Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 3

Division mit Rest

In dieser und der nächsten Vorlesung stehen die ganzen Zahlen $\mathbb{Z}$ im Vordergrund, wobei wir uns insbesondere für die Gruppenstruktur $(\mathbb{Z}, 0, +)$ interessieren. Zu einer ganzen Zahl d ist die Menge

$$\mathbb{Z}d = \{kd | \, k \in \mathbb{Z}\}$$

aller Vielfachen von d eine Untergruppe von $\mathbb{Z}$. Wir wollen zeigen, dass jede Untergruppe der ganzen Zahlen $\mathbb{Z}$ diese Gestalt besitzt, also von einem Element erzeugt wird.

Satz 3.1. *Sei d eine fixierte positive natürliche Zahl. Dann gibt es zu jeder ganzen Zahl n eine eindeutig bestimmte ganze Zahl q und eine eindeutig bestimmte natürliche Zahl r, $0 \leq r \leq d-1$, mit*

$$n = qd + r \, .$$

Proof. Zur Existenz. Bei $n = 0$ ist $q = r = 0$ eine Lösung. Sei n positiv. Da d positiv ist, gibt es ein Vielfaches $ad \geq n$. Daher gibt es auch eine Zahl q mit $qd \leq n$ und $(q+1)d > n$. Sei $r := n - qd$. Dann ist

$$qd \leq qd + r < qd + d$$

und daher ist $0 \leq r < d$ wie gewünscht. Bei n negativ kann man schreiben $-n = \tilde{q}d + \tilde{r}$ nach dem Resultat für positive Zahlen. Daraus ergibt sich

$$n = (-\tilde{q})d - \tilde{r} = \begin{cases} (-\tilde{q})d + 0 \text{ bei } \tilde{r} = 0 \\ (-\tilde{q} - 1)d + d - \tilde{r} \text{ sonst} \, . \end{cases}$$

Im zweiten Fall erfüllen $q = -\tilde{q} - 1$ und $r = d - \tilde{r}$ die Bedingungen.

Zur Eindeutigkeit. Sei $qd + r = n = \tilde{q}d + \tilde{r}$, wobei die Bedingungen jeweils erfüllt seien. Es sei ohne Einschränkung $\tilde{r} \geq r$. Dann gilt $(q - \tilde{q})d = \tilde{r} - r$. Diese Differenz ist nichtnegativ und kleiner als d, links steht aber ein Vielfaches von d, so dass die Differenz null sein muss und die beiden Darstellungen überein stimmen. □

In der Notation des vorstehenden Satzes soll q an *Quotient* und r an *Rest* erinnern. Die Division mit Rest kann man auch so verstehen, dass man jede rationale Zahl n/d schreiben kann als

$$\frac{n}{d} = \lfloor \frac{n}{d} \rfloor + \frac{r}{d} \, ,$$

wobei $\lfloor s \rfloor$ die größte ganze Zahl $\leq s$ bedeutet und der rationale Rest r/d die Bedingungen $0 \leq r/d < 1$ erfüllt. In dieser Form kann man auch eine Division mit Rest für jede reelle Zahl aus den Axiomen der reellen Zahlen beweisen.

SATZ 3.2. *Die Untergruppen von $\mathbb{Z}$ sind genau die Teilmengen der Form*

$$\mathbb{Z}d = \{kd | \, k \in \mathbb{Z}\}$$

mit einer eindeutig bestimmten nicht-negativen Zahl d.

Proof. Eine Teilmenge der Form $\mathbb{Z}d$ ist aufgrund der Distributivgesetze eine Untergruppe. Sei umgekehrt $H \subseteq \mathbb{Z}$ eine Untergruppe. Bei $H = 0$ kann man $d = 0$ nehmen, so dass wir voraussetzen dürfen, dass H neben 0 noch mindestens ein weiteres Element x enthält. Wenn x negativ ist, so muss die Untergruppe H auch das Negative davon, also $-x$ enthalten, welches positiv ist. D.h. H enthält auch positive Zahlen. Sei nun d die kleinste positive Zahl aus H. Wir behaupten $H = \mathbb{Z}d$. Dabei ist die Inklusion $\mathbb{Z}d \subseteq H$ klar, da mit d alle (positiven und negativen) Vielfache von d dazugehören müssen. Für die umgekehrte Inklusion sei $h \in H$ beliebig. Nach Satz 3.1 gilt

$$h = qd + r \text{ mit } 0 \leq r < d \, .$$

Wegen $h \in H$ und $qd \in H$ ist auch $r = h - qd \in H$. Nach der Wahl von d muss wegen $r < d$ gelten: $r = 0$. Dies bedeutet $h = qd$ und damit $h \in \mathbb{Z}d$, also $H \subseteq \mathbb{Z}d$. □

Bevor wir uns fragen, wie man zu einer durch verschiedene Zahlen erzeugte Untergruppe einen einzigen Erzeuger findet, besprechen wir einige Folgerungen für endliche Gruppen.

LEMMA 3.3. *Es sei G eine Gruppe und $x \in G$ ein Element mit endlicher Ordnung $d = \operatorname{ord}(x)$. Dann ist die Menge*

$$M = \{k \in \mathbb{Z} | \, x^k = e_G\}$$

eine Untergruppe von $\mathbb{Z}$, die von d erzeugt wird.

