Musterlösung 16

EINFACHE UND ALGEBRAISCHE ERWEITERUNGEN

1. 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 $(X-\alpha)(X-\beta) \in \mathbb{Q}[X]$ 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 Serie 15 Exercise 4 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 $[\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}] = 3$ is coprime to $[\mathbb{Q}(\sqrt{3})/\mathbb{Q}] = 2$. With Serie 15 Exercise 2 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 that $[\mathbb{Q}(\alpha)/\mathbb{Q}] = 6$. Notice 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 $f(X) = X^6 - 9X^4 + 6X^3 + 27X^2 + 54X - 18$ 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.

2. Stelle für $\alpha = \sqrt{-3 + \sqrt{12}}$ folgende Zahlen als Polynom in α mit möglichst kleinem Grad dar:

   (a) $(\alpha^3 + 1)(\alpha^3 - \alpha + 4)$.

   (b) $\frac{1}{\alpha^2 + \alpha + 1}$.

Lösung: Wir bestimmen zunächst das Minimalpolynom von α. Quadrieren ergibt $\alpha^2 = -3 + \sqrt{12}$ und $\alpha^4 + 6\alpha^2 + 9 = 12$. Ein annullierendes Polynom ist also $X^4 + 6X^2 - 3$ und nach Eisenstein mit $p = 3$ ist es irreduzibel. Also ist

$$m_{\alpha,\mathbb{Q}}(X) = X^4 + 6X^2 - 3.$$

a) Ausmultiplizieren ergibt $(X^3 + 1)(X^3 - X + 4) = X^6 - X^4 + 5X^3 - X + 4$ und durch Polynomdivision mit Rest erhalten wir

$$X^6 - X^4 + 5X^3 - X + 4 = (X^2 - 7)(X^4 + 6X^2 - 3) + (5X^3 + 45X^2 - X - 17).$$

Einsetzen in diese Gleichung liefert

$$\begin{aligned} \alpha^6 - \alpha^4 + 5\alpha^3 - \alpha + 4 &= (\alpha^2 - 7)(\alpha^4 + 6\alpha^2 - 3) + (5\alpha^3 + 45\alpha^2 - \alpha - 17) \\ &= 5\alpha^3 + 45\alpha^2 - \alpha - 17. \end{aligned}$$

b) Wir suchen ein Polynom u, sodass ein Polynom v existiert mit

$$u(X)(X^2 + X + 1) + v(X)(X^4 + 6X^2 - 3) = 1.$$

Das gesuchte Inverse ist dann $u(\alpha)$. Wir wenden den Euklidischen Algorithmus an und erhalten durch Division mit Rest

$$X^4 + 6X^2 - 3 = \left(X^2 - X + 6\right)\left(X^2 + X + 1\right) + (-5X - 9)$$

und

$$X^2 + X + 1 = \left(-\frac{1}{5}X + \frac{4}{25}\right)(-5X - 9) + \frac{61}{25}.$$

Rückwärtseinsetzen liefert

$$u(X) = \frac{1}{61}\left(-5X^3 + 9X^2 - 34X + 49\right) \quad \text{und} \quad v(X) = \frac{1}{61}\left(5X - 4\right).$$

Also ist

$$\frac{1}{\alpha^2 + \alpha + 1} = \frac{1}{61}\left(-5\alpha^3 + 9\alpha^2 - 34\alpha + 49\right).$$

3. Sei L/K eine Körpererweiterung und seien $\alpha, \beta \in L$. Zeige: α und β sind genau dann algebraisch über K, wenn $\alpha + \beta$ und $\alpha \cdot \beta$ algebraisch über K sind.

   Lösung: In der Vorlesung wurde gezeigt, dass die Summe und das Produkt über K algebraischer Elemente ebenfalls algebraisch über K sind.

   Nehmen wir jetzt an, dass $\alpha + \beta$ und $\alpha \cdot \beta$ algebraisch seien und betrachten wir die Körpererweiterung $K' = K(\alpha + \beta, \alpha \cdot \beta)$ von K. Dann ist K'/K algebraisch. Ausserdem ist das Polynom $X^2 - (\alpha + \beta)X + \alpha \cdot \beta \in K'[X] \backslash \{0\}$ ein annullierendes Polynom von α und β, was impliziert, dass α und β algebraisch über K' sind. Folglich ist $K(\alpha, \beta)/K'$ algebraisch und als algebraische Erweiterung einer algebraischen Erweiterung ist daher auch $K(\alpha, \beta)/K$ algebraisch. Insbesondere sind α und β algebraisch über K.

4. Zeige, dass πi transzendent ist.

   Lösung: Nimm an, πi sei algebraisch. Weil i algebraisch ist, ist nach der vorigen Aufgabe auch $\pi = \pi i(-i)$ algebraisch. Dies ist ein Widerspruch zu einem Satz aus der Vorlesung.

   Aliter: Wenn πi algebraisch ist, gilt das auch für $(\pi i)^2 = -\pi^2$, also ist die Erweiterung $\mathbb{Q}(\pi^2)/\mathbb{Q}$ algebraisch. Die Zahl π hat ein annullierendes Polynom mit Koeffizienten in $\mathbb{Q}(\pi^2)$, nämlich $X^2 - \pi^2$, liegt dann also in einer algebraischen Erweiterung das algebraischen Körpers $\mathbb{Q}(\pi^2)$. Mit Kapitel 5.4 Proposition 6 folgt, dass π ebenfalls algebraisch ist. Dies ist ein Widerspruch zu einem Satz aus der Vorlesung.

