Musterlösung Wiederholungsserie Sternaufgaben

*37. Zeige: Für jede Primzahl p und jede endliche p-Gruppe G und jede Untergruppe $H < G$ gilt

$$H = G \iff H \cdot [G, G] = G.$$

Lösung: Die Implikation $\Rightarrow$ ist klar. Für die Umkehrung zeigen wir zuerst, dass jede maximale echte Untergruppe von G Index p hat und normal ist. Sei $M < G$ eine maximale echte Untergruppe. Nach Proposition 5.6.4 der Vorlesung ist dann M echt in ihrem Normalisator enthalten. Dieser muss gleich G sein, weil M maximal ist. Daher ist M normal in G. Weil G eine p-Gruppe ist, ist sie auflösbar, also ist auch G/M auflösbar. Nach der Korrespondenz von Untergruppen von G/M und Untergruppen von G, die M enthalten folgt, dass G/M einfach ist, weil M eine maximale Untergruppe von G ist. Nun ist G/M einfach und auflösbar, muss also Primzahlordnung p haben, was wir zeigen wollten.

Sei nun $H < G$ eine Untergruppe mit $H \cdot [G, G] = G$. Angenommen H sei eine echte Untergruppe, dann existiert eine maximale echte Untergruppe $M \lneq G$ die H enthält. Der Index $[G : M]$ ist nach obigem Beweis p, also ist die Faktorgruppe G/M abelsch. Nach Aufgabe 3(b) von Serie 3 bedeutet dies $[G, G] < M$, also folgt $G = H \cdot [G, G] < M \lneq G$; Widerspruch. Daher folgt aus $H \cdot [G, G] = G$ auch $H = G$.

*38. Für jede natürliche Zahl $n \geqslant 1$ betrachte die von den Transpositionen (1 2), (3 4), $\ldots$, $(2^n{-}1\ 2^n)$ erzeugte Untergruppe Q_n der symmetrischen Gruppe S_{2^n}. Betrachte ausserdem die Einbettung $j\colon S_{2^{n-1}} \hookrightarrow S_{2^n}$, die für alle $\sigma \in S_{2^{n-1}}$ und $1 \leqslant i \leqslant 2^{n-1}$ gegeben ist durch $j(\sigma)(2i-1) = 2\sigma(i) - 1$ und $j(\sigma)(2i) = 2\sigma(i)$. Zeige:

(a) $Q_n \cong Z_2^{2^{n-1}}$.

(b) Der Normalisator von Q_n in S_{2^n} ist gleich $Q_n \rtimes j(S_{2^{n-1}})$.

Sodann konstruiere Untergruppen $P_n < S_{2^n}$ induktiv durch $P_0 := S_1$ und $P_n := Q_n \rtimes j(P_{n-1})$ für alle $n \geqslant 1$. Konstruiere Homomorphismen $\chi_{n,m}\colon P_n \to \{\pm 1\}$ für alle $n \geqslant m \geqslant 1$ durch $\chi_{n,n} := \operatorname{sgn}|P_n$ und $\chi_{n,m}(\tau \cdot j(\sigma)) := \chi_{n-1,m}(\sigma)$ für alle $\tau \in Q_n$ und $\sigma \in P_{n-1}$ im Fall $n > m$. Zeige:

(c) Die Gruppe P_n ist eine 2-Sylowgruppe von S_{2^n}. Bestimme ihre Ordnung.

(d) Der Homomorphismus $\underline{\chi}_n := (\chi_{n,m})_{m=1}^n\colon P_n \to \{\pm 1\}^n$ ist surjektiv.

(e) Der Kern dieses Homomorphismus ist die Kommutatorgruppe $[P_n, P_n]$.

(f) Folgere: Für jedes $n \geqslant 1$ und jede Untergruppe $G < P_n$ gilt $G = P_n$ genau dann, wenn die Einschränkung $\underline{\chi}_n|G\colon G \to \{\pm 1\}^n$ surjektiv ist.

