H19T3A4 Sei p eine Primzahl.

(a) Sei $g \in \mathbb{F}_p[x]$ ein irreduzibles Polynom vom Grad m ($m \in \mathbb{N}$). Zeigen Sie, dass g ein Teiler von $x^{p^m} - x$ ist.

(b) Beweisen Sie für jedes nicht-konstante Polynom $g \in \mathbb{F}_p[x]$ die Äquivalenz

g ist irreduzibel $\Leftrightarrow$ $ggT(g, x^{p^m} - x) = 1$ für $1 \leq m \leq \frac{1}{2}\,\mathrm{grad}(g)$

(b) Beweisen Sie für jedes nicht-konstante

zu (a) Sei $\mathbb{F}_p^{alg}$ ein algebraischer Abschluss von $\mathbb{F}_p$.
Aus der Vorlesung ist bekannt, dass der Teilkörper
$\mathbb{F}_{p^m} \subseteq \mathbb{F}_p^{alg}$ genau aus den Nullstellen des
Polynoms $f_m = x^{p^m} - x \in \mathbb{F}_p[x]$ besteht. [Erinnerung: $\alpha \in \mathbb{F}_{p^m}^\times \Rightarrow |\mathbb{F}_{p^m}^\times| = p^m - 1$
$\alpha^{p^m - 1} = \bar{1} \Rightarrow$
$\alpha^{p^m} = \alpha \Rightarrow f_m(\alpha) = \alpha^{p^m} - \alpha = \alpha - \alpha = \bar{0}$. ebenso
$f_m(\bar{0}) = \bar{0}$ Mehr als p^m Nullstellen kann f_m als
Polynom vom Grad p^m nicht besitzen.]
Sei $\alpha \in \mathbb{F}_p^{alg}$ mit $g(\alpha) = \bar{0}$. g irreduzibel $\Rightarrow$
$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \text{grad}(g) = m \Rightarrow \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$

separabel

zu (b) „

Ang.
stell
wie
$\alpha \in$
α and
folgt
$\Leftarrow$
irredu
$d = \text{gra}$

(weil $\mathbb{F}_{p^m}$ der einzige Zwischenkörper von $\mathbb{F}_p^{alg} / \mathbb{F}_p$ vom Grad m über $\mathbb{F}_p$ ist) $\Rightarrow \alpha \in \mathbb{F}_{p^m} \Rightarrow f_m(\alpha) = \bar{0}$

Also ist jede Nullstelle von g in $\mathbb{F}_p^{alg}$ auch eine Nullstelle von f_m. Daraus folgt $g \mid f_m$, da g als irred. Polynom über $\mathbb{F}_p$ separabel ist und somit in $\mathbb{F}_p^{alg}$ keine mehrfachen Nullstellen hat.

zu (⇐) „$\Longrightarrow$" Vor: g ist irreduzibel Sei $m \in \mathbb{N}$ mit $1 \leq m \leq \frac{1}{2} d$, wobei $d = \text{grad}(g)$.

z.zg: $ggT(g, f_m) = 1$ $ggT(g, f_m) \mid g$,

g ist irreduzibel $\Rightarrow ggT(g, f_m) = 1$ oder $ggT(g, f_m) = g$

f ist und somit in $\mathbb{F}_p^{alg}$ keine mehrfachen Nullstellen hat.

zu (b) „$\Longrightarrow$" Vor: g ist irreduzibel Sei $m \in \mathbb{N}$

Ang. $ggT(g, f_m) = g$ $\Rightarrow$ $g \mid f_m$ $\Rightarrow$ Jede Nullstelle von g in $\mathbb{F}_p^{alg}$ ist auch eine Nullstelle von f_m. Wie in Teil (a) gezeigt, gilt für jede Nullstelle $\alpha \in \mathbb{F}_p^{alg}$ von g jeweils $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Weil dieses α auch in $\mathbb{F}_{p^m}$ liegt, folgt $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^m}$. Daraus folgt $d \mid m$ $\Rightarrow$ $d \leq m$ $\lightning$ da $d > \frac{1}{2} d = m$.

„$\Longleftarrow$" Ang. g ist reduzibel. Dann besitzt g einen irreduziblen Faktor $h \in \mathbb{F}_p[x]$ von Grad $\leq \frac{1}{2} d$, wobei $d = \text{grad}(g)$ ist. Teil (a), angewandt auf h $\Rightarrow$ (*)

$h \mid (x^{p^m} - x)$, wobei $m = \operatorname{grad}(h)$

$\overset{h \mid g}{\Rightarrow} h \mid \operatorname{ggT}(x^{p^m} - x, g) \Rightarrow$

$\operatorname{ggT}(x^{p^m} - x, g) \neq 1$ $\square$

(*) ausführliches: Ang. g ist reduzibel.

