Prof. Dr. H. Brenner **Osnabrück WS 2009/2010**

Vorkurs Mathematik

Vorlesung 7

Körper

Wir werden von nun an den axiomatischen Aufbau der reellen Zahlen besprechen. Diese Axiome gliedern sich in algebraische Axiome, Anordnungsaxiome und das Vollständigkeitsaxiom. Die algebraischen Axiome werden im Begriff des Körpers zusammengefasst.

DEFINITION 7.1. 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, 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 $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$.

In einem Körper gilt die *Klammerkonvention*, dass die Multiplikation stärker bindet als die Addition. 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 Körper werden als *Nullelement* und als *Einselement* bezeichnet. Nach der Definition müssen sie verschieden sein.

Die wichtigsten Beispiele für einen Körper sind für uns die rationalen Zahlen und die reellen Zahlen.

Beispiel 7.2. Wir suchen nach einer Körperstruktur auf der Menge $\{0,1\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element der Multiplikation sein soll, so ist dadurch schon alles festgelegt, da $1+1=0$ sein muss, da 1 ein inverses Element bzgl. der Addition besitzen muss, und da in jedem Körper $0 \cdot 0 = 0$ gelten muss. Die Operationstafeln sehen also wie folgt aus.

$$\begin{array}{c|c|c} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{und} \quad \begin{array}{c|c|c} * & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

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

Lemma 7.3. *In einem Körper K ist zu einem Element $x \in K$ das Element y mit $x+y=0$ eindeutig bestimmt. Bei $x \neq 0$ ist auch das Element z mit $xz=1$ eindeutig bestimmt.*

Diese Aussage ist also eine Eindeutigkeitsaussage, und zwar wird behauptet, dass es nur ein Element gibt mit der Eigenschaft, dass seine Summe mit einem vorgegebenen x gleich 0 ist. Diese Eigenschaft bestimmt also das Element eindeutig. Eine solche Eindeutigkeitsaussage wird dadurch bewiesen, dass man sich zwei beliebige Elemente hernimmt, von denen man annimmt, dass sie beide die Eigenschaft erfüllen, darüber hinaus ist nichts von ihnen bekannt. Man muss dann zeigen, dass die beiden Elemente gleich sind. Häufig wählt man für die beiden Elemente ähnliche Symbole, um anzudeuten, dass sie die gleiche Eigenschaft erfüllen.

Beweis. Sei x vorgegeben und seien y und y' Elemente mit $x+y=0=x+y'$. Dann gilt

$$y = y+0 = y+(x+y') = (y+x)+y' = (x+y)+y' = 0+y' = y'.$$

Insgesamt ist also $y=y'$. Für den zweiten Teil sei x vorgegeben mit $x \neq 0$. Es seien z und z' Elemente mit $xz=1=xz'$. Dann ist

$$z = z1 = z(xz') = (zx)z' = 1z' = z'.$$

Also ist $z=z'$. □

Diese Aussage ist also eine Eindeutigkeitsaussage, und zwar wird behauptet, dass es nur ein Element gibt mit der Eigenschaft, dass seine Summe mit einem vorgegebenen x gleich 0 ist. Diese Eigenschaft bestimmt also das Element eindeutig. Eine solche Eindeutigkeitsaussage wird dadurch bewiesen, dass man sich zwei beliebige Elemente hernimmt, von denen man annimmt, dass sie beide die Eigenschaft erfüllen, darüber hinaus ist nichts von ihnen bekannt. Man muss dann zeigen, dass die beiden Elemente gleich sind. Häufig wählt man für die beiden Elemente ähnliche Symbole, um anzudeuten, dass sie die gleiche Eigenschaft erfüllen.

Zu einem Element $a \in K$ nennt man das nach diesem Lemma eindeutig bestimmte Element b mit $a + b = 0$ das *Negative* von a und bezeichnet es mit $-a$. 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 Negativen zurückgeführt.

Das zu $a \in K$, $a \neq 0$, nach diesem Lemma eindeutig bestimmte Element c mit $ac = 1$ nennt man das *Inverse* von a und bezeichnet es mit a^{-1}.

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 eine Abkürzung für den rechten Ausdruck.

