Algebra – Freiwilliges Blatt 14 – Lösungsvorschlag

L/K ist galoissch, da $\mathrm{char}(K) = 0$.

A1 (a) Beh: Für $\sigma \in \mathrm{Aut}(L/K)$ gilt $\sigma(b) = b$.

Bew: Sei $\sigma \in \mathrm{Aut}(L/K)$ beliebig. Nach Blatt 13 A3b* ist $\{\sigma(a_1), \dots, \sigma(a_4)\}$ die Menge der Nullstellen von $\sigma(f)$. Da $f \in K[X]$ und $\sigma|_K = \mathrm{id}_K$ ist $\sigma(f) = f$, also $\{\sigma(a_1), \dots, \sigma(a_4)\} = \{a_1, \dots, a_4\}$.

Es folgt
$$\sigma(b) = \sigma(a_1^5 + a_2^5 + a_3^5 + a_4^5) = \sigma(a_1)^5 + \sigma(a_2)^5 + \sigma(a_3)^5 + \sigma(a_4)^5 = a_1^5 + a_2^5 + a_3^5 + a_4^5 = b.$$

Also ist $b \in \mathrm{Fix}(\mathrm{Aut}(L/K)) = K$ (Hauptsatz).

*) für $f \in L[X]$

(b) Nach Satz 3.6.5 gibt es genau $[K(a_1+a_2):K]$ viele Einbettungen von $K(a_1+a_2)$ in K^{alg}, die auf K die Identität sind. Jede solche lässt sich (nach Satz 3.4.8) zu einem $\sigma \in \mathrm{Aut}(K^{alg}/K)$ fortsetzen. (d.h. $\sigma|_{K(a_1+a_2)}$ ist die ursprgl. Einbettung von $K(a_1+a_2)$ in K^{alg})

Jedes solche σ bildet die Nullstellen von f auf die Nullstellen von f ab, d.h. $\sigma(a_1+a_2) = a_i + a_j$ für geeignete $i, j \in \{1,2,3,4\}$, $i \neq j$. Dafür gibt es (höchstens) 6 Möglichkeiten:

a_1+a_2, a_1+a_3, a_1+a_4,
a_2+a_3, a_2+a_4, a_3+a_4

Da $\sigma|_{K(a_1+a_2)}$ schon durch $\sigma(a_1+a_2)$ festgelegt wird gibt es höchstens 6 Einbettungen, d.h. $[K(a_1+a_2):K] \leq 6$.

Bem: Die Voraussetzung $\mathrm{char}(K) = 0$ ist nicht wirklich notwendig, wir haben sie nur benutzt um zu wissen, dass L/K separabel ist. Es gilt aber allgemein, dass der Zerfällungskörper eines Polynoms ohne doppelte Nullstellen separabel über dem Grundkörper ist.

A2 (a) Da der Zerfällungskörper von einem beliebigen Vielfachen $\lambda \cdot f$, $\lambda \in K$, ebenfalls L ist können wir o.E. annehmen, dass f normiert ist. Dann ist f das Minimalpolynom jeder seiner Nullstellen (da irreduzibel und normiert).

Nach A13 A3b ist $\{\sigma(a), \sigma(b), \sigma(c)\} = \{a,b,c\}$ für $\sigma \in Aut(L/K)$ und a,b,c die Nullstellen von f (möglicherweise $\#\{a,b,c\} < 3$).

Da $\sigma \in Aut(L/K)$ durch die Bilder von a,b,c eindeutig bestimmt ist, folgt $Aut(L/K) \leq Sym(\{a,b,c\}) \leq S_3$, also $Aut(L/K) \cong \{id\}$ oder $\cong S_2 = \mathbb{Z}/2$ oder $\cong \mathbb{Z}/3$ oder $\cong S_3$.

Da $\deg(f) = 3$ ist enthält K keine der Nullstellen von f (sonst wäre es nicht irreduzibel!)

