Erinnerung:
Der kleinste Teilkörper eines Körpers K wird der Primkörper von K genannt.

Satz (18.1)

Sei K ein Körper und P sein Primkörper.

(i) Ist $\mathrm{char}(K) = 0$, dann gilt $P \cong \mathbb{Q}$.

(ii) Ist $\mathrm{char}(K) = p$ für eine Primzahl p, dann gilt $P \cong \mathbb{F}_p$.

Satz (18.2)

Ist K ein endlicher Körper, dann ist $|K|$ eine Primzahlpotenz.
Es gilt also $|K| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$.

Endliche Körper als Zerfällungskörper

Proposition (18.5)

Sei p eine Primzahl, $n \in \mathbb{N}$ und K ein Körper mit p^n Elementen. Dann ist der Primkörper P von K zu $\mathbb{F}_p$ isomorph, und K ist ein Zerfällungskörper von $f_n = x^{p^n} - x \in P[x]$ über dem Körper P.

„Freshman's Dream“ und Frobenius-Endomorphismus

Proposition (18.6)

Sei p eine Primzahl, R ein Ring der Charakteristik p und $n \in \mathbb{N}$. Dann gilt

$$(a+b)^{p^n} \quad = \quad a^{p^n} + b^{p^n} \qquad \text{für alle} \quad a, b \in R.$$

Definition (18.7)

Ist R ein Ring der Charakteristik p, dann bezeichnet man die Abbildung $\varphi : R \to R$, $a \mapsto a^p$ als Frobenius-Endomorphismus des Rings R.

Beweis von Proposition 18.6

geg: Ring R der Char. p, p Primzahl, $n \in \mathbb{N}$

Beh: $\forall a, b \in R: (a+b)^{p^n} = a^{p^n} + b^{p^n}$

Es genügt, die Aussage für $n=1$ zu zeigen, da sich der allgem. Fall leicht durch vollst. Ind. ergibt.

Seien nun $a, b \in R$. Binomischer Lehrsatz $\Rightarrow$

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p$$

Die Zahlen $\binom{p}{k}$ sind wg. $\mathrm{char}(R) = p$ im Ring R gleich 0_R, weil sie in $\mathbb{N}$ durch p teilbar sind:

Es gilt $\binom{p}{k} = \frac{p!}{(p-k)!\,k!}$ Der Zähler ist durch p teilbar, im Gegensatz zum Nenner, falls $1 \leq k \leq p-1$. In $\mathbb{N}$ ist $\binom{p}{k}$ also Vielfaches von p. □

Zur Existenz endlicher Körper

Proposition (18.8)

Sei p eine Primzahl, P ein Körper mit p Elementen, $n \in \mathbb{N}$ und K ein Zerfällungskörper von $f_n = x^{p^n} - x \in P[x]$ über P. Dann gilt

$$|K| = p^n.$$

Beweis von Proposition 18.8

geg.: Primzahl p, P Körper mit $|P| = p$

$n \in \mathbb{N}$, $f_n = x^{p^n} - x \in P[x]$

Sei K ein Zerfällungskörper von f_n über P.

Beh.: $|K| = p^n$

Es gilt $\mathrm{char}(P) = p$, weil $\mathrm{char}(P)$ einerseits eine Primzahl, und andererseits die Ordnung von 1_P in $(P, +)$ ist (d.h. die Ordnung muss ein Teiler von $|P| = p$ sein). Damit gilt auch $\mathrm{char}(K) = p$. ($\Rightarrow$ „Freshman's Dream" ist anwendbar)

Sei $M \subseteq K$ die Menge der Nullstellen von f_n in K.

Beh.: M ist ein Zwischenkörper von $K \mid P$

Zum Nachweis der Teilkörpereigenschaft müssen wir überprüfen: $1_K \in M$. $\forall \alpha, \beta \in M: \alpha - \beta \in M$ und $\alpha\beta \in M$, im Fall $\alpha \neq 0_K$ auch $\alpha^{-1} \in M$

Vorweg: Offenbar gilt die Äquivalenz

$$f_n(\gamma) = 0_K \iff \gamma^{p^n} - \gamma = 0_K \iff \gamma^{p^n} = \gamma$$

für alle $\gamma \in K$, d.h. es gilt jeweils

$$\gamma \in M \iff \gamma^{p^n} = \gamma$$

Zunächst: $1_K^{p^n} = 1_K \Rightarrow 1_K \in M$

Seien nun $\alpha, \beta \in M$. $\Rightarrow \alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$

$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \Rightarrow \alpha\beta \in M$

Im Fall $\alpha \neq 0_K$ gilt auch $(\alpha^{-1})^{p^n} = \alpha^{-p^n} = (\alpha^{p^n})^{-1}$

$= \alpha^{-1} \Rightarrow \alpha^{-1} \in M$. außerdem:

$(\alpha-\beta)^{p^n} = (\alpha+(-\beta))^{p^n} = \alpha^{p^n} + (-\beta)^{p^n} = \alpha^{p^n} + (-1)^{p^n}\beta^{p^n}$

↑ Prop. 18.6

Ist p ungerade, dann auch p^n, somit $(-1)^{p^n} = -1_K$ und

$(\alpha-\beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta \Rightarrow \alpha-\beta \in M$. Im Fall

$p=2$ gilt $-1_K = 1_K$, folglich $(\alpha-\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} =$

$\alpha+\beta = \alpha-\beta \Rightarrow \alpha-\beta \in M$ ↑ $(-1)^{p^n} = 1_K$

Also ist M ein Teilkörper von K.

