Aufgabe 1

Vermöge der Galois-Korrespondenz schauen wir uns die Untergruppen von $\mathbb{Z}/18\mathbb{Z}$ an:

$$
\begin{tikzcd}[column sep=small]
 & \mathbb{Z}/18\mathbb{Z} \arrow[dl, phantom, "\supset_{2}"] \arrow[dr, phantom, "\supset^{3}"] & & \\
2\mathbb{Z}/18\mathbb{Z} \arrow[dr, phantom, "\supset^{3}"] & & 3\mathbb{Z}/18\mathbb{Z} \arrow[dl, phantom, "\supset_{2}"] \arrow[dr, phantom, "\supset^{3}"] & \\
 & 6\mathbb{Z}/18\mathbb{Z} \arrow[dr, phantom, "\supset^{3}"] & & 9\mathbb{Z}/18\mathbb{Z} \arrow[dl, phantom, "\supset_{2}"] \\
 & & 0 &
\end{tikzcd}
$$

jeweils der Index...

UG-zykl. Grp- sind zykl. + Lagrange

Somit sind die Zwischenkörper durch

$$
\begin{tikzcd}[column sep=small]
 & K \arrow[dl, phantom, "\subset_{2}"] \arrow[dr, phantom, "\subset^{3}"] & & \\
L^{2\mathbb{Z}/18\mathbb{Z}} \arrow[dr, phantom, "\subset_{3}"] & & L^{3\mathbb{Z}/18\mathbb{Z}} \arrow[dl, phantom, "\subset_{2}"] \arrow[dr, phantom, "\subset^{3}"] & \\
 & L^{6\mathbb{Z}/18\mathbb{Z}} \arrow[dr, phantom, "\subset_{3}"] & & L^{9\mathbb{Z}/18\mathbb{Z}} \arrow[dl, phantom, "\subset_{2}"] \\
 & & L &
\end{tikzcd}
$$

jeweils der Grad

Es gibt also insgesamt sechs Zwischenkörper mit Graden

$[L:L] = 1$

$[L:L^{9\mathbb{Z}/18\mathbb{Z}}] = 2$

$[L:L^{6\mathbb{Z}/18\mathbb{Z}}] = 3$

$[L:L^{3\mathbb{Z}/18\mathbb{Z}}] = 6$

$[L:L^{2\mathbb{Z}/18\mathbb{Z}}] = 9$

Gradformel... wird ab jetzt ohne Kommentar verwendet

$[L:K] = 18$

$[L^{9\mathbb{Z}/18\mathbb{Z}}:L^{3\mathbb{Z}/18\mathbb{Z}}] = 3$

$[L^{9\mathbb{Z}/18\mathbb{Z}}:K] = 9$

$[L^{6\mathbb{Z}/18\mathbb{Z}}:L^{3\mathbb{Z}/18\mathbb{Z}}] = 2$

$[L^{6\mathbb{Z}/18\mathbb{Z}}:L^{2\mathbb{Z}/18\mathbb{Z}}] = 3$

$[L^{6\mathbb{Z}/18\mathbb{Z}}:K] = 6$

$[L^{3\mathbb{Z}/18\mathbb{Z}}:K] = 3$

$[L^{2\mathbb{Z}/18\mathbb{Z}}:K] = 2$

$[K:K] = 1.$

Aufgabe 2

(i)

Offenbar ist $0^p = 0$. Daher betrachten wir $\mathbb{F}_p^\times$ mit Ordnung $|\mathbb{F}_p^\times| = p-1$. Nach Lagrange ist also $a^{p-1} = 1$ für alle $a \in \mathbb{F}_p^\times$ und somit $a^p = a$ für alle $a \in \mathbb{F}_p^\times$. Insgesamt also $a^p = a$ für alle $a \in \mathbb{F}_p$.

(ii)

Es ist

$$\begin{aligned} f(x+a) = (x+a)^p - (x+a) - \lambda &\overset{\text{Char } p}{=} x^p + \cancel{a^p} - x - \cancel{a} - \lambda \\ &\overset{(i)}{=} x^p - x - \lambda \\ &= f(x) \end{aligned}$$

für alle $a \in \mathbb{F}_p$.

(iii)

Sei $\omega \in K^{alg}$ eine Nullstelle von f. Dann ist $f(\omega) = 0$ und somit nach (ii) auch $f(\omega + a) = 0$ für alle $a \in \mathbb{F}_p$. Also sind

$$\omega, \omega+1, \omega+2, \dots, \omega+p-1 \in K^{alg}$$

die Wurzeln von f und f ist demnach separabel.

