

Musterlösung Serie 22

GALOISGRUPPEN

- 110.** Sei $L : K$ eine algebraische Körpererweiterung und sei $A \subseteq L$ eine Untermenge mit $L = K(A)$. Formalisieren und beweisen Sie folgende Aufgabe: *Jedes Element der Galoisgruppe von $L : K$ ist durch seine Wirkung auf die Elemente in A vollständig bestimmt.*

Lösung: Seien $\varphi, \psi : L \rightarrow L$ zwei Elemente der Galoisgruppe mit $\varphi|_A = \psi|_A$. 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 .

- 111.** Sei L_f der Zerfällungskörper von einem Polynom $f \in K[X]$ vom Grad n . Beweisen Sie die Teilungsrelation $|\text{Gal}(f)| \mid n!$.

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

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

Weil nun $S(a_1, \dots, a_n)$ isomorph ist zu einer Untergruppe von S_n , folgt, dass $\text{Gal}(f)$ isomorph ist zu einer Untergruppe von S_n . Mit $|S_n| = n!$ und dem Satz von Lagrange erhalten wir $|\text{Gal}(f)| \mid n!$.

- 112.** Sei K ein Körper mit positiver Charakteristik p . Wir betrachten das Polynom

$$P = X^p - X - a \in K[X]$$

mit $a \in K$. Sei L ein Zerfällungskörper von P über K und $\alpha \in L$ eine Nullstelle von P .

- (a) Beweisen Sie die Gleichung

$$P = \prod_{x \in \mathbb{F}_p} (X - (\alpha + x)).$$

Schliessen Sie daraus, dass P separabel ist.

- (b) Sei $\sigma \in \text{Gal}(P)$. Beweisen Sie $\sigma(\alpha) - \alpha \in \mathbb{F}_p$.

- (c) Beweisen Sie, dass die Abbildung

$$\Phi: \text{Gal}(P) \rightarrow \mathbb{F}_p, \sigma \mapsto \sigma(\alpha) - \alpha$$

ein injektiver Gruppenhomomorphismus ist.

- (d) Beweisen Sie, dass P irreduzibel ist, dann und nur dann falls Φ ein Isomorphismus ist.
 (e) Beweisen Sie, dass P reduzibel ist, dann und nur dann falls ein $g \in K$ mit $g^p - g = a$ existiert.

Lösung:

- (a) Sei $x \in \mathbb{F}_p$. Dann gilt $x^p = x$, also haben wir die Gleichung

$$\begin{aligned} P(\alpha + x) &= (\alpha + x)^p - (\alpha + x) - a \\ &= \alpha^p + x^p - \alpha - x - a \\ &= (\alpha^p - \alpha - a) + x^p - x = P(\alpha) = 0. \end{aligned}$$

Also ist $\alpha + x$ auch eine Nullstelle von P . Somit gilt $(X - (\alpha + x)) | P$.

Da die Polynome $(X - (\alpha + x))$ für verschiedene $x \in \mathbb{F}_p$ teilerfremd sind, folgt nun

$$P = \prod_{x \in \mathbb{F}_p} (X - (\alpha + x)).$$

Die obige Gleichung impliziert, dass jede Nullstelle von P einfach ist. Insbesondere hat jeder irreduzible Faktor von P einfache Nullstellen, also ist P separabel.

- (b) Es gilt

$$P(\sigma(\alpha)) = \sigma(P(\alpha)) = 0.$$

Also folgt aus Aufgabe (a) $\sigma(\alpha) - \alpha \in \mathbb{F}_p$.

