Aufgabe 1

f ist irreduzibel nach Eisenstein und die Erweiterung ist separabel, weil endliche Körper vollkommen sind. Sei α eine Nullstelle von f, d.h. f ist das Minimalpolynom zu α. Behauptung: Der Zerfällungskörper von f ist gegeben durch $\mathbb{F}_3(\alpha)$. Es gilt

$$\begin{aligned}(\alpha^3)^4 + 2(\alpha^3)^2 + 2 &= (\alpha^6)^2 + 2\alpha^6 + 2\\ &= (2\alpha^2+1)^2 + 2(2\alpha^2+1) + 2\\ &= \alpha^4 + \alpha^2 + 1 + \alpha^2 + 2 + 2\\ &= \alpha^4 + 2\alpha^2 + 2\\ &= 0\end{aligned}$$

und wegen $2^2 = 1$ sind dann offensichtlich auch 2α und $2\alpha^3$ Nullstellen von f. Ein $\sigma \in G \coloneqq \mathrm{Gal}(L/K)$ ist bereits eindeutig bestimmt durch seinen Wert auf α, daher besitzt G vier Elemente,

$$G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\},$$

mit $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = 2\alpha$, $\sigma_3(\alpha) = \alpha^3$ und $\sigma_4(\alpha) = 2\alpha^3$. Untergruppen von G haben demnach die Ordnung 2. Jede Untergruppe enthält aber auch σ_1. Wegen $2^2 = 1$ ist $\sigma_2^2 = \mathrm{id}$. Damit bildet $U = \{\sigma_1, \sigma_2\}$ eine Untergruppe. Wegen

$$\alpha^9 = \alpha^3 \cdot \alpha^6 = \alpha \cdot \alpha^2 \cdot (2\alpha^2 + 1) = \alpha \cdot (2\alpha^4 + \alpha^2) = 2\alpha$$

gilt außerdem $\sigma_3^2 = \sigma_4^2 = \sigma_2$. Es kann also keine Untergruppe geben, die σ_3 oder σ_4 enthält, aber nicht σ_2. Daher ist U die einzige Untergruppe von G. Insbesondere existiert nur ein echter Zwischenkörper von $L/\mathbb{F}_3$. Diese Zwischenerweiterung hat die Ordnung 2 und ist gegeben durch

$$K \coloneqq L^U = \{x \in L : \sigma_2(x) = x\}$$

Offensichtlich ist $\mathbb{F}_3(\alpha^2) \subset K$. Es gilt außerdem $[\mathbb{F}_3(\alpha^2) : \mathbb{F}_3] = 2$, da α^2 das Minimalpolynom $X^2 + 2X + 2$ besitzt. Daraus folgt $K = \mathbb{F}_3(\alpha^2)$.

Aufgabe 2

(a) Es gilt $\deg \Phi_{2n} = \varphi(2n) \overset{(2,n)=1}{=} \varphi(2)\varphi(n) = \varphi(n) = \deg \Phi_n$. Ist zudem ζ eine primitive Einheitswurzel in μ_n, so gilt $\mathrm{ord}_{\mu_n} \zeta = n$. Wir folgern

$$\zeta^n = 1 \implies (-\zeta)^n = (-1)^n \zeta^n = -1.$$

Wegen $\mathrm{ord}_{\mu_{2n}} -\zeta | 2n$, aber $\zeta^n \neq 1$ folgt $\mathrm{ord}_{\mu_{2n}} -\zeta = 2n$. Also ist $-\zeta$ primitive Einheitswurzel in μ_{2n}. Jede Nullstelle ζ von Φ_n ist primitive Einheitswurzel in μ_n, also ist stets $-\zeta$ eine primitive Einheitswurzel in μ_{2n} und damit Nullstelle von Φ_{2n}. Da Φ_n $\varphi(n)$ Nullstellen besitzt und zu jeder Nullstelle ζ von Φ_n $-\zeta$ eine Nullstelle von Φ_{2n} darstellt, besitzt Φ_{2n} mindestens $\varphi(n)$ Nullstellen. Wegen $\deg \Phi_{2n} = \varphi(n)$ sind damit bereits alle Nullstellen von Φ_{2n} bestimmt. Es folgt $\Phi_{2n}(-X) = \Phi_n(X)$ oder äquivalent $\Phi_{2n}(X) = \phi_n(-X)$.

