Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Grundkurs Mathematik I

Vorlesung 19

Kommutative Ringe

Wir erfassen die in der letzten Vorlesung etablierten algebraischen Eigenschaften der ganzen Zahlen mit einem neuen Begriff.

DEFINITION 19.1. 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 19.2. 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 (1d), der Existenz des Negativen. Dieses Negative ist eindeutig bestimmt: Wenn nämlich sowohl b als auch c die Eigenschaft haben, dass ihre Addition zu a den Wert 0 ergibt, so erhält man direkt

$$b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c.$$

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 $-(-a) = a$. Bei $R = \mathbb{Z}$ stimmt diese Definition mit der in der letzten Vorlesung gemachten Definition überein, wie der Beweis der Existenz des Negativen in Lemma 18.8 zeigt.

Mit diesem neuen Begriff können wir festhalten.

Satz 19.3. *Die ganzen Zahlen $(\mathbb{Z}, 0, 1, +, \cdot)$ bilden einen kommutativen Ring.*

Beweis. Dies folgt unmittelbar aus Lemma 18.8. □

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. Bei natürlichen Zahlen a, b mit $b \leq a$ stimmt die innerhalb der natürlichen Zahlen genommenen Differenz (siehe die zehnte Vorlesung) mit der hier in $\mathbb{Z}$ über das Negative genommenen Differenz überein. Dies beruht darauf, dass es sich jeweils um eine Lösung der Gleichung

$$b + x = a$$

handelt und diese Gleichung eine eindeutige Lösung besitzt.

Lemma 19.4. *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. 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 20.10.

Gruppen

Wir schauen uns kurz die Addition in einem kommutativen Ring genauer an. Hier begegnen wir einer Struktur, die später bei Körpern wieder auftaucht. Mit dieser Struktur kann man viele strukturelle Gemeinsamkeiten zwischen der Addition (in $\mathbb{Z}$) und der Multiplikation (beispielsweise in $\mathbb{Q} \setminus \{0\}$ oder in $\mathbb{R} \setminus \{0\}$) erfassen.

Definition 19.5. 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
$$h \circ g = g \circ h = e\,.$$

Definition 19.6. 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 19.7. *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

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

□

Ein kommutativer Ring R ist bezüglich der Addition insbesondere eine kommutative Gruppe. Insbesondere bilden die ganzen Zahlen $(\mathbb{Z}, 0, +)$ eine kommutative Gruppe, das inverse Element zu x ist das negative Element $-x$. Allgemein gilt in Gruppen die eindeutige Lösbarkeit von mit der Verknüpfung formulierten Gleichungen.

LEMMA 19.8. *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. □

Die Ordnung auf den ganzen Zahlen

Wir erweitern die Größergleichrelation auf den natürlichen Zahlen zu einer Ordnung auf den ganzen Zahlen.

DEFINITION 19.9. Auf den ganzen Zahlen definieren wir folgendermaßen die *Größergleichrelation* $\geq$. Wir sagen

$$a \geq b,$$

wenn es eine natürliche Zahl n mit

$$a = b + n$$

gibt.

Damit gilt bei der Interpretation am Zahlenstrahl wieder, dass

$$a \geq b$$

bedeutet, dass a rechts von b liegt.

BEMERKUNG 19.10. (1) Wenn $a, b \in \mathbb{N}$ ist, so ist

$$a \geq b$$

einfach die Ordnung auf $\mathbb{N}$, wie unmittelbar aus Lemma 10.2 folgt.

(2) Wenn $a \in \mathbb{N}$ ist und b negativ, so ist

$$a \geq b,$$

da ja dann

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

mit $a - b \in \mathbb{N}$ ist, da ja sowohl a als auch $-b$ natürliche Zahlen sind.

(3) Wenn a und b beide negativ sind, so ist

$$a \geq b$$

genau dann, wenn (innerhalb der natürlichen Zahlen)

$$-b \geq -a$$

gilt. Die Beziehung $a = b + n$ mit einer natürlichen Zahl n ist ja zu $-a = -b - n$ äquivalent, was man als $-b = -a + n$ schreiben kann.