- (c) Seien $\sigma, \sigma' \in \text{Gal}(P)$. Es gilt $\sigma'(z) = z$ für alle $z \in K$, insbesondere gilt $\sigma'(x) = x$ für alle $x \in \mathbb{F}_p$. Also folgt

$$\Phi(\sigma) = \sigma'(\Phi(\sigma)) = \sigma'(\sigma(\alpha)) - \sigma'(\alpha).$$

Dies impliziert

$$\Phi(\sigma'\sigma) = \sigma'(\sigma(\alpha)) - \alpha = \sigma'(\sigma(\alpha)) - \sigma'(\alpha) + \sigma'(\alpha) - \alpha = \Phi(\sigma) + \Phi(\sigma').$$

Seien $\sigma, \sigma' \in \text{Gal}(P)$ mit $\Phi(\sigma) = \Phi(\sigma')$. Aufgabe (a) impliziert $L = K(\alpha)$. Wir erhalten

$$\sigma(\alpha) = \alpha + \Phi(\sigma) = \alpha + \Phi(\sigma') = \sigma'(\alpha).$$

Also folgt $\sigma = \sigma'$ aus Aufgabe 110.

- (d) Wir nehmen an, die Abbildung Φ ist ein Isomorphismus. Die Separabilität von P impliziert $[L : K] = |\text{Gal}(P)| = p$. Wir haben $L = K(\alpha)$, also hat das Minimalpolynom von α über K Grad p . Da das Minimalpolynom das Polynom P teilt, folgt dass P das Minimalpolynom ist. Also ist es irreduzibel über K .

Wir nehmen an P ist irreduzibel. Das Minimalpolynom von $\alpha \in L$ teilt P , also ist es P . Insbesondere gilt $[L : K] \geq p$. Weil P separabel ist, folgt $|\text{Gal}(P)| \geq p$. Also ist Φ ein Isomorphismus, denn Φ ist injektiv.

- (e) Wir nehmen an P ist reduzibel. Dann ist die Abbildung Φ kein Isomorphismus, also ist die Galois-Gruppe von P trivial, denn die Abbildung Φ identifiziert die Galois-Gruppe von P mit einer echten Untergruppe von $\mathbb{F}_p$. Die einzige solche Gruppe ist jedoch die triviale Gruppe. Da P separabel ist, hat der Zerfallungskörper $L : K$ Grad 1. Also liegt eine Nullstelle von P in K .

Falls eine Nullstelle von P in K liegt, dann kann P nicht irreduzibel sein.

- 113.** Sei $n \geq 1$ und K ein Körper. Wir nehmen an, es existiert eine primitive n -te Einheitswurzel $\zeta_n \in K$, das heisst $\zeta_n^n = 1$ und $\zeta_n^m \neq 1$ für alle $1 \leq m < n$. Wir betrachten das Polynom

$$P = X^n - a \in K[X]$$

mit $a \in K$. Sei L ein Zerfallungskörper von P über K und $\alpha \in L$ eine Nullstelle von P . Wir definieren die abelsche Gruppe der n -ten Einheitswurzeln

$$\mu_n := \{x \in K : x^n = 1\},$$

wobei die Gruppenoperation die Multiplikation ist.

- (a) Beweisen Sie, dass der Gruppenhomomorphismus

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \mu_n, a \mapsto \zeta_n^a$$

ein Gruppenisomorphismus ist. Wieso ist diese Abbildung nicht natürlich?

- (b) Beweisen Sie die Gleichung

$$P = \prod_{\xi \in \mu_n} (X - \xi \alpha).$$

Schliessen Sie daraus, dass P separabel ist.

- (c) Sei $\sigma \in \text{Gal}(P)$. Beweisen Sie $\frac{\sigma(\alpha)}{\alpha} \in \mu_n$.

- (d) Beweisen Sie, dass die Abbildung

$$\Phi: \text{Gal}(P) \rightarrow \mu_n, \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

ein injektiver Gruppenhomomorphismus ist.

- (e) Beweisen Sie, dass diese Abbildung ein Isomorphismus ist, dann und nur dann falls P irreduzibel ist.

Lösung:

- (a) Wir nehmen an, der Homomorphismus ist nicht injektiv. Dann ist der Kern dieser Abbildung nichttrivial, also existiert ein $m \in \mathbb{Z}/n\mathbb{Z}$ mit $m \neq 0$ und $\zeta_n^m = 1$. Somit ist ζ_n keine primitive n -te Einheitswurzel und wir erhalten einen Widerspruch. Jedes Element $\xi \in \mu_n$ ist eine Nullstelle des Polynoms $X^n - 1$. Da dieses Polynom höchstens n Nullstellen hat, folgt

$$|\mu_n| \leq n.$$

Also ist der Homomorphismus eine Bijektion, denn er ist bereits injektiv.

