Musterlösung Serie 24

DER FUNDAMENTALSATZ DER ALGEBRA

---

122. In dieser Aufgabe beweisen wir den Fundamentalsatz der Algebra (der besagt, dass $\mathbb{C}$ der algebraische Abschluss von $\mathbb{R}$ ist) mit Hilfe der Galoistheorie.

Sei $L : \mathbb{R}$ eine endliche Körpererweiterung, wobei in (a) – (e) angenommen wird, dass die Körpererweiterung $L : \mathbb{R}$ *galoissch* ist.

(a) Zeige, dass ein sogenannter *Körperturm* $L = L_n : \ldots : L_0 : \mathbb{R}$ existiert, sodass $[L_0 : \mathbb{R}]$ ungerade ist und für jedes $0 \leqslant i \leqslant n-1$ die Erweiterung $L_{i+1} : L_i$ den Grad 2 hat.

(b) Zeige, dass $\mathbb{R}$ keine nichttriviale Erweiterung von ungeradem Grad hat.

(c) Zeige, dass jede Erweiterung von $\mathbb{R}$ vom Grad 2 isomorph zu $\mathbb{C}$ ist.

(d) Zeige, dass $\mathbb{C}$ keine Erweiterung vom Grad 2 hat.

(e) Folgere, dass L entweder $\mathbb{R}$ oder $\mathbb{C}$ ist.

Sei nun $L : \mathbb{R}$ eine endliche Körpererweiterung die nicht galoissch ist.

(f) Zeige, dass L entweder $\mathbb{R}$ oder $\mathbb{C}$ ist.

Lösung: (a) Sei $G := \mathrm{Gal}(L : \mathbb{R})$. Wir schreiben $|G| = 2^n m$, wobei m eine ungerade natürliche Zahl ist, also $2 \nmid m$. Ist $n = 0$, so sind wir fertig. Ist $n > 0$, so existiert mit dem Sylow-Theorem eine Untergruppe $G_0 \leqslant G$ der Ordnung $|G_0| = 2^n$. Mit dem Hauptsatz der Galoistheorie (bzw. Korollar 20.6) existiert dann ein Zwischenkörper L_0 mit $L \subseteq L_0 \subseteq L_n$, sodass gilt

$$[L_0 : \mathbb{R}] = [G : G_0] = m \quad \text{wobei } m \text{ ungerade ist.}$$

Nun betrachten wir die Gruppe G_0 der Ordnung 2^n: Mit dem Satz von Cauchy (siehe Serie 6, Aufgabe 41) existiert ein $g_{n-1} \in G_0$ mit $\mathrm{ord}(g_{n-1}) = 2$. Sei $L_{n-1} := L^{\langle g_{n-1} \rangle}$ der Fixkörper bzgl. der Gruppe $\langle g_{n-1} \rangle \leqslant G_0$. Dann ist $[G_0 : \mathrm{Gal}(L : L_{n-1}] = 2$, d.h. $\mathrm{Gal}(L : L_{n-1})$ ist ein Normalteiler von $\mathrm{Gal}(L : L_0)$ und mit Korollar 20.9 ist die Körpererweiterung $L_{n-1} : L_0$ galoissch. Für $G_1 := \mathrm{Gal}(L_{n-1} : L_0)$ gilt $|G_1| = [L_{n-1} : L_0] = 2^{n-1}$. Ist $n - 1 = 0$, so sind wir fertig. Andernfalls betrachten wir die Gruppe G_1 der Ordnung 2^{n-1} und fahren fort wie oben, bis im i-ten Schritt $n - i = 0$ ist.

