Algebra

Übungsblatt 9

Prof. Dr. Markus Land
Dr. Maksim Zhykhovich

WiSe 2022/2023
19.12.2022

Aufgabe 1. Sei L/K eine Galoiserweiterung mit $\mathrm{Gal}(L/K) \simeq S_n$.
Zeige: Es gibt genau einen Zwischenkörper $K \subset E \subset L$ mit $|E : K| = 2$ und E/K ist Galois.

Aufgabe 2. Sei p eine Primzahl, $a \in \mathbb{Q} \setminus \mathbb{Q}^{*p}$ und L ein Zerfällungskörper des Polynoms $X^p - a$ über $\mathbb{Q}$. Zeige:
(1) Die Menge $\mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$ ausgestattet mit der Verknüpfung $(m, k)\cdot(m', k') := (m + km', kk')$ ist eine Gruppe, geschrieben $\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$.
(2) Die Galois Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ ist isomorph zu $\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$.
Hinweis: Benutze Aufgabe 3, Übungsblatt 7.

Aufgabe 3. Seien K ein Körper mit $\operatorname{char} K \neq 2$ und $f \in K[X]$ ein separables Polynom vom Grad $n \geq 1$ mit Nullstellen $\alpha_1, \ldots, \alpha_n$ in einem algebraischen Abschluss $\bar{K}$ von K. Wie immer fassen wir G als Untergruppe von S_n auf. Die Diskriminante von f ist wie folgt gegeben: $\mathrm{disc}(f) = \prod_{i<j}(\alpha_j - \alpha_i)^2$ in $\bar{K}$.
Zeige:
(1) $\mathrm{disc}(f) \in K$.
(2) G ist eine Untergruppe von A_n genau dann wenn $\mathrm{disc}(f)$ ein Quadrat in K ist.
Hinweis: Betrachte die Wirkung der Galoisgruppe auf $\prod_{i<j}(\alpha_j - \alpha_i)$.

Aufgabe 4. Berechne die Galoisgruppen der Zerfällungskörper folgender Polynome über $\mathbb{Q}$:
a) $X^3 - 4X + 2$
b) $X^3 - 3X + 1$
Hinweis: Benutze Aufgabe 3 und die Formel $\mathrm{disc}(X^3 + aX + b) = -4a^3 - 27b^2$.

Aufgabe 5. Sei p eine Primzahl, $n \geq 1$ und φ die Eulersche φ-Funktion. Zeige:
(1) $\varphi(p^n) = p^{n-1}(p - 1)$, und
(2) $n = \sum\limits_{d|n, d\geq 1} \varphi(d)$.

Übungsblatt 9
(Galoiskorrespondenz)

Aufgabe 1 Nach Satz 4.6 gibt es eine Bijektion

$$\left\{ \begin{array}{l} K \subset E \subset L \\ \text{mit } [E:K]=2 \end{array} \right\} \xleftrightarrow{\text{Bijektion}} \left\{ \begin{array}{l} \text{Untergruppen } H \subset Gal(L/K) \simeq S_n \\ \text{mit Index} = 2 \end{array} \right\}$$

$A_n \subseteq S_n$ ist eine solche UG

Dann ist es genug zu zeigen, dass A_n die einzige UG von S_n mit Index $= 2$ ist.

Bmk 1 G Gruppe, $H \leq G$ UG mit Index $= 2$. Dann $H \trianglelefteq G$.

Bmk 2 Seien τ, τ' zwei Transpositionen in S_n.
Dann $\exists \sigma \in S_n$ mit $\tau' = \sigma \tau \sigma^{-1}$.

~~Ang~~ Sei $H \subset S_n$ mit Index $= 2$. Zu zeigen: $H = A_n$.

Nach Bmk 1 : H ist eine normale UG, $H \trianglelefteq G$.

Dann $\pi : G \longrightarrow G/H \simeq \{\pm 1\}$

Gruppe mit 2 Elemente $\simeq \mathbb{Z}/2$

Nach Bmk 2 haben wir:

$$(*) \quad \pi(\tau') = \pi(\sigma \tau \sigma^{-1}) = \pi(\sigma)\,\pi(\tau)\,\pi(\sigma)^{-1} = \pi(\sigma)\,\pi(\sigma)^{-1}\,\pi(\tau) = \pi(\tau)$$

G/H ist abelsch, da $G/H \simeq \mathbb{Z}/2$.

