Prof. Dr. H. Brenner **Osnabrück WS 2017/2018**

Lineare Algebra und analytische Geometrie I

Vorlesung 3

Kultur ist Reichtum an Problemen.

Egon Friedell

Gruppen

In der linearen Algebra wird im Allgemeinen ein *Grundkörper* K zugrunde gelegt, über dem sich alles aufbaut. Der wichtigste Körper ist für uns der Körper der reellen Zahlen $\mathbb{R}$, den wir schon verwendet haben und der in der Analysis axiomatisch eingeführt wird. Wie die reellen Zahlen ist ein Körper durch die Existenz von zwei Verknüpfungen mit bestimmten Eigenschaften festgelegt, nämlich einer Addition und einer Multiplikation. Erstaunlicherweise gehören diese beiden Verknüpfungen (bei der Multiplikation muss man die 0 herausnehmen) für sich genommen zu einer wichtigen algebraische Struktur: Es handelt sich um Gruppen.

Definition 3.1. Eine Menge G mit einem ausgezeichneten Element $e \in G$ und mit einer Verknüpfung

$$G \times G \longrightarrow G,\ (g,h) \longmapsto g \circ h,$$

heißt *Gruppe*, wenn folgende Eigenschaften erfüllt sind.

(1) Die Verknüpfung ist *assoziativ*, d.h. für alle $f,g,h \in G$ gilt

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

(2) Das Element e ist ein *neutrales Element*, d.h. für alle $g \in G$ gilt

$$g \circ e = g = e \circ g\,.$$

(3) Zu jedem $g \in G$ gibt es ein *inverses Element*, d.h. es gibt ein $h \in G$ mit

$$h \circ g = g \circ h = e\,.$$

Eine Gruppe heißt *kommutativ*, wenn die Verknüpfung kommutativ ist. Wichtige Beispiele für kommutative Gruppen sind $(\mathbb{Z},0,+)$, $(\mathbb{R},0,+)$, $(\mathbb{R}\setminus\{0\},1,\cdot)$ oder $(\mathbb{R}^n,0,+)$ mit der komponentenweisen Null

$$0 \;=\; (0,0,\ldots,0)$$

und der komponentenweisen Addition.

In einer Gruppe $(G, e, \circ)$ ist das neutrale Element eindeutig bestimmt. Wenn nämlich e' ein weiteres Element mit der für das neutrale Element charakteristischen Eigenschaft, also

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

für alle $x \in G$, ist, so ergibt sich direkt

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

LEMMA 3.2. *Es sei $(G, e, \circ)$ eine Gruppe. Dann ist zu jedem $x \in G$ das Element $y \in G$ mit*

$$x \circ y = y \circ x = e$$

eindeutig bestimmt.

Beweis. Sei

$$x \circ y = y \circ x = e$$

und

$$x \circ z = z \circ x = e.$$

Dann ist

$$y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z.$$

□

Solche abstrakte Strukturen wie eine Gruppe führen ein Doppelleben: Einerseits sind sie wirklich nur die gegebene formale Struktur, die Elemente sind nur irgendwelche Elemente einer irgendwie gegebenen Menge, die Verknüpfung ist irgendeine Verknüpfung, unter der man sich nichts Bestimmtes vorstellen soll. Die gewählten Symbole sind willkürlich und ohne Bedeutung. Andererseits erhalten solche abstrakte Strukturen dadurch ihr Leben, dass konkrete mathematische Strukturen darunter subsummiert werden können. Die konkreten Strukturen sind *Beispiele* oder *Modelle* für die abstrakte Struktur (und sie sind mathematikhistorisch auch die Motivation, abstraktere Strukturen einzuführen). Beide Ebenen sind wichtig, man sollte sie aber stets auseinander halten.

Die Gruppentheorie ist ein eigenständiger Zweig in der Mathematik, den wir hier aber nicht systematisch entwickeln werden. Stattdessen beschäftigen wir uns mit Ringen und vor allem mit Körpern.

