ulm university universität uulm

Musterlösung zur Probeklausur zur Algebra

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 130 Punkte, 100 Punkte= 100 %, keine Abgabe

1. Es sei L der Zerfällungskörper von $f(X) = X^3 - 2$ über $\mathbb{Q}$.

   (a) Gib eine Basis des Vektorraums L über $\mathbb{Q}$ an.

   Das Polynom f hat Nullstellen in $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$ und $\sqrt[3]{2}\zeta_3^2$ mit $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$, einer dritten Einheitswurzel. Damit ist der Zerfällungskörper von f über $\mathbb{Q}$ durch $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ gegeben und eine Basis des Vektorraums L über $\mathbb{Q}$ wegen $\zeta^2 = -\zeta - 1$ etwa durch

   $$\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \sqrt[3]{2}\zeta, \sqrt[3]{2}^2\zeta\}.$$

   (b) Finde ein $\sigma \in G(L/\mathbb{Q})$ mit $|\langle\sigma\rangle| = 3$ und beschreibe $\sigma(\vec{b})$ für die in Teilaufgabe a) gefundenen Basiselemente $\vec{b}$.

   Wir wählen für eine Untergruppe der Ordnung 3 die Abbildung

   $$\sigma_{0,1} \colon \zeta_3 \to \zeta_3, \ \sqrt[3]{2} \to \sqrt[3]{2}\zeta_3$$

   als Erzeuger, die die Gruppe $\langle\sigma_{0,1}\rangle = \{\sigma_{0,1}, \sigma_{0,2}, id\}$ mit $\sigma_{0,2} \colon \zeta_3 \to \zeta_3, \ \sqrt[3]{2} \to \sqrt[3]{2}\zeta_3^2$ erzeugt. Für die sechs Basiselemente gilt dann

   $$\begin{aligned}
   \sigma_{0,1}(\vec{b}_1) &= \sigma_{0,1}(1) = 1\\
   \sigma_{0,1}(\vec{b}_2) &= \sigma_{0,1}(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3\\
   \sigma_{0,1}(\vec{b}_3) &= \sigma_{0,1}(\sqrt[3]{2}^2) = \sqrt[3]{2}^2\zeta_3^2\\
   \sigma_{0,1}(\vec{b}_4) &= \sigma_{0,1}(\zeta_3) = \zeta_3\\
   \sigma_{0,1}(\vec{b}_5) &= \sigma_{0,1}(\sqrt[3]{2}\zeta_3) = \sqrt[3]{2}\zeta_3^2\\
   \sigma_{0,1}(\vec{b}_6) &= \sigma_{0,1}(\sqrt[3]{2}^2\zeta_3) = \sqrt[3]{2}^2.
   \end{aligned}$$

   (8 Punkte)

2. Es sei $f \in \mathbb{Q}[X]$, $\deg(f) = 5$ und $G(f, \mathbb{Q}) \cong \gamma_5$. Weiter sei L ein Zerfällungskörper von f über $\mathbb{Q}$. Es sei mit $\alpha_j \in L$

   $$f(X) = \prod_{j=1}^{5}(X - \alpha_j).$$

   Die Folge der Zwischenkörper K_j sei durch $K_0 = \mathbb{Q}$ und $K_j = K_{j-1}(\alpha_j)$ für $1 \leq j \leq 5$ definiert.

   (a) Bestimme die Grade $[K_j \colon K_{j-1}]$ der Körpererweiterungen.

   Wegen $G(f, \mathbb{Q}) \cong \gamma_5$ sind die einzelnen Grade gerade die Zahlen von 1 bis 5. Es gilt $[K_1 \colon \mathbb{Q}] = 5$, $[K_2 \colon K_1] = 4$, $[K_3 \colon K_0] = 3$, $[K_4 \colon K_3] = 2$ und $[K_5 \colon K_4] = 1$.

   (b) Ist f über $\mathbb{Q}$ bzw. über K_2 auflösbar?

