Aufgabe 1 (Frühjahr 2014)**.** Seien $a, b \in \mathbb{Q}$, und sei K der Zerfällungskörper des Polynoms

$$p = x^3 + x + b \in \mathbb{Q}[x].$$

Wir nehmen an, daß p keine Nullstelle in $\mathbb{Q}$ hat. Zeigen Sie:

(a) p ist irreduzibel in $\mathbb{Q}[x]$ und hat keine mehrfache Nullstellen in K.

(b) Die Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{Q})$ ist eine Untergruppe von $\mathfrak{S}_3$.

(c) G hat entweder 3 oder 6 Elemente.

(d) Sei $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, wobei $\alpha_1, \alpha_2, \alpha_3 \in K$ die Nullstellen von p sind. Dann gilt für $\sigma \in G$ stets $\sigma(\delta) = \delta$ oder $\sigma(\delta) = -\delta$.

(e) Gilte $\sigma(\delta) = \delta$ für alle $\sigma \in G$, dann ist G zyklische und hat Ordnung 3. Andernfalls ist $G = \mathfrak{S}_3$.

Lösung. **Zu (a):** Da p ein Polynom vom Grad 3 über $\mathbb{Q}$ ist, und keine Nullstelle in $\mathbb{Q}$ hat, ist es irreduzibel über $\mathbb{Q}$. Für eine Zerlegung in nichttriviale normierte Faktoren $p = fg$ mit $f, g \in \mathbb{Q}[x]$ gilt nämlich

$$3 = \deg(p) = \deg(f) + \deg(g).$$

Die natürliche Zahl 3 hat aber nur die Zerlegungen $2+1 = 3 = 1+2$, also wäre eines der beiden Polynome f oder g linear, und dann hätter p eine Nullstelle in $\mathbb{Q}$, Widerspruch.
Da $\mathbb{Q}$ von Charakteristik 0 ist, ist jedes irreduzible Polynom über $\mathbb{Q}$ separabel. Insbesondere hat das irreduzible Polynom p über keinem Zerfällungskörper mehrfache Nullstellen.

Zu (b): Sei $N = \{\alpha_1, \alpha_2, \alpha_3\}$ die Menge der Nullstellen von p. Die Galoisgruppe eines Zerfällungskörpers von p operiert transitiv auf dieser Menge durch

$$\mathrm{Gal}(K/\mathbb{Q}) \times N \to N, (\sigma, \alpha) \mapsto \sigma(\alpha).$$

(Es ist klar, daß für eine Nullstelle $\alpha \in N$ von p, $\sigma(\alpha)$ wieder eine Nullstelle von p ist, denn $\sigma(p) = p$, und $p(\sigma(\alpha)) = \sigma(p)(\sigma(\alpha)) = \sigma\left(p(\alpha)\right) = \sigma(0) = 0$.)
Weiterhin ist die Abbildung $\mathrm{Gal}(K/\mathbb{Q}) \to \mathfrak{S}_N, \sigma \mapsto (\alpha \mapsto \sigma(\alpha))$ ein injektiver Gruppenhomomorphismus. Denn gilt für $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ daß $\sigma(\alpha) = \tau(\alpha)$ für alle $\alpha \in N$, so ist bereits $\tau = \alpha$. Aber $\mathfrak{S}_N \cong \mathfrak{S}_3$, die Permutationsgruppe von drei Elementen. Damit kann man $\mathrm{Gal}(K/\mathbb{Q})$ als Untergruppe von $\mathfrak{S}_3$ ansehen.

Zu (c): Nach (b) ist $\mathrm{Gal}(K/\mathbb{Q})$ zu einer Untergruppe von $\mathfrak{S}_3$ isomorph, welche Ordnung 6 hat. Also $|\mathrm{Gal}(K/\mathbb{Q})|\big|6$. Es ist eine Folgerung des Fortsetzungssatzes, daß $\mathrm{Gal}(K/\mathbb{Q})$ transitiv auf N operiert. INsbesondere gibt es für je zwei Elemente $\alpha, \beta \in N$ ein Element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ mit $\sigma(\alpha) = \beta$. Zum Beispiel gibt es für jedes $i \in \{1, 2, 3\}$ ein $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ mit $\sigma(\alpha_1) = \alpha_i$, also mindestens drei StÃ¼ck. Aus

$$3 \leqslant |\mathrm{Gal}(K/\mathbb{Q})|\big|6$$

folgt also $|\mathrm{Gal}(K/\mathbb{Q})| \in \{3, 6\}$.

