Musterlösung Serie 20

GALOISGRUPPEN

---

108. Sei K ein Körper mit $\mathrm{char}(K) = p$ für eine Primzahl p.

Zeige: Ein irreduzibles Polynom $f \in K[X]$ ist genau dann inseparabel über K, wenn gilt $f = \sum_{i=0}^{n} a_i X^{ip}$.

Lösung: ($\Leftarrow$): Ist f von dieser Form, so ist

$$Df = p \cdot a_1 X^{p-1} + 2p \cdot a_2 X^{2p-1} \ldots + np \cdot a_n X^{np-1},$$

und weil $\mathrm{char}(K) = p$ ist $Df = 0$. Somit ist f inseparabel.

($\Rightarrow$): Mit Kontraposition. Ist $f = \sum_{i=0}^{n} a_i X^{n_i}$ nicht von dieser Form, so existiert ein j mit $1 \leqslant j \leqslant n$ sodass $a_j \neq 0$ und $p \nmid n_j$. Dann ist $Df \neq 0$, und weil f irreduzibel ist und $\deg(Df) < \deg(f)$, existiert kein gemeinsamer Faktor von Df und f. Somit ist f separabel.

109. Sei $L : K$ eine algebraische Körpererweiterung und sei $A \subseteq L$ mit $L = K(A)$.

Formalisiere und beweise folgende Aussage: *Jedes Element der Galoisgruppe von $L : K$ ist durch die Bilder von A vollständig bestimmt.*

Lösung: Seien $\varphi, \psi \colon L \to L$ zwei Elemente der Galoisgruppe, sodass gilt $\varphi|_A = \psi|_A$. Dann ist $\varphi = \psi$.

Beweis: Die Menge $\{b \in L : \varphi(b) = \psi(b)\}$ ist ein Zwischenkörper der Erweiterung $L : K$, der A enthält, denn offensichtlich ist die Menge abgeschlossen unter Addition, Subtraktion, Multiplikation und Division. Da L aber der kleinste Körper ist, der K und A enthält, folgt $\{b \in L : \varphi(b) = \psi(b)\} = L$. Somit stimmen φ und ψ auf ganz L überein und sind folglich gleich.

Bemerkung: In diesem Beweis haben wir weder gebraucht, dass $L : K$ algebraisch ist, noch irgendeine Aussage über den Bildbereich von φ oder ψ.

110. Berechne die Galoisgruppen folgender Körpererweiterungen.

(a) $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$

(c) $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$

Lösung: Wegen Aufgabe;109 ist jedes Element von $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q})$ durch $\sigma|_{\{\alpha\}}$ vollständig bestimmt.

(a) Sei $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$. Nach Korollar 19.3 ist $\sigma(\sqrt{2})$ zu $\sqrt{2}$ konjugiert, also gleich $\pm\sqrt{2}$. Nach Satz 14.4.(b) sind beide Fälle möglich. Beachte, dass $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ ist.

Somit hat $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ genau zwei Elemente und es gilt $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \cong C_2$.

(b) Sei $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$. Nach Korollar 19.3 ist $\sigma(\sqrt[3]{2})$ zu $\sqrt[3]{2}$ konjugiert, also gleich $\sqrt[3]{2}$, denn dies ist die einzige Nullstelle von $X^3 - 2$, die auch in $\mathbb{Q}(\sqrt[3]{2})$ liegt.

Also ist $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ die triviale Gruppe.

(c) Sei $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$. Nach Korollar 19.3 ist $\sigma(\sqrt[4]{2})$ zu $\sqrt[4]{2}$ konjugiert, also gleich $\pm\sqrt[4]{2}$, denn dies ist die einzigen Nullstellen von $X^4 - 2$, die auch in $\mathbb{Q}(\sqrt[4]{2})$ liegen. Nach Satz 14.4.(b) sind beide Fälle möglich. Beachte, dass $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(-\sqrt[4]{2})$ ist.

Somit hat $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$ genau zwei Elemente und es gilt $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}) \cong C_2$.

111. Sei L_f der Zerfällungskörper von $f \in K[X]$.

Zeige: Ist $\deg(f) = n$, so gilt $|\mathrm{Gal}(f)| \mid n!$.

Lösung: Seien $a_1, \ldots, a_n$ die Nullstellen von f und sei $S(a_1, \ldots, a_n)$ die Symmetriegruppe von $\{a_1, \ldots, a_n\}$, d.h. die Gruppe aller Permutationen von $a_1, \ldots, a_n$.

Weil nach Definition $\mathrm{Gal}(f) = \mathrm{Gal}(L_f : K)$, ist mit Satz 19.4 $\mathrm{Gal}(f)$ isomorph zu einer Untergruppe von $S(a_1, \ldots, a_n)$.

Weil nun $S(a_1, \ldots, a_n)$ isomorph ist zu einer Untegruppe von S_n (beachte, dass nicht alle a_i's verschieden sein müssen), folgt, dass $\mathrm{Gal}(f)$ isomorph ist zu einer Untergruppe von S_n. Mit $|S_n| = n!$ und dem Satz von Lagrange erhalten wir $|\mathrm{Gal}(f)| \mid n!$.