Lösung:

(a) Die Transpositionen $(2i{-}1\ 2i)$ für alle $1 \leqslant i \leqslant 2^{n-1}$ haben Ordnung 2 und kommutieren miteinander; deshalb haben wir einen Homomorphismus

$$(\mathbb{Z}/2\mathbb{Z})^{2^{n-1}} \to Q_n, \quad (k_i)_{i=1}^{2^{n-1}} \mapsto \prod_{i=1}^{2^{n-1}} (2i{-}1\ 2i)^{k_i}.$$

Nach Konstruktion von Q_n ist dieser surjektiv. Er ist injektiv, da jedes $k_i \in \mathbb{Z}/2\mathbb{Z}$ durch die Wirkung der Permutation auf der Ziffer $2i-1$ bestimmt ist.

(b) Die Teilmenge $T_n := \{(2i{-}1\ 2i) \mid 1 \leqslant i \leqslant 2^{n-1}\}$ ist genau die Menge aller Transpositionen in Q_n. Der Normalisator $\mathrm{Norm}_{S_n}(Q_n)$ operiert daher auf T_n durch Konjugation. Umgekehrt bildet jedes Element von S_n, welches T_n auf sich abbildet, auch die davon erzeugte Untergruppe Q_n auf sich ab. Daher ist der Normalisator von Q_n genau der Stabilisator von T_n unter der Konjugationsoperation.

Nach Konstruktion liegen Q_n und $j(S_{2^{n-1}})$ darin. Ausserdem ist $Q_n \cap j(S_{2^{n-1}}) = \{1\}$; daher erzeugen diese beiden Gruppen zusammen ein semidirektes Produkt $Q_n \rtimes j(S_{2^{n-1}})$, das im gesuchten Normalisator enthalten ist.

Betrachte umgekehrt eine beliebige Permutation τ im Normalisator von Q_n. Dann existiert genau ein $\sigma \in S_{2^{n-1}}$, so dass $j(\sigma)$ die Transpositionen $(2i{-}1\ 2i)$ auf die gleiche Weise vertauscht wie τ. Somit fixiert die Permutation $\rho := \tau \cdot j(\sigma)^{-1}$ jede dieser Transpositionen unter Konjugation. Darum lässt ρ jedes Paar $\{2i{-}1, 2i\}$ invariant und liegt daher in der Gruppe Q_n. Insgesamt folgt daraus $\tau = \rho \cdot j(\sigma) \in Q_n \cdot j(S_{2^{n-1}})$. Zusammen zeigt dies

$$\mathrm{Norm}_{S_n}(Q_n) \ = \ Q_n \rtimes j(S_{2^{n-1}}).$$

(c) Offenbar hat jedes Q_n die Ordnung $|Z_2^{2^{n-1}}| = 2^{2^{n-1}}$, und nach Konstruktion gilt $|P_0| = 1$ sowie $|P_n| = |Q_n| \cdot |P_{n-1}|$ für alle $n \geqslant 1$. Daraus folgt

$$|P_n| \ = \ 2^{2^{n-1}} \cdot 2^{2^{n-2}} \cdots 2^1 \cdot 2^0 \ = \ 2^{2^{n-1}+2^{n-2}+\ldots+1+0} \ = \ 2^{2^n-1}.$$

Andererseits gilt für jede Primzahl p und jede natürliche Zahl m die Formel

$$\mathrm{ord}_p(m!) \ = \ \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \left\lfloor \frac{m}{p^3} \right\rfloor + \ldots,$$

was man für festes p leicht durch Induktion über m zeigen kann; siehe auch Seite 182 von
`http://www.fuchs-braun.com/media/532896481f9c1c47ffff8077fffffff0.pdf`.
Für $p = 2$ und $m = 2^n$ folgt daraus

$$\mathrm{ord}_2(|S_{2^n}|) \ = \ \left\lfloor \frac{2^n}{2} \right\rfloor + \left\lfloor \frac{2^n}{2^2} \right\rfloor + \left\lfloor \frac{2^n}{2^3} \right\rfloor + \ldots \ = \ 2^{n-1} + 2^{n-2} + \ldots \ = \ 2^n - 1.$$

Somit ist $[S_{2^n} : P_n]$ ungerade und P_n eine 2-Sylowgruppe von S_{2^n}.

