Musterlösung Serie 23

Separable, inseparable, normale Körpererweiterungen

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 $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

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

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

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 $a = a_1 = \sqrt[4]{2}$ und $a_2 = -\sqrt[4]{2}$ und $a_3 = i\sqrt[4]{2}$ und $a_4 = -i\sqrt[4]{2}$ und die Nullstellen von g sind $b = b_1 = i$ und $b_2 = -i$. Die Menge

$$\big\{(a_j - a)(b - b_2)^{-1} \bigm| j = 1, \ldots 4\big\} \;=\; \big\{0, i\sqrt[4]{2}, 2^{-3/4}(1+i), 2^{-3/4}(-1+i)\big\}$$

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 $a = a_1 = \sqrt{2}$ und $a_2 = -\sqrt{2}$ und die Nullstellen von g sind $b = b_1 = \sqrt[3]{2}$ und $b_2 = \zeta_3\sqrt[3]{2}$ und $b_3 = \zeta_3^2\sqrt[3]{2}$, wobei ζ_3 eine primitive dritte Einheitswurzel ist. Die Menge

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

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

Aliter: 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 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

2. Beweise die folgende Proposition aus der Vorlesung: Für jeden algebraischen Körperturm $M/L/K$ der Charakteristik $p > 0$ ist M/K rein inseparabel genau dann, wenn M/L und L/K rein inseparabel sind.

   Lösung: Angenommen, die Körpererweiterungen M/L und L/K sind rein inseparabel. Weil M/L rein inseparabel ist, existiert für jedes Element $a \in M$ eine Zahl $r \geqslant 0$ mit $a^{p^r} \in L$. Weil L/K rein inseparabel ist, existiert dann auch eine Zahl $s \geqslant 0$ so dass $a^{p^{r+s}} = (a^{p^r})^{p^s} \in K$ ist. Daraus folgt, dass M/K rein inseparabel ist.

   Umgekehrt nehmen wir jetzt an, dass M/K rein inseparabel ist. Für jedes Element $a \in M$ existiert dann eine Zahl $r \geqslant 0$ so dass $a^{p^r} \in K \subset L$ liegt. Also ist M/L rein inseparabel. Für jedes $b \in L \subset M$ existiert dann ebenfalls eine Zahl $s \geqslant 0$ so dass $b^{p^s} \in K$ liegt, also ist auch L/K rein inseparabel.

3. Sei K ein Körper der Charakteristik $p > 0$, und sei L/K eine endliche Körpererweiterung. Zeige: Ist $[L/K]$ teilerfremd zu p, so ist L/K separabel.

   Lösung: Sei $a \in L$ beliebig, und sei f das Minimalpolynom von a über K. Wir betrachten den Körperturm $L/K(a)/K$. Wegen $p \nmid [L/K]$ und der Multiplikativität des Körpergrades ist auch $[K(a)/K]$ nicht durch p teilbar. Folglich ist $\deg(f) = [K(a)/K]$ teilerfremd zu p. Aus der Vorlesung wissen wir, dass es ein $r \geqslant 0$ und ein separables irreduzibles Polynom $g(Y) \in K[Y]$ mit $f(X) = g(X^{p^r})$ gibt. Daraus folgt

   $$p^r \deg(g) = \deg(f).$$

   Da $\deg(f)$ nicht durch p teilbar ist, gilt $r = 0$ und damit ist $f = g$ separabel. Folglich ist a separabel über K. Da a beliebig war, ist damit L/K eine separable Erweiterung.

*4. Betrachte eine algebraische Körpererweiterung L/K und setze

   $$L' \;:=\; \{a \in L \mid a \text{ separabel über } K\}.$$

   Zeige:

   (a) L' ist der eindeutige grösste Zwischenkörper von L/K, welcher separabel über K ist.

   (b) Ist $L' \neq L$, so ist $p := \mathrm{char}(K) > 0$ und für jedes $a \in L$ existiert ein $r \geqslant 0$ mit $a^{p^r} \in L'$. (Man nennt L/L' dann *rein inseparabel.*)

   (c) Ist L algebraisch abgeschlossen, so ist jede separable algebraische Körpererweiterung von L' trivial. (Man nennt L' dann *separabel abgeschlossen.*)

   Lösung: (a) Seien $a, b \in L'$. Dann ist $K(a, b)$ von über K separablen Elementen erzeugt und daher separabel über K. Also liegen Summe, Differenz, Produkt und, falls definiert, Quotient von a und b in einer separablen Erweiterung von K, sind daher separabel und liegen somit in L'. Also ist L' ein Körper. Nach Definition ist er separabel über K. Sei L'' ein weiterer Zwischenkörper der Erweiterung L/K mit L''/K separabel. Dann ist jedes Element $c \in L''$ separabel über K und liegt daher in L'. Also gilt $L'' \subset L'$ und L' ist eindeutig maximal.

(b) In der Vorlesung wurde bewiesen, dass jede algebraische Körpererweiterung eines Körpers der Charakteristik 0 separabel ist. Also folgt aus $L \neq L'$, dass $p := \mathrm{char}(K) > 0$ gilt. Sei $a \in L'$. Nach Satz 6.5.9 der Vorlesung hat das Minimalpolynom von a über K die Form $g(X^{p^r})$ für ein $r \geqslant 0$ und ein separables irreduzibles Polynom $g \in K[X]$. Dann ist a^{p^r} eine Nullstelle von g, also ist g das Minimalpolynom von a^{p^r} über K. Da g separabel ist, ist folglich a^{p^r} separabel über K, also $a^{p^r} \in L'$.