Exkurs: Gruppentheorie

Die beiden Eindeutigkeitsbeweise im vorausgegangenen Lemma zeigen eine ähnliche Struktur. Wenn man im ersten Teilbeweis überall die Addition durch die Multiplikation und die 0 durch die 1 ersetzt und die Symbole anpasst, so erhält man den zweiten Teilbeweis. Insbesondere fällt auf, dass im ersten Teilbeweis nur die Addition vorkommt, nicht aber die Multiplikation, und dass nur das Nullsymbol 0 vorkommt. Wenn man die Beweisschritte anschaut, so sieht man, dass von der Axiomenmenge des Körpers nur ein Bruchteil verwendet wurde, und zwar ausschließlich solche Axiome, die sich auf die Addition beziehen. Im zweiten Beweisteil ist es genau umgekehrt.

Ein wesentlicher Vorteil der axiomatischen Methode ist, dass man stets weiß, was man verwenden darf und was nicht, und damit ist auch stets klar, was man in einem Beweis verwendet hat und was nicht. Wenn man in einem umfassenden Axiomensystem einen Beweis erbracht hat und dann schaut, welche der Axiome man wirklich verwendet hat (sozusagen sich das Beweisprotokoll noch mal ansieht) und diese eine echte Teilmenge des Axiomensystems bilden, so kann man die Aussage auch mit diesem kleineren Axiomensystem beweisen. Da man in der Mathematik nichts verschenken möchte, und insbesondere keine überflüssigen Voraussetzungen mitschleppen möchte, fasst man Axiome zu kleineren Einheiten zusammen, und leitet aus ihnen so viel wie möglich ab. Dies ist aus ökonomischen Gründen auch dann sinnvoll, wenn man sich nur für ein einziges mathematisches Objekt interessiert, für das ein reichhaltiges Axiomensystem zur Verfügung steht (wie wir für die reellen Zahlen).

Für den Körperbegriff heißt dies beispielsweise, dass es sinnvoll ist, zu untersuchen, welche Eigenschaften man für die Addition allein aus den Gesetzen der Addition und welche Eigenschaften man für die Multiplikation allein aus den Gesetzen der Multiplikation beweisen kann. Dabei fällt auf, dass von den algebraischen Eigenschaften her eine weitgehende Parallelität zwischen

diesen beiden Operationen besteht, die sich auch in den obigen Eindeutigkeitsbeweisen niederschlug. Es ist also sinnvoll, diese Parallelitäten auf den Punkt zu bringen und durch ein gemeinsames übergeordnetes Vokabular auszudrücken. Dies geschieht mit dem Begriff der *Gruppe*.

Definition 7.4. 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
$$h \circ g = g \circ h = e\,.$$

Man beachte, dass kein Kommutativitätsgesetz vorausgesetzt wird, so dass man die zweifachen Formulierungen in Teil (2) und (3) benötigt (eine Gruppe, wo zusätzlich die Kommutativität gilt, heißt *kommutative Gruppe*). Die Symbole $\circ$ für die Verknüpfung und e für das neutrale Element sind willkürlich gewählt, man könnte sie auch anders nennen. Es ist aber sinnvoll, bei der abstrakten Einführung eine Bezeichnung zu wählen, die intuitiv nicht vorbelastet ist. Eine Bezeichnung wie $\cdot$ für die Verknüpfung und 1 für das neutrale Element birgt die Gefahr, dass man sich zu Schlüssen verleiten lässt, die von der Multiplikation von Zahlen her vertraut sind, die aber eventuell für eine beliebige Gruppe nicht gelten müssen.

Die additiven Körperaxiome kann man nun so lesen, dass die Menge K zusammen mit dem ausgezeichneten Element 0 und der Addition $+$ als Verknüpfung eine Gruppe bildet, die zusätzlich kommutativ ist. Ebenso bildet die Menge $K \setminus \{0\}$ (also ganz K ohne die 0) mit dem neutralen Element 1 (das wegen der expliziten Voraussetzung der Körperaxiome von 0 verschieden ist und daher zu $K \setminus \{0\}$ gehört) und der Multiplikation $\cdot$ eine (ebenfalls kommutative) Gruppe. Wenn ein Körper K vorliegt, so hat man also zugleich zwei Gruppen vorliegen, es ist aber falsch zu sagen, dass K auf zweifache Weise eine Gruppe ist, da einerseits K mit der Addition und andererseits $K \setminus \{0\}$ (und eben nicht K) eine Gruppe mit der Multiplikation bildet.

