Musterlösung 23

Satz vom primitiven Element und Galoiserweiterungen

1. Finde ein primitives Element der Erweiterung L von K in den folgenden Fällen:
   (a) $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[4]{2}, i)$.
   (b) $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.
   (c) $K = \mathbb{C}(t, u)$ mit t, u algebraisch unabhängig über $\mathbb{C}$ und $L = K(\alpha, \beta)$, wobei α eine Nullstelle des Polynoms $X^n - t$ und β eine Nullstelle von $X^m - u$ ist.

   Lösung: In jedem Fall ist die Erweiterung L/K endlich, und wegen $\mathrm{char}(K) = 0$ ist sie ausserdem separabel. Nach dem Satz vom primitiven Element existiert also tatsächlich ein primitives Element c in L über K. Der Beweis dieses Satzes sagt sogar, wie man c findet, wenn L über K von zwei Elementen a und b erzeugt wird:

   Man betrachtet die Menge $\{a = a_1, \dots, a_m\}$ der Nullstellen des Minimalpolynoms $m_{a,K}$ in einem algebraischen Abschluss von K und die Menge $\{b = b_1, \dots, b_n\}$ der Nullstellen von $m_{b,K}$. Nach dem Beweis ist dann für jedes

   $$\gamma \in K \smallsetminus \{(a_j - a)(b - b_i)^{-1} \mid j = 1, \dots, m;\ i = 2, \dots n\}$$

   das Element $c = a + \gamma b$ ein primitives Element von L über K. Diese Konstruktion wenden wir jetzt auf die gegebenen Beispiele einzeln an:

   (a) Das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist $f(X) = X^4 - 2$ und das von i ist $g(X) = X^2 + 1$. Die Nullstellen von f sind $a = a_1 = \sqrt[4]{2}, a_2 = -\sqrt[4]{2}, a_3 = i\sqrt[4]{2}, a_4 = -i\sqrt[4]{2}$ und die Nullstellen von g sind $b = b_1 = i, b_2 = -i$. Die Menge

   $$\{(a_j - a)(b - b_2)^{-1} \mid j = 1, \dots 4\} = \{0, i\sqrt[4]{2}, 2^{-3/4}(1 + i), 2^{-3/4}(-1 + i)\}$$

   enthält nicht 1. Demnach ist $a + b = \sqrt[4]{2} + i$ ein primitives Element von L.

   (b) Das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $f(X) = X^2 - 2$ und das von $\sqrt[3]{2}$ ist $g(X) = X^3 - 2$. Die Nullstellen von f sind $a = a_1 = \sqrt{2}, a_2 = -\sqrt{2}$ und die Nullstellen von g sind $b = b_1 = \sqrt[3]{2}, b_2 = \zeta_3\sqrt[3]{2}, b_3 = \zeta_3^2\sqrt[3]{2}$, wobei ζ_3 eine primitive dritte Einheitswurzel ist. Die Menge

   $$\{(a_j - a)(b - b_k)^{-1} \mid j = 1, 2;\ k = 2, 3\} = \left\{0, -\frac{2^{7/6}}{1 - \zeta_3}, -\frac{2^{7/6}}{1 - \zeta_3^2}\right\}$$

   enthält nicht 1. Demnach ist $a + b = \sqrt{2} + \sqrt[3]{2}$ ein primitives Element von L.

Variante: Es gilt sowohl $\sqrt[6]{2} = \frac{\sqrt{2}}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ als auch $\sqrt{2} = (\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2})$ und $\sqrt[3]{2} = (\sqrt[6]{2})^2 \in \mathbb{Q}(\sqrt[6]{2})$. Folglich haben wir $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

(c) Das Minimalpolynom von α über K ist $f(X) = X^n - t$ und das von β ist $g(X) = X^m - u$. Sei ζ_n, bzw. ζ_m, eine primitive n-te, bzw. m-te, Einheitswurzel. Dann sind $\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha$ die Nullstellen von f und $\beta, \zeta_m\beta, \ldots, \zeta_m^{m-1}\beta$ die Nullstellen von g; die betrachtete Menge wird in diesem Fall zu

$$\left\{ \frac{\alpha(\zeta_n^j - 1)}{\beta(1 - \zeta_m^k)} \mid j = 0, \ldots, n-1;\ k = 1, \ldots, m-1 \right\}.$$

Sie besteht nur aus 0 und über $\mathbb{C}$ transzendenten Elementen der Form $\frac{\alpha}{\beta} \cdot d$ mit $d \in \mathbb{C}^\times$, enthält also 1 nicht. Demnach ist $\alpha + \beta$ ein primitives Element von L.

*2. Sei K ein Körper der Charakteristik $p > 0$, und sei $\overline{K}$ ein algebraischer Abschluss von K.

