Vorlesung vom 12.11.24

Nun sind wir berechtigt + und ° 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.

Beispiel: $m = 7$

+	[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]
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
[6]	⋮	⋮	⋮	⋮	⋮	⋮	⋮

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$[1]^{-1} \cdot [1]$ $\quad$ $[5]^{-1} = [3]$

$[2]^{-1} \cdot [4]$ $\quad$ $[6]^{-1} = [6]$

$[3]^{-1} = [5]$

$[4]^{-1} = [2]$

Proposition

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

Beispiel: $m = 6$ $\quad$ in $\mathbb{Z}_6$

·	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

2.3. Körper

2.3.1. 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 Abelsche Gruppe (mit dem neutralen Element 0)
- $(\mathbb{K} \setminus \{0\}, \cdot)$ ist Abelsche Gruppe (mit dem neutralen Element 1)
- Für alle $a, b, c \in \mathbb{K}$ gilt das Distributivgesetz $(a+b) \cdot c = a \cdot c + b \cdot c$.

> Mit anderen Worten: $(\mathbb{K}, +, \cdot)$ ist Körper, wenn es ein kommutativer Ring mit 1 ist, in dem $0 \neq 1$ ist und alle nicht-0-Elemente ein multiplikatives Inverses besitzen (d.h. zu jedem $a \in \mathbb{K} \setminus \{0\}$ gibt es ein eindeutiges Element $a^{-1} \in \mathbb{K} \setminus \{0\}$ mit $a \cdot a^{-1} = 1$.

Beispiel:
$(\mathbb{Z}, +, \cdot)$ kein Körper
$(\mathbb{Q}, +, \cdot)$ ein Körper
$(\mathbb{R}, +, \cdot)$ ein Körper
$(\mathbb{Z}_7, +, \cdot)$ ein Körper
$(\mathbb{Z}_6, +, \cdot)$ kein Körper
$(\mathbb{Q}[x], +, \cdot)$ kein Körper

2.3.2. Restklassenkörper

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

- Seien $a, b \in \mathbb{Z}$. Dann heißt die größte Zahl $k \in \mathbb{N}$, die sowohl a als auch b teilt, der größte gemeinsame Teiler von a und b, wenn a und b nicht beide 0 sind.

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

Proposition: Seien $a, b \in \mathbb{Z}$. Dann existieren $x, y \in \mathbb{Z}$ mit $\boxed{a \cdot x + b \cdot y = ggT(a, b)}$

↪ Beweis: Übungsaufgabe.

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

↳ Beweis: In $\mathbb{Z}_1$ ist $0 = 1$, d.h. $[0]_1 = [1]_1 \Rightarrow \mathbb{Z}_1$ ist kein Körper.

Ist m zusammengesetzt, so gilt $m = a \cdot b$ mit $a, b \in \mathbb{N}$, $a \geq 2$, $b \geq 2$

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

Es folgt nun, dass $[a]_m$ (es ist eine Restklasse, die ungleich 0 ist, denn $0 < a < m$) kein Inneres besitzt.

Denn, gäbe es ein Inneres $[a]_m^{-1}$, so hätte man $0 = [a]_m^{-1} \cdot 0 = [a]_m^{-1} \cdot [a]_m \cdot [b]_m = [b]_m \Rightarrow [b]_m = 0$.

$[b]_m = 0 \Rightarrow \lightning$ zu $0 < b < m$.

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

Dann ist $\mathrm{ggT}(c, m) = 1$. Also gilt $x \cdot c + y \cdot m = 1$, für gewisse $x, y \in \mathbb{Z}$.

$$\begin{aligned}
\Rightarrow [x]_m \cdot [c]_m &= [x \cdot c]_m \\
&= [1 - y \cdot m]_m \\
&= [1]_m = 1.
\end{aligned}$$

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

Wir haben somit gezeigt, dass alle Nicht-0-Element von $\mathbb{Z}_m$ invertierbar sind, sodass $\mathbb{Z}_m$ ein Körper ist. $\square$