(b) Jede n-te Einheitswurzel ist primitive d-te Einheitswurzel für genau einen Teiler d von n. Daher gilt

$$\underbrace{X^n - 1}_{\in \overline{K}[X]} = \Psi_n(X) \prod_{\substack{d \mid n \\ d<n}} \Psi_d(X)$$

Nun argumentieren wir per Induktion über n. Der Fall $n = 1$ ist trivial. Sei $n > 1$. Dann gilt

$$\begin{aligned}
\underbrace{X^n - 1}_{\in \overline{K}[X]} &= \Psi_n(X) \prod_{\substack{d \mid n \\ d<n}} \Psi_d(X) \\
\underbrace{\overline{X^n - 1}}_{\in \mathbb{Z}[X]} &= \Psi_n(X) \prod_{\substack{d \mid n \\ d<n}} \overline{\Phi}_d(X) \\
\overline{\Phi_n(X) \prod_{\substack{d \mid n \\ d<n}} \Phi_d(X)} &= \Psi_n(X) \prod_{\substack{d \mid n \\ d<n}} \overline{\Phi}_d(X)
\end{aligned}$$

$\overline{\cdot}$ Homomorphismus

$$\begin{aligned}
\overline{\Phi}_n(X) \prod_{\substack{d \mid n \\ d<n}} \overline{\Phi}_d(X) &= \Psi_n(X) \prod_{\substack{d \mid n \\ d<n}} \overline{\Phi}_d(X) \\
0 &= (\overline{\Phi}_n(X) - \Psi_n(X)) \prod_{\substack{d \mid n \\ d<n}} \overline{\Phi}_d(X)
\end{aligned}$$

$\overline{K}[X]$ nullteilerfrei

$$\begin{aligned}
\implies 0 &= \overline{\Phi}_n(X) - \Psi_n(X) \\
\Psi_n(X) &= \overline{\Phi}_n(X)
\end{aligned}$$

Aufgabe 3

(a) Genau dann, wenn f nicht separabel, existieren Nullstellen α_i, α_j mit $i \neq j$ aber $\alpha_i = \alpha_j$. Genau dann, wenn es solche zwei Nullstellen gibt, ist ein Faktor von δ_f Null. Genau dann, wenn ein Faktor von δ_f null ist, gilt $\delta_f = 0 \Leftrightarrow \Delta_f = 0$.

(b) Sei zunächst $\operatorname{char} K \neq 2$. Dann gilt (bekannt aus der Schule oder auch durch quadratische Erweiterung schnell nachgerechnet) $f(x) = 0 \Leftrightarrow x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$. Die Diskriminante ergibt sich daher zu

$$\begin{aligned}
\Delta_f &= \left(\frac{-b + \sqrt{b^2 - 4ac} - (-b - \sqrt{b^2 - 4ac})}{2a} \right)^2 \\
&= \frac{4(b^2 - 4ac)}{4a^2} \\
&= \frac{b^2 - 4ac}{a^2}
\end{aligned}$$

Für $\operatorname{char} K = 2$ gilt $a = 1$, sonst handelt es sich nicht um ein quadratisches Polynom. Daher verbleiben nur 4 Möglichkeiten für f. Für $b = c = 0$ gilt $X^2 = X \cdot X$, für $b = 1, c = 0$ gilt $X^2 + X = X(X+1)$ und für $b = 0, c = 1$ gilt $X^2 + 1 = (X+1)^2$. Nur das Polynom $X^2 + X + 1$ ist irreduzibel und, weil endliche Körper vollkommen sind auch separabel. Über $\mathbb{F}_4$ besitzt es zwei Lösungen. Sei α eine dieser Lösungen. Dann gilt $\alpha^2 + \alpha + 1 = 0$ und damit auch $(\alpha+1)^2 + (\alpha+1) + 1 = \alpha^2 + \alpha + 1 = 0$. Daher ist mit α auch $\alpha + 1$ Nullstelle des Polynoms. Die Differenz der beiden Nullstellen ist daher 1. Damit ist die Diskriminante durch 1 gegeben, was genau mit $b^2 - 4ac = b^2 = 1$ übereinstimmt.