(d) Offenbar ist $\underline{\chi}_n\colon P_n \to \{\pm 1\}^n$ surjektiv für $n = 0$. Gilt dies für $n-1$ anstatt n, so ist nach der induktiven Konstruktion von P_n und $\chi_{n,m}$ der Homomorphismus $(\chi_{n,m})_{m=1}^{n-1}\colon j(P_{n-1}) \to \{\pm 1\}^{n-1}$ surjektiv. Da auch $\chi_{n,n}|Q_n\colon Q_n \to \{\pm 1\}$ surjektiv ist, ist dann auch $\underline{\chi}_n := (\chi_{n,m})_{m=1}^{n}\colon P_n = Q_n \rtimes j(P_{n-1}) \to \{\pm 1\}^n$ surjektiv. Die Behauptung folgt also durch Induktion über n.

(e) Setze $P'_n := \mathrm{Kern}(\underline{\chi}_n)$. Da $P_n/P'_n \cong \{\pm 1\}^n$ abelsch ist, gilt $[P_n, P_n] < P'_n$. Mit $Q'_n := \mathrm{Kern}(\mathrm{sgn}\,|Q_n)$ ist andererseits $P'_1 = Q'_1 = \{1\}$ und $P'_n = Q'_n \rtimes j(P'_{n-1})$ für alle $n \geqslant 2$. Für die Gleichheit $[P_n, P_n] = P'_n$ genügt es daher zu zeigen, dass sowohl Q'_n als auch $j(P'_{n-1})$ in $[P_n, P_n]$ enthalten sind.

Aber für jedes $2 \leqslant i \leqslant 2^{n-1}$ erfüllt die Transposition $\sigma := (1\ i) \in S_{2^{n-1}}$ die Gleichungen $j(\sigma) = (1\ 2i{-}1)(2\ 2i)$ und somit $j(\sigma)(1\ 2)j(\sigma)^{-1} = (2i{-}1\ 2i)$ und daher

$$[P_n, P_n] \ \ni\ [j(\sigma), (1\ 2)] = (2i{-}1\ 2i)(1\ 2)^{-1} = (1\ 2)(2i{-}1\ 2i).$$

Da diese Permutationen die Gruppe Q'_n erzeugen, folgt daraus $Q'_n < [P_n, P_n]$. Zum anderen gilt trivialerweise $P'_1 = \{1\} < [P_1, P_1]$. Gilt ausserdem $P'_{n-1} < [P_{n-1}, P_{n-1}]$, so folgt auch $j(P'_{n-1}) < [j(P_{n-1}), j(P_{n-1})] < [P_n, P_n]$. Insgesamt folgt die Inklusion $P'_n < [P_n, P_n]$ daraus durch Induktion über n.

(f) Nach (d) und (e) induziert $\underline{\chi}_n$ einen Isomorphismus $P_n/[P_n, P_n] \xrightarrow{\sim} \{\pm 1\}^n$. Für eine Untergruppe $G < P_n$ ist daher $\underline{\chi}_n|G\colon G \to \{\pm 1\}^n$ genau dann surjektiv, wenn $G \cdot [P_n, P_n] = P_n$ ist. Da P_n eine p-Gruppe ist für $p = 2$, ist dies nach Aufgabe 37 äquivalent zu $G = P_n$.

**39. Bestimme die von allen Grundoperationen mit Rubiks Würfel erzeugte Symmetriegruppe und deren Ordnung. Wenn man den Würfel auseinandernimmt, auf wieviele verschiedene Arten kann man ihn wieder zusammensetzen, so dass die Resultate sich nicht durch eine Folge von Grundoperationen ineinander überführen lassen?

