun gilt für $j \in \underline{n}$:

$$f_A(e^j) \quad = \quad A \cdot e^j \quad = \quad \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \quad = \quad a^j \quad ,$$

wobei a^j der $j-$te Spaltenvektor von A ist. Also gilt

$\dim f_A(K^n) = \dim \text{span}(a^1, \ldots, a^n) = \text{SRg}(A) = \text{Rg}A \quad .$ $\qquad \square$

Damit wissen wir alles über homogene lineare Gleichungssysteme. Wann ist nun ein inhomogenes System $A \cdot x = b$ lösbar ?

Definition 4.6.6 : Sei $A \in M(m \times n, K)$ und $b \in K^m$. Dann heißt die Matrix

A die **einfache Matrix** des Systems $A \cdot x = b$

und die $m \times (n+1)-$Matrix, die entsteht, wenn man zu A den Vektor b als zusätzliche Spalte nimmt, also

$$(A, b) \quad := \quad \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix}$$

die **erweiterte Matrix** des Systems $A \cdot x = b$.

Satz 4.6.7 : Für die Lösungsmenge des linearen Gleichungssystems

$$A \cdot x \quad = \quad b \quad \text{mit} \quad A \in M(m \times n, K) \quad , \quad b \in K^m \quad \text{gilt :}$$

$$\boxed{\text{Lös}\,(A,b) \neq \emptyset \quad \Longleftrightarrow \quad \text{Rg}A \quad = \quad \text{Rg}\,(A,b) \quad ,}$$

wobei (A,b) die erweiterte Matrix des Systems ist.
Beweis : Sei

$$f_A : \; K^n \; \longrightarrow \; K^m \quad , \quad x \longmapsto A \cdot x \quad ,$$

dann gilt:

$$\text{Lös}\,(A,b) \neq \emptyset \quad \Longleftrightarrow \quad \exists\, x \in K^n : \; f_A(x) \quad = \quad b$$

$$\Longleftrightarrow \quad b \in f_A(K^n) \quad .$$

Wie wir beim Beweis von Satz 4.6.5 gesehen haben, ist

$$f_A(K^n) \quad = \quad \text{span}(a^1, \ldots, a^n) \quad ,$$

wobei $a^1, \ldots, a^n$ die Spaltenvektoren von A sind, also gilt

$$\text{Lös}\,(A,b) \neq \emptyset \quad \Longleftrightarrow \quad b \in \text{span}(a^1, \ldots, a^n)$$

$$\Longleftrightarrow \quad \text{span}(a^1, \ldots, a^n, b) \quad = \quad \text{span}(a^1, \ldots, a^n)$$

$$\overset{4.2.24\,(2)}{\Longleftrightarrow} \dim \text{span}(a^1, \ldots, a^n, b) \quad = \quad \dim \text{span}(a^1, \ldots, a^n)$$

$$\Longleftrightarrow \quad \text{Rg}\,(A,b) \quad = \quad \text{Rg}A \quad .$$

Man mache sich bei jedem Schritt klar, warum " $\Longleftrightarrow$ " gilt. □

Es kann durchaus sein, dass $A \cdot x = b$ mehrere Lösungen hat. Es gilt
Satz 4.6.8 : Für $A \in M(m \times n, K)$ und $b \in K^m$ sind folgende Aussagen gleichbedeutend:
(i) $A \cdot x = b$ ist eindeutig lösbar.
(ii) $\text{Rg}A \quad = \quad \text{Rg}\,(A,b) \quad = \quad n \quad .$
Beweis : (i) $\Longrightarrow$ (ii) : $A \cdot x = b$ sei eindeutig lösbar, dann ist $A \cdot x = b$ lösbar, und nach Satz 4.6.7 folgt

$$\text{Rg}A \quad = \quad \text{Rg}\,(A,b) \quad .$$

Für die Lösungsmenge von $A \cdot x = b$ gilt nach Satz 4.6.3 :

$$\text{Lös}\,(A,b) \quad = \quad a + \ker f_A \quad ,$$

wobei a eine feste Lösung ist. Da $A \cdot x = b$ eindeutig lösbar ist, ist $\ker f_A = \{0\}$, also $\dim \ker f_A = 0$, $\dim \text{Lös}(A,0) = 0$, also nach Satz 4.6.5 : $n - \text{Rg}A = 0$, also $n = \text{Rg}A$.

(ii) $\Longrightarrow$ (i) : Es gelte $\text{Rg}A = \text{Rg}\,(A,b) = n$. Wegen $\text{Rg}A = \text{Rg}\,(A,b)$ folgt nach Satz 4.6.7 : $A \cdot x = b$ ist lösbar, und nach Satz 4.6.3:

$$\text{Lös}\,(A,b) \quad = \quad a + \ker f_A \quad ,$$

wobei a eine Lösung ist, und nach Satz 4.6.5:

$$\dim \ker f_A \quad = \quad \dim \text{Lös}(A,0) \quad = \quad n - \text{Rg}A \quad = \quad 0 \quad , \quad \text{also}$$

$$\ker f_A = \{0\} \quad , \quad \text{Lös}\,(A,b) = \{a\} \quad .$$

□

- Wie kann man nun ein lineares Gleichungssystem $A \cdot x = b$ praktisch lösen? Man bringt dazu die erweiterte Matrix (A,b) durch elementare Zeilenumformungen auf Zeilenstufenform (B,c) und löst dann

$$B \cdot x = c \quad ,$$

was, wie wir sehen werden, ganz einfach ist. Zunächst

Hilfssatz 4.6.9 : Wird aus der $m \times (n+1)-$Matrix (A,b) durch endlich viele elementare **Zeilen**umformungen die Matrix (B,c) , so gilt

$$\text{Lös}\,(A,b) \quad = \quad \text{Lös}(B,c) \quad ,$$

d.h. an der Lösungsmenge ändert sich nichts.

Beweis : Beim Beweis von Hilfssatz 4.5.10 haben wir gesehen, dass man elementare Zeilemformungen einer Matrix A durch Multiplikation von links mit Matrizen aus $\text{GL}(m,K)$ erhält : Aus $A \in M(m \times n, K)$ wird

$$F_1 \cdot F_2 \cdot \ldots \cdot F_r \cdot A \text{ mit } r \in \mathbb{N}_0 \text{ und } F_1, \ldots, F_r \in \text{GL}(m,K) \quad .$$

Da $\text{GL}(m,K)$ eine Gruppe ist, ist auch

$$F \quad := \quad \prod_{j=1}^{r} F_j \in \text{GL}(m,K) \quad ,$$

und durch elementare Zeilenumformungen wird aus (A,b) also die Matrix $F \cdot (A,b)$. Nun gilt für $x \in K^n$:

$$A \cdot x = b \quad \Longleftrightarrow \quad F \cdot A \cdot x = F \cdot b \quad , \quad ,$$

wobei man für "$\Longleftarrow$" braucht, dass F invertierbar ist. Also ist

$$\text{Lös}\,(A,b) \quad = \quad \text{Lös}(F \cdot A, F \cdot b) \quad = \quad \text{Lös}(B,c) \quad . \qquad \square$$

Warnung : Für elementare **Spalten**umformungen an (A,b) gilt 4.6.9 nicht. Sie ändern zwar den Rang von (A,b) nicht, wohl aber die Lösungsmenge von $A \cdot x = b$. □

(4.6.10) Gaußsches Eliminationsverfahren : Gegeben sei ein lineares Gleichungssystem

$$A \cdot x = b \text{ mit } A \in M(m \times n, K)\,,\ b \in K^m \text{ gegeben,}$$
$$\text{und } x \in K^n \text{ gesucht.}$$

Dann schreibt man sich die erweiterte Koeffizientenmatrix (A, b) auf und bringt sie, wie in Satz 4.5.12 beschrieben, durch endlich viele elementare **Zeilen**umformungen auf Zeilenstufenform (B, c), und nach Hilfssatz 4.6.9 sind die Lösungen von

$$B \cdot x = c \text{ genau die Lösungen von } A \cdot x = b\,,$$

und es gilt nach Hilfssatz 4.5.10 :

$$\mathrm{Rg}A = \mathrm{Rg}B \text{ und } \mathrm{Rg}\,(A, b) = \mathrm{Rg}(B, c)\ .$$

Die Matrix (B, c) hat die Form

$$\begin{pmatrix}
\ast & \cdots & \ast & c_1 \\
 & & & \vdots \\
 & & & c_r \\
 & & & c_{r+1} \\
 & & & 0
\end{pmatrix}$$

mit $\ast = b_{1j_1}, b_{2j_2}, \ldots, b_{rj_r}$ und 0 in der letzten Zeile.

und daraus kann man alles ablesen, was man wissen möchte:

a) Ist $c_{r+1} \neq 0$, so ist $\mathrm{Rg}B = r$, $\mathrm{Rg}(B, c) = r + 1$, also ist das System nach Satz 4.6.7 nicht lösbar.

b) Ist $c_{r+1} = 0$, so ist

$$\mathrm{Rg}B = \mathrm{Rg}(B, c) = r\,,$$

das System ist also lösbar, und eindeutig lösbar, wenn auch noch

$r = n =$ Anzahl der Unbekannten ist. Die Lösungen erhält man folgendermaßen: Für die Unbekannten

$$x_j \ , \quad j \notin \{j_1\,, \ldots\,, j_r\}$$

kann man beliebige Werte aus K einsetzen. Die Unbekannten

$x_{j_1}\,, \ldots\,, x_{j_r}$ erhält man in Abhängigkeit von diesen Unbekannten,

wenn man die Gleichungen

$$\begin{array}{rcl} b_{rj_r} \; x_{j_r} \; + \; \ldots & = & c_r \\ \vdots & & \vdots \\ b_{1j_1} \; x_{j_1} \; + \; \ldots & = & c_1 \end{array}$$

in dieser Reihenfolge nach $x_{j_r}, \ldots, x_{j_1}$ auflöst. Man sieht das am besten an Beispielen.

Beispiele 4.6.11 : 1) Gegeben sei das lineare Gleichungssystem

$$\begin{array}{rcrcrcrcrcl} x_1 & + & 2x_2 & - & x_3 & & & + & 4x_5 & = & 2 \\ x_1 & + & 4x_2 & - & 5x_3 & + & x_4 & + & 3x_5 & = & 1 \\ 3x_1 & + & 2x_2 & + & 5x_3 & + & 2x_4 & + & 2x_5 & = & 12 \\ 2x_1 & - & 2x_2 & + & 10x_3 & + & 4x_4 & - & x_5 & = & 11 \\ 2x_1 & + & 6x_2 & - & 6x_3 & + & x_4 & + & 7x_5 & = & 3 \end{array}$$

Die erweiterte Matrix

$$\left(\begin{array}{ccccc|c} 1 & 1 & -1 & 0 & 4 & 2 \\ 1 & 4 & -5 & 1 & 3 & 1 \\ 3 & 2 & 5 & 2 & 2 & 12 \\ 2 & -2 & 10 & 4 & -1 & 11 \\ 2 & 6 & -6 & 1 & 7 & 3 \end{array}\right)$$

bringen wir, wie im Beweis von Satz 4.5.12 beschrieben, auf Zeilenstufenform:

$$(A', b') = \left(\begin{array}{ccccc|c} 1 & 2 & -1 & 0 & 4 & 2 \\ 0 & 2 & -4 & 1 & -1 & -1 \\ 0 & -4 & 8 & 2 & -10 & 6 \\ 0 & -6 & 12 & 4 & -9 & 7 \\ 0 & 2 & -4 & 1 & -1 & -1 \end{array}\right),$$

$$(A'', b'') = \left(\begin{array}{ccccc|c} 1 & 2 & -1 & 0 & 4 & 2 \\ 0 & 2 & -4 & 1 & -1 & -1 \\ 0 & 0 & 0 & 4 & -12 & 4 \\ 0 & 0 & 0 & 7 & -12 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right),$$

$$(A''', b''') = \left(\begin{array}{ccccc|c} 1 & 2 & -1 & 0 & 4 & 2 \\ 0 & 2 & -4 & 1 & -1 & -1 \\ 0 & 0 & 0 & 4 & -12 & 4 \\ 0 & 0 & 0 & 0 & 9 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Wir sehen: $\mathrm{Rg}A''' = \mathrm{Rg}(A''', b''') = 4 \neq 5$, das System ist also lösbar, aber nicht eindeutig lösbar. Wir wählen

$x_3 \in \mathbb{R}$ beliebig und erhalten damit

$9x_5 = -3$, also $x_5 = -\frac{1}{3}$,

$4x_4 - 12x_5 = 4$, also $x_4 = 1 + 3x_5 = 0$,

$2x_2 - 4x_3 + x_4 - x_5 = -1$, also $x_2 = 2x_3 - \frac{1}{2} - 0 - \frac{1}{2} \cdot \frac{1}{3} = 2x_3 - \frac{2}{3}$,

$x_1 + 2x_2 - x_3 + 4x_5 = 2$, also $x_1 = 2 - 4x_3 + \frac{4}{3} + x_3 + \frac{4}{3} = \frac{14}{3} - 3x_3$.

2)
$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & - & x_3 & = & 1 \quad , \\ 2x_1 & - & x_2 & + & x_3 & = & 2 \quad , \\ -x_1 & + & 3x_2 & - & 2x_3 & = & 1 \quad . \end{array}$$

Die erweiterte Matrix ist

$$(A, b) = \left(\begin{array}{ccc|c} 1 & 2 & -1 & 1 \\ 2 & -1 & 1 & 2 \\ -1 & 3 & -2 & 1 \end{array} \right) ,$$

wir bringen sie auf Zeilenstufenform:

$$(A', b') = \left(\begin{array}{ccc|c} 1 & 2 & -1 & 1 \\ 0 & -5 & 3 & 0 \\ 0 & 5 & -3 & 2 \end{array} \right) ,$$

$$(A'', b'') = \left(\begin{array}{ccc|c} 1 & 2 & -1 & 1 \\ 0 & -5 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{array} \right) .$$

Wir sehen: Es war

$\mathrm{Rg}A = 2$, aber $\mathrm{Rg}(A, b) = 3$,

das System ist also nicht lösbar. □

Für das nächste Rechenverfahren brauchen wir

Satz 4.6.12 : Sei $n \in \mathbb{N}$ und K ein Körper. Dann sind für eine Matrix $A \in M(n \times n, K)$ die folgenden Aussagen gleichbedeutend:

(i) $A \in \mathrm{GL}(n, K)$,
(ii) $\mathrm{Rg}\ A = n$,
(iii) $f_A : K^n \longrightarrow K^n$, $f_A(x) := A \cdot x$ ist ein Isomorphismus.

