Lösungen zu Übungsblatt 10
Modul Algebra-2, SoSe 2006

(29/30) (a) Sei $L := \mathbb{Q}[\sqrt{p}]$. Wir wollen zeigen, dass $f := x^2 - q$ unzerlegbar in $L[x]$ ist. Wenn f nicht unzerlegbar in $L[x]$ ist, so muss es eine Nullstelle $a + b\sqrt{p}$ in L haben. Dann gilt: $q = (a + b\sqrt{p})^2 = (a^2 + b^2 p) + 2ab\sqrt{p}$. Da $(1, \sqrt{p})$ eine $\mathbb{Q}$-Basis von L ist, folgt u.a. $a^2 + b^2 p = q$. Nun gibt es folgende Fälle zu unterscheiden:

(i) $b = 0$: Dann ist $a^2 = q$. Somit liegt ein Widerspruch zur Voraussetzung, dass q prim ist, vor.

(ii) $b \neq 0$: Falls $a = 0$ folgt $b^2 p = q$, was wiederum ein Widerspruch dazu ist, dass q prim ist. Falls $a \neq 0$ folgt $a^2 + b^2 p = q$ und somit (vgl. oben) müsste aber auch $2ab\sqrt{p} = 0$ gelten, was wenn $a, b \neq 0$ nicht möglich ist.

Also ist f unzerlegbar. □.

(b) Wir wenden den Satz vom primitiven Element (15.5) an um zu zeigen, dass $L[\sqrt{q}] = \mathbb{Q}[\sqrt{p} + \sqrt{q}]$ ist. Das hier betrachtete Szenario ist

$$a := a_1 := \sqrt{p}, a_2 := -\sqrt{p}, b := b_1 := \sqrt{q}, b_2 := -\sqrt{q}.$$

Offensichtlich sind $\mathrm{MiPo}_{\mathbb{Q}}(a)$ und $\mathrm{MiPo}_{\mathbb{Q}}(b)$ ohne mehrfache Nullstellen im ZK und $|\mathbb{Q}| = \infty$. Nun müssen wir ein passendes $c \neq 0$ wählen, so dass $c \neq \dfrac{a - a_i}{b - b_j}$ für $i, j \in \{1, 2\}$. Zu betrachtende Fälle sind hier nur $i = 1, j = 2$ und $i = 2, j = 2$, da für $j = 1$ der Nenner des Bruches null wird, der Ausdruck also insbesondere ungleich c ist. Für $i = 1, j = 2$ muss gelten $c \neq \dfrac{a - a}{b - b_2} = 0$ und für $i = 2, j = 2$ gilt $c \neq \dfrac{\sqrt{p} + \sqrt{p}}{\sqrt{q} + \sqrt{q}} = 2\dfrac{\sqrt{p}}{\sqrt{q}}$. Da $\sqrt{p}, \sqrt{q} > 0$, ist $c = -1$ eine mögliche Wahl, und damit $\mathbb{Q}[\sqrt{p}, \sqrt{q}] = \mathbb{Q}[\sqrt{p} - c\sqrt{q}] = \mathbb{Q}[\sqrt{p} + \sqrt{q}]$. □

(c) Es gilt nach Satz 14.10 und (a),(b): $[\mathbb{Q}[\sqrt{p} + \sqrt{q}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{p}, \sqrt{q}] : \mathbb{Q}[\sqrt{p}]] \cdot [\mathbb{Q}[\sqrt{p}] : \mathbb{Q}] = 4$, also hat das Minimalpolynom den Grad 4. Betrachte mit $\alpha := \sqrt{p} + \sqrt{q}$: $\alpha^2 = (p + q) + 2\sqrt{p}\sqrt{q}$ und $(\alpha^2 - (p + q))^2 = 4pq$. Also ist $(x^2 - (p + q))^2 - 4pq$ ein über $\mathbb{Q}$ unzerlegbares Polynom vom Grad 4 in $\mathbb{Q}[x]$, welches $\alpha = \sqrt{p} + \sqrt{q}$ als Nullstelle hat. Also ist $f = \mathrm{MiPo}_Q(\sqrt{p} + \sqrt{q})$.

(d) Es ist $-(\sqrt{p} + \sqrt{q})$ ebenfalls eine Nullstelle von f, da f biquadratisch ist. Somit ist $(x - (\sqrt{p} + \sqrt{q}))(x + (\sqrt{p} + \sqrt{q})) = x^2 - 2\sqrt{p}\sqrt{q} - (p + q)$ quadratischer Faktor in f. Mit Polynomdivision folgt:

$$f : (x^2 - 2\sqrt{p}\sqrt{q} - (p + q)) = x^2 + 2\sqrt{p}\sqrt{q} - (p + q)$$

$$= (x - (\sqrt{p} - \sqrt{q}))(x + (\sqrt{p} - \sqrt{q})).$$

Also sind die Nullstellen von f: $(\sqrt{p} + \sqrt{q}), -(\sqrt{p} + \sqrt{q}), (\sqrt{p} - \sqrt{q})$ und $-(\sqrt{p} - \sqrt{q})$.

