

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 $\text{char}(K) = 0$, dann gilt $P \cong \mathbb{Q}$.
- (ii) Ist $\text{char}(K) = p$ 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 $n \in \mathbb{N}$.

Formale Ableitung und mehrfache Nullstellen

Definition (18.3)

Sei K ein Körper und $f = \sum_{k=0}^n a_k x^k \in K[x]$, mit $n \in \mathbb{N}_0$ und $a_0, \dots, a_n \in K$. Dann nennt man

$$f' = \sum_{k=1}^n k a_k x^{k-1} \quad \text{die formale Ableitung von } f.$$

Proposition (18.4)

Sei K ein Körper, $f \in K[x]$ ein Polynom vom Grad $n \geq 1$ und $\tilde{L}$ ein Erweiterungskörper von K , über dem f in Linearfaktoren zerfällt. Dann sind die folgenden beiden Aussage äquivalent:

- (i) Es gilt $\text{ggT}(f, f') = 1$ in $K[x]$.
- (ii) Das Polynom f besitzt in $\tilde{L}$ nur **einfache** Nullstellen, d.h. es ein $a \in K^\times$ und n verschiedene Elemente $\alpha_1, \dots, \alpha_n \in L$, so dass $f = a \prod_{i=1}^n (x - \alpha_i)$.

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 .

Beweis von Proposition 18.5

geg. Primzahl p , $n \in \mathbb{N}$, K Körper mit p^n

Elementen Sei P der Primkörper von K .

Beh. (i) $P \cong \mathbb{F}_p$

(ii) K ist Zerst.-korp. von $f_n = x^{p^n} - x \in P[x]$
über dem Körper P

zuli) folgt direkt aus Satz 18.1 (Es ist $P \cong \mathbb{Q}$ oder

$P \cong \mathbb{F}_q$ für eine Primzahl q . $P \cong \mathbb{Q}$ scheitert aus, da

K und P endlich sind also: $P \cong \mathbb{F}_q$ für eine

Primzahl q außerdem: $(P, +)$ ist Untergruppe von

$(K, +)$, $|K| = p^n \Rightarrow q = |P|$ teilt $p^n \Rightarrow q = p$)
Lagrange

zu iii) Es ist $K^\times$ eine Gruppe der Ordnung $p^n - 1 \Rightarrow x^{p^n - 1} = 1_K$
 $\forall x \in K^\times \Rightarrow x^{p^n - 1} - 1 = 0_K$ und $x^{p^n} - x = 0_K \forall x \in K^\times$. Also ist
jedes Elt. von $K^\times$ eine Nullstelle des Polynoms f_n . Dasselbe
gilt offenbar auch für 0_K , also: K besteht genau aus den Null-
stellen von f_n . Wegen $|K| = p^n = \text{grad } f_n$ zerfällt f_n damit
über K in Linearfaktoren, und K wird über P durch die Null-
stellen von f_n erzeugt. $\Rightarrow K$ ist zut. krp. von f_n über P . $\square$

Proposition (18.6)

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

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

Definition (18.7)

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

Beweis von Proposition 18.6

geg: p Primzahl, R Ring mit $\text{char}(R) = p$

$$(\Rightarrow p \cdot 1_R = 0_R)$$

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

Beweis für $n=1$: Seien $a, b \in R$

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

Sei $k \in \{1, \dots, p-1\}$. $\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{N}$

Der Zähler ist durch p teilbar, der Nenner $k!(p-k)!$ wegen $k, p-k < p$ aber nicht.