Beweis : Sei $\mathfrak{K} := (e^1, \ldots, e^n)$ die kanonische Basis des K^n (als Spaltenvektoren geschrieben), dann ist

$$A = M_{\mathfrak{K}}^{\mathfrak{K}}(f_A) .$$

(i) $\Longrightarrow$ (ii) : Ist $A \in \mathrm{GL}(n,K)$, so gilt

$$\mathrm{Rg}A \;=\; \mathrm{ZRg}(A) \;=\; \mathrm{ZRg}(A \cdot E_n) \overset{4.5.7}{=} \mathrm{ZRg}(E_n) \;=\; n \quad .$$

(ii) $\Longrightarrow$ (iii) : Wenn (ii) gilt, haben wir

$$n \quad = \quad \mathrm{Rg}\, A \quad = \quad \dim \mathrm{span}(a^1, \ldots, a^n) \quad =$$

$$\dim \mathrm{span}(f_A(e^1), \ldots, f_A(e^n)) \quad = \quad \dim f_A(K^n) \quad ,$$

also $f_A(K^n) = K^n$, also ist f_A surjektiv. Nach der Dimensionsformel (4.3.13) ist $\dim \ker f_A = 0$, also ist f_A injektiv. Also ist f_A ein Isomorphismus.
(iii) $\Longrightarrow$ (i) : Ist f_A ein Isomorphismus, so ist f_A bijektiv, wir haben also die Umkehrfunktion $G : K^n \longrightarrow K^n$, die, wie wir nachrechnen können, wiederum $K-$linear ist. Aus

$$f_A \circ G \quad = \quad G \circ f_A \quad = \quad \mathrm{id}_{K^n}$$

folgt nach (4.4.15) :

$$M^{\mathfrak{K}}_{\mathfrak{K}}(f_A) \cdot M^{\mathfrak{K}}_{\mathfrak{K}}(G) \quad = \quad M^{\mathfrak{K}}_{\mathfrak{K}}(G) \cdot M^{\mathfrak{K}}_{\mathfrak{K}}(f_A) \quad = \quad M^{\mathfrak{K}}_{\mathfrak{K}}(\mathrm{id}_{K^n}) \quad ,$$

also für $B := M^{\mathfrak{K}}_{\mathfrak{K}}(G)$:

$$A \cdot B \quad = \quad B \cdot A \quad = \quad E_n \quad ,$$

also $A \in \mathrm{GL}(n,K)$. □

Anwendung 4.6.13 : Man kann das Gaußsche Eliminationsverfahren anwenden, um mit geringem Rechenaufwand das Inverse einer Matrix

$$A \;\in\; M(n \times n, K)$$

auszurechnen, und man sieht bei der Rechnung auch, ob es existiert : Die inverse Matrix

$$B \quad = \quad (b_{kj}) \quad := \quad A^{-1} \quad ,$$

erfüllt, falls sie existiert, die Gleichung $A \cdot B = E_n$, also

$$\forall\, k,j \in \underline{n} : \;\; \sum_{l=1}^{n} a_{kl} \cdot b_{lj} \;=\; \delta_{kj} \;=\; \begin{cases} 1 & \text{für } k = j \\ 0 & \text{für } k \neq j \end{cases} \quad .$$

Das sind n^2 lineare Gleichungen mit den n^2 Unbekannten b_{kj}, aber man muss erfreulicherweise nicht alle diese Gleichungen hinschreiben: Für jedes feste $j \in \underline{n}$ hat man n Gleichungen mit n Unbekannten $b_{1j}, \ldots, b_{nj}$:

$$\sum_{l=1}^{n} a_{kl} \cdot b_{lj} \quad = \quad \delta_{kj}\,, \quad \text{also}$$

$$A \cdot b^j \quad = \quad e^j$$

mit dem unbekannten Spaltenvektor b^j . Die einfache Matrix A ist für alle $j \in \underline{n}$ dieselbe, nur die "rechte Seite" hängt von j ab. Wir lösen nun diese n Gleichungssysteme (mit jeweils n Gleichungen mit n Unbekannten) dadurch, dass wir alle "rechten Seiten", also die Spaltenvektoren e^j , auf einmal rechts neben die Matrix A schreiben, das ergibt die Matrix

$$\left(\begin{array}{ccc|ccc} a_{11} & \dots & a_{1n} & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ a_{n1} & \dots & a_{nn} & 0 & & 1 \end{array}\right) \quad = \quad (A \mid E_n) \quad ,$$

und mit allen rechten Seiten gleichzeitig, also mit E_n , die elementaren Zeilenumformungen ausführen. Wir kommen dann zunächst auf eine Matrix der Form

$$(\, A' \mid C' \,) \quad .$$

Hat dieses A' nun weniger als n Stufen, so war

$$\operatorname{Rg} A \quad = \quad \operatorname{Rg} A' < n$$

und nach Satz 4.6.12 ist A nicht invertierbar, wir brauchen also nicht weiter zu rechnen. Hat man n Stufen, so ist

$$A' \quad = \quad \left(\begin{array}{cccccc} \boxed{a'_{11}} & & & * & & \\ & \boxed{a'_{22}} & & & & \\ & & \ddots & & & \\ 0 & & & & \boxed{a'_{nn}} & \end{array}\right) \quad , \quad \text{mit} \quad a'_{11}, \dots, a'_{nn} \neq 0 \quad ,$$

und man führt weitere elementare Zeilenumformungen an $(A' \mid C')$ aus: Man dividiert die $k-$te Zeile durch a'_{kk} , für $k = 1, \dots, n$, und addiert dann, beginnend mit der letzten Zeile, passende Vielfache jeder Zeile zu den vorhergehenden, so dass man auch oberhalb der Diagonale nur noch Nullen hat. Insgesamt hat man dann die Matrix

$$(\, E_n \mid C \,) \quad ,$$

und wenn man sich nun wieder die einzelnen Gleichungssysteme ansieht, so steht da

$$E_n \cdot b^j \quad = \quad c^j \qquad \text{für} \quad j = 1, \dots, n,$$

für die "unbekannten" Vektoren b^j . Also gilt

$$c^j \quad = \quad b^j \quad , \quad C \quad = \quad B \quad ,$$

die rechts stehende Matrix ist also die Inverse von A :

$$(E_n \mid A^{-1}) \quad .$$

□

4.7 Summen von Vektorräumen

Definition und Satz 4.7.1 : Sei K ein Körper, $n \in \mathbb{N}$, und für jedes $j \in \underline{n}$ sei V_j ein $K-$Vektorraum. Dann ist nach Definition 1.0.16 das cartesische Produkt

$$\prod_{j \in \underline{n}} V_j \quad := \quad V_1 \times V_2 \times \ldots \times V_n$$

definiert. Diese Menge wird ein $K-$Vektorraum, wenn man für

$$(v_1, \ldots, v_n)\,, (w_1, \ldots, w_n) \quad \in \quad \prod_{j \in \underline{n}} V_j \quad \text{und} \quad \lambda \in K \quad \text{definiert :}$$

$$(v_1, \ldots, v_n) + (w_1, \ldots, w_n) \quad := \quad (v_1 + w_1, \ldots, v_n + w_n) \quad ,$$

$$\lambda(v_1, \ldots, v_n) \quad := \quad (\lambda v_1, \ldots, \lambda v_n) \quad .$$

Dieser $K-$Vektorraum heißt das **äußere direkte Produkt** von V_1 , ... , V_n . Sind V_1 , ... , V_n endlichdimensional,

$$\dim V_j \; = \; k_j \quad \text{für} \quad j \in \underline{n}\,,$$

so ist auch $\prod_{j \in \underline{n}} V_j$ endlichdimensional,

$$\dim_K \prod_{j \in \underline{n}} V_j \quad = \quad k_1 + \ldots + k_n \quad .$$

Beweis : Dass für $\prod_{j \in \underline{n}} V_j$ die Vektorraum-Axiome gelten, kann man nachrechnen. Hat man $\dim_K V_j \; = \; k_j \in \mathbb{N}_0$ für $j \in \underline{n}$, so hat man für jedes $j \in \underline{n}$ Basen

$$(b_1^{(j)}, \ldots, b_{k_j}^{(j)}) \quad \text{von} \quad V_j \quad , \quad \text{und man sieht, dass}$$

$$((b_1^{(1)}, 0, \ldots, 0)\,, \ldots\,, (b_{k_1}^{(1)}, 0, \ldots, 0)\,, (0, b_1^{(2)}, 0, \ldots, 0)\,, \ldots\,, (0, b_{k_2}^{(2)}, 0, \ldots, 0)\,,$$

$$\ldots\ ,\ (0,\ldots,0,b_1^{(n)})\ ,\ \ldots\ ,\ (0,\ldots,0,b_{k_n}^{(n)}))$$

eine Basis von $\prod\limits_{j\in\underline{n}} V_j$ ist.

□

- Meistens benutzt man diese Konstruktion für $n = 2$. Aber man kann diese Konstruktion sogar für beliebig (möglicherweise unendlich) viele Vektorräume machen :

Definition und Satz 4.7.2 : Sei I eine nichtleere Menge, K ein Körper, und für jedes $j \in I$ sei V_j ein $K-$Vektorraum. Dann setzt man

$$\prod_{j\in I} V_j \quad := \quad \left\{ \ (v_j)_{j\in I} \in \mathcal{F}(I, \bigcup_{j\in I} V_j) \ \middle| \ \forall\, j \in I \ :\ v_j \in V_j \ \right\} \quad ,$$

man nimmt also die Menge aller Familien $(v_j)_{j\in I}$, bei denen $v_j \in V_j$ für jedes $j \in I$ gilt, und definiert

$$\text{für} \quad (v_j)_{j\in I}\,,\,(w_j)_{j\in I} \quad \text{und} \quad \lambda \in K \ :$$

$$\begin{aligned} (v_j)_{j\in I} \,+\, (w_j)_{j\in I} \quad &:= \quad (v_j + w_j)_{j\in I} \quad , \\ \lambda\,(v_j)_{j\in I} \quad &:= \quad (\lambda\, v_j)_{j\in I} \quad , \end{aligned}$$

dann wird $\prod\limits_{j\in I} V_j$ ein $K-$Vektorraum, den man das **äußere direkte Produkt** der Vektorräume V_j , $j \in I$, nennt. Man hat darin den Untervektorraum

$$\bigoplus_{j\in I} V_j \quad := \quad \left\{ \ (v_j)_{j\in I} \in \prod_{j\in I} V_j \ \middle| \ \forall' \, j \in I \ :\ v_j \,=\, 0 \ \right\} \quad ,$$

also die Menge der Familien, bei denen fast alle Komponenten Null sind. $\bigoplus\limits_{j\in I} V_j$ heißt die **äußere direkte Summe** der V_j , $j \in I$, und für eine **endliche** Indexmenge I ist

$$\bigoplus_{j\in I} V_j \quad = \quad \prod_{j\in I} V_j \quad ,$$

es ist dann also egal, ob man von der äußeren direkten Summe oder dem äußeren direkten Produkt spricht.
Der **Beweis** dieser Aussagen ist leicht.

□

(4.7.3) Beachte hierbei, dass die V_j beliebige $K-$Vektorräume sind. Sie können ganz verschieden sein. Es kann aber auch $V_1 = V_2 =: V$ und $I = \{1,2\}$ gelten, dann hat man

$$V_1 \times V_2 \quad = \quad \bigoplus_{j \in \underline{2}} V_j \quad = \quad V \times V \quad ,$$

und wenn $\dim V = n$ ist, ist

$$\dim(V \times V) \quad = \quad 2n \quad .$$

Soweit war alles ganz einfach. Etwas verwirrend wird die Situation dadurch, dass man noch eine andere Konstruktion hat:

Definition 4.7.4 : Sei V ein $K-$Vektorraum, $r \in \mathbb{N}$ und $W_1, \ldots, W_r$ seien **Unter**vektorräume von V . Dann setzt man

$$\begin{aligned} \sum_{j=1}^{r} W_j \; &:= \; W_1 + \ldots + W_r \\ &:= \quad \{ \; v \in V \; \mid \; \forall\, j \in \underline{r} \, \exists\, w_j \in W_j \; : \; v \; = \; w_1 + \ldots + w_r \; \} \\ &= \quad \{ \; w_1 + \ldots + w_r \; \mid \; \forall\, j \in \underline{r} \; : \; w_j \in W_j \; \} \quad . \end{aligned}$$

Satz und Definition 4.7.5 : Sei V ein $K-$Vektorraum, $r \in \mathbb{N}$, und

$$W_1 \, , \, \ldots \, , \, W_r \quad \text{seien Untervektorräume von} \quad V \quad .$$

Dann sind folgende Aussagen gleichbedeutend :

(1) Zu jedem $w \in \sum_{j=1}^{r} W_j$ gibt es ein **eindeutig bestimmtes** $r-$tupel $(w_1, \ldots, w_r) \in W_1 \times \ldots \times W_r$ mit

$$w \quad = \quad w_1 + \ldots + w_r \quad .$$

(2) Für jedes $j \in \underline{r}$ sei $w_j \in W_j$, und es sei $w_1 + \ldots + w_r = 0$, dann folgt:

$$\forall\, j \in \underline{r} \; : \;\; w_j \; = \; 0 \quad .$$

(3) Für alle $k \in \underline{r}$ ist $W_k \cap \sum_{j \in \underline{r} \setminus \{k\}} W_j = \{0\}$.

Falls eine dieser drei Aussagen erfüllt ist (und damit alle drei Aussagen gelten) , nennen wir $W := \sum_{j=1}^{r} W_j$ die **innere direkte Summe** der W_j und schreiben

$$W \quad = \quad W_1 \oplus W_2 \oplus \ldots \oplus W_r \quad = \quad \bigoplus_{j=1}^{r} W_j \quad .$$

Beweis : (1) $\Longrightarrow$ (2) ist trivial: Wenn sich jeder Vektor $w \in \sum_{j=1}^{r} W_j$ eindeutig als $w = w_1 + \ldots + w_r$ mit $w_j \in W_j$ darstellen läßt, dann auch 0.
(2) $\Longrightarrow$ (3) : Sei $w \in W_k \cap \sum_{j \in \underline{r} \setminus \{k\}} W_j$, dann gibt es zu jedem $j \in \underline{r} \setminus \{k\}$ ein $w_j \in W_j$ mit

$$w \quad = \quad \sum_{j \in \underline{r} \setminus \{k\}} w_j \quad , \quad \text{und es ist} \quad w_k := -w \in W_k \quad , \quad \text{also}$$

$$0 \quad = \quad \sum_{j=1}^{r} w_j \quad \text{mit} \quad w_j \in W_j \quad \text{für alle} \quad j \in \underline{r} \quad .$$

Nach (2) folgt daraus

$$\forall\, j \in \underline{r} : \ w_j = 0 \quad , \quad \text{insbesondere}$$

$$w = -w_k = 0 \quad .$$

(3) $\Longrightarrow$ (1) : Sei $w \in \sum_{j=1}^{r} W_j$, dann gibt es $w_1, \ldots, w_r$ mit

$$w = \sum_{j=1}^{r} w_j \quad \text{und} \quad \forall\, j \in \underline{r} : \ w_j \in W_j \quad . \quad \text{Sei auch}$$

$$w = \sum_{j=1}^{r} v_j \quad \text{mit} \quad \forall\, j \in \underline{r} : \ v_j \in W_j \quad ,$$

dann gilt für jedes $k \in \underline{r}$:

$$v_k - w_k = \sum_{j \in \underline{r} \setminus \{k\}} (w_j - v_j) \in \left(\sum_{j \in \underline{r} \setminus \{k\}} W_j \right) \cap W_k \quad ,$$

und nach (3) : $v_k - w_k = 0$, also

$$\forall\, k \in \underline{r} : \ v_k = w_k \quad .$$

□

Bemerkung 4.7.6 : Sei V ein $K-$Vektorraum, $r \in \mathbb{N}$, und seien $W_1, \ldots, W_r$ **Unter**vektorräume von V , für die die Aussage

(3) Für alle $k \in \underline{r}$ ist $W_k \cap \sum_{j \in \underline{r} \setminus \{k\}} W_j = \{0\}$

gilt, dann hat man also die innere direkte Summe $\sum_{j=1}^{r} W_j$. Man kann aber auch die **Vektorräume** W_j nehmen und gemäß Definition 4.7.1 deren äußeres direktes Produkt $\prod_{j \in \underline{r}} W_j$ bilden (das wir in 4.7.2 auch als äußere direkte Summe bezeichnet hatten). Erfreulicherweise gibt es keine Verwechslungsgefahr, denn innere und äußere direkte Summe sind in diesem Fall isomorph. Genauer: Sei

$$\varphi : \underbrace{\prod_{j \in \underline{r}} W_j}_{\text{äußere}} \longrightarrow \underbrace{\bigoplus_{j=1}^{r} W_j}_{\text{innere}} \quad , \quad (w_1, \ldots, w_r) \longmapsto w_1 + \ldots + w_r \quad ,$$

direkte Summe

dann ist φ ein Isomorphismus.

Beweis : Seien $(v_1, \ldots, v_r), (w_1, \ldots, w_r) \in \prod_{j \in \underline{r}} W_j$ und $\lambda \in K$, dann gilt

$$\begin{aligned} \varphi((v_1, \ldots, v_r) + (w_1, \ldots, w_r)) &= \varphi(v_1 + w_1, \ldots, v_r + w_r) \\ = \; v_1 + w_1 + \ldots + v_r + w_r &= v_1 + \ldots + v_r + w_1 + \ldots + w_r \\ = \; \varphi(v_1, \ldots, v_r) + \varphi(w_1, \ldots, w_r) &\quad , \\ \varphi(\lambda(v_1, \ldots, v_r)) = \varphi(\lambda v_1, \ldots, \lambda v_r) &= \lambda v_1 + \ldots + \lambda v_r \\ = \; \lambda(v_1 + \ldots + v_r) = \lambda \varphi(v_1, \ldots, v_r) &\quad , \end{aligned}$$

also: φ ist $K-$linear. φ ist surjektiv, denn

$$\bigoplus_{j=1}^{r} W_j = \{ \; w_1 + \ldots + w_r \mid \forall\, j \in \underline{r} : \; w_j \in W_j \; \}$$

$$= \{ \; \varphi(w_1, \ldots, w_r) \mid \forall j \in \underline{r} : \; w_j \in W_j \; \} = \varphi\left(\prod_{j=1}^{r} W_j \right) \quad .$$

Und: φ ist injektiv, denn sei $(w_1, \ldots, w_r) \in \ker \varphi$, dann ist

$$w_1 + \ldots + w_r = 0 \quad .$$

Es gilt die Aussage (3), also auch die Aussage (2), von Satz 4.7.5, also

$$\forall\, j \in \underline{r} : \; w_j = 0 \quad , \quad \text{also} \quad (w_1, \ldots, w_r) = (0, 0, \ldots, 0) \quad .$$

□

Folgerung 4.7.7 : Äußere und innere direkte Summe von Vektorräumen $W_1 , \ldots , W_r$ (wobei man die innere direkte Summe nur bilden kann, wenn alle $W_j , j \in \underline{r}$, **Unter-**Vektorräume eines Vektorraums V sind), sind zwar nicht gleich, aber isomorph.

