Prof. Dr. H. Brenner **Osnabrück SS 2020**

Diskrete Mathematik

Vorlesung 5

... dass jeder und jede meint, dass Vorli ihn oder sie ganz besonders mag.

Gruppen

Wir besprechen Gruppen. Mit dieser Struktur kann man viele strukturelle Gemeinsamkeiten zwischen der Menge der bijektiven Abbildungen auf einer Menge oder der Addition in einem kommutativen Ring wie $\mathbb{Z}$ oder der Multiplikation in einem Körper, wenn man die 0 herausnimmt (wie in $\mathbb{Q} \setminus \{0\}$ oder in $\mathbb{R} \setminus \{0\}$), erfassen.

Definition 5.1. 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 ist also ein Monoid, in dem jedes Element ein inverses Element besitzt.

DEFINITION 5.2. Eine Gruppe $(G, e, \circ)$ heißt *kommutativ* (oder *abelsch*), wenn die Verknüpfung kommutativ ist, wenn also $x \circ y = y \circ x$ für alle $x, y \in G$ gilt.

LEMMA 5.3. *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

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

□

Allgemeiner gilt in Gruppen die eindeutige Lösbarkeit von mit der Verknüpfung formulierten Gleichungen.

LEMMA 5.4. *Sei $(G, e, \circ)$ eine Gruppe. Dann besitzen zu je zwei Gruppenelementen $a, b \in G$ die beiden Gleichungen*

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

eindeutige Lösungen $x, y \in G$.

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

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

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

In einer (multiplikativ geschriebenen) Gruppe kann man Potenzen allgemeiner als in einem Monoid definieren, nämlich auch für negative ganze Zahlen im Exponenten. Wie in jedem Monoid bezeichnet zu $a \in G$ und $n \in \mathbb{N}$ der Ausdruck a^n das n-fache Produkt von a mit sich selbst, was $a^0 = 1$ einschließt. Die Schreibweise a^{-1} für das inverse Element zu a reiht sich in die neue Potenzschreibweise ein. Für eine negative ganze Zahl n mit $n = -k$ und $k \in \mathbb{N}_+$ setzt man

$$a^n := \left(a^{-1}\right)^k.$$

Dass dies die richtige Definition ist, zeigt sich darin, dass sich die Potenzgesetze aus Lemma 4.8 in die neue Situation übertragen.

LEMMA 5.5. *Es sei $(G, 1, \cdot)$ eine Gruppe und seien $a, b \in G$. Dann gelten die folgenden Potenzgesetze für $m, n \in \mathbb{Z}$.*

(1) *Es ist*
$$\left(a^{-1}\right)^{-1} = a.$$
(2) *Es ist $a^{-n} = (a^{-1})^n$ das inverse Element zu a^n.*
(3)
$$a^{m+n} = a^m \cdot a^n.$$
(4)
$$(a^m)^n = a^{mn}.$$

Beweis. (1) folgt aus Aufgabe 5.2, da $K \setminus \{0\}$ eine Gruppe ist. (2). Bei $n \in \mathbb{N}$ ist die linke Gleichheit eine Definition und die Behauptung folgt aus

$$\left(a^{-1}\right)^n \cdot a^n = \left(a^{-1}a\right)^n = 1^n = 1.$$

Daraus folgt auch die Aussage für negatives n. Für (3), (4) siehe Aufgabe 5.9. □

In einer kommutativen Gruppe gilt für $a, b \in G$ und $n \in \mathbb{Z}$ wieder die Gleichheit

$$(ab)^n = a^n b^n,$$

siehe Aufgabe 5.10.

