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

Einführung in die Algebra

Vorlesung 4

Das Lemma von Bezout

Satz 1. *(Lemma von Bézout)*

Jede Menge von ganzen Zahlen $a_1, \ldots, a_n$ besitzt einen größten gemeinsamen Teiler d, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt ganze Zahlen $r_1, \ldots, r_n$ mit

$$r_1a_1 + r_2a_2 + \ldots + r_na_n = d\,.$$

Insbesondere gibt es zu teilerfremden ganzen Zahlen $a_1, \ldots, a_n$ eine Darstellung der 1.

Beweis. Dies folgt direkt aus Lemma 3.9 und Satz 3.2. □

Man beachte, dass ein größter gemeinsamer Teiler, der nach dem Lemma von Bézout existiert, nicht eindeutig bestimmt ist. Denn ebenso ist mit g auch das Negative $-g$ ein größter gemeinsamer Teiler. Häufig wählt man den Vertreter ≥ 0, um Eindeutigkeit zu erreichen, und spricht dann von *dem größten gemeinsamer Teiler* der $a_1, \ldots, a_n$. Diese Zahl wird dann mit

$$\mathrm{ggT}\,(a_1, \ldots, a_n)$$

bezeichnet. Wir besprechen nun, wie man algorithmisch zu vorgegebenen ganzen Zahlen den ggT finden kann.

Der Euklidische Algorithmus

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.

DEFINITION 1. 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 Division mit Rest

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

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

SATZ 2. *Seien zwei 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 $\mathrm{ggT}(r_{i+1}, r_i) = \mathrm{ggT}(r_i, r_{i-1})$.*
(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+1} und von r_{i+2} ist, so zeigt die Beziehung

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

dass t auch ein Teiler von r_i 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

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

□

BEISPIEL 3. Aufgabe: Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 71894 und 45327.

Lösung:

Der Euklidischen 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 4. 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

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

Gemeinsame Vielfache

Nachdem wir schon die gemeinsamen Teiler von ganzen Zahlen behandelt haben, wenden wir uns einem verwandten Begriff zu, der ebenfalls aus der Schule bekannt ist, nämlich dem des kleinsten gemeinsamen Vielfachen von ganzen Zahlen. In der Schule wird dabei „kleinste“ in Bezug auf die $\leq$-Ordnung verstanden. Wir benutzen einen äquivalenten Begriff, der sich besser auf eine weit allgemeinere Situation übertragen lässt.

Definition 2. Zu einer Menge von ganzen Zahlen

$$a_1, \ldots, a_n$$

heißt eine ganze Zahl b ein *gemeinsames Vielfaches*, wenn b ein Vielfaches von jedem a_i ist, also von jedem a_i geteilt wird. Die Zahl b heißt ein *kleinstes gemeinsames Vielfaches* der $a_1, \ldots, a_n$, wenn b ein gemeinsames Vielfaches ist und wenn jedes andere gemeinsame Vielfache ein Vielfaches von b ist.

Wir werden gleich sehen, dass es stets ein kleinstes gemeinsames Vielfaches gibt, und dass dieses, wenn man es ≥ 0 wählt, auch eindeutig bestimmt ist. Man spricht dann einfach von *dem* kleinsten gemeinsamen Vielfachen, geschrieben $\mathrm{kgV}\,(a_1, \ldots, a_n)$.

Satz 5. *Zu einer Menge von ganzen Zahlen*

$$a_1, \ldots, a_n$$

existiert genau ein kleinstes gemeinsames Vielfaches ≥ 0*, und zwar ist* $\mathrm{kgV}\,(a_1, \ldots, a_n)$ *der eindeutig bestimmte Erzeuger* $b \geq 0$ *der Untergruppe*

$$\mathbb{Z}a_1 \cap \ldots \cap \mathbb{Z}a_n\,.$$

Beweis. Es ist klar, dass eine ganze Zahl b ein gemeinsames Vielfaches der $a_1, \ldots, a_n$ ist genau dann, wenn

$$b \in \mathbb{Z}a_1 \cap \ldots \cap \mathbb{Z}a_n \text{ bzw. } \mathbb{Z}b \subseteq \mathbb{Z}a_1 \cap \ldots \cap \mathbb{Z}a_n$$

gilt. Nach Satz 3.2 gibt es ein eindeutig bestimmtes $c \geq 0$ mit

$$\mathbb{Z}c = \mathbb{Z}a_1 \cap \ldots \cap \mathbb{Z}a_n\,.$$

Nach der Vorüberlegung ist daher c ein gemeinsames Vielfaches und für jedes weitere gemeinsame Vielfache b gilt

$$\mathbb{Z}b \subseteq \mathbb{Z}c\,.$$

Dies bedeutet, dass b ein Vielfaches von c ist. □

Lemma 6. *Für ganze Zahlen* a, b, g *mit* $g \geq 0$ *gelten folgende Aussagen.*

(1) *Für teilerfremde* a, b *ist* $\mathrm{kgV}\,(a, b) = ab$.
(2) *Es gibt* $c, d \in \mathbb{Z}$ *mit* $a = c \cdot \mathrm{ggT}\,(a, b)$ *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* $\mathrm{ggT}\,(a, b)\,\mathrm{kgV}\,(a, b) = ab$.

Beweis. (1) Zunächst ist natürlich das Produkt ab ein gemeinsames Vielfaches von a und b. Sei also f irgendein gemeinsames Vielfaches, also $f = ua$ und $f = vb$. Nach Satz 4.1 gibt es im teilerfremden Fall Zahlen $r, s \in \mathbb{Z}$ mit $ra + sb = 1$. Daher ist

$$f = f \cdot 1 = f(ra + sb) = fra + fsb = vbra + uasb = (vr + us)ab$$

ein Vielfaches von ab.

(2) Die Existenz von c und d ist klar. Hätten c und d einen gemeinsamen Teiler $e \neq 1, -1$, so ergebe sich sofort der Widerspruch, dass $e \cdot \mathrm{ggT}\,(a,b)$ ein (größerer) gemeinsamer Teiler wäre.

(3) Die rechte Seite ist offenbar ein gemeinsames Vielfaches von ga und gb. Sei n ein Vielfaches der linken Seite, also ein gemeinsames Vielfaches von ga und gb. Dann kann man schreiben $n = uga$ und $n = vgb$. Damit ist $uga = vgb$ und somit ist $k := ua = vb$ (bei $n \neq 0$; $n = 0$ ist erst recht ein Vielfaches der rechten Seite) ein gemeinsames Vielfaches von a und b. Also ist $n = gk$ ein Vielfaches der rechten Seite.

(4) Wir schreiben unter Verwendung der ersten Teile

$$\begin{aligned}
\mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(a,b) &= \mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(c \cdot (\mathrm{ggT}\,(a,b)), d \cdot (\mathrm{ggT}\,(a,b))) \\
&= \mathrm{ggT}\,(a,b) \cdot \mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(c,d) \\
&= \mathrm{ggT}\,(a,b) \cdot \mathrm{ggT}\,(a,b) \cdot cd \\
&= c \cdot \mathrm{ggT}\,(a,b) \cdot d \cdot \mathrm{ggT}\,(a,b) \\
&= ab\,.
\end{aligned}$$

□

Abbildungsverzeichnis