□

4.8 Anwendung: Körpererweiterungen

Bemerkung 4.8.1 : Sei $(K, +, \cdot)$ ein Körper. Dann suchen wir zunächst den "kleinsten" in K enthaltenen Körper, den wir $P(K)$ nennen, d.h. den Körper $P(K)$, für den für jeden Unterkörper U von K gilt:

$$P(K) \subset U \subset K \quad .$$

$P(K)$ heißt der **Primkörper** von K . $P(K)$ ist dann ein Unterring von $(K, +, \cdot)$, und wenn wir das Einselement von K mal mit 1_K bezeichnen, gilt

$$1_K \in P(K) \quad .$$

Da $(K, +)$ eine abelsche Gruppe ist, folgt mit Induktion

$$\forall\, n \in \mathbb{N}_0 \, : \;\; n\, 1_K \in P(K)$$

und da auch das Negative dazugehört,

$$\forall\, n \in \mathbb{Z} \, : \;\; n\, 1_K \in P(K) \quad .$$

$n\, 1_k$ bezeichnet dabei stets das $n-$fache von 1_K. Also ist

$$U_K := \{ \;\; n\, 1_K \;\; | \;\; n \in \mathbb{Z} \;\; \}$$

eine Teilmenge von K, sogar ein Untering. Man braucht dazu die Potenzregeln 2.1.6 (umgeschrieben für die Vielfachen von 1_K), und die Regel $(*)$ aus dem Beweis von Satz 3.2.16. Die Abbildung

$$\varphi \, : \;\; \mathbb{Z} \;\; \longrightarrow \;\; U_K \quad , \quad n \mapsto n\, 1_K$$

ist dann ein surjektiver Ring-Homomorphismus. In Def. und Satz 3.2.16 hatten wir nun die Charakteristik von K definiert, und das ergibt für $P(K)$ zwei Möglichkeiten:

(1.) char $K \;=\; p \quad , \quad p$ eine Primzahl: Dann ist

$$p\, 1_K \;=\; 0\,,$$

p ist die kleinste natürliche Zahl n mit $n\,1_K = 0$, und wir haben

$$\ker \varphi = (p) \quad .$$

Nach dem Homomorphiesatz für Ringe (3.1.11) haben wir genau einen Ring-Isomorphismus

$$\iota : \mathbb{Z}/_{\ker \varphi} \longrightarrow U_K \quad \text{mit} \quad \iota(a + \ker \varphi) = \varphi(a) \quad \text{für} \quad a \in \mathbb{Z}\,, \quad \text{also}$$

$$\iota : \mathbb{Z}/_{(p)} \longrightarrow U_K \quad , \quad a + (p) \mapsto a\,1_K \quad .$$

Da $\mathbb{Z}/_{(p)}$ ein Körper ist, ist auch U_K ein Körper: Das Inverse eines Elements $x \in U_K \setminus \{0\}$ ist

$$x^{-1} = \iota((\iota^{-1}(x))^{-1}) \quad \text{mit} \quad (\iota^{-1}(x))^{-1} \in \mathbb{Z}/_{(p)} \quad .$$

Es ist also $P(K) = U_K$ und damit

$$P(K) \cong \mathbb{Z}/_{(p)} \quad .$$

(2.) char $K = 0$. Dann sind alle Elemente aus U_K verschieden, denn wäre etwa

$$n\,1_k = m\,1_k \quad \text{mit} \quad n, m \in \mathbb{Z} \quad , \quad n < m \quad ,$$

dann wäre $m - n \in \mathbb{N}$, die Menge

$$\{\ k \in \mathbb{N} \mid k\,1_K = 0\ \}$$

wäre nichtleer, Widerspruch zu char $K = 0$. Die Abbildung φ ist nur ein Isomorphismus von Ringen, U_K ist kein Körper. In $P(K)$ liegen aber auch die Inversen der Elemente von $U_K \setminus \{0\}$, wir setzen

$$B_K := \left\{\ (n\,1_K) \cdot (m\,1_K)^{-1} \;\middle|\; n, m \in \mathbb{Z} \wedge m \neq 0\ \right\} \quad ,$$

dann ist $B_K \subset P(K)$ und

$$\psi : \mathbb{Q} \longrightarrow B_K \quad , \quad \frac{n}{m} \mapsto (n\,1_K) \cdot (m\,1_k)^{-1}$$

ist ein Ring-Isomorphismus. Dazu müssen wir nur zeigen, dass ψ wohldefiniert ist: Seien $n, n' \in \mathbb{Z}$, $m, m' \in \mathbb{Z} \setminus \{0\}$, dann gilt

$$\frac{n}{m} = \frac{n'}{m'} \quad \Longrightarrow \quad n{\cdot}m' = m{\cdot}n' \quad \Longrightarrow \quad (n\,1_K){\cdot}(m'\,1_K) = (m\,1_K){\cdot}(n'\,1_K)$$

$$\Longrightarrow \quad (n\,1_K) \cdot (m\,1_K)^{-1} = (n'\,1_K) \cdot (m'\,1_K)^{-1}\,,$$

die Homomorphiebedingungen (RH1) - (RH3) sind offensichtlich erfüllt. Da $\mathbb{Q}$ ein Körper ist, ist es auch B_K und damit

$$P(K) = B_K \cong \mathbb{Q} \quad .$$

□

Folgerung 4.8.2 : Für einen beliebigen Körper K haben wir also den Unterkörper $P(K)$, und nach Folgerung 4.1.3 ist K ein $P(K)-$Vektorraum, wir haben also

$$\dim_{P(K)} K \in \mathbb{N} \quad \text{oder} \quad \dim_{P(K)} K = \infty \quad .$$

Allgemein mit Körpererweiterungen beschäftigt man sich in der Algebra. Hier nur einige

Beispiele 4.8.3 :(1) Sei K ein endlicher Körper. Dann ist auch $P(K)$ endlich, also existieren eine Primzahl p mit $P(K) \cong \mathbb{Z}/_{(p)}$ und ein $n \in \mathbb{N}$ mit $\dim_{P(K)} K = n$. Man kann dann nachzählen:

$$\#(K) = p^n \quad .$$

Körper mit 6 Elementen braucht man also gar nicht erst zu suchen.
(2) Der Primkörper von $\mathbb{R}$ und $\mathbb{C}$ ist also $\mathbb{Q}$. Es ist

$$\dim_{\mathbb{Q}} \mathbb{R} = \infty \quad .$$

Zum Beweis kann man zeigen, dass die Familie $(\sqrt{p})_{p\in\mathbb{P}}$ eine linear unabhängige Familie ist, oder auch: $\mathbb{Q}$ ist abzählbar, d.h. es gibt eine bijektive Abbildung von $\mathbb{Z}$ auf $\mathbb{Q}$, aber für $\mathbb{R}$ gilt das nicht. Das gehört aber in die Analysis.
(3) Schreibt man die komplexen Zahlen z als $a + i \cdot b$ mit $a, b \in \mathbb{R}$, so sind a und b eindeutig bestimmt. Daher ist $(1, i)$ eine Basis des $\mathbb{R}-$Vektorraums $\mathbb{C}$,

$$\dim_{\mathbb{R}} \mathbb{C} = 2 \quad .$$

Daraus sieht man, dass es keinen Körper K mit $\mathbb{R} \subsetneq K \subsetneq \mathbb{C}$ gibt, weil es keine Zahl $n \in \mathbb{N}$ mit $1 < n < 2$ gibt.
(4) Für einen beliebigen Köper K und den Körper $K(X)$ der rationalen Funktionen mit Koeffizienten aus K gilt

$$\dim_K K(X) = \infty \quad .$$

(5) Es gibt beliebig viele Körper K mit $\mathbb{Q} \subsetneq K \subsetneq \mathbb{R}$ oder $\mathbb{Q} \subsetneq K \subsetneq \mathbb{C}$. Dazu gehören

$$\mathbb{Q}(\sqrt{2}) := \{\ a+b\cdot\sqrt{2}\ \mid\ a,b\in\mathbb{Q}\ \}\quad ,$$
$$\mathbb{Q}(\sqrt{-3}) := \{\ a+b\cdot i\cdot\sqrt{3}\ \mid\ a,b\in\mathbb{Q}\ \}\quad ,\quad \text{auch}$$
$$\mathbb{Q}(i) := \{\ a+b\cdot i\ \mid\ a,b\in\mathbb{Q}\ \}\quad .$$

Mit solchen Körpern und Unterringen davon beschäftigt man sich in der Zahlentheorie.

(6) Es gibt keinen Körper K mit

$$\mathbb{C}\ \stackrel{\subset}{\neq}\ K\quad\text{und}\quad \dim_{\mathbb{C}} K\ =\ n\in\mathbb{N}\quad .$$

Angenommen, es gibt doch so einen Körper K, dann haben wir ein $a\in K\setminus\mathbb{C}$. Die Familie

$$(a^0,a^1,\ldots,a^n)$$

ist dann eine linear abhängige Familie im $\mathbb{C}-$Vektorraum K, da sie aus $n+1$ Elementen besteht. Es gibt dann

$$\alpha_0,\ldots,\alpha_n\in\mathbb{C}\quad\text{mit}\quad(\alpha_0,\ldots,\alpha_n)\neq 0\quad\text{und}\quad\sum_{j=0}^{n}\alpha_j a^j\ =\ 0\,,$$

also ein Polynom

$$f(X)\ :=\ \sum_{j=0}^{n}\alpha_j\cdot X^j\in\mathbb{C}[X]\setminus\{0\}\quad\text{mit}\quad f(a)\ =\ 0\quad .$$

Man hat dann $k\ :=\ \deg f(X)\,,\ 0\leq k\leq n$, und nach dem Fundamentalsatz der Algebra (3.5.13) :

$$\exists\, c,b_1,\ldots,b_k\in\mathbb{C}:\ \ f(X)\ =\ c\cdot\prod_{j=1}^{k}(X-b_j)\quad .$$

Wegen $f(a)\ =\ 0$ folgt daraus

$$a\in\{b_1,\ldots,b_k\}\subset\mathbb{C}\quad ,\quad\text{Widerspruch.}$$

Sie sehen also, dass man Sätze und Methoden der Linearen Algebra in anderen Gebieten der Mathematik, insbesondere der Algebra und der Zahlentheorie, braucht !

4.9 Die Algebra der $n\times n$-Matrizen, Quaternionen

Bemerkung 4.9.1 : Sei $n\in\mathbb{N}$ und K rin Körper. Nach Bemerkung 4.4.5

hat man eine Addition

$$+ : M(n\times n,K)\times M(n\times n,K) \longrightarrow M(n\times n,K)\,,\ ((a_{kj}),(b_{kj})) \mapsto (a_{kj}+b_{kj})$$

und eine äußere Operation ω,

$$\omega : K \times M(n\times n,K) \longrightarrow M(n\times n,K) \quad , \quad (\lambda,(a_{kj})) \mapsto (\lambda\cdot a_{kj}) \quad ,$$

so dass $(M(n\times n,K),+,\omega)$ ein $K-$Vektorraum ist. Nach Definition 4.4.9 haben wir in $M(n\times n,K)$ auch noch eine Multiplikation $\cdot$, und damit ist $(M(n\times n,K),+,\cdot)$ nach Satz 4.4.13 ein Ring. Die Regel

$$\text{(L)} \quad \forall\,\lambda\in K\,\forall\,A,B\in M(n\times n,K) : \ \lambda(A\cdot B) = (\lambda A)\cdot B = A\cdot(\lambda B)$$

kann man nachrechnen. Man sagt: $(M(n\times n,K),+,\cdot,\omega)$ ist eine $K-$Algebra:

Defnition 4.9.2 : Sei K ein Körper. A sei eine Menge mit zwei Verknüpfungen $+,\cdot$ und einer äußeren Operation ω von K auf A, so dass gilt

(R) $(A,+,\cdot)$ ist ein Ring.

(V) $(A,+,\omega)$ ist ein $K-$Vektorraum.

(L) $\forall\,\lambda\in K\,\forall a,b\in A : \ \lambda(a\cdot b) = (\lambda a)\cdot b = a\cdot(\lambda b)$,

dann heißt $(A,+,\cdot,\omega)$ (kurz: A) eine **$K-$Algebra** (Plural : $K-$Algébren).

□

Bemerkung 4.9.3 : Wir wollen die $K-$Algebra $M(n\times n,K)$ etwas genauer untersuchen. Nach Bemerkung 4.4.3 ist die Familie $(E_{jk})_{(j,k)\in\underline{n}\times\underline{n}}$, wobei E_{jk} die Matrix ist, die am Schnittpunkt der $j-$ten Zeile mit der $k-$ten Spalte die 1 aus K hat und sonst nur Nullen, eine Basis des $K-$Vektorraums $M(n\times n,K)$. Für jedes $A = (a_{jk}) \in M(n\times n,K)$ gilt also

$$A \quad = \quad \sum_{j,k=1}^{n} a_{jk}\,E_{jk} \quad .$$

Die Matrizen-Multiplikation wird nun sehr einfach, wenn man die Regel 4.4.7 (1) für die Multiplikation der Basiselemente verwendet: Es war

$$E_{jk}\cdot E_{rs} \quad = \quad \delta_{kr}E_{js} \quad \text{für} \quad j,k,r,s\in\underline{n}, \quad \text{mit}$$

$$\delta_{kr} = \begin{cases} 1 & \text{für } k=r \\ 0 & \text{für } k\neq r \end{cases} \quad .$$

Definition und Satz 4.9.4 : Sei $(R,+,\cdot)$ ein Ring. Dann heißt

$$Z(R) := \{\ a\in R \mid \forall\, r\in R : a\cdot r = r\cdot a\ \}$$

das **Zentrum** von R. $Z(R)$ ist ein Unterring von R.
Beweis : Sei 1 das Einselement von R. Dann ist $1 \in Z(R)$, also $Z(R) \neq \emptyset$.
Für alle $a, b \in Z(R)$ und alle $r \in R$ gilt

$$(a-b)\cdot r \;=\; a\cdot r - b\cdot r \;=\; r\cdot a - r\cdot b \;=\; r\cdot(a-b) \quad \text{und}$$

$$(a\cdot b)\cdot r \;=\; a\cdot(b\cdot r) \;=\; a\cdot(r\cdot b) \;=\; (a\cdot r)\cdot b \;=\; (r\cdot a)\cdot b \;=\; r\cdot(a\cdot b)\,,$$

also $a-b \in Z(R), a\cdot b \in Z(R)$.

□

Wie sieht nun das Zentrum des Ringes $M(n\times n, K)$ aus? Es zeigt sich, dass nur die Matrizen dazu gehören, von denen man das sowieso erwartet:

Satz 4.9.5 : Sei K ein Körper, $n \in \mathbb{N}$. Dann ist

$$Z(M(n\times n, K)) \quad = \quad K\,E_n \quad := \quad \{\ \lambda E_N \mid \lambda \in K\ \} \quad .$$

Beweis : Für $n = 1$ ist das klar, da $(M(1\times 1), \cdot)$ kommutativ ist und $M(1\times 1, K) \;=\; K\,E_1$ ist.
Sei nun $n \geq 2$, und seien $s, t \in \underline{n}$ zwei Indizes mit $s \neq t$. Sei $A \;=\; (a_{jk})_{(j,k)\in \underline{n}\times\underline{n}} \in Z(M(n\times n, K))$. Wir haben nach 4.4.3 :

$$A \quad = \quad \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,E_{jk} \quad .$$

Dann gilt

$$\begin{aligned}
E_{st}\cdot A \quad &= \quad A\cdot E_{st} \quad , \\
E_{st}\cdot \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,E_{jk} \quad &= \quad \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,E_{jk}\cdot E_{st} \quad , \\
\sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,E_{st}\cdot E_{jk} \quad &= \quad \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,E_{jk}\cdot E_{st} \quad ,
\end{aligned}$$

und nach der Multiplikationsregel in 4.4.7 :

$$\sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,\delta_{tj}E_{sk} \quad = \quad \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\,\delta_{ks}E_{jt} \quad .$$

Links enthält die Summe über j höchstens einen Summanden ungleich 0, nämlich den mit $j = t$. Rechts enthält die Summe über k höchstens einen Summanden ungleich 0, nämlich den mit $k = s$. Wir erhalten

$$\sum_{k=1}^{n} a_{tk}\, E_{sk} \quad = \quad \sum_{j=1}^{n} a_{js}\, E_{jt} \quad ,$$

$$(*) \qquad \sum_{k=1}^{n} a_{tk}\, E_{sk} \; - \sum_{j=1}^{n} a_{js}\, E_{jt} \; = \; 0 \quad .$$

Nun ist die Familie $(E_{jk})_{(j,k)\in \underline{n}\times\underline{n}}$ linear unabhängig. Wir sehen daher aus der Gleichung $(*)$:
(1.) Für $k \neq t$ ist $a_{tk} = 0$, da E_{sk} in der zweiten Summe nicht vorkommt, ebenso: $a_{js} = 0$ für $j \neq s$. Jedenfalls ist A eine Matrix mit 0 außerhalb der Diagonale.
(2.) Die Gleichung $(*)$ vereinfacht sich also zu

$$a_{tt}E_{st} \quad = \quad a_{ss}E_{st} \quad ,$$

A ist also eine Diagonalmatrix, bei der alle Diagonalelemente gleich sind, etwa $a_{tt} =: \lambda \in K$,

$$A \quad = \quad \lambda\, E_n \in K\, E_n \quad , \qquad \text{also} \quad Z(M(n\times n, K)) \subset K\, E_n \quad .$$

Dass $K\, E_n \subset Z(M(n\times n, K))$ gilt, sieht man mit Regel (L) und der Tatsache $E_n \in Z(M(n\times n, K))$.