Für jedes $a \in P$ gilt $a^p = a$, und somit erst recht $a^{p^n} = a$

denn: $|P^\times| = p-1 \Rightarrow a^{p-1} = 1_K \; \forall a \in P^\times \Rightarrow a^p = a \; \forall a \in K^\times$

Außerdem gilt $0_K^p = 0_K$ also: $P \subseteq M$

Insgesamt ist M also ein Zwischenkörper von $K|P$.

$f_n = x^{p^n} - x \longrightarrow f_n' = p^n x^{p^n-1} - 1_K = -1_K$

$\overset{\uparrow}{=} p = 0_K$

$\Rightarrow$ ggT(f_n, f_n') sind teilerfremd $\rightarrow$ f_n besitzt im Körper K p^n verschiedene Nullstellen $\Rightarrow |M| = p^n$

Da M ein Erweiterungskörper von P ist, über dem f_n in Linearfaktoren zerfällt, und da über P von den Nullstellen von f_n erzeugt wird (sogar aus den Nullstellen besteht!), ist M bereits Zerfällungskörper von f_n über P.

$\Rightarrow K = M \Rightarrow |K| = |M| = p^n$. □

Existenz und Eindeutigkeit der endlichen Körper

Satz (18.9)

Sei p eine Primzahl und $n \in \mathbb{N}$. Dann gibt es einen Körper mit p^n Elementen, und je zwei Körper mit p^n Elementen sind zueinander isomorph.

Beweis von Satz 18.9

geg. Primzahl p, $n \in \mathbb{N}$

Existenzaussage: Sei $f_n = x^{p^n} - x \in \mathbb{F}_p[x]$ und K ein Zerfällungskörper von f_n über $\mathbb{F}_p$. Prop 18.8 $\Rightarrow |K| = p^n$

Eindeutigkeit: Ang. L ist ein weiterer Körper mit $|L| = p^n$.

Prop. 18.5 $\rightarrow$ L ist Zerfällungskörper von $\tilde{f}_n = x^{p^n} - x \in P[x]$, wobei P den Primkörper von L bezeichnet. Es gilt $\operatorname{char}(L) = p$, somit $|P| = p$ und $P \cong \mathbb{F}_p$. Sei $\phi : \mathbb{F}_p \to P$ ein Isom. Dann gilt $\tilde{f}_n = \phi(f_n)$. Nach § 17 kann

dieser Fsom. ϕ zu einem Fsom. $K \cong L$ der Zerfällungskörper fortgesetzt werden. $\square$

Der algebraische Abschluss von $\mathbb{F}_p$

Folgerung (18.10)

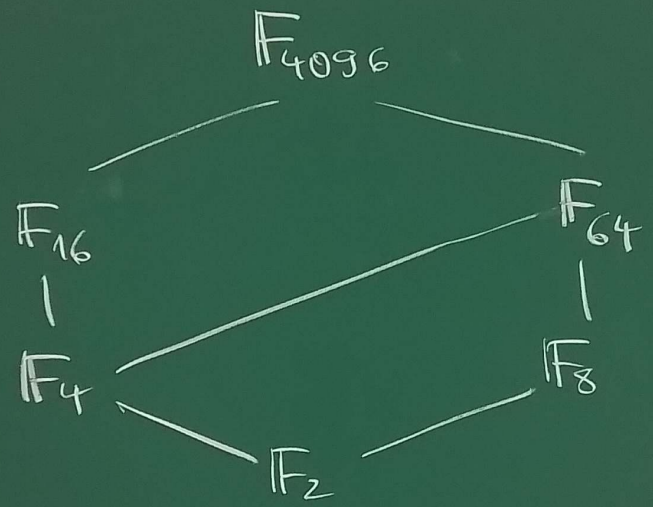
Sei p eine prim und $\mathbb{F}_p^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$.

(i) Für jedes $n \in \mathbb{N}$ gibt es genau einen Teilkörper $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p^{\mathrm{alg}}$ mit p^n Elementen.

(ii) Für $m, n \in \mathbb{N}$ gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ genau dann, wenn m ein Teiler von n ist.

(iii) Es gilt $\mathbb{F}_p^{\mathrm{alg}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$.

