Anzahl der Generatoren

Satz Anzahl Generatoren eines Körpers

Sei K ein Körper mit q Elementen. Dann besitzt K^* genau $\phi(q-1)$ viele Generatoren.

Beweis:

- K^* ist zyklisch, d.h. K^* besitzt einen Generator a mit
$$K = \{a, a^2, \ldots, a^{|K^*|}\}.$$
- Wir bestimmen $\mathrm{ord}(a^j)$ für ein $j \in \mathbb{Z}_{|K^*|}$. D.h. wir suchen ein minimales $k = ord(a^j)$ so dass jk ein Vielfaches von $|K^*|$ ist.
- Für $k = \frac{|K^*|}{\mathrm{ggT}(j,|K^*|)}$ gilt $jk = \frac{j}{\mathrm{ggT}(j,|K^*|)} \cdot |K^*| = 0 \bmod |K^*|$.
- k ist minimal mit dieser Eigenschaft, d.h. $\mathrm{ord}(a^j) = \frac{|K^*|}{\mathrm{ggT}(j,K^*)}$.
- D.h. falls $\mathrm{ggT}(j, |K^*|) = 1$, dann gilt $\mathrm{ord}(a^j) = |K^*| = q-1$.
- Es existieren $|\{j \in \mathbb{Z}_{|K^*|} \mid \mathrm{ggT}(j, |K^*|) = 1\}| = \phi(|K^*|) = \phi(q-1)$ viele Elemente mit Ordnung $q-1$.
- D.h. es gibt $\phi(q-1)$ viele Generatoren in K^*.

Konstruktion von Generatoren

Satz Konstruktion von Generatoren

Sei K^* zyklisch. Ein Element $a \in K^*$ ist ein Generator falls $a^k \neq 1$ für alle nicht-trivialen Teiler k von $|K^*|$.

Beweis:

- Da K^* zyklisch ist, besitzt es einen Generator mit Ordnung $|K^*|$.
- Die Ordnung jeden Elements a teilt die maximale Ordnung $|K^*|$.
- D.h. es genügt, für $\mathrm{ord}(a)$ alle möglichen Teiler von $|K^*|$ zu testen.

Beispiel: zyklische Gruppe $\mathbb{Z}_{11}^*$

- $\mathbb{Z}_{11}^*$ besitzt 10 Elemente und $\phi(10) = 4$ Generatoren.
- 2 ist ein Generator, denn $2^2 = 4$ und $2^5 = 10$.
- Da $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$, sind auch die Elemente $2^3 = 8, 2^7 = 7$ und $2^9 = 6$ Generatoren von $\mathbb{Z}_{11}^*$.

Teilbarkeitsbegriff für Polynome

Definition Teilbarkeit von Polynomen

Sei K ein Körper und $f, g, \pi \in K[x]$. Wir definieren

- $g \mid f$ gdw ein $h \in K[x]$ existiert mit $gh = f$.
- $f = g \bmod \pi$ gdw π die Differenz $f - g$ teilt.
- $\mathrm{ggT}(f, g)$ ist ein Polynom maximalen Grads, das sowohl f als auch g teilt. Vorsicht: $\mathrm{ggT}(f, g)$ ist im allgemeinen nicht eindeutig.

Anmerkungen:

- Bei der Reduktion modulo π erhalten wir Äquivalenzklassen.
- Repräsentanten der Äquivalenzklassen sind
$$R = \{f \in K[x] | \mathrm{grad}(f) < \mathrm{grad}(\pi)\}.$$
- Sei K ein Körper mit p Elementen und $\mathrm{grad}(\pi) = n$.
- Dann gilt $|R| = p^n$. Wir schreiben $R = K[x]/(\pi(x))$.

Erweiterter Euklischer Algorithmus für Polynome

Algorithmus ERWEITERTER EUKLIDISCHER ALG. (EEA)

EINGABE: $a(x), b(x) \in K[x]$

1. If $(b = 0)$ then return $(a, 1, 0)$;
2. $(d, r, s) \leftarrow \text{EEA}(b, a \bmod b)$;
3. $(d, r, s) \leftarrow (d, s, r - \lfloor \frac{a}{b} \rfloor s)$;

AUSGABE: $d = \text{ggT}(a, b) = ra + sb$

Korrektheit:

- Analog zu EEA über $\mathbb{Z}$.

Beispiel für EEA

Beispiel: $\mathrm{ggT}(x^3+2x^2-1, x^2+x)$ in $\mathbb{F}_3[x]$

a	b	$\lfloor \frac{a}{b} \rfloor$	r	s
x^3+2x^2-1	x^2+x	$x+1$	1	$-x-1$
x^2+x	$2x-1$	$2x$	0	1
$2x-1$	0	-	1	0

- D.h. $\mathrm{ggT}(a,b) = 2x-1$. Man beachte, dass der ggT eindeutig bis auf Multiplikation mit Elementen aus $\mathbb{F}_3^*$ ist.
- Z.B. ist $2(2x-1) = x+1$ ebenfalls ein Teiler von a, b.
- $x-(-1)$ teilt a, b, da (-1) gemeinsame Nullstelle von a, b ist.
- Der EEA für Polynome liefert die Linearkombination

  $\mathrm{ggT}(a,b) = ra+sb = x^3+2x^2-1-(x+1)(x^2+x) = -x-1 = 2x-1.$

Irreduzible Polynome

Definition Irreduzibilität von Polynomen

Sei K ein Körper und $\pi \in K[x]$. Wir bezeichnen π als *irreduzibel über* K gdw jede Zerlegung $\pi = \pi_1 \cdot \pi_2$ mit $\pi_1, \pi_2 \in K[x]$ impliziert dass $\mathrm{grad}(\pi_1) = 0$ oder $\mathrm{grad}(\pi_2) = 0$.
Andernfalls bezeichen wir π als *reduzibel über* K.