□

In 3.1.8 haben wir gelernt, was das Ideal eines Ringes ist, hier haben wir den

Satz 4.9.6 : Sei K ein Körper, $n \in \mathbb{N}$. Dann enthält $(M(n\times n, K), +, \cdot)$ nur die Ideale $\{0\}$ und $M(n\times n, K)$.
Beweis : Sei I ein Ideal in $M(n\times n, K)$. Es kann $I = \{0\}$ sein. Anderenfalls enthält I eine Matrix

$$A \quad = \quad \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\, E_{jk} \quad ,$$

in der nicht alle $a_{jk} = 0$ sind. Seien etwa $s, t \in \underline{n}$ mit $a_{st} \neq 0$. Da I ein Ideal ist, enthält I mit A auch

$$E_{ss}\cdot A \quad = \quad \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\, E_{ss}\cdot E_{jk} \; = \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}\, \delta_{sj} E_{sk} \; = \sum_{k=1}^{n} a_{sk}\, E_{sk} \quad ,$$

und I enthält auch

$$E_{ss} \cdot A \cdot E_{tt} \;=\; \sum_{k=1}^{n} a_{sk}\, E_{sk} \cdot E_{tt} \;=\; \sum_{k=1}^{n} a_{sk}\, \delta_{kt}\, E_{st} \;=\; a_{st} E_{st}\,,$$

und auch

$$((a_{st})^{-1} E_n) \cdot E_{ss} \cdot A \cdot E_{tt} \;=\; (a_{st})^{-1} \cdot a_{st}\, E_{st} \;=\; E_{st} \quad ,$$

für dieses feste Paar (s,t). Sei nun aber $j \in \underline{n}$ beliebig, dann enthält I auch

$$(E_{js} \cdot E_{st}) \cdot E_{tj} \;=\; E_{jt} \cdot E_{tj} \;=\; E_{jj}$$

und damit auch $\sum\limits_{j=1}^{n} E_{jj} \;=\; E_n$. Für eine beliebige Matrix $B \in M(n \times n, K)$ enthält I dann auch $B \;=\; B \cdot E_n$. Also ist $I \;=\; M(n \times n, K)$.

□

Satz und Definition 4.9.7 : In $M(2 \times 2, \mathbb{C})$ sei

$$\mathbb{H} \;:=\; \left\{ \left(\begin{array}{cc} u & v \\ -\overline{v} & \overline{u} \end{array} \right) \;\middle|\; u, v \in \mathbb{C} \right\} \quad ,$$

wobei $\overline{u}$ das Konjugiert-Komplexe von u bezeichnet. Dann gilt:

a) $\mathbb{H}$ ist ein Unterring von $(M(2 \times 2, \mathbb{C}), +, \cdot)$, mit Einselement E_2.

b) Wegen $\mathbb{R} \subset \mathbb{C}$ ist $\omega(\alpha, A) \;:=\; \alpha\, A$ für $\alpha \in \mathbb{R}$ und $A \in \mathbb{H}$ definiert, und $\mathbb{H}$ wird auf diese Weise ein $\mathbb{R}-$Vektorraum. Eine Basis dieses $\mathbb{R}-$Vektorraums ist (E_2, I, J, K) mit

$$I \;:=\; \left(\begin{array}{cc} i & 0 \\ 0 & -i \end{array} \right) \quad , \quad J \;:=\; \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right) \quad , \quad K \;:=\; \left(\begin{array}{cc} 0 & i \\ i & 0 \end{array} \right) .$$

Für die Produkte gilt

$$I \cdot J \;=\; -J \cdot I \;=\; K\,,\; J \cdot K \;=\; -K \cdot J \;=\; I\,,\; K \cdot I \;=\; -I \cdot K \;=\; J\,,$$

$$I \cdot I \;=\; J \cdot J \;=\; K \cdot K \;=\; -E_2 \quad .$$

$\mathbb{H}$ ist eine $\mathbb{R}-$Algebra.

c) Jedes Element aus $\mathbb{H} \setminus \{0\}$ besitzt bezüglich $\cdot$ ein Inverses.

d) Die Abbildung

$$\varphi : \mathbb{C} \longrightarrow \mathbb{H} \quad , \quad u \mapsto \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix}$$

ist ein injektiver Ringhomomorphismus. φ ist $\mathbb{R}-$linear, aber nicht $\mathbb{C}-$linear.

$(\mathbb{H}, +, \cdot, \omega)$ heißt die Algebra der (HAMILTONschen) **Quaternionen** .

Beweis : a) Es ist $\mathbb{H} \subset M(2 \times 2, \mathbb{C})$,

$$\mathbb{H} \neq \emptyset \quad \text{wegen} \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{H} \quad . \quad \text{Seien}$$

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}, \begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix} \in \mathbb{H} \quad ,$$

also $u, v, x, y \in \mathbb{C}$. Dann gilt

$$\begin{pmatrix} u, & v \\ -\overline{v}, & \overline{u} \end{pmatrix} - \begin{pmatrix} x, & y \\ -\overline{y}, & \overline{x} \end{pmatrix} = \begin{pmatrix} u - x, & v - y \\ -\overline{v} + \overline{y}, & \overline{u} - \overline{x} \end{pmatrix}$$

$$= \begin{pmatrix} u - x, & v - y \\ -\overline{(v - y)}, & \overline{u - x} \end{pmatrix} \in \mathbb{H} \quad ,$$

$$\begin{pmatrix} u, & v \\ -\overline{v}, & \overline{u} \end{pmatrix} \cdot \begin{pmatrix} x, & y \\ -\overline{y}, & \overline{x} \end{pmatrix} = \begin{pmatrix} u \cdot x - v \cdot \overline{y}, & u \cdot y + v \cdot \overline{x} \\ -\overline{v} \cdot x - \overline{u} \cdot \overline{y}, & -\overline{v} \cdot y + \overline{u} \cdot \overline{x} \end{pmatrix}$$

$$= \begin{pmatrix} u \cdot x - v \cdot \overline{y}, & u \cdot y + v \cdot \overline{x} \\ -\overline{(u \cdot y + v \cdot \overline{x})}, & \overline{(u \cdot x - v \cdot \overline{y})} \end{pmatrix} \in \mathbb{H} \quad ,$$

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\overline{0} & \overline{1} \end{pmatrix} \in \mathbb{H} \quad .$$

b) Sei $\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \in \mathbb{H}$, dann gibt es eindeutig bestimmte $a, b, c, d \in \mathbb{R}$ mit $u = a + ib$, $v = c + id$, also

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} = \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix} = aE_2 + bI + cJ + dK \, .$$

Also ist (E_2, I, J, K) eine Basis von $\mathbb{H}$ als $\mathbb{R}-$Vektorraum. Die Produkte der Basiselemente rechnen wir hier nicht alle aus, vielleicht ein Beispiel:

$$I \cdot J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = K = -J \cdot I \quad .$$

Dass $\mathbb{H}$ die Algebra-Bedingung (L) erfüllt, folgt daraus, dass $M(2 \times 2, \mathbb{C})$ eine $\mathbb{C}-$Algebra ist.

c) Sei $q := \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, dann ist

$$N(q) := u \cdot \overline{u} - v \cdot (-\overline{v}) = u \cdot \overline{u} + v \cdot \overline{v} = |u|^2 + |v|^2 \in \mathbb{R}_+^* \quad .$$

Also ist

$$\frac{1}{N(q)} \begin{pmatrix} \overline{u} & -v \\ \overline{v} & u \end{pmatrix} = \frac{1}{N(q)} \begin{pmatrix} \overline{u} & -v \\ -\overline{(-v)} & \overline{\overline{u}} \end{pmatrix} \in \mathbb{H} \quad ,$$

wobei wir auch noch benutzt haben, dass $\mathbb{H}$ ein $\mathbb{R}-$Vektorraum ist. Es gilt

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \cdot \frac{1}{N(q)} \begin{pmatrix} \overline{u} & -v \\ \overline{v} & u \end{pmatrix} = \frac{1}{N(q)} \begin{pmatrix} u \cdot \overline{u} + v \cdot \overline{v} & -u \cdot v + v \cdot u \\ -\overline{v} \cdot \overline{u} + \overline{v} \cdot \overline{u} & \overline{v} \cdot v + \overline{u} \cdot u \end{pmatrix}$$

$$= \frac{1}{N(q)} \begin{pmatrix} N(q) & 0 \\ 0 & N(q) \end{pmatrix} = E_2$$

und ebenso

$$\frac{1}{N(q)} \begin{pmatrix} \overline{u} & -v \\ \overline{v} & u \end{pmatrix} \cdot \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} = E_2 \quad .$$

Wir haben also

$$q^{-1} = \frac{1}{N(q)} \begin{pmatrix} \overline{u} & -v \\ \overline{v} & u \end{pmatrix} \quad \text{für} \quad q = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \quad .$$

d) Schreiben wir zur Abkürzung $\overset{+}{\cdot}$ für $+$ oder $\cdot$, so gilt für $u, x \in \mathbb{C}$:

$$\varphi(u \overset{+}{\cdot} x) = \begin{pmatrix} u \overset{+}{\cdot} x & 0 \\ 0 & \overline{u \overset{+}{\cdot} x} \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix} \overset{+}{\cdot} \begin{pmatrix} x & 0 \\ 0 & \overline{x} \end{pmatrix} = \varphi(u) \overset{+}{\cdot} \varphi(x) \quad ,$$

und es gilt

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & \overline{1} \end{pmatrix} = E_2 \quad ,$$

φ ist also ein Ring-Homomorphismus, und injektiv wegen

$$\ker \varphi = \{ \ u \in \mathbb{C} \mid \varphi(u) = 0 \ \}$$

$$= \left\{ u \in \mathbb{C} \,\middle|\, \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} = \{0\} \quad .$$

φ ist $\mathbb{R}-$ linear, denn für $\lambda \in \mathbb{R}$, $u \in \mathbb{C}$ gilt

$$\varphi(\lambda\, u) = \begin{pmatrix} \lambda\, u & 0 \\ 0 & \overline{\lambda\, u} \end{pmatrix} = \begin{pmatrix} \lambda\, u & 0 \\ 0 & \lambda\, \overline{u} \end{pmatrix} = \lambda \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix} = \lambda\, \varphi(u)\,.$$

Für $\lambda \in \mathbb{C}$ gilt das zweite Gleichheitszeichen im Allgemeinen nicht!

Bemerkung 4.9.8 : $\mathbb{H}$ erfüllt also alle Körperaxiome, bis auf die Kommutativität von $\cdot\quad,\quad$ was man an den Produkten der Basiselemente sieht. Man nennt $\mathbb{H}$ deshalb auch einen **Schiefkörper** . Wegen (4.9.7) (d) kann man $\mathbb{C}$ als Unterring von $\mathbb{H}$ auffassen. Aber $\mathbb{H}$ ist kein $\mathbb{C}-$Vektorraum, und Körper K mit $\mathbb{C} \overset{\subset}{\neq} K$ und $\dim_{\mathbb{C}} K \in \mathbb{N}$ gibt es ja nach 4.8.3 (6) nicht !

(4.10) Aufgaben

(4.1) a) $\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum mit $\dim_{\mathbb{R}} \mathbb{C} = 2$. Zeigen Sie, dass die Abbildung

$$\overline{} : \mathbb{C} \longrightarrow \mathbb{C} \quad , \quad z \mapsto \overline{z}$$

$\mathbb{R}-$linear ist. Bestimmen Sie $M_{\mathfrak{B}}^{\mathfrak{B}}(\overline{})$ bezüglich der Basis
$a_1)$ $\mathfrak{B} := (1, i)$, $a_2)$ $\mathfrak{B} := (1+i, 1-i)$.
b) Ist $\overline{}$ auch $\mathbb{C}-$linear?

(4.2) (Hier werden einfache Analysis-Kenntnisse vorausgesetzt:)
Im $\mathbb{R}-$Vektorraum $\mathcal{F}(\mathbb{R}, \mathbb{R})$ haben wir die Funktionen $\sin, \cos, \exp$. Zeigen Sie, dass die Familie $\mathfrak{B} := (\sin, \cos, \exp)$ linear unabhängig ist. Sei $V := \operatorname{span}(\mathfrak{B})$ und $D(f) := f'$ für $f \in V$ die erste Ableitung von f. Zeigen Sie, dass durch $D(f) := f'$ eine lineare Abbildung von V nach V definiert ist, und berechnen Sie $B := M_{\mathfrak{B}}^{\mathfrak{B}}(D)$. Besitzt B ein Inverses?

(4.3) Sei V ein $K-$Vektorraum und $\mathfrak{B} = (b_j)_{j \in I}$ eine Basis von V.
Nach Definition 4.3.7 war $V^* = \operatorname{Hom}_K(V, K)$ der Dualraum von V.
Zeigen Sie:

a) Durch $\beta_j(b_k) := \delta_{jk}$, $\delta_{jk} := \begin{cases} 1 & \text{für} \quad j = k \\ 0 & \text{für} \quad j \neq k \end{cases}$ für $j, k \in I$ sind Elemente $\beta_j \in V^*$ definiert, und $\mathfrak{B}^* := (\beta_j)_{j \in I}$ ist in V^* linear unabhängig.

b) Ist $n \in \mathbb{N}$ und $I = \underline{n}$, so ist $\mathfrak{B}^*$ sogar eine Basis von V^* . $\mathfrak{B}^*$ heißt die zu $\mathfrak{B}$ **duale Basis** von V^*.

c) Ist I nicht endlich, so wird durch $\beta(b_j) := 1$ für alle $j \in I$ ein Element aus V^* definiert, für das $\beta \notin \operatorname{span} \mathfrak{B}^*$ gilt.

(4.4) Sei V ein $K-$Vektorraum und V^* der Dualraum von V.
a) Zeigen Sie, dass
$\varphi : V \longrightarrow (V^*)^*$,
$\varphi(a) := f_a$, wobei $f_a(\beta) := \beta(a)$ für $a \in V$, $\beta \in V^*$
ist, ein Vektorraum-Homomorphismus von V in $(V^*)^*$ ist.
b) Sei $\dim_K V \in \mathbb{N}$, dann ist φ sogar ein Isomorphismus. (Man kann Aufgabe (4.3) b) verwenden.)

(4.5) Sei V ein $K-$Vektorraum, U und W seien Untervektorräume von V. Nach Definition 4.7.4 ist

$$U + W := \{ u + w \mid u \in U \wedge w \in W \}$$

ein Untervektorraum von V, und nach Definition 4.7.1 ist

$$U \times W := \{ (u, w) \mid u \in U \wedge w \in W \}$$

ein $K-$Vektorraum. Zeigen Sie :
a) $F : U \times W \longrightarrow U + W$, $F(u, w) := u + w$
ist $K-$linear und surjektiv. Bestimmen Sie $\ker F$.
b) Seien U und W endlichdimensional, dann gilt

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W .$$

(4.6) Seien $a, b \in \mathbb{C}$ und $P(X) := X^2 - a \cdot X - b \in \mathbb{C}[X]$. Zeigen Sie, dass

$$U := \{ (u_n)_{n\in\mathbb{N}_0} \in \mathcal{F}(\mathbb{N}_0, \mathbb{C}) \mid \forall\, n \in \mathbb{N}_0 : u_{n+2} = a \cdot u_{n+1} + b \cdot u_n \}$$

ein Untervektorraum von $\mathcal{F}(\mathbb{N}_0, \mathbb{C})$ ist, und dass gilt:
a) Hat $P(X)$ zwei verschiedene Wurzeln $\lambda, \mu \in \mathbb{C}$,so bilden die Folgen $(\lambda^n)_{n\in\mathbb{N}_0}$ und $(\mu^n)_{n\in\mathbb{N}_0}$ eine Basis von U.
b) Hat $P(X)$ eine zweifache Nullstelle $\lambda \in \mathbb{C}$, gilt also $a^2 + 4b = 0$, und ist $b \neq 0$, so bilden die Folgen $(\lambda^n)_{n\in\mathbb{N}_0}$ und $(n\lambda^n)_{n\in\mathbb{N}_0}$ eine Basis von U.
c) Finden Sie eine Basis von U für den Fall $a = b = 0$.
d) Geben Sie mit a) eine nicht-rekursive Formel zur Berechnung der durch

$$F_0 := 0 \quad , \quad F_1 := 1 \quad , \quad F_{n+2} := F_{n+1} + F_n \quad \text{für} \quad n \in \mathbb{N}_0$$

definierten FIBONACCI-Zahlen an.

