1.3.3 Einheiten und Nullteiler

Definition 20 Es sei $(R, +, \cdot)$ ein Ring und $r \in R$. Hat r ein multiplikatives Inverses (d. h. gibt es ein $r^{-1} \in R$ mit $r \cdot r^{-1} = r^{-1} \cdot r = 1$), so heißt r *Einheit*.

Beispiel 22 Die Menge der Einheiten von $\mathbb{Z}$ ist $\{1, -1\}$ und die von $\mathbb{Q}$ ist $\mathbb{Q} \setminus \{0\}$.

Definition 21 Es sei $(R, +, \cdot)$ ein Ring und $a \in R$. Dann ist a ein *Nullteiler* von R, wenn $a \neq 0$ ist und wenn es ein $b \in R$ mit $b \neq 0$ gibt, sodass $a \cdot b = 0$ ist.

Bemerkung 10 Die Zahlbereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind allesamt nullteilerfrei, d. h. man kann in ihnen aus der Gültigkeit der Gleichung $a \cdot b = 0$ folgern, dass a oder b gleich Null ist. Das ist bei Restklassenringen nicht unbedingt so, d. h. es gibt Restklassenringe, die Nullteiler enthalten. Man sieht beispielsweise an der Verknüpfungstafel aus Beispiel 21, dass $(\mathbb{Z}_4, \odot)$ nicht nullteilerfrei ist: Es gibt Elemente ungleich $\overline{0}$, deren Produkt $\overline{0}$ ist. Beispielsweise ist $\overline{2} \odot \overline{2} = \overline{0}$.

1.3.4 Der euklidische Algorithmus

Satz 17 (Eindeutige Division mit Rest in $\mathbb{N}$) *Für alle $n, q \in \mathbb{N}$ mit $q \neq 0$ gibt es genau ein $s \in \mathbb{N}$ und genau ein $r \in \mathbb{N}$, sodass*

$$n = s \cdot q + r$$

mit $0 \leq r < q$ gilt.

BEWEIS Nachweis der Existenz) Fall 1: Es sei $q > n$. Dann ist $n = s \cdot q + r$ mit $s = 0$ und $r = n$ erfüllt.

Fall 2: Es sei $q \leq n$. Man betrachte die Menge $H = \{h \in \mathbb{N} \mid n \geq h \cdot q\}$. Da $n \geq q > 0$ ist, ist $n - 0 \cdot q > 0$ und damit $0 \in H$. Also ist H nicht leer. Da $n \cdot q > n$ und damit $n - n \cdot q \notin \mathbb{N}$ ist, ist n eine obere Schranke von H. Also existiert nach **??** das Maximum $max(H)$ von H. Es sei $s := max(H)$ und $r := n - s \cdot q$. Mit diesen Werten für s und r ist $n = s \cdot q + r$ erfüllt. Nun ist nur noch zu zeigen, dass $0 \leq r < q$ ist. Man nehme an, dass $r \geq q$ sei. Dann ist $q \leq r = n - s \cdot q$, also $0 \leq n - s \cdot q - q = n - (s + 1) \cdot q$, d. h. $n \geq (s + 1) \cdot q$. Das steht aber im Widerspruch dazu, dass s das Maximum von H ist. Also ist $r \not\geq q$ und damit $0 \leq r < q$. Insgesamt ist dadurch gezeigt, dass es ein s und ein r mit den gewünschten Eigenschaften gibt.

Nachweis der Eindeutigkeit) Es seien s^* und r^* natürliche Zahlen mit $n = s^* \cdot q + r^*$ und $0 \leq r^* < q$. Nun ist zu zeigen, dass $r = r^*$ und $s = s^*$ ist. Ohne Beschränkung der Allgemeingültigkeit kann man annehmen, dass $s^* \geq s$ ist (andernfalls vertausche man die Bezeichnungen). Dann ist wegen $n = s^* \cdot q + r^* = s \cdot q + r$ auch $(s^* - s) \cdot q = r - r^*$. Da wegen $s^* \geq s$ auch $s^* - s \geq 0$ gilt, ist $(s^* - s) \cdot q \geq 0$ und daher $r - r^* \geq 0$. Da sowohl $0 \leq r < q$ als auch $0 \leq r^* < q$ gelten, ist $r - r^* < q$ und daher $(s^* - s) \cdot q = r - r^* < q$. Da aber $s^* - s \in \mathbb{N}$ ist, ist die Ungleichung $(s^* - s) \cdot q < q$ nur für $s^* - s = 0$ erfüllt.