Aufgabe 3

Vermöge der Galois-Korrespondenz erhalten wir

$\operatorname{ord}(\operatorname{Gal}(L/\mathbb{Q})) = [L : \mathbb{Q}] = [L : \mathbb{Q}(a_1)][\mathbb{Q}(a_1) : \mathbb{Q}]$.

Da $f(a_1) = 0$ ist und f irreduzibel ist, erhalten wir

$\deg(\mu_{a_1}) = \deg(f) = p$,

sodass $p = [\mathbb{Q}(a_1) : \mathbb{Q}]$ ein Teiler von der Ordnung von $\operatorname{Gal}(L/\mathbb{Q})$ ist. Somit besitzt $\operatorname{Gal}(L/\mathbb{Q})$ ein Element der Ordnung p nach dem Satz von Cauchy. Da $\operatorname{Gal}(L/\mathbb{Q})$ eine Untergruppe von S_p ist und p prim ist, muss dieses Element allerdings bereits ein p-Zykel sein.

(ii)

Sei $\overline{(\ )} : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation, aufgefasst als Automorphismus von $\mathbb{Q}^{alg}$ über $\mathbb{Q}$. Da $\mathbb{Q} \subset L$ per Definition normal ist, definiert $\overline{(\ )}$ einen Automorphismus von L über $\mathbb{Q}$, also ein Element von $\operatorname{Gal}(L/\mathbb{Q})$. Nun besitzt f genau zwei echt-komplexe Nullstellen, sodass $\overline{(\ )}|_L$ diese beiden permutieren muss und die anderen $p-2$ Nullstellen fix lässt. Anders gesagt, ist $\overline{(\ )}|_L$ also eine Transposition.

(iii)

Nach Aufgabe 3 von Blatt 5 muss $\operatorname{Gal}(L/\mathbb{Q}) = S_p$ sein, da $\operatorname{Gal}(L/\mathbb{Q})$ einen p-Zykel ((i)) und eine Transposition ((ii)) enthält.

Aufgabe 4

Der Körper $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \overline{\zeta}_3\sqrt[3]{2})$

$\uparrow$ $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})$ ist eine Grad 2 Erweiterung und somit normal

ist der Zerfällungskörper von $x^3 - 2 \in \mathbb{Q}[x]$. Somit ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})$ galoisch. Nach Aufgabe 3 ist zudem $Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})/\mathbb{Q}) = S_3$.

Der Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3})$ ist der Zerfällungskörper des separablen Polynomes $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$ und somit eine Galois-Erweiterung von $\mathbb{Q}$. Wir zeigen nun, dass $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ ist. Die Gradformel liefert zunächst

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]}_{\le 2, \text{ da } \sqrt{3} \text{ Nullstelle von } x^2-3 \text{ ist.}} \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{= 2, \text{ da } \mu_{\sqrt{2}} = x^2-2},$$

sodass wir nur zeigen müssen, dass $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ ist. Ang., $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Dann ex. $a, b \in \mathbb{Q}$ mit $\sqrt{3} = a + b\sqrt{2}$ und somit $3 = \underbrace{a^2}_{\ge 0} + 2ab\sqrt{2} + \underbrace{2b^2}_{\ge 0}$. Also $a = 0$ oder $b = 0$. Ist $a = 0$, so ist $3 = 2b^2$ und somit $b = \pm\sqrt{\frac{3}{2}} \notin \mathbb{Q}$. Ist $b = 0$, so ist $3 = a^2$ und somit $a = \pm\sqrt{3} \notin \mathbb{Q}$.

Es ist also $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. Damit ist auch $|Gal(\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q})| = 4$ und $\sigma(\sqrt{2}) = \pm\sqrt{2}$ und $\sigma(\sqrt{3}) = \pm\sqrt{3}$ für jedes Element $\sigma \in Gal(\sqrt{2},\sqrt{3})/\mathbb{Q})$ nach Satz 3.5.2. Diese Bedingungen legen ein solches σ aber auch fest, da σ den Körper $\mathbb{Q}$ fixiert und $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$ ist. Es ist also

$$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{id, \tau_1, \tau_2, \tau_1 \circ \tau_2\},$$

wobei $\tau_1(\sqrt{2}) = -\sqrt{2}$, $\tau_1(\sqrt{3}) = \sqrt{3}$ und $\tau_2(\sqrt{2}) = \sqrt{2}$ und $\tau_2(\sqrt{3}) = -\sqrt{3}$. Da all diese Elemente der Ordnung 2 sind, muss nun $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}^2$ sein.