(4.7) Bestimmen Sie den Rang von

$$\begin{pmatrix} \frac{1}{2} - \frac{i}{2}\sqrt{3} & 0 & 1 \\ 1 & \frac{1}{2} - \frac{i}{2}\sqrt{3} & 0 \\ 0 & 1 & \frac{1}{2} - \frac{i}{2}\sqrt{3} \end{pmatrix} \in M(3 \times 3, \mathbb{C}) .$$

(4.8) Bestimmen Sie für $n \in \mathbb{N}$ die Lösungsmenge $L \subset \mathbb{R}^n$ des linearen Gleichungssystems

$$\sum_{j=1}^{n} (1 - \delta_{jk}) x_j = 1 \,,\, k \in \underline{n} \quad , \quad \text{wobei} \quad \delta_{jk} = \begin{cases} 1 & \text{für } j = k \\ 0 & \text{für } j \neq k \end{cases} .$$

(4.9) Für welche $\lambda \in \mathbb{R}$ ist die Matrix

$$A := \begin{pmatrix} 1 & \lambda & 0 & 0 \\ \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \end{pmatrix} \in M(4 \times 4, \mathbb{R})$$

invertierbar? Berechnen Sie A^{-1} für diese λ .

(4.10) Eine Matrix $A \in M(3 \times 3, \mathbb{R})$ heißt ein **magisches Quadrat**, wenn es ein $c \in \mathbb{R}$ gibt, so dass alle Zeilensummen, alle Spaltensummen und alle Diagonalsummen gleich c sind. Zeigen Sie, dass die Menge V aller magischen Quadrate ein Untervektorraum von $M(3 \times 3, \mathbb{R})$ ist, und geben Sie eine Basis von V an.
(Tipp: Setzen Sie $a := a_{12}$, $b := a_{21}$ und drücken Sie die anderen Marixelemente durch a, b und c aus.)

(4.11) Konstruieren Sie einen Körper mit 4 Elementen.

(4.12) Im Körper $\mathbb{Z}/_{(5)}$ sei $\overline{a} := a + (5)$ für $a \in \mathbb{Z}$. Bestimmen Sie die Lösungsmenge $L \subset (\mathbb{Z}/_{(5)})^4$ des linearen Gleichungssystems $A \cdot x = b$ für

$$A := \begin{pmatrix} \overline{1} & \overline{3} & \overline{1} & \overline{3} \\ \overline{2} & \overline{2} & \overline{4} & \overline{0} \\ \overline{4} & \overline{1} & \overline{0} & \overline{2} \\ \overline{0} & \overline{2} & \overline{3} & \overline{4} \end{pmatrix} \quad , \quad b := \begin{pmatrix} \overline{0} \\ \overline{1} \\ \overline{2} \\ \overline{0} \end{pmatrix} .$$

(4.13) Sei $n \in \mathbb{N}$. Eine Matrix $A \in M(n \times n, K)$ heißt **nilpotent**, wenn es ein $m \in \mathbb{N}$ mit $A^m = 0$ gibt. Zeigen Sie:

a) A sei eine **echte obere Dreiecksmatrix** , d.h. $A = (a_{kj})$ mit

$$a_{kj} = 0 \quad \text{für} \quad k \geq j \quad ,$$

dann ist A nilpotent.

b) A sei nilpotent. Dann ist $E_n - A$ invertierbar.
(Tipp: Eine Idee liefert die geometrische Reihe aus der Analysis:
Für $q \in \mathbb{R}$ mit $|\, q \,| < 1$ gilt

$$(1-q)^{-1} = \sum_{s=0}^{\infty} q^s \quad . \quad)$$

§5 Determinanten

5.1 Permutationen

(5.1.1) Zur Wiederholung : Schon in (2.2.10) hatten wir für $n \in \mathbb{N}$ die symmetrische Gruppe S_n kennengelernt, das war die Menge aller bijektiven Abbildungen von

$$\underline{n} \;=\; \{1, \ldots, n\}$$

auf sich selbst, mit der Hintereinanderausführung $\circ$ von Abbildungen als Verknüpfung. Die Elemente von S_n hatten wir Permutationen von $\underline{n}$ genannt.
Behauptung (5.1.2) : $\#(S_n) \;=\; n!\,,$
wobei $n!$ für $n \in \mathbb{N}_0$ rekursiv definiert ist durch

$$0! \;:=\; 1 \quad , \quad (n+1)! \;:=\; n! \cdot (n+1) \quad .$$

Beweis : Wir zeigen mit Induktion nach n die folgende, scheinbar allgemeinere Aussage:
$(P(n))$: Seien S, T Mengen mit $\#(S) \;=\; \#(T) \;=\; n\,,\; n \in \mathbb{N}\,,$ dann gibt es genau $n!$ bijektive Abbildungen von S auf T.
Induktionsanfang: Für $n = 1$ hat man je genau ein Element $a \in S, b \in T$, es gibt genau eine bijektive Abbildung von S auf T, nämlich die Abbildung mit $a \mapsto b$. Wegen $1 = 1!$ ist $P(1)$ richtig.
Induktionsschluss : Sei $n \in \mathbb{N}$. Sei nun $\#(S) = n+1$ und $\#(T) = n+1$, dann hat man ein $a \in S$ und $S' := S \setminus \{a\}$, so dass

$$S \;=\; S' \cup \{a\} \quad \text{und} \quad \#(S') \;=\; n$$

ist, und es ist

$$T \;=\; \{b_1, \ldots, b_{n+1}\}$$

mit $n+1$ verschiedenen Elementen $b_1, \ldots, b_{n+1}$. Für $j \in \underline{n+1}$ setzen wir

$$M_j \;:=\; \{\; f : S \;\longrightarrow\; T \;\mid\; f \text{ ist bijektiv und } \; f(a) \;=\; b_j \;\} \quad .$$

Wenn nun $P(n)$ richtig ist, hat M_j genau $n!$ Elemente, nämlich so viele, wie es bijektive Abbildungen von S' auf $T \setminus \{b_j\}$ gibt. Und

$$\{\; f : S \;\longrightarrow\; T \;\mid\; f \text{ ist bijektiv } \;\} \quad = \quad \bigcup_{j=1}^{n+1} M_j \quad ,$$

wobei rechts die Vereinigung elementfremder Mengen steht. Also ist

$$\#(\{\; f : S \;\longrightarrow\; T \;\mid\; f \text{ ist bijektiv } \;\}) \quad = \quad (n+1)\cdot n! \quad = \quad (n+1)! \quad ,$$

was zu beweisen war. Für $S = T = \underline{n}$ erhalten wir die Behauptung.

□

Definition 5.1.3 : Sei $n \in \mathbb{N}$, $\tau \in S_n$ und es gebe $j, k \in \underline{n}$, $j \neq k$, mit
$\tau = (j, k)$,
dann heißt τ eine **Transposition** .
Man sieht, dass für Transpositionen τ gilt
$\tau = \tau^{-1}$.

Satz 5.1.4 : Sei $n \in \mathbb{N}$, dann ist jedes $\sigma \in S_n$ ein Produkt von endlich vielen Zyklen.
Beweis : Für jedes $\sigma \in S_n$ setzen wir

$$B(\sigma) \quad := \quad \{ \ j \in \underline{n} \mid \ \sigma(j) \neq j \ \} \quad .$$

Wir beweisen die Behauptung durch Induktion nach $\#(B(\sigma))$:
Induktionsanfang : Ist $\#(B(\sigma)) = 0$, so ist $\sigma = \mathrm{id}_{\underline{n}} = (1)$.
Induktionsschluss : Sei $k \in \mathbb{N}_0$, und für die $\varphi \in S_n$ mit
$\#(B(\varphi)) \leq k$
sei die Behauptung richtig. Sei $\sigma \in S_n$ mit
$\#(B(\sigma)) = k + 1$, also

$$B(\sigma) \quad = \quad \{a_1, \ldots, a_{k+1}\} \subset \underline{n} \quad ,$$

dann ist $\sigma(a_{k+1})$ gleich einem der a_j mit $j \neq k + 1$ und

$$\tau \quad := \quad (a_j, a_{k+1}) \in S_n \quad . \quad \text{Es gilt}$$

$$(\tau \circ \sigma)(a_{k+1}) \quad = \quad \tau(a_j) \quad = \quad a_{k+1} \quad , \qquad \text{also}$$
$$B(\tau \circ \sigma) \subset \{a_1, \ldots, a_k\} \quad ,$$

denn für die $l \in \underline{n} \setminus \{a_1, \ldots, a_{k+1}\}$ gilt

$$(\tau \circ \sigma)(l) \quad = \quad \tau(l) \quad = \quad l \quad ,$$

sie werden weder von τ noch von σ verändert. Also ist

$$\#(B(\tau \circ \sigma)) \leq k$$

und daher $\tau \circ \sigma$ ein Produkt endlich vieler Zyklen: Es gibt Zyklen $\psi_1, \ldots, \psi_m \in S_n$ mit

$$\tau \circ \sigma \quad = \quad \psi_1 \circ \ldots \circ \psi_m \quad , \quad \text{und wegen} \quad \tau = \tau^{-1} :$$

$$\sigma \quad = \quad \tau \circ \psi_1 \circ \ldots \circ \psi_m \quad .$$

Da auch τ ein Zyklus ist, gilt die Behauptung auch für σ. $\square$

Definition 5.1.5 : Für jedes $\sigma \in S_n$ nennen wir

$$\operatorname{sign} \sigma \quad := \quad \prod_{\substack{(k,j) \in \underline{n} \times \underline{n} \\ \text{mit } k<j}} \frac{\sigma(j) - \sigma(k)}{j - k}$$

das **Signum** von σ .

Folgerung 5.1.6 : Es ist $\operatorname{sign} \sigma \in \{-1, 1\}$, und zwar

$$\operatorname{sign} \sigma \quad = \quad +1 \quad ,$$

wenn die Anzahl der **Fehlstände** von σ , worunter man die Paare

$$(k, j) \in \underline{n} \times \underline{n} \quad \text{mit} \quad k < j \quad , \quad \text{aber} \quad \sigma(k) > \sigma(j)$$

versteht, gerade ist, und

$$\operatorname{sign} \sigma \; = \; -1 \, , \quad ,$$

wenn die Anzahl der Fehlstände von σ ungerade ist.

Beweis : In dem Bruch

$$\prod_{\substack{(k,j) \in \underline{n} \times \underline{n} \\ \text{mit } k<j}} \frac{\sigma(j) - \sigma(k)}{j - k}$$

treten im Nenner für alle zweielementigen Teilmengen $\{k, j\}$ von $\underline{n}$ die Differenzen auf, genau einmal und mit positivem Vorzeichen. Da σ bijektiv ist, sind auch die Mengen $\{\sigma(k), \sigma(j)\}$ mit $(k, j) \in \underline{n} \times \underline{n}$ und $k < j$ alle zweielementigen Teilmengen von $\underline{n}$. Also treten auch im Zähler alle Differenzen $j - k$ auf, aber mit negativem Vorzeichen, wenn $\sigma(j) < \sigma(k)$ ist. Bis auf diese Vorzeichen kürzt sich alles weg, und es bleiben so viele Faktoren (-1) übrig, wie σ Fehlstände hat.

$\square$

Beispiele 5.1.7: In S_3 gilt

a) $\operatorname{sign}(1,2) \quad = \quad \dfrac{(1-2)(3-2)(3-1)}{(2-1)(3-1)(3-2)} \quad = \quad -1 \quad ,$

b) $\operatorname{sign}(1,3,2) \quad = \quad \dfrac{(1-3)(2-3)(2-1)}{(2-1)(3-1)(3-2)} \quad = \quad 1 \quad .$

Satz 5.1.8 : Für $\sigma, \tau \in S_n$ gilt

$$\operatorname{sign}(\tau \circ \sigma) \quad = \quad \operatorname{sign}\tau \cdot \operatorname{sign}\sigma \quad .$$

Beweis : Es gilt

$$\operatorname{sign}(\tau \circ \sigma) = \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{j-k} = a \cdot b \quad \text{mit}$$

$$a := \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{\sigma(j)-\sigma(k)} \quad , \quad b := \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j}} \frac{\sigma(j)-\sigma(k)}{j-k} \quad .$$

Es ist $b = \operatorname{sign}\sigma$, und

$$a = \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j\wedge\sigma(k)<\sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{\sigma(j)-\sigma(k)} \cdot \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j\wedge\sigma(k)>\sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{\sigma(j)-\sigma(k)}$$

$$= \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j\wedge\sigma(k)<\sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{\sigma(j)-\sigma(k)} \cdot \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k>j\wedge\sigma(k)<\sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{\sigma(j)-\sigma(k)} \ ,$$

hier haben wir im zweiten Produkt zuerst die Variablen umbenannt (j in k und k in j) , und dann mit -1 erweitert. Also ist

$$a \quad = \quad \prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } \sigma(k)<\sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(k))}{\sigma(j)-\sigma(k)} \quad ,$$

denn mit $k<j$ und $k>j$ erhält man (wegen $\sigma(k)<\sigma(j)$, also $k \neq j$) alle Paare $(k,j) \in \underline{n} \times \underline{n}$ mit $\sigma(k) < \sigma(j)$. Da σ bijektiv ist, enthält a bis auf die Reihenfolge dieselben Faktoren wie

$$\prod_{\substack{(k,j)\in \underline{n}\times\underline{n} \\ \text{mit } k<j}} \frac{\tau(j)-\tau(k)}{j-k} \quad ,$$

also $a = \operatorname{sign}\tau$.

□

Korollar 5.1.9 : Für alle $\sigma \in S_n$ gilt $\operatorname{sign}\sigma^{-1} = \operatorname{sign}\sigma$.

Beweis : Es ist $\sigma \circ \sigma^{-1} = \mathrm{id}_{\underline{n}}$, also nach 5.1.8 :

$$\operatorname{sign}\sigma \cdot \operatorname{sign}\sigma^{-1} \quad = \quad \operatorname{sign}\mathrm{id}_{\underline{n}} \overset{5.1.6}{=} 1 \quad ,$$

also $\operatorname{sign}\sigma^{-1} = \dfrac{1}{\operatorname{sign}\sigma}$, und wegen $\operatorname{sign}\sigma \in \{1,-1\}$ ist das gleich $\operatorname{sign}\sigma$.

□

Korollar 5.1.10 : Sei $n \in \mathbb{N}$, $n \geq 2$ und $\tau \in S_n$ eine Transposition. Dann ist

$$\operatorname{sign}\tau \quad = \quad -1 \quad .$$

Beweis : Nach Definition 5.1.3 gibt es $k, l \in \underline{n}$ mit $k \neq l$ und

$$\tau \quad = \quad (k,l) \quad .$$

a) Ist $\{k,l\} = \{1,2\}$, so ist

$$\tau \quad = \quad (1,2) \quad \text{und}$$

$$\operatorname{sign}\tau = \prod_{k=1}^{n} \prod_{j=k+1}^{n} \frac{\tau(j)-\tau(k)}{j-k} = \prod_{k=1}^{2} \prod_{j=k+1}^{n} \frac{\tau(j)-\tau(k)}{j-k}$$

$$= \prod_{j=2}^{n} \frac{\tau(j)-2}{j-1} \cdot \prod_{j=3}^{n} \frac{\tau(j)-1}{j-2} = \frac{1-2}{2-1} \cdot \prod_{j=3}^{n} \frac{j-2}{j-1} \cdot \prod_{j=3}^{n} \frac{j-1}{j-2} = -1\,.$$

Haben $\{k,l\}$ und $\{1,2\}$ genau ein Element gemeinsam, etwa $k = 2$, so gilt

$$(l,1) \circ (1,2) \circ (l,1) \quad = \quad (l,2) \quad = \quad (2,l) \quad = \quad (k,l) \quad = \quad \tau \quad , \quad \text{also}$$

$$\operatorname{sign}\tau \;=\; \operatorname{sign}(l,1) \cdot \operatorname{sign}(1,2) \cdot \operatorname{sign}(l,1) \;=\; (-1) \cdot (\operatorname{sign}(l,1))^2 \;=\; -1\,.$$

c) Ist $\{k,l\} \cap \{1,2\} = \emptyset$, so gilt

$$(k,1) \circ (l,2) \circ (1,2) \circ (k,1) \circ (l,2) \quad = \quad (k,l) \quad = \quad \tau \quad , \quad \text{also}$$

$$\operatorname{sign}\tau \;=\; \operatorname{sign}(1,2) \cdot (\operatorname{sign}(k,1))^2 \cdot (\operatorname{sign}(l,2))^2 \;=\; \operatorname{sign}(1,2) \;=\; -1 \quad .$$

□

Hilfssatz 5.1.11 : Ist $n \in \mathbb{N}, n \geq 2$, so gibt es zu jedem $\sigma \in S_n$ Transpositionen $\tau_1, \ldots, \tau_q \in S_n$ mit

$$\sigma \quad = \quad \tau_1 \circ \ldots \circ \tau_q \quad ,$$

also nach Satz 5.1.8 und Korollar 5.1.10 :

$$(*) \quad \operatorname{sign}\sigma \quad = \quad (-1)^q \quad .$$

Weder q noch die Transpositionen $\tau_1, \ldots, \tau_q$ sind eindeutig bestimmt.
Wegen $(*)$ ist durch σ aber festgelegt, ob q gerade oder ungerade ist.

