Endliche Körper

Hauptsatz

(i) Ist K ein endlicher Körper, dann existiert eine Primzahl p und ein $n \in \mathbb{N}$ mit $|K| = p^n$. Dabei ist $p = \mathrm{char}(K)$, der Primkörper P von K ist isomorph zu $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, und es ist $n = [K : P]$.

(ii) Umgekehrt existiert zu jeder Primzahlpotenz q mit $q > 1$ ein Körper mit q

Dabei ist $p = \mathrm{char}(K)$ der Primkörper P von Elementen, und dieser ist eindeutig bis auf Isomorphie.

(iii) Ist K ein endlicher Körper, P sein Primkörper und $n = [K : P]$, dann ist K der Zerfällungskörper des Polynoms $f_n = x^{p^n} - x$ über P. (Daraus folgt die Eindeutigkeit.)

(iv) Ist umgekehrt p eine Primzahl, P ein p-elementiger Körper, $n \in \mathbb{N}$ und $f_n = x^{p^n} - x \in P[x]$, und ist K Zerfällungskörper von f_n über P, dann ist $|K| = p^n$. (Daraus folgt die Existenz.)

$= p^n$.

Für alle $m, n \in \mathbb{N}$ gilt die Äquivalenz

F_2^{alg}

(v) Ist $L|K$ eine Erweiterung bestehend aus endlichen Körpern und $n = [L:K]$, dann ist $L|K$ galoissch (= normal und separabel), und es gilt $Gal(L|K) \cong \mathbb{Z}/n\mathbb{Z}$, d.h. die Galoisgruppe ist zyklisch. Dabei wird die Galoisgruppe erzeugt vom sog. Frobenius-Automorphismus $\varphi \in Gal(L|K)$ gegeben durch $\varphi(\alpha) = \alpha^q \quad \forall \alpha \in L$, wobei $q = |K|$ ist.

(vi) Ist K ein endlicher Körper mit $q = K$, dann ist $K^\times$ eine zyklische Gruppe der Ordnung $q-1$.

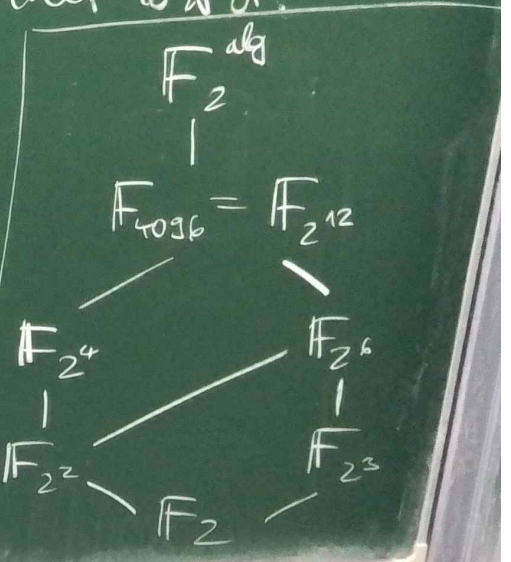
(vii) Sei p eine Primzahl und $\mathbb{F}_p^{alg}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann gibt es für jedes $n \in \mathbb{N}$ genau einen Zwischenkörper von $\mathbb{F}_p^{alg} / \mathbb{F}_p$ mit p^n Elementen, der mit $\mathbb{F}_{p^n}$ bezeichnet wird.

Für alle $m, n \in \mathbb{N}$ gilt die Äquivalenz

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$$

(beachte: z.B. $\mathbb{F}_4 \not\subseteq \mathbb{F}_8$, da $2+3$)

Frage: Wie kann man für eine Primzahl p und ein $n \in \mathbb{N}$ die Elemente von $\mathbb{F}_{p^n}$ konkret angeben?



Achtung: Im Fall $n > 1$ ist $\mathbb{F}_{p^n}$ nicht isomorph zu $\mathbb{Z}/p^n\mathbb{Z}$, erst recht stimmen die Ringe nicht überein.

