von L/K. Dann sind die Abbildungen

Übung zu F25T3A4 : H24T3A5

F23T3A5 Sei $\zeta = \zeta_7 = e^{2\pi i/7}$, $a = \zeta + \zeta^{-1}$ und $b = \zeta + \zeta^2 + \zeta^4$.

(a) Geben Sie einen konkreten Isom. $\phi : (\mathbb{Z}/7\mathbb{Z})^\times \to G$ an, wobei $G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ ist.

Laut Vorlesung existiert für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,7) = 1$ ein eindeutig bestimmtes Element $\sigma_a \in G$ mit $\sigma_a(\zeta) = \zeta^a$, und durch $\phi : (\mathbb{Z}/7\mathbb{Z})^\times \to G$, $a + 7\mathbb{Z} \mapsto \sigma_a$ ist eine wohldefinierte Abb. und ein Gruppenisom. definiert.

in (b) gezeigt: Das Element a hat ein Minimalpolynom vom Grad 3, und das Minimalpolynom von f ist vom Grad 2.

Hauptsatz der Galoistheorie:

Sei $L|K$ eine endl. Galois-Erw. und $G = \mathrm{Gal}(L|K)$. Sei $\mathcal{U}$ die Menge der Untergruppen von G und $\mathcal{Z}$ die Menge der Zwischenkörper von $L|K$. Dann sind die Abbildungen

$$\phi: \mathcal{U} \to \mathcal{Z},\ U \mapsto L^U = \{x \in L \mid \sigma(x) = x\ \forall \sigma \in U\}$$

(ii)

(iii)

(iv)

und $\Psi: \mathcal{Z} \to \mathcal{U},\ M \mapsto \mathrm{Gal}(L|M)$ zueinander inverse Bijektionen. Außerdem gilt

(i) Antitonie: $\forall U, V \in \mathcal{U}: U \subseteq V \iff L^U \supseteq L^V$

$\forall F, M \in \mathcal{Z}: F \subseteq M \iff \mathrm{Gal}(L|F) \supseteq \mathrm{Gal}(L|M)$

(ii) $L^{\{\mathrm{id}_L\}} = L,\ L^G = K,\ \mathrm{Gal}(L|K) = G,\ \mathrm{Gal}(L|L) = \{\mathrm{id}_L\}$

(iii) Erweiterungsgrad und Untergruppe:
Ist $U \in \mathcal{U}$ und $M = L^U$, dann gilt
$[L:M] = |U|$ und $[M:K] = (G:U)$.

(iv) Normalteiler: Sei $U \in \mathcal{U}$ und $M = L^U$.

ist $U \leq G$ und $M = L^U$, dann gilt
$[L:M] = |U|$ und $[M:K] = (G:U)$.

Dann gilt die Äquivalenz

$U \trianglelefteq G \iff M|K$ ist normal $\iff M|K$ ist galois'sch

Sind diese Aussagen erfüllt, dann gilt $G/U \cong \mathrm{Gal}(M|K)$.

F25 T3 A4 (c) Zeigen Sie, dass $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galois'sche Erweiterungen sind, und bestimmen Sie den Isomorphietyp der Galoisgruppen.

Nach Teil (a) gilt $G \leq (\mathbb{Z}/7\mathbb{Z})^\times$, also ist G abelsch, und somit ist jede Untergruppe von G ein Normalteiler. Wegen $a, b \in \mathbb{Q}(\zeta)$ sind $\mathbb{Q}(a)$ und $\mathbb{Q}(b)$ Zwischenkörper von $\mathbb{Q}(\zeta)|\mathbb{Q}$, und somit sind

$U = \mathrm{Gal}(\mathbb{Q}(\zeta_5) \mid \mathbb{Q}(a))$ und $V = \mathrm{Gal}(\mathbb{Q}(\zeta_5) \mid \mathbb{Q}(b))$

Untergruppen von G, also auch (wie gerade bemerkt) Normalteiler. Laut Galoistheorie folgt daraus, dass $\mathbb{Q}(a) \mid \mathbb{Q}$ und $\mathbb{Q}(b) \mid \mathbb{Q}$ Galois-Erweiterungen sind. Außerdem folgt aus der Galoistheorie, dass $G/U \cong \mathrm{Gal}(\mathbb{Q}(a) \mid \mathbb{Q})$ und $G/V \cong \mathrm{Gal}(\mathbb{Q}(b) \mid \mathbb{Q})$ gilt. Weil 7 eine Primzahl ist, ist $(\mathbb{Z}/7\mathbb{Z})^\times$ zyklisch von Ordnung $7-1=6$, also gilt dasselbe für G.