(e) Eine Primzerlegung in $(\mathbb{Q}[\sqrt{p}])[x]$ ist: $(x^2 - 2\sqrt{p}\,x + (p - q))(x^2 + 2\sqrt{p}\,x + (p - q))$ und eine Primzerlegung in $(\mathbb{Q}[\sqrt{q}])[x]$ ist: $(x^2 - 2\sqrt{q}\,x - (p - q))(x^2 + 2\sqrt{q}\,x - (p - q))$. Beide erhält man durch "geschickte" Multiplikation der Linearfaktoren von f, welche nach (a) jeweils nicht in $(\mathbb{Q}[\sqrt{p}])[x]$ und $(\mathbb{Q}[\sqrt{q}])[x]$ liegen, womit die Unzerlegbarkeit der Faktoren in beiden Zerlegungen folgt.

(31) (a) Wir zeigen, dass $\Pi : \mathrm{Aut}_K(L) \to S_n, \sigma \mapsto \sigma|_{N_f}$ ein wohldefinierter Gruppenmorphismus ist. Betrachte $\tau := \sigma|_{N_f}$ und $N_f = \{\alpha_1, \ldots, \alpha_n\}$. Sei o.E. S_n die Gruppe der Permutationen von N_f. Dann ist $\tau(\alpha_k) \in N_f, k \in \{1, \ldots, n\}$, da für $f = \sum_{i=0}^{d} a_i x^i$ gilt: $f(\tau(\alpha_k)) = \sum_{i=0}^{d} a_i \tau(\alpha_k)^i = 0$, also gilt $\tau(\alpha_k) \in N_f$. Da σ bijektiv ist folgt somit $\tau \in S_n$, also ist Π wohldefiniert. Ausserdem gilt offensichtlich $\Pi(\sigma_1 \circ \sigma_2) = (\sigma_1 \circ \sigma_2)|_{N_f} = \sigma_1|_{N_f} \circ \sigma_2|_{N_f} = \Pi(\sigma_1) \circ \Pi(\sigma_2)$, daher ist Π Gruppenmorphismus. □

(b) Sei $L = K[N_f]$. Um zu beweisen, dass Π in diesem Fall injektiv ist, betrachten wir $\ker \Pi$ und zeigen, dass dieser nur die Identität enthält. $\{id_L\} \subseteq \ker \Pi$ ist klar, da $id_L|_{N_f} = id_{N_f}$. Aber es gilt auch $\ker \Pi \subseteq \{id_L\}$, denn: Sei $\sigma \in \ker \Pi$, also $\sigma|_{N_f} = id_{N_f}$. Dann gilt für alle $g = \sum_{i=1}^{d} a_i \prod_{j=1}^{n} \alpha_j^{e_{i,j}} \in L : \sigma(g) = \sum_{i=1}^{d} a_i \prod_{j=1}^{n} \sigma(\alpha_j)^{e_{i,j}} = g = id_L(f)$. Also ist $\sigma = id_L$. □

(32) (a) Wir zeigen: $\mathbb{Q}[\zeta] \cap \mathbb{R} = \mathbb{Q}[a_1]$: Es ist $\zeta\bar{\zeta} = |\zeta| = 1$, also ist $\bar{\zeta} = \zeta^{-1}$ und somit $a_1 = \zeta^1 + \zeta^{-1} = 2Re(\zeta) \in \mathbb{R}$. Damit ist $Re(\zeta) \in \mathbb{Q}[a_1]$. Ausserdem ist $a_1 \in \mathbb{Q}[\zeta]$, da $\zeta^{-1} \in \mathbb{Q}[\zeta]$. Also gilt: $\mathbb{Q}[a_1] \subseteq \mathbb{Q}[\zeta] \cap \mathbb{R}$. Da wegen $\zeta^{-1} = \bar{\zeta} \in \mathbb{Q}[\zeta]$ auch folgt, dass $\mathbb{Q}[\zeta] \cap \mathbb{R} = \mathbb{Q}[Re(\zeta)] \subseteq \mathbb{Q}[a_1]$, gilt auch die Rückrichtung.
Jetzt bleibt noch zu zeigen, dass $\mathbb{Q}[a_1]$ ZK von f in $\mathbb{C}$ ist. Dazu zeigen wir, dass $a_2, a_4 \in \mathbb{Q}[a_1]$: Sei $\zeta := a + ib; a, b \in \mathbb{R}$. Jetzt gilt $a_2 = \zeta^2 + \zeta^{-2} = \zeta^2 + \bar{\zeta}^2 = 2a^2 - 2b^2 = 2(Re(\zeta)^2 - Im(\zeta)^2) \in \mathbb{R}$ und $a_4 = 2a^4 - 12a^2b^2 + 2b^4 \in \mathbb{R}$. Durch sukzessive Anwendung des Satzes 14.10 erhalten wir die Behauptung: Es ist $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 6$, da $\deg \mathrm{MiPo}_Q(\zeta) = 6$. Ferner ist $[\mathbb{Q}[a_1] : \mathbb{Q}] = 3$, da f unzerlegbar über $\mathbb{Q}$ ist. Somit muss also gelten