Statt dessen: Es gibt stets ein in $\mathbb{F}_p[x]$ irreduzibles Polynom f vom Grad n und eine Nullstelle $\alpha \in \mathbb{F}_p^{alg}$ von f mit $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) =$

$$\{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbb{F}_p\}$$

Bsp: $\mathbb{F}_8 = \{\underbrace{\bar{0}, \bar{1}}_{\in \mathbb{F}_2}, \alpha, \alpha + \bar{1}, \alpha^2, \alpha^2 + \bar{1}, \alpha^2 + \alpha, \alpha^2 + \alpha + \bar{1}\}$, wobei α z.B. Nullstelle von $x^3 + x + \bar{1} \in \mathbb{F}_2[x]$ ist.

glei
$p^2 \equiv$
gilt
mod
$4 \equiv 1$
Fall
ungerade
$\Rightarrow p^2 \equiv$
also auch

F24TZA1 Sei p eine Primzahl mit $p > 3$. Zeigen Sie, dass in $\mathbb{F}_{p^2}^\times$ ein Element der Ordnung 12 existiert.

Da $\mathbb{F}_{p^2}$ ein endl. Körper mit p^2 Elementen ist, ist $\mathbb{F}_{p^2}^\times$ eine zyklische Gruppe der Ordnung p^2-1. Allgemein existiert in einer endl. zyklischen Gruppe der Ordnung $n \in \mathbb{N}$ für jeden Teiler $d \in \mathbb{N}$ von n ein Element der Ordnung d. Es genügt also zu zeigen, dass 12 ein Teiler von p^2-1 ist. Wegen $\text{kgV}(3,4) = 12$ reicht es z.Zg., dass p^2-1 von 3 und von 4 geteilt wird. Dies ist

gleichbedeutend mit $p^2 \equiv 1 \bmod 3$ und $p^2 \equiv 1 \bmod 4$. Da p eine Primzahl größer als 3 ist, gilt $3 \nmid p$ und somit $p \equiv 1 \bmod 3$ oder $p \equiv 2 \bmod 3$. $\Rightarrow p^2 \equiv 1^2 \equiv 1 \bmod 3$ oder $p^2 \equiv 2^2 \equiv 4 \equiv 1 \bmod 3$, also $p^2 \equiv 1 \bmod 3$ in jedem Fall. Ebenso: p Primzahl, $p > 3 \Rightarrow p$ ist ungerade $\Rightarrow p \equiv 1 \bmod 4$ oder $p \equiv 3 \bmod 4$ $\Rightarrow p^2 \equiv 1^2 \equiv 1 \bmod 4$ oder $p^2 \equiv 3^2 \equiv 9 \equiv 1 \bmod 4$, also auch $p^2 \equiv 1 \bmod 4$ in jedem Fall. $\square$

H23T1A5

(c) Zeigen Sie, dass $x^4 + x + \bar{1}$ in $\mathbb{F}_2[x]$ irreduzibel ist.

(d) Sei $\mathbb{F}_2^{alg}$ ein algebraischer Abschluss von $\mathbb{F}_2$, $\mathbb{F}_{16}$ der eind. bestimmte Zwischenkörper von $\mathbb{F}_2^{alg} | \mathbb{F}_2$ mit 16 Elementen und $\alpha \in \mathbb{F}_2^{alg}$ mit $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ (*). Bestimmen Sie $[\mathbb{F}_2(\beta) : \mathbb{F}_2]$ und $[\mathbb{F}_2(\gamma) : \mathbb{F}_2]$ für $\beta = \alpha + \bar{1}$ und $\gamma = \alpha^3 + \bar{1}$.

zu (c) Sei $f = x^4 + x + \bar{1}$. Wegen $f(\bar{0}) = \bar{1}$ und $f(\bar{1}) = \bar{3} = \bar{1}$ hat f in $\mathbb{F}_2$ keine Nullstellen. Wäre f dennoch reduzibel, dann müsste es zwei irreduzible Polynome $g, h \in \mathbb{F}_2[x]$ vom Grad 2 mit $f = g \cdot h$ geben. Das einzi-

ge irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[x]$ ist bekanntlich $x^2+x+\bar{1}$. $\Rightarrow$ einzig Möglichkeit:

$f = (x^2+x+\bar{1})^2$ aber: $(x^2+x+\bar{1})^2 = (x^2)^2 + x^2 + \bar{1}^2$

$= x^4 + x^2 + \bar{1} \neq f$ ↯ Also ist f in $\mathbb{F}_2[x]$ irreduzibel.