Jede Faktorgruppe einer zyklischen Gruppe G ist zyklisch. (denn: Sei G eine Gruppe und $g \in G$ mit $G = \langle g \rangle$. Sei $N \trianglelefteq G$ und $\bar{h} \in G/N$. Dann gilt $\bar{h} = hN$ für ein $h \in G$. $G = \langle g \rangle \Rightarrow \exists a \in \mathbb{Z}$ mit $h = g^a$
$\Rightarrow \bar{h} = hN = g^a N = (gN)^a \Rightarrow h \in \langle gN \rangle$.
Also gilt $G/N = \langle gN \rangle$.) $\Rightarrow$ G/U und G/V sind zyklische Gruppen, also ebenso $\mathrm{Gal}(\mathbb{Q}(a)|\mathbb{Q})$ und $\mathrm{Gal}(\mathbb{Q}(b)|\mathbb{Q})$. außerdem:
$|\mathrm{Gal}(\mathbb{Q}(a)|\mathbb{Q})| = [\mathbb{Q}(a):\mathbb{Q}] = \mathrm{grad}\, m_{a,\mathbb{Q}}$
$\overset{(6)}{=} 3$ Da die Galoisgruppe zyklisch ist.

)(5)|Q(6))

lösa

kant

Q(a)|Q

gen sind.

ne, dass

al(Q(6)|Q)

, ist

7-1=6,

ist sie also isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Ebenso folgt aus $\text{grad}\, M_{6,\mathbb{Q}} = 2$, dass $\text{Gal}(\mathbb{Q}(6)|\mathbb{Q})$ isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist. □

F2ST1A5 Sei $f = x^{15} - 7 \in \mathbb{Q}[x]$ und L ein Zerfällungskörper von f über $\mathbb{Q}$.

in (a) gezeigt: $L = \mathbb{Q}(\alpha, \zeta)$, wobei $\alpha, \zeta \in L$ Elemente mit $\alpha^{15} = 7$ und $\text{ord}(\zeta) = 15$ in $L^\times$ sind

außerdem: $[L:\mathbb{Q}] = 120$

(b) Zeigen Sie, dass in $\text{Gal}(L|\mathbb{Q})$ ein Normalteiler der Ordnung 15 existiert.

Es genügt zu zeigen, dass in $L|\mathbb{Q}$ eine normale Teilerweiterung $M|\mathbb{Q}$ mit $[M:\mathbb{Q}] = 8$ existiert. Setzen wir nämlich $U = \mathrm{Gal}(L|M)$, dann folgt aus der Galois-theorie $U \trianglelefteq G$ für $G = \mathrm{Gal}(L|\mathbb{Q})$ (weil $M|\mathbb{Q}$ normal ist); und außerdem $|U| = \frac{|G|}{(G:U)} = \frac{[L:\mathbb{Q}]}{[M:\mathbb{Q}]} = \frac{120}{8} = 15$.

Sei $M = \mathbb{Q}(\zeta)$. Aus Teil (b) ist bereits $[M:\mathbb{Q}] = \varphi(15) = 8$ bekannt.

Außerdem ist die Erweiterung $M|\mathbb{Q}$ normal. Dafür reicht es zu überprüfen, dass M Zerfällungskörper des 15-ten Kreisteilungspolynoms

Φ_{15} ist. Die Nullstellen von Φ_{15} in L sind genau die Elemente in L^* von Ordnung 15.
Wegen $\operatorname{ord}(S) = 15$ ist $\langle S \rangle$ eine zykl. Untergruppe der Ordn. 15 mit $\langle S \rangle \subseteq M$.
Weil jede solche Gruppe genau $\varphi(15) = 8$ Elemente der Ordn. 15 enthält gibt es in M mind. 8 Elemente mit multiplikativer Ordnung 15. $\Rightarrow$ Φ_{15} hat in M mind. 8 Nullst.
$\underline{\text{grad}\,\Phi_{15} = 8}$ $\Rightarrow$ Φ_{15} zerfällt über M in Linearfaktoren

Weil jede solche Gruppe genau $\varphi(15) = 8$

Elemente der Ordnung 15 enthält, gibt es

Außerdem wird M über $\mathbb{Q}$ von den Nullstellen von Φ_{15} über $\mathbb{Q}$ erzeugt, weil $M = \mathbb{Q}(\zeta)$ ist, und ζ eine Nullstelle von Φ_{15}. Also ist M insgesamt der Zerfällungskörper von Φ_{15} über $\mathbb{Q}$.

□

damit wegen $\mathrm{char}\,\mathbb{Q} = 0$ auch separabel.

Eine Rechnung ergibt, dass f in $\mathbb{R}$ die Ver-

F24T1A5 Sei $\alpha = \sqrt{10 - 5\sqrt{2}} \in \mathbb{R}$.

(a) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}$.

