H12T2A4 Sei p eine Primzahl und K ein Körper mit $\mathrm{char}(K) = 0$.

(a) Sei $E|K$ eine endliche Galois-Erw. Zeigen Sie, dass es einen Zwischenkörper F von $E|K$ gibt, so dass $[E:F]$ eine p-Potenz und $[F:K]$ teilerfremd zu p ist.

Sei $G = \mathrm{Gal}(E|K)$, U eine Untergruppe von G und $F = E^U$ der zugehörige Fixkörper. Laut Galoistheorie gilt $[E:F] = |U|$ und $[F:K] = (G:U)$. Sei nun U_1 eine p-Sylowgruppe. Nach

e
de
w
[E
te
(b)
m
p

und K ein

is-Erw.

enkörper

$E:F]$ eine

fremd zu p ist.

itergruppe von

Fixkörper. Laut

und $[F:k]$ =

gruppe. Nach

Definition der p-Sylowgruppen ist $|U_1|$ eine p-Potenz und $(G:U_1)$ teilerfremd zu p. (Dass es mind. eine p-Sylowgr. gibt, folgt aus dem Nullten Sylowsatz.) Setzen wir also $F_1 = E^{U_1}$, dann ist $[E:F_1]$ eine p-Potenz und $[F_1:k]$ teilerfremd zu p.

(β) Wir setzen nun voraus, dass für jede nichttriv. endl. Erweiterung $L|K$ die Zahl p jeweils ein Teiler von $[L:K]$ ist.

Beweise

endl.

ist.

Sei $L|$

Dann ist

char(K)

$\Rightarrow L|K$

Satz vom

$L = K(\alpha$

E ein Ze

Als Zef. k

ogruppen ist
$(G : U_1)$
es mind.
folgt aus
) Setzen
ann ist
nd $[F_1 : K]$

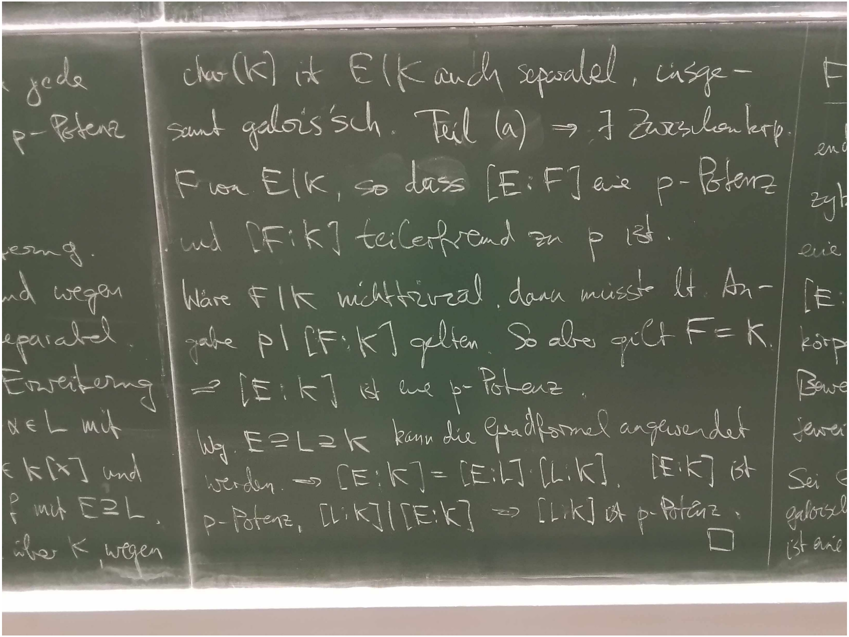
, dass für jede
g $L|K$ die Zahl
$K]$ ist.

Beweisen Sie, dass $[L:K]$ für jede endl. Erweiterung $L|K$ eine p-Potenz ist.

