Musterlösung Serie 14

KÖRPERERWEITERUNGSGRADE, MINIMALPOLYNOME

---

83. Sei $L : K$ eine algebraische Körpererweiterung. Seien K_1, K_2 zwei Zwischenkörper, d.h. $K \subseteq K_1, K_2 \subseteq L$, sodass die Körpererweiterungen $K_1 : K$ und $K_2 : K$ endlich sind. Das *Kompositum* von K_1 und K_2 ist definiert als $K_1K_2 := K(K_1 \cup K_2)$. Zeige:

(a) $[K_1K_2 : K_2] \leqslant [K_1 : K]$

(b) $[K_1K_2 : K] \leqslant [K_1 : K] \cdot [K_2 : K]$

(c) Falls $\mathrm{ggT}([K_1 : K], [K_2 : K]) = 1$ ist, so gilt Gleichheit in (b).

Bemerkung: Falls in (b) Gleichheit gilt, so heissen K_1 und K_2 *linear disjunkt* über K.

Lösung (a) Sei A eine Basis von K_1 über K. Wegen $K_1 = K(A)$ gilt auch $K_1K_2 = K_2(A)$. Satz 14.3(a) iteriert auf die Elemente von A angewendet ergibt, dass $K_2(A) = K_2[A]$ ist. Somit sehen wir, dass $K_1K_2 = \{\sum' a_ib_i : a_i \in K_1, b_i \in K_2\}$ ist, wobei $\sum'$ eine endliche Summe bezeichnet. Daraus können wir sehen, dass A ein Erzeugendensystem von K_1K_2 als K_2-Vektorraum ist. Folglich gilt $[K_1K_2 : K_2] \leqslant |A| = [K_1 : K]$.

(b) Multiplikativität des Körpergrades und Teil (a) implizieren

$$[K_1K_2 : K] = [K_1K_2 : K_2][K_2 : K] \leqslant [K_1 : K][K_2 : K].$$

Für (c) genügt es zu zeigen, dass aus $\mathrm{ggT}([K_1 : K], [K_2 : K]) = 1$ die Ungleichung $[K_1K_2 : K] \geqslant [K_1 : K] \cdot [K_2 : K]$ folgt.

Wegen $[K_1K_2 : K] = [K_1K_2 : K_2] \cdot [K_2 : K]$ ist $[K_2 : K]$ ein Teiler von $[K_1K_2 : K]$. Analog ist $[K_1 : K]$ ein Teiler von $[K_1K_2 : K]$. Aus der Teilerfremdheit erhalten wir, dass $[K_1 : K] \cdot [K_2 : K]$ den Grad $[K_1K_2 : K]$ teilt, und deshalb gilt

$$[K_1K_2 : K] \geqslant [K_1 : K] \cdot [K_2 : K].$$

84. (a) Sei ω eine primitive 3. Einheitswurzel über $\mathbb{Q}$.
Zeige: $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

(b) Zeige: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

(c) Zeige: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Lösung (a) Wegen $\omega \notin \mathbb{Q}$ gilt $[\mathbb{Q}(\omega) : \mathbb{Q}] > 1$. Andererseits ist ω eine Nullstelle des quadratischen Polynoms $\frac{X^3-1}{X-1} = (X^2 + X + 1)$. Daher ist $[\mathbb{Q}(\omega) : \mathbb{Q}] \leqslant 2$ und die Aussage folgt.

(b) Wegen $\sqrt{2} \notin \mathbb{Q}$ und $\sqrt{2}^2 - 2 = 0$ gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Weiter behaupten wir, dass $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ gilt. Daraus folgt wegen $\sqrt{3}^2 - 3 = 0$ dann

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

und mit der Multiplikativität der Körpergrade daher

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\cdot 2 = 4.$$

Für die Behauptung $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$ nehmen wir an, es sei $\sqrt{3}=\alpha+\beta\sqrt{2}$ mit $\alpha,\beta\in\mathbb{Q}$. Wegen $\sqrt{3}\notin\mathbb{Q}$ gilt $\beta\neq 0$. Wir quadrieren und erhalten $3=\alpha^2+2\beta\sqrt{2}+\beta^2 2$, was ein Widerspruch ist zu $\sqrt{2}\notin\mathbb{Q}$.

(c) Wir müssen zeigen, dass $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ ist. Wegen

$$\frac{1}{\sqrt{3}+\sqrt{2}} = \sqrt{3}-\sqrt{2}$$

ist

$$\sqrt{3} = \frac{1}{2}\left(\frac{1}{\sqrt{3}+\sqrt{2}}+\sqrt{3}+\sqrt{2}\right)\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$$

und daher auch

$$\sqrt{2} = \sqrt{3}+\sqrt{2}-\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Nach Definition des erzeugten Zwischenkörpers folgt $\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ und somit Gleichheit.