$\Rightarrow \exists\, h_1, h_2 \in \mathbb{F}_p[x] \setminus \mathbb{F}_p$ und $g = h_1 h_2$

$\Rightarrow \operatorname{grad}(h_1) + \operatorname{grad}(h_2) \leq d \Rightarrow$

$\operatorname{grad}(h_1) \leq \frac{1}{2} d$ oder $\operatorname{grad}(h_2) \leq \frac{1}{2} d$

o.B.d.A. $\operatorname{grad}(h_1) \leq \frac{1}{2} d$ Sei h ein irred. Faktor von $h_1 \Rightarrow \operatorname{grad}(h) \leq \frac{1}{2} d$, und h ist auch Faktor von g.

Normale Erweiterungen

Def. Sei $L|K$ eine Körpererweiterung

$L|K$ normal $\Leftrightarrow$ $L|K$ ist algebraisch und es gilt: Jedes über K irreduzible Polynom, dass in L eine Nullstelle hat, zerfällt über L in Linearfaktoren.

Erinnerung:

(i) $[L:K]=2 \Rightarrow L|K$ ist normal

(ii) $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal, denn: $f=x^3-2 \in \mathbb{Q}[x]$ hat in $\mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle (nämlich $\sqrt[3]{2}$), ist über $\mathbb{Q}$ irreduzibel (Eisenstein), zerfällt aber nicht über

$\mathbb{Q}(\sqrt[3]{2})$ in Linearfaktoren. (Die irreduzible Zerlegung von f in $\mathbb{Q}(\sqrt[3]{2})[x]$ ist $f = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$, und die Nullstellen des Faktors vom Grad 2, $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$ mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ liegen nicht in $\mathbb{R}$, erst recht nicht in $\mathbb{Q}(\sqrt[3]{2})$.

(iii) Eine endliche Erweiterung L/K ist genau dann normal, wenn L Zerfällungskörper eines Polynoms $f \in K[x]$ über K ist.
Eine weitere äquivalente Bed. lautet $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, \tilde{L})$, wobei $\tilde{L}$ einen bel. alg. abgeschlossenen Erweiterungskörper

von L bezeichnet.

Separable Erweiterungen

Def. Sei K ein Körper.

i) Ein irreduzibles Polynom $f \in K[x]$ heißt separabel, wenn $ggT(f', f) = 1$ ist.

ii) Sei $L|K$ eine Körpererweiterung und $\alpha \in L$. Man nennt α separabel über K, wenn α algebraisch über K und das Minimalpol. $M_{\alpha,K}$ separabel ist.

iii) $L|K$ ist separabel $\Rightarrow$ Jedes $\alpha \in L$ ist separabel über K. (also insbesondere: $L|K$ separabel $\Rightarrow L|K$ algebraisch)

Erinnerung:

(i) K endlicher Körper $\Rightarrow$ Jede alg. Erweiterung von K ist separabel.

(ii) K Körp. mit $\mathrm{char}(K) = 0 \Rightarrow$ Jede alg. Erw. von K ist separabel.

(iii) Sei p eine Primzahl und $\mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$, also der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$. Dann ist $\mathbb{F}_p(t) \mid \mathbb{F}_p(t^p)$ eine inseparable (= nicht separable) Erweiterung.

(iv) Satz vom primitiven Element: Jede endliche separable Erweiterung $L|K$ wird von einem einzigen Element erzeugt, d.h. es gibt ein $\alpha \in L$ mit $L = K(\alpha)$.

Def.: Eine Galois-Erweiterung ist eine Körpererweiterung, die normal und separabel ist.

H24T1A5

(a) Sei $L|K$ eine Körpererweiterung vom Grad 2 mit $\mathrm{char}(K) \neq 2$. Zeigen Sie, dass $L|K$ galoissch ist.

zu (a) bekannt: Als Erweiterung vom Grad 2 ist $L|K$ normal.

noch z.zg.: $L|K$ ist separabel. Dafür muss gezeigt werden, dass jedes $\alpha \in L$ separabel über K ist. Sei also $\alpha \in L$.

1. Fall: $\alpha \in K$. Dann ist $f = x - \alpha$ das Minipol von α über K. Dieses ist wegen $ggT(f, f') = ggT(x-\alpha, 1) = 1$ separabel, also ist α separabel über K.