   Wegen $G(f, \mathbb{Q}) \cong \gamma_5$ und der Nichtausflösbarkeit von γ_5 ist auch f über $\mathbb{Q}$ nicht auflösbar. Über K_2 ist f auflösbar. (10 Punkte)

3. Bestimme das zehnte Kreisteilungspolynom $\Phi_{10}(X)$.

   Wegen $\varphi(10) = 4$ muss dieses Polynom vom Grad 4 sein. Wir bestimmen

$$\begin{aligned}\Phi_{10}(X) &= \frac{X^{10}-1}{\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_5(X)} = \frac{X^{10}-1}{(X-1)\cdot(X+1)\cdot(X^4+X^3+X^2+X+1)} \\ &= X^4 - X^3 + X^2 - X + 1\end{aligned}$$

(6 Punkte)

4. Bestimme sämtliche $d \in \mathbb{N}$, für welche der Körper $GF(3^6)$ die d- ten Einheitswurzeln enthält.

   Wir betrachten dazu das Polynom $p(x) = x^{3^6} - x = x(x^{3^6-1} - 1)$. Über das Polynom $x^{3^6-1} - 1$ erhalten wir d- te Einheitswurzeln, sofern d ein Teiler des Exponenten $3^6 - 1 = 728 = 2^3 \cdot 7 \cdot 13$ ist. Folglich gilt $d \in \{2, 4, 7, 8, 13, 14, 26, 28, 52, 56, 91, 104, 182, 364, 728\}$. (8 Punkte)

5. Es seien p eine Primzahl, $\zeta_p = e^{\frac{2\pi i}{p}}$ und $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$. Weiter sei

$$G(p) = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} : r \in (\mathbb{Z}/p\mathbb{Z})^*,\ s \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

   Zeige:

   (a) $G(p)$ ist eine Gruppe bzgl. der Matrixmultiplikation.

   Die Menge $G(p)$ ist wegen $E_2 \in G(p)$ nichtleer. Mit

$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in G(p)$$

   ist auch

$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix} \in G(p),$$

   da ebenfalls $r^{-1} \in (\mathbb{Z}/p\mathbb{Z})^*$ und $-r^{-1}s \in \mathbb{Z}/p\mathbb{Z}$ gelten. Mit

$$\begin{pmatrix} r_1 & s_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} r_2 & s_2 \\ 0 & 1 \end{pmatrix} \in G(p)$$

   gilt dann

$$\begin{pmatrix} r_1 & s_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} r_2 & s_2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} r_1 r_2^{-1} & -r_1 r_2^{-1} s_2 + s_1 \\ 0 & 1 \end{pmatrix} \in G(p),$$

   da wieder $r_1 r_2^{-1} \in (\mathbb{Z}/p\mathbb{Z})^*$ und $-r_1 r_2^{-1} s_2 + s_1 \in \mathbb{Z}/p\mathbb{Z}$ gelten. Also ist $G(p)$ eine Gruppe bzgl. der Matrixmultiplikation.

   (b) $G(L/\mathbb{Q}) \cong G(p)$

   In der Galoisgruppe $G(L/\mathbb{Q})$ liegen die Automorphismen

$$\sigma_{r,s} \colon \zeta_p \to \zeta_p^k,\ \sqrt[p]{2} \to \sqrt[p]{2} \cdot \zeta_p^l$$

   mit $r \in (\mathbb{Z}/p\mathbb{Z})^*$ und $s \in \mathbb{Z}/p\mathbb{Z}$ sowie $k \in r$ und $l \in s$. Wir betrachten die Wirkung der Komposition $\tau = \sigma_{r_1,s_1} \circ \sigma_{r_2,s_2}$ auf ζ_p und $\sqrt[p]{2}$. Es gilt

$$\tau(\zeta_p) = \sigma_{r_1,s_1} \circ \sigma_{r_2,s_2}(\zeta_p) = \sigma_{r_1,s_1}(\sigma_{r_2,s_2}(\zeta_p)) = \sigma_{r_1,s_1}(\zeta_p^{k_2}) = (\zeta_p^{k_2})^{k_1} = \zeta_p^{k_1 k_2},$$

   also $\sigma_{r_1,s_1} \circ \sigma_{r_2,s_2}(\zeta_p) = \zeta_p^{r_1 r_2}$.