$\Rightarrow p \mid \binom{p}{k} \Rightarrow$ Das Bild von $\binom{p}{k}$ in R ist gleich 0
 $\Rightarrow (a+b)^p = a^p + b^p \quad (*)$

Beweise nun $\forall a, b \in R \quad \forall n \in \mathbb{N}: (a+b)^{p^n} = a^{p^n} + b^{p^n}$
 durch vollst. Ind über n . Ind.-Anf. ($n=1$) ist
 bereits erledigt. Ist $n \in \mathbb{N}$ und setzt man
 die Gleichung für n voraus, dann folgt

$$\begin{aligned} (a+b)^{p^{n+1}} &= ((a+b)^{p^n})^p \stackrel{\text{Ind.}}{=} (a^{p^n} + b^{p^n})^p \stackrel{\text{Fall } n=1}{=} \\ &= (a^{p^n})^p + (b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}} \end{aligned}$$

(*) allgemein: Ist $a \in \mathbb{Z}$, R Ring mit $\text{char}(R) = p$.
 $p \mid a$, dann ist das Bild von a in R , also $a \cdot 1_R$,
 gleich 0 in R , denn: $p \mid a \Rightarrow \exists l \in \mathbb{Z}$ mit $a = pl \Rightarrow$

$$a \cdot 1_R = (l_p) \cdot 1_R = l \cdot (p \cdot 1_R) = l \cdot 0_R = 0_R$$

$\uparrow$ Potenzgesetz $\uparrow$ char(R) = p
 $\text{in } (R, +)$

$p-k$ k
 a b

$\mathbb{N}$

immer
 nicht

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

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

+ gleich

Beweis von Proposition 18.8

$a^{p^n} = a$
= 1) ist

es man
folgt

$a^{p^n} = a$
Fall $n=1$

das $(\mathbb{R}) = \mathbb{P}$
also $a \in \mathbb{R}$
 $a = p! \Rightarrow$

geg. Primzahl p , P Körper mit $|P| = p$,
 $f_n = x^{p^n} - x \in P[x]$, K Zerfällungskörper von
 f_n über P Beh.: $|K| = p^n$

Sei $M = \{ \alpha \in K \mid f_n(\alpha) = 0_K \}$. zeige:

(1) M ist Teilkörper von K

(2) M ist Erweiterungskörper von P

zu (1) zu überprüfen (i) $1_K \in M$ (ii) $\forall \alpha, \beta \in M : \alpha - \beta, \alpha\beta \in M$ (iii) $\forall \alpha \in M \setminus \{0_K\} : \alpha^{-1} \in M$

Für alle $\alpha \in K$ gilt die Äquivalenz $\alpha \in M \iff$

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

zu li) folgt direkt aus $1_K^{p^n} = 1_K$

zu ii) geg. $\alpha, \beta \in M \xrightarrow{\text{s.o.}} \alpha^{p^n} = \alpha, \beta^{p^n} = \beta \Rightarrow (\alpha\beta)^{p^n}$
 $= \alpha^{p^n} \beta^{p^n} = \alpha\beta \Rightarrow \alpha\beta \in M$

Für die Addition unterscheiden zwei Fälle

1 Fall: p ungerade $(\alpha - \beta)^{p^n} = (\alpha + (-1)\beta)^{p^n} \stackrel{\text{Prop 18.6}}{=} \alpha^{p^n} + (-1)^{p^n} \beta^{p^n}$
 $= \alpha + (-1)^{p^n} \beta \stackrel{p^n \text{ ungerade}}{=} \alpha + (-1)\beta = \alpha - \beta \Rightarrow \alpha - \beta \in M$

2 Fall: $p = 2$ Dann gilt $\text{char}(p) = \text{char}(K) = 2 \Rightarrow$

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

$(\alpha + \beta)^{p^n} \stackrel{\text{Prop 18.6}}{=} \alpha^{p^n} + \beta^{p^n} = \alpha + \beta = \alpha - \beta \Rightarrow \alpha - \beta \in M$

zu iii) geg. $\alpha \in M \setminus \{0\} \Rightarrow \alpha^{p^n} = \alpha \Rightarrow (\alpha^{-1})^{p^n} = \alpha^{-p^n} =$

2. Fall: $p = 2$ Dann gilt $\text{char}(P) = \text{char}(K) = 2 \Rightarrow$

$$(x^{p^n})^{-1} = x^{-1} \Rightarrow x^{-1} \in M$$

zu (2) z.zg: $P \subseteq M$ Wegen $|P| = p$ gilt $x^p = x \quad \forall x \in P$ (vgl. Bew. von Prop. 18.5), somit auch $x^{p^n} = x \quad \forall x \in P \Rightarrow x \in M \quad \forall x \in P$