Dieser Isomorphismus ist nicht natürlich, weil in seiner Konstruktion eine Wahl einer primitiven n -ten Einheitswurzel getroffen wurde. Man könnte diesen Isomorphismus mit einer beliebigen anderen n -ten Einheitswurzel konstruieren.

(b) Für jedes $\xi \in \mu_n$ gilt

$$(\xi\alpha)^n = \xi^n \alpha^n = \alpha^n = a.$$

Also sind die Elemente $\xi\alpha$ Nullstellen des Polynoms P . Aus Aufgabe (a) folgt, dass dies n verschiedene Elemente sind. Es folgt

$$P = \prod_{\xi \in \mu_n} (X - \xi\alpha).$$

Die Nullstellen von P sind einfach, also sind die Nullstellen der irreduziblen Faktoren von P einfach. Also ist P separabel.

(c) Es gilt

$$P(\sigma(\alpha)) = 0,$$

also folgt die Behauptung aus Aufgabe (b).

(d) Seien $\sigma, \sigma' \in \text{Gal}(P)$. Dann gilt $\sigma(\xi) = \xi$ für alle $\xi \in \mu_n$, also folgt

$$\Phi(\sigma) = \sigma'(\Phi(\sigma)) = \frac{\sigma'(\sigma(\alpha))}{\sigma'(\alpha)}.$$

Dies impliziert

$$\Phi(\sigma'\sigma) = \frac{\sigma(\sigma'(\alpha))}{\alpha} = \frac{\sigma'(\sigma(\alpha))}{\sigma'(\alpha)} \frac{\sigma'(\alpha)}{\alpha} = \Phi(\sigma)\Phi(\sigma').$$

Aus Aufgabe (a) folgt $L = K(\alpha)$. Wie in Aufgabe 112 (c) kann man nun schliessen, dass die Abbildung Φ injektiv ist.

(e) Wir nehmen an, die Abbildung Φ ist ein Isomorphismus. Das Polynom P ist separabel, also hat die Erweiterung $K(\alpha) : K$ Grad n , denn $L = K(\alpha)$. Also hat das Minimalpolynom von α über K Grad n . Somit ist P irreduzibel.

Wir nehmen nun an, das Polynom P ist irreduzibel. Das Minimalpolynom von $\alpha \in L$ teilt P , also ist es P . Insbesondere folgt $[L : K] \geq n$. Da P separabel ist, folgt $|\text{Gal}(P)| \geq n$. Die Abbildung Φ ist also ein Isomorphismus, da sie injektiv ist.

114. Sei K ein Körper mit positiver Charakteristik p . Wir betrachten ein irreduzibles Polynom $P = X^p - a \in K[X]$. Bestimmen Sie die Galois-Gruppe $\text{Gal}(P)$.

Lösung: Wir betrachten die Erweiterung $L := K[X]/(P)$ von K . Sei $a^{1/p} := \overline{X} \in L$, dann gilt

$$X^p - a = (X - a^{1/p})^p.$$

Sei $L' : K$ ein Zerfallungskörper von P und $\alpha \in L'$ eine Nullstelle von P . Dann ist P das Minimalpolynom von α über K , denn P ist irreduzibel. Also folgt $p \mid [L' : K]$. Die Erweiterung $L : K$ ist eine Erweiterung von Grad p , in welcher P zerfällt, also folgt die Ungleichung $[L' : K] \leq p$. Somit gilt $[L' : K] = p$, also ist $L : K$ ein Zerfallungskörper von P über K .

Sei $\sigma : L \rightarrow L$ ein K -Automorphismus von L . Wir haben $P(\sigma(a^{1/p})) = 0$, also folgt $\sigma(a^{1/p}) = a^{1/p}$. Da die Erweiterung $L : K$ durch $a^{1/p}$ generiert wird, folgt $\sigma = \text{id}$. Also ist die Galois-Gruppe von P trivial.