$\alpha = \sqrt{10 - 5\sqrt{2}} \Rightarrow \alpha^2 = 10 - 5\sqrt{2} \Rightarrow \alpha^2 - 10 = -5\sqrt{2}$

$\Rightarrow (\alpha^2 - 10)^2 = 50 \Rightarrow \alpha^4 - 20\alpha^2 + 100 = 50$

$\Rightarrow \alpha^4 - 20\alpha^2 + 50 = 0 \Rightarrow \alpha$ ist Nullstelle von $f = x^4 - 20x^2 + 50$

Wegen $2 \mid (-20), 2 \mid 50, 2^2 \nmid 50$ ist f nach dem Eisenstein-Kriterium irreduzibel, außerdem normiert.

Insgesamt gilt also $f = \mathrm{Mx}_{\cdot,\mathbb{Q}}$.

(b) Zeigen Sie, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine Galois-Erweiterung ist.

Wegen $f(\alpha) = 0$ und $f \neq 0$ ist α algebraisch über $\mathbb{Q}$.
Damit ist die Erweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}$ algebraisch, und damit wegen $\operatorname{char}\mathbb{Q} = 0$ auch separabel.

Eine Rechnung ergibt, dass f in $\mathbb{R}$ die verschiedenen Nullstellen $\pm\alpha, \pm\beta$ besitzt, mit $\beta = \sqrt{10+5\sqrt{2}}$.

$$\alpha\beta = \sqrt{10-5\sqrt{2}} \cdot \sqrt{10+5\sqrt{2}} = \sqrt{(10-5\sqrt{2})(10+5\sqrt{2})}$$

$\swarrow\ 10 \pm 5\sqrt{2} > 0$

$$= \sqrt{10^2 - (5\sqrt{2})^2} = \sqrt{100-50} = \sqrt{50} = 5\sqrt{2}$$

$\alpha \in \mathbb{Q}(\alpha) \Rightarrow \alpha^2 = 10 - 5\sqrt{2} \in \mathbb{Q}(\alpha)$

$\Rightarrow -5\sqrt{2} \in \mathbb{Q}(\alpha) \Rightarrow \beta = \frac{5\sqrt{2}}{\alpha} \in \mathbb{Q}(\alpha)$

Also besitzt f in $\mathbb{Q}(\alpha)$ die vier Null-stellen $\pm\alpha, \pm\beta$. Wegen $\operatorname{grad}(f) = 4$ zer-fällt f somit über $\mathbb{Q}(\alpha)$ in Linearfaktoren. Außerdem wird $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ durch die Null-stellen erzeugt, weil α eine dieser Nullstellen ist. Also: $\mathbb{Q}(\alpha)$ ist Zerfällungskörp. von f über $\mathbb{Q} \Rightarrow \mathbb{Q}(\alpha)/\mathbb{Q}$ ist eine normale Erweiterung, insgesamt eine Galois-Erweiterung.

(c) Zeigen Sie: $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$

Es gilt $|\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})| = [\mathbb{Q}(\alpha):\mathbb{Q}]$ $= \mathrm{grad}\, M_{\alpha,\mathbb{Q}} = \mathrm{grad}(f) = 4$. Somit genügt es zu zeigen, dass die Galoisgruppe G ein Element der Ordnung 4 besitzt. Weil f über $\mathbb{Q}$ irreduzibel ist und $\alpha, \beta \in \mathbb{Q}(\alpha)$ Nullstellen von f sind, existiert ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$.

Beh.: $\mathrm{ord}(\sigma) = 4$

Wegen $|G| = 4$ gilt jedenfalls $\sigma^4 = \mathrm{id}_{\mathbb{Q}(\alpha)}$.

Wenn wir zeigen können, dass $\sigma^2 \neq \mathrm{id}_{\mathbb{Q}(\alpha)}$

gilt, dann folgt $\mathrm{ord}(\sigma) = 4$ (da 2 einziges Primteiler von 4, und $4/2 = 2$).

Es gilt $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\beta) = \sigma\left(\frac{5\sqrt{2}}{\alpha}\right)$

$$= \frac{\sigma(5\sqrt{2})}{\sigma(\alpha)} = \frac{\sigma(5\sqrt{2})}{\beta} \overset{\text{s.o.}}{=} \frac{\sigma(10-\alpha^2)}{\beta} =$$

$$= \frac{10-\sigma(\alpha)^2}{\beta} = \frac{10-\beta^2}{\beta} = \frac{10-(10+5\sqrt{2})}{\beta} =$$

$$-\frac{5\sqrt{2}}{\beta} = -\alpha \neq \alpha \Rightarrow \sigma^2 \neq \mathrm{id}_{\mathbb{Q}(\alpha)}$$

$\uparrow \alpha\beta = 5\sqrt{2}$

Also gilt tatsächlich $\mathrm{ord}(\sigma) = 4$. □

Übung: F23T1A3