II. 2.3 Restklassenringe

Neben der Addition in $\mathbb{Z}_m$, die bereits eingeführt wurde ist, wird nun in $\mathbb{Z}_m$ auch die Multiplikation eingeführt.

Prop. Sei $m \in \mathbb{N}$ und seien $A, B \in \mathbb{Z}_m$ Restklassen, dann existiert eine eindeutige Restklasse $C \in \mathbb{Z}_m$ derart, dass $a \cdot b \in C$ für alle $a \in A$, $b \in B$ gilt.

Bew.: Man setzt $C = [a \cdot b]_m$ und zeigt, dass C nicht von $a \in A$ und $b \in B$ abhängig ist.
D.h. wenn man die Vertreter ändert, würde sich C nicht ändern. □

$$(\mathbb{Z}_m, +, \cdot)$$

VL 5.2 →

Nun sind wir berechtigt $+$ und $\cdot$ in $\mathbb{Z}_m$ durch

$$[a]_m + [b]_m := [a+b]_m$$
$$[a]_m \cdot [b]_m := [a \cdot b]_m$$

für $a, b \in \mathbb{Z}$ einzuführen.

Bsp.: $m = 7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Prop. Für jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit [1].

↑ Beweis ist direkt!

Bsp. $m = 6$

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

→ kein Körper

Gespiegelt, kann weggelassen werden

II.3 Körper

II.3.1 Körper

Eine Menge $\mathbb{K}$, die mit zwei Verknüpfungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ heißt Körper, wenn folgendes gilt:

- $(\mathbb{K}, +)$ ist eine Abelsche Gruppe (mit neutralem Elmt 0)
- $(\mathbb{K} \setminus \{0\}, \cdot)$ ist eine Abelsche Gruppe (mit neutralem Elmnt 1)
- $\forall a, b, c \in \mathbb{K}$ gilt das Distributivgesetz: $(a+b) \cdot c = a \cdot c + b \cdot c$

Mit anderen Worten: $(\mathbb{K}, +, \cdot)$ ist Körper, wenn es ein kommutativen Ring mit 1 ist, wo $0 \neq 1$ und alle nicht 0 Elemente ein multiplikatives inverses besitzen.

d.h.: $\forall a \in \mathbb{K} \setminus \{0\} : \exists a^{-1} \in \mathbb{K} \setminus \{0\} : a \cdot a^{-1} = 1$

Bsp.: $(\mathbb{Z}, +, \cdot)$ kein Körper

$(\mathbb{Q}, +, \cdot)$ Körper

$(\mathbb{R}, +, \cdot)$ Körper (sogar geordnet und Vollständig)

$(\mathbb{Z}_{11}, +, \cdot)$ Körper

$(\mathbb{Z}_6, +, \cdot)$ kein Körper

$(\mathbb{Q}, +, \cdot)$ kein Körper

II. 3.2 Restklassenkörper

Für welche $m \in \mathbb{N}$ ist $\mathbb{Z}_m$ ein Körper?

→ Es sind nur die Elemente in $\mathbb{Z}_m$ invertierbar, die keine gemeinsamen Teiler mit m haben.

Seien $a, b \in \mathbb{Z}$, dann heißt die größte Zahl $c \in \mathbb{N}$, die sowohl a als auch b teilt, der größte gemeinsame Teiler von a und b, wenn $a \neq 0, b \neq 0$.

Bezeichnung: $ggT(a,b)$. Außerdem setzen wir $ggT(0,0) = 0$.

Prop.: Seien $a, b \in \mathbb{Z}$, dann existieren $x, y \in \mathbb{Z}$ mit $ax + by = ggT(a,b)$

Beweis: Übung

Theorem: Sei $m \in \mathbb{N}$, dann ist $\mathbb{Z}_m$ genau dann ein Körper, wenn m eine Primzahl ist.

Bew.: In $\mathbb{Z}_1$ ist $0 = 1$ d.h. $[0]_1 = [1]_1$ → $\mathbb{Z}_1$ kein Körper.

$\exists\, a, b \in \mathbb{N}: a \cdot b = m,\ a \geq 2,\ b \geq 2$

$\Rightarrow [a]_m \cdot [b]_m = [a \cdot b]_m = [m]_m = [0]_m = 0$

$\Rightarrow [a]_m$ besitzt kein inverses Element, denn gäbe es ein inverses Element, so hätte man:

$0 = [a]_m^{-1} \cdot 0 = [a]_m^{-1} \cdot [a]_m \cdot [b]_m = [b]_m \Rightarrow [b]_m = 0$ ↯, da $0 < b < m$

Sei m eine Primzahl. Wir betrachten eine beliebige Restklasse c in $\mathbb{Z}_m$, die $\neq 0$ ist, d.h. $[c]_m$ mit $c \in \{1, 2, \dots, m-1\}$

Dann ist $ggT(c, m) = 1$, Also gibt $x \cdot c + y \cdot m = 1$

für $x, y \in \mathbb{Z}$ $\Rightarrow [x]_m \cdot [c]_m = [x \cdot c]_m = [1 - y \cdot m]_m \overset{m=0 \text{ in } \mathbb{Z}_m}{=} [1]_m = 1$

$\Rightarrow [c]_m^{-1} = [x]_m$

Damit sei gezeigt, dass alle nicht 0 Elemente in $\mathbb{Z}_m$ invertierbar ist.

$\Rightarrow \mathbb{Z}_m$ ist Körper □