Zu (d): Sei $\mathcal{P} = \{\{1,2\}, \{1,3\}, \{2,3\}\}$ die Menge der zweielementigen Teilmengen von $\{1, 2, 3\}$ (bei Mengen ist die Reihenfolge unrelevant, es gilt also $\{1, 2\} = \{2, 1\}$). Jede Permutation $\sigma \in \mathfrak{S}_3$ induziert eine bijektive Abbildung auf $\mathcal{M}$.
Sei für $\{i, j\} \in \mathcal{P}$

$$\alpha_{\{i,j\}} := (\alpha_i - \alpha_j)^2 = (\alpha_j - \alpha_i)^2.$$

Dann ist für $\sigma \in \mathrm{Gal}(K/\mathbb{Q} \subset \mathcal{S}_3$

$$\sigma(\alpha_{\{i,j\}}) = \sigma(\alpha_i - \alpha_j)^2 = (\sigma(\alpha_i) - \sigma(\alpha_j))^2 = (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2 = \alpha_{\sigma(\{i,j\})}.$$

Also

$$\sigma(\delta)^2 = \sigma(\delta^2) = \sigma\left(\prod_{\{i,j\}\in\mathcal{P}} \alpha_{\{i,j\}}\right) = \prod_{\{i,j\}\in\mathcal{P}} \alpha_{\sigma(\{i,j\})} = \prod_{\{i,j\}\in\mathcal{P}} \alpha_{\{i,j\}} = \delta^2$$

Es folgt $\sigma(\delta) = \pm\delta$.

Zu (e): Wir zeigen, daß $\mathrm{Gal}(K/\mathbb{Q}) \subset \mathfrak{S}_3$ genau dann eine echte Untergruppe ist, wenn $\sigma(\delta) = \delta$ für alle $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.
Angenommen $\mathrm{Gal}(K/\mathbb{Q})$ ist eine echte Untergruppe, dann muß diese nach (c) Ordnung drei haben. Die einzige Untergruppe der Ordnung drei von $\mathfrak{S}_3$ ist die zyklische Gruppe $\{\mathrm{id}, (123), (213)\} = \langle(123)\rangle$. Für diese Permutationen gilt

$$\begin{aligned}
\mathrm{id}(\delta) &= \delta \\
(123)(\delta) &= (123)\left((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\right) = (\alpha_2-\alpha_3)(\alpha_2-\alpha_1)(\alpha_3-\alpha_1) = \delta \\
(231)(\delta) &= (213)\left((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\right) = (\alpha_3-\alpha_1)(\alpha_3-\alpha_2)(\alpha_1-\alpha_2) = \delta
\end{aligned}$$

Angenommen $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$, so enhält $\mathrm{Gal}(K/\mathbb{Q})$ Elemente der Ordnung 2, nämlich $\{(12), (23), (13)\}$. Für diese gilt

$$\begin{aligned}
(12)(\delta) &= (12)\left((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\right) = (\alpha_2-\alpha_1)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3) = -\delta \\
(23)(\delta) &= (23)\left((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\right) = (\alpha_1-\alpha_3)(\alpha_1-\alpha_2)(\alpha_3-\alpha_2) = -\delta \\
(13)(\delta) &= (13)\left((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\right)(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)(\alpha_2-\alpha_1) = -\delta
\end{aligned}$$

Gilt also $\sigma(\delta) = \delta$ für alle $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ so muß $\mathrm{Gal}(K/\mathbb{Q}) \subsetneq \mathfrak{S}_3$.

Aufgabe 2. Für $k \in \mathbb{Z}$ sei $a = k^2 + k + 7$. Man zeige: Das Polynom $X^3 - aX + a$ ist irreduzibel über $\mathbb{Q}$ und hat Galoisgruppe isomorph zu A_3.

