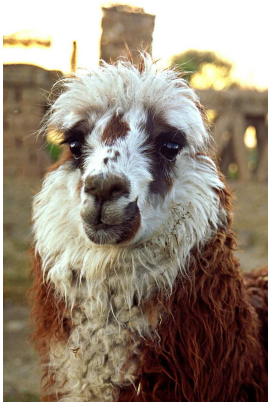
Prof. Dr. H. Brenner **Osnabrück SS 2020**

Diskrete Mathematik

Vorlesung 8



Als Alternative wurde über ein Vorlesungslama ...

In dieser Vorlesung besprechen wir die Teilbarkeitsrelation innerhalb der natürlichen und der ganzen Zahlen genauer. Dies ist einerseits eine wichtige Ordnungsrelation, die darüber hinaus eng mit der additiven und der multiplikativen Struktur der ganzen Zahlen verbunden ist. Insbesondere werden wir die Untergruppen der ganzen Zahlen charakterisieren, was wiederum eine wichtige Voraussetzung für die Konstruktion von endlichen Ringen und Körpern in der zwölften Vorlesung ist, und wir werden die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ beweisen. Ferner führen die Überlegungen zum euklidischen Algorithmus.

Das Lemma von Bezout

Beispiel 8.1. Die Wasserspedition „Alles im Eimer“ verfügt über einen 7- und einen 10-Liter-Eimer, die allerdings keine Markierungen haben. Sie erhält den Auftrag, insgesamt genau einen Liter Wasser von der Nordsee in die Ostsee zu transportieren. Kann sie diesen Auftrag erfüllen?

Die Aufgabe ist lösbar: Man macht dreimal den 7-Liter-Eimer in der Nordsee voll und transportiert dies in die Ostsee. Danach (oder gleichzeitig) macht man zweimal den 10-Liter-Eimer in der Ostsee voll und transportiert dies in die Nordsee. Unterm Strich hat man dann

$$3 \cdot 7 - 2 \cdot 10 = 1$$

Liter transportiert (eine andere Möglichkeit ist $5 \cdot 10 - 7 \cdot 7 = 1$).

Die dieser Überlegung zugrunde liegende Aussage heißt *Lemma von Bezout*.

Satz 8.2. *Es seien $a, b \in \mathbb{N}$ zwei teilerfremde natürliche Zahlen. Dann gibt es ganze Zahlen $r, s \in \mathbb{Z}$ mit $ra + sb = 1$.*

Beweis. Dies wird sich weiter unten als Korollar zu Korollar 8.5 ergeben, man kann es aber auch direkt durch Induktion über das Maximum von a und b beweisen, siehe Aufgabe 8.7. □

Man sagt auch, dass $ra + sb = 1$ eine *Darstellung* der 1 als eine *Linearkombination* der a und b ist. Die r, s heißen *Koeffizienten* der Darstellung.

Die Untergruppen von $\mathbb{Z}$

Die Division mit Rest für ganze Zahlen ist analog zur Polynomdivision.

Satz 8.3. *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*

$$n = qd + r.$$

Beweis. Siehe Aufgabe 8.8. □

Wie im eingangs gegebenen Beispiel kann man sich eine Menge $a_1, \ldots, a_k$ von ganzen Zahlen (Eimergrößen) vorgeben und sich fragen, welche Zahlen man daraus mit Hilfe von ganzzahligen Koeffizienten bilden kann (welche Wassermengen man transportieren kann). Es geht also um die Menge aller Zahlen der Form

$$n_1a_1 + \cdots + n_ka_k \text{ mit } n_j \in \mathbb{Z}\,.$$

Diese Gesamtmenge bildet eine Untergruppe von $\mathbb{Z}$, siehe Aufgabe 8.37, man spricht von der von den $a_1, \ldots, a_k$ *erzeugten Untergruppe* von $\mathbb{Z}$. Statt Eimern kann man sich auch eine Menge von ganzzahligen Pfeilen, die man hintereinanderlegen und umdrehen kann, vorstellen, oder eine vorgegebene Menge an Sprungmöglichkeiten, oder eine Menge an Gewichten. Der folgende Satz heißt auch „Ein-Eimer-Satz“.

Satz 8.4. *Die Untergruppen von $\mathbb{Z}$ sind genau die Teilmengen der Form*

$$\mathbb{Z}d = \{kd \mid k \in \mathbb{Z}\}$$

mit einer eindeutig bestimmten nichtnegativen Zahl d.

