$|\mathbb{Z}_7| = 7$

$|\mathbb{Z}_7^*| = 6$ (Anzahl Teilerfremd)

↳ $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$\mathbb{Z}_{12}^* = \{1,5,7,11\}$

$\varphi(m) = |\mathbb{Z}_m^*|$

— zyklische Gruppen

↳ Generator

$\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_7^* = \langle 3 \rangle$ „zyklisch"

$\mathbb{Z}_{14}^* = \{1,3,5,9,11,13\}$

$\varphi(14) = 6$. Da $\text{ord}(a) \mid 6$,

$\text{ord}(a) \in \{1,2,3,6\}$,

für Generator muss $\text{ord}(a) = 6$ sein.

$\text{ord}(a) \notin \{1,2,3\} \Rightarrow \text{ord}(a) = 6$

z.B. 3: $3^1 \equiv_{14} 3$,

$3^2 \equiv_{14} 9$

$3^3 \equiv_{14} 13$,

also $\text{ord}(3) = 6$,

$\langle 3 \rangle = \mathbb{Z}_{14}^*$

Ring R $\langle R; +, -, 0, \cdot, 1 \rangle$

mit $\langle R; +, -, 0 \rangle$ abelsche Gruppe

$\langle R; \cdot, 1 \rangle$ Monoid (nicht immer kommutativ!)

Nullteiler: $ab \equiv_m 0 \Rightarrow a \equiv_m 0 \vee b \equiv_m 0$

z.B. 2 in $\mathbb{Z}_{2m}$

R Integritätsbereich, wenn R keiner Nullteiler hat, z.B.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_m$ für m prim

z.B.

$\mathbb{Z}_5 = 0,1,2,3,4$

gibt keine $a, b \neq 0$ mit $ab = 0$

Einheit: $a \cdot b = 1$ für ein $b \in R$

R^* — alle invertierbaren Elemente, also alle Einheiten

Irreduzibilität: Element, das keine (interessanten) Zerlegungen hat (z.B. Primzahlen)

Einheiten zählen nicht als irreduzibel

z.B. (x^2+1) in $\mathbb{R}$ irreduzibel, in $\mathbb{C}$ $x^2+1 = (x+i)(x-i)$, also nein

---

Lemma 5.17

Polynomringe: $R[x]$,

z.B. $\mathbb{R}[x]$,

$\mathbb{Z}_5[x]$,

nur Konstanten sind invertierbar, also

$R[x]^* = R^*$

monisch/normiert: max. Potenz hat Koeffizient 1

Grad: $\deg(x^5) = 5$

$\deg(2) = 0$

$\deg(0) = -\infty$

$R^* = R \setminus \{0\}$ kommutativ

↳ „Körper" ↯

Körper

z.B. $\mathbb{Z}_m$ Körper $\iff$ m prim,

$\mathbb{R}, \mathbb{Q}, \mathbb{C}$

F Körper $\Rightarrow$ F Integritätsbereich (kein Nullteiler)

↳ Beweis: sei $v \in F \setminus \{0\}$

$v \cdot V = 0 \Rightarrow V = 0$:

$V = 1 \cdot V$

$V = v^{-1} \cdot v \cdot V$

$v \cdot V$ = 0 per Annahme

$V = v^{-1} \cdot 0 = 0$

Def. „GF"

$GF(p) = \mathbb{Z}_p$ für p prim

Polynomdivision: z.B. über $GF(7) = \mathbb{Z}_7$

$a(x) = b(x) \cdot q(x) + r(x)$

$x^3 + 2x^2 + 5x + 4 = (2x^2 + x + 1)(4x + 6) + (2x + 5)$

$-(x^3 + 4x^2 + 4x)$

$5x^2 + x + 4$

$-(5x^2 + 6x + 6)$

$2x + 5$