(c) Sei L''/L' separabel. Da schon L'/K separabel ist, ist dann auch L''/K separabel. Da L algebraisch abgeschlossen und L''/L' algebraisch ist, existiert ein Homomorphismus $L'' \to L$ über L'. Dessen Bild besteht aus Elementen von L, die separabel über K sind, und liegt daher in L'. Somit ist $L'' = L'$, wie gewünscht.

**5. Betrachte eine algebraische Körpererweiterung L/K mit der Eigenschaft, dass jedes irreduzible Polynom in $K[X]$ eine Nullstelle in L hat. Zeige, dass L ein algebraischer Abschluss von K ist.

Hinweis: Benutze den Satz vom primitiven Element und die obige Aufgabe 4.

Lösung: Es genügt zu zeigen, dass jedes irreduzible Polynom in $K[X]$ über L in Linearfaktoren zerfällt, denn dann folgt die gewünschte Aussage aus Aufgabe 2 von Serie 21. Siehe dafür Theorem 2 in Keith Conrad, Constructing Algebraic Closures:

`https://kconrad.math.uconn.edu/blurbs/galoistheory/algclosure.pdf`

6. Ist für folgendes $\alpha \in \mathbb{R}$ die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ normal? Falls nicht, bestimme eine normale Hülle.

(a) $\alpha = \sqrt{2+\sqrt{2}}$

(b) $\alpha = \sqrt{1+\sqrt{3}}$

Lösung: (a) Doppeltes Quadrieren ergibt, dass α eine Nullstelle des Polynoms $f(X) = X^4 - 4X^2 + 2$ ist. Dieses ist nach Eisenstein mit $p = 2$ irreduzibel in $\mathbb{Q}[X]$ und deshalb das Minimalpolynom von α. Die anderen drei Nullstellen von f sind $-\alpha$ und

$$\pm\sqrt{2-\sqrt{2}} \;=\; \pm\frac{\sqrt{2}}{\alpha} \;=\; \pm\frac{\alpha^2-2}{\alpha}$$

und liegen ebenfalls in $\mathbb{Q}(\alpha)$. Also ist $\mathbb{Q}(\alpha)$ der Zerfällungskörper von $f = m_{\alpha,\mathbb{Q}}$ und somit ist $\mathbb{Q}(\alpha)/\mathbb{Q}$ normal.

(b) Doppeltes Quadrieren ergibt, dass α eine Nullstelle des Polynoms $f(X) = X^4 - 2X^2 - 2$ ist. Dieses ist nach Eisenstein mit $p = 2$ irreduzibel in $\mathbb{Q}[X]$ und deshalb das Minimalpolynom von α. Die anderen drei Nullstellen von f sind $-\alpha$ und

$$\pm i\sqrt{\sqrt{3}-1} \;=\; \pm\frac{i\sqrt{2}}{\alpha} \;\notin\; \mathbb{Q}(\alpha) \;\subset\; \mathbb{R}.$$

Somit ist $\mathbb{Q}(\alpha)/\mathbb{Q}$ nicht normal. Seine normale Hülle ist der Zerfällungskörper von $f = m_{\alpha,\mathbb{Q}}$, also seine echte Erweiterung

$$\mathbb{Q}(\alpha, i\sqrt{\sqrt{3}-1}) = \mathbb{Q}(\alpha, i\sqrt{2}).$$

7. Beweise oder widerlege: Jede rein inseparable algebraische Erweiterung L/K ist normal.

   Lösung: Das ist richtig, denn: Sei $\overline{L}$ ein algebraischer Abschluss von L. Dies ist auch ein algebraischer Abschluss von K. Nach Proposition 6.9.1 (c) der Vorlesung ist die Einbettung $L \hookrightarrow \overline{L}$ dann das einzige Element $\varphi \in \mathrm{Hom}_K(L, \overline{L})$. Für dieses gilt offenbar $\varphi(L) = L$. Nach Proposition 6.10.1 (e) der Vorlesung ist L/K also normal.

*8. Sei $L \subset \mathbb{C}$ der Körper der über $\mathbb{Q}$ mit Zirkel und Lineal konstruierbaren Zahlen. Zeige, dass $L/\mathbb{Q}$ eine normale Erweiterung ist.

   Lösung: Wir erinnern daran, dass L die Menge der Elemente in $\mathbb{C}$ ist, die in einem quadratischen Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ über $\mathbb{Q}$ enthalten sind. Für jeden solchen Körperturm und jeden Homomorphismus $\varphi \in \mathrm{Hom}(L, \overline{\mathbb{Q}})$ in einen algebraischen Abschluss $\overline{\mathbb{Q}}$ ist $\varphi(\mathbb{Q}) = \mathbb{Q} \subset \varphi(K_1) \subset \ldots \subset \varphi(K_n)$ wiederum ein quadratischer Erweiterungsturm über $\mathbb{Q}$, also in L enthalten. Damit gilt $\varphi(L) \subset L$ für jeden solchen Homomorphismus φ; anders gesagt ist $L/\mathbb{Q}$ eine normale Erweiterung.