Beweis. 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) Vielfachen von d dazugehören müssen. Für die umgekehrte Inklusion sei $h \in H$ beliebig. Nach der Division mit Rest 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 $H \subseteq \mathbb{Z}d$. □

Korollar 8.5. *Es seien $a_1, \ldots, a_k$ ganze Zahlen und $H = (a_1, \ldots, a_k) = \{n_1a_1 + n_2a_2 + \cdots + n_ka_k \mid n_j \in \mathbb{Z}\}$ 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.*

Beweis. Siehe Aufgabe 8.15. □

Dies besagt insbesondere, dass es stets einen größten gemeinsamen Teiler gibt. Im teilerfremden Fall bedeutet es, dass es eine Darstellung der 1 als ganzzahlige Linearkombination der a_i gibt.

Der Euklidische Algorithmus

Der euklidische Algorithmus dient dazu, zu gegebenen Zahlen a, b ihren größten gemeinsamen Teiler zu bestimmen, und eine Darstellung dieses größten gemeinsamen Teilers ale eine Linearkombination der a und b explizit zu finden.

Es seien a, b ganze Zahlen, $b \neq 0$. Dann kann man die Division mit Rest durchführen und erhält $a = qb + r$ mit $0 \leq r < b$. Danach kann man (bei $r \neq 0$) die Division mit Rest von b durch r durchführen, d.h. b nimmt die Rolle von a und r die Rolle von b ein und erhält einen neuen Rest. Dies kann man fortsetzen, und da dabei die Reste immer kleiner werden bricht das Verfahren irgendwann ab.

Euklid (4. Jahrhundert v. C.)

Definition 8.6. Seien zwei ganze Zahlen a, b (mit $b \neq 0$) gegeben. Dann nennt man die durch die Anfangsbedingungen $r_0 = a$ und $r_1 = b$ und die mittels der Division mit Rest

$$r_i = q_i r_{i+1} + r_{i+2}$$

rekursiv bestimmte Folge r_i die *Folge der euklidischen Reste.*

Satz 8.7. *Seien ganze Zahlen $r_0 = a$ und $r_1 = b \neq 0$ gegeben. Dann besitzt die Folge r_i, $i = 0, 1, 2, \ldots,$, der euklidischen Reste folgende Eigenschaften.*

(1) *Es ist $r_{i+2} = 0$ oder $r_{i+2} < r_{i+1}$.*
(2) *Es gibt ein (minimales) $k \geq 2$ mit $r_k = 0$.*
(3) *Es ist*

$$\mathrm{ggT}(r_{i-1}, r_i) = \mathrm{ggT}(r_i, r_{i+1})$$

für alle $i = 1, \ldots, k$

(4) *Sei $k \geq 2$ der erste Index derart, dass $r_k = 0$ ist. Dann ist*

$$\mathrm{ggT}(a, b) = r_{k-1}.$$

Beweis. (1) Dies folgt unmittelbar aus der Definition der Division mit Rest.

(2) Solange $r_i \neq 0$ ist, wird die Folge der natürlichen Zahlen r_i immer kleiner, so dass irgendwann der Fall $r_i = 0$ eintreten muss.

(3) Wenn t ein gemeinsamer Teiler von r_i und von r_{i+1} ist, so zeigt die Beziehung

$$r_{i-1} = q_{i-1} r_i + r_{i+1},$$

dass t auch ein Teiler von r_{i-1} und damit ein gemeinsamer Teiler von r_{i-1} und von r_i ist. Die Umkehrung folgt genauso.

(4) Dies folgt aus (3) mit der Gleichungskette

$$\begin{aligned} \mathrm{ggT}(a, b) &= \mathrm{ggT}(b, r_2) \\ &= \mathrm{ggT}(r_2, r_3) \\ &= \dots \\ &= \mathrm{ggT}(r_{k-2}, r_{k-1}) = \mathrm{ggT}(r_{k-1}, r_k) = \mathrm{ggT}(r_{k-1}, 0) = r_{k-1}. \end{aligned}$$

□

Beispiel 8.8. Aufgabe:

Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 71894 und 45327.

Lösung:

Der Euklidische Algorithmus liefert:

$$71894 = 1 \cdot 45327 + 26567$$

$$45327 = 1 \cdot 26567 + 18760$$

$$26567 = 1 \cdot 18760 + 7807$$

$$18760 = 2 \cdot 7807 + 3146$$

$$7807 = 2 \cdot 3146 + 1515$$

$$3146 = 2 \cdot 1515 + 116$$

$$1515 = 13 \cdot 116 + 7$$

$$116 = 16 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1\,.$$

Die Zahlen 71894 und 45327 sind also teilerfremd.