Weiter ist

$$\begin{aligned}\tau(\sqrt[p]{2}) &= \sigma_{r_1,s_1}\circ\sigma_{r_2,s_2}(\sqrt[p]{2}) = \sigma_{r_1,s_1}(\sigma_{r_2,s_2}(\sqrt[p]{2})) = \sigma_{r_1,s_1}(\sqrt[p]{2}\cdot\zeta_p^{l_2}) = \sqrt[p]{2}\cdot\zeta_p^{l_1}\cdot(\zeta_p^{l_2})^{k_1} \\ &= \sqrt[p]{2}\cdot\zeta_p^{l_1+k_1l_2},\end{aligned}$$

und somit $\sigma_{r_1,s_1}\circ\sigma_{r_2,s_2}(\sqrt[p]{2}) = \sqrt[p]{2}\cdot\zeta_p^{s_1+r_1s_2}$.
Analog dazu gilt für die gegebene Matrizengruppe

$$\begin{pmatrix} r_1 & s_1 \\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix} r_2 & s_2 \\ 0 & 1\end{pmatrix} = \begin{pmatrix} r_1r_2 & r_1s_2+s_1 \\ 0 & 1\end{pmatrix},$$

womit ein Isomorphismus $G(L/\mathbb{Q})\to G(p)$ über

$$\sigma_{r,s}\to\begin{pmatrix} r & s \\ 0 & 1\end{pmatrix}$$

gegeben ist. (11 Punkte)

6. Gib die Definition folgender Begriffe an:

   (a) Kompositionsreihe

   Eine Normalreihe der Form $G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_k = \{1_G\}$ heißt Kompositionsreihe von G, wenn die Faktoren N_{i-1}/N_i für $1\le i\le k$ einfach sind.

   (b) Kommutatoruntergruppe

   Die von allen Kommutatoren erzeugte Untergruppe $[G\colon G] := \langle\{[g,h]\colon g,h\in G\}\rangle$ heißt Kommutatorgruppe von G.

   (c) Galoiserweiterung

   Eine endliche Erweiterung L/K heißt Galoiserweiterung, wenn die Ordnung der Galoisgruppe mit dem Grad der Körpererweiterung übereinstimmt, also $|G(L/K)| = [L\colon K]$.

   (d) Diskriminante

   Unter der Diskriminante von $f\in R[X]$ für einen Ring R mit $f(X) = c\cdot(X-\alpha_1)\cdots(X-\alpha_n)$ versteht man den Ausdruck

   $$D(f) = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2.$$

   (e) freier Modul

   Ein R- Modul M heißt freier Modul über R, wenn M eine Basis besitzt. (20 Punkte)

7. Es sei $f(X) = X^{15}+21X^{10}-3X^5+2\in\mathbb{Q}[X]$. Zeige, dass f auflösbar ist.

   Mit der Substitution $Y = X^5$ ergibt sich $f(Y) = Y^3+21Y^2-3Y+2$. Mittels einer weiteren Substitution $Y = Z-\frac{21}{3} = Z-7$ erhalten wir die Gleichung $Z^3-150Z+709$. Die Lösungen dieser Gleichung sind aber über die Formel von Cardano

   $$x = \sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

   durch Radikale darstellbar. Damit ist aber auch die ursprüngliche Gleichung durch Radikale auflösbar. (6 Punkte)

8. Es sei $R = K[X_1, X_2, X_3]$ der Ring der Polynome in drei Unbestimmten über einem Körper K. Stelle das symmetrische Polynom $f = X_1^3 + X_2^3 + X_3^3$ als Polynom in den elementarsymmetrischen Polynomen $s_0, s_1, s_2, s_3 \in R$ mit Koeffizienten aus K dar.