Lösung: See `https://en.wikipedia.org/wiki/Rubik%27s_Cube_group`

*40. (a) Zeige: Jede endliche Gruppe der Ordnung $2m$ mit m ungerade hat die Form $G = N \rtimes Z_2$ mit einer endlichen Gruppe N der Ordnung m und einem Homomorphismus $Z_2 \to \mathrm{Aut}(N)$.

(b) Zeige, dass zwei solche Gruppen mit demselben N genau dann isomorph sind, wenn die Bilder des Erzeugenden von Z_2 unter den beiden Homomorphismen $Z_2 \to \mathrm{Aut}(N)$ unter $\mathrm{Aut}(N)$ konjugiert sind.

(c) Bestimme alle Isomorphieklassen von Gruppen der Ordnung 18.

∗(d) Bestimme alle Isomorphieklassen von Gruppen der Ordnung 54.

∗(e) Zeige, dass die Aussage von (b) im Allgemeinen nicht stimmt, wenn N gerade Ordnung hat.

Lösung: (a) Nach Aufgabe 1 (a) von Serie 20 besitzt G eine normale Untergruppe N vom Index 2, und nach den Sylowsätzen eine Untergruppe H der Ordnung 2. Wegen der Ordnungen ist dann $N \cap H = \{1\}$ und $NH = G$. Also ist G das semidirekte Produkt $N \rtimes H$ mit einem Homomorphismus $Z_2 \cong H \to \mathrm{Aut}(N)$.

(b) Betrachte zwei Gruppen $G = N \rtimes H$ und $G' = N \rtimes H'$ zu Homomorphismen $Z_2 \cong H \to \mathrm{Aut}(N)$ und $Z_2 \cong H' \to \mathrm{Aut}(N)$.

Sind diese isomorph, so wählen wir einen Isomorphismus $\varphi\colon G \xrightarrow{\sim} G'$. Dann ist $\varphi(H)$ eine Untergruppe der Ordnung 2 von G', also eine 2-Sylowgruppe von G'. Nach den Sylowsätzen gilt daher $\varphi(H) = {}^xH'$ für ein $x \in G'$. Nach Ersetzen von φ durch $\mathrm{int}_x \circ \varphi$ können wir oBdA $\varphi(H) = H'$ annehmen. Dann induziert φ einen Isomorphismus $H \xrightarrow{\sim} H'$. Wegen $H \cong Z_2 \cong H'$ gibt es überhaupt nur einen solchen Isomorphismus; nennen wir ihn κ.

Sodann ist $\varphi(N)$ eine Untergruppe der Ordnung m von G', also ihr Bild in $G'/N \cong Z_2$ eine Untergruppe von ungerader Ordnung; also gleich 1. Somit ist $\varphi(N) < N$ und wegen der Gleichheit der Ordnungen also $\varphi(N) = N$. Daher ist $\psi := \varphi|N$ ein Automorphismus von N. Zusammen ist φ dann gegeben durch die Formel

$$(*) \qquad \varphi(nh) = \psi(n)\kappa(h) \qquad \text{für alle } n \in N \text{ und } h \in H.$$

Seien $\alpha, \alpha' \in \mathrm{Aut}(N)$ die Bilder der Erzeugenden unter den beiden Homomorphismen $Z_2 \cong H \to \mathrm{Aut}(N)$ und $Z_2 \cong H' \to \mathrm{Aut}(N)$. Eine schnelle Rechnung zeigt dann, dass die Formel $(*)$ für ein $\psi \in \mathrm{Aut}(N)$ genau dann einen Homomorphismus $G \to G'$ induziert, wenn $\alpha \circ \psi = \psi \circ \alpha'$ ist, das heisst, wenn $\alpha = \psi \circ \alpha' \circ \psi^{-1}$ ist. Ist also $G \cong G'$, so sind α und α' konjugiert in $\mathrm{Aut}(N)$.

Sind umgekehrt α und α' konjugiert in $\mathrm{Aut}(N)$, so existiert ein $\psi \in \mathrm{Aut}(N)$ mit $\alpha = \psi \circ \alpha' \circ \psi^{-1}$. Die obige Rechnung liefert dann einen Homomorphismus $G \to G'$; und da dieser automatisch bijektiv und somit ein Isomorphismus ist, ist (b) bewiesen.