Weitere Beispiele für Gruppen sind $(\mathbb{Z},+,0)$,[1] dagegen ist $\mathbb{Z}$ mit der Multiplikation und ebensowenig $\mathbb{Z} \setminus \{0\}$ keine Gruppe. Eine Gruppe ist niemals leer, da es ja ein neutrales Element enthalten muss. Die Menge, die nur aus einem

[1]Eine Gruppe wird häufig in *Tupelschreibweise* in der Form (Gruppe, Operation, neutrales Element) geschrieben.

einzigen Element besteht, ist mit der einzig darin möglichen Verknüpfung und dem einzig darin möglichen neutralen Element eine Gruppe. Man spricht von der *trivialen Gruppe*. Eine weitere Gruppe ist die zweielementige Menge

$$(\{-1,1\},\cdot,1)$$

mit der von $\mathbb{Z}$ bekannten Multiplikation.

In einer Gruppe ist zu einem Element $x \in G$ das Element y mit der Eigenschaft $x \circ y = e = y \circ x$ (das es aufgrund der Gruppenaxiome geben muss) eindeutig bestimmt. Wenn nämlich y und y' beide diese Eigenschaft besitzen, so gilt

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

Man beachte, dass in diesen Beweis die Bedingungen an y und y' nicht völlig symmetrisch eingehen. Diese Eindeutigkeit erlaubt es, das zu einem Gruppenelement $x \in G$ eindeutig bestimmte inverse Element als

$$x^{-1}$$

zu bezeichnen.

Im Fall eines Körpers haben wir damit einen einzigen Beweis für die Eindeutigkeit des Negativen (also des Inversen der Addition) und des Inversen der Multiplikation gefunden.

In der Mathematik geht es zu einem beträchtlichen Teil um die Lösung von Gleichungen, und zwar um die Existenz von Lösungen, die Berechnung von Lösungen und die Eindeutigkeit von Lösungen. Bei einer Gruppe besitzen die formulierbaren Einzelgleichungen eine eindeutige Lösung. Insofern handelt es sich bei einer Gruppe um eine besonders einfache mathematische Struktur.

LEMMA 7.5. *Sei G eine Gruppe. Dann besitzen zu je zwei Gruppenelementen $a, b \in G$ die Gleichungen*

$$ax = b \text{ und } ya = b$$

eindeutige Lösungen $x, y \in G$.

Beweis. Wir betrachten die linke Gleichung. Aus beidseitiger Multiplikation[2] mit a^{-1} (bzw. mit a) von links folgt, dass nur

$$x = a^{-1}b$$

als Lösung in Frage kommt. Wenn man dies einsetzt, so sieht man, dass es sich in der Tat um eine Lösung handelt. □

LEMMA 7.6. *Es sei K ein Körper und seien a, b, c, a_i, b_k Elemente aus K. Dann gelten folgende Aussagen*

[2]Hier wird das Gleichheitsprinzip angewendet: wenn $x = y$ ist, so kann man beidseitig eine beliebige Abbildung φ anwenden und erhält eine neue Gleichung $\varphi(x) = \varphi(y)$. Im vorliegenden Fall ist die beidseitige Multiplikation mit einem festen Gruppenelement auch eine Abbildung.

(1) $a0 = 0$ *(*Annullationsregel*),*
(2) $a(-b) = -ab = (-a)b$
(3) $(-a)(-b) = ab$ *(*Vorzeichenregel*),*
(4) $a(b-c) = ab - ac$,
(5) $(\sum_{i=1}^{r} a_i)(\sum_{k=1}^{s} b_k) = \sum_{1 \le i \le r,\, 1 \le k \le s} a_i b_k$ *(*allgemeines Distributivgesetz*).*

Beweis. (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 Doppelinduktion, siehe Aufgabe 7.11.

□