LEMMA 19.11. *Die Größergleichrelation $\geq$ auf den ganzen Zahlen erfüllt die folgenden Eigenschaften.*

(1) *Es liegt eine totale Ordnung vor.*
(2) *Aus $a \geq b$ folgt $a + c \geq b + c$ für beliebige $a, b, c \in \mathbb{Z}$,*
(3) *Aus $a \geq 0$ und $b \geq 0$ folgt $ab \geq 0$ für beliebige $a, b \in \mathbb{Z}$.*

Beweis. (1) Aufgabe

(2) Die Beziehung $a \geq b$ bedeutet, dass es eine natürliche Zahl n mit $a = b + n$ gibt. Durch beidseitige Addition von c ergibt sich $a + c = b + c + n$, was $a + c \geq b + c$ bedeutet.

(3) Die Voraussetzung bedeutet, dass $a, b \in \mathbb{N}$ sind. Somit ist auch $ab \in \mathbb{N}$, also $ab \geq 0$.

□

Damit bilden die ganzen Zahlen $(\mathbb{Z}, \geq)$ einen angeordneten Ring im Sinne der folgenden Definition.

DEFINITION 19.12. Ein kommutativer Ring heißt *angeordnet*, wenn es eine totale Ordnung „$\geq$“ auf R gibt, die die beiden Eigenschaften

(1) Aus $a \geq b$ folgt $a + c \geq b + c$ für beliebige $a, b, c \in R$,
(2) Aus $a, b \geq 0$ folgt $ab \geq 0$,

erfüllt.

Neben den ganzen Zahlen werden wir später zwei weitere angeordnete Ringe kennenlernen, nämlich den Körper der rationalen Zahlen und den Körper der reellen Zahlen. Für all diese Ringe bzw. Körper gelten die folgenden Eigenschaften. Man überlege sich für den Fall der ganzen Zahlen, ob und inwiefern sich die Beweise der folgenden Aussage vereinfachen.

LEMMA 19.13. *In einem angeordneten Ring gelten die folgenden Eigenschaften.*

(1) $1 \geq 0$.
(2) *Es ist* $a \geq 0$ *genau dann, wenn* $-a \geq 0$ *ist.*
(3) *Es ist* $a \geq b$ *genau dann, wenn* $a - b \geq 0$ *ist.*
(4) *Es ist* $a \geq b$ *genau dann, wenn* $-a \leq -b$ *ist.*
(5) *Aus* $a \geq b$ *und* $c \geq d$ *folgt* $a + c \geq b + d$.
(6) *Aus* $a \geq b$ *und* $c \geq 0$ *folgt* $ac \geq bc$.
(7) *Aus* $a \geq b$ *und* $c \leq 0$ *folgt* $ac \leq bc$.
(8) *Aus* $a \geq b \geq 0$ *und* $c \geq d \geq 0$ *folgt* $ac \geq bd$.
(9) *Aus* $a \geq 0$ *und* $b \leq 0$ *folgt* $ab \leq 0$.
(10) *Aus* $a \leq 0$ *und* $b \leq 0$ *folgt* $ab \geq 0$.

Beweis. (1) Nehmen wir an, dass $1 \geq 0$ nicht gilt. Da eine totale Ordnung vorliegt, muss

$$1 < 0$$

gelten, Dies müssen wir zum Widerspruch führen. Nehmen wir $1 < 0$ an. Aufgrund der Verträglichkeit mit der Addition kann man beidseitig -1 addieren und erhält

$$0 < -1\,.$$

Aufgrund der Verträglichkeit mit der Multiplikation mit positiven Elementen kann man diese Abschätzung quadrieren und erhält

$$0 \leq (-1)(-1) = 1,$$

also ist zugleich $1 \geq 0$, ein Widerspruch.

(2) Folgt unmittelbar aus der Verträglichkeit mit der Addition.
(3) Folgt unmittelbar aus der Verträglichkeit mit der Addition.
(4) Folgt unmittelbar aus der Verträglichkeit mit der Addition.
(5) Zweimalige Anwendung der Verträglichkeit mit der Addition liefert

$$a + c \geq a + d \geq b + d.$$

(6) Aus $a \geq b$ folgt durch Subtraktion mit b aufgrund der Verträglichkeit mit der Addition die Abschätzung $a - b \geq b - b = 0$. Aus der Verträglichkeit mit der Multiplikation ergibt sich

$$ca - cb = c(a - b) \geq 0.$$

Addition mit cb ergibt $ca \geq cb$.