(c) Nach (a) und (b) entsprechen die Isomorphieklassen von Gruppen der Ordnung $18 = 3^2 \cdot 2$ den Isomorphieklassen von Gruppen N der Ordnung $9 = 3^2$ zusammen mit der Konjugationsklasse eines Elements $\alpha \in \mathrm{Aut}(N)$ mit $\alpha^2 = 1$. Als Gruppe der Ordnung p^2 für p prim ist N abelsch und nach dem Klassifikationssatz daher

$$N \cong \mathbb{Z}/9\mathbb{Z} \qquad \text{oder} \qquad N \cong (\mathbb{Z}/3\mathbb{Z})^2 = \mathbb{F}_3^2.$$

Im Fall $N \cong \mathbb{Z}/9\mathbb{Z}$ ist $\mathrm{Aut}(N) \cong (\mathbb{Z}/9\mathbb{Z})^\times$. Dies ist eine abelsche Gruppe der Ordnung 6 und besitzt ± 1 als einzige Elemente α mit $\alpha^2 = 1$. Die beiden resultierenden Gruppen sind entsprechend

$$\begin{aligned} \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\cong \mathbb{Z}/18\mathbb{Z} = Z_{18}, \\ \mathbb{Z}/9\mathbb{Z} \rtimes \{\pm 1\} &\cong D_9. \end{aligned}$$

Im Fall $N \cong \mathbb{F}_3^2$ ist $\mathrm{Aut}(N) \cong \mathrm{GL}_2(\mathbb{F}_3)$. Für jede Matrix $\alpha \in \mathrm{GL}_2(\mathbb{F}_3)$ mit $\alpha^2 = 1$ teilt das Minimalpolynom das Polynom $(X^2 - 1) = (X - 1)(X + 1)$ mit den zwei verschiedenen einfachen Nullstellen $\pm 1 \in \mathbb{F}_3$. Daher ist α diagonalisierbar mit Eigenwerten in der Menge $\{\pm 1\}$. Somit ist α konjugiert zu einer der Matrizen

$$\alpha_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \alpha_1 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \alpha_2 := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Da diese drei Matrizen paarweise verschiedene charakteristische Polynome haben, sind sie nicht zueinander konjugiert; sie sind also Repräsentanten für die fraglichen Konjugationsklassen in $\mathrm{Aut}(N)$. Die drei resultierenden Gruppen sind entsprechend

$$\begin{aligned} \mathbb{F}_3^2 \times \mathbb{Z}/2\mathbb{Z} &\cong Z_6 \times Z_3, \\ \mathbb{F}_3^2 \rtimes \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\} &\cong D_3 \times Z_3, \\ \mathbb{F}_3^2 \rtimes \left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right\}. & \end{aligned}$$

(d) Nach (a) und (b) entsprechen die Isomorphieklassen von Gruppen der Ordnung $54 = 3^3 \cdot 2$ den Isomorphieklassen von Gruppen N der Ordnung $27 = 3^3$ zusammen mit der Konjugationsklasse eines Elements $\alpha \in \mathrm{Aut}(N)$ mit $\alpha^2 = 1$. Nach der Vorlesung gibt es genau 5 Isomorphieklassen für N. Für jede von diesen bestimmen wir die fraglichen Konjugationsklassen in $\mathrm{Aut}(N)$.