Lösung. Für jede ganze Zahl k ist $k^2 + k + 7$ ungerade, denn da entweder k oder $k+1$ gerade ist, ist

$$k^2 + k + 7 = k(k+1) + 7 \equiv 0 + 1 \mod 2.$$

Für jede beliebige ungerade Zahl a nun ist

$$X^3 - aX + a \equiv X^3 + X + 1 \mod 2.$$

Und dies ist irreduzibel in $\mathbb{F}_2$, da es dort keine Nullstelle hat. Nach dem Reduktionskriterium ist also $X^3 - aX + a$ irreduzibel in $\mathbb{Z}$ und somit in $\mathbb{Q}$.

Wir berechnen nun die Diskriminante. Für ein beliebiges Polynom in $\mathbb{Q}[X]$ von folgender Form

$$X^3 + aX + b = (X - x_1)(X - x_2)(X - x_3) = X^3 - X^2(x_1 + x_2 + x_3) + X(x_1x_2 + x_2x_3 + x_1x_3) - x_1x_2x_3$$

gilt $x_1 + x_2 + x_3 = 0$, $x_1x_2 + x_2x_3 + x_1x_3 = a$, $-x_1x_2x_3 = b$. Damit gilt für die Diskriminante

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -4a^3 - 27b^2.$$

Die Diskriminante des Polynoms $X^3 - aX + a$ ist

$$D = -4(-a)^3 - 27a^2 = a^2(4a - 27).$$

Die Galoisgruppe von $X^3 - aX + a$ ist genau dann isomorph zu A_3, wenn D ein Quadrat in $\mathbb{Q}$ ist. Dies ist der Fall, wenn $4a - 27$ ein Quadrat ist. Wir berechnen

$$4a - 27 = 4(k^2 + k + 7) - 27 = 4k^2 + 4k + 1 = (2k + 1)^2.$$

Aufgabe 3 (Frühjahr 1978)**.** (a) Jede endliche abelsche Gruppe ist isomorph zu einer Faktorgruppe der Gruppe

$$\prod_p \mathbb{Z}/(p-1)\,\mathbb{Z},$$

wobei p alle Primzahlen durchläuft.
Hinweis: Man benutze den Dirichletschen Primzahlsatz: Zu jeder natürlichen Zahl n gibt es unendlich viele Primzahlen mit $p \equiv 1 \mod n$.

(b) Jede endliche abelsche Gruppe ist isomorph zu einer Faktorgruppe der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ der teilerfremden Reste modulo n, wenn n passend gewählt wird.

(c) Zu jeder endlichen abelschen Gruppe A gibt es eine Galois'sche Erweiterung $K/\mathbb{Q}$, deren Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ zu A isomorph ist.

(z) Man konstruiere eine Galoiserweiterung $K/\mathbb{Q}$ deren Galoisgruppe isomorph zu einer abelschen Gruppe der Ordnung 2019 ist.
Hinweis: 2693 ist prim in $\mathbb{Z}$.

Lösung. **Zu (a):** Sei A eine endliche abelsche Gruppe. Nach dem Hauptsatz über endliche abelsche Gruppen gibt es Primzahlpotenzen $q_1, \dots, q_r$ mit $A \cong \prod_{i=1}^r \mathbb{Z}/q_i\mathbb{Z}$. Nach dem Dirichlet'schen Primzahlsatz enthält jede Restklasse $1+q_i\mathbb{Z}$, $1 \leqslant i \leqslant r$, unendlich viele Primzahlen. Also gibt es paarweise verschiedene Primzahlen $p_1, \dots, p_r$ mit $p_i \equiv 1 \mod q_i$, $1 \leqslant i \leqslant r$. Die Abbildung

$$\gamma : \prod_{i=1}^r \mathbb{Z}/(p_i-1)\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/q_i\mathbb{Z}, z_i + (p_i-1)\mathbb{Z} \mapsto z_i + q_i\mathbb{Z}$$

ist surjektiver Gruppenhomomorphismus.
Sei weiter $\pi : \prod_p \mathbb{Z}/(p-1)\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/(p_i-1)\mathbb{Z}$ die kanonische Projektion. Dann ist die Komposition

$$\gamma' = \gamma \circ \pi : \prod_p \mathbb{Z}/(p-1)\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/(p_i - 1\mathbb{Z}) \to \prod_{i=1}^r \mathbb{Z}/q_i\mathbb{Z}$$

ebenso surjektiv und $G \cong \prod_{i=1}^r \mathbb{Z}/q_i\mathbb{Z} \cong \left(\prod_p \mathbb{Z}/(p-1)\mathbb{Z}\right)/\ker(\gamma')$ ist eine Darstellung von A als Faktorgruppe von $\prod_p \mathbb{Z}/(p-1)\mathbb{Z}$.