(c) Es gilt

$$\begin{aligned}\sigma(\delta_f) &= \prod_{1 \le i < j \le n} (\sigma(\alpha_i) - \sigma(\alpha_j)) \\ &= \prod_{1 \le i < j \le n} (\alpha_{\varphi(\sigma)(i)} - alpha_{\varphi(\sigma)(j)})\end{aligned}$$

Jede Permutation lässt sich schreiben als Produkt von Transpositionen. Jede Transposition führt dazu, dass in einem Faktor von δ_f das Vorzeichen umgedreht wird. Sei n die Anzahl der Transpositionen.

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

Dann ist per Definition $\operatorname{sgn}(\varphi(\sigma)) = (-1)^n$

$$= \operatorname{sgn}(\varphi(\sigma))\delta_f.$$

(d) $\sigma(\Delta_f) = \sigma(\delta_f)^2 = \operatorname{sgn}(\varphi(\sigma))^2 \delta_f^2 = 1 \cdot \Delta_f$ und daher $Delta_f \in L^G = K$.

(e) $\Delta_f \in (K^\times)^2 \Leftrightarrow \delta_f \in K$. Außerdem gilt $\varphi(G) \subset \mathfrak{A}_n \Leftrightarrow \operatorname{sgn}(\varphi(\sigma)) = 1 \forall \sigma \in G$.

$$\begin{aligned}\Delta_f \in (K^\times)^2 &\Leftrightarrow \delta_f \in K \\ &\Leftrightarrow \delta_f \in L^G \\ &\Leftrightarrow \sigma(\delta_f) = \delta_f \forall \sigma \in G \\ &\Leftrightarrow \operatorname{sgn}(\varphi(\sigma))\delta_f = \delta f \forall \sigma \in G \\ &\Leftrightarrow \operatorname{sgn}(\varphi(\sigma)) = 1 \forall \sigma \in G \\ &\Leftrightarrow \varphi(G) \subset \ker(\operatorname{sgn}) = \mathfrak{A}_n\end{aligned}$$

Aufgabe 4

(a) Es gilt $\overline{a} := a \mod q \in \mathbb{F}_q^\times$, da a zu q teilerfremd ist. Nach Aufgabe 6.3(c) gilt

$$\overline{a}^{\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } \overline{a} = a \mod q \in (\mathbb{F}_q^\times)^2, \\ -1, & \text{falls } \overline{a} = a \mod q \notin (\mathbb{F}_q^\times)^2 \end{cases}.$$

Daher ist $\left(\frac{a}{q}\right) = \overline{a}^{\frac{q-1}{2}}$. Daraus folgt bereits

$$\left(\frac{ab}{q}\right) = \overline{ab}^{\frac{q-1}{2}} = \overline{a}^{\frac{q-1}{2}}\overline{b}^{\frac{q-1}{2}} = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right).$$

Für $a = -1$ erhalten wir

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}.$$

Für $q \equiv 1 \mod 4$ gilt $\frac{q-1}{2} \equiv 0 \mod 2$, für $q \equiv 3 \mod 4$ gilt $\frac{q-1}{2} \equiv 1 \mod 2$. Wegen $(-1)^2 = 1$ genügt es, die Kongruenzen modulo 2 des Exponenten zu betrachten und wir vervollständigen

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } q \equiv 1 \ (\mod 4) \\ -1, & \text{falls } q \equiv 3 \ (\mod 4). \end{cases}$$

(b) Für die Diskriminante von $f = X^p - 1$ erhalten wir nach der Formel

$$\Delta_f = (-1)^{p(p-1)/2)} p^p (-1)^{p-1} = \left((-1)^{(p-1)/2} p\right)^p.$$

Das Bild von G in $\mathfrak{S}_p$ ist genau dann in $\mathfrak{A}_p$ enthalten, wenn $\Delta_f \in (\mathbb{F}_q^\times)^2$ gilt. Es gilt

$$\begin{aligned} \varphi(G) \subset \mathfrak{A}_p &\Leftrightarrow \Delta_f \in (\mathbb{F}_q^\times)^2 \\ &\Leftrightarrow 1 = \left(\frac{\left((-1)^{(p-1)/2} p\right)^p}{q}\right) \\ &\Leftrightarrow 1 = \left(\frac{(-1)^{(p-1)/2} p}{q}\right)^p \end{aligned}$$

p ungerade, $1^p = 1$, $(-1)^p = -1$.