Anwendung: Der Verband der Teilkörper von $\mathbb{F}_{4096}$



(Es gilt $\mathbb{F}_8 \not\subseteq \mathbb{F}_{16}$, denn $8 = 2^3$, $16 = 2^4$, und 3 ist kein Teiler von 4.)

(Es gilt $\mathbb{F}_8 \not\subseteq \mathbb{F}_{16}$, denn $8 = 2^3$, $16 = 2^4$, und 3 ist kein Teiler von 4.)

Beweis von Folgerung 18.10

zu (i) Sei $\mathbb{F}_{p^n}$ für jedes $n \in \mathbb{N}$ jeweils der Zerfällungskörper von $f_n = x^{p^n} - x \in \mathbb{F}_p[x]$ in $\mathbb{F}_p^{alg}$. (beachte: Da $\mathbb{F}_p^{alg}$ algebraisch abgeschlossen ist, zerfällt f_n über $\mathbb{F}_p^{alg}$ in Linearfaktoren. Man erhält $\mathbb{F}_{p^n}$ also durch $\mathbb{F}_{p^n} = \mathbb{F}_p(N)$, mit $N = \{\alpha \in \mathbb{F}_p^{alg} \mid f_n(\alpha) = \bar{0}\}$.)
Eindeutigkeit: Sei K ein Zwi. Teilkörper von $\mathbb{F}_p^{alg}$ mit $|K| = p^n$. Dann besteht K aus den Nullstellen von f_n (folgt aus Prop. 18.5 und dem Bew. von Prop. 18.8) $\Rightarrow K = \mathbb{F}_{p^n}$

zu (ii) Seien $m, n \in \mathbb{N}$. Beh: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$

„$\Leftarrow$" $m \mid n \rightarrow \exists d \in \mathbb{N}$ mit $n = dm$. s.o. $\Rightarrow$ Die Elemente

von $\mathbb{F}_{p^m}$ sind die Nullst. von f_m, die von $\mathbb{F}_{p^n}$ die Nullst. von f_n. Sei nun $\gamma \in \mathbb{F}_{p^m}$ $\Rightarrow$
$f_m(\gamma) = \bar{0} \Rightarrow \gamma^{p^m} = \gamma$ Durch vollst. Ind. erhält man $\gamma^{(p^m)^k} = \gamma \; \forall k \in \mathbb{N}$, insb. $\gamma^{(p^m)^q} = \gamma$
$\Rightarrow \gamma^{p^{mq}} = \gamma \Rightarrow \gamma^{p^n} = \gamma \Rightarrow f_n(\gamma) = \bar{0} \Rightarrow \gamma \in \mathbb{F}_{p^n}$
also: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$

„$\Rightarrow$" $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Rightarrow \mathbb{F}_{p^n} \mid \mathbb{F}_{p^m}$ ist eine Körpererweiterung (endlich, da $\mathbb{F}_{p^n}$ endlich ist)
Sei $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \Rightarrow \mathbb{F}_{p^n}$ ist d-dim. $\mathbb{F}_{p^m}$-Vektorraum. $p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d =$

$(p^m)^d = p^{md} \longrightarrow n = dm \Rightarrow m \mid n$.

zu (iii) z.Zg.: $\mathbb{F}_p^{alg} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$

„⊇" gilt nach Def. der Teilkörper $\mathbb{F}_{p^n}$.

„⊆" Sei $\alpha \in \mathbb{F}_p^{alg}$. α ist algebraisch über $\mathbb{F}_p$ (nach Def. von $\mathbb{F}_p^{alg}$) Sei $f = Min_{\alpha, \mathbb{F}_p} \in \mathbb{F}_p[x]$ und $n = grad(f)$. $\Rightarrow [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = grad(f) = n \Rightarrow \mathbb{F}_p(\alpha)$ ist n-dim. $\mathbb{F}_p$-Vektorraum $\Rightarrow$ $|\mathbb{F}_p(\alpha)| = p^n \xrightarrow[\text{siehe (i)}]{\text{Eindeutigkeit}} \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n} \Rightarrow$ $\alpha \in \mathbb{F}_{p^n}$

□

Definition (19.1)

Sei K ein Körper. Ein irreduzibles Polynom $f \in K[x]$ wird separabel genannt, wenn $\mathrm{ggT}(f, f') = 1$ gilt.

Nach Proposition 18.4 ist die Separabilität von f gleichbedeutend damit, dass das irreduzible Polynom f in jedem Erweiterungskörper L von K nur einfache Nullstellen besitzt.

Separable Elemente und separable Körpererweiterungen

Definition (19.2)

Sei $L|K$ eine Körpererweiterung. Ein Element $\alpha \in L$ wird separabel über K genannt, wenn es algebraisch über K ist und sein Minimalpolynom $f \in K[x]$ separabel ist. Wir nennen die Erweiterung $L|K$ separabel, wenn jedes $\alpha \in L$ über K separabel ist.