Algebra I

Musterlösung 13

Körpererweiterungsgrade, Minimalpolynome

---

81. (a) Sei $L : K$ eine Körpererweiterung.

Zeige: Sie ist genau dann endlich, wenn sie algebraisch und von endlich vielen Elementen erzeugt ist.

(b) Seien $M : L$ und $L : K$ Körpererweiterungen.

Zeige: $M : K$ ist genau dann algebraisch, wenn $M : L$ und $L : K$ algebraisch sind.

Lösung: (a) Sei $L : K$ endlich. Dann ist L ein endlich dimensionaler K-Vektorraum. Offensichtlich ist L über K von einer Vektorraumbasis erzeugt. Daher ist $L : K$ von endlich vielen Elementen erzeugt.

Sei nun $a \in L$. Wir müssen zeigen, dass a algebraisch über K ist. Dann sind $1, a, a^2, \ldots, a_{[L:K]}$ linear abhängig. Somit existieren $\alpha_i \in K$, nicht alle gleich null, mit $\sum_{i=0}^{[L:K]} \alpha_i a^k = 0$. Offensichtlich ist nun $\sum_{i=0}^{[L:K]} \alpha_i X^k$ ein nichtverschwindendes annulierendes Polynom von a mit Koeffizienten in K. Somit ist a algebraisch über K und die Körpererweiterung $L : K$ ist algebraisch.

Die andere Richtung wurde in der Vorlesung gezeigt.

(b) Sei $M : K$ algebraisch. Dann ist jedes Element von M algebraisch über K. Somit ist es auch algebraisch über L, da wegen $K \subseteq L$ ein annulierendes Polynom mit Koeffizienten in K auch alle seine Koeffizienten in L hat. Ausserdem liegen Elemente aus L auch in M. Somit ist somit jedes Element von L algebraisch über K. Somit ist $L : K$ algebraisch.

Seien nun $M : L$ und $L : K$ algebraisch. Sei $a \in M$. Sei $\sum_{i=0}^{n} \alpha_i X^i$ das Minimalpolynom von a über L. Wegen Aufgabe (a) gilt $[K(\alpha_0, \ldots, \alpha_n) : K] < \infty$. Ausserdem ist a algebraisch über $K(\alpha_0, \ldots, \alpha_n)$. Folglich gilt auch $[K(a, \alpha_0, \ldots, \alpha_n) : K(\alpha_0, \ldots, \alpha_n)] < \infty$. Insgesamt folgern wir mit der Multiplikativität des Körpergrades

$$\begin{aligned}
[K(a) : K] &= \frac{[K(a, \alpha_0, \ldots, \alpha_n) : K]}{[K(a, \alpha_0, \ldots, \alpha_n) : K(a)]} \\
&\leq [K(a, \alpha_0, \ldots, \alpha_n) : K] \\
&= [K(a, \alpha_0, \ldots, \alpha_n) : K(\alpha_0, \ldots, \alpha_n)] \cdot [K(\alpha_0, \ldots, \alpha_n) : K] \\
&< \infty.
\end{aligned}$$

Somit ist a algebraisch über K und die Körpererweiterung $M : K$ ist algebraisch.

82. Sei $L : K$ eine algebraische Körpererweiterung. Seien K_1, K_2 zwei Zwischenkörper, 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) $[K_1K_2 : K_2] \leq [K_1 : K]$

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

(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 $[K_1K_2 : K_2] \leq |A| = [K_1 : K]$.

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

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

Zu zeigen bleibt die umgekehrte Ungleichung.

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

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

83. (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 $\frac{X^3-1}{X-1}$. Daher ist $[\mathbb{Q}(\omega) : \mathbb{Q}] \leq 2$ 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 $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] \geq 2$. 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 $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{6})] \geq 2$. Aus der Multiplikativität der Körpergrade folgt

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

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.

84. Bestimme das Minimalpolynom folgender komplexer Zahlen über $\mathbb{Q}$.

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

(b) $\sqrt{3}-\sqrt[3]{3}$

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

Lösung: a) Let $\alpha := \sqrt{2}+\sqrt{5}$. Then we have $\alpha^2 = 7+2\sqrt{10}$, which by subtracting 7 from both sides and squaring them implies $\alpha^4 - 14\alpha^2 + 49 = 40$, so that α is a root of the polynomial $f(X) := X^4 - 14X^2 + 9$. We claim that f is the minimal polynomial of α. Since f is already monic in $\mathbb{Q}[X]$, it remains to check that it is irreducible over $\mathbb{Q}$.

The complex roots of f are the four numbers $\pm\sqrt{2} \pm \sqrt{5}$. Since

$$(\pm\sqrt{2} \pm \sqrt{5})^2 = 2 \pm 2\sqrt{10} + 5 \notin \mathbb{Q},$$

we also have $\pm\sqrt{2} \pm \sqrt{5} \notin \mathbb{Q}$; hence there is no linear factor in the decomposition of f over $\mathbb{Q}$. The only remaining possibility for f not to be irreducible would be that it factors into two rational polynomials of degree 2, in which case one of two factors would be equal to $(X-\alpha)(X-\beta) \in \mathbb{Q}[X]$ for β one of the remaining roots. It can be easily checked that none of those polynomials have rational coefficients, contradiction. Hence $f(X) = X^4 - 14X^2 + 9$ is the minimal polynomial of $\alpha = \sqrt{2}+\sqrt{5}$.

