

19.11. | Remember $GF(p) = \mathbb{Z}_p$

Polynom irreduzibel, wenn

1. $\deg(m(x)) \geq 1$, und
2. jedes Polynom $d(x)$ mit $d(x) | m(x)$ hat a) Grad 0, oder b) gleichen Grad wie $m(x)$

also a) eine Konstante, oder b) das Polynom selbst

Einsetzen eines Wertes in ein Polynom:
"Auswertungshomomorphismus"

$F[x]$: Menge der Polynome mit Koeffizienten aus F . z.B. $3x^2 + 2x + 1$

Schreibweise φ_α : Ich setze α für x ein. Ergebnis: Zahl aus F .
 $\varphi_\alpha(\alpha) = \varphi_\alpha(\alpha)$

Homomorphismus von Gruppen:

$$1) \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$2) \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

gilt.

Def. Wurzel (Nullstelle)

$$\alpha \text{ Wurzel von } q(x) \Leftrightarrow q(\alpha) = 0$$

Lemma $q(\alpha) = 0 \Leftrightarrow (x-\alpha) | q(x)$

Beweis: ($\Rightarrow$) T. 5.25:

$$q(x) = (x-\alpha) \cdot q_1(x) + r(x)$$

Auswerten:

$$q(\alpha) = (\alpha-\alpha) \cdot q_1(\alpha) + r(\alpha) = 0$$

$$\Rightarrow r(x) = 0$$

Da Rest 0, teilt.

$$(\Leftarrow) q(x) = (x-\alpha) \cdot b(x)$$

Auswerten:

$$q(\alpha) = \underbrace{(\alpha-\alpha)}_0 \cdot b(\alpha)$$

$$q(\alpha) = 0$$

Quick-Facts:

• $\deg(q(x)) = n$ größer als $-\infty$
 $\Rightarrow q$ hat höchstens n Wurzeln

• Polynom hat Nullstelle
 $\Rightarrow$ ist reduzierbar

Grad 52: irreduzierbar wenn keine Nullstelle

• $GF(7) = \mathbb{Z}_7$

• $|GF(p)^*| = \text{Anzahl invertierbarer Elemente}$

Beispiel:

$$q(x) = x^p - x \in GF(p)[x]$$

Es gilt

$$|GF(p)^*| = p-1, \text{ also } \alpha^p = \alpha \text{ in } GF(p)$$

Element hoch Gruppenordnung ist neutrales Element, denn nochmal ist wieder das Element selbst.

$$\text{Also } (x^p - x)(\alpha) = 0$$

$$\text{Somit } x^p - x = \prod_{\alpha \in GF(p)} (x - \alpha)$$

"Polynom hat nur Nullstellen"

Lemma 5.32

$q(x) \in F[x]$ mit $\deg(q(x)) \leq d$ ist eindeutig festgelegt durch Auswertung $q(\alpha_1), \dots, q(\alpha_{d+1})$ für bel., unters. $\alpha_1, \dots, \alpha_{d+1} \in F$

"Ich brauche $d+1$ viele Stellen, an denen ich die Funktion kenne, damit ich die Funktion aufstellen kann. Vorstellung: Grad 1; linear; brauche 2 Stellen."

$F[x]_{m(x)}$

"Polynomring modulo $m(x)$ "

$$F[x]_{m(x)} = \left\{ q(x) \in F[x] \mid \deg(q(x)) < \deg(m(x)) \right\}$$

$m(x)$ irreduzibel

... ist Ring mit Add./

Mult. mod $m(x)$

(Betrachte nur Rest)

bei Addition ändert sich Grad nicht

Ist auch Körper. Zu zeigen: gibt Inverse zu $m(x)$

$$(F[x]_{m(x)})^* = F[x]_{m(x)} \setminus \{0\}$$

Invertierung mittels

$$\gcd(q(x), m(x)) = 1 = q(x) \cdot \underbrace{b(x)}_{a(x)^{-1}} + m(x) \cdot q(x)$$

da $m(x)$ irreduzibel

für $q(x) \neq 0$

$q(x)$ ist bel. anderes Polynom mit kleineren Grad

$\Rightarrow$ gleich wie bei $\mathbb{Z}$; "Idealbehandlung"

Beispiel:

$$m(x) = x^2 + x + 1 \in GF(2)[x] \text{ irred.}$$

$$F[x]_{m(x)} = \{0, 1, x, 1+x\}$$

alle Polynome, Grad kleiner 2

weil

$$\text{z.B. } (x+1)^2 \equiv_{m(x)} x^2 + 2x + 1 \equiv_{m(x)} x$$

$$\text{z.B. } (x+1)x \equiv_{m(x)} x^2 + x \equiv_{m(x)} 1$$