Da M ein Zwischenkörper von $K|P$ ist, da alle Nullstellen von f_n in K bereits enthält, stimmt M mit dem Zerf.-korp. K überein. Es genügt also z.zg: $|M| = p^n$. Da f_n über M in Linearfaktoren zerfällt und $\text{grad } f_n = p^n$ ist, reicht es dafür zu überprüfen, dass f_n in K keine mehrfachen Nullstellen hat. $f_n = x^{p^n} - x \Rightarrow f_n' = p^n \cdot x^{p^n-1} - 1_K = -1_K \Rightarrow \text{ggT}(f_n, f_n') = 1_K \xrightarrow{\text{Prop. 18.4}} f_n \text{ hat in } K \text{ nur einfache Nullstellen.}$ $\triangle \text{char}(K) = p$



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.

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

Folgerung (18.10)

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

- (i) Für jedes $n \in \mathbb{N}$ gibt es **genau einen** Teilkörper $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p^{\text{alg}}$ 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 $\mathbb{F}_p^{\text{alg}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$.

Die Aussage (iii) wurde im Skript **nachträglich ergänzt**.

3 kein Teiler von k ist
(2) $\mathbb{F}_4$ ist nicht isomorph $\mathbb{Z}/4\mathbb{Z}$, ebenso $\mathbb{F}_8$ nicht zu $\mathbb{Z}/8\mathbb{Z}$ usw.

Beweis von Folgerung 18.10:

geg: p Primzahl, $\mathbb{F}_p^{\text{alg}}$ algebraischer Abschluss von $\mathbb{F}_p$

zul i) Sei $n \in \mathbb{N}$. Beh.: Es gibt genau einen Zwischenkörper von $\mathbb{F}_p^{\text{alg}} | \mathbb{F}_p$ mit p^n Elementen

Existenz: Sei K der Zsf. körp. von $f_n = x^{p^n} - x \in \mathbb{F}_p[x]$ über $\mathbb{F}_p$.

Prop. 18.8 $\Rightarrow |K| = p^n$ Dehnische $\mathbb{F}_{p^n} = K$

Eindeutigkeit: Sei nun K_1 ein bel. Zwischenkörper von $\mathbb{F}_p^{\text{alg}} | \mathbb{F}_p$ mit $|K_1| = p^n$. Dann ist $\mathbb{F}_p$ der Primkörper von K_1 , und nach Prop. 18.5 ist K_1 der Zsf. körp. von f_n über $\mathbb{F}_p$ in $\mathbb{F}_p^{\text{alg}}$.

$\Rightarrow K_1 = \mathbb{F}_{p^n}$

zul ii) Seien $m, n \in \mathbb{N}$. z.zg. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m | n$

" $\Leftarrow$ " $m \mid n \Rightarrow \exists d \in \mathbb{N}$ mit $n = dm$

in Prop. 18.8 gezeigt: $\mathbb{F}_{p^m}$ ist die Nullstellenmenge von f_m , $\mathbb{F}_{p^n}$ die Nullstellenmenge von f_n in $\mathbb{F}_p^{\text{alg}}$. Definiere $\phi: \mathbb{F}_p^{\text{alg}} \rightarrow \mathbb{F}_p^{\text{alg}}$ durch $\phi(x) = x^{p^m} \quad \forall x \in \mathbb{F}_p^{\text{alg}}$

$$\text{Sei nun } x \in \mathbb{F}_{p^m} \Rightarrow f_m(x) = 0 \Rightarrow x^{p^m} = x$$

$$\Rightarrow \phi(x) = x \Rightarrow \phi^d(x) = x \Rightarrow x^{(p^m)^d} = x$$

$$\Rightarrow x^{p^{md}} = x \Rightarrow x^{p^n} = x \Rightarrow f_n(x) = 0$$

$$\Rightarrow x \in \mathbb{F}_{p^n}$$

" $\Rightarrow$ " Vor: $\mathbb{F}_{p^n}$ ist Erw.-bsp. von $\mathbb{F}_{p^m}$

Sei $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = d \in \mathbb{N}$, und $\mathbb{F}_{p^n}$ ist endl.