(a) Zeige: Für jede algebraische Erweiterung der Form $L = K(A)$ von K sind äquivalent:

(i) Für jedes $a \in L$ existiert ein $r \geqslant 0$ mit $a^{p^r} \in K$.

(ii) Für jedes $a \in A$ existiert ein $r \geqslant 0$ mit $a^{p^r} \in K$.

(iii) $|\operatorname{Hom}_K(L, \overline{K})| = 1$.

Eine Körpererweiterung L/K mit diesen Eigenschaften heisst *rein inseparabel* oder *total inseparabel* oder *radiziell*.

(b) Zeige: Für jeden algebraischen Körperturm $M/L/K$ ist M/K rein inseparabel genau dann, wenn M/L und L/K rein inseparabel sind.

Lösung: (a) Da L/K algebraisch und $\overline{K}$ algebraisch abgeschlossen ist, existiert ein K-Homomorphismus $L \to \overline{K}$ und wir können $\overline{K}$ als Oberkörper von L betrachten.

Die Implikation (i) $\Rightarrow$ (ii) ist klar.

Nehme nun (ii) an und betrachte einen Homomorphismus $\varphi \in \operatorname{Hom}_K(L, \overline{K})$. Sei $a \in A$ und wähle $r \geqslant 0$ so, dass a^{p^r} in K liegt. Dann ist a eine Nullstelle des Polynoms $X^{p^r} - a^{p^r} \in K[X]$. Über $\overline{K}$ gilt $X^{p^r} - a^{p^r} = (X - a)^{p^r}$, also ist a die einzige Nullstelle dieses Polynoms in $\overline{K}$. Nach Abschnitt 5.7 permutiert jeder K-Homomorphismus $\varphi\colon L \to \overline{K}$ die Nullstellen in L jedes Polynoms in $K[X]$, es folgt $\varphi(a) = a$. Folglich ist $\varphi|_A = id$ und wegen $L = K(A)$ ist φ auf L die Identität. Also gilt $\operatorname{Hom}_K(L, \overline{K}) = \{id|_L\}$ und wir haben (iii) bewiesen.

Nehme nun (iii) an, das heisst $\operatorname{Hom}_K(L, \overline{K}) = \{id|_L\}$. Betrachte $a \in L$. Sei $b \in \overline{K}$ eine Nullstelle des Minimalpolynoms $m_{a,K}$ von a. Dann existiert ein K-Isomorphismus $\psi\colon K(a) \to K(b)$ mit $\psi(a) = b$. Da $L/K(a)$ algebraisch und $\overline{K}$ algebraisch abgeschlossen ist, lässt sich ψ zu einem K-Homomorphismus $\overline{\psi}\colon L \to \overline{K}$ fortsetzen. Wegen $|\operatorname{Hom}_K(L, \overline{K})| = 1$ ist $\overline{\psi}|_L = id$. Es folgt $a = b$; also ist a

die einzige Nullstelle von $m_{a,K}$ in $\overline{K}$. Das Minimalpolynom von a über K hat also die Form $(X-a)^n$. Nach dem Satz aus Abschnitt 5.10 gilt $(X-a)^n = m_{a,K}(X) = g(X^{p^r})$ für ein eindeutiges $r \geqslant 0$ und ein separables irreduzibles Polynom $g \in K[X]$. Als separables Polynom mit genau einer Nullstelle muss g linear sein. Also gibt es ein $c \in K$ mit $(X-a)^n = X^{p^r} - c$. Koeffizientenvergleich liefert $a^{p^r} = c \in K$ und (i) ist bewiesen.

(b) Wir verwenden Kriterium (i) aus Teil (a).

Sei M/K rein inseparabel und sei $a \in M$. Dann existiert ein $r \geqslant 0$ mit $a^{p^r} \in K$. Dann liegt a^{p^r} auch in L. Also ist die Erweiterung M/L rein inseparabel. Sei nun $b \in L$. Dann liegt b auch in M und es gibt ein $s \geqslant 0$ mit $b^{p^s} \in K$. Also ist die Erweiterung L/K rein inseparabel.

Seien nun M/L und L/K rein inseparabel und sei $a \in M$. Dann existiert ein $r \geqslant 0$ mit $a^{p^r} \in L$. Da L/K rein inseparabel ist, existiert ein $s \geqslant 0$ mit $\left(a^{p^r}\right)^{p^s} \in K$. Also liegt $\left(a^{p^r}\right)^{p^s} = a^{p^r p^s} = a^{p^{r+s}}$ in K und die Erweiterung M/K ist rein inseparabel.

3. Zeige, dass die Substitutionen $t \mapsto 1/t$ und $t \mapsto 1-t$ eine endliche Untergruppe G der Automorphismengruppe des rationalen Funktionenkörpers $L := \mathbb{Q}(t)$ erzeugen. Bestimme den Fixkörper $K := L^G$ in der Form $K = \mathbb{Q}(s)$ sowie das Minimalpolynom von t über K.