Beweis : Nach Satz 5.1.4 wissen wir, dass σ ein Produkt von endlich vielen Zyklen ist. Wir müssen also nur zeigen, dass jeder Zyklus

$$(a_1, \ldots, a_q) \quad \text{mit verschiedenen Elementen} \quad a_1, \ldots, a_q \in \underline{n}$$

ein Produkt von Transpositionen ist: Man rechnet nach:

$$(a_1, a_q) \circ (a_1, a_{q-1}) \circ \ldots \circ (a_1, a_2) \quad = \quad (a_1, \ldots, a_q) \quad .$$

Dass q nicht eindeutig bestimmt ist, sieht man an

$$\mathrm{id}_{\underline{n}} \quad = \quad (1,2) \circ (1,2) \quad ,$$

hier kann man also $q = 0$ oder $q = 2$ nehmen.

□

Definition und Satz 5.1.12 : Sei $n \in \mathbb{N}$, $n \geq 2$, dann setzen wir

$$A_n \quad := \quad \{ \ \sigma \in S_n \ \mid \ \mathrm{sign}\, \sigma \ = \ 1 \ \} \quad .$$

$(A_n, \circ)$ ist eine Untergruppe von $(S_n, \circ)$ und heißt die
alternierende Gruppe vom Grad n.

A_n enthält $\dfrac{n!}{2}$ Elemente.

Beweis : 1) Nach Definition ist $A_n \subset S_n$, und es ist $A_n \neq \emptyset$ wegen $\mathrm{id}_{\underline{n}} \in A_n$. Seien $\sigma, \tau \in A_n$, dann gilt $\sigma \circ \tau^{-1} \in S_n$ und

$$\mathrm{sign}\,(\sigma \circ \tau^{-1}) \quad = \quad \mathrm{sign}\,\sigma \cdot \mathrm{sign}\,\tau^{-1} \quad = \quad 1 \cdot 1 \quad = \quad 1 \quad ,$$

denn wegen $\tau \circ \tau^{-1} = \mathrm{id}_{\underline{n}}$ ist auch $\mathrm{sign}\ \tau^{-1} = 1$. Also ist $\sigma \circ \tau^{-1} \in A_n$. Also ist A_n eine Untergruppe von $(S_n, \circ)$.
2) Nach dem Satz von Lagrange (2.2.5) haben wir

$$\#(S_n) \ = \ [S_n : A_n] \cdot \#(A_n) \quad ,$$

wobei $[S_n : A_n]$ die Anzahl der Linksnebenklassen von S_n bezüglich A_n ist. Außer A_n selbst gibt es nur noch die Linksnebenklasse $(1,2) \circ A_n$, die aus allen Permutationen aus S_n mit Signum -1 besteht. Also ist $[S_n : A_n] = 2$ und damit $\#(A_n) \quad = \quad \dfrac{1}{2} \#(\, S_n \,) \quad = \quad \dfrac{n!}{2}$.

□

5.2 Definition der Determinante

Definition 5.2.1 : Sei $n \in \mathbb{N}$ und R ein kommutativer Ring. Eine Abbildung

$$\det : \; M(n \times n, R) \;\longrightarrow\; R \quad , \quad A \longmapsto \det A$$

heißt (eine) **Determinante**, falls gilt :

(D1) det ist R **-linear** als Funktion jedes Zeilenvektors. Das soll heißen: Ist $j \in \underline{n}$ fest und gilt für den $j-$ten Zeilenvektor von A:

(a) $a_j = a'_j + a''_j$, so gilt

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} \quad = \quad \det \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ a'_j \\ a_{j+1} \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ a''_j \\ a_{j+1} \\ \vdots \\ a_n \end{pmatrix} \quad ,$$

(b) $a_j = \lambda a'_j$ mit $\lambda \in R$, so gilt

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} \quad = \quad \lambda \det \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ a'_j \\ a_{j+1} \\ \vdots \\ a_n \end{pmatrix} \quad .$$

(D2) det ist **alternierend**, das soll heißen: Gilt

$a_j = a_k$ für zwei Zeilenvektoren a_j, a_k mit $k \neq j$, so ist

$\det A \;=\; 0$.

(D3) det ist **normiert** , d.h. $\det E_n = \det \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 1$.

(5.2.2) Motivation dafür, warum man eine Funktion mit diesen Eigenschaften sucht: Hat man n Vektoren $a_1, \ldots, a_n$ im $\mathbb{R}^n$, so soll das Volumen des von $a_1, \ldots, a_n$ aufgespannten **Parallelotops**

$$P(a_1, \ldots, a_n) \quad := \quad \left\{ \sum_{j=1}^{n} \alpha_j a_j \;\middle|\; \forall\, j \in \underline{n} : \; 0 \leq \alpha_j \leq 1 \right\}$$

gerade die Eigenschaften (D1) - (D3) haben. Für $n = 3$ nennt man ein Parallelotop auch einen **Spat**, und für $n = 2$ ein **Parallelogramm**.

Die Eigenschaften (D1) - (D3) sind dann folgende Eigenschaften, die man von einem Flächeninhalt erwartet:

(D1)(a) Hat man zwei Parallelogramme P' und P'' mit den Seiten
a_1' und a_2 bzw. a_1'' und a_2
mit den Flächeninhalten F' bzw. F'', so hat das Parallelogramm mit den Seiten $a_1' + a_1''$ und a_2 den Flächeninhalt $F' + F''$,

(b) Hat das Parallelogramm mit den Seiten a_1 und a_2 den Flächeninhalt F und ist $\lambda \in \mathbb{R}$, so hat das Parallelogramm mit den Seiten λa_1 und a_2 den Flächeninhalt λF.

(D2) Ein Parallelogramm mit den Seiten a_1 und a_1 hat den Flächeninhalt 0.

(D3) Das Parallelogramm mit den kanonischen Basisvektoren e_1 und e_2 als Seiten hat den Flächeninhalt 1.

□

Bevor wir zeigen, dass es genau eine Abbildung det mit den Eigenschaften (D1) - (D3) gibt, wollen wir aus diesen Eigenschaften einige Folgerungen ziehen:

Satz 5.2.3 : Sei R ein kommutativer Ring, $n \in \mathbb{N}$. Eine Determinante

$$\det : \ M(n \times n, R) \ \longrightarrow \ R$$

hat die folgenden weiteren Eigenschaften:

(D4) Für alle $\lambda \in R$ ist $\det(\lambda A) = \lambda^n \det A$.

(D5) Ist eine Zeile von A der Nullvektor, so ist $\det A = 0$.

(D6) Entsteht B aus A durch eine Zeilenvertauschung, so gilt
$\det B = -\det A$.
(Daher kommt der Name "alternierend" !)
Also: Eine elementare Zeilenumformung vom Typ IV ändert an $\det A$ das Vorzeichen.

(D7) Ist $\lambda \in R$, und entsteht B aus A durch Addition des $\lambda-$fachen der $j-$ten Zeile zur $k-$ten Zeile, $k \neq j$, so ist

$\det B \;=\; \det A\,.$

Also: Eine elementare Zeilenumformung vom Typ III ändert nichts an $\det A\,.$

Beweis : (D4) Nach (D1)(b) , n mal angewendet, gilt

$$\det(\lambda A) \quad = \quad \det \begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix} \quad = \quad \lambda^n \det A \quad .$$

(D5) Ist $j \in \underline{n}$ und $a_j \;=\; 0\,,$ so gilt $a_j \;=\; 0 \cdot a_j\,,$ also nach (D1)(b) :

$\det A \quad = \quad 0 \cdot \det A \quad = \quad 0 \quad .$

(D6) B entstehe aus A durch Vertauschen der Zeilen a_k und a_j . Schreiben wir uns in A und B die unveränderten Zeilen $a_l\,,\; l \notin \{k, j\}\,,$ gar nicht erst hin, so gilt

$$\det A + \det B \quad = \quad \det \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_k \\ \vdots \end{pmatrix} \overset{\text{(D2)}}{=}$$

$$\det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_k \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_k \\ \vdots \end{pmatrix} \overset{\text{(D1)(a)}}{=}$$

$$\det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_j + a_k \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j + a_k \\ \vdots \end{pmatrix} \overset{\text{(D1)(a)}}{=} \det \begin{pmatrix} \vdots \\ a_j + a_k \\ \vdots \\ a_j + a_k \\ \vdots \end{pmatrix} \overset{\text{(D2)}}{=} 0 \quad ,$$

also $\det B \;=\; -\det A\,.$

(D7) Mit derselben Schreibweise wie eben gilt

$$\det B \quad = \quad \det \begin{pmatrix} \vdots \\ a_k + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \overset{\text{(D1)(a)}}{=} \det \begin{pmatrix} \vdots \\ a_k \\ \vdots \\ a_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

$$\overset{\text{(D1)(b)}}{=} \det A + \lambda \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \overset{\text{(D2)}}{=} \det A + 0 \quad .$$

□

Eine Verallgemeinerung von (D6) ist

Korollar 5.2.4 : Sei R ein kommutativer Ring, $n \in \mathbb{N}$, $b_1, \ldots, b_n$ seien (Zeilen-)Vektoren aus R^n und $\sigma \in S_n$. Dann gilt

$$\det \begin{pmatrix} b_{\sigma(1)} \\ \vdots \\ b_{\sigma(n)} \end{pmatrix} \quad = \quad \operatorname{sign} \sigma \cdot \det \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \quad .$$

Beweis : Nach Hilfssatz 5.1.11 gibt es Transpositionen $\tau_1, \ldots, \tau_q \in S_n$ mit

$$\sigma \quad = \quad \tau_1 \circ \ldots \circ \tau_q \quad , \quad \text{und es ist} \quad \operatorname{sign} \sigma \; = \; (-1)^q \quad .$$

Wir zeigen nun

$$(*) \quad \det \begin{pmatrix} b_{(\tau_1 \circ \ldots \circ \tau_q)(1)} \\ \vdots \\ b_{(\tau_1 \circ \ldots \circ \tau_q)(n)} \end{pmatrix} \quad = \quad (-1)^q \det \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

durch Induktion nach q :
Induktionsanfang: Für $q = 0$ ist $(*)$ trivial wegen $\tau_1 \circ \ldots \circ \tau_q \; = \; \mathrm{id}_{\underline{n}}$.
Induktionsschluss : Sei $q \in \mathbb{N}$ und für $q-1$ sei $(*)$ richtig. τ_q ist eine Transposition, etwa $\tau_q = (k, j)$ mit $k, j \in \underline{n}$ und $k \neq j$. Dann ensteht die Matrix

$$A \quad = \quad \begin{pmatrix} b_{(\tau_1 \circ \ldots \circ \tau_q)(1)} \\ \vdots \\ b_{(\tau_1 \circ \ldots \circ \tau_q)(n)} \end{pmatrix} \quad \text{aus} \quad A' \quad := \quad \begin{pmatrix} b_{(\tau_1 \circ \ldots \circ \tau_{q-1})(1)} \\ \vdots \\ b_{(\tau_1 \circ \ldots \circ \tau_{q-1})(n)} \end{pmatrix}$$

durch Vertauschung der k-ten mit der j-ten Zeile, also durch **eine** Vertauschung, also nach (D6) :

$$\det A \;=\; -\det A' \overset{(**)}{=} -(-1)^{q-1} \det \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \;=\; (-1)^q \det \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \quad ,$$

wobei wir bei $(**)$ die Induktionsvoraussetzung benutzt haben.

□

Satz 5.2.5 : Ist $n \in \mathbb{N}$ und R ein kommutativer Ring, so gibt es genau eine Funktion

$$\det : \; M(n \times n, R) \;\longrightarrow\; R$$

mit den Eigenschaften (D1) - (D3) , und zwar die für

$A = (a_{kj}) \in M(n \times n, R)$ durch

$$(*) \quad \det A \;:=\; \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}$$

definierte Funktion.

Bemerkung 5.2.6 : $(*)$ heißt die **Leibniz-Formel** für $\det$. Zur Berechnung von $\det$ ist sie − außer für $n \in \{1, 2\}$ − unpraktisch, da man die Summe über $n!$ Summanden zu bilden hat. Zur Berechnung von $\det$ verwendet man besser die Eigenschaften (D1)-(D7) und weitere Sätze, die folgen.

Beweis von Satz 5.2.5 : (1) Wir zeigen, dass aus (D1) - (D3) die Regel $(*)$ folgt, dass es also für $\det A$ nur eine Möglichkeit gibt, also die Eindeutigkeit von $\det$: Für $l \in \mathbb{N}$ seien die a_l die Zeilenvektoren von A, dann gilt

$$a_l \;=\; a_{l1}e_1 + \ldots + a_{ln}e_n \quad ,$$

wobei $e_1, \ldots, e_n$ die (als Zeilen geschriebenen) kanonischen Basisvektoren von K^n sind, und wir wenden (D1) nacheinander für alle Zeilen an :

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \;=\; \det \begin{pmatrix} \sum_{k_1=1}^{n} a_{1k_1}e_{k_1} \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \;=\; \sum_{k_1=1}^{n} a_{1k_1} \det \begin{pmatrix} e_{k_1} \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

$$= \sum_{k_1=1}^{n} a_{1k_1} \cdot \sum_{k_2=1}^{n} a_{2k_2} \det \begin{pmatrix} e_{k_1} \\ e_{k_2} \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \dots$$

$$= \sum_{k_1=1}^{n} \sum_{k_2=1}^{n} \dots \sum_{k_n=1}^{n} a_{1k_1} a_{2k_2} \cdot \dots \cdot a_{nk_n} \det \begin{pmatrix} e_{k_1} \\ \vdots \\ e_{k_n} \end{pmatrix} .$$

Hier wird also summiert über alle $n-$tupel

$(k_1, \dots, k_n) \in \underline{n}^n$,

also über n^n Summanden. Ist in einem solchen $n-$tupel aber

$k_j = k_l$ für ein Paar $(j,l) \in \underline{n} \times \underline{n}$ mit $j \neq l$,

so ist nach (D2)

$$\det \begin{pmatrix} e_{k_1} \\ \vdots \\ e_{k_j} \\ \vdots \\ e_{k_l} \\ \vdots \\ e_{k_n} \end{pmatrix} = 0 .$$

Wir müssen also nur summieren über die $n-$tupel $(k_1, \dots, k_n)$, für die die Abbildung

$\sigma : \underline{n} \longrightarrow \underline{n}$, $\sigma(j) := k_j$

injektiv ist, also, da $\underline{n}$ endlich ist, bijektiv ist. Also ist

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)} \cdot \det \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix} ,$$

und nach Korollar 5.2.4 :

$$\det A = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)} \cdot \operatorname{sign} \sigma \cdot \det \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} ,$$

und aus (D3) folgt $(*)$.