Sei $L|K$ eine endl. Erweiterung. Dann ist $L|K$ algebraisch, und wegen $\mathrm{char}(K) = 0$ damit auch separabel.
$\Rightarrow$ $L|K$ ist endl. separable Erweiterung
Satz vom prim. Elt. $\Rightarrow$ $\exists \alpha \in L$ mit $L = K(\alpha)$. Sei $f = \mu_{\alpha,K} \in K[x]$ und E ein Zerfällungskörper von f mit $E \supseteq L$.
Als Zerf.körp. ist E normal über K, wegen

cha
samt
F vo
und
Wäre
gabe
$\Rightarrow [E$
Wg. E
werden
p-Potenz

Korrektur erste Zeile: „$\mathrm{char}(K) = 0$ ist $E|K$ auch separabel,…“



insge-
Zwischenkörp.
e p-Potenz
ist.

wisste lt. An-
e gilt $F = K$.

mel angewendet
$:K]$. $[E:K]$ ist
$:K]$ ist p-Potenz. $\square$

<u>F15T3A5</u> Sei $E|K$ eine endliche Galois-Erweiterung mit zyklischer Galoisgruppe. Sei p eine Primzahl und $n \in \mathbb{N}$ mit $[E:K] = p^n$. Sei F ein Zwischenkörper von $E|K$ mit $[F:K] = p^{n-1}$. Beweisen Sie, dass für jedes $\alpha \in E \setminus F$ jeweils $E = K(\alpha)$ gilt.

Sei $G = \mathrm{Gal}(E|K)$. Da $E|K$ endlich und galoisch ist, gilt $|G| = [E:K] = p^n$, d.h. G ist eine zyklische Gruppe der Ordnung p^n.

Sei
gilt (
somit $|G$

Sei nun
Sei $V=$
ist $E=$
$V = Ga$
Es genügt
Aus $\alpha \notin F$
theorie fo

...e

... mit

... Sei p

... mit

... Zwischen-

$:K] = p^{n-1}$.

...des $\alpha \in E \setminus F$

$E|K$ endlich und

$:K] = p^n$, d.h. G

Ordnung p^n.

Sei $U = \mathrm{Gal}(E|F)$. Laut Galoistheorie gilt $(G:U) = [F:K] = p^{n-1}$ und somit $|U| = \dfrac{|G|}{(G:U)} = \dfrac{p^n}{p^{n-1}} = p$.

Sei nun $\alpha \in E \setminus F$. z.zg.: $E = K(\alpha)$

Sei $V = \mathrm{Gal}(E|K(\alpha))$. Laut Galoistheorie ist $E = K(\alpha)$ äquivalent zu

$$V = \mathrm{Gal}(E|K(\alpha)) = \mathrm{Gal}(E|E) = \{id_E\}.$$

Es genügt also $V = \{id_E\}$ zu zeigen.

Aus $\alpha \notin F$ folgt $K(\alpha) \supsetneq F$. Laut Galoistheorie folgt daraus $V \subsetneq U$.

$\ell \iff$

$^n - 1$

$\zeta \in \mathbb{C}^*$

-inheits-

-wurzeln

-ten Einheits-

$\mathrm{ggT}(k,n) = 1\}$

Weil G eine zyklische Gruppe der Ordnung p^n ist, existiert für $0 \le k \le n$ jeweils eine eindeutig bestimmte Untergruppe U_k von G mit $|U_k| = p^k$. Für $j, k \in \{0, \dots, n\}$ gilt dabei jeweils $U_j \subseteq U_k \iff |U_j| \mid |U_k|$ $\iff p^j \mid p^k \iff j \le k$. s.o. $\Rightarrow$ $|U| = p \Rightarrow U = U_1$. Sei $k \in \{0, \dots, n\}$ mit $V = U_k$. $V \not\supseteq U \rightarrow U_k \not\supseteq U_1 \overset{s.o.}{\Longrightarrow}$ $\neg(1 \le k) \iff k < 1 \Rightarrow k = 0 \Rightarrow V = U_0 = \{id_E\}$. $\square$

s Polynom

$\prod (x-\zeta)$

$\zeta\in\mu_n^*$

genannt.

lle $n\in\mathbb{N}$.

ist in $\mathbb{Z}[x]$ und

grad $\Phi_n = \varphi(n)$

$|\mu_n^*| = \varphi(n)$).

$= \prod_{d|n} \Phi_d$.

Kreisteilungspolynome

Def. Sei $n\in\mathbb{N}$.