Falls $\pi(\tau) = 1$, dann nach $(*)$ $\pi($~~beliebige~~ jede Transposition$) = 1$
Dann liegen alle Transposition in $H \Rightarrow H = S_n$ (Widerspruch)

Wir haben $\pi($jede Transposition$) = -1$

Dann $\pi($Produkt der geraden Anzahl der Transp.$) = 1 \Rightarrow A_n \subseteq H \Rightarrow$

$\Rightarrow A_n = H$

Aufgabe 2

(1) • $(m,k)\cdot(0,1) = (m,k) = (0,1)\cdot(m,k)$

$(0,1)$ ist das neutrale Element

• $(m,k)\cdot \underbrace{(-k^{-1}m, k^{-1})}_{\text{Invese}} = (0,1)$

Assoziativität

• $\big((m,k)(m',k')\big)\cdot(m'',k'') = (m+km', kk')(m'',k'')$

$$= (m+km'+kk'm'', kk'k'')$$

$$= (m,k)\big((m',k')\cdot(m'',k'')\big)$$

(2) Nach Aufgabe 3 (Üblatt 7)

$L = \mathbb{Q}(\sqrt[p]{a}, \xi_p) \subset \mathbb{C}$ ist der ZK von $X^p - a$ über $\mathbb{Q}$.

~~$X^p - 1$ hat~~

$X^{p-1} + \dots + X + 1$ hat die NS $\xi_p, \xi_p^2, \dots, \xi_p^{p-1}$ in L.

$X^p - a$ hat die NS $\sqrt[p]{a}, \sqrt[p]{a}\,\xi_p, \dots, \sqrt[p]{a}\,\xi_p^{p-1}$ in L

Sei $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, dann $\sigma(\xi_p) = \xi_p^{k_\sigma}$

$\sigma(\sqrt[p]{a}) = \sqrt[p]{a}\,\xi_p^{m_\sigma}$

$$\varphi : \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$$
$$\sigma \longmapsto (m_\sigma, k_\sigma)$$

ist ein injektiven Gruppen hom.

$(\tau\circ\sigma)(\xi_p) = \tau(\sigma(\xi_p)) = \tau(\xi_p)^{k_\sigma} = (\xi_p^{k_\tau})^{k_\sigma} = \xi_p^{k_\tau \cdot k_\sigma}$

$(\tau\circ\sigma)(\sqrt[p]{a}) = \cancel{\tau(\sigma(\sqrt[p]{a})\sigma(\xi_p))} = \tau(\sqrt[p]{a}\,\xi_p^{m_\sigma}) =$

$= \tau(\sqrt[p]{a})\,\tau(\xi_p)^{m_\sigma} = \sqrt[p]{a}\,\xi_p^{m_\tau}\,\xi_p^{k_\tau m_\sigma} = \sqrt[p]{a}\,\xi_p^{m_\tau + k_\tau m_\sigma}$

$$\left|\mathbb{Z}/p\mathbb{Z} \rtimes \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}\right| = p(p-1) \underset{\substack{\uparrow \\ \text{Aufgabe 3.2 (Übungsblatt 7)}}}{=} \left|\mathrm{Gal}(L/\mathbb{Q})\right|$$

Es folgt: $\varphi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^{\times}$ ist ein Gruppenisomorphismus.

Aufgabe 3

$L = K(\alpha_1, \dots, \alpha_n) \subset \overline{K}$ der ZK von f über K.

(1) Zu zeigen: $\operatorname{disc}(f) \in K = L^G = \{ x \in L \mid \sigma(x) = x \ \forall \sigma \in G = Gal(L/K) \}$.

Sei $\sigma \in Gal(L/K) = G$

Dann $\sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_n\}$ und wir bezeichnen $\sigma(\alpha_i)$ als $\alpha_{\sigma(i)}$, wobei σ eine Permutation $\in S_n$

$$\sigma(\operatorname{disc} f) = \sigma\left(\prod_{i<j} (\alpha_j - \alpha_i)^2 \right) = \underset{\substack{\uparrow}}{\prod_{i<j} (\alpha_{\sigma(j)} - \alpha_{\sigma(i)})^2} = \operatorname{disc}(f)$$

σ permutiert die Faktoren $(\alpha_j - \alpha_i)^2$ aber der Produkt ändert nicht

Es folgt: $\operatorname{disc} f \in L^G = K$

(2) Sei $\delta = \prod_{i<j} (\alpha_j - \alpha_i) \in L$ ($\delta \neq 0$, da f separabel ist)

