Endliche Körper

Hauptsatz

(i) Ist K ein endlicher Körper, dann existiert eine Primzahl p und ein $n \in \mathbb{N}$ mit $|K| = p^n$. Umgekehrt existiert zu jeder Primzahlpotenz $q > 1$ ein Körper mit q Elementen, und dieser ist bis auf Isomorphie eindeutig.

(ii) Ist K ein Körper, p eine Primzahl und $n \in \mathbb{N}$

mit $|K| = p^n$, dann gilt $P \cong \mathbb{F}_p$ für den Primkörper P von K, und es gilt $[K : P] = n$.

(iii) In der Situation von (ii) existiert ein $\alpha \in K$ mit $K = P(\alpha)$, und α ist Nullstelle eines irreduziblen Polynoms $f \in P[x]$ vom Grad n. Die Elemente von K sind dann gegeben durch

$$K = \{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in P \}$$

Beispiel: Körper $\mathbb{F}_4$ mit vier Elementen

$$\mathbb{F}_4 = \{ a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_2 \} = \{ \bar{0}, \bar{1}, \alpha, \bar{1} + \alpha \}$$

wobei α eine Nullstelle von $f = x^2 + x + \overline{1} \in \mathbb{F}_2[x]$ bezeichnet. (Achtung: $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$)

(iv) In der Situation von iii) ist K stets der Zerfällungskörper des Polynoms $x^{p^n} - x \in P[x]$. (Dies zeigt die Eindeutigkeit des Körpers mit p^n Elementen bis auf Isomorphie.)

(v) Für jede Primzahl p gilt $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ nach Definition. Bezeichnet $\mathbb{F}_p^{alg}$ einen algebraischen Abschluss von $\mathbb{F}_p$, dann existiert für jedes $n \in \mathbb{N}$ genau ein Zwischenkörper von $\mathbb{F}_p^{alg}$ / $\mathbb{F}_p$ mit

p^n Elementen, für den die Notation $\mathbb{F}_{p^n}$ verwendet wird. Es gilt die Äquivalenz

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n \quad \forall m, n \in \mathbb{N}$$

(Zum Beispiel gilt nicht $\mathbb{F}_4 \subseteq \mathbb{F}_8$, denn es ist $4 = 2^2$, $8 = 2^3$, aber 2 kein Teiler von 3.) Der algebraische Abschluss ist dann gegeben durch

$$\mathbb{F}_p^{alg} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$$

(vi) Für jede Primzahl p und jedes $n \in \mathbb{N}$ ist die Erweiterung $\mathbb{F}_{p^n} | \mathbb{F}_p$ galoissch.

Nullstelle von $f = x^2 + x + \overline{1} \in \mathbb{F}_2[x]$

Für die Galoisgruppe $G = \mathrm{Gal}(\mathbb{F}_{p^n} | \mathbb{F}_p)$ gilt $G \cong \mathbb{Z}/n\mathbb{Z}$. Sie wird erzeugt durch den Frobenius-Automorphismus $\varphi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\alpha \mapsto \alpha^p$.

H21T3A4 Sei $f = x^4 + x + \bar{1} \in \mathbb{F}_2[x]$.

(a) Zeigen Sie: f ist irreduzibel

(b) Sei $K = \mathbb{F}_2(\alpha)$, wobei α eine Nullstelle von f in einem alg. Abschluss $\mathbb{F}_2^{alg}$ von $\mathbb{F}_2$ bezeichnet. Zeigen Sie, dass α ein Erzeuger der multiplikativen Gruppe $K^\times$ ist.

(b) Sei $K = \mathbb{F}_2(\alpha)$, wobei α eine Nullstelle

f ist irred. in $\mathbb{F}_2[x]$, normiert, $f(\alpha) = \bar{0}$

$\Rightarrow f = \mu_{\alpha, \mathbb{F}_2} \Rightarrow [K : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2]$

$= \operatorname{grad} f = 4 \Rightarrow K \cong \mathbb{F}_2^4$ als $\mathbb{F}_2$-Vektorraum $\Rightarrow |K| = |\mathbb{F}_2^4| = 2^4 = 16$

$\Rightarrow |K^*| = |K \setminus \{0_K\}| = |K| - 1 = 15$

[Bem.: K und $\mathbb{F}_2^4$ sind nur isomorph als $\mathbb{F}_2$-Vektorräume, aber nicht als Ringe oder Körper, obwohl $\mathbb{F}_2^4$ eine Ringstruktur besitzt, gegeben durch die komponentenweise Addition und Multiplikation.]

x ist Nullstelle

$f(\alpha) = \bar{0}$

$[\mathbb{F}_2(\alpha) : \mathbb{F}_2]$

als $\mathbb{F}_2$-Vek-

$= 16$

$= 15$

isomorph als

ist als Ringe

ein Ring-

durch die kompo-

Multiplikation.

bekannt: Für jede endl

z.zg. also: $\mathrm{ord}(\alpha) = 15$ in $K^\times$

Es genügt dafür zu überprüfen, dass $\alpha^3 \neq \bar{1}$ und $\alpha^5 \neq \bar{1}$ gilt.

