Aufgabe	A1	A2	A3	A4	$\sum$
Punkte					

Aufgabe 1. Beh.: f irreduzibel

Beweis. Es ist $f(0) = 2$, $f(1) = 1$, $f(2) = 2$ als hat f keine Nullstellen in $\mathbb{F}_3$. Ang.: f ist reduzibel, dann ex. $g, h \in \mathbb{F}_3[X]$ mit $\deg(g) = \deg(h) = 2$, da sonst f eine Nullstelle in $\mathbb{F}_3$ hätte. Dann folgt mit $a, b, c, d \in \mathbb{F}_3$:

$$\begin{aligned} X^4 + 2X^2 + 2 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + \underbrace{(a+c)}_{=0} X^3 + (b + d + ac)X^2 + \underbrace{(bc + ad)}_{=0} X + bd \end{aligned}$$

.

Es folgt direkt $c = -a$ und damit $a(d - b) = 0$, also $a = 0$ oder $d = b$. Falls $a = 0$: Dann ist $b + d = 2$ und $bd = 2$ mit $b, d \in \mathbb{F}_3$ ↯. Also ist $b = d$. Dann ist $b^2 = 2$, aber 2 kein Quadrat in $\mathbb{F}_3$ ↯.

Es folgt also f irreduzibel. □

Da f irreduzibel und $\mathbb{F}_3[X]$ HIR ist $\mathbb{F}_{81} = \mathbb{F}_3[X]/(f)$ also ein Körper mit $3^4 = 81$ Elementen. Dann folgt sofort, dass $f(\overline{X}) = \overline{X}^4 + 2\overline{X}^2 + 2 = 0$. Setze $L \coloneqq \mathbb{F}_3(\overline{X}) \subseteq \mathbb{F}_{81}$. Da $\mathbb{F}_3$ endlich ist $L/\mathbb{F}_3$ normal und separabel, also galoissch. Sei σ der Frobenius-Automorphismus für $p = 3$. Dann gilt

$$\begin{aligned} \sigma(\overline{X}) &= \overline{X}^3 \\ \sigma^2(\overline{X}) &= 2\overline{X} \\ \sigma^3(\overline{X}) &= 2\overline{X}^3 \\ \sigma^4(\overline{X}) &= \overline{X}. \end{aligned}$$

Also ist $\mathrm{ord}(\sigma) = 4$. Da $\mathrm{Gal}(L/\mathbb{F}_3) = \langle\sigma\rangle$ folgt $\#\mathrm{Gal}(L/\mathbb{F}_3) = 4$ und $[L : \mathbb{F}_3] = 4$, da aber $[\mathbb{F}_{3^4} : \mathbb{F}_3] = 4$ folgt $L = \mathbb{F}_{81}$. Außerdem überführt σ Nullstellen von f in Nullstellen von f. Da f genau 4 Nullstellen in $\overline{\mathbb{F}_3}$ hat, sind die Nullstellen von f bereits $\{\overline{X}, \overline{X}^3, 2\overline{X}, 2\overline{X}^3\}$ und $\mathbb{F}_{81}$ ist Zerfällungskörper von f über $\mathbb{F}_3$.

Wegen $\mathrm{Gal}(\mathbb{F}_{81}/\mathbb{F}_3) = \langle\sigma\rangle$, ist diese zyklisch der Ordnung 4, also $\mathrm{Gal}(\mathbb{F}_{81}/\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$. Diese hat genau 1 echte nicht-triviale Untergruppe, da $\mathrm{ord}(1) = \mathrm{ord}(3) = 4$ und $\mathrm{ord}(2) = 2$. Damit folgen als Untergruppen von $\mathrm{Gal}(\mathbb{F}_{81}/\mathbb{F}_3)$:

$$\begin{aligned} H_1 &= \langle \mathrm{id} \rangle \\ H_2 &= \langle \sigma^2 \rangle \\ H_3 &= \langle \sigma \rangle. \end{aligned}$$

Es ist $\sigma^2(\overline{X}^2) = \sigma^2(\overline{X})^2 = (2\overline{X})^2 = \overline{X}^2$. Also ist $\overline{X}^2 \in \mathbb{F}_{81}^{H_2}$, insbesondere $\mathbb{F}_3(\overline{X}^2) \subseteq \mathbb{F}_{81}^{H_2}$. Es ist $\mathrm{Gal}(\mathbb{F}_{81}/\mathbb{F}_3(\overline{X}^2)) = H_2$, insbesondere $[\mathbb{F}_{81} : \mathbb{F}_{81}^{H_2}] = 2$ und da $[\mathbb{F}_{81} : \mathbb{F}_3] = 4$ folgt auch $[\mathbb{F}_{81}^{H_2} : \mathbb{F}_3] = 2$. Da aber $\overline{X}^2 \notin \mathbb{F}_3$ gilt ebenfalls $[\mathbb{F}_3(\overline{X}^2) : \mathbb{F}_3] \geq 2$. Mit Gradformel folgt also $\mathbb{F}_3(\overline{X}^2) = \mathbb{F}_{81}^{H_2}$. Damit folgen nach dem Hauptsatz die Zwischenkörper:

$$\begin{aligned} \mathbb{F}_{81}^{H_1} &= \mathbb{F}_{81} \\ \mathbb{F}_{81}^{H_2} &= \mathbb{F}_3(\overline{X}^2) \\ \mathbb{F}_{81}^{H_3} &= \mathbb{F}_3. \end{aligned}$$