Sei $\sigma \in Gal(L/K)$

$$\sigma(\delta) = \prod_{i<j} (\sigma(\alpha_j) - \sigma(\alpha_i)) = \prod_{i<j} (\alpha_{\sigma(j)} - \alpha_{\sigma(i)}) =$$

$$= \underbrace{\operatorname{sign}(\sigma)}_{= (-1)^{\text{Anzahl der Inversionen}}} \prod_{i<j} (\alpha_i - \alpha_j) = \operatorname{sign}(\sigma)\, \delta$$

$\left(\sigma \in A_n \iff \operatorname{sign}(\sigma) = 1 \overset{\delta \neq -\delta, \text{ da Char } K \neq 2}{\iff} \sigma(\delta) = \delta \right)$

$\forall \sigma \in Gal(L/K),\ \sigma \in A_n \iff \forall \sigma \in Gal(L/K),\ \sigma(\delta) = \delta \iff$

$\iff \delta \in L^G = K \underset{\operatorname{disc} f = \delta^2}{\iff} \operatorname{disc} f$ ist ein Quadrat in K

Aufgabe 4

Das Polynom f aus a) oder b) ist irreduzibel $/\mathbb{Q}$

Sei $L \subset \mathbb{C}$ der ZK von $f/\mathbb{Q}$.

$$\mathbb{Q} \underset{3}{\subset} \mathbb{Q}(\alpha) \subseteq L$$, wobei α eine NS von f in L

$$\mathrm{Gal}(L/\mathbb{Q}) \leq S_3$$

und $|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] \geq 3$

Es folgt: $\mathrm{Gal}(L/\mathbb{Q}) = A_3$

oder

$\mathrm{Gal}(L/\mathbb{Q}) = S_3$

Nach Aufgabe 3: $\mathrm{Gal}(L/\mathbb{Q}) = A_3 \iff \mathrm{disc}\, f$ ist ein Quadrat in $\mathbb{Q}$.

a) $\mathrm{disc}\, f = -4(-4)^3 - 27 \cdot 4 = 4 \cdot (64-27) = 4 \cdot 37$ kein Quadrat in $\mathbb{Q}$

$\Rightarrow \mathrm{Gal}(L/\mathbb{Q}) = S_3$.

b) $\mathrm{disc}\, f = -4(-3)^3 - 27 \cdot 1 = 4 \cdot 27 - 27 = 3 \cdot 27 = 9^2$

$\Rightarrow \mathrm{Gal}(L/\mathbb{Q}) = A_3$

Aufgabe 5

$n \in \mathbb{N}$

$\varphi(n) = \{ 1 \le m \le n \mid g.g.T(m,n) = 1 \}$

(1) $n = p^k$, p Primzahl

$g.g.T(m, p^k) = 1 \iff p \nmid m$

$g.g.T(m, p^k) \ne 1 \iff p \mid m$

$$\varphi(p^k) = p^k - \{ 1 \le m \le p^k \mid g.g.T(m,p^k) \ne 1 \} =$$
$$= p^k - \{ 1 \le m \le p^k \mid p \mid m \} = p^k - p^{k-1} = p^{k-1}(p-1)$$

(2) $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$, wobei p_i verschiedene Primzahle sind und $k_i \in \mathbb{N}_0$

$d \mid n \iff d = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$ mit $l_i \le k_i$

Dann $$\sum_{d\mid n} d = (1 + p_1 + p_1^2 + \ldots + p_1^{k_1}) \cdot \ldots \cdot (1 + p_r + \ldots + p_r^{k_r})$$

nach der Multiplikation $\sum_{0 \le l_i \le k_i} p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$

Genau so $$\sum_{d \mid n} \varphi(d) \overset{\text{Lemma 4.14a}}{=} \underbrace{(1 + \varphi(p_1) + \ldots + \varphi(p_1^{k_1}))}_{\text{nach (1)}} \cdot \ldots \cdot (1 + \varphi(p_r) + \ldots + \varphi(p_r^{k_r}))$$

$$1 + (p_1 - 1) + (p_1 - 1)p_1 + \ldots + (p_1 - 1)p_1^{k_1 - 1} =$$

$$= 1 + (p_1 - 1)(1 + p_1 + \ldots + p_1^{k_1 - 1}) =$$

$$= 1 + (p_1 - 1)\frac{p_1^{k_1} - 1}{p_1 - 1} = p_1^{k_1}$$

$$= p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} = n$$