Wegen $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$ hat jedes Element in $K = \mathbb{F}_2(\alpha)$ eine eindeutige Darstellung der Form $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ mit $a_0, a_1, a_2, a_3 \in \mathbb{F}_2$. Wäre $\alpha^3 = \bar{1}$, dann würde

$$\bar{0} + \bar{0}\cdot\alpha + \bar{0}\cdot\alpha^2 + \bar{1}\cdot\alpha^3 = \bar{1} + \bar{0}\cdot\alpha + \bar{0}\cdot\alpha^2 + \bar{0}\cdot\alpha^3$$

gelten, im Widerspruch zur Eindeutigkeit.

Zeige noch: $\alpha^5 \neq \bar{1}$

$p^n \mid \mathbb{F}_p$)

gt durch

$\mathbb{F}_p{}^n \to \mathbb{F}_p{}^n$,

$\in \mathbb{F}_2[x]$.

eine Nullstelle

$\mathbb{F}_2^{alg}$ von $\mathbb{F}_2$

α ein

en Gruppe $K^\times$

$f(\alpha) = \bar{0} \Rightarrow \alpha^4 + \alpha + \bar{1} = \bar{0} \Rightarrow$

$\alpha^4 = -\bar{1} - \alpha = \bar{1} + \alpha \Rightarrow \alpha^5 = \alpha \cdot \alpha^4$

$= \alpha(\bar{1} + \alpha) = \alpha + \alpha^2$. Ang. $\alpha^5 = \bar{1} \Rightarrow$

$\alpha + \alpha^2 = \bar{1} \Rightarrow \bar{0} + \bar{1} \cdot \alpha + \bar{1} \cdot \alpha^2 =$

$\bar{1} + \bar{0} \cdot \bar{1} + \bar{0} \cdot \alpha + \bar{0} \cdot \alpha^2$ ↯ zur Eindeutigk.

(c) Zeigen Sie:

$f = (x - \alpha) \cdot (x - \alpha^2) \cdot (x - \alpha^4)(x - \alpha^8)$

bekannt: Für jede endl. Erweiterung $L \mid \mathbb{F}_2$ ist $L \to L$, $\beta \mapsto \beta^2$ ein $\mathbb{F}_2$-Automorphismus von L, der sog. Frobenius-Automorphismus. Insb. existiert ein $\mathbb{F}_2$-Aut.: $\varphi: K \to K$, $\beta \mapsto \beta^2$.

Ist $\beta \in K$ eine Nullstelle von f ist, dann muss auch $\varphi(\beta)$ eine Nullstelle von f sein, auf Grund der $\mathbb{F}_2$-Automorphismus-Eig. von φ. $\Rightarrow$ Mit α sind auch $\alpha^2 = \varphi(\alpha)$, $\alpha^4 = \varphi(\alpha^2)$ und $\alpha^8 = \varphi(\alpha^4)$ Nullstellen von f. Wegen $\operatorname{ord}(\alpha) = 15$ sind α^j mit $0 \leq j < 15$ verschiedene Elemente von $K^\times$. Also sind $\alpha, \alpha^2, \alpha^4, \alpha^8$ vier verschiedene Nullstellen von f. $\Rightarrow (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$ ist Teiler von f in $K[x]$. Weil beide Polynome normiert sind und den gleichen Grad haben, folgt daraus die Gleichheit. $\square$

$= \mathbb{F}_{p^{15}}$

$= \mathbb{F}_{p^{15}}$

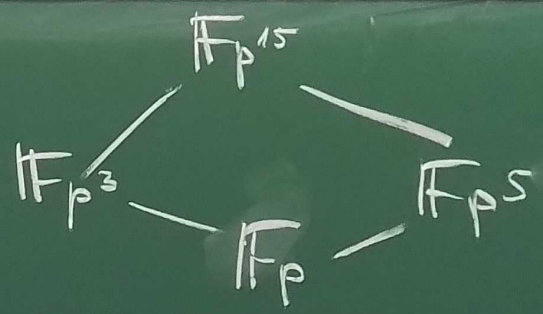
vier verschiedene Nullstellen von f. $\Rightarrow (x-\alpha)\cdot(x-\alpha^2)\cdot(x-\alpha^4)(x-\alpha^8)$ ist Teiler von f in $K[x]$. Weil beide Polynome normiert sind und den gleichen Grad haben

Übung: Ist jedes Element $\beta \in K$ mit $K = \mathbb{F}_2(\beta)$ ein Erzeuger von K^*? Gilt die Umkehrung? Bitte begründen Sie jeweils ihre Antwort.

F23T2A5 (V) Übung: F22T2A4

Sei p eine Primzahl, $\mathbb{F}_p^{alg}$ ein algebraischer Abschluss von $\mathbb{F}_p$ und $\mathbb{F}_{p^{15}}$ der eindeutig bestimmte Zwischenkörper von $\mathbb{F}_p^{alg} | \mathbb{F}_p$ mit p^{15} Elementen. Geben Sie eine Formel für die Anzahl der Elemente $\alpha \in \mathbb{F}_{p^{15}}$ mit $\mathbb{F}_{p^{15}} = \mathbb{F}_p(\alpha)$ an.