Aufgabe 2. (a) Es ist $\deg(\Phi_n(-X)) = \deg(\Phi_n(X))$. Außerdem ist $(2, n) = 1$, da n ungerade. Damit folgt $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$. Also folgt insgesamt

$$\deg(\Phi_{2n}) = \varphi(2n) = \varphi(n) = \deg(\Phi_n(X)) = \deg(\Phi_n(-X)).$$

Außerdem sei ζ Nullstelle von Φ_{2n}. Dann ist $\zeta \in \mu_{2n}$ und primitiv. Also ex. ein $k \in \mathbb{N}$ mit $(2n,k)=1$ und $\zeta = \exp(\frac{2\pi i}{2n}k)$. Betrachte nun

$$-\zeta = \exp\left(\pi i + \frac{\pi i}{n}k\right) = \exp\left(\frac{\pi i(n+k)}{n}\right).$$

Da $(2n,k)=1$ und $2n$ gerade, folgt k ungerade. Da n ebenfalls ungerade, folgt $n+k \in 2\mathbb{N}$. Also ex. ein $l \in \mathbb{N}$, s.d. $n+k=2l$. Damit folgt

$$-\zeta = \exp\left(\frac{2\pi i l}{n}\right).$$

Es ist $(2n,k)=1$, d.h. es existieren $a,b \in \mathbb{Z}$, s.d.

$$1 = a2n + bk = n(2a+b-b) + bk = b(n+k) + (2a-b)n = \underbrace{2b}_{\in\mathbb{Z}} l + \underbrace{(2a-b)}_{\in\mathbb{Z}} n.$$

Es folgt $(l,n)=1$, also ist $-\zeta$ primitive n-te Einheitswurzel. Also $-\zeta$ Nullstelle von $\Phi_n(X)$ und damit ζ Nullstelle von $\Phi_n(-X)$.

Da nun $\deg(\Phi_{2n}) = \deg(\Phi_n(-X))$ und jede Nullstelle von Φ_{2n} auch Nullstelle von $\Phi_n(-X)$ folgt $\Phi_n(-X) \stackrel{\sim}{=} \Phi_{2n}$. Da Φ_n normiert für $n \in \mathbb{N}$ folgt $a \in \{\pm 1\}$ und a ist gerade der Leitkoeffizient von $\Phi_n(-X)$. Es genügt jetzt zu zeigen, dass $\phi(n)$ gerade ist für $n \geq 3$ und n ungerade. Denn dann ist der Leitkoeffizient $e(\Phi_n(-X)) = (-1)^{2l} = 1$ für ein $l \in \mathbb{N}$ und damit $\Phi_n(-X) = \Phi_{2n}$.

Da $\mathbb{Z}$ faktoriell und $n \geq 3$, ungerade ex. p_i und r_i mit p_i paarweise verschieden und $r_i \in \mathbb{N}$, s.d.

$$n = \prod_{i=1}^{s} p_i^{r_i}.$$

Da n ungerade ist $p_i \neq 2$ und damit $p_i - 1$ gerade für alle i. Da die p_i paarweise verschieden sind diese teilerfremd und es gilt

$$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{r_i}) = \prod_{i=1}^{s} (p_i - 1) p_i^{r_i - 1}.$$

Da die $p_i - 1$ gerade und $s \geq 1$ wegen $n \geq 3$, folgt $2 \mid \varphi(n)$.

Aufgabe 3. (a) Da $\overline{K}$ nullteilerfrei folgt

$$\Delta_f = 0 \iff \alpha_i - \alpha_j = 0 \text{ für } i \neq j \iff \alpha_i = \alpha_j \text{ für } i \neq j \iff f \text{ nicht separabel.}$$

(b) Die Aussage ist offensichtlich falsch für $a = 0$. Sei also $a \neq 0$ und im folgenden $\mathrm{char}(K) \neq 2$. Sei außerdem $\sqrt{a} \in \overline{K}$ mit $\sqrt{a}^2 = a$ und $\sqrt{b^2-4ac} \in \overline{K}$ mit $\sqrt{b^2-4ac}^2 = b^2 - 4ac$. Dann sind die Nullstellen von f gegeben als $\alpha_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a} \in \overline{K}$.