(7) Siehe Aufgabe 19.15.
(8) Nach (2) ist $-b \geq 0$, also
$$a(-b) \geq 0,$$
was wiederum $ab \leq 0$ bedeutet.
(9) Zweimalige Anwendung von (6) liefert
$$ac \geq bc \geq bd.$$
(10) Folgt aus (2) und aus $(-a)(-b) = ab$.

□

Die Eigenschaft (2) kann man so verstehen, dass das Negative eines positiven Elementes negativ ist. Allerdings tritt dabei negativ in zwei verschiedenen Bedeutungen auf!

Die Teilbarkeitsbeziehung für ganze Zahlen

Wir wollen die Teilbarkeitsbeziehung von $\mathbb{N}$ auf $\mathbb{Z}$ erweitern.

Definition 19.14. Man sagt, dass die ganze Zahl a die ganze Zahl b *teilt* (oder dass b von a *geteilt* wird, oder dass b ein *Vielfaches* von a ist), wenn es eine ganze Zahl c derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Für natürliche Zahlen a, b gilt $a|b$ in $\mathbb{N}$ genau dann, wenn $a|b$ in $\mathbb{Z}$ gilt. Die folgende Aussage ist eine direkte Verallgemeinerung von Lemma 12.3, sie beruht ausschließlich auf Eigenschaften eines kommutativen Ringes.

Lemma 19.15. *In $\mathbb{Z}$ gelten folgende Teilbarkeitsbeziehungen.*

(1) *Für jede ganze Zahl a gilt $1 \mid a$ und $a \mid a$.*
(2) *Für jede ganze Zahl a gilt $a \mid 0$.*
(3) *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
(4) *Gilt $a \mid b$ und $c \mid d$, so gilt auch $ac \mid bd$.*
(5) *Gilt $a \mid b$, so gilt auch $ac \mid bc$ für jede ganze Zahl c.*
(6) *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid (rb + sc)$ für beliebige ganze Zahlen r, s.*

Beweis. Siehe Aufgabe 19.15. □

Die Zifferndarstellung für ganze Zahlen

Die Zifferndarstellung von natürlichen Zahlen überträgt sich direkt auf ganze Zahlen, wobei die Zifferndarstellung einer negativen Zahl
$$n = -k$$
einfach die Zifferndarstellung von k (also der im Betrag genommenen Zahl) mit einem Minuszeichen davor ist. Für die schriftliche Durchführung des

Addierens, des Multiplizierens und des Subtrahierens geht man abhängig davon vor, ob die beteiligten Zahlen beide positiv, beide negativ oder ob eine positiv, eine negativ ist. Wenn beide positiv sind werden die Verfahren für natürliche Zahlen direkt angewendet. Die Korrektheit der folgenden Regeln beruht auf Lemma 19.4 und der Korrektheit der schriftlichen Operationen innerhalb der natürlichen Zahlen.

Zur Addition

(1) Wenn beide Zahlen negativ sind, so nimmt man den Betrag der beiden Zahlen, addiert diese und nimmt davon das Negative.
(2) Wenn eine Zahl positiv ist und eine negativ ist, so zieht man von der betragsmäßig größeren Zahl die betragsmäßig kleinere Zahl ab. Wenn die positive Zahl betragsmäßig größer ist, so hat man die Lösung, wenn die negative Zahl betragsmäßig größer ist, so muss man das Errechnete negieren.

Zur Multiplikation

(1) Wenn beide Zahlen negativ sind, so multipliziert man einfach die Beträge der beiden Zahlen miteinander.
(2) Wenn eine Zahl positiv ist und eine negativ ist, so multipliziert man ebenfalls die Beträge miteinander und nimmt dieses Ergebnis negativ.

Die Subtraktion fasst man als Addition mit eventuell negativen Zahlen auf.

Wenn eine ganze Zahl in der Form

$$n = c_k 10^k + c_{k-1} 10^k + \cdots + c_2 10^2 + c_1 10^1 + c_0 10^0$$

gegeben ist, wobei die c_i beliebige ganze Zahlen sind, so kann man nicht unmittelbar die zugehörige Dezimalentwicklung ablesen, da dies wesentlich davon abhängt, ob die Zahl positiv oder negativ ist.