Kommutative Ringe

DEFINITION 5.6. 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 5.7. Ein Ring R heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

Ein kommutativer Ring ist insbesondere ein kommutativer Halbring, alle für Halbringe geltenden Eigenschaften wie beispielsweise die allgemeine binomische Formel gelten insbesondere auch für kommutative Ringe. Der wesentliche Unterschied liegt in der zusätzlichen Bedingung (1.4), der Existenz des Negativen. Dies bedeutet, dass in einem Ring das additive Monoid $(R, +, 0)$ eine (kommutative) Gruppe ist. Dieses Negative ist nach Lemma 5.3 eindeutig bestimmt. Für das zu jedem $a \in R$ eindeutig bestimmte Negative schreiben wir $-a$. Wegen

$$a + (-a) = 0$$

ist a auch das Negative zu $-a$, also $-(-a) = a$.

Mit diesem Begriff können wir festhalten.

SATZ 5.8. *Die ganzen Zahlen* $(\mathbb{Z}, 0, 1, +, \cdot)$ *bilden einen kommutativen Ring.*

BEISPIEL 5.9. Die einelementige Menge $R = \{0\}$ kann man zu einem Ring machen, indem man sowohl die Addition als auch die Multiplikation auf die einzig mögliche Weise erklärt, nämlich durch $0 + 0 = 0$ und $0 \cdot 0 = 0$. In diesem Fall ist $1 = 0$, dies ist also ausdrücklich erlaubt. Diesen Ring nennt man den *Nullring*.

Einen weiteren endlichen Ring (und zwar einen Körper) haben wir bereits in Beispiel 4.12 kennengelernt. In der zwölften Vorlesung werden wir einer Vielzahl von weiteren endlichen Ringen begegnen.

In einem kommutativen Ring R und Elemente $a, b \in R$ verwendet man

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

als abkürzende Schreibweise. Man spricht von der *Subtraktion* bzw. der *Differenz*. Die Subtraktion $a - b$ ist also die Addition von a mit dem Negativen (also $-b$) von b.

LEMMA 5.10. *Es sei R ein kommutativer Ring und seien a, b, c Elemente aus R. Dann gelten folgende Aussagen.*

(1)
$$0a = 0$$
*(*Annullationsregel*),*

(2)
$$a(-b) = -(ab) = (-a)b,$$

(3)
$$(-a)(-b) = ab$$
*(*Vorzeichenregel*),*

(4)
$$a(b-c) = ab - ac.$$

Beweis. (1) Es ist $a0 = a(0+0) = a0+a0$. Durch beidseitiges Abziehen (also Addition mit $-a0$) 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 $-(-a) = a$ folgt die Behauptung.

(4) Dies folgt auch aus dem bisher Bewiesenen.

□

Wie in jedem kommutativen Halbring kann man in jedem kommutativen Ring R Ausdrücke der Form nx mit $n \in \mathbb{N}$ und $x \in R$ sinnvoll interpretieren, und zwar ist nx die n-fache Summe von x mit sich selbst. Auch die Potenzschreibweise x^n wird wieder verwendet und es gelten insbesondere die in Lemma 4.8 formulierten Potenzgesetze. Darüber hinaus kann man auch für negative Zahlen $-n$ den Ausdruck $(-n)x$ interpretieren, nämlich als

$$(-n)x = n(-x) = \underbrace{(-x) + \cdots + (-x)}_{n\text{-mal}}.$$

Insbesondere ist

$$-n = (-n) \cdot 1 = n \cdot (-1) = \underbrace{(-1) + \cdots + (-1)}_{n\text{-mal}}$$

in jedem kommutativen Ring sinnvoll interpretierbar. Dabei gelten naheliegende Rechengesetze, siehe Aufgabe 5.22.

Körper

Definition 5.11. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

Ein Körper ist also insbesondere ein kommutativer Ring. Jede Eigenschaft, die in einem kommutativen Ring gilt, gilt auch in einem Körper (aber nicht umgekehrt).

