Zahlentheorie Restklassen-Strukturen, Addieren von Restklassen

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

In zahlentheoretischer Sicht setzt man $\overline{a}+\overline{b}:=\overline{a+b}$ und muss als erstes zeigen, dass damit eine Addition der Klassen "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: $\overline{a'}+\overline{b'}=\overline{a}+\overline{b}$.

Die Voraussetzung lässt sich auch schreiben als

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

Fall A $r_a+r_b<m\ \Rightarrow r_a+r_b=r_{a+b}$, Fall B $m\le r_a+r_b<2m\ \Rightarrow r_a+r_b=m+r_{a+b}$

Damit gilt:

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

$$\begin{cases}\underset{Fall\ A}{=}\overline{(k+q)\cdot m\quad+r_{a+b}}\underset{per\ def\equiv}{=}\overline{a+b}\underset{per\ def+}{=}\overline{a}+\overline{b}\\ \underset{Fall\ B}{=}\overline{(k+q+1)\cdot m+r_{a+b}}\underset{per\ def\equiv}{=}\overline{a+b}\underset{per\ def+}{=}\overline{a}+\overline{b}\end{cases}$$

Also ist die Addition wohldefiniert.

Abgeschlossenheit liegt vor, weil Definition als Ergebnis ja eine Klasse angibt.
Damit ist die Menge der Restklassen bzgl. der Addition eine algebraische Struktur.
Mit Blick auf allgemeinere algebraische Sichtweisen kann man die Restklassen auch so schreiben: $\overline{0}=Z\cdot m=mZ,\ \overline{1}=mZ+1,\ \overline{2}=mZ+2,....$ Dabei ist $mZ=V_m$, die Menge der Vielfachen von m. $(mZ,+)$ ist eine Gruppe, wie man sich leicht überlegt, und damit eine Untergruppe von $(Z,+)$, den ganzen Zahlen. Die Restklassen sind dann die additiven Nebenklassen. Diesen Begriff gibt es allgemein in der Gruppentheorie und daher kommt die Bezeichnung Z/mZ für die Menge der Restklassen. (Lies $Z\ nach\ mZ$)

In funktionaler Sicht ist die Abbildung Mod damit ein Homomorphismus bzgl. +, das Bild einer Summe ist die Summe der Bilder.

Im Modul 5: $\overline{47}+\overline{11}=\overline{47+11}=\overline{58}=\overline{3}$, aber auch $\overline{47}+\overline{11}=\overline{2}+\overline{1}=\overline{2+1}=\overline{3}$

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

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

Da nach dem Satz von der Divison mit Rest

$c=r_{a+b}\bmod m\ \ mit\ \ 0\le c\le m-1$ eindeutig bestimmt ist, ist die Addition in Z_m wohldefiniert und abgeschlossen. $(Z_m,+)$ ist eine algebraische Struktur.

Satz: $(Z_m,+)\cong(Z/mZ,+)$ Die Menge der Reste und die Restklassen sind bzgl. + 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.