$\zeta\in\mathbb{C}^\times$ ist n-te Einheitswurzel $\iff$

$\zeta^n=1 \iff \zeta$ ~~ist~~ Nullst. von x^n-1

Für $n\geq 2$ werden die Elemente $\zeta\in\mathbb{C}^\times$ mit $\mathrm{ord}(\zeta)=n$ primitive n-te Einheitswurzeln genannt.

Notation:

μ_n = Menge der n-ten Einheitswurzeln

$= \{e^{2\pi i k/n} \mid 0\le k<n\}$

μ_n^* = Teilmenge der primitiven n-ten Einheitswurzeln $= \{e^{2\pi i k/n} \mid 0\le k<n,\ \mathrm{ggT}(k,n)=1\}$

Weil

ist, d

denti

mit |

dabei

$\iff$

$|U| =$

$V = U$

$\neg(1\le k$

$U_0 = \{$

Def: Für alle $n \geq 2$ wird das Polynom $\Phi_n \in \mathbb{C}[x]$ geg. durch $\Phi_n = \prod_{\zeta \in \mu_n^*} (x - \zeta)$ das <u>n-te Kreisteilungspolynom</u> genannt.

Konvention: $\Phi_1 = x - 1$

Eigenschaften:

(i) Es gilt $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$.

(ii) Jedes Kreisteilungspolynom ist in $\mathbb{Z}[x]$ und in $\mathbb{Q}[x]$ <u>irreduzibel.</u>

(iii) Für jedes $n \in \mathbb{N}$ gilt $\operatorname{grad} \Phi_n = \varphi(n)$ (und im Fall $n \geq 2$ auch $|\mu_n^*| = \varphi(n)$).

(iv) Für jedes $n \in \mathbb{N}$ gilt $x^n - 1 = \prod_{d \mid n} \Phi_d$.

Beispiele:

(i) Für jede Primzahl p gilt

$$x^p - 1 = \Phi_1 \Phi_p = (x-1)\cdot \Phi_p \Longrightarrow$$

$$\Phi_p = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

(ii) $x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6 \Longrightarrow$

$$\Phi_6 = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{x^6-1}{(x-1)\,\Phi_2\,\frac{x^3-1}{x-1}} =$$

$$\frac{x^6-1}{\Phi_2(x^3-1)} = \frac{(x^3)^2-1}{\Phi_2\,(x^3-1)} = \frac{x^3+1}{\Phi_2}$$

$$= \frac{x^3+1}{x+1} \underset{\text{Pol-div}}{=} x^2 - x + 1$$

von $x^n - 1$

Nullstelle

μ_A ein Teiler

$A^n = E$.

$.4, 6\}$ gilt

te Kreisteilungs-

(Φ_d = d-tes Kreis-

die Teiler von n).

F22T1A1

Sei A eine (2×2)-Matrix über $\mathbb{Q}$ und $n \in \mathbb{N}$ mit $A^n = E$, wobei E die Einheitsmatrix bezeichnet. Es sei $\mu_A \in \mathbb{Q}[x]$ das Minimalpolynom von A.

(a) Zeigen Sie, dass $\operatorname{grad}(\mu_A) \leq 2$ gilt.

Laut VL. ist μ_A ein Teiler des char. Polynoms χ_A, es gilt somit $\operatorname{grad}(\mu_A) \leq \operatorname{grad}(\chi_A)$. Für jede $n\times n$-Matrix B über einem Körper K gilt $\operatorname{grad}\chi_B = n$. Insgesamt gilt also $\operatorname{grad}(\mu_A) \leq \operatorname{grad}(\chi_A) = 2$.

Beis

(i)

$x^p -$

$\Phi_p =$

(ii)

Φ

$\frac{x^6 - 1}{\Phi_2(x^3 \ldots}$

$= \frac{x^3 + \ldots}{x + \ldots}$

(b) Zeigen Sie, dass μ_A ein Teiler von $x^n - 1$ in $\mathbb{Q}[x]$ ist.

Wegen $A^n - E = 0$ ist A eine Nullstelle von $x^n - 1$. Daraus folgt, dass μ_A ein Teiler dieses Polynoms ist.