Bei kleinen Zahlen sieht man häufig relativ schnell direkt, was ihr größter gemeinsamer Teiler ist, da man die Primfaktorzerlegung kennt bzw. mögliche gemeinsame Teiler schnell übersehen kann. Bei zwei größeren Zahlen müssten aber viel zu viele Probedivisionen durchgeführt werden! Der euklidische Algorithmus ist also zur Bestimmung des größten gemeinsamen Teilers ein sehr effektives Verfahren!

Darstellung des größten gemeinsamen Teilers

Mit dem euklidischen Algorithmus kann man auch durch Zurückrechnen eine Darstellung des größten gemeinsamen Teilers als Linearkombination der beiden vorgegebenen Zahlen erhalten. Dazu seien

$$r_i \;=\; q_i r_{i+1} + r_{i+2}$$

die Gleichungen im euklidischen Algorithmus und $r_{k-1} \;=\; \mathrm{ggT}\,(r_0, r_1)$. Aus der letzten Gleichung

$$r_{k-3} \;=\; q_{k-3} r_{k-2} + r_{k-1}$$

erhält man die Darstellung

$$r_{k-1} \;=\; r_{k-3} - q_{k-3} r_{k-2}$$

von r_{k-1} als Linearkombination mit r_{k-3} und r_{k-2}. Mit der vorhergehenden Zeile

$$r_{k-4} \;=\; q_{k-4} r_{k-3} + r_{k-2}$$

bzw.

$$r_{k-2} \;=\; r_{k-4} - q_{k-4} r_{k-3}$$

kann man in dieser Darstellung r_{k-2} ersetzen und erhält eine Darstellung von r_{k-1} als Linearkombination von r_{k-3} und r_{k-4}. So fortfahrend erhält man schließlich eine Darstellung von

$$r_{k-1} \;=\; \mathrm{ggT}\,(r_0, r_1)$$

als Linearkombination von r_0 und r_1.

Beispiel 8.9. Wir wollen für 52 und 30 eine Darstellung des größten gemeinsamen Teilers finden. Wir führen dazu den euklidischen Algorithmus durch.

$$52 = 1 \cdot 30 + 22$$

$$30 = 1 \cdot 22 + 8$$

$$22 = 2 \cdot 8 + 6$$

$$8 = 1 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0\,.$$

D.h. 2 ist der größte gemeinsame Teiler von 52 und 30. Rückwärts gelesen erhält man daraus die Darstellung

$$\begin{aligned} 2 &= 8 - 6 \\ &= 8 - (22 - 2 \cdot 8) \\ &= 3 \cdot 8 - 22 \\ &= 3 \cdot (30 - 22) - 22 \\ &= 3 \cdot 30 - 4 \cdot 22 \\ &= 3 \cdot 30 - 4 \cdot (52 - 30) \\ &= 7 \cdot 30 - 4 \cdot 52. \end{aligned}$$

Kleinstes gemeinsames Vielfaches und größter gemeinsamer Teiler

Zu einer ganzen Zahl a besteht $\mathbb{Z}a$ aus allen Vielfachen von a. Zu zwei Zahlen a, b besteht somit der Durchschnitt $\mathbb{Z}a \cap \mathbb{Z}b$ aus allen Zahlen, die sowohl von a als auch von b Vielfache sind, also aus allen gemeinsamen Vielfachen von a und b. In der Tat gilt die folgende Aussage.

Lemma 8.10. *Es seien $a_1, \ldots, a_k$ ganze Zahlen. Dann ist*

$$\mathbb{Z}a_1 \cap \mathbb{Z}a_2 \cap \ldots \cap \mathbb{Z}a_k \;=\; \mathbb{Z}u,$$

wobei u das kleinste gemeinsame Vielfache der $a_1, \ldots, a_k$ ist.

Beweis. Siehe Aufgabe 8.27. □

Für ganze Zahlen setzen wird den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache stets positiv an, um Eindeutigkeit zu erzielen. Grundsätzlich hat jeweils das Negative dazu die gleichen Eigenschaften.

Lemma 8.11. *Für natürliche Zahlen a, b, g gelten folgende Aussagen.*

(1) *Für teilerfremde a, b ist*

$$\mathrm{kgV}\,(a,b) \;=\; ab.$$

(2) *Es gibt $c, d \in \mathbb{Z}$ mit*

$$a = c \cdot \mathrm{ggT}\,(a,b) \text{ und } b = d \cdot \mathrm{ggT}\,(a,b)\,,$$

wobei c, d teilerfremd sind.

