H20T2A5 (Forts.)

geg: Körper K mit $\mathrm{char}(K) = 0$, p Primzahl

Voraussetzung: Für jede endliche Erweiterung $L \supsetneq K$ ist p ein Teiler von $[L:K]$.

zu zeigen: Für jede endl. Erw. $L|K$ ist der Erweiterungsgrad $[L:K]$ eine p-Potenz.

Sei $L|K$ eine endl. Erweiterung.

bereits gezeigt: Es gibt eine Galois-Erw.

$E|K$ mit $E \supseteq L$. Sei $G = \mathrm{Gal}(E|K)$.
Sei P eine p-Sylowgruppe von G und
$M = E^P$ der zugehörige Fixkörper. Dies
ist ein Zwischenkörper von $E|K$.

Ang. $[L:K]$ ist keine p-Potenz. Dann gibt eine
Primzahl $q \neq p$ mit $q \mid [L:K]$.
L Zwischenkörper von $E|K$, Gradformel
$\Rightarrow [E:K] = [E:L] \cdot [L:K] \Rightarrow |G|$
$= [E:K]$ ist Vielfaches von $[L:K]$.

Aus $q \mid [L:K]$ folgt also $q \mid |G|$.

Schreibe $|G| = p^r m$ mit $r \in \mathbb{N}_0$ und $m \in \mathbb{N}$, wobei $p \nmid m$ ist. Wegen $q \mid |G|$ und $q \nmid p^r$ folgt $q \mid m$.

Weil P eine p-Sylowgruppe von G ist, gilt $|P| = p^r$ und $(G:P) = \frac{|G|}{|P|} = \frac{p^r m}{p^r} = m$.

Laut Galoistheorie gilt $[M:K] = [E^P:K] = (G:P) = m \Rightarrow q \mid [M:K] \Rightarrow [M:K] > 1 \Rightarrow M \neq K$ Auf Grund der Voraussetzung

an den Körper K müsste [M : K] ein Vielfaches von p sein. Aber dies ist wegen p ∤ m nicht der Fall ↯ also: [L : K] muss eine p-Potenz sein. □

Übungen zu H21T1A5: F21T2A4, F17T2A5

Übungen zu H20T2A5: H12T2A4, H14T1A1

F15T3A5 Sei E|K eine Galois-Erw. mit zyklischer Galoisgruppe G. Es sei [E : K] = p^n, wobei p eine Primzahl und n ≥ 1 ist. Sei F ein Zwischenkörper von E|K mit

$[F:K] = p^{n-1}$. Zeigen Sie, dass für alle $\alpha \in E \setminus F$ jeweils $E = K(\alpha)$ gilt.

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

Seien $U, V \leq G$ die Untergruppen von G definiert durch $U = \mathrm{Gal}(E|F)$ und $V = \mathrm{Gal}(E|K(\alpha))$. Laut Galoistheorie gilt $(G:U) = [F:K] = p^{n-1} \Rightarrow |U| = \frac{|G|}{(G:U)} = \frac{p^n}{p^{n-1}} = p$

$\alpha \in E \setminus F \Rightarrow K(\alpha) \nsubseteq F$ Laut Ga-

alle $x \in E \setminus F$ genau dann $E = K(x)$ gilt.

Galoistheorie folgt daraus $\mathrm{Gal}(E|K(x)) \not\supseteq \mathrm{Gal}(E|F)$, also $V \not\supseteq U$. Die Gleichung $E = K(x)$ ist laut Galoistheorie äquivalent zu $\{id_E\} = V$.

Aus den Voraussetzungen ergibt sich also:
G ist zyklisch von Ordnung p^n, U, V sind Untergruppen mit $|U| = p$ und $V \not\supseteq U$, und zu zeigen ist $V = \{id_E\}$.

Weil G zyklisch von Ordnung p^n ist, und die einzigen Teiler von p^n durch p^m mit $0 \leq m \leq n$ sind, besitzt G

H1

Sei

der

imed

p-te

f mi

(a) Z

f i

[Skiz

$0 \leq k \leq$

stellen

f über

für jedes $m \in \{0, 1, \ldots, n\}$ genau eine Untergruppe U_m mit $|U_m| = p^m$, und keine weiteren. Außerdem gilt für alle $l, m \in \{0, \ldots, n\}$ jeweils die Äquivalenz $l \leq m \Leftrightarrow U_l \subseteq U_m$.

$|U| = p \Rightarrow U = U_1$ Außerdem gibt es ein $m \in \{0, \ldots, n\}$ mit $V = U_m$.