(c) Sei nun $n \in \mathbb{N}$ <u>minimal</u> mit $A^n = E$. Zeigen Sie, dass $n \in \{1, 2, 3, 4, 6\}$ gilt. (Hinweis: Betrachten Sie geeignete Kreisteilungspolynome.)

Laut Vl. gilt $x^n - 1 = \prod_{d \mid n} \Phi_d$ (Φ_d = d-tes Kreisteilungspolynom, $d \in \mathbb{N}$ durchläuft die Teiler von n).

)}

Φ_6]

mit.

wird

1).

$n=2$

Teil (b) $\Rightarrow \exists\, g \in \mathbb{Q}[x]$ mit $x^n - 1 = g\,\mu_A$.

$\Rightarrow g\,\mu_A = x^n - 1 = \prod_{d \mid n} \Phi_d$ Da jedes Φ_d lt. Vl. in $\mathbb{Q}[x]$ irreduzibel ist, ist μ_A also ein Produkt von einigen dieser Φ_d (mit $d \mid n$).

Teil (a) $\Rightarrow$ grad$(\mu_A) \leq 2 \Rightarrow \mu_A$ ist entweder gleich einem Kreisteilungspolynom vom Grad 2 oder Produkt von einem oder zwei Kreisteilungspolynomen vom Grad 1.

Allgemein gilt: $m \in \mathbb{N}$, $m = \prod_{i=1}^{r} p_i^{e_i}$ Primfaktorzerlegung von m, mit $p_1, \dots, p_r$ prim, $e_1, \dots, e_r \in \mathbb{N} \Rightarrow$

$$\varphi(m) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$$ also: $\varphi(m) \leq 2 \Rightarrow p_i \leq 3\ \forall i$

$\Rightarrow m = 2^a 3^b$ mit $a, b \in \mathbb{N}_0$

$\varphi(m) = 2^{a-1} \cdot 2 \cdot 3^{b-1}$ falls $a, b \geq 1$ $\Rightarrow$

$(a,b) \in \{(0,0), (0,1), (1,0), (1,1), (2,0)\}$

$\Rightarrow m \in \{1, 2, 3, 6, 4\}$

$\Rightarrow \mu_A \in \{\Phi_1, \Phi_2, \Phi_1\Phi_2, \Phi_3, \Phi_4, \Phi_6\}$

Für jedes $n \in \mathbb{N}$ gilt jeweils die Äquiv.
$A^n = E \Leftrightarrow \mu_A \mid (x^n - 1)$. Gesucht wird also das kleinste $n \in \mathbb{N}$ mit $\mu_A \mid (x^n - 1)$.

1. Fall: $\mu_A = \Phi_1 = x - 1 \Rightarrow n = 1$

2. Fall: $\mu_A = \Phi_2$ oder $\mu_A = \underbrace{\Phi_1 \Phi_2}_{= x^2 - 1} \Rightarrow n = 2$

Tei

$\Rightarrow$

Lt. V

Produ

Teil (

gleich

Produk

Allgemei

von m.

$\varphi(m)$

3. Fall: $\mu_A = \Phi_3 = x^2 + x + 1$
Dieses Polynom ist kein Teiler von $x - 1$ oder $x^2 - 1$, aber von $x^3 - 1$. Also ist $n = 3$.

4. Fall: $\mu_A = \Phi_4 = x^2 + 1$
Dieses Polynom ist kein Teiler von $x^k - 1$ für $k \in \{1, 2, 3\}$, aber von $x^4 - 1$. Also ist $n = 4$.

5. Fall: $\mu_A = \Phi_6 = x^2 - x + 1$
Dieses Polynom ist kein Teiler von $x^k - 1$ für $k \leq 5$, weil die Nullstellen von Φ_6 primitive sechste Einheitswurzeln, die Nullstellen der Polynome $x^k - 1$ aber Einheitswurzeln von Ordnung ≤ 5 sind. Jede primitive 6-te Einheitswurzel ist aber eine Nullstelle von $x^6 - 1$, deshalb ist Φ_6 Teiler von $x^6 - 1$ und somit $n = 6$.