(3) *Es ist*

$$\mathrm{kgV}\,(ga,gb) \;=\; g \cdot \mathrm{kgV}\,(a,b).$$

(4) *Es ist*

$$\mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(a,b) \;=\; ab.$$

Beweis. Siehe Aufgabe 8.28. □

Der Teil (4) der vorstehenden Aussage erlaubt es, das kleinste gemeinsame Vielfache zu zwei Zahlen algorithmisch dadurch zu bestimmen, dass man ihren größten gemeinsamen Teiler mit Hilfe des euklidischen Algorithmus bestimmt und das Produkt durch diesen teilt.

Der Hauptsatz der elementaren Zahlentheorie

Wir möchten nun zur Primfaktorzerlegung, deren Existenz wir bereits in Satz 2.5 (Mathematik für Anwender (Osnabrück 2019-2020)) gezeigt haben, beweisen, dass sie eindeutig ist. Natürlich kann man

$$12 \;=\; 3 \cdot 2 \cdot 2 \;=\; 2 \cdot 3 \cdot 2 \;=\; 2 \cdot 2 \cdot 3$$

schreiben, mit eindeutig ist also eindeutig bis auf die Reihenfolge gemeint. Um dies zu zeigen brauchen wir zunächst das sogenannte *Lemma von Euklid*, das eine wichtige Eigenschaft einer Primzahl beschreibt.

Satz 8.12. *Es sei p eine Primzahl und p teile ein Produkt ab von natürlichen Zahlen $a, b \in \mathbb{N}$. Dann teilt p einen der Faktoren.*

Beweis. Wir setzen voraus, dass a kein Vielfaches von p ist (andernfalls sind wir fertig). Dann müssen wir zeigen, dass b ein Vielfaches von p ist. Unter der gegebenen Voraussetzung sind a und p teilerfremd. Nach dem Lemma von Bezout gibt es ganze Zahlen r, s mit

$$ra + sp \;=\; 1$$

Da ab ein Vielfaches von p ist, gibt es ein t mit

$$ab \;=\; tp.$$

Daher ist

$$b \;=\; b \cdot 1 \;=\; b(ra + sp) \;=\; abr + bsp \;=\; tpr + bsp \;=\; p(tr + bs).$$

Also ist b ein Vielfaches von p. □

Aus dem Lemma von Euklid folgt sofort die etwas stärkere Aussage: Wenn eine Primzahl p ein beliebiges Produkt $a_1a_2\cdots a_n$ teilt, dann teilt p mindestens einen Faktor. Man wendet das Lemma einfach auf $(a_1a_2\cdots a_{n-1})\cdot a_n$ an (formal ist das eine Induktion über die Anzahl der Faktoren). Dies wird im Beweis des folgenden *Hauptsatzes der elementaren Zahlentheorie* verwendet.

SATZ 8.13. *Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine eindeutige Zerlegung in Primfaktoren.*

D.h. es gibt eine Darstellung

$$n = p_1\cdots p_r$$

mit Primzahlen p_i, und dabei sind die Primfaktoren bis auf ihre Reihenfolge eindeutig bestimmt.

Beweis. Die Existenz der Primfaktorzerlegung wurde bereits in Satz 2.5 (Mathematik für Anwender (Osnabrück 2019-2020)) gezeigt. Die Eindeutigkeit wird durch Induktion über n gezeigt. Für $n = 2$ liegt eine Primzahl vor. Sei nun $n \geq 3$ und seien zwei Zerlegungen in Primfaktoren gegeben, sagen wir

$$n = p_1\cdots p_r = q_1\cdots q_s.$$

Wir müssen zeigen, dass nach Umordnung die Primfaktorzerlegungen übereinstimmen. Die Gleichheit bedeutet insbesondere, dass die Primzahl p_1 das Produkt rechts teilt. Nach Satz 6.12 muss dann p_1 einen der Faktoren rechts teilen. Nach Umordnung können wir annehmen, dass q_1 von p_1 geteilt wird. Da q_1 selbst eine Primzahl ist, folgt, dass $p_1 = q_1$ sein muss. Daraus ergibt sich durch Kürzen, dass

$$p_2\cdots p_r = q_2\cdots q_s$$

ist. Nennen wir diese Zahl n'. Da $n' < n$ ist, können wir die Induktionsvoraussetzung auf n' anwenden und erhalten, dass links und rechts die gleichen Primzahlen stehen. □

In der *kanonischen Primfaktorzerlegung* schreibt man die beteiligten Primzahlen in aufsteigender Reihenfolge mit ihrem jeweiligen Exponenten, also beispielsweise

$$840 = 2^3 \cdot 3 \cdot 5 \cdot 7.$$

Abbildungsverzeichnis