Lösung: Die Menge der Substitutionen

$$t \mapsto t, \quad t \mapsto \frac{1}{t}, \quad t \mapsto 1-t, \quad t \mapsto \frac{1}{1-t}, \quad t \mapsto 1-\frac{1}{t}, \quad t \mapsto \frac{t}{t-1}$$

wird von $t \mapsto 1/t$ und $t \mapsto 1-t$ erzeugt und ist unter Komposition und Inversenbildung abgeschlossen, also ist G genau die Menge der von diesen Substitutionen induzierten Automorphismen von L; insbesondere ist $|G| = 6$. (Man überprüft übrigens leicht, dass G nicht kommutativ und daher isomorph zu S_3 ist.)

Nach Konstruktion ist das Polynom $f(X) := \prod_{\sigma \in G}(X - \sigma(t))$ invariant unter G, also liegen seine Koeffizienten in K. Explizite Rechnung liefert

$$\begin{aligned} f(X) &= (X-t)(X-\tfrac{1}{t})(X-(1-t))(X-\tfrac{1}{1-t})(X-(1-\tfrac{1}{t}))(X-\tfrac{t}{t-1}) \\ &= X^6 - 3X^5 - sX^4 + (2s+5)X^3 - sX^2 - 3X + 1 \end{aligned}$$

mit

$$s := \frac{t^6 - 3t^5 + 5t^3 - 3t + 1}{t^2(1-t)^2} \in K.$$

Nach Serie 16 Aufgabe 5b ist $[L/\mathbb{Q}(s)]$ das Maximum von Zählergrad und Nennergrad von s, also gleich 6. Nach Abschnitt 6.1 der Vorlesung ist andererseits $[L/K] = |G| = 6$. Wegen $\mathbb{Q}(s) \subset K$ folgt daraus $K = \mathbb{Q}(s)$. Schliesslich ist t eine Nullstelle des normierten Polynoms $f \in K[X]$ vom Grad $6 = [L/K] = [K(t)/K]$; also ist f das Minimalpolynom von t über K.

4. Sei $f \in K[X]$ irreduzibel und separabel und sei L ein Zerfällungskörper von f über K. Zeige: Ist $\mathrm{Gal}(L/K)$ abelsch, so ist $L = K(a)$ für eine beliebige Nullstelle $a \in L$ von f.

   Lösung: Wir stellen zunächst fest, dass L/K galoissch ist, da L ein Zerfällungskörper eines separablen Polynoms über K ist. Aus dem gleichen Grund ist $L/K(a)$ galoissch. Nach Definition ist $\mathrm{Gal}(L/K(a))$ die Untergruppe aller $\gamma \in \mathrm{Gal}(L/K)$ mit $\gamma|_{K(a)} = \mathrm{id}_{K(a)}$, oder äquivalent $\gamma(a) = a$.

   Sei $a' \in L$ eine zweite Nullstelle von f. Wir behaupten, dass ein $\delta \in \mathrm{Gal}(L/K)$ existiert mit $\delta(a) = a'$. Um dies zu zeigen, beachte zuerst, dass $K(a)$ und $K(a')$ Stammkörper desselben irreduziblen Polynoms f sind. Es existiert daher ein Isomorphismus $\varphi\colon K(a) \xrightarrow{\sim} K(a')$ über K mit $\varphi(a) = a'$. Sodann sei $\overline{L}$ ein algebraischer Abschluss von L. Dann besitzt φ eine Fortsetzung zu einem Homomorphismus $\psi\colon L \to \overline{L}$ über K. Da L/K normal ist, gilt $\psi(L) = L$ und wir können den von ψ induzierten Automorphismus $L \xrightarrow{\sim} L$ als δ wählen. (*Aliter:* Da f irreduzibel ist, operiert $\mathrm{Gal}(L/K)$ transitiv auf der Menge der Nullstellen von f nach §6.2 der Vorlesung.)

   Für jedes $\gamma \in \mathrm{Gal}(L/K(a))$ gilt nun $\gamma(a) = a$ und $\delta(a) = a'$. Da $\mathrm{Gal}(L/K)$ abelsch ist, gilt ausserdem $\gamma \circ \delta = \delta \circ \gamma$ und folglich $\gamma(a') = \gamma(\delta(a)) = \delta(\gamma(a)) = \delta(a) = a'$. Variieren wir a', so sehen wir, dass γ jede Nullstelle von f auf sich abbildet. Da L von diesen Nullstellen über K erzeugt wird, ist γ auf ganz L die Identität. Also ist $\mathrm{Gal}(L/K(a))$ die triviale Untergruppe von $\mathrm{Gal}(L/K)$. Wegen $|\mathrm{Gal}(L/K(a))| = [L/K(a)]$ folgt also $[L/K(a)] = 1$ und somit $L = K(a)$.