Also ist $s = s^*$. Andererseits ist dann auch $r - r^* = (s^* - s) \cdot q = 0 \cdot q = 0$, also $r = r^*$. Damit ist die Eindeutigkeit gezeigt.

Beispiel 23 Es ist

$$49 = 5 \cdot 9 + 4$$

Also ist $49 = s \cdot 9 + r$ mit $s = 5$ und $r = 4$ erfüllt. Der Beweis zum Satz 17 ist konstruktiv, d. h. man kann ihn benutzen, um s und r zu berechnen. Die im Beweis definierte Menge $H = \{h \in \mathbb{N} \mid 49 \geq h \cdot 9\}$ enthält gerade die Faktoren h, mit denen man 9 multiplizieren kann, sodass $h \cdot 9$ kleiner oder gleich 49 ist, d. h. es ist $H = \{1, 2, 3, 4, 5\}$. Also ist nach dem Beweis $s = max(H) = 5$. Man erhält r dann durch Umstellen der Gleichung $n = s \cdot q + r$ nach r, d. h. es ist $r = n - s \cdot q = 49 - s \cdot 9 = 49 - 5 \cdot 9 = 4$.

Satz 18 *Es seien $n, s, q, r \in \mathbb{N}$ mit $n = s \cdot q + r$ und $0 \leq r < q$ sowie $q \neq 0$ und $n \neq 0$. Dann ist*

$$T_n \cap T_q = T_q \cap T_r$$

und damit insbesondere

$$ggT(n, q) = ggT(q, r).$$

BEWEIS Es sei t ein gemeinsamer Teiler von n und q, d. h. es gelte $t \in T_n \cap T_q$. Dann gilt $t \mid n$ und $t \mid q$ und n auch $t \mid s \cdot q$. Daraus folgt $t \mid r$. Also ist t ein gemeinsamer Teiler von q und r, d. h. $t \in T_q \cap T_r$ bzw. $T_n \cap T_q \subseteq T_q \cap T_r$

Umgekehrt sei t ein gemeinsamer Teiler von q und r. Dann gilt auch $t \mid s \cdot q$ und daher auch $t \mid n$. Also ist t ein gemeinsamer Teiler von n und q, d. h. $t \in T_n \cap T_q$ bzw. $T_q \cap T_r \subseteq T_n \cap T_q$

Insgesamt erhält man, dass $T_n \cap T_q = T_q \cap T_r$ ist, und damit auch dass $ggT(n, q) = max(T_n \cap T_q) = max(T_q \cap T_r) = ggT(q, r)$ ist.

Beispiel 24 Satz 18 kann man benutzen, um die Berechnung des größten gemeinsamen Teilers zu vereinfachen. Sucht man $ggT(984, 972)$, so kann man zunächst eine Division mit Rest durchführen und erhält

$$984 = 1 \cdot 972 + 12.$$

Also ist $ggT(984, 972) = ggT(972, 12)$. Nun kann man Satz 18 ein zweites Mal bemühen und für 972 und 12 eine Division mit Rest durchführen. Man erhält dann

$$972 = 81 \cdot 12 + 0.$$

Also ist 12 ein gemeinsamer Teiler von 972 und 12, und da 12 keinen größeren Teiler als 12 hat, ist 12 zugleich der größte gemeinsame Teiler der beiden Zahlen. Also ist $12 = ggT(974, 12) = ggT(984, 972)$.