Proof. Es ist einfach zu sehen, dass M eine Untergruppe von $\mathbb{Z}$ ist. Da d die Ordnung von x ist, gilt $d \in M$ und damit $\mathbb{Z}d \subseteq M$. Nach Satz 3.2 ist $M = \mathbb{Z}a$ mit $0 \leq a \leq d$. Bei $a < d$ wäre aber $x^a = e$ nach Definition von M und d könnte nicht die Ordnung sein. □

Endliche zyklische Gruppen

SATZ 3.4. *Sei G eine zyklische Gruppe. Dann ist auch jede Untergruppe von G zyklisch.*

Proof. Sei u ein Erzeuger von G, d.h. jedes Element $z \in G$ lässt sich darstellen als ku mit $k \in \mathbb{Z}$. Es sei $H \subseteq G$ eine Untergruppe. Dazu definieren wir die Menge

$$M = \{k \in \mathbb{Z} | \, ku \in H\}.$$

Dies ist eine Untergruppe von $\mathbb{Z}$. Aus $ku \in H$ und $mu \in H$ folgt sofort aufgrund von Lemma 2.2

$$(k+m)u = ku + mu \in H,$$

also $k + m \in M$. Ebenso gehört wegen

$$(-k)u = -(ku) \in H$$

auch das Negative zu M. Daher ist nach Satz 3.2 $M = \mathbb{Z}d$ mit einem eindeutig bestimmten $d \geq 0$. Wir behaupten, dass

$$H = (du)$$

ist, dass also das d-Fache von u die Untergruppe erzeugt. Wegen $d \in M$ ist $du \in H$ und die Inklusion $(du) \subseteq H$ klar. Sei umgekehrt $h \in H$ und $h = ku$. Dann ist $k = rd$ für ein $r \in \mathbb{Z}$ und daher

$$h = ku = (rd)u = r(du).$$

□

Die folgende Aussage gilt allgemeiner in jeder endlichen Gruppe und für jede Untergruppe, der Beweis braucht dann aber das Konzept der Nebenklassen.

Korollar 3.5. *Sei G eine endliche zyklische Gruppe und $x \in G$ ein Element. Dann teilt die Ordnung* $\operatorname{ord}(x)$ *die Gruppenordnung* $\operatorname{ord}(G)$.

Proof. Sei u ein Erzeuger von G. Dann ist die Ordnung von u gleich der Ordnung n von G. Wir schreiben $x = u^m$. Dann ist

$$x^n = (u^m)^n = u^{mn} = (u^n)^m = e^m = e.$$

Daher gehört die Gruppenordnung n zur Menge

$$M = \{k \in \mathbb{Z} | \, x^k = e\}.$$

Diese hat nach Lemma 3.3 die Gestalt $M = \mathbb{Z}d$, wobei d die Ordnung von x ist. Also ist $n \in \mathbb{Z}d$ und d ist ein Teiler von n. □

Teilbarkeitsbegriffe

Es sei $d_1, \ldots, d_n$ eine Menge von ganzen Zahlen und $H \subseteq \mathbb{Z}$ die dadurch erzeugte Untergruppe von $\mathbb{Z}$, also

$$H = (d_1, \ldots, d_n) = \{a_1 d_1 + \ldots + a_n d_n | \, a_i \in \mathbb{Z}\}.$$

Nach den obigen Resultaten gibt es ein eindeutig bestimmtes $d \in \mathbb{N}$ mit $H = \mathbb{Z}d$. Wie findet man dieses d? Hierzu muss man vor allem den Fall von zwei Erzeugern verstehen. Denn wenn $(d_1, d_2) = \mathbb{Z}d$ ist, so ist auch

$$(d_1, \ldots, d_n) = (d, d_3, \ldots, d_n)\,,$$

und die Anzahl der Erzeuger ist um eins reduziert. In diesem Zusammenhang erinnern wir an verschiedene Sprechweisen, die schon aus der Schule bekannt sind.

DEFINITION 3.6. 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 gibt derart, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

LEMMA 3.7. *(Teilbarkeitsregeln)*

In $\mathbb{Z}$ gelten folgende Teilbarkeitsbeziehungen.

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

Proof. □

Siehe Aufgabe 3.6.

DEFINITION 3.8. Seien $a_1, \ldots, a_k$ ganze Zahlen. Dann heißt eine ganze Zahl t *gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn t jedes a_i teilt ($i = 1, \ldots, k$).

Eine ganze Zahl g heißt *größter gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn g ein gemeinsamer Teiler ist und wenn jeder gemeinsame Teiler t dieses g teilt.

Die Elemente $a_1, \ldots, a_k$ heißen *teilerfremd*, wenn 1 ihr größter gemeinsamer Teiler ist.

LEMMA 3.9. *Seien $a_1, \ldots, a_k$ ganze Zahlen und $H = (a_1, \ldots, a_k)$ die davon erzeugte Untergruppe. Eine ganze Zahl t ist ein gemeinsamer Teiler der $a_1, \ldots, a_k$ genau dann, wenn $H \subseteq \mathbb{Z}t$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn $H = \mathbb{Z}t$ ist.*

Proof. Aus $H = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $a_i\mathbb{Z} \subseteq t\mathbb{Z}$ für jedes $i = 1, \ldots k$, was gerade bedeutet, dass t diese Zahlen teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in t\mathbb{Z}$ und da $H = (a_1, \ldots, a_k)$ die kleinste Untergruppe ist, die alle a_i enthält, muss $H \subseteq t\mathbb{Z}$ gelten.

Aufgrund von Satz 3.2 wissen wir, dass es eine ganze Zahl g gibt mit $H = \mathbb{Z}g$. Für einen anderen gemeinsamen Teiler t der a_i gilt $\mathbb{Z}g = H \subseteq \mathbb{Z}t$, so

dass g von allen anderen gemeinsamen Teilern geteilt wird, also ein größter gemeinsamer Teiler ist. $\square$