Denn es gilt

$$f = aX^2 + bX + \left(\frac{b}{2\sqrt{a}}\right)^2 - \left(\frac{b}{2\sqrt{a}}\right)^2 + c = \left(\sqrt{a}X + \frac{b}{2\sqrt{a}}\right)^2 - \frac{b^2}{4a} + c$$

Damit folgt

$$f(\alpha_{1,2}) = \left(\sqrt{a}\frac{-b \pm \sqrt{b^2-4ac}}{2a} + \frac{b}{2\sqrt{a}}\right)^2 - \frac{b^2}{4a} + c = 0.$$

Damit folgt

$$\begin{aligned}\Delta_f &= (\alpha_1 - \alpha_2)^2 \\ &= \left[\frac{-b+\sqrt{b^2-4ac}}{2a} - \frac{-b-\sqrt{b^2-4ac}}{2a}\right]^2 \\ &= \frac{1}{a^2}(b^2-4ac).\end{aligned}$$

(c) Sei $\sigma \in G$. Dann ist $\sigma(\alpha_i) = \alpha_j$ für geeignete $i, j \in \{1, \dots, n\}$. Damit folgt

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

Es ist $\varphi(\sigma)$ als Produkt von s Transpositionen darstellbar für $s \in \mathbb{N}$. Jede dieser s Transpositionen ändert das Vorzeichen von δ_f um (-1). Also folgt

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

(d) Es ist für $\sigma \in G$:

$$\sigma(\Delta_f) = \sigma(\delta_f^2) = \sigma(\delta_f)^2 \overset{\text{(c)}}{=} (\operatorname{sgn}(\varphi(\sigma))\delta_f)^2 = \Delta_f.$$

Also folgt $\Delta_f \in L^G = K$.

(e) Sei zunächst $\varphi(G) \subseteq \mathfrak{A}_n$. Dann ist für $\sigma \in G$ wegen (c) $\sigma(\delta_f) = \sigma(\delta_f)$, also $\delta_f \in L^G = K$, also da f separabel und nach (a) also $\Delta_f \neq 0$ auch $\Delta_f = \delta_f^2 \in (K^x)^2$.

Sei nun $\Delta_f \in (K^\times)^2$. Dann ist $\delta_f \in K^\times$. Sei nun $\sigma \in G$. Dann folgt

$$\delta_f = \sigma(\delta_f) = \operatorname{sgn}(\varphi(\sigma))\delta_f \implies \delta_f(\operatorname{sgn}(\varphi(\sigma)) - 1) = 0.$$

Da $\delta_f \in K^x$ folgt $\operatorname{sgn}(\varphi(\sigma)) = 1 \overset{\text{char } K \neq 2}{\neq} -1$. Also $\varphi(G) \subseteq \mathfrak{A}_n$.

Aufgabe 4. (a) Seien $a, b \in \mathbb{Z}$ mit $(a, q) = 1$ und $(b, q) = 1$. Dann ist auch $(ab, q) = 1$, da $\mathbb{Z}$ faktoriell. Damit ist $\overline{a}, \overline{b} \in \mathbb{F}_p^\times$. Damit folgt nach Zettel 6, Aufgabe 3(c):

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

Erneut nach Zettel 6 ist $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} \in \{\pm 1\}$. Da q ungerade ist weiter $q \equiv 3 \pmod 4$ oder $q \equiv 1 \pmod 4$, also g.z.z., dass $(-1)^{\frac{q-1}{2}} = 1 \iff q \equiv 1 \pmod 4$. Es gilt

$$(-1)^{\frac{q-1}{2}} = 1 \iff 2 \mid \frac{q-1}{2} \iff 4 | (q-1) \iff q \equiv 1 \pmod 4.$$

(b) Es ist $f = X^p - 1$ nach Vorlesung separabel, da $p \neq q$ Primzahlen und damit $\operatorname{char}(\mathbb{F}_q) = q \nmid p$. Außerdem ist mit der angegebenen Formel:

$$\Delta_f = (-1)^{\frac{p(p-1)}{2}} p^p (-1)^{p-1}.$$

Da q ungerade ist $\operatorname{char}(\mathbb{F}_q) \neq 2$. Nach 3(e) ist damit das Bild von G in $\mathfrak{S}_p$ g.d. in $\mathfrak{A}_p$ enthalten, wenn

$$\Delta_f \in \left(\mathbb{F}_q^\times\right)^2 \iff \left(\frac{\Delta_f}{q}\right) = 1. \tag{2}$$

