Übungsaufgaben „Algebra I“

Serie 12 zum 7.7.04

1. Wir betrachten die algebraischen Körpererweiterungen $K[\alpha]$ und $K[\beta]$ und bezeichnen mit f bzw. g die Minimalpolynome von α bzw. β aus dem Polynomring $K[X]$.

   Beweisen Sie: Ist $f = g$, so existiert genau ein K-Isomorphismus $\sigma : K[\alpha] \to K[\beta]$, mit $\sigma(\alpha) = \beta$.

2. Es sei $K' \supseteq K$ eine Körpererweiterung und $M \subseteq K'$ eine Teilmenge. Beweisen Sie: Der Durchschnitt aller Zwischenkörper $\tilde{K}$ mit $K \subseteq \tilde{K} \subseteq K'$ und $M \subseteq \tilde{K}$ ist ein Körper.

   Hinweis. Dies wurde ohne Beweis bereits in der Vorlesung erwähnt. Wir bezeichnen den so erhaltenen Körper mit $K(M)$ und nennen ihn den durch die Menge M erzeugten Körper.

3. Bestimmen Sie alle Unterkörper der komplexen Zahlen, die über dem Primkörper durch die folgende Menge M erzeugt werden. Entscheiden Sie, in welchem Fall eine algebraische Erweiterung vorliegt und geben Sie dann den Erweiterungsgrad an.

   (1) $M = \{0, 1, 2\}$

   (2) $M = \{0\}$

   (3) $M = \{\sqrt{2}\}$

   (4) $M = \{\sqrt{2}, \sqrt{3}\}$

   (5) $M = \{3, i\}$

   (6) $M = \mathbb{R}$

   Lösung. In den Fällen (1) - (4) ist $K = \mathbb{Q}(M)$ eine algebraische Erweiterung des Primkörpers $\mathbb{Q}$, und zwar vom Grad 0, 0, 2, 4 bzw. 2. Unter (5) liegt keine algebraische Erweiterung vor (die Menge der über $\mathbb{Q}$ algebraischen komplexen Zahlen ist abzählbar, kann also nicht $\mathbb{R}$ enthalten).

   Wir zeigen (4): Zunächst ist $f = X^4 - 10X^2 + 1$ ein irreduzibles (warum) Polynom mit der Nullstelle $\alpha = \sqrt{2} + \sqrt{3}$. Leicht ist zu sehen, dass in $\mathbb{Q}[\alpha]$ auch $\sqrt{2}$ und $\sqrt{3}$ enthalten sind, also $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ gilt. Der Grad von α über $\mathbb{Q}$ ist 4, womit die Behauptung folgt.

4. $K' \supseteq K$ sei eine Körpererweiterung. Mit $\mathrm{Aut}_K(K')$ bezeichnen wir die Menge der Automorphismen $\sigma : K' \to K'$ mit der Eigenschaft $\sigma(x) = x$ für alle $x \in K$ (K-*Automorphismen*, vgl. Vorlesung). Beweisen Sie: $\mathrm{Aut}_K(K')$ bildet mit der Hintereinanderausführung von Abbildungen eine Gruppe (die *Automorphismengruppe* der Körpererweiterung $K' \supseteq K$).

5. K sei der Zerfällungskörper des Polynoms $f = X^3 - 2$ über $\mathbb{Q}$.

   (i) Zeigen Sie $K = \mathbb{Q}[i\sqrt[3]{2}\sqrt{3}]$ und geben Sie den Erweiterungsgrad $[K : \mathbb{Q}]$ an.

(ii) Bestimmen Sie die Automorphismengruppe $G = \mathrm{Aut}_{\mathbb{Q}}(K)$ der obigen Körpererweiterung.

(iii) Bestimmen Sie die Untergruppen von G und die zugehörigen Fixkörper. Welche dieser Körper bilden normale Erweiterungen von $\mathbb{Q}$?

