Algebra I

Musterlösung 18

Galoisgruppen

105. Sei $L : K$ eine algebraische Körpererweiterung und sei $A \subset L$ 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 für alle $a \in A$ gilt $\varphi(a) = \psi(a)$. Dann folgt $\varphi = \psi$.

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.

106. 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 105 ist jedes Element von $\mathrm{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q})$ durch α 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 sind beide Fälle möglich. Beachte, dass $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ ist.

Also hat $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ genau zwei Elemente, ist also isomorph zu C_2.

(b) Sei $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$. Nach Korollar 19.3 ist $\sigma(\sqrt{2})$ zu $\sqrt{2}$ 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 sind beide Fälle möglich. Beachte, dass $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(-\sqrt[4]{2})$ ist. Also hat $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$ genau zwei Elemente, ist also isomorph zu C_2.

107. Für welche Werte von k ist die Körpererweiterung $\mathbb{F}_7(X)/\mathbb{F}_7(X^k)$

(a) separabel?

(b) normal?

(c) beides, d.h. galoissch?

Lösung: (a) Eine Körpererweiterung ist genau dann separabel, wenn sie von separablen Elementen erzeugt wird. Das Minimalpolynom von X über $\mathbb{F}_7(X^k)$ ist $T^k - X^k$, da X^k ein Primelement in $\mathbb{F}_7[X^k]$ ist und wir Eisenstein mit $p = X^k$ auf $T^k - X^k$ anwenden können. Dieses genau dann ist separabel, wenn seine Ableitung nicht verschwindet, also genau dann, wenn k nicht durch 7 teilbar ist.

(b) Die Körpererweiterung ist normal genau dann, wenn alle Nullstellen von $T^k - X^k$ in einem algebraischen Abschluss L von $\mathbb{F}_7(X)$ schon in $\mathbb{F}_7(X)$ liegen. Das ist genau dann der Fall, wenn $\mathbb{F}_7(X)$ alle k-ten Einheitswurzeln von L enthält.

Schreibe $k = \ell \cdot 7^n$ mit $7 \nmid \ell$. Dann gilt $X^k - 1 = (X^\ell - 1)^{7^n}$ über $\mathbb{F}_7$, also ist jede k-te Einheitswurzel in L schon eine ℓ-te Einheitswurzel. Dagegen ist $X^\ell - 1$ separabel über $\mathbb{F}_7$, und die Gruppe der ℓ-ten Einheitswurzeln von L ist zyklisch der Ordnung ℓ nach Aufgabe 95.

Jede Einheitswurzel in $\mathbb{F}_7(X)$ ist algebraisch über $\mathbb{F}_7$. Allerdings ist jedes Element von $\mathbb{F}_7(X) \setminus \mathbb{F}_7$ transzendent. Somit sind die Einheitswurzeln von $\mathbb{F}_7(X)$ gleich denen in $\mathbb{F}_7$. Diese bilden die zyklische Gruppe $\mathbb{F}_7^\times$ der Ordnung 6.

Insgesamt enthält also $\mathbb{F}_7(X)$ alle k-ten Einheitswurzeln von L genau dann, wenn $\mathbb{F}_7$ alle ℓ-ten Einheitswurzeln von L enthält. Dies ist genau dann der Fall, wenn ℓ ein Teiler von 6 ist, also für

$$k \in \{7^n, 2 \cdot 7^n, 3 \cdot 7^n, 6 \cdot 7^n : n \geq 0\}.$$

(c) Die Erweiterung ist genau dann normal und separabel, wenn $k \in \{1, 2, 3, 6\}$ ist.

108. Ist L der Zerfällungskörper von $g \in K[X]$, so heisst $\mathrm{Gal}(L : K)$ die *Galoisgruppe von* g, bezeichnet mit $\mathrm{Gal}(g)$.

Zeige: Ist $g \in K[X]$ mit $\mathrm{grad}(g) = n$, so ist $\mathrm{Gal}(g)$ isomorph zu einer Untergruppe von S_n. Insbesondere gilt $|\mathrm{Gal}(g)| \mid n!$.

Lösung: Nach Korollar 19.3 ist das Bild jeder Nullstelle von g wieder eine Nullstelle von g. Seien $a_1, \ldots, a_n$ die Nullstellen von g. Dann ist die Abbildung $\Phi\colon\ \mathrm{Gal}(g) \to S(a_1, \ldots, a_n)$ mit $\Phi(\sigma) = \sigma|_{\{a_1,\ldots,a_n\}}$ ein Gruppenhomomorphismus. Nach Aufgabe 105 ist jedes Element der Galoisgruppe eindeutig durch das Bild jeder Nullstelle bestimmt. Daher ist Φ injektiv. Somit ist $\mathrm{Gal}(g)$ isomorph zu einer Untergruppe von $S(a_1, \ldots, a_n)$. Offensichtlich ist $S(a_1, \ldots, a_n) \cong S_n$. Nach dem Satz von Lagrange gilt somit $|\mathrm{Gal}(g)| \mid n!$.

109. Sei L der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$.

Berechne $\mathrm{Gal}(L : \mathbb{Q})$.

Lösung: Nach Aufgabe 108 gilt $\mathrm{Gal}(L : \mathbb{Q}) \leq S_3$. Seien a_1, a_2 Nullstellen von $X^3 - 2$. Nach Satz 14.4 existiert ein Homomorphismus $\mathbb{Q}(a_1) \to \mathbb{Q}(a_2)$, der a_1 auf a_2 abbildet. Nach Satz 17.5 können wir diesen zu einem Isomorphismus $L \to L$ erweitern. Somit können wir je zwei Nullstellen von $X^3 - 2$ durch Elemente der Galoisgruppe aufeinander abbilden. Ausserdem ist die komplexe Konjugation in $\mathrm{Gal}(L : \mathbb{Q})$, das heisst $\mathrm{Gal}(L : \mathbb{Q})$ hat ein Element der Ordnung 2. Daraus folgt, dass $\mathrm{Gal}(L : \mathbb{Q}) \cong S_3$ ist; zum Beispiel indem wir überprüfen, dass S_3 von einer Transposition und einem beliebigen anderen nichttrivialen Element erzeugt wird.