Zahlentheorie Restklassen-Strukturen, Multiplikation von Restklassen

Prof. Dr. Dörte Haftendorn, www.uni-lueneburg.de/mathe-lehramt Mai 05

In zahlentheoretischer Sicht setzt man $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ und muss als erstes zeigen, dass damit eine Multiplikation der Klassen jeweils "wohldefiniert" ist, d.h. dass das Verküpfungsergebnis nicht von der Wahl der Repräsentanten der Klassen abhängt.

Bew.: Wähle $a', b' \; mit \; \overline{a'} = \overline{a} = \overline{r_a}, \; \overline{b'} = \overline{b} = \overline{r_b}$ Zu zeigen ist: $\overline{a'} \cdot \overline{b'} = \overline{a} \cdot \overline{b}$.

Die Voraussetzung lässt sich auch schreiben als

$a' = k'm + r_a, \quad a = km + r_a, \quad b' = q'm + r_b, \quad b = qm + r_b$.

Für $r_a \cdot r_b$ gibt es nach dem Satz von der Division mit Rest eine eindeutige Darstellung

$r_a \cdot r_b = s_r \cdot m + r_{ab} \; mit 0 \le r_{ab} < m$ (*) Damit gilt:

$$\overline{a'} \cdot \overline{b'} \underset{per\ def}{=} \overline{(k'm + r_a)(q'm + r_b)} = \overline{s' \cdot m + r_a \cdot r_b} \underset{per\ def \equiv}{=} \overline{s \cdot m + r_a \cdot r_b}$$

$$= \overline{s \cdot m + s_r m + r_{ab}} \underset{per\ def \equiv}{\underset{(*)}{=}} \overline{a \cdot b} \underset{per\ def \bullet}{=} \overline{a} \cdot \overline{b}$$ Also ist die Multiplikation wohldefiniert.

Abgeschlossenheit liegt vor, weil Definition als Ergebnis ja eine Klasse angibt.

Damit ist die Menge der Restklassen $(Z / mZ, \bullet)$ bzgl. der Multiplikation eine algebraische Struktur.

In funktionaler Sicht ist die Abbildung Mod damit ein Homomorphismus bzgl. $\bullet$, das Bild eines Produktes ist das Produkt der Bilder.

Im Modul 5: $\overline{7} \cdot \overline{11} = \overline{7 \cdot 11} = \overline{77} = \overline{2}$, aber auch $\overline{7} \cdot \overline{11} = \overline{2} \cdot \overline{1} = \overline{2 \cdot 1} = \overline{2}$

In algebraischer Sicht betrachtet man $Z_m := \{0, 1, ..., m-1\}$ einfach als eine Menge, für die es nun gilt die Verknüpfung $\bullet$ zu definieren.

Definition $a, b \in Z_m := \{0, 1, ..., m-1\} \quad a \cdot b := c \; mit \; c = r_{a \cdot b} \bmod m$

Da nach dem Satz von der Divison mit Rest $c = r_{a \cdot b} \bmod m \; mit \; 0 \le c \le m-1$ eindeutig bestimmt ist, ist die Miltiplikaition in Z_m wohldefiniert und abgeschlossen. $(Z_m, \cdot)$ ist eine algebraische Struktur.

Satz: $(Z_m, \bullet) \cong (Z / mZ, \bullet)$ Die Menge der Reste und die Restklassen sind bzgl. $\bullet$ isomorph, d.h. strukturgleich, beides modulo m betrachtet.

Bew.: Offensichtlich haben sie beide m Elemente, und für die Übertragung sorgt der oben bewiesene Homomorphismus von Z auf Z / mZ, der nun zum Isomorphismus zwischen Z / mZ und Z_m wird.

Folgerung aus den Isomorphiesätzen für + und $\bullet$ ist, dass man große Freiheit bei der Notation hat. In der Kryptographie ist die algebraische Schreibweise ohne die Querstriche üblich. Der betrachtete Modul m ergibt sich aus dem Kontext.

Für die Lehre ist die Schreibweise mit den drei Strichen oft günstig, da sie den Zusammenhang besser beleuchtet.

Im Modul 11: $7 + 5 = 1$ oder $7 + 5 \underset{11}{\equiv} 1$ oder $7 + 5 = 1 \bmod 11$ oder $\overline{7} + \overline{5} = \overline{1}$

$7^2 + 5^2 \underset{11}{\equiv} 5 + 3 = 8$ oder $7^2 + 5^2 = 49 + 25 = 74 \underset{11}{\equiv} 8$ oder $\overline{7^2} + \overline{5^2} = \overline{49} + \overline{25} = \overline{5} + \overline{3} = \overline{8}$