Zu (b): Sei A wie oben und $n = p_1 \cdots p_r$ das Produkt der paarweise verschiedenen Prizahlen aus (a). Dann gibt es nach dem chinesischen Restsatz einen Ringisomorphismus

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z}$$

und einen Gruppenisomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\prod_{i=1}^r} (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod_{i=1}^r \mathbb{Z}/(p_i-1)\mathbb{Z},$$

wobei die letzte Isomorphie daraus folgt, daß für jede Primzahl p $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch von der Ordnung $p-1$ ist.
Die Komposition des obigen Isomorphismus mit der surjektiven Abbildung γ aus (a) ergibt einen surjektive Gruppenhomomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^r \mathbb{Z}/(p_i-1)\mathbb{Z} \xrightarrow{\gamma} \prod_{i=1}^r \mathbb{Z}/q_i\mathbb{Z} \cong A,$$

und damit lässt sich A als Faktorgruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ darstellen.

Zu (c): Sei wieder A eine endliche abelsche Gruppe, $q_1, \dots, q_r$ und $n = p_1 \cdots p_r$ wie zuvor. Betrchte den n^{te} Kreisteilungskörper $\mathbb{Q}^{(n)}$ über $\mathbb{Q}$. Man hat die Gruppenhomomorphismen

$$\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^r (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod_{i=1}^r \mathbb{Z}/(p_i-1)\mathbb{Z} \xrightarrow{\gamma} \prod_{i=1}^r \mathbb{Z}/q_i\mathbb{Z} \cong A.$$

Die Komposition dieser Homomorphismen ist surjektiv. Sei N der Kern dieser Komposition, $K = \mathrm{Fix}_{\mathbb{Q}^{(n)}}(N)$. Da N Normalteiler ist, ist $K/\mathbb{Q}$ Galois'sch mit $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})/N \cong A$.

Zu (z): Die Primfaktorzerlegung von 2019 ist $2019 = 3 \cdot 673$ (siehe Einführung: es ist klar, daß 3 eine Primzahl ist; um zu zeigen, daß 673 eine Primzahl ist, testen wir alle Primzahlen bis $\sqrt{673} < \sqrt{676} = 26$). Es gibt bis auf Isomorphie genau eine abelsche Gruppe der Ordnung 2019, nämlich $\mathbb{Z}/2019\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/673\mathbb{Z}$.
Nun finden wir Primzahlen p_1, p_2 mit $p_1 \equiv 1 \mod (3)$ und $p_2 \equiv 1 \mod (673)$. Es ist leicht zu sehen, daß man $p_1 = 7$ wählen kann. Weiterhin berechnet man, daß $2693 \equiv 1 \mod (673)$ ist und nach Angabe ist 2693 prim. Wähle also $p_2 = 2693$.
Sei $n = p_1 \cdot p_2 = 7 \cdot 2693 = 18851$. Wir betrachten den 18851sten Kreiteilungskörper $\mathbb{Q}^{(18851)}$ über $\mathbb{Q}$. Nach (c) gibt es einen kanonischen surjektiven Gruppenhomomorphismus

$$\mathrm{Gal}(\mathbb{Q}^{(18851)}/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2692\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/673\mathbb{Z} \cong \mathbb{Z}/2019\mathbb{Z}.$$