Beh: Für jedes $\alpha \in \mathbb{F}_{p^{15}}$ gilt die Äquivalenz



$$\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{15}} \iff \alpha \in \mathbb{F}_{p^{15}} \setminus \left(\mathbb{F}_{p^3} \cup \mathbb{F}_{p^5} \right)$$

„$\Rightarrow$" Setze $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{15}}$ voraus. z.zg.:
$\alpha \notin \mathbb{F}_{p^3}$ und $\alpha \notin \mathbb{F}_{p^5}$

Ang. $\alpha \in \mathbb{F}_{p^3}$. $\Rightarrow \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^3}$ ↯ zu $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{15}}$

Ang. $\alpha \in \mathbb{F}_{p^5} \Rightarrow \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^5}$ ↯ zu $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{15}}$

„$\Leftarrow$" Vor.: $\alpha \in \mathbb{F}_{p^{15}} \setminus (\mathbb{F}_{p^3} \cup \mathbb{F}_{p^5})$

$\mathbb{F}_p(\alpha)$ ist Zwischenkörper von $\mathbb{F}_{p^{15}} | \mathbb{F}_p$ wegen $\alpha \in \mathbb{F}_{p^{15}}$. Laut VL sind die Zwischenkörper dieser Erw. geg. durch $\mathbb{F}_{p^d}$, wobei $d \in \mathbb{N}$ die Teiler von 15 durchläuft, also die Werte 1, 3, 5, 15. $\Rightarrow \mathbb{F}_p(\alpha) \in \{\mathbb{F}_p, \mathbb{F}_{p^3}, \mathbb{F}_{p^5}, \mathbb{F}_{p^{15}}\}$

Ang. $\mathbb{F}_p(\alpha) = \mathbb{F}_p \Rightarrow \alpha \in \mathbb{F}_p \underset{\mathbb{F}_p \subseteq \mathbb{F}_{p^3}}{\Rightarrow} \alpha \in \mathbb{F}_{p^3}$

↯ zu $\alpha \notin \mathbb{F}_{p^3} \cup \mathbb{F}_{p^5}$

Genauso führt die Annahme $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^3}$ bzw. $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^5}$ zu einem Widerspruch mit der Voraussetzung. Also gilt $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{15}}$

Die gesuchte Elementezahl ist also gleich

$$|\mathbb{F}_{p^{15}} \setminus (\mathbb{F}_{p^3} \cup \mathbb{F}_{p^5})| = |\mathbb{F}_{p^{15}}| - |\mathbb{F}_{p^3} \cup \mathbb{F}_{p^5}|$$

$$= p^{15} - |\mathbb{F}_{p^3} \cup \mathbb{F}_{p^5}|.$$

Jeder Teilkörper $K \subseteq \mathbb{F}_{p^3} \cap \mathbb{F}_{p^5}$ ist ein gemeinsamer Teilkörper von $\mathbb{F}_{p^3}$ und $\mathbb{F}_{p^5}$. $\Rightarrow K = \mathbb{F}_{p^d}$, wobei $d \in \mathbb{N}$ ein gemeinsamer Teiler von 3 und 5 ist.

$ggT(3,5) = 1 \Rightarrow d = 1 \Rightarrow \mathbb{F}_p$ ist der einzige gem. Teilkörper. Weil also $\mathbb{F}_{p^3} \cap \mathbb{F}_{p^5}$ ein gem. Teilkörper von $\mathbb{F}_{p^3}$ und $\mathbb{F}_{p^5}$ ist, folgt

$\mathbb{F}_{p^3} \cap \mathbb{F}_{p^5} = \mathbb{F}_p \Rightarrow |\mathbb{F}_{p^3} \cup \mathbb{F}_{p^5}| =$

$|\mathbb{F}_{p^3}| + |\mathbb{F}_{p^5}| - |\mathbb{F}_{p^3} \cap \mathbb{F}_{p^5}| =$

$p^3 + p^5 - |\mathbb{F}_p| = p^3 + p^5 - p$

Die gesuchte Elementezahl ist also

$$p^{15} - p^3 - p^5 + p$$

Übung: Wieviele Elemente $\alpha \in \mathbb{F}_{p^{30}}$ mit $\mathbb{F}_{p^{30}} = \mathbb{F}_p(\alpha)$ gibt es?
Wieviele Elemente erfüllen die Gleichung

$$\mathbb{F}_{p^{30}} = \mathbb{F}_{p^2}(\alpha) \quad ?$$

H22T3A4

Wir betrachten in $\mathbb{Z}[x]$ das Ideal $I = (x^5+2,\ x^4+x^3+x^2+x+1)$ und den Faktorring $K = \mathbb{Z}[x]/I$.

(a) Zeigen Sie: $3 \in I$

$$3 = 1\cdot(x^5+2) + (-x-1)\cdot(\underbrace{x^4+x^3+x^2+x+1}_{5\text{-tes Kreisteilungspol}})$$

$$\in (x^5+2,\ x^4+x^3+x^2+x+1)$$