$\mathbb{F}_{p^n}$ ist d -dim. $\mathbb{F}_{p^m}$ -Vektorraum $\Rightarrow \mathbb{F}_{p^n}$ ist

$\mathbb{F}_{p^m}$ -Vektorraum isomorph zu $(\mathbb{F}_{p^m})^d \Rightarrow$

$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d = (p^m)^d = p^{md}$$

$$\Rightarrow n = md \Rightarrow m \mid n$$

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

" $\supseteq$ " Für alle $n \in \mathbb{N}$ gilt $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p^{\text{alg}}$ auf Grund der Definition von $\mathbb{F}_{p^n}$.

" $\subseteq$ " Sei $\alpha \in \mathbb{F}_p^{\text{alg}}$. Sei $K = \mathbb{F}_p(\alpha)$. Da α algebraisch über $\mathbb{F}_p$ ist, ist $\mathbb{F}_p(\alpha) / \mathbb{F}_p$ eine endliche Erweiterung. Sei $n = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$.

ebenso: Ist K ein endlicher Körper, dann
Ist jedes irreduzible Polynom in $K[x]$

$\Rightarrow \mathbb{F}_p(\alpha)$ ist n -dim. $\mathbb{F}_p$ -Vektorraum $\Rightarrow$

Ist $|\mathbb{F}_p(\alpha)| = p^n \xrightarrow{(1)} \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n} \Rightarrow \alpha \in \mathbb{F}_{p^n}$



auf

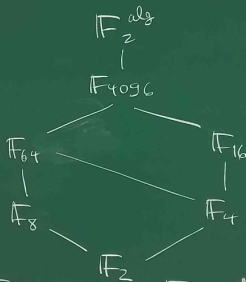
Da α

eine

$\mathbb{F}_p$.

Beispiel zu Folgerung 18.10:

Die Teilkörper von $\mathbb{F}_{4096} = \mathbb{F}_{2^{12}}$



Hinweise:

- (1) $\mathbb{F}_8$ ist kein Teilkörper von $\mathbb{F}_{16}$, da $8 = 2^3$, $16 = 2^4$ und 3 kein Teiler von 4 ist
- (2) $\mathbb{F}_4$ ist nicht isomorph $\mathbb{Z}/4\mathbb{Z}$, ebenso $\mathbb{F}_8$ nicht zu $\mathbb{Z}/8\mathbb{Z}$ usw.

§ 19. Separable Erweiterungen und Galois-Erweiterungen

Definition (19.1)

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

zum Begriff des separablen Polynoms:

i) $K = \mathbb{Q}$, $f = x^2 - 2 \Rightarrow f' = 2x$

$\Rightarrow \text{ggT}(f, f') = 1 \Rightarrow f$ ist separabel

ii) werden später sehen: Ist K ein Körper mit $\text{char}(K) \neq 0$, dann ist jedes irreduzible Polynom über K separabel.

ebenso: Ist K ein endlicher Körper, dann ist jedes irreduzible Polynom in $K[x]$ separabel über K .

Frage: Gibt es Körper K , die weder endlich sind, noch die Bed. $\text{char}(K) \neq 0$ erfüllen?

Antwort: Ja! Sei $\mathbb{F}_p[t]$ der Polynomring über $\mathbb{F}_p$.
Dann wird der Quotientenkörper $\mathbb{F}_p(t)$ dieses Rings der
rationale Funktionenkörper über $\mathbb{F}_p$ genannt.

$$\text{Es gilt } \mathbb{F}_p(t) = \left\{ \frac{u}{v} \mid u, v \in \mathbb{F}_p[t], v \neq 0 \right\}$$

Es gilt $\text{char } \mathbb{F}_p[t] = \text{char } \mathbb{F}_p(t) = p$, und
da $\mathbb{F}_p[t]$ unendlich ist, gilt dasselbe für $\mathbb{F}_p(t)$.