   Es ist

$$\begin{aligned} s_1^3 &= (X_1 + X_2 + X_3)^3 \\ &= X_1^3 + X_2^3 + X_3^3 + 3X_1^2X_2 + 3X_1^2X_3 + 3X_1X_2^2 + 3X_1X_3^2 + 3X_2^2X_3 + 3X_2X_3^2 + 6X_1X_2X_3. \end{aligned}$$

   Weiter gilt

$$\begin{aligned} s_1s_2 &= (X_1 + X_2 + X_3) \cdot (X_1X_2 + X_1X_3 + X_2X_3) \\ &= X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2 + 3X_1X_2X_3. \end{aligned}$$

   Daraus ergibt sich schließlich

$$f = s_1^3 - 3s_1s_2 + 3s_3$$

   mit $s_3 = X_1X_2X_3$. (8 Punkte)

9. Es sei L/K eine Galoiserweiterung und Z ein Zwischenkörper.
   Formuliere und beweise eine Bedingung, unter der jeder K- Isomorphismus von Z ein Automorphismus ist.

   Die gesuchte Bedingung ist, dass die Körpererweiterung Z/K ebenfalls galoissch ist.
   "$\Rightarrow$":
   Es sei Z/K galoissch. Damit ist Z der Zerfällungskörper eines Polynoms $f \in K[X]$, also gilt $Z = K(\alpha_1, \ldots, \alpha_n)$ mit den Nullstellen $\alpha_1, \ldots, \alpha_n$ von f in Z. Ein $\sigma \in G(L/K)$ permutiert also diese Nullstellen, und insbesondere gilt $\sigma(\alpha_i) \in K(\alpha_1, \ldots, \alpha_n) = Z$ für alle $i = 1 \ldots, n$ und damit ist $\sigma(Z) \subset Z$. Da jeder K- Homomorphismus $\varphi\colon L \to L$ bereits ein K- Isomorphismus ist, folgt die Behauptung.
   "$\Leftarrow$":
   Es sei nun jeder K- Isomorphismus von Z ein Automorphismus, also sei für alle $\sigma \in G(L/K)$ die Bedingung $\sigma(Z) = Z$ erfüllt. Damit lässt sich σ zu einem K- Automorphismus von Z einschränken, womit es einen Gruppenhomomorphismus

$$\varphi\colon G(L/K) \to G(Z/K), \quad \sigma \to \sigma_{|Z}$$

   mit $\operatorname{Kern}\varphi = \{\sigma \in G(L/K)\colon \sigma_{|Z} = id\} = G(L/Z)$ gibt. Insbesondere ist $G(L/Z)$ als Kern eines Homomorphismus ein Normalteiler in $G(L/K)$. Es folgt mit dem Satz von Lagrange und dem Homomorphiesatz

$$\begin{aligned} [L\colon K] &= |G(L/K)| = |G(L/K)/G(L/Z)| \cdot |G(L/Z)| = |\operatorname{Bild}\varphi| \cdot |G(L/Z)| \\ &\leq |G(Z/K)| \cdot |G(L/Z)| \leq |[Z\colon K] \cdot [L\colon Z] = [L\colon K], \end{aligned}$$

   weswegen überall die Gleichheit stehen muss. Insbesondere gilt dann auch $|G(Z/K)| = [Z\colon K]$, womit Z/K galoissch ist. (8 Punkte)

10. Bestimme in den folgenden Körpererweiterungen L/K für die angegebenen Elemente $\alpha \in L$ das Minimalpolynom.

    (a) $L = \mathbb{C}$, $K = \mathbb{R}$ und $\alpha = \sqrt{7}$

    Wegen $\sqrt{7} \in \mathbb{R}$ gilt $m_{\mathbb{R}}(\sqrt{7}, X) = X - \sqrt{7}$.

(b) $L = \mathbb{C}$, $K = \mathbb{Q}$ und $\alpha = \frac{-1+\sqrt{3}i}{2}$

Wir wissen, dass $\alpha = \zeta_3$, einer dritten Einheitswurzel, gilt und somit Nullstelle des irreduziblen dritten Kreisteilungspolynoms ist. Damit gilt $m_{\mathbb{Q}}(\alpha, X) = \Phi_3(X) = X^2 + X + 1$. (8 Punkte)

11. Es sei $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

(a) Zeige, dass L Zerfällungskörper von $f(X) = X^4 - 2$ über $\mathbb{Q}$ ist.