*5. Sei K ein Körper und $L = K(t)$ der rationale Funktionenkörper über K in einer Variablen t.

   (a) Zeige, dass für jeden Zwischenkörper $K \subsetneq K' \subset L$ die Erweiterung L/K' algebraisch und die Erweiterung K'/K transzendent ist.

   (b) Sei $s = P(t)/Q(t) \in L$ mit teilerfremden Polynomen $P(X)$, $Q(X) \in K[X]$. Bestimme den Grad der Körpererweiterung $L/K(s)$ in Termen der Grade von P und Q.

   (c) Zeige, dass die Körperautomorphismen von L, welche auf K die Identität sind, genau die Abbildungen der Form

   $$L \to L,\ f(t) \mapsto f\Big(\frac{at+b}{ct+d}\Big)$$

   sind für alle Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$.

   Lösung: (a) Sei $s = P(t)/Q(t) \in K' \smallsetminus K$ für teilerfremde Polynome $P(X)$, $Q(X) \in K[X]$ mit $Q \neq 0$. Dann ist t eine Nullstelle des Polynoms $F(X) := P(X) - s \cdot Q(X) \in K'[X]$. Wir werden zeigen, dass dieses Polynom nicht identisch verschwindet. Sei dafür $b \in K$ der höchste nicht-verschwindende Koeffizient von $Q(X)$, und $a \in K$ der Koeffizient derselben Potenz von X in $P(X)$. Wenn $F(X)$ verschwindet, muss $a - sb = 0$ sein, also $s = a/b \in K$, im Widerspruch zur Annahme. Da $F(X)$ nicht verschwindet, ist t algebraisch über K'. Wegen $s \in K(t)$ gilt nun $L = K(s,t) = K'(t)$. Nach einem Satz der Vorlesung ist also L/K' eine algebraische Erweiterung.

   Wäre auch K'/K eine algebraische Erweiterung, so wäre nach einem Satz der Vorlesung ebenso L/K algebraisch. Aber $t \in L$ ist nicht algebraisch über K. Somit ist K'/K transzentent, wie zu zeigen war. Insbesondere ist das Erzeugende s transzendent über K.

   (b) Ist $s \in K$, so müssen P und Q konstant sein. In diesem Fall ist $[L/K(s)] = [L/K] = \infty$. Sei also $s \notin K$. Die obige Überlegung zeigt dann genauer, daß

$\deg(F) = \deg(Q)$ ist, falls $\deg(Q) \geqslant \deg(P)$ ist. In dem Fall $\deg(Q) < \deg(P)$ gilt dagegen offensichtlich $\deg(F) = \deg(P)$. Also ist $\deg(F)$ stets das Maximum der Grade von P und von Q. Wir werden zeigen, dass F irreduzibel in $K(s)[X]$ ist. Dann ist es bis auf einen Faktor in $K(s)^\times$ das Minimalpolynom von t über $K(s)$, und sein Grad ist gleich dem gesuchten Körpergrad $[L/K(s)]$.

Da s transzendent über K ist, können wir es für die folgende Überlegung als formale Unbestimmte auffassen. Nach Konstruktion liegt F in $K[s, X]$, was wir als Polynomring in zwei unabhängigen Variablen auffassen können. Dieser hat eindeutige Primfaktorzerlegung (siehe Algebra I). Es genügt daher zu beweisen, daß F als Element von $K[s, X]$ irreduzibel ist. Da F linear in s ist, kann es in $K[s, X]$ höchstens einen in s konstanten Faktor abspalten. Da aber P und Q als teilerfremd vorausgesetzt wurden, ist auch das nicht möglich.

(c) Betrachte zuerst eine beliebige Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. Dann ist $ct + d \neq 0$ und folglich $s := \frac{at+b}{ct+d} \in L$ wohldefiniert. Wegen $ad - bc \neq 0$ sind die Polynome $aX + b$ und $cX + d$ teilerfremd und mindestens eines hat den Grad 1. Nach Teil (b) ist daher $[K(t)/K(s)] = 1$ und somit $K(s) = K(t)$. Insbesondere ist s transzendent über K, und somit für jede rationale Funktion $f \in K(X)$ das Element $f(s) \in K(t)$ wohldefiniert. Also ist $K(t) \to K(t)$, $f(t) \mapsto f(s)$ ein wohldefinierter Körperhomomorphismus. Wegen $K(s) = K(t)$ ist dieser surjektiv und folglich bijektiv. Ausserdem ist er auf allen Konstanten in K die Identität. Dies zeigt die eine Richtung der Behauptung.

Für die andere Richtung betrachte einen beliebigen Automorphismus φ von L mit $\varphi|_K = \mathrm{id}_K$. Schreibe $s := \varphi(t) = P(t)/Q(t)$ wie in (b). Die Surjektivität von φ impliziert $L = K(s)$, also $[L/K(s)] = 1$, und aus (b) folgt, dass P und Q höchstens linear sind. Folglich ist $s = \frac{at+b}{ct+d}$ für gewisse $a, b, c, d \in K$. Wegen $L = K(s)$ ist s auch nicht konstant; daraus folgt $ad - bc \neq 0$. Da φ ein Körperhomomorphismus mit $\varphi|_K = \mathrm{id}_K$ ist, folgt nun $\varphi(f(t)) = f(s)$ für alle $f \in K(X)$. Also hat φ die gesuchte Form.