Die wichtigsten Körper sind für uns der Körper der rationalen Zahlen, der Körper der reellen Zahlen und der Körper der komplexen Zahlen. Der Körper mit zwei Elementen wurde in Beispiel 4.12 besprochen. Wir werden weitere endliche Körper in der zwölften Vorlesung konstruieren. Zu einem Element $x \in K$ bezeichnet man, wie in jedem kommutativen Ring, dasjenige Element, das mit x addiert die 0 ergibt, als das Negative von x, geschrieben $-x$. Zu einem Element $x \in K$, $x \neq 0$, bezeichnet man dasjenige Element, das mit x multipliziert die 1 ergibt, als das Inverse von x (oder den *Kehrwert* von x oder die zu x *reziproke Zahl*), geschrieben x^{-1}. Auch dieses ist eindeutig bestimmt.

Bemerkung 5.12. In einem Körper K wird für beliebige Elemente $x, y \in K$ mit $y \neq 0$, die *Bruchschreibweise*

$$\frac{x}{y} := x \cdot y^{-1}$$

verwendet. Es handelt sich also um eine Abkürzung für das Produkt von x mit dem inversen Element von y. Die Zahl $\frac{x}{y}$ ist das eindeutig bestimmte Element, das mit y multipliziert das Element x ergibt. Diese Schreibweise passt mit der Bruchschreibweise für rationale Zahlen zusammen, da ja

$$\frac{a}{b} \cdot b = \frac{a}{b} \cdot \frac{b}{1} = \frac{ab}{b} = a$$

ist.

Die Berechnung von

$$\frac{x}{y} = x : y$$

nennt man *Division*, wobei x der *Dividend* und y der *Divisor* der Division heißt, das Ergebnis heißt *Quotient*.

Bemerkung 5.13. In einem Körper K ist wie in jedem kommutativen Ring die additive Struktur $(K, 0, +)$ eine kommutative Gruppe. Insbesondere besitzt in jedem Körper eine Gleichung der Form

$$a + x = b$$

mit $a, b \in K$ eine eindeutige Lösung, nämlich

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

wie sich direkt aus Lemma 5.4 ergibt. Darüber hinaus ist zu jedem Körper K die multiplikative Struktur, wenn man die 0 herausnimmt, also $(K \setminus \{0\}, \cdot, 1)$ eine kommutative Gruppe. Dies bedeutet wiederum, dass eine Gleichung der Form

$$c \cdot x = d$$

mit $c, d \neq 0$ eine eindeutige Lösung in K besitzt, nämlich

$$dc^{-1} = \frac{d}{c}.$$

Die folgende Eigenschaft heißt die *Nichtnullteilereigenschaft* eines Körpers. Sie gilt auch für $\mathbb{Z}$, im Allgemeinen aber nicht für jeden kommutativen Ring, siehe Aufgabe 5.5.

LEMMA 5.14. *Es sei K ein Körper. Aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.*

Beweis. Siehe Aufgabe 5.27. □

In einem Körper K kann man die Potenzschreibweise erweitern, da ja $K \setminus \{0\}$ eine Gruppe ist und man daher zu $x \in K$, $x \neq 0$ und $n \in \mathbb{Z}$ der Ausdruck x^n wohldefiniert ist. Wie bei jeder Gruppe ist zu einer natürlichen Zahl $n \in \mathbb{N}$ x^n das n-fache Produkt von x mit sich selbst (n Faktoren), was den Fall $x^0 = 1$ miteinschließt. Für negatives $n \in \mathbb{Z}_-$ schreibt man $n = -k$ mit $k \in \mathbb{N}_+$ und setzt

$$x^n := \left(x^{-1}\right)^k = \left(x^{-1}\right)^{-n} = \left(x^{-n}\right)^{-1}.$$

Für diese Potenzen gelten insbesondere die in Lemma 5.5 formulierten *Potenzgesetze*, die die Potenzgesetze für positive Exponenten (siehe Lemma 4.8), die in jedem kommutativen Halbring gelten, wesentlich erweitern.

Abbildungsverzeichnis