Um die Existenz einer Funktion det mit den Eigenschaften (D1) - (D3) zu

zeigen, **definieren** wir $\det A$ durch die Leibniz-Formel $(*)$ und zeigen, dass das so definierte $\det A$ die Eigenschaften (D1) - (D3) hat:

(D1)(a) Ersetzt man in A die Zeile a_j durch $a'_j + a''_j$, so erhält man aus $(*)$

$$\begin{aligned}
\det \begin{pmatrix} \vdots \\ a'_j + a''_j \\ \vdots \end{pmatrix} &= \sum_{\sigma \in S_n} \operatorname{sign}\sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot (a'_{j\sigma(j)} + a''_{j\sigma(j)}) \cdot \ldots \cdot a_{n\sigma(n)} \\
&= \sum_{\sigma \in S_n} \operatorname{sign}\sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot a'_{j\sigma(j)} \cdot \ldots \cdot a_{n\sigma(n)} \\
&\quad + \sum_{\sigma \in S_n} \operatorname{sign}\sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot a''_{j\sigma(j)} \cdot \ldots \cdot a_{n\sigma(n)} \\
&= \det \begin{pmatrix} a_1 \\ \vdots \\ a'_j \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a''_j \\ \vdots \\ a_n \end{pmatrix} \quad ,
\end{aligned}$$

(b) Ersetzt man a_j durch λa_j, $\lambda \in R$, so wird

$$\begin{aligned}
\det \begin{pmatrix} \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} &= \sum_{\sigma \in S_n} \operatorname{sign}\sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot \lambda a_{j\sigma(j)} \cdot \ldots \cdot a_{n\sigma(n)} \\
&= \lambda \sum_{\sigma \in S_n} \operatorname{sign}\sigma \, a_{1\sigma(1)} \cdot \ldots \cdot a_{j\sigma(j)} \cdot \ldots \cdot a_{n\sigma(n)} \\
&= \lambda \det \begin{pmatrix} \vdots \\ a_j \\ \vdots \end{pmatrix} \quad .
\end{aligned}$$

(D2) Sei A eine Matrix, in der die $k-$te und die $l-$te Zeile gleich sind, etwa $k < l$. Sei τ die Transposition (k, l), dann ist

$$S_n = A_n \cup A_n \circ \tau \text{ und } A_n \cap A_n \circ \tau = \emptyset .$$

Für $\sigma \in A_n$ ist $\operatorname{sign}\sigma = 1$. Wenn σ die Gruppe A_n durchläuft, durchläuft $\sigma \circ \tau$ die Menge $A_n \circ \tau$, und es ist $\operatorname{sign}(\sigma \circ \tau) = -1$. Also ist

$$(**) \quad \det A = \sum_{\sigma \in A_n} a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} - \sum_{\sigma \in A_n} a_{1\sigma(\tau(1))} \cdot \ldots \cdot a_{n\sigma(\tau(n))} \quad .$$

Die $k-$te und die $l-$te Zeile sind gleich, also gilt wegen $\tau = (k,l)$:

$$\begin{array}{ccccccccccccc} a_{1\sigma(\tau(1))} & \cdot & \ldots & \cdot & a_{k\sigma(\tau(k))} & \cdot & \ldots & \cdot & a_{l\sigma(\tau(l))} & \cdot & \ldots & \cdot & a_{n\sigma(\tau(n))} \\ a_{1\sigma(1)} & \cdot & \ldots & \cdot & a_{k\sigma(l)} & \cdot & \ldots & \cdot & a_{l\sigma(k)} & \cdot & \ldots & \cdot & a_{n\sigma(n)} \\ a_{1\sigma(1)} & \cdot & \ldots & \cdot & a_{l\sigma(l)} & \cdot & \ldots & \cdot & a_{k\sigma(k)} & \cdot & \ldots & \cdot & a_{n\sigma(n)} \\ a_{1\sigma(1)} & \cdots & \ldots & \cdot & a_{k\sigma(k)} & \cdot & \ldots & \cdot & a_{l\sigma(l)} & \cdot & \ldots & \cdot & a_{n\sigma(n)} \end{array} \begin{array}{c} = \\ \downarrow \\ = \\ = \\ , \end{array}$$

im letzten Schritt haben wir die Kommutativität von $(K,\cdot)$ benutzt. In $(**)$ heben sich also immer zwei Summanden gegenseitig auf, es ist

$$\det A \quad = \quad 0 \quad .$$

(D3) Es ist $E_n = (\delta_{kj})$ mit $\delta_{kj} = \begin{cases} 1 & \text{für } k = j \\ 0 & \text{für } k \neq j \end{cases}$ also nach $(*)$:

$$\det E_n \quad = \quad \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot \delta_{1\sigma(1)} \cdot \ldots \cdot \delta_{n\sigma(n)} \quad .$$

Ist nun $\sigma \neq \mathrm{id}_{\underline{n}}$, so steht im Produkt $\delta_{1\sigma(1)} \cdot \ldots \cdot \delta_{n\sigma(n)}$ ein Faktor $\delta_{j\sigma(j)}$ mit $\sigma(j) \neq j$, also 0 . Also ist

$$\det E_n \quad = \quad \operatorname{sign} \mathrm{id}_{\underline{n}} \cdot \delta_{11} \cdot \ldots \cdot \delta_{nn} \quad = \quad 1 \quad .$$

□

Korollar 5.2.7 : Sei $n \in \mathbb{N}$, R ein kommutativer Ring und $A \in M(n \times n, R)$. Dann gilt

$$\det {}^t A \quad = \quad \det A \quad .$$

Beweis : Für $A = (a_{kj})$ ist ${}^t A = (a'_{kj})$ mit $a'_{kj} = a_{jk}$, also nach der Leibniz-Formel:

$$\begin{aligned} \det {}^t A \quad &= \quad \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot a'_{1\sigma(1)} \cdot \ldots \cdot a'_{n\sigma(n)} \\ &= \quad \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot a_{\sigma(1)1} \cdot \ldots \cdot a_{\sigma(n)n} \end{aligned}$$

Da $(R,\cdot)$ kommutativ ist, gilt für $b_1, \ldots, b_n \in R$:

$$\prod_{j=1}^{n} b_j \quad = \quad \prod_{j=1}^{n} b_{\sigma^{-1}(j)} \quad , \quad \text{also folgt}$$

$$\det {}^t A \quad = \quad \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot a_{\sigma(\sigma^{-1}(1)),\sigma^{-1}(1)} \cdot \ldots \cdot a_{\sigma(\sigma^{-1}(n)),\sigma^{-1}(n)}$$

und wegen $\operatorname{sign}\sigma = \operatorname{sign}\sigma^{-1}$:

$$\det {}^tA \quad = \quad \sum_{\sigma\in S_n} \operatorname{sign}\sigma^{-1}\cdot a_{1,\sigma^{-1}(1)}\cdot \ldots \cdot a_{n,\sigma^{-1}(n)}$$

Da die Abbildung $S_n \longrightarrow S_n\,,\ \sigma \longmapsto \sigma^{-1}$ bijektiv ist, können wir den "Summationsindex" σ^{-1} durch σ ersetzen :

$$\begin{aligned}\det {}^tA \quad &= \quad \sum_{\sigma^{-1}\in S_n} \operatorname{sign}\sigma\cdot a_{1\sigma(1)}\cdot \ldots \cdot a_{n\sigma(n)} \\ &= \quad \sum_{\sigma\in S_n} \operatorname{sign}\sigma\cdot a_{1\sigma(1)}\cdot \ldots \cdot a_{n\sigma(n)} \quad = \quad \det A \quad . \qquad \square\end{aligned}$$

Korollar 5.2.8 : Die Aussagen (D1) - (D7) für die Determinante bleiben richtig, wenn man überall "Zeile" durch "Spalte" ersetzt.

5.3 Der Laplacesche Entwicklungssatz

Definition 5.3.1 : Sei $n \in \mathbb{N}$ und R ein kommutativer Ring,
$A \in M(n\times n, R)$ und seien $j,k \in \underline{n}$ fest. Dann bezeichnen wir mit A'_{jk} die Matrix, die aus A durch Streichen der $j-$ten Zeile und $k-$ten Spalte entsteht, also

$$A'_{jk} := \left(\begin{array}{ccc|ccc} a_{11} & \ldots & a_{1,k-1} & a_{1,k+1} & \ldots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{j-1,1} & \ldots & a_{j-1,k-1} & a_{j-1,k+1} & \ldots & a_{j-1,n} \\ \hline a_{j+1,1} & \ldots & a_{j+1,k-1} & a_{j+1,k+1} & \ldots & a_{j+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \ldots & a_{n,k-1} & a_{n,k+1} & \ldots & a_{nn} \end{array}\right) \in M((n-1)\times(n-1), K) \quad .$$

Hilfssatz 5.3.2 : Sei $n \in \mathbb{N}$, R ein kommutativer Ring. Seien $j,k \in \underline{n}$ fest, und die Matrix $A \in M(n\times n, R)$ habe als $j-$ten Zeilenvektor den Vektor $e_k = (\delta_{kl})_{l\in\underline{n}}$, es sei also

$$A \quad = \quad \left(\begin{array}{ccccc} a_{11} & \ldots & a_{1k} & \ldots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{j-1,1} & \ldots & a_{j-1,k} & \ldots & a_{j-1,n} \\ 0 & \ldots & 1 & \ldots & 0 \\ a_{j+1,1} & \ldots & a_{j+1,k} & \ldots & a_{j+1,n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \ldots & a_{nk} & \ldots & a_{nn} \end{array}\right) \quad .$$

Dann gilt

$$\det A \quad = \quad (-1)^{j+k} \det A'_{jk} \quad .$$

Beweis : 1) Im Spezialfall $j = k = n$ hat man

$$A \quad = \quad \begin{pmatrix} a_{11} & \dots & a_{1,n-1} & a_{1n} \\ \vdots & & \vdots & \vdots \\ a_{n-1,1} & \dots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \dots & 0 & 1 \end{pmatrix} \quad .$$

Nach der LEIBNIZ - Formel ist

$$\det A \quad = \quad \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \quad .$$

Ist nun $\sigma \in S_n$ mit $\sigma(n) \neq n$, so ist $a_{n\sigma(n)} = 0$. Wir müssen also nur über die $\sigma \in S_n$ mit $\sigma(n) = n$ summieren. Für diese ist

$$\sigma' : \underline{n-1} \longrightarrow \underline{n-1} \quad , \quad \sigma'(l) := \sigma(l)$$

ein Element aus S_{n-1} , die Abbildung

$$' : \{ \sigma \in S_n \mid \sigma(n) = n \} \longrightarrow S_{n-1} \quad , \quad \sigma \longmapsto \sigma'$$

ist eine Bijektion, und es gilt noch $\operatorname{sign} \sigma' = \operatorname{sign} \sigma$. Also ist

$$\begin{aligned} \det A \quad &= \quad \sum_{\sigma' \in S_{n-1}} \operatorname{sign} \sigma' \cdot a_{1\sigma'(1)} \cdot \ldots \cdot a_{n-1,\sigma'(n-1)} \cdot 1 \\ &= \quad \det A'_{nn} \quad = \quad (-1)^{n+n} \det A'_{nn} \quad , \end{aligned}$$

in diesem Fall ist die Behauptung also richtig.
2) Seien nun $j, k \in \underline{n}$ beliebig. Durch $n-j$ Zeilenvertauschungen in A bringen wir die Zeile e_k nach unten, das gibt nach (D6) $n-j$ Vorzeichenwechsel. Nun bringen wir durch $n-k$ Spaltenvertauschungen die unten stehende 1 nach hinten, das gibt nach (D6) und Korollar 5.2.8 $n-k$ Vorzeichenwechsel. Dann können wir 1) anwenden auf die Matrix

$$\left(\begin{array}{ccc|c} & & & a_{1k} \\ & & & \vdots \\ & & & a_{j-1,k} \\ & A'_{jk} & & - \\ & & & a_{j+1,k} \\ & & & \vdots \\ & & & a_{nk} \\ \hline - & - & - & - \\ 0 & \dots & 0 & 1 \end{array} \right)$$

und erhalten insgesamt :

$$\det A \quad = \quad (-1)^{n-j} \cdot (-1)^{n-k} \det A'_{jk} \quad = \quad (-1)^{j+k} \det A'_{jk} \,. \qquad \square$$

Satz 5.3.3 (Laplacescher Entwicklungssatz) : Sei R ein kommutativer Ring, $n \in \mathbb{N}$, $n \geq 2$ und $A \in M(n \times n, R)$. Dann gilt für feste $j, k, l \in \underline{n}$:

$$(1) \qquad \sum_{s=1}^{n} a_{sl} \cdot (-1)^{s+j} \det A'_{sj} \quad = \quad \delta_{lj} \cdot \det A \,,$$

für $l = j$ nennt man diese Formel die "Entwicklung von det A nach der $j-$ten Spalte", und

$$(2) \qquad \sum_{s=1}^{n} a_{ls} \cdot (-1)^{k+s} \det A'_{ks} \quad = \quad \delta_{lk} \cdot \det A \,,$$

für $l = k$ heißt das "Entwicklung von det A nach der $k-$ten Zeile ".

Beweis : (2) Für die $k-$te Zeile a_k von A gilt

$$a_k \,=\, \sum_{s=1}^{n} a_{ks}\, e_s \quad \text{mit den Zeilenvektoren} \quad e_s \,=\, (0, \ldots, 0, \underset{\substack{\uparrow \\ s-\text{te Stelle}}}{1}\, 0, \ldots, 0) \quad ,$$

${}^t e_s \in K^n$. Nach (D1) ist det linear als Funktion der $k-$ten Zeile, also

$$(*) \qquad \det A \quad = \quad \det \begin{pmatrix} a_1 \\ \vdots \\ a_{k-1} \\ \sum\limits_{s=1}^{n} a_{ks}\, e_s \\ a_{k+1} \\ \vdots \\ a_n \end{pmatrix} \quad = \quad \sum_{s=1}^{n} a_{ks} \underbrace{\det \begin{pmatrix} a_1 \\ \vdots \\ a_{k-1} \\ e_s \\ a_{k+1} \\ \vdots \\ a_n \end{pmatrix}}_{= (-1)^{k+s} \det A'_{ks}}$$

nach Hilfssatz 5.3.2. Für $l = k$ haben wir damit (2) bewiesen. Für $l \neq k$ betrachten wir statt A die Matrix B, die aus A entsteht, wenn man die $k-$te Zeile durch die $l-$te Zeile ersetzt. B hat dann zwei gleiche Zeilen, also gilt nach (D2) :

$$\det B \quad = \quad 0 \quad .$$

Entwickeln wir nun B nach der $k-$ten Zeile, so erhalten wir nach $(*)$:

$$0 \quad = \quad \sum_{s=1}^{n} a_{ls}\, (-1)^{k+s} \det A'_{ks} \quad ;$$

wegen $\delta_{lk} = 0$ also (2) in diesem Fall.
(1) folgt nach Kor. 5.2.7 durch Vertauschen von Zeilen und Spalten aus (2). □
Es mag merkwürdig erscheinen, den Laplaceschen Entwicklungssatz auch hinzuschreiben für $l \neq j$ bzw. $l \neq k$. Man erhält damit aber sofort den

Satz 5.3.4 : Sei R ein kommutativer Ring, $n \in \mathbb{N}$ und $A \in M(n \times n, R)$. Sei $\det A \in R^\times$, dann besitzt A die inverse Matrix

$$A^{-1} = (c_{kj})_{(k,j)\in \underline{n}\times\underline{n}} \quad \text{mit} \quad c_{kj} := (\det A)^{-1} \cdot (-1)^{k+j} \det A'_{jk} \quad .$$

Beweis : Mit den so definierten c_{kj} gilt nach den Formeln (1) und (2) im Laplaceschen Entwicklungssatz für $j, k, l \in \underline{n}$:

$$(1) \quad \sum_{s=1}^{n} c_{js} a_{sl} = \delta_{jl} \quad , \quad (2) \quad \sum_{s=1}^{n} a_{ls} c_{sk} = \delta_{lk} \quad , \quad \text{also}$$

$$C \cdot A = E_n \quad , \quad A \cdot C = E_n \quad ,$$

also $C = A^{-1}$.