Indem wir das Polynom f über $\mathbb{C}$ zerlegen, erhalten wir

$$f = X^4 - 2 = (X^2 + \sqrt{2}) \cdot (X^2 - \sqrt{2}) = (X + i\sqrt[4]{2}) \cdot (X - i\sqrt[4]{2}) \cdot (X + \sqrt[4]{2}) \cdot (X - \sqrt[4]{2}).$$

Also ist $L = \mathbb{Q}(\sqrt[4]{2}, i)$ Zerfällungskörper von f über $\mathbb{Q}$.

(b) Bestimme $[L\colon \mathbb{Q}]$.

Nach dem Eisensteinkriterium ist f über $\mathbb{Q}$ mit $p = 2$ irreduzibel. Damit gilt $f = m_{\mathbb{Q}}(\sqrt[4]{2}, X)$ und folglich $[\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}] = 4$. Weiter ist $X^2 + 1$ über $\mathbb{Q}(\sqrt[4]{2})$ irreduzibel, weil das Polynom $X^2 + 1 = (X + i) \cdot (X - i)$ die beiden Nullstellen $\pm i \notin \mathbb{Q}(\sqrt[4]{2})$ besitzt.
Somit gilt $m_{\mathbb{Q}(\sqrt[4]{2})}(i, X) = X^2 + 1$ und folglich ist $[L\colon \mathbb{Q}] = [L\colon \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}] = 2 \cdot 4 = 8$.

(c) Zeige, dass $L/\mathbb{Q}$ eine Galoiserweiterung ist und bestimme die Galoisgruppe $G(L/\mathbb{Q})$.

Die Erweiterung ist mit $[L\colon \mathbb{Q}] = 8$ endlich und normal, da L Zerfällungskörper von f über $\mathbb{Q}$ ist. Die vier Nullstellen $\pm\sqrt[4]{2}$ und $\pm\sqrt[4]{2}i$ sind wegen $\deg(f) = 4$ auch alle Nullstellen von f. Damit sind alle Nullstellen von f in L verschieden, womit die Erweiterung auch separabel ist, weswegen eine Galoiserweiterung vorliegt.
Wegen $m_{\mathbb{Q}(\sqrt[4]{2})}(i, X) = X^2 + 1$ gibt es ein Element $\tau \in G(L/\mathbb{Q}(\sqrt[4]{2})) \subset G(L/\mathbb{Q})$ mit $\tau(i) = -i$.
Wegen $\tau \in G(L/\mathbb{Q}(\sqrt[4]{2}))$ ist $\tau_{|_{\mathbb{Q}(\sqrt[4]{2})}} = id$, also $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$.
Wegen $[L\colon \mathbb{Q}] = [L\colon \mathbb{Q}(i)] \cdot [\mathbb{Q}(i)\colon \mathbb{Q}] = 8$ und $[\mathbb{Q}(i)\colon \mathbb{Q}] = 2$ gilt $[L\colon \mathbb{Q}(i)] = [\mathbb{Q}(\sqrt[4]{2}, i)\colon \mathbb{Q}] = 4$.
Daher ist $\deg(m_{\mathbb{Q}(i)}(\sqrt[4]{2}, X)) = 4$, weswegen $m_{\mathbb{Q}(i)}(\sqrt[4]{2}, X) = X^4 - 2 = f$ gilt.
Nun ist auch $\sqrt[4]{2}$ Nullstelle von $f = m_{\mathbb{Q}(i)}(\sqrt[4]{2}, X)$, also gibt es ein $\sigma \in G(L/\mathbb{Q}(i)) \subset G(L/\mathbb{Q})$ mit $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. Analog gilt wegen $\sigma_{|_{\mathbb{Q}(i)}} = id$ auch $\sigma(i) = i$.
Dementsprechend ist nun $\{id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \subset G(L/\mathbb{Q})$. Berechnung der Wirkung der Abbildungen auf die Elemente $\sqrt[4]{2}$ und i zeigt, dass diese acht Element paarweise verschieden sind. Wegen $|G(L/K)| = 8$, ist dies dann bereits die Galoisgruppe.