Da p ungerade ist $(-1)^p = -1$. Damit ist auch $\left(\frac{p}{q}\right)^p = \left(\frac{p}{q}\right)$ $(*)$ Außerdem ist deshalb $p - 1$ gerade und damit $\left(\frac{-1}{q}\right)^{p-1} = 1$ $(**)$. Damit folgt

$$\begin{aligned}\left(\frac{\Delta_f}{q}\right) &\overset{\text{(a)}}{=} \left(\frac{(-1)^{\frac{p(p-1)}{2}}}{q}\right)\left(\frac{p^p}{q}\right)\left(\frac{(-1)^{p-1}}{q}\right) \\ &\overset{\text{(a)}}{=} \left(\frac{-1}{q}\right)^{\frac{p(p-1)}{2}}\left(\frac{p}{q}\right)^p \underbrace{\left(\frac{-1}{q}\right)^{p-1}}_{=1 (**)} \\ &\overset{(*),\,\text{(a)}}{=} (-1)^{p\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right) \\ &\overset{p \text{ ungerade}}{=} (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right).\end{aligned}$$

Mit (2) zeigt das die gewünschte Äquivalenz.

(c) Für $a \in \mathbb{Z}/p\mathbb{Z}$ gilt $\pi(a)^r = aq^r$ für $r \in \mathbb{N}_0$. Es gilt $\pi(a)^k = aq^k = a$. Jedes Element in $a \in \mathbb{Z}/p\mathbb{Z}$ wird also von π zyklisch vertauscht. π erzeugt also disjunkte Zykeln der Länge k. Zwei Elemente $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ liegen genau dann im selben Zykel, wenn $b^{-1}a \in \langle q \rangle$. Also g.d.w $b \sim_{\langle q \rangle} a$. Also besteht π aus genau $((\mathbb{Z}/p\mathbb{Z})^\times : \langle q \rangle) \overset{\text{Lagrange}}{=} \frac{p-1}{k}$ disjunkten Zykeln. Das Signum eines Zykels der Länge k ist genau $(-1)^k$. Da weiterhin sgn Gruppenhomomorphismus folgt:

$$\operatorname{sgn}(\pi) = ((-1)^{k-1})^{\frac{p-1}{k}} = (-1)^{k-1\frac{p-1}{k}}.$$

(d) Sei $\gamma \in \mathbb{F}_p^\times$ ein Erzeuger.
Beh.: $\gamma^n \in (\mathbb{F}_p^\times)^2 \iff 2 \mid n$.

- $2 \mid n \implies n = 2l$ für ein $l \in \mathbb{N} \implies \gamma^n = \gamma^{2l} = (\gamma^l)^2$.
- $\gamma^n \in (\mathbb{F}_p^x)^2 \implies \exists l \in \mathbb{N}$: $(\gamma^l)^2 = \gamma^n \implies \gamma^{2l \bmod p} = \gamma^{n \bmod p} \implies 2l \equiv n \bmod \text{p} \implies 2 \mid n$.

Da γ Erzeuger, ex. ein $n \in \mathbb{N}$, s.d. $q = \gamma^n$. Es ist $\gamma^{nk} = q^k = 1 = \gamma^{p-1} \implies n = \frac{p-1}{k}$. Damit folgt

$$1 = \left(\frac{q}{p}\right) \iff q = \gamma^{2l} \text{ für ein } l \in \mathbb{N} \iff 2 \mid \frac{p-1}{k}. \tag{3}$$

Es gilt außerdem $p-1 = ((\mathbb{Z}/p\mathbb{Z})^\times : \langle q \rangle)k = \underbrace{\frac{p-1}{k}}_{\in \mathbb{N}} k$. Falls $\frac{p-1}{k}$ ungerade, dann ist also k gerade, da $p-1$ gerade und damit $k-1$ ungerade. Damit folgt $2 \mid (k-1)\frac{p-1}{k} \iff 2 \mid \frac{p-1}{k}$.
Das Bild von G ist g.d. in $\mathfrak{A}_n$ enthalten, wenn $\operatorname{sgn}(\pi) = 1$. Weiter gilt mit (c)

$$\operatorname{sgn}(\pi) = 1 \iff 1 = (-1)^{(k-1)\frac{p-1}{k}} \iff 2 \mid (k-1)\frac{p-1}{k} \iff 2 \mid \frac{p-1}{k}.$$

Das zeigt mit (3) die behauptete Äquivalenz.
Nun gilt also mit (b), dass

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

Damit folgt:

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

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

$$\begin{aligned}
\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\
&= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \\
&\overset{\text{(a)}}{=} \begin{cases} (-1)^{\frac{p-1}{2}} & q \equiv 3 \pmod 4 \\ 1 & q \equiv 1 \pmod 4 \end{cases} \\
&\overset{\text{(a)}}{=} \begin{cases} -1 & q, p \equiv 3 \pmod 4 \\ 1 & \text{sonst} \end{cases}.
\end{aligned}$$