□

(5.3.5) Bemerkungen : 1) Man beachte die Indexvertauschung:

$$c_{kj} = (\det A)^{-1}(-1)^{k+j} \det A'_{jk} \quad .$$

2) Sei R ein Körper. Zur numerischen Berechnung von A^{-1} ist Satz 5.3.4 für $n \geq 3$ ungeeignet, da man n^2 Determinanten ausrechnen muss. Das als Anwendung 4.6.13 angegebene Verfahren geht schneller. Aber für theoretische Zwecke ist es gut, dass man überhaupt eine Formel zur Berechnung von A^{-1} hat.
3) Sei R ein kommutativer Ring. Für

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2\times 2, R) \quad \text{mit} \quad \det A = ad - bc \in R^\times \quad \text{erhält man}$$

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \quad .$$

□

Satz 5.3.6 (Determinanten-Multiplikationssatz) : Sei $n \in \mathbb{N}$, R ein kommutativer Ring und seien $A, B \in M(n \times n, R)$. Dann gilt

$$\det(A \cdot B) = \det A \cdot \det B$$

Beweis : Sei $A = (a_{lk})_{(l,k)\in \underline{n}\times\underline{n}}$, $B = (b_{kj})_{(k,j)\in\underline{n}\times\underline{n}}$, dann ist

$$A \cdot B \quad = \quad (c_{lj}) \quad \text{mit} \quad c_{lj} \quad = \quad \sum_{k=1}^{n} a_{lk} b_{kj} \, ,$$

$A \cdot B$ hat also die Zeilenvektoren

$$c_l \quad = \quad \sum_{k=1}^{n} a_{lk} \, b_k \, ,$$

wobei $b_k = (b_{k1}, \ldots, b_{kn})$ der $k-$te Zeilenvektor von B ist. Also gilt

$$\det(A \cdot B) \quad = \quad \det \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \quad = \quad \det \begin{pmatrix} \sum\limits_{k_1=1}^{n} a_{1k_1} \, b_{k_1} \\ \vdots \\ \sum\limits_{k_n=1}^{n} a_{nk_n} \, b_{k_n} \end{pmatrix}$$

$$\overset{(D1)}{=} \quad \sum_{k_1=1}^{n} \ldots \sum_{k_n=1}^{n} a_{1k_1} \cdot \ldots \cdot a_{nk_n} \, \det \begin{pmatrix} b_{k_1} \\ \vdots \\ b_{k_n} \end{pmatrix} \quad .$$

Wir summieren also über alle $n-$tupel $k := (k_1, \ldots, k_n) \in \underline{n}^n$:

$$\det(A \cdot B) \quad = \quad \sum_{k\in\underline{n}^n} a_{1k_1} \cdot \ldots \cdot a_{nk_n} \, \det \begin{pmatrix} b_{k_1} \\ \vdots \\ b_{k_n} \end{pmatrix} \quad .$$

Da $\det$ alternierend ist , also wegen (D2) , ist

$$\det \begin{pmatrix} b_{k_1} \\ \vdots \\ b_{k_n} \end{pmatrix} \quad = \quad 0 \quad , \quad \text{falls es} \quad r, s \in \underline{n} \ \text{mit} \ r \neq s \ \text{und} \ k_r = k_s \ \text{gibt,}$$

wir müssen also nur über die $n-$tupel summieren, für die

$$\sigma : \ \underline{n} \ \longrightarrow \ \underline{n} \quad , \quad \sigma(r) := k_r \quad \text{bijektiv ist :}$$

$$\det(A \cdot B) \quad = \quad \sum_{\sigma\in S_n} a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \cdot \det \begin{pmatrix} b_{\sigma(1)} \\ \vdots \\ b_{\sigma(n)} \end{pmatrix} \quad ,$$

also nach Korollar 5.2.4 :

$$\det(A \cdot B) \quad = \quad \underbrace{\sum_{\sigma \in S_n} a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \cdot \operatorname{sign}(\sigma)}_{\det A} \cdot \underbrace{\det \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_{\det B} \quad ,$$

wobei wir hier für $\det A$ die LEIBNIZ-Formel verwendet haben.

□

Folgerung 5.3.7 : Sei $n \in \mathbb{N}$, R ein kommutativer Ring. Eine Matrix $A \in M(n \times n, R)$ ist genau dann invertierbar, wenn $\det A \in R^\times$ ist, also $\det A$ invertierbar in R.

Beweis : 1) Sei $\det A \in R^\times$, dann existiert

$$A^{-1} \; = \; (\det A)^{-1} \, \left((-1)^{k+j} \, \det A'_{jk} \right)_{(k,j) \in \underline{n} \times \underline{n}}$$

nach Satz 5.3.4.

2) Ist A invertierbar, so existiert $A^{-1} \in M(n \times n, R)$ mit

$A \cdot A^{-1} \; = \; E_n \quad , \quad$ also nach Satz 5.3.6 :

$\det A \cdot \det A^{-1} \; = \; \det E_n \overset{(D3)}{=} 1 \quad , \quad$ also $\det A \in R^\times \quad .$

□

Satz 5.3.8 : Sei $n \in \mathbb{N}$, R ein kommutativer Ring. Die Determinante

$$\det \; : \; M(n \times n, R) \; \longrightarrow \; R$$

hat noch die Eigenschaften:

(D8) Ist A eine obere Dreiecksmatrix, also

$$A \quad = \quad \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit} \quad \lambda_1, \ldots, \lambda_n \in R$$

und irgendwelchen Elementen aus R bei $*$,

so ist $\det A \; = \; \lambda_1 \cdot \ldots \cdot \lambda_n \quad .$

(D9) Sei $A \in M(n \times n, R) \quad , \quad n \geq 2 \quad , \quad$ von der Form

$$A \quad = \quad \begin{pmatrix} B & | & C \\ - & + & - \\ 0 & | & D \end{pmatrix} \quad , \quad \text{wobei} \quad B \quad \text{und} \quad D \quad \text{quadratisch sind, so gilt}$$

$$\det A \quad = \quad \det B \cdot \det D \quad .$$

Beweis : (D9) Sei $B \in M(r \times r, R)$, $D \in M((n-r) \times (n-r), R)$, mit $1 \leq r < n$, dann haben wir

$$A \quad = \quad \left(\begin{array}{ccc} B & | & C \\ - & + & - \\ 0 & | & D \end{array}\right) \quad = \quad \left(\begin{array}{ccc} E_r & | & C \\ - & + & - \\ 0 & | & D \end{array}\right) \cdot \left(\begin{array}{ccc} B & | & 0 \\ - & + & - \\ 0 & | & E_{n-r} \end{array}\right) \quad ,$$

wie man mit der Definition des Matrizenprodukts nachrechnet, also mit

$$D' \quad := \quad \left(\begin{array}{ccc} E_r & | & C \\ - & + & - \\ 0 & | & D \end{array}\right) \quad , \quad B' \quad := \quad \left(\begin{array}{ccc} B & | & 0 \\ - & + & - \\ 0 & | & E_{n-r} \end{array}\right) :$$

$$\det A \quad = \quad \det D' \cdot \det B'$$

nach dem Determinanten-Multiplikationssatz 5.3.6 . Entwickelt man
det D' nacheinander nach der 1. bis $r-$ten Spalte und
det B' nacheinander nach der $n-$ten bis $(r+1)-$ten Spalte,
so erhält man:

$$\det D' \quad = \quad \det D \quad , \quad \det B' \quad = \quad \det B \quad , \quad \text{also die Beh.}$$

(D8) folgt aus (D9) durch Induktion nach n : Für $n = 1$ gilt

$$\det A \quad = \quad \det(\lambda_1) \quad = \quad \lambda_1 \quad \text{nach der Leibniz-Formel,}$$

und wenn (D8) für $n - 1 \in \mathbb{N}$ richtig ist , folgt nach (D9) :

$$\det \left(\begin{array}{cccc} \lambda_1 & & * & | \\ & \ddots & & | \quad * \\ 0 & & \lambda_{n-1} & | \\ - & - & - & + \quad - \\ & 0 & & | \quad \lambda_n \end{array}\right) \quad = \quad \det \left(\begin{array}{ccc} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_{n-1} \end{array}\right) \cdot \det(\lambda_n)$$

$$= \quad \lambda_1 \cdot \ldots \cdot \lambda_{n-1} \cdot \lambda_n \quad .$$

□

5.4 Determinante eines Endomorphismus

Definition 5.4.1 : Sei V ein $K-$Vektorraum mit $\dim_K V = n$, $n \in \mathbb{N}$, K ein Körper, und

$F \in \mathrm{End}_K V = \mathrm{Hom}_K(V, V)$,

also nach Definition 4.3.8 : F ein Endomorphismus von V . Sei $\mathfrak{A}$ eine Basis von V , dann ist

$$A \quad := \quad M_{\mathfrak{A}}^{\mathfrak{A}}(F) \in M(n \times n, K)$$

nach Formel (4.4.12) definiert. Bezüglich einer anderen Basis $\mathfrak{B}$ von V haben wir

$$B \quad := \quad M_{\mathfrak{B}}^{\mathfrak{B}}(F) \in M(n \times n, K) \quad ,$$

und nach der Formel (4.4.17) für die Koordinatentransformation haben wir

$$B \quad = \quad S \cdot A \cdot S^{-1}$$

mit $S = M_{\mathfrak{A}}^{\mathfrak{B}}(\mathrm{id}_V) \in \mathrm{GL}(n, K)$, also nach dem Determinanten - Multiplikationssatz 5.3.6 :

$$\begin{aligned} \det B &= \det S \cdot \det A \cdot \det(S^{-1}) \\ &= \det S \cdot \det S^{-1} \cdot \det A = \det(S \cdot S^{-1}) \cdot \det A \\ &= \det E_n \cdot \det A = \det A, \end{aligned}$$

die Determinante $\det M_{\mathfrak{A}}^{\mathfrak{A}}(F)$ ist also unabhängig davon, welche Basis $\mathfrak{A}$ von V wir nehmen, und wir können

$$\det F \quad := \quad \det M_{\mathfrak{A}}^{\mathfrak{A}}(F) \tag{5.4.2}$$

setzen, wobei es egal ist, welche Basis $\mathfrak{A}$ von V wir wählen.

Folgerung 5.4.3 : Sei V ein $n-$dimensionaler $K-$Vektorraum, K ein Körper, $n \in \mathbb{N}$, dann sind für einen Endomorphismus $F : V \longrightarrow V$ die folgenden Eigenschaften gleichbedeutend :

(i) F ist ein Vektorraum-Automorphismus, d.h. F ist bijektiver Endomorphismus.

(ii) $\det F \neq 0$.

Beweis : Sei $\mathfrak{A}$ eine Basis von V , dann gilt:

$$\begin{aligned} & F \text{ ist Automorphismus von } V \\ \iff & \exists\, G \in \mathrm{End}(V) : \; G \circ F \quad = \quad F \circ G \quad = \quad \mathrm{id}_V \\ \iff & \exists\, G \in \mathrm{End}(V) : \; M_{\mathfrak{A}}^{\mathfrak{A}}(G) \cdot M_{\mathfrak{A}}^{\mathfrak{A}}(F) = M_{\mathfrak{A}}^{\mathfrak{A}}(F) \cdot M_{\mathfrak{A}}^{\mathfrak{A}}(G) = E_n \\ \overset{(*)}{\iff} & M_{\mathfrak{A}}^{\mathfrak{A}}(F) \in \mathrm{GL}(n, K) \\ \overset{(5.3.7)}{\iff} & \det M_{\mathfrak{A}}^{\mathfrak{A}}(F) \neq 0 \\ \overset{(5.4.2)}{\iff} & \det F \neq 0 \quad . \end{aligned}$$

Bei $(*)$, "$\Longleftarrow$" benutzen wir, dass

$$M_{\mathfrak{A}}^{\mathfrak{A}} \;:\; \mathrm{End}_K(V) \;\longrightarrow\; M(n\times n, K)$$

ein Vektorraumisomorphismus ist, zu $B := (M_{\mathfrak{A}}^{\mathfrak{A}}(F))^{-1}$ hat man also ein $G \in \mathrm{End}_K(V)$ mit

$$M_{\mathfrak{A}}^{\mathfrak{A}}(G) = B \quad .$$

□

5.5 Aufgaben

(5.1) Sei K ein Körper, $n \in \mathbb{N}$ und $a_1, \ldots, a_n, b_1, \ldots, b_n \in K$. Berechnen Sie die Determinante D von

a)
$$\begin{pmatrix} 1 & 1 & 1 & \ldots & & 1 \\ b_1 & a_1 & a_1 & \ldots & & a_1 \\ b_1 & b_2 & a_2 & \ldots & & a_2 \\ & & b_3 & & & \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ b_1 & b_2 & b_3 & \ldots & b_n & a_n \end{pmatrix} ,$$

b)
$$\begin{pmatrix} a_1+b_1 & b_2 & b_3 & & \ldots & b_n \\ b_1 & a_2+b_2 & b_3 & & \ldots & b_n \\ b_1 & b_2 & a_3+b_3 & b_4 & \ldots & b_n \\ & & b_3 & \ddots & & \vdots \\ \vdots & \vdots & \vdots & & \ddots & b_n \\ b_1 & b_2 & b_3 & \ldots & b_{n-1} & a_n+b_n \end{pmatrix} ,$$

c) $(1-\delta_{jk})_{(j,k)\in \underline{n}\times\underline{n}}$.

(5.2) Sei K ein Körper, 1 das Einselement von K und $a, b \in M(n\times 1, K)$. Zeigen Sie :

$$\det(E_n + a \cdot {}^t b) \quad = \quad 1 + {}^t a \cdot b \quad .$$

(5.3) Sei K ein Körper, $n \in \mathbb{N}$, $\mathrm{char}\, K \neq 2$ und $A \in M(n\times n, K)$ **schiefsymmetrisch** , d.h. $A = -{}^t A$. Zeigen Sie:

a) Ist n ungerade, so ist $\det A = 0$.

b) Ist n gerade, so ist $\det A$ ein Quadrat in K. Zeigen Sie dazu, dass man A für $n > 2$ durch elementare Zeilen- und Spaltenumformungen auf die Form

$$\begin{pmatrix} 0 & \alpha & \\ & & 0 \\ -\alpha & 0 & \\ & & \\ & * & B \end{pmatrix}$$

mit $\alpha \in K$ und einer schiefsymmetrischen Matrix B bringen kann, und machen Sie Induktion.

(5.4) Sei K ein Körper, $n \in \mathbb{N}$, $A \in \mathrm{GL}(n,K)$ und $b \in M(n \times 1, K)$ ein Spaltenvektor. Dann hat das lineare Gleichungssystem

$$A \cdot x \;=\; b$$

die eindeutig bestimmte Lösung

$$x \;=\; A^{-1} \cdot b \quad \text{mit} \quad x \;=\; (x_j)_{j \in \underline{n}} \quad \text{und}$$

$$x_j \;=\; (\det A)^{-1} \cdot \det B_j \,,$$

wobei B_j die Matrix ist, die man erhält, wenn man aus A die $j-$te Spalte herausnimmt und sie durch den Spaltenvektor b ersetzt (**Cramer**sche Regel).
Achtung: Obwohl diese Regel elegant aussieht, sollte man sie nicht zum Lösen linearer Gleichungssysteme benutzen: Man kann zeigen, dass der Rechenaufwand dabei proportional zu n^3 ist, bei dem in (4.6.10) beschriebenen GAUSSschen Eliminationsverfahren aber nur proportional zu n^2 - abgesehen davon, dass (4.6.10) auch funktioniert, wenn das System nicht eindeutig lösbar ist.

(5.5) Sei K ein Körper, $a, b, c, d \in K$. Zeigen Sie:

$$\det \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \;=\; (a^2+b^2+c^2+d^2)^2 \quad .$$

(5.6) (**Vandermonde**sche Determinante:) Sei K ein Körper, $a_1, \ldots, a_n \in K$. Zeigen Sie :

$$\det \begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{pmatrix} \quad = \quad \prod_{(k,j) \in \underline{n} \times \underline{n} \text{ mit } k<j} (a_j - a_k) \quad .$$

(Tipp: Zum Beweis subtrahiere man nacheinander für $k = n$, $n-1, \ldots, 3, 2$ das a_1-fache der $(k-1)-$ten Spalte von der $k-$ten Spalte und forme dann so um, dass man Induktion nach n machen kann.)

Empfehlenswerte Literatur

zur Linearen Algebra :

Gerd Fischer : Lineare Algebra, eine Einführung für Studienanfänger. 18.Auflage. Springer 2014.

Bertram Huppert, Wolfgang Willems : Lineare Algebra, 2., überarbeitete und erweiterte Auflage. Vieweg+Teubner 2010.

Max Koecher : Lineare Algebra und analytische Geometrie. 4.Auflage, Springer Berlin 1997.

H.-J.Kowalsky, G.O.Michler : Lineare Algebra. 12., überarbeitete Auflage. De Gruyter Lehrbuch, Berlin 2008.

M.Roczen und H.Wolter, W.Pohl, D.Popescu, R.Laza: Lineare Algebra individuell. Online Ver. 0.62, 20.3.2010.

zur Analysis :

Konrad Königsberger: Analysis 1, 6.Auflage. Springer-Lehrbuch 2004.

Otto Forster : Analysis 1, 11., erweiterte Auflage. Springer Spektrum 2013.

Harro Heuser : Lehrbuch der Analysis, Teil 1. 15.Auflage. Vieweg+Teubner, 2003.

zur Algebra :

Siegfried Bosch : Algebra, 6.Auflage. Springer-Lehrbuch 2006.

Nathan Jacobson : Basic Algebra I, 2nd edition, Dover Publications 2009.

Chr.Kapfinger, K.Meyberg : Algebra, 3.Auflage.Springer Spektrum 2013.

zur elementaren Zahlentheorie :

Ivan Niven, Herbert S.Zuckerman, Hugh L.Montgomery : An Introduction to the Theory of Numbers. 5th edition, Wiley 1991.

Harold M.Stark : An Introduction to Number Theory. New edition, MIT Press 1978.

Verzeichnis der Definitionen

Abkürzungen: e. : einer, eines, v. : von