2. Fall: $\alpha \in L \setminus K$. Sei $f = \mu_{\alpha, K} \in K[x]$.

$K(\alpha)$ ist Zwischenkörper von $L|K$. Gradformel $\Rightarrow$

$2 = [L:K] = [L:K(\alpha)] \cdot [K(\alpha):K]$ $\quad \alpha \notin K \Rightarrow$

$[K(\alpha):K] > 1$, außerdem $[K(\alpha):K] \mid 2 \Rightarrow [K(\alpha):K] = 2$

$[K(\alpha):K] > 1$, außerdem $[K(\alpha):K] \mid 2 \Rightarrow [K(\alpha):K] = 2$

$\Rightarrow \operatorname{grad}(f) = [K(\alpha):K] = 2 \rightarrow \exists a, b \in K$ mit
$f = x^2 + ax + b$ (und f ist irred. über K).
$f' = 2x + a$ Wegen $\operatorname{char}(K) \neq 2$ gilt $2 \neq 0$ in K, somit ist
f' ein Polynom vom Grad 1. f irred., $\operatorname{ggT}(f, f') \mid f \Rightarrow$
$\operatorname{ggT}(f, f') = 1$ oder $\operatorname{ggT}(f, f') = f$.

1. Fall: $\operatorname{ggT}(f, f') = 1$ Dann ist f separabel, und somit ist α separabel über K.

2 Fall: $\operatorname{ggT}(f, f') = f$ $\operatorname{ggT}(f, f') \mid f' \Rightarrow f \mid f'$
↯ da $\operatorname{grad}(f) = 2 > 1 = \operatorname{grad}(f')$

Als normale und separable Erw. ist $L \mid K$ galois'sch.

(6) Geben Sie eine Erweiterung vom Grad 2 an, die nicht galois'sch ist.

Sei $\mathbb{F}_2(t)$ der rationale Funktionenkörper über $\mathbb{F}_2$. Beh.: (1) $[\mathbb{F}_2(t) : \mathbb{F}_2(t^2)] = 2$

(2) $\mathbb{F}_2(t) \mid \mathbb{F}_2(t^2)$ ist nicht separabel, und damit auch nicht galois'sch

zu (1) Es gilt $\mathbb{F}_2(t) = \mathbb{F}_2(t^2)(t)$ wegen $\mathbb{F}_2 \subseteq \mathbb{F}_2(t^2)(t)$ und $t \in \mathbb{F}_2(t^2)(t)$ einerseits, und da andererseits aus $t^2 \in \mathbb{F}_2(t)$ auch $\mathbb{F}_2(t^2) \subseteq \mathbb{F}_2(t)$ folgt, und wegen $t \in \mathbb{F}_2(t)$ damit auch $\mathbb{F}_2(t^2)(t) \subseteq \mathbb{F}_2(t)$.

zu (2)

nich

=

Char

über

separa

$\mathbb{F}_2(t)$

$\mathbb{F}_2(t^2$

Sei $\mathbb{F}_2(t)$ der rationale Funktionenkörper

Beh: $M_{t,K} = x^2 - t^2$, wobei $K = \mathbb{F}_2(t^2)$

Das Pol. $f = x^2 - t^2 \in K[x]$ ist normiert, und es gilt $f(t) = t^2 - t^2 = 0$. Aug. f ist über K reduzibel. Wegen $\operatorname{grad}(f) = 2$ liegt dann eine Nullstelle von $x^2 - t^2$ in K. $f = (x-t)^2$ da $\operatorname{char}(K) = 2 \Rightarrow t$ ist die einzige Nullstelle von f

Also wäre $t \in K$. $\Rightarrow \exists u, v \in \mathbb{F}_2[t]$ mit $t = \frac{u(t^2)}{v(t^2)}$, da jedes Element aus K diese Form hat.

$\Rightarrow t\,v(t^2) = u(t^2)$ ↯ da der Grad von $v(t^2)$ in t gerade und der von $t\,v(t^2)$ ungerade ist ($\Rightarrow$ Beh)

$\Rightarrow [\mathbb{F}_2(t) : \mathbb{F}_2(t^2)] = [\mathbb{F}_2(t^2)(t) : \mathbb{F}_2(t^2)] = \operatorname{grad}(f) = 2$.

zu (2) Das Polynom $f = M_{t,k} = x^2 - t^2$ ist nicht separabel, da $ggT(f, f') = ggT(f, 2x)$
$= ggT(f, 0) = f \neq 1 \Rightarrow t$ ist nicht separabel über $k = \mathbb{F}_2(t^2)$ $\overset{t \in \mathbb{F}_2(t)}{\Rightarrow}$ $\mathbb{F}_2(t) / \mathbb{F}_2(t^2)$ ist nicht separabel.

$\mathbb{F}_2(t) = \left\{ \frac{u}{v} \mid u, v \in \mathbb{F}_2[t],\ v \neq 0 \right\}$

$\mathbb{F}_2(t^2) = \left\{ \frac{u(t^2)}{v(t^2)} \mid u, v \in \mathbb{F}_2[t],\ v \neq 0 \right\}$