Aber $L \supseteq K(a)$, dh. $[L:K] \geq [K(a):K] = 3$ und $\underset{\text{(da } L/K \text{ galoissch)}}{[L:K] = \# Aut(L/K)}$. Also folgt $Aut(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ oder $\cong S_3$.

(b) Für $Aut(L/K) \cong S_3$ siehe Blatt 13 A2(f): $f = X^3 + X + 3 \in \mathbb{Q}[X]$ über $K = \mathbb{Q}$ liefert $Aut(L/K) \cong S_3$.

Wir können jetzt
$$H := \{\sigma \in Aut(L/K) \mid \sigma^3 = id\} = \left\{ \sigma_1 : \begin{array}{l} a_1 \mapsto a_2 \\ a_2 \mapsto a_3 \\ a_3 \mapsto a_1 \end{array},\ \sigma_2 : \begin{array}{l} a_1 \mapsto a_3 \\ a_2 \mapsto a_1 \\ a_3 \mapsto a_2 \end{array},\ id \right\} \cong \mathbb{Z}/3\mathbb{Z}$$
betrachten und $K' := Fix(H)$ setzen. Dann ist $\# Gal(L/K') = \# H = 3$ und L ist immernoch Zerfällungskörper von $f \in K'[X] \supseteq K[X]$.

$Gal(L/Fix(H)) = H$

Auch ist $f \in K'[X]$ irreduzibel, da $a_i \notin K'$ für $i = 1,2,3$ (Sonst wäre $\sigma_1(a_i) = a_i$).

Explizit: Mit Bsp. 3.7.10. Sei $K = \mathbb{Q}(\zeta_3)$ und $b \in K$ ein Element mit $\sqrt[3]{b} \notin K$ (etwa $b = 2$), L der Zerfällungskörper von $X^3 - b \in K[X]$. Dann ist $[L:K] \leq 3$ und $S_3 \geq Aut(L/K) \neq \{id\}$ da $L \neq K$, also $Aut(L/K) \cong \mathbb{Z}/3\mathbb{Z}$

A3 Die Zwischenkörper entsprechen genau den Untergruppen von $\mathbb{Z}/12\mathbb{Z}$. Dies sind:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Z}/12\mathbb{Z} = H_0 \arrow[dl, dash, "\supseteq"'] \arrow[dr, dash, "\supseteq"] & \\
H_1 = 3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \arrow[d, dash, "\cup"'] & & H_2 = 2\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \arrow[dll, dash, "\supseteq"'] \arrow[d, dash, "\cup"] \\
H_3 = 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \arrow[dr, dash, "\supseteq"'] & & H_4 = 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \arrow[dl, dash, "\supseteq"] \\
 & H_5 := 12\mathbb{Z}/12\mathbb{Z} \cong \{1\} &
\end{tikzcd}$$

Übersetzt in Zwischenkörper ergibt das

$$\begin{tikzcd}[column sep=small]
 & F_5 := L = \mathrm{Fix}(H_5) \arrow[dl, dash, "\subseteq"'] \arrow[dr, dash, "\subseteq"] & \\
F_3 := \mathrm{Fix}(H_3) \arrow[d, dash, "\cup"'] \arrow[drr, dash, "\subseteq"] & & \mathrm{Fix}(H_4) =: F_4 \arrow[d, dash, "\cup"] \\
F_1 := \mathrm{Fix}(H_1) \arrow[dr, dash, "\subseteq"'] & & \mathrm{Fix}(H_2) =: F_2 \arrow[dl, dash, "\subseteq"] \\
 & F_0 := \mathrm{Fix}(H_0) = K &
\end{tikzcd}$$

Dabei ist $[L:F_i] = \#\mathrm{Gal}(L/F_i) = \#H_i$, d.h.

$$\begin{tikzcd}[column sep=small]
 & L \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
F_3 \arrow[d, dash, "2"'] \arrow[drr, dash, "3"] & & F_4 \arrow[d, dash, "2"] \\
F_1 \arrow[dr, dash, "3"'] & & F_2 \arrow[dl, dash, "2"] \\
 & F_0 \arrow[dl, equal] & \\
K & &
\end{tikzcd}$$