$V \not\subseteq U \Rightarrow U_m \not\subseteq U_1 \Rightarrow \neg(m \geq 1)$

$\Rightarrow m = 0 \Rightarrow V = \{\mathrm{id}_E\}$ □

K(α) gilt.

(E|K(α))

Die

Galoistheorie

h also:

U, V sind

p und V ⊄ U,

ung p^n ist,

p^n durch p^m

besitzt G

H15T3A4

Sei p eine ungerade Primzahl, $a \in \mathbb{Q}$ mit der Eigenschaft, dass $f = x^p - a$ in $\mathbb{Q}[x]$ irreduzibel ist. Sei $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel, $\alpha \in \mathbb{C}$ eine Nullstelle von f und $L = \mathbb{Q}(\alpha, \zeta)$.

(a) Zeigen Sie, dass L Zerfällungskörper von f über $\mathbb{Q}$ ist und $[L : \mathbb{Q}] = p(p-1)$ gilt.

[Skizze: Überprüfe, dass durch $\zeta^k \alpha$ mit $0 \le k \le p-1$ p verschiedene komplexe Nullstellen von f gegeben sind. Daraus folgt, dass f über $\mathbb{Q}(\zeta, \alpha)$ in Linearfaktoren zerfällt.

Außerdem bilden die Nullstellen ein Erzeugendensystem von $\mathbb{Q}(\alpha, S)$, denn mit $\alpha, S\alpha$ liegt auch $S = \frac{S\alpha}{\alpha}$ in dem Erz.-körper, der von den Nullstellen des Polynoms f erzeugt wird. Für den Nachweis von $[L:\mathbb{Q}] = p(p-1)$ nutzt man die Teilerfremdheit von p und $p-1$ aus.]

(6) Zeigen Sie, dass $G = \mathrm{Gal}(L|\mathbb{Q})$ eine normale p-Sylowgruppe N besitzt, und dass $G/N \cong (\mathbb{Z}/p\mathbb{Z})^\times$ gilt. (normale Untergr. = Normalteiler)

(b) Zeigen Sie, dass $G = \mathrm{Gal}(L|\mathbb{Q})$ eine normale p-Sylowuntergruppe N besitzt und dass G/N

Sei ν_p die Anzahl der p-Sylowgruppen von G.
z.Zg.: $\nu_p = 1$ Daraus folgt dann, dass die einzige p-Sylowgruppe ein Normalteiler ist, auf Grund des 2. Sylowsatzes. Es ist $|G| = p \cdot (p-1)$ und $p \nmid (p-1)$
3. Sylowsatz $\Rightarrow \nu_p \mid (p-1)$, insb. $\nu_p < p$
Außerdem gilt $\nu_p \equiv 1 \bmod p$. Aus $p \equiv 1 \bmod p$ und $\nu_p < p$ folgt $\nu_p = 1$.
Sei $N = \mathrm{Gal}(L|\mathbb{Q}(\zeta))$. Laut Vl $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p) = p-1$. Laut Galoistheorie folgt $(G:N) = p-1$ und $|N| = \frac{|G|}{(G:N)} = \frac{p(p-1)}{p-1} = p$

Also ist N die einzige p-Sylowgruppe von G.
Laut Galoistheorie gilt allgemein: Ist $K|\mathbb{Q}$ eine galois'sche Teilerweiterung von $L|\mathbb{Q}$, dann gilt $G/\mathrm{Gal}(L|K) \cong \mathrm{Gal}(K|\mathbb{Q})$. Weil $N = \mathrm{Gal}(L|\mathbb{Q}(\zeta))$ ein Normalteiler von G ist, ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ (lt. Galoisth.) eine galois'sche Teilerweiterung von $L|\mathbb{Q}$, gilt also $G/N \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Lt. Vl. gilt für die Kreisteilungserweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ außerdem $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

$G/N \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Lt. Vl. gilt für die Kreisteilungserweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ außerdem $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$

(c) Geben Sie einen Isomorphismus $\mathrm{Gal}(L|\mathbb{Q}(\alpha)) \to (\mathbb{Z}/p\mathbb{Z})^\times$ an.

Für jedes $\sigma \in \mathrm{Gal}(L|\mathbb{Q}(\alpha))$ ist $\sigma|_{\mathbb{Q}(\zeta)} : \mathbb{Q}(\zeta) \to L$ ein $\mathbb{Q}$-Hom. Weil $\mathbb{Q}(\zeta)|\mathbb{Q}$ galois'sch und damit normal ist, ist $\sigma|_{\mathbb{Q}(\alpha)}$ ein $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\zeta)$, also ein Element von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$.