Ringe

DEFINITION 3.3. Eine Menge R heißt ein *Ring*, wenn es zwei Verknüpfungen (genannt *Addition* und *Multiplikation*)

$$+ : R \times R \longrightarrow R \text{ und } \cdot : R \times R \longrightarrow R$$

und (nicht notwendigerweise verschiedene) Elemente $0, 1 \in R$ gibt, die die folgenden Eigenschaften erfüllen.

(1) Axiome der Addition
   (a) Assoziativgesetz: Für alle $a, b, c \in R$ gilt: $(a+b)+c = a+(b+c)$.
   (b) Kommutativgesetz: Für alle $a, b \in R$ gilt $a + b = b + a$.
   (c) 0 ist das neutrale Element der Addition, d.h. für alle $a \in R$ ist $a + 0 = a$.
   (d) Existenz des Negativen: Zu jedem $a \in R$ gibt es ein Element $b \in R$ mit $a + b = 0$.
(2) Axiome der Multiplikation
   (a) Assoziativgesetz: Für alle $a, b, c \in R$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
   (b) 1 ist das neutrale Element der Multiplikation, d.h. für alle $a \in R$ ist $a \cdot 1 = 1 \cdot a = a$.
(3) Distributivgesetz: Für alle $a, b, c \in R$ gilt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

DEFINITION 3.4. Ein Ring R heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

Die wichtigsten kommutativen Ringe sind für uns die Mengen der ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$. Dass all diese Axiome für die reellen Zahlen (und die rationalen Zahlen) mit den natürlichen Verknüpfungen gelten, ist aus der Schule bekannt. Eine axiomatische Begründung ist möglich, wird aber hier nicht durchgeführt. Mit der Addition ist ein Ring $(R, 0, +)$ insbesondere eine kommutative Gruppe.

In einem Ring gilt die *Klammerkonvention*, dass die Multiplikation stärker bindet als die Addition (*Punktrechnung vor Strichrechnung*). Man kann daher $a \cdot b + c \cdot d$ statt $(a \cdot b) + (c \cdot d)$ schreiben. Zur weiteren Notationsvereinfachung wird das Produktzeichen häufig weggelassen. Die besonderen Elemente 0 und 1 in einem Ring werden als *Nullelement* und als *Einselement* bezeichnet. Zu einem Element $a \in R$ nennt man das nach Lemma 3.2 eindeutig bestimmte Element y mit $a + y = 0$ das *Negative* von a und bezeichnet es mit $-a$. Es ist $-(-a) = a$, da wegen $a + (-a) = 0$ das Element a gleich dem eindeutig bestimmten Negativen von $-a$ ist. Statt $b + (-a)$ schreibt man abkürzend $b - a$ und spricht von der *Differenz*. Die Differenz ist also keine grundlegende Verknüpfung, sondern wird auf die Addition mit dem Negativen zurückgeführt.

Die folgenden Eigenschaften sind für den Ring der reellen Zahlen vertraut, wir beweisen sie aber allein aus den Axiomen eines Rings. Sie gelten daher für jeden Ring.

LEMMA 3.5. *Sei R ein Ring und seien $a, b, c, a_1, \ldots, a_r, b_1, \ldots, b_s$ Elemente aus R. Dann gelten folgende Aussagen.*

(1)
$$0a = a0 = 0$$
*(*Annullationsregel*),*
(2)
$$a(-b) = -(ab) = (-a)b,$$

(3)
$$(-a)(-b) = ab$$
*(*Vorzeichenregel*),*
(4) $a(b-c) = ab - ac$ *und* $(b-c)a = ba - ca$*,*
(5)
$$\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{k=1}^{s} b_k\right) = \sum_{1\le i\le r,\, 1\le k\le s} a_i b_k$$
*(*allgemeines Distributivgesetz*).*

Beweis. Wir beweisen im nicht kommutativen Fall je nur eine Hälfte.