Das eben in Beispiel 24 veranschaulichte Verfahren aus Satz 18 wird im euklidischen Algorithmus systematisch ausgenutzt, um den größten gemeinsamen Teiler zweier

natürlicher Zahlen zu berechnen. Mit diesem Algorithmus werden wir uns jetzt näher beschäftigen.

Satz 19 (Euklidischer Algorithmus) *Es seien $n, q \in \mathbb{N}$ mit $n > q > 0$. Dann gibt es für ein $l \in \mathbb{N}$ natürliche Zahlen $s_1, s_2, \ldots, s_{l+1}$ und $r_1, r_2, \ldots, r_l, r_{l+1}$ mit den folgenden Eigenschaften:*

$$\begin{array}{rcll} n & = & s_1 \cdot q + r_1 & \text{mit } 0 < r_1 < q \\ q & = & s_2 \cdot r_1 + r_2 & \text{mit } 0 < r_2 < r_1 \\ r_1 & = & s_3 \cdot r_2 + r_3 & \text{mit } 0 < r_3 < r_2 \\ r_2 & = & s_4 \cdot r_3 + r_4 & \text{mit } 0 < r_4 < r_3 \\ & \vdots & & \vdots \\ r_{l-2} & = & s_l \cdot r_{l-1} + r_l & \text{mit } 0 < r_l < r_{l-1} \\ r_{l-1} & = & s_{l+1} \cdot r_l + r_{l+1} & \text{mit } r_{l+1} = 0 \end{array}$$

mit $q > r_1 > r_2 > \ldots > r_{l-1} > r_l > 0$ und $r_{l+1} = 0$ sowie $ggT(n, q) = r_l$.

BEWEIS Induktionsanfang) Für n und q gibt es nach Satz 17 $s_1, r_1 \in \mathbb{N}$ mit $n = s_1 \cdot q + r_1$ und $0 \leq r_1 < q$, und nach Satz 18 ist $ggT(n, q) = ggT(q, r_1)$.

Induktionssschritt) Für $k \in \mathbb{N}$ sei bereits gezeigt, dass es $s_k, r_k \in \mathbb{N}$ mit $r_{k-2} = s_k \cdot r_{k-1} + r_k$ und $0 \leq r_k < r_{k-1}$ und $ggT(n, q) = ggT(r_{k-1}, r_k)$ gebe. Dann gibt es nach Satz 17 $s_{k+1}, r_{k+1} \in \mathbb{N}$ mit $r_{k-1} = s_{k+1} \cdot r_k + r_{k+1}$ und $0 \leq r_{k+1} < r_k$. Nach Satz 18 ist $ggT(r_{k-1}, r_k) = ggT(r_k, r_{k+1})$ und damit $ggT(n, q) = ggT(r_k, r_{k+1})$.

Da $r_i > r_{i+1} \geq 0$ für alle $i \in \mathbb{N}$ gilt, gibt es ein $l \in \mathbb{N}$ mit $r_l > r_{l+1} = 0$. Dann ist $r_l = ggT(r_l, 0) = ggT(r_l, r_{l+1}) = ggT(n, q)$.

Beispiel 25 Man kann $ggT(963, 657)$ mit dem euklidischen Algorithmus folgendermaßen berechnen:

$$\begin{array}{rcl} 963 & = & 1 \cdot 657 + 306 \\ 657 & = & 2 \cdot 306 + 45 \\ 306 & = & 6 \cdot 45 + 36 \\ 45 & = & 1 \cdot 36 + 9 \\ 36 & = & 4 \cdot 9 + 0 \end{array}$$

Also ist $ggT(963, 657) = 9$, was man daran erkennen kann, dass 9 der letzte Rest ungleich Null ist.

Nun erfolgt der Übergang nach $\mathbb{Z}$. Die Schlüsselstelle ist der Satz, dass die eindeutige Division in $\mathbb{Z}$ ebenfalls möglich ist, wenn man die Reste auf Werte aus $\mathbb{N}_0$ beschränkt. Damit lässt sich auch der euklidische Algorithmus in $\mathbb{Z}$ anwenden.