Beispiel: Polynom $f(x) = x^2 + 1$

- f ist irreduzibel über $\mathbb{R}$, denn $f(x) > 0$ für alle $x \in R$.
- D.h. f besitzt keine Nullstelle x_0 in $\mathbb{R}$ und damit können wir keinen Linearfaktor $(x - x_0)$ von $f(x)$ abspalten.
- f ist reduzibel über $\mathbb{C}$, denn $f(x) = (x + i)(x - i)$.
- f ist irreduzibel über $\mathbb{F}_3$, denn weder $0, 1$ noch 2 sind Nullstellen von $f(x)$ in $\mathbb{Z}_3$.
- f ist reduzibel über $\mathbb{F}_2$, denn $f(x) = (x + 1)(x + 1)$.

Polynomringe modulo reduziblen Polynomen

- Sei K ein Körper und $\pi \in K[x]$ reduzibel.
- Dann gilt $\pi = \pi_1 \cdot \pi_2$ mit $0 < \text{grad}(\pi_1), \text{grad}(\pi_2) < \text{grad}(\pi)$.
- Wir definieren den Ring $K[x]/(\pi)$.
- Es gilt $\pi_1, \pi_2 \in K[x]/(\pi)$.
- Ferner gilt $\pi_1 \cdot \pi_2 = \pi = 0$ in $K[x]/(\pi)$.
- D.h. das Produkt von zwei von Null verschiedenen Elementen liefert Null in $K[x]/(\pi)$. Damit sind π_1, π_2 Nullteiler in $K[x]/(\pi)$.
- Es folgt, dass der Ring $K[x]/(\pi)$ kein Körper sein kann.

Galoiskörper

Satz Galoiskörper

Sei K ein Körper mit p Elementen. Sei $\pi \in K[x]$ irreduzibel vom Grad n. Dann ist $K[x]/(\pi)$ ein Körper mit $q = p^n$ Elementen.

Notation: $K[x]/(\pi) = \mathbb{F}_{p^n} = \mathbb{F}_q$ oder auch *Galoiskörper* $GF(q)$.

Beweisskizze:

- **Additiv:** $(K[x]/(\pi), +)$ ist eine abelsche Gruppe.
- Dazu definieren wir $H = \{k \cdot \pi \mid k \in K[x]\}$.
- H ist eine Untergruppe von $K[x]$.
- $K[x]/(\pi)$ ist isomorph zur Faktorgruppe $K[x]/H$.
- **Multiplikativ:** $((K[x] \setminus \{0\})/(\pi), \cdot)$ ist eine abelsche Gruppe.
- Abgeschlossenheit: Seien $f, g \in K[x] \setminus \{0\}$.
- Annahme: $fg = 0 \bmod \pi$. Dann folgt $\pi \mid fg$ und damit $\pi \mid f$ oder $\pi \mid g$. (Widerspruch, da $f, g \neq 0$)
- Berechnen von Inversen liefert der EEA für Polynome.
- **Distributivgesetz:** Folgt aus Distributivität von $K[x]$.

Beispiel: Körper $\mathbb{F}_4$

Beispiel: $\mathbb{F}_{2^2} = \mathbb{F}_4$

- Der Körper $\mathbb{F}_4$ ist eine Körpererweiterung des Körpers $\mathbb{F}_2$.
- Über $\mathbb{F}_2$ ist $\pi = x^2 + x + 1$ irreduzibel, denn $\pi(0) = \pi(1) = 1$.
- D.h. wir können den $\mathbb{F}_4$ definieren als $\mathbb{F}_2[x]/(x^2 + x + 1)$.
- Die Repräsentanten des $\mathbb{F}_4$ sind $\{0, 1, x, x + 1\}$.
- Berechnung des Inversen von x mittels EEA(π, x) liefert
$$1 \cdot (x^2 + x + 1) + (x + 1) \cdot x = 1.$$
- Das Inverse von x in $\mathbb{F}_4$ ist $x + 1$, denn $(x + 1)x = 1 \bmod \pi$.

- Alternativ können wir $x^{-1} = ax + b$ setzen und a, b ermitteln:
$1 = (ax + b)x = ax^2 + bx = a(-x - 1) + bx = (a + b)x + a$ in $\mathbb{F}_4$.
- Koeffizientenvergleich liefert $a = 1$ und $a + b = 0$, d.h. $b = 1$.
- Damit ist $ax + b = x + 1$ das Inverse von x in $\mathbb{F}_4$.

- $\mathbb{F}_4$ besitzt die $\phi(3) = 2$ Generatoren x und $x + 1$.

Existenz und Eindeutigkeit der Galoiskörper $\mathbb{F}_{p^n}$

Satz Existenz von irreduziblen Polynomen

Für jedes prime p und jedes $n \in \mathbb{N}$ existiert ein irreduzibles Polynom $\pi \in \mathbb{F}_p[x]$ vom Grad n.

(ohne Beweis)

Korollar Existenz eines Galoiskörpers $\mathbb{F}_{p^n}$

Für jedes prime p und jedes $n \in \mathbb{N}$ existiert ein Galoiskörper $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(\pi)$ für ein irreduzibles $\pi \in \mathbb{F}_p[x]$.

Satz Eindeutigkeit der Galoiskörper

Je zwei endliche Körper mit gleicher Anzahl von Elementen sind isomorph.

(ohne Beweis)