$[L:F_3] = 2$

$[L:F_4] = 3 \quad \Rightarrow [F_4:F_2] = 2$

$[L:F_2] = 6 \quad \Rightarrow [F_3:F_2] = 3$

$[L:F_1] = 4 \quad \Rightarrow [F_3:F_1] = 2$

$[L:F_0] = [L:K] = 12.$

$\Rightarrow [F_1:F_0] = 3$

und $[F_2:F_0] = 2$

A4 $\#\mathrm{Gal}(L/K) = [L:K] = 90 = 2\cdot 3^2 \cdot 5$

$\Rightarrow$ Es gibt eine 3-Sylowgruppe $H \leq \mathrm{Gal}(L/K)$ mit

$\#H = 3^2 = 9$

$\Rightarrow$ Es gibt einen Zwischenkörper $F = \mathrm{Fix}(H)$ mit

$[L:F] = \#\underbrace{\mathrm{Aut}(L/F)}_{=\mathrm{Aut}(L/\mathrm{Fix}(H))} = \#H = 9$, d.h.

da L/F galoisch

$90 = [L:K] = \underbrace{[L:F]}_{=9} \cdot [F:K] \quad \Rightarrow [F:K] = 10.$

$\boxed{A5}$ $G = Gal(L/K)$ hat 49 Elemente.

1. Fall: G ist abelsch. Dann ist $G \cong \mathbb{Z}/49$ oder $G \cong \mathbb{Z}/7 \times \mathbb{Z}/7$. In beiden Fällen gibt es $H \leq G$ mit $\# H = 7$. Da G abelsch ist, ist $H \trianglelefteq G$.

2. Fall: G ist nicht abelsch. Nach 1.6.7 ist $Z(G) \neq \{1\}$, da G eine p-Gruppe ist ($p = 7$). Nach Def. ist $Z(G) \neq G$, da G nicht abelsch. Also ist $H := Z(G) \leq G$, $\# H = 7$. Nach 1.6.5 ist $H \trianglelefteq G$.

In beiden Fällen gibt es also einen Normalteiler $H \trianglelefteq G$ mit $\# H = 7$.

Nach Satz 3.7.8 (c) ist $F = Fix(H)$ ein Zwischenkörper mit F/K normal und $[L:F] = \# H = 7$, also $[F:K] = 7$. (Da $49 = 7^2 = [L:K] = [L:F] \cdot [F:K]$.)

Bem: Die nebenstehende Lösung ist zwar korrekt, aber Fall 2 kann gar nicht auftreten. Denn:

Beh: Sei G eine Gruppe mit $\# G = p^2$, p prim. Dann ist G abelsch.

Bew: Nach 1.6.7 ist $Z(G) \neq \{1\}$. Also $\# Z(G) = p$ oder $= p^2$. Angenommen $\# Z(G) = p$. Dann gibt es $a \in Z(G)$ mit $ord(a) = p$ und $\langle a \rangle = Z(G)$. Wähle $b \in G \setminus Z(G)$. Ist $ord(b) = p^2$, so ist $\langle b \rangle = G$ zyklisch, also abelsch. Andernfalls ist $ord(b) = p$.

Nun ist
$$\varphi: \langle a \rangle \times \langle b \rangle \longrightarrow \langle a \rangle \cdot \langle b \rangle \leq G$$
$$(a^n, b^m) \longmapsto a^n b^m$$
ein surj. Homom., da $ab = ba$, also $a^n b^m a^{n'} b^{m'} = a^{n+n'} b^{m+m'}$ gilt. Wegen $\# \langle a \rangle \times \langle b \rangle = p^2 = \# \langle a \rangle \cdot \langle b \rangle$ (sonst wäre $\langle a \rangle \cdot \langle b \rangle \leq \langle a \rangle$ oder $\leq \langle b \rangle$, im Widerspruch zu $b \notin \langle a \rangle$) folgt, dass φ ein Iso ist. Insbesondere ist G abelsch.