Der Kern der Abbildung $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ ist $3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Der Kern der Abbildung $\mathbb{Z}/2692\mathbb{Z} \to \mathbb{Z}/673\mathbb{Z}$ ist $673\mathbb{Z}/2692\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$. Also ist der Kern von $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2692\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/673\mathbb{Z}$ gegeben durch $3\mathbb{Z}/6\mathbb{Z} \times 673\mathbb{Z}/2692\mathbb{Z}$ und hat Ordnung 8. Sei N das Urbild von $3\mathbb{Z}/6\mathbb{Z} \times 673\mathbb{Z}/2692\mathbb{Z}$ in $\mathrm{Gal}(\mathbb{Q}^{(18851)}/\mathbb{Q})$. Dann ist $N = N_1 \times N_2$ wobei N_1 das Urbild von $3\mathbb{Z}/6\mathbb{Z}$ ist und N_2 das Urbilds von $673\mathbb{Z}/2692\mathbb{Z}$. Sei $K = \mathrm{Fix}_{\mathbb{Q}^{(18851)}}(N)$, dann hat die Erweiterung $K/\mathbb{Q}$ die Galoisgruppe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/673\mathbb{Z}$. Wollen wir dies genauer bestimmen, so genügt es die Fixkörper $K_1 = \mathrm{Fix}_{\mathbb{Q}^{(7)}}(N_1)$ und $K_2 = \mathrm{Fix}_{\mathbb{Q}^{(2693)}}(N_2$ zu bestimmen.
Im ersten Fall müssen wir also einen Zwischenkörper $\mathbb{Q} \subset K_1 \subset \mathbb{Q}^{(7)} = \mathbb{Q}(\zeta_7)$ bestimmen, der Grad 3 über $\mathbb{Q}$ hat. Wir wissen von Blatt 19 Aufgabe 3, daß $[\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) : \mathbb{Q}] = \frac{1}{2}\varphi(7) = 3$. Dies ist also der gesuchte Zwischenkörper.
Im zweiten Fall geht dies wohl über den Stoff für das Examen hinaus.

Aufgabe 4 (Herbst 1992)**.** Es sei $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in K[X]$ ein nichtkonstantes separables Polynom mit $a_0 a_n \neq 0$. Sei $g = a_0 X^n + a_1 X^{n-1} + \ldots + a_{n-1}X + a_n$ das sogenannte „reziproke“ Polynom zu f. Zeigen Sie:
f und g haben die gleiche Galoisgruppe über K.

Lösung. Wir bemerken zunächst: da $a_0 \neq 0$ ist 0 keine Nullstelle von f. Ebendso ist 0 keine Nullstelle von g, weil $a_n \neq 0$. Sei L ein Zerfällungskörper von f und $x \in L$ eine Nullstelle von f. Dann ist auch $\frac{1}{x} \in L\backslash\{0\}$ und es ist klar, daß $\frac{1}{x} \in L$ eine Nullstelle von g ist:

$$\begin{aligned} g\left(\frac{1}{x}\right) &= a_0\left(\frac{1}{x}\right)^n + a_1\left(\frac{1}{x}\right)^{n-1} + \ldots + a_{n-1}\left(\frac{1}{x}\right) + a_n \\ &= \left(\frac{1}{x}\right)^n (a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n) \\ &= \left(\frac{1}{x}\right)^n f(x) = 0 \end{aligned}$$

Seien $x_1, \ldots, x_n \in L\backslash\{0\}$ die Nullstellen von f. Dann ist nach Definition $L = K(x_1, \ldots, x_n)$. Nach obiger Rechnung sind $\frac{1}{x_1}, \ldots, \frac{1}{x_n} \in L\backslash\{0\}$ die Nullstellen von g. Und $K(\frac{1}{x_1}, \ldots, \frac{1}{x_n})$ ist ein Zerfällungskörper von g. Es ist aber klar, daß

$$K(x_1, \ldots, x_n) = K(\frac{1}{x_1}, \ldots, \frac{1}{x_n}).$$

Da die Galoisgruppe eines Polynoms die Galoisgruppe eines Zerfällungskörpers ist, folgt

$$G(f) = \mathrm{Gal}(K(x_1, \ldots, x_n)/K) = \mathrm{Gal}(L/K) = \mathrm{Gal}(K(\frac{1}{x_1}, \ldots, \frac{1}{x_n})/K) = G(g)$$

was zu zeigen war.