$$[\mathbb{Q}[\zeta] : \mathbb{Q}] = 6 = [\mathbb{Q}[\zeta] : \mathbb{Q}[a_1]] \cdot [\mathbb{Q}[a_1] : \mathbb{Q}] = x \cdot 3.$$

Also ist $x = [\mathbb{Q}[\zeta] : \mathbb{Q}[a_1]] = 2$. Da $a_1, a_2, a_4 \in \mathbb{R}$ und $\zeta \notin \mathbb{R}$ gilt, dass $[\mathbb{Q}[\zeta] : \mathbb{Q}[a_1, a_2, a_4]] > 1$ ist. Nun gilt aber auch

$$[\mathbb{Q}[\zeta] : \mathbb{Q}] = [\mathbb{Q}[\zeta] : \mathbb{Q}[a_1, a_2, a_4]][\mathbb{Q}[a_1, a_2, a_4] : \mathbb{Q}[a_1]][\mathbb{Q}[a_1] : \mathbb{Q}]$$

$$= 6 = c \cdot [\mathbb{Q}[a_1, a_2, a_4] : \mathbb{Q}[a_1]] \cdot 3$$

mit einem $c > 1$.
Also muss $[\mathbb{Q}[a_1, a_2, a_4] : \mathbb{Q}[a_1]] = 1$ sein und somit $\mathbb{Q}[a_1, a_2, a_4] = \mathbb{Q}[a_1]$. □

(b) Betrachte $f = x^3 - 3x^3 + 1 = (x - a_1)(x - a_2)(x - a_3)$. ZK von f ist $\mathbb{Q}[a_1]$, also ist $[\mathbb{Q}[a_1] : \mathbb{Q}] = 3$. Nun brauchen wir noch zwei Erweiterungen vom Grad 2. Betrachte $g = x^2 - 3$ und $h = x^2 - 5$. Wir wissen bereits aus der Vorlesung, dass $\mathbb{Q}[\sqrt{3}]$ ZK von g und $\mathbb{Q}[\sqrt{5}]$ ZK von h ist. Ferner gilt nach Aufgabe (29/30): $[\mathbb{Q}[\sqrt{3}, \sqrt{5}] : \mathbb{Q}] = 4$. Nach der Dimensionsformel (14.10) gilt also $[\mathbb{Q}[\sqrt{3}, \sqrt{5}, a_1] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}, \sqrt{5}] : \mathbb{Q}[a_1]][\mathbb{Q}[a_1] : \mathbb{Q}] = c \cdot 3$. Es gilt aber auch $[\mathbb{Q}[\sqrt{3}, \sqrt{5}, a_1] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}, \sqrt{5}, a_1] : \mathbb{Q}[\sqrt{3}, \sqrt{5}]][\mathbb{Q}[\sqrt{3}, \sqrt{5}] : \mathbb{Q}] = d \cdot 4$. Also ist $[\mathbb{Q}[\sqrt{3}, \sqrt{5}, a_1] : \mathbb{Q}] \geq kgV(3, 4) = 12$. Da $\mathbb{Q}[\sqrt{3}, \sqrt{5}, a_1]$ der ZK von $x^2 - 3$ ueber $\mathbb{Q}[a_1, \sqrt{5}]$ ist und somit höchstens Grad 2 ueber $\mathbb{Q}[a_1, \sqrt{5}]$ hat, und die dazu analoge Aussage auch für $\mathbb{Q}[\sqrt{3}, a_1]$ über $\mathbb{Q}[a_1]$ gilt, ist der Grad des ZK des Polynoms

$$l := fgh = x^7 - 11x^5 + x^4 + 39x^3 - 8x^2 - 45x + 15$$

genau 12.