Aliter: We can also proceed as in Exercise 83(b) to prove $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, which, together with the proposition from the lecture stating that $\deg(m_{\alpha,\mathbb{Q}}) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, gives us that $X^4 - 14X^2 + 9$ is the minimal polynomial of α over $\mathbb{Q}$.

b) Let $\alpha := \sqrt{3} - \sqrt[3]{3}$. Then $(\alpha - \sqrt{3})^3 = (-\sqrt[3]{3})^3$, i.e.,

$$\alpha^3 + 9\alpha + 3 = \sqrt{3}(3\alpha^2 + 3),$$

which implies, by squaring both sides,

$$\begin{aligned} &\alpha^6 + 81\alpha^2 + 9 + 18\alpha^4 + 6\alpha^3 + 54\alpha = 27(\alpha^4 + 2\alpha^2 + 1) \iff \\ &\alpha^6 - 9\alpha^4 + 6\alpha^3 + 27\alpha^2 + 54\alpha - 18 = 0. \end{aligned}$$

Then α is a root of $f(X) := X^6 - 9X^4 + 6X^3 + 27X^2 + 54X - 18$ and we claim this polynomial is irreducible. This is true if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. To prove this, we observe that $\sqrt{3} = \frac{\alpha^3+9\alpha+3}{3\alpha^2+3} \in \mathbb{Q}(\alpha)$ and therefore also $\sqrt[3]{3} = \sqrt{3} - \alpha \in \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt{3})\mathbb{Q}(\sqrt[3]{3})$. The minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}$ is $X^3 - 3$ (it obviously annihilates $\sqrt[3]{3}$ and is irreducible by Eisenstein with $p = 3$), therefore the degree $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ is coprime to $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. With Exercise 82(c) we conclude that $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{3})$ are linearly disjoint over $\mathbb{Q}$, i.e. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 6$. Thus the minimal polynomial of α over $\mathbb{Q}$ has degree 6 and is therefore equal to $f(X)$.

Aliter: We present a different method for showing $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Note that $\alpha \in \mathbb{Q}(\sqrt[6]{3})$, which is a degree-6 extension of $\mathbb{Q}$, because the polynomial $X^6 - 3$ is irreducible in $\mathbb{Q}[X]$ by Eisenstein Criterion with $p = 3$ and Gauss Lemma. Hence f is irreducible if and only if $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[6]{3})$, which is true if and only if $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ are generators for $\mathbb{Q}(\sqrt[6]{3})$. Denote $\beta := \sqrt[6]{3}$, so that $\alpha = \beta^3 - \beta^2 = \beta^2(\beta - 1)$. Then we have

$$\begin{aligned}
\alpha^2 &= 3 + \beta^4 - 2\beta^5, \\
\alpha^3 &= 3(\beta-1)^3 = -3 + 9\beta - 9\beta^2 + 3\beta^3 \\
\alpha^4 &= 3\beta^2(\beta-1)^4 = 9 + 3\beta^2 - 12\beta^3 + 18\beta^4 - 12\beta^5 \\
\alpha^5 &= 3\beta^4(\beta-1)^5 = -90 + 90\beta - 45\beta^2 + 9\beta^3 - 3\beta^4 + 15\beta^5,
\end{aligned}$$

which can be written in matrix notation as

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & -2 \\ -3 & 9 & -9 & 3 & 0 & 0 \\ 9 & 0 & 3 & -12 & 18 & -12 \\ -90 & 90 & -45 & 9 & -3 & 15 \end{pmatrix} \begin{pmatrix} 1 \\ \beta \\ \beta^2 \\ \beta^3 \\ \beta^4 \\ \beta^5 \end{pmatrix}.$$

Since the determinant of the square matrix can be computed to be $-3^4 \cdot 73$, it is invertible, making $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ a $\mathbb{Q}$-basis for $\mathbb{Q}(\beta)$, so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and therefore the polynomial $f(X) = X^6 - 9X^4 + 6X^3 + 27X^2 + 54X - 18$ is the minimal polynomial of α.

c) Let $\alpha := \sqrt[4]{5} + \sqrt[4]{5}i$. Then $\alpha^4 = 5 \cdot (1+i)^4 = -20$ and α is a root of $f(X) = X^4 + 20$. This is a polynomial with integer coefficients which is irreducible in $\mathbb{Z}[X]$ by Eisenstein's Criterion with $p = 5$. As it is monic, it has coprime coefficients, so that it is also irreducible in $\mathbb{Q}[X]$ by Gauss Lemma. Then $f(X) = X^4 + 20$ is the minimal polynomial of α.

85. (a) Zeige, dass die Menge

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

abzählbar ist.

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

Lösung: (a) Die Menge lässt sich umformulieren zu

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

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.