(d) Bestimme zu sämtlichen Untergruppen H von $G(L/\mathbb{Q})$ die Fixkörper L^H.

Aufgrund der Struktur ist die Galoisgruppe zur Diedergruppe D_4 isomorph. Diese hat die nichttrivialen Untergruppen $U_1 = \{id, \sigma^2\}$, $U_2 = \{id, \tau\} = \langle\tau\rangle$, $U_3 = \{id, \sigma\tau\}$, $U_4 = \{id, \sigma^2\tau\}$, $U_5 = \{id, \sigma^3\tau\}$, die allesamt die Ordnung 2 besitzen, und $U_6 = \langle\sigma\rangle$, $U_7 = \{id, \sigma^2, \tau, \sigma^2\tau\}$ sowie $U_8 = \{id, \sigma^2, \sigma\tau, \sigma^3\tau\}$ mit Ordnung 4. Insbesondere ist $L^{G(L/\mathbb{Q})} = \mathbb{Q}$ und $L^{\{id\}} = L$. Es gilt

$$\mathbb{Q}(\sqrt{2}, i) \subset L^{U_1},\ \mathbb{Q}(\sqrt[4]{2}) \subset L^{U_2},\ \mathbb{Q}(\sqrt{2}i) \subset L^{U_3},\ \mathbb{Q}(\sqrt[4]{2}i) \subset L^{U_4},$$
$$\mathbb{Q}(\sqrt{2}i) \subset L^{U_5},\ \mathbb{Q}(i) \subset L^{U_6},\ \mathbb{Q}(\sqrt{2}) \subset L^{U_7},\ \mathbb{Q}(\sqrt{2}i) \subset L^{U_8}.$$

Wegen $[L^{U_i}\colon \mathbb{Q}] = |G(L/\mathbb{Q})|/|U_i|$ folgt für $i = 1, 2, 4, 6, 7, 8$ bereits die Gleichheit.
Für $i = 3, 5$ suchen wir noch ein $x \in L^{U_3}$ bzw. $x \in L^{U_5}$ mit $\deg(m_{\mathbb{Q}}(x)) = 4$. Mit $x_1 = (1+i)\sqrt[4]{2}$ ist $\mathbb{Q}(x_1) \subset L^{U_3}$ und mit $x_2 = (1-i)\sqrt[4]{2}$ dann $\mathbb{Q}(x_2) \subset L^{U_5}$. Somit haben wir jeweils ein solches Element, denn wegen $\mathbb{Q}(j, x_j) = L$ für $j = 1, 2$ und

$$8 = [\mathbb{Q}(i, x_j)\colon \mathbb{Q}] = [\mathbb{Q}(i, x_j)\colon \mathbb{Q}(x_j)] \cdot [\mathbb{Q}(x_j)\colon \mathbb{Q}] = 2[\mathbb{Q}(x_j)\colon \mathbb{Q}]$$

ist in der Tat $[\mathbb{Q}(x_j)\colon \mathbb{Q}] = 4$. Schließlich gilt $L^{U_3} = \mathbb{Q}((1 + i)\sqrt[4]{2})$ und $L^{U_5} = \mathbb{Q}((1 - i)\sqrt[4]{2})$.

(e) Welche der in Teilaufgabe d) bestimmten Fixkörper sind über $\mathbb{Q}$ galoisch?