Betrachte nun die Abb. $\phi : \mathrm{Gal}(L|\mathbb{Q}(\alpha)) \to \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ gegeben durch $\sigma \mapsto \sigma|_{\mathbb{Q}(\zeta)}$. Für bel. $\sigma, \tau \in \mathrm{Gal}(L|\mathbb{Q}(\alpha))$ gilt $(\sigma \circ \tau)|_{\mathbb{Q}(\zeta)} = (\sigma|_{\mathbb{Q}(\zeta)}) \circ (\tau|_{\mathbb{Q}(\zeta)})$, also ist ϕ ein Gruppenhom. Beh: $\ker(\phi) = \{\mathrm{id}_L\}$

Sei $\sigma \in \ker(\phi)$. $\sigma \in Gal(L|\mathbb{Q}(\alpha))$

$\Rightarrow \sigma(\alpha) = \alpha$ $\sigma \in \ker(\phi) \Rightarrow \phi(\sigma)$

$= id_{\mathbb{Q}(\beta)} \Rightarrow \sigma|_{\mathbb{Q}(\beta)} = id_{\mathbb{Q}(\beta)} \Rightarrow$

$\sigma(\beta) = \beta$ $L = \mathbb{Q}(\alpha, \beta)$, $\sigma(\alpha) = \alpha$, $\sigma(\beta)$

$= \beta \Rightarrow \sigma = id_L$ ($\Rightarrow$ Beh.)

Der Homomorphiesatz liefert einen

Isom. $Gal(L|\mathbb{Q}(\alpha))/_{\ker(\phi)} \cong im(\phi)$

$\ker(\phi) = \{id_L\} \Rightarrow |im(\phi)| =$

$$\frac{|Gal(L|\mathbb{Q}(\alpha))|}{|\ker(\phi)|} = |Gal(L|\mathbb{Q}(\alpha))| =$$

$[L:\mathbb{Q}(\alpha)]$ Aus Teil (a) ist $[\mathbb{Q}(\alpha):\mathbb{Q}]$

gesam

(d) Zei

gr

[Ansat

zwei ver

$L|\mathbb{Q}$ u

theorie

Untergr

$p-1$. Of

U bzw. V

weil $2+p$

$= p$ bekannt. Gradformel $\Rightarrow [L : \mathbb{Q}(\alpha)]$

$$= \frac{[L:\mathbb{Q}]}{[\mathbb{Q}(\alpha):\mathbb{Q}]} = \frac{p(p-1)}{r} = p-1 \Rightarrow$$

$|\mathrm{im}(\phi)| = p-1 = [\mathbb{Q}(\zeta):\mathbb{Q}] = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$

$\Rightarrow \mathrm{im}(\phi) \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ $\mathrm{im}(\phi) = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$

Insgesamt ist durch ϕ also ein Isomorphismus $\mathrm{Gal}(L|\mathbb{Q}(\alpha)) \to \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ gegeben. Durch Komposition mit dem Isomorphismus $\chi: \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ aus der Vorlesung, der für jedes $a \in \mathbb{Z}\setminus p\mathbb{Z}$ das Element $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ geg. durch $\sigma_a(\zeta) = \zeta^a$ abbildet, erhalten wir ins-

gesamt einen Isom. $\mathrm{Gal}(L|\mathbb{Q}(\alpha)) \to (\mathbb{Z}/p\mathbb{Z})^\times$

(d) Zeigen Sie, dass G mehr als eine 2-Sylowgruppe besitzt.

[Ansatz: Durch $\mathbb{Q}(\alpha)|\mathbb{Q}$ und $\mathbb{Q}(\gamma\alpha)|\mathbb{Q}$ sind zwei verschiedene Teilerweiterungen von $L|\mathbb{Q}$ vom Grad p gegeben. Laut Galoistheorie entsprechen diese zwei verschiedenen Untergruppen U, V von G von Ordnung $p-1$. Offenbar ist jede 2-Sylowgruppe von U bzw. V auch 2-Sylowgruppe von G, weil $2 \nmid p$. Betrachte in U, V nun eine

Untergruppen U V von G von Ordnung

$\mathbb{Q}(\alpha)]$

$\Rightarrow$

$(S|\mathbb{Q})$

$\mathbb{Q})$

morphismus

en. Durch

us

us der

$p\mathbb{Z}$ das

g durch

en wir uns-

2-Sylowgruppe U_1 bzw. V_1. Dann muss noch $U_1 \neq V_1$ gezeigt werden. Ist α so gewählt, dass α in $\mathbb{R}$ liegt, dann kann U_1 so gewählt werden, dass das Elt. σ ges. durch komplexe Konjugation in U_1 liegt, während $\sigma \notin V_1$ gilt.]