↑ „Freshman's Dream"
char $(\mathbb{F}_2[x]) = 2$

Übung: Sei $f \in \mathbb{F}_2[x]$ ein Polynom vom Grad 4 oder 5. Zeigen Sie: Besitzt f in $\mathbb{F}_4$ keine Nullstelle, dann ist f in $\mathbb{F}_2[x]$ irreduzibel.

Ergänzung: Die einzigen irreduziblen Polynome vom Grad 3 in $\mathbb{F}_2[x]$ sind $x^3+x+\bar{1}$ und $x^3+x^2+\bar{1}$.

zu (d) Es gilt $\mathbb{F}_2(\alpha) = \mathbb{F}_2(\beta)$ wegen $\beta = \alpha + \bar{1} \in \mathbb{F}_2(\alpha)$ und $\alpha = \beta - 1 = \beta + \bar{1} \in \mathbb{F}_2(\beta) \Rightarrow [\mathbb{F}_2(\beta) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = [\mathbb{F}_{16} : \mathbb{F}_2]$. Allgemein gilt $[\mathbb{F}_{2^n} : \mathbb{F}_2] = n$ für alle $n \in \mathbb{N}$, wegen $16 = 2^4$ also $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 4$.

(*) Ergänzung: α ist Nullstelle von $f = x^4 + x + \bar{1}$. Nach Teil (a) ist f irred., außerdem normiert, somit $f = \mu_{\alpha, \mathbb{F}_2} \Rightarrow [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \operatorname{grad}(f) = 4 \Rightarrow \mathbb{F}_2(\alpha) = \mathbb{F}_{2^4} = \mathbb{F}_{16}$

$\alpha^4 + \alpha + \bar{1} = f(\alpha) = \bar{0} \Rightarrow \gamma \cdot \alpha = (\alpha^3 + \bar{1})\,\alpha = \alpha^4 + \alpha$

$= (\alpha + \bar{1}) + \alpha = \bar{2}\,\alpha + \bar{1} = 1 \Rightarrow \gamma = \alpha^{-1}$

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

$\bar{2} = 0$

Daraus folgt $\mathbb{F}_2(\alpha) = \mathbb{F}_2(\gamma)$, denn
$\gamma = \alpha^{-1} \in \mathbb{F}_2(\alpha)$ und $\alpha = \gamma^{-1} \in \mathbb{F}_2(\gamma)$.
$\Rightarrow [\mathbb{F}_2(\gamma) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$

Frage: Die Erweiterung $\mathbb{F}_{16} | \mathbb{F}_2$ besitzt genau drei Zwischenkörper, nämlich $\mathbb{F}_2$, $\mathbb{F}_4$ und $\mathbb{F}_{16}$. Jedes Element in $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ hat die Form $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ mit $a_0, a_1, a_2, a_3 \in \mathbb{F}_2$. Gibt es eine Möglichkeit zu entscheiden, welchen Körper ein solches Element erzeugt?

Sei $\delta := a_0 + a_1 x + a_2 x^2 + a_3 x^3$ wie oben

klar: $\mathbb{F}_2(\delta) = \mathbb{F}_2 \iff \delta \in \mathbb{F}_2 \iff$

$a_1 = a_2 = a_3 = \bar{0}$ Es genügt also, die Elemente von $\mathbb{F}_4$ zu erkennen. Dies sind lt Vorlesung genau die Nullstellen von $x^4 - x \in \mathbb{F}_2[x]$ (*)

also: $\mathbb{F}_2(\delta) = \mathbb{F}_4 \iff \delta \notin \mathbb{F}_2$ und $\delta^4 = \delta$.

z.B.: $\delta = x^2 + x + \bar{1}$ erfüllt $\delta^4 = \delta$,

denn $\delta^2 = (x^2 + x + \bar{1}) = x^4 + x^2 + 1 =$

$(x + \bar{1}) + x^2 + 1 = x^2 + x$, $\delta^4 = (\delta^2)^2 =$

$(x^2 + x)^2 = x^4 + x^2 = (x + 1) + x^2 = \delta$