$$\begin{aligned} &\Leftrightarrow 1 = \left(\frac{(-1)^{(p-1)/2} p}{q}\right) \\ &\Leftrightarrow 1 = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{p}{q}\right) \\ &\Leftrightarrow 1 = \left(\frac{(-1)}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) \\ &\Leftrightarrow 1 = \left((-1)^{\frac{q-1}{2}}\right)^{(p-1)/2}\left(\frac{p}{q}\right) \\ &\Leftrightarrow 1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \end{aligned}$$

(c) Der Zyklus, in dem die 1 liegt, hat die Gestalt $(1, q, q^2, \ldots, q^{k-1})$. Notwendigerweise muss jeder weitere Zyklus die Gestalt $(a, aq, aq^2, \ldots, aq^{k-1})$ haben. Jeder Zyklus bricht nämlich nach k Elementen ab, da $q^k = 1$ ist. Gäbe es einen kürzeren Zyklus, so wäre k nicht die Ordnung von q. Außerdem sind verschiedene Zyklen natürlich disjunkt. Daher zerfällt $(\mathbb{Z}/p\mathbb{Z})^\times$ in die disjunkte Vereinigung von Teilmengen mit k Elementen, die jeweils im selben Zyklus liegen. Die Anzahl der Zyklen ist daher gegeben durch $\frac{\#(\mathbb{Z}/p\mathbb{Z})^\times}{k} = \frac{p-1}{k}$. Das Signum eines Zyklus der Länge k ist genau $k-1$, da sich jeder Zyklus der Länge k als Komposition von $k-1$ Transpositionen schreiben lässt (Offensichtlich für $k=2$, durch Überprüfen für a_{n-1} und a_n sieht man dann leicht $(a_1,\ldots,a_n) = (a_1,a_n)(a_1,\ldots,a_{n-1})$, woraus per Induktion die Behauptung folgt). Die Komposition von $\frac{p-1}{k}$ Zyklen der Länge k lässt sich also als Komposition von $k\frac{p-1}{k}$ Transpositionen schreiben und es gilt $\operatorname{sgn}(\pi) = (-1)^{(k-1)\frac{p-1}{k}}$.

(d) Da der q-Frobenius σ die Gruppe G erzeugt, gilt $\operatorname{sgn}(\varphi(\sigma')) = 1 \forall \sigma' \in G \Leftrightarrow \operatorname{sgn}(\varphi(\sigma)) = 1$. Wir rechnen also

$$\begin{aligned} 1 &= (-1)^{(k-1)\frac{p-1}{k}} \\ &= (-1)^{k\frac{p-1}{k} - \frac{p-1}{k}} \\ (-1)^{\frac{p-1}{k}} &= (-1)^{p-1}(-1)^{\frac{p-1}{k}} && = 1 \end{aligned}$$

Das ist äquivalent zur Existenz eines $l \in \mathbb{Z}$ mit

$$\begin{aligned} \frac{p-1}{k} &= 2 \cdot l \\ \frac{p-1}{2} &= k \cdot l \end{aligned}$$

$\frac{p-1}{2}$ ist genau dann ein Vielfaches von k, wenn $q^{\frac{p-1}{2}} = 1$ gilt (wegen $k = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(q)$). Aufgrund der Identität

$$\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}}$$

erhalten wir schließlich die gesuchte Äquivalenz

$$\varphi(G) \subset \mathfrak{A}_n \Leftrightarrow \left(\frac{q}{p}\right) = 1.$$

Aus Teilaufgabe (b) wissen wir, dass für $\varphi(G) \subset \mathfrak{A}_n$ auch

$$1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \Leftrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right)$$

gilt. Wegen $\left(\frac{q}{p}\right) = 1$ folgern wir im Fall $\varphi(G) \subset \mathfrak{A}_n$ bereits

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Im Fall $\varphi(G) \subsetneq \mathfrak{A}_n$ erhalten wir aus (b), da der Ausdruck entweder 1 oder -1 sein kann

$$-1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \Leftrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -\left(\frac{p}{q}\right)$$

und mit analoger Schlussweise folgern wir aus

$$\varphi(G) \subset \mathfrak{A}_n \Leftrightarrow \left(\frac{q}{p}\right) = 1.$$

die Äquivalenz

$$\varphi(G) \subsetneq \mathfrak{A}_n \Leftrightarrow \left(\frac{q}{p}\right) = -1.$$

Multipliziert ergibt sich

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -\left(\frac{p}{q}\right) \cdot -\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Damit haben wir das quadratische Reziprozitätsgesetz für alle Fälle bewiesen.