Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Grundkurs Mathematik I

Vorlesung 20

Wir kehren zur Thematik der Primzahlen und der Primfaktorzerlegung einer natürlichen Zahl zurück. Bisher kennen wir nur die Existenz einer Primfaktorzerlegung (siehe Satz 12.9), aber noch nicht die Eindeutigkeit. Obwohl wir diese Fragestellung für natürliche Zahlen formuliert haben, ergibt sich im Kontext der ganzen Zahlen ein neuer Zusammenhang, der für diese Thematik hilfreich ist.

Teilerfremdheit und das Lemma von Bezout

Aufgabe 20.1. 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 20.2. *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. Wir beweisen die Aussage durch Induktion über das Maximum von a und b, wobei wir ohne Einschränkung $a \leq b$ wählen können. Wenn das Maximum 0 ist, so sind beide Zahlen 0 und somit nicht teilerfremd. Wenn das Maximum 1 ist, so ist $b = 1$ und somit ergeben $r = 0$ und $s = 1$ eine Darstellung der 1. Seien nun $a \leq b$ teilerfremd, $b \geq 2$ und die Aussage sei für alle Zahlenpaare, deren Maxima kleiner als b sind, schon bewiesen. Dann ist $a < b$, da bei $a = b$ die beiden Zahlen nicht teilerfremd sind. Ebenso können wir $a = 0$ ausschließen. Wir betrachten das Zahlenpaar $(a, b - a)$ und wollen darauf die Induktionsvoraussetzung anwenden. Das Maximum dieses neuen Paares ist jedenfalls kleiner als b. Allerdings müssen wir, damit die Induktionsvoraussetzung wirklich eingesetzt werden kann, wissen, dass auch a und $b-a$ teilerfemd sind. Dazu führen wir einen Widerspruchsbeweis. Nehmen wir also an, dass a und $b - a$ nicht teilerfremd sind. Dann gibt es eine natürliche Zahl $t \geq 2$, die sowohl a als auch $b - a$ teilt. Dies bedeutet wiederum, dass es natürliche Zahlen m, n mit $a = mt$ und $b - a = nt$ gibt. Doch dann ist

$$b = (b - a) + a = nt + mt = (n + m)t$$

ebenfalls ein Vielfaches von t, im Widerspruch zur Teilerfremdheit von a und b. Die Induktionsvoraussetzung ist also auf a und $b-a$ anwendbar und somit gibt es ganze Zahlen r, s mit

$$ra + s(b - a) = 1.$$

Dann ist aber auch

$$(r - s)a + sb = ra + s(b - a) = 1$$

und wir haben eine Darstellung der 1 mit a und b gefunden. □

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, die wir bisher nur für natürliche Zahlen formuliert haben, überträgt sich unmittelbar auf ganze Zahlen (der Divisor bleibt eine natürliche Zahl).

Satz 20.3. *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 20.9. □

Definition 20.4. Sei $(G, e, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe* von G wenn folgendes gilt.

(1) $e \in H$.
(2) Mit $g, h \in H$ ist auch $g \circ h \in H$.
(3) Mit $g \in H$ ist auch $g^{-1} \in H$.

In einer Untergruppe kann man also die Verknüpfung der Gruppe ausführen, man kann das Inverse nehmen und das neutrale Element gehört dazu. In additiver Schreibweise, die für uns im Mittelpunkt steht, bedeuten die Bedingungen einfach

(1) $0 \in H$.
(2) Mit $g, h \in H$ ist auch $g + h \in H$.
(3) Mit $g \in H$ ist auch das Negative $-g \in H$.

Beispielsweise bilden alle Vielfachen der 5 innerhalb der ganzen Zahlen eine Untergruppe, die wir mit $\mathbb{Z}5$ bezeichnen. Es ist ja

$$0 = 0 \cdot 5,$$

wenn $g = 5 \cdot a$ und $h = 5 \cdot b$ sind, so ist

$$h + g = 5 \cdot (a + b)$$

nach dem Distributivgesetz und mit $g = 5 \cdot a$ ist $-g = 5 \cdot (-a)$. 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

$$n_1 a_1 + \cdots + n_k a_k \text{ mit } n_j \in \mathbb{Z}\,.$$

Diese Gesamtmenge bildet eine Untergruppe von $\mathbb{Z}$, siehe Aufgabe 20.27, 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 20.5. *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.

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 $H \subseteq \mathbb{Z}d$. □

Lemma 20.6. *Seien $a_1, \ldots, a_k$ ganze Zahlen und*

$$H = (a_1, \ldots, a_k) = \{n_1a_1 + n_2a_2 + \cdots + n_ka_k | \, n_j \in \mathbb{Z}\}$$

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. 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 20.4 wissen wir, dass es eine ganze Zahl g gibt mit $H = \mathbb{Z}d$. Für einen anderen gemeinsamen Teiler t der a_i gilt $\mathbb{Z}d = H \subseteq \mathbb{Z}t$, so dass d von allen anderen gemeinsamen Teilern geteilt wird, also ein größter gemeinsamer Teiler ist. □

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 20.7. 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 20.8. *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 20.9. 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!

Wenn man mit dem euklidischen Algorithmus den größten gemeinsamen Teiler d von zwei Zahlen a und b gefunden hat, so kann man aus diesen Rechnungen auch die Quotienten $\frac{a}{d}$ und $\frac{b}{d}$ bestimmen, da dann alle euklidischen Reste Vielfache von d sind.

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 20.10. 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

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

Kommensurabilität

Es seien zwei Strecken s und t gegeben. Man sagt, dass t ein (ganzzahliges) Vielfaches von s ist, wenn es eine natürliche Zahl n mit der Eigenschaft gibt, dass sich die Strecke t ergibt, wenn man die Strecke s n-fach gerade hintereinanderlegt (die Strecke wird also n-mal genommen). Für zwei Strecken s und t gibt es das folgende Konzept, das ihre ganzzahlige Vergleichbarkeit ausdrückt. Man beachte, dass dieses Konzept unabhängig von solchen Messungen ist, die die Längen in Zahlen mit Hilfe von Einheiten ausdrücken. Es werden nur die beiden Längen gegeneinander gemessen, man verwendet keine normierten Standardlängen.

Definition 20.11. Zwei Strecken s und t heißen *kommensurabel*, wenn es eine Strecke g mit der Eigenschaft gibt, dass beide Strecken ganzzahlige Vielfache von g sind.

Auch vom euklidischen Algorithmus gibt es in diesem Kontext eine sinnvolle Version. Die Strecke t sei mindestens so lang wie s. Dann ist

$$t = ns + r$$

mit $n \in \mathbb{N}$ und einer „Reststrecke“ r, die kürzer als s ist und eventuell 0 ist. Die Gleichung ist dabei als eine Gleichung von hintereinander hingelegten Strecken zu verstehen. Wie in Satz 20.7 ergibt sich, dass mit s und t auch s und r kommensurabel sind. Wenn man dieses Verfahren rekursiv fortsetzt, so tritt im Falle der Kommensurabilität irgendwann die Situation auf, wo die kleine Strecke in die größere Strecke voll aufgeht. Somit hat man dann auch die größte gemeinsame Teilerstrecke gefunden.

Abbildungsverzeichnis