(1) Es ist $a0 = a(0+0) = a0 + a0$. Durch beidseitiges Abziehen von $a0$ ergibt sich die Behauptung.
(2)
$$(-a)b + ab = (-a+a)b = 0b = 0$$
nach Teil (1). Daher ist $(-a)b$ das (eindeutig bestimmte) Negative von ab.
(3) Nach (2) ist $(-a)(-b) = (-(-a))b$ und wegen $-(-a) = a$ (dies gilt in jeder Gruppe) folgt die Behauptung.
(4) Dies folgt auch aus dem bisher Bewiesenen.
(5) Dies folgt aus einer einfachen Doppelinduktion.

□

Körper

Einen Großteil der linearen Algebra kann man über einem beliebigen Ring aufbauen, was aber einen ungleich umfassenderen Begriffsapparat erfordert. Stattdessen werden wir stets über einem Körper arbeiten.

Definition 3.6. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

Ausgeschrieben bedeutet dies:

Definition 3.7. Eine Menge K heißt ein *Körper*, wenn es zwei Verknüpfungen (genannt Addition und Multiplikation)
$$+ : K \times K \longrightarrow K \text{ und } \cdot : K \times K \longrightarrow K$$
und zwei verschiedene Elemente $0, 1 \in K$ gibt, die die folgenden Eigenschaften erfüllen.

(1) Axiome der Addition
  (a) Assoziativgesetz: Für alle $a, b, c \in K$ gilt: $(a+b)+c = a+(b+c)$.
  (b) Kommutativgesetz: Für alle $a, b \in K$ gilt $a + b = b + a$.

(c) 0 ist das neutrale Element der Addition, d.h. für alle $a \in K$ ist $a + 0 = a$.
(d) Existenz des Negativen: Zu jedem $a \in K$ gibt es ein Element $b \in K$ mit $a + b = 0$.

(2) Axiome der Multiplikation
(a) Assoziativgesetz: Für alle $a, b, c \in K$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(b) Kommutativgesetz: Für alle $a, b \in K$ gilt $a \cdot b = b \cdot a$.
(c) 1 ist das neutrale Element der Multiplikation, d.h. für alle $a \in K$ ist $a \cdot 1 = a$.
(d) Existenz des Inversen: Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein Element $c \in K$ mit $a \cdot c = 1$.

(3) Distributivgesetz: Für alle $a, b, c \in K$ gilt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Die oben beschriebenen Eigenschaften (und Konventionen) für Ringe gelten insbesondere für Körper. Unter Verwendung des Gruppenbegriffs kann man auch sagen, dass ein Körper eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ und zwei fixierten Elementen $0 \neq 1$ ist, derart, dass $(K, +, 0)$ und $(K \setminus \{0\}, \cdot, 1)$ jeweils kommutative Gruppen[1] sind und dass das Distributivgesetz gilt.

Zu einem Element $x \in K$ und einer natürlichen Zahl $n \in \mathbb{N}$ definiert man nx als die n-fache Summe von x mit sich selbst. Dabei setzt man $0x = 0$. Für

$$n1_K = \underbrace{1_K + 1_K + \cdots + 1_K}_{n Summanden}$$

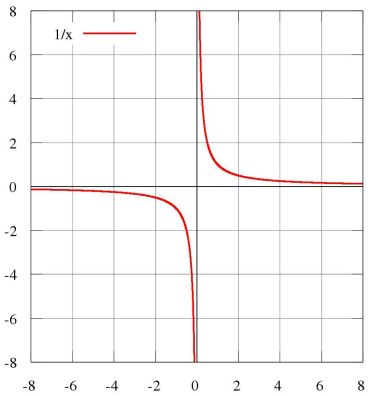
schreibt man auch einfach n_K oder n. Man findet also jede natürliche Zahl in jedem Körper (auch in jedem Ring) wieder, allerdings kann es sein, dass diese Zuordnung nicht injektiv ist und beispielsweise $2 = 0$ oder $7 = 0$ in einem Körper gilt (siehe die Beispiele weiter unten). Für negative ganze Zahlen n setzt man