Lösung. Der Erweiterungsgrad $[K : \mathbb{Q}]$ ist 6 (Erweiterung von $\mathbb{Q}[\sqrt[3]{2}]$ durch die fehlenden Nullstellen von f):
$X^3 - 2 = (X - w_1)(X - w_2)(X - w_3)$ mit $w_1 = \sqrt[3]{2},\ w_2 = uw_1, w_3 = u^2 w_1$ (wobei $u = (1/2)(-1 + i\sqrt{3})$ ist und $u^3 = 1$).
Die Galoisgruppe G der Körpererweiterung besteht daher aus 6 Automorphismen, die die Nullstellen von f permutieren. Da nur 6 Permutationen von w_1, w_2, w_3 existieren, ist S_3 isomorph zu G, und durch jede Permutation der w_i ist eindeutig ein $\mathbb{Q}$-Automorphismus bestimmt.
Für $w = i\sqrt[3]{2}\sqrt{3}$ gilt $K = \mathbb{Q}[w]$, denn $-6w/w^3 = \sqrt[3]{2} \in \mathbb{Q}[w]$.
$X^6 + 108$ ist Minimalpolynom von w, denn wegen $[K : \mathbb{Q}] = 6$ existiert kein echter Teiler mit Nullstelle w.
Es gilt sogar $K = \mathbb{Q}[w_1, w_2, w_3] = K = \mathbb{Q}[w_1, u]$, und ein Element der Galoisgruppe ist durch die Bilder von w_1 und u eindeutig bestimmt.
Beispiele für $\mathbb{Q}$-Automorphismen von K:
a) $\phi(w_1) = w_2 (= uw_1),\ \phi(u) = u$ (entspricht der Bedingung $\phi(w_2) = w_3$)
b) $\psi(w_1) = w_1,\ \psi(u) = u^2$ (entspricht der Bedingung $\psi(w_2) = w_3$)
Nun hat ϕ die Ordnung 3, ψ die Ordnung 2, und wir sehen dass ϕ, ψ eine 6-elementige Untergruppe und damit die Galoisgruppe G erzeugen.
Die nichttrivialen Untergruppen sind mit dieser Bezeichnung $(\phi),\ (\sigma),\ (\phi \cdot \sigma),\ (\phi^2 \cdot \sigma)$.
Bestimmung der Zwischenkörper: I. (ϕ) hat Index 2 und ist daher Normalteiler (entsprechend einer normalen Erweiterung von $\mathbb{Q}$, die den Grad 2 haben muß. Offenbar ist $\mathbb{Q}[u] = \mathbb{Q}[i \cdot \sqrt{3}]$ darin enthalten und vom selben Grad, daher folgt Gleichheit.
II. Die anderen drei aufgelisteten Untergruppen sind zueinander konjugiert, ihre Fixkörper daher nicht normal. Wir erhalten die verbleibenden Zwischenkörper $\mathbb{Q}[w_i]$ $(i = 1, 2, 3)$ ($i = 1$ muß jedenfalls vorkommen und entspricht einer Erweiterung vom Grad 3; von den anderen ist nur zu zeigen, daß sie nicht gleich sind – weitere nichttriviale Zwischenkörper gibt es nicht wegen der Galoiskorrespondenz).

6. K bezeichne den Körper $K := \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

(i) Zeigen Sie, dass $K \supseteq \mathbb{Q}$ eine Galoiserweiterung ist (Hinweis: K ist Zerfällungskörper eines Polynoms aus $\mathbb{Q}[X]$).

(ii) Zeigen Sie, dass $[K : \mathbb{Q}] = 4$ ist.

(iii) Bestimmen Sie die Galoisgruppe G der Erweiterung $K \supseteq \mathbb{Q}$ und geben Sie die Gruppentafel an.

(iv) Zeigen Sie, dass G kommutativ ist und beschreiben Sie diese Gruppe als direkte Summe zyklischer Gruppen von Primzahlpotenzordnung.

Lösung. K ist Zerfällungskörper des Polynoms $g = (X^2 - 2) \cdot (X^2 - 3) \in \mathbb{Q}[X]$ und daher eine Galoiserweiterung.
(ii) wurde bereits unter Aufgabe 3. (4) bewiesen.

Wir bemerken nun, dass ein $\mathbb{Q}$-Automorphismus σ von K die Eigenschaft $(\sigma(\sqrt{2}))^2 = 2$ und $(\sigma(\sqrt{3}))^2 = 3$ besitzt, es gilt also $\sigma(\sqrt{2}) = \pm\sqrt{2}$ sowie $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Daraus folgt, dass die Galoisgruppe G als Untergruppe der Permutationsgruppe S_4 durch die Permutationen aus $\{\mathrm{id}, (12), (34), (12)(34)\}$ beschrieben werden kann (Begründung?), womit die Antwort zu (iii) unmittelbar abzulesen ist.
(iv) Die unter (iii) gefundene kommutative Gruppe G besitzt genau 4 Elemente. Nach dem Klassifikationssatz für endlich erzeugte abelsche Gruppen kommen daher bis auf Isomorphie genau die Gruppen $\mathbb{Z}/(4)$ und $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ in Frage. Die erstgenannte Gruppe besitzt ein Element der Ordnung 4, was für G offenbar nicht stimmt. Wir erhalten $G \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Hinweis. Die Übungen der letzten Semesterwoche (am 14. / 15.7.04) können Sie insbesondere dazu nutzen, Ihre Fragen zum Stoff der gesamten Vorlesung zu stellen.