Aliter: Wegen $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$ gilt $\mathbb{Q}(\sqrt{6})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Wegen $\sqrt{6}\notin\mathbb{Q}$ ist dabei $[\mathbb{Q}(\sqrt{6}):\mathbb{Q}]\geqslant 2$. Weiter gilt $\sqrt{2}+\sqrt{3}\notin\mathbb{Q}(\sqrt{6})$, da andernfalls für gewisse $\alpha,\beta\in\mathbb{Q}$ gilt

$$\sqrt{2}+\sqrt{3}=\alpha\sqrt{6}+\beta \quad\Leftrightarrow\quad \sqrt{3}=\frac{\sqrt{2}-\beta}{\alpha\sqrt{2}-1}\in\mathbb{Q}(\sqrt{2}),$$

was wir in Teil (b) bereits ausgeschlossen haben. Also gilt $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{6})]\geqslant 2$. Aus der Multiplikativität der Körpergrade folgt

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{6})]\cdot[\mathbb{Q}(\sqrt{6}):\mathbb{Q}]\geqslant 2\cdot 2 = 4.$$

Wegen $\mathbb{Q}(\sqrt{2},\sqrt{3})\supseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$ gilt andererseits

$$4 = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})]\cdot[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}].$$

Somit muss der erste Faktor auf der rechten Seite gleich 1 sein, woraus die gesuchte Gleichheit folgt.

85. Bestimme das Minimalpolynom folgender (komplexer) Zahlen über $\mathbb{Q}$.

(a) $\sqrt{2}+\sqrt{5}$

(b) $\sqrt[4]{5}+\sqrt[4]{5}i$

Lösung (a) Sei $\alpha := \sqrt{2}+\sqrt{5}$. Dann haben wir $\alpha^2 = 7+2\sqrt{10}$, und nach Subtraktion von 7 auf beiden Seiten und Quadrieren erhalten wir $\alpha^4-14\alpha^2+49 = 40$. Somit ist α eine Nullstelle des Polynoms $f(X) := X^4-14X^2+9$. Wir zeigen nun, dass f das Minimalpolynom von α ist. Weil $f\in\mathbb{Q}[X]$ normiert ist, müssen wir nur noch zeigen, dass f irreduzibel über $\mathbb{Q}$ ist.

Die Nullstellen von $Y^2 - 14Y + 9$ sind $7 \pm 2\sqrt{10}$, und damit sind die Nullstellen von f

$$\pm\sqrt{7 \pm 2\sqrt{10}} = \pm\sqrt{2} \pm \sqrt{5},$$

und weil $(\pm\sqrt{2} \pm \sqrt{5})^2 = 7 \pm 2\sqrt{10} \notin \mathbb{Q}$, sind auch $\pm\sqrt{2} \pm \sqrt{5} \notin \mathbb{Q}$. Somit kann kein Faktor einer Zerlegung von f linear sein, und weil auch kein Produkt von zwei Linearfaktoren $(X - \beta) \cdot (X - \gamma)$ mit $\beta, \gamma \in \{\pm\sqrt{2} \pm \sqrt{5}\}$ ein Polynom in $\mathbb{Q}[X]$ ist, kann kein Faktor einer Zerlegung von f quadratisch sein. Somit ist $f = X^4 - 14X^2 + 9$ das Minimalpolynom von $\alpha = \sqrt{2} + \sqrt{5}$.

(b) Sei $\alpha := \sqrt[4]{5} + \sqrt[4]{5}i$. Dann ist $\alpha^4 = 5 \cdot (1 + i)^4 = -20$ und α ist eine Nullstelle von $f(X) = X^4 + 20$. Dies ist ein primitives Polynom in $\mathbb{Z}[X]$, und aus dem Kriterium von Schönemann-Eisenstein mit $p = 5$ folgt, dass $f = X^4 + 20$ irreduzibel ist in $\mathbb{Q}[X]$. Somit ist $f = X^4 + 20$ das Minimalpolynom von α.

86. (a) Zeige, dass die Menge

$$\big\{a \in \mathbb{R} : a \text{ ist algebraisch über } \mathbb{Q}\big\}$$

abzählbar ist.

(b) Zeige, dass $[\mathbb{R} : \mathbb{Q}]$ überabzählbar ist.

Lösung (a) Die Menge lässt sich umformulieren zu

$$\big\{a \in \mathbb{R} : a \text{ hat ein nichtverschwindendes annulierendes Polynom mit Koeffizienten in } \mathbb{Q}\big\}.$$

Die Menge aller normierten Polynome vom Grad n ist offensichtlich gleich mächtig wie die Menge $\mathbb{Q}^n$, also abzählbar. Also gibt es eine Bijektion $\mathbb{Q}[X] \to \bigsqcup_{i=1}^{\infty} \mathbb{Q}^n$. Folglich ist die Menge $\mathbb{Q}[X]$ abzählbar. Jedes Polynom in $\mathbb{Q}[X]$ hat höchstens endlich viele Nullstellen. Somit ist die Menge der reellen algebraischen Zahlen über $\mathbb{Q}$ abzählbar.

(b) Der $\mathbb{Q}$-Vektorraum $\mathbb{Q}[X]$ ist abzählbar dimensional über $\mathbb{Q}$. Wie in (a) ist er jedoch auch selber abzählbar. Da jeder $\mathbb{Q}$-Vektorraum mit abzählbar unendlicher Dimension über $\mathbb{Q}$ als Vektorraum isomorph zu $\mathbb{Q}[X]$ sein muss, und da $\mathbb{R}$ überabzählbar ist, ist $[\mathbb{R} : \mathbb{Q}]$ überabzählbar.