(b) Wir nehmen an, dass $[L : \mathbb{R}]$ ungerade ist. Sei $\alpha \in L$ beliebig und sei $f \in \mathbb{R}[X]$ das Minimalpolynom von α über $\mathbb{R}$. Dann ist $\deg(f) = [\mathbb{R}(\alpha) : \mathbb{R}]$, und weil $[\mathbb{R}(\alpha) : \mathbb{R}]$ ein Teiler ist von $[L : \mathbb{R}]$, muss also auch $\deg(f)$ ungerade sein. Nun hat aber jedes Polynom $f \in \mathbb{R}[X]$ von ungeradem Grad eine reelle Nullstelle. Sei $\beta \in \mathbb{R}$ eine reelle Nullstelle von f. Weil nun $(X - \beta)$ ein Teiler von f ist und f, als Minimalpolynom von α über $\mathbb{R}$, irreduzibel über $\mathbb{R}$ ist, muss gelten $f(X) = X - \beta$. Somit gilt $\alpha = \beta \in \mathbb{R}$, und weil $\alpha \in L$ beliebig war, ist $L = \mathbb{R}$ mit $[L : \mathbb{R}] = 1$.

(c) Ist $[L : \mathbb{R}] = 2$, dann ist $L = \mathbb{R}(\alpha)$ für ein Element $\alpha \in L \backslash \mathbb{R}$. Ist $X^2 + rX + s \in \mathbb{R}[X]$ das Minimalpolynom von α über $\mathbb{R}$, so ist $X^2 - (\frac{r^2}{4} - s)$ das Minimalpolynom von $\beta := \alpha + \frac{r}{2}$ und es ist $\mathbb{R}(\alpha) = \mathbb{R}(\beta)$. Damit ist $\beta^2 \in \mathbb{R}$ und das Minimalpolynom von β über $\mathbb{R}$ ist $f = X^2 - \beta^2$. Weil f irreduzibel ist über $\mathbb{R}$, muss gelten $\beta^2 < 0$, denn sonst wären $\pm\sqrt{\beta} \in \mathbb{R}$. Sei nun $\gamma := \sqrt{-\beta^2}$. Dann ist $\gamma \in \mathbb{R}$ somit ist $L = \mathbb{R}(\beta) = \mathbb{R}(\frac{\beta}{\gamma})$. Weil nun gilt $\left(\frac{\beta}{\gamma}\right)^2 = \frac{\beta^2}{\gamma^2} = \frac{\beta^2}{-\beta^2} = -1$, folgt $L \cong \mathbb{C}$.

(d) Ist $[L : \mathbb{C}] = 2$, dann ist $L = \mathbb{C}(\alpha)$ für ein $\alpha \in L \backslash \mathbb{C}$. Wie oben können wir annehmen, dass $\alpha^2 \in \mathbb{C}$. Das Minimalpolynom von α über $\mathbb{C}$ ist dann $f = X^2 - \alpha^2$. Weil nun jede komplexe Zahl eine Wurzel in $\mathbb{C}$ hat, also auch die Zahl $\alpha^2 \in C$, zerfällt das Polynom f über $\mathbb{C}$ in Linearfaktoren. Somit kann f nicht das Minimalpolynom von α üeber $\mathbb{C}$ sein.

(e) Wir nehmen zuerst an, dass $L : \mathbb{R}$ galoissch ist. Sei $L = L_n : \ldots : L_0 : \mathbb{R}$ wie in (a). Mit (b) ist dann $L_0 = \mathbb{R}$. Ist $n = 0$, dann ist $L = \mathbb{R}$. Andernfalls erhalten wir mit (c), dass $L_1 \cong \mathbb{C}$, und aus (d) folgt, dass $L_i = L_1$ für alle $1 \leqslant i \leqslant n$. Somit ist $L = L_n \cong \mathbb{C}$.

(f) Für den allgemeinen Fall, d.h. wenn $L : \mathbb{R}$ zwar endlich aber nicht galoissch ist, sei $\tilde{L}$ der normale Abschluss von $L : \mathbb{R}$. Dann können wir, weil $\tilde{L} : \mathbb{R}$ galoissch ist, wie oben schliessen, dass $\tilde{L} \cong \mathbb{R}$ oder $\tilde{L} \cong \mathbb{C}$, und weil $L \subseteq \tilde{L}$ gilt dasselbe auch für den Körper L.