$$nx = (-n)(-x),$$

wobei $-x$ das Negative von x in dem Körper ist. Aufgrund von Aufgabe 3.26 passt alles zusammen. Z.B. kann man $(-n)(-x)$ wie eben als die $-n$-fache Summe von $-x$ mit sich selbst verstehen oder als Produkt aus $-x$ und $-n$, letzteres als die $-n$-fache Summe von 1_K mit sich selbst.

Das zu $a \in K$, $a \neq 0$, nach Lemma 3.2 (hier lohnt sich schon der Gruppenbegriff) eindeutig bestimmte Element z mit $az = 1$ nennt man das *Inverse* von a und bezeichnet es mit a^{-1}.

[1] Das beinhaltet hier insbesondere, dass die Multiplikation sich zu einer Verknüpfung auf $K \setminus \{0\}$ einschränken lässt. Aus den Körperaxiomen folgt dies, wie wir gleich sehen werden.



Der Graph zur reellen Funktion, die einer Zahl $a \neq 0$ ihr Inverses zuordnet. Im Nullpunkt ist die Abbildung nicht definiert und auch nicht stetig fortsetzbar.

Für $a, b \in K$, $b \neq 0$, schreibt man auch abkürzend

$$a/b := \frac{a}{b} := ab^{-1}.$$

Die beiden linken Ausdrücke sind also Abkürzungen für den rechten Ausdruck.

Zu einem Körperelement $a \in K$ und $n \in \mathbb{N}$ wird die *n-Potenz*, geschrieben a^n, als das n-fache Produkt von a mit sich selbst definiert (n gibt die Anzahl der Faktoren an). Man setzt weiterhin $a^0 = 1$, und bei $a \neq 0$ wird für $n \in \mathbb{N}_+$ der Ausdruck a^{-n} als $(a^{-1})^n$ interpretiert.

Ein „kurioser“ Körper wird im folgenden Beispiel beschrieben. Dieser Körper mit zwei Elementen ist in der Informatik und der Kodierungstheorie wichtig, wird für uns aber keine große Rolle spielen. Er zeigt, dass es nicht für jeden Körper sinnvoll ist, seine Elemente auf der Zahlengeraden zu verorten.

Beispiel 3.8. Wir suchen nach einer Körperstruktur auf der Menge $\{0, 1\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element einer Multiplikation sein soll, so ist dadurch schon alles festgelegt, da $1+1 = 0$ sein muss, da 1 ein inverses Element bezüglich der Addition besitzen muss, und da in jedem Körper nach Lemma 3.5 $0 \cdot 0 = 0$ gelten muss. Die Operationstafeln sehen also wie folgt aus.

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Durch etwas aufwändiges Nachrechnen stellt man fest, dass es sich in der Tat um einen Körper handelt.

Beispiel 3.9. Auf der Menge $\{0,1,2,3,4,5,6\}$ (mit sieben Elementen) kann man durch die Festlegungen

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

ebenfalls einen Körper machen. Ohne weitere Theorie ist der Nachweis der Körpereigenschaften sehr aufwändig.

Lemma 3.10. *Es sei K ein Körper. Aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.*

Beweis. Nehmen wir an, dass a und b beide von 0 verschieden sind. Dann gibt es dazu inverse Elemente a^{-1} und b^{-1} und daher ist $(ab)\left(b^{-1}a^{-1}\right) = 1$. Andererseits ist aber nach Voraussetzung $ab = 0$ und daher ist nach Lemma 3.5 (1)

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

so dass sich der Widerspruch $0 = 1$ ergibt. □

Abbildungsverzeichnis