Satz 20 (Eindeutige Division mit Rest in $\mathbb{Z}$) *Für alle $p, q \in \mathbb{Z}$ mit $q \neq 0$ gibt es genau ein $s \in \mathbb{Z}$ und genau ein $r \in \mathbb{N}$, sodass*

$$p = s \cdot q + r$$

mit $0 \leq r < |q|$ ist.

1.3.5 Einheiten und Nullteiler von Restklassenringen

Satz 21 (Lemma von Bézout) *Es sei $\overline{a} \in \mathbb{Z}_n$ und $\overline{a} \neq \overline{0}$. Dann gilt:*

1. *Wenn $ggT(a,n) > 1$ ist, dann ist $\overline{a}$ ein Nullteiler von $(\mathbb{Z}_m, \oplus, \odot)$.*
2. *Wenn $ggT(a,n) = 1$ ist, dann ist $\overline{a}$ invertierbar, d. h. eine Einheit von $(\mathbb{Z}_m, \oplus, \odot)$ und das Inverse $\overline{a}^{-1}$ lässt sich durch den euklidischen Algorithmus berechnen.*

Insbesondere gilt: Die Elemente von $\mathbb{Z}_n \setminus \{\overline{0}\}$ lassen sich in zwei disjunkte Klassen einteilen: Entweder sind sie Einheiten oder Nullteiler.

BEWEIS Es sei $ggT(a,n) > 1$. Zu zeigen ist, dass es dann ein $\overline{b} \in \mathbb{Z}_n$ gibt, sodass $\overline{b} \neq \overline{0}$ und $\overline{a} \odot \overline{b} = \overline{0}$ ist. Wegen der Repräsentantenunabhängigkeit kann annehmen, dass a eine positive, d. h. natürliche Zahl ist. Dann gilt:

$$\begin{aligned} kgV(a,n) &= \frac{a \cdot n}{ggT(a,n)} \\ &= a \cdot \frac{n}{ggT(a,n)} \end{aligned}$$

Nun setze man $b = \frac{n}{ggT(a,n)}$. Da $ggT(a,n) > 1$ ist, gilt $1 < b < n$. Also ist $\overline{b} \neq \overline{0}$. Andererseits ist $a \cdot b = kgV(a,n)$. Da $n \mid kgV(a,n)$, also $n \mid a \cdot b$ gilt, ist $\overline{a \cdot b} = \overline{0}$. Insgesamt gilt also $\overline{a} \odot \overline{b} = \overline{0}$ mit $\overline{a} \neq \overline{0}$ und $\overline{b} \neq \overline{0}$. Also ist $\overline{a}$ ein Nullteiler.

Nun sei $ggT(a,n) = 1$. Zu zeigen ist, dass $\overline{a}$ invertierbar ist, d. h. dass es ein $\overline{u} \in \mathbb{Z}_n$ mit $\overline{a} \odot \overline{u} = \overline{1}$ gibt. Es gilt:

$$\begin{aligned} & \overline{1} = \overline{a} \odot \overline{u} \\ \Leftrightarrow\ & \overline{0} = \overline{a} \odot \overline{u} \ominus \overline{1} \\ \Leftrightarrow\ & a \cdot u - 1 \equiv 0 \bmod n \\ \Leftrightarrow\ & n \mid a \cdot u - 1 \\ \Leftrightarrow\ & \exists k \in \mathbb{Z} : n \cdot k = a \cdot u - 1 \\ \Leftrightarrow\ & \exists l \in \mathbb{Z} : 1 = n \cdot l + a \cdot u \end{aligned}$$

Letzteres ist genau dann der Fall, wenn es eine Darstellung von 1 als Vielfachensumme $1 = n \cdot l + a \cdot u$ gibt. Da $ggT(a,n) = 1$ ist, gibt es (wie man aus der Zahlentheorie weiß) eine solche Darstellung. Also ist $\overline{a}$ invertierbar.