Die Untergruppen U_6, U_7 und U_8 sind Normalteiler von $G(L/\mathbb{Q})$, da sie Index 2 besitzen, womit die Fixkörper $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}i)$ über $\mathbb{Q}$ galoissch sind.
Nachrechnen der Normalteilereigenschaft zeigt, dass auch U_1 ein Normalteiler ist, womit auch $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ galoissch ist. Nachrechnen zeigt auch, dass U_2, U_3, U_4 und U_5 keine Normalteiler sind, weswegen die zugehörigen Fixkörper über $\mathbb{Q}$ daher auch keine Galoiserweiterungen sind. Die trivialen Erweiterungen sind galoissch. (15 Punkte)

12. Es sei L/K eine Galoiserweiterung und $[L\colon K] = 15$. Weiter sei H eine Untergruppe von $G(L/K)$ mit $|H| = 5$. Es sei $\sigma \in H$. Für $\alpha \in L$ sei $\eta = \sum_{j=0}^{4} \sigma^j(\alpha)$.
Zeige, dass $[K(\eta)\colon K] \leq 3$ gilt.

Nachrichtlich: es sollte $\sigma \neq id$ vorausgesetzt werden.
Wegen $\sigma^5 = id$ folgt
$$\sigma(\eta) = \sum_{j=0}^{4} \sigma^{j+1}(\alpha) = \sum_{j=0}^{4} \sigma^j(\alpha) = \eta.$$
Damit ist $\eta \in L^H = L^{\langle\sigma\rangle}$ und $G(L/L^H) = H$. Wir erhalten $[L\colon L^H] = |H| = 5$. Nach dem Gradsatz gilt nun $[L\colon K] = [L\colon L^H] \cdot [L^H\colon K] = 15$, also $[L^H\colon K] = 3$. Wegen $\eta \in L^H$ gilt $K(\eta) \subset L^H$, und somit $[K(\eta)\colon K] \leq 3$. (8 Punkte)

13. Es sei $\mathcal{A}$ ein Ideal eines Rings R. Beweise, dass $\mathcal{A}$ genau dann ein freier R- Modul ist, wenn $\mathcal{A}$ ein Hauptideal ist, das von einem Nichtnullteiler erzeugt wird.

"$\Rightarrow$:"
Es sei $\mathcal{A}$ ein freier Modul, besitze also eine Basis, welche $\mathcal{A}$ erzeuge. In einem Ring R sind zwei Elemente r_1, r_2 aber stets linear abhängig, denn für $r_1, r_2 \neq 0$ ist $r_2 \cdot r_1 + (-r_1) \cdot r_2 = 0$ eine nichttriviale Darstellung der Null. Damit ist die Basis einelementig und somit $\mathcal{A}$ auch ein Hauptideal. Das Nullideal ist übrigens ebenfalls ein Hauptideal.
Es verbleibt noch die Nullteilerfreiheit zu zeigen. Wir nehmen an, es gebe einen Nullteiler $a \in R$ mit $a \neq 0$ und $ab = 0$ für $b \neq 0$. Es sei $I = (a)$ das von a erzeugte Ideal. Da $\{a\}$ wegen $ba = 0$ nicht linear unabhängig ist, ist $\{a\}$ keine Basis von I. Allerdings besitzt I eine Basis $\{r\}$ für ein $r \neq 0$ und wegen der linearen Unabhängigkeit ist r kein Nullteiler. Wegen $(r) = (a)$ ist aber $r = sa$ für ein $s \in R$, und damit gilt $rb = sab = s \cdot 0 = 0$, womit r eben doch ein Nullteiler ist, ein Widerspruch.
"$\Leftarrow$:"
Es sei nun $\mathcal{A}$ ein Hauptideal, welches von einem Nichtnullteiler $a \in R$ erzeugt wird. Wir haben also $\mathcal{A} = (a) = \{ra\colon r \in R\}$ vorliegen. Da a ein Nichtnullteiler ist, ist bereits $\{a\}$ eine Basis von $\mathcal{A}$, und folglich ist das Ideal $\mathcal{A}$ ein freier R- Modul. (8 Punkte)

14. Finde ein Erzeugendensystem des $\mathbb{Z}$- Moduls $\mathbb{Z}^2$, das nicht zu einer Basis verkleinert werden kann.

Betrachte etwa das Erzeugendensystem $\{(3,0), (2,0), (0,1)\}$ von $\mathbb{Z}^2$. Jede Verkleinerung führt zu einem Verlust der Basiseigenschaft. (6 Punkte)

Viel Erfolg!