Fall 1: $N \cong \mathbb{Z}/27\mathbb{Z}$. In diesem Fall ist $\mathrm{Aut}(N) \cong (\mathbb{Z}/27\mathbb{Z})^\times$ und die einzigen Elemente α mit $\alpha^2 = 1$ sind ± 1. Also gibt es dann genau die Möglichkeiten

$$\begin{aligned} \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\cong Z_{54}, \\ \mathbb{Z}/27\mathbb{Z} \rtimes \{\pm 1\} &\cong D_{27}. \end{aligned}$$

Fall 2: $N \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Nach Aufgabe 4 der Wiederholungsserie Algebra II hat $\mathrm{Aut}(N)$ dann die Ordnung $3^3 \cdot 2^2$. Sei R eine 2-Sylowgruppe davon. Nach den Sylowsätzen liegt jedes Element $\alpha \in \mathrm{Aut}(N)$ der Ordnung 2 in einer 2-Sylowgruppe und daher in einem Konjugierten von R. Es gibt also höchstens 4 Konjugationsklassen von solchen Elementen. Betrachte die Automorphismen $(a, b) \mapsto (\lambda a, \mu b)$ von $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ für alle $\lambda, \mu \in \{\pm 1\}$. Da diese sich in der Anzahl ihrer Fixpunkte (nämlich 27, 9, 3, 1) unterscheiden, sind sie paarweise nicht konjugiert. Dies liefert also genau 4 Isomorphieklassen, nämlich

$$\begin{aligned} (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times Z_2 &\cong Z_{18} \times Z_3, \\ (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle &\cong Z_9 \times D_3, \\ (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \left\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle &\cong D_9 \times Z_3, \\ (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \left\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle. & \end{aligned}$$

Fall 3: $N \cong (\mathbb{Z}/3\mathbb{Z})^3 = \mathbb{F}_3^3$. Hier ist $\mathrm{Aut}(N) \cong \mathrm{GL}_3(\mathbb{F}_3)$. Analog zu (c) besitzen die Konjugationsklassen von Elementen α mit $\alpha^2 = 1$ die Repräsentanten

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

die insgesamt vier verschiedene Isomorphieklassen von Gruppen der Form $\mathbb{F}_3^3 \rtimes Z_2$ liefern.

Fall 4: (Skizze) Wir haben ein nicht-abelsches semidirektes Produkt $N \cong \mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. Hier gibt es das direkte Produkt $N \times Z_2$ sowie die Gruppe $\mathbb{Z}/9\mathbb{Z} \rtimes (\mathbb{Z}/9\mathbb{Z})^\times$, die sich in der Anzahl von Fixpunkten von α unterscheiden und daher nicht isomorph sind. Man kann zeigen, dass dies alle Isomorphieklassen liefert.

Fall 5: (Skizze) Wir haben ein nicht-abelsches semidirektes Produkt $N \cong (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$. Bis auf Isomorphie ist dann

$$N = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} < \mathrm{GL}_3(\mathbb{F}_3) \quad \text{mit Zentrum} \quad Z(N) = \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hier gibt es die Gruppen $N \rtimes \langle\alpha\rangle$ mit α gleich

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

die sich in der Anzahl von Fixpunkten von α auf N und auf $Z(N)$ unterscheiden und daher nicht isomorph sind. Man kann zeigen, dass dies alle Isomorphieklassen liefert.

(e) Sei $n \geqslant 3$ und $G = S_n \times \{\pm 1\}$. Dieses direkte Produkt entspricht dem trivialen Homomorphismus $\{\pm 1\} \to \mathrm{Aut}(S_n)$. Betrachte die normale Untergruppe $N := S_n \times \{1\}$ und das von dem Element $((1\ 2), -1)$ erzeugte Komplement H. Dann ist G auch das innere semidirekte Produkt $N \rtimes H$ mit $N \cong S_n$ und $H \cong \{\pm 1\}$. Jetzt entspricht die Operation von $((1\ 2), -1) \in H$ auf N aber der Konjugation mit $(1\ 2)$ auf S_n und ist daher nicht-trivial.

*41. *(Cohen-Lenstra Heuristik)* Wie in Aufgabe 4 von Serie 2 fixieren wir eine natürliche Zahl $n \geqslant 1$ und eine Menge X der Kardinalität n.

(a) Zeige: Die Anzahl der Isomorphieklassen von Gruppen der Ordnung n ist > 0 und $< \infty$. Seien $G_1, \ldots, G_r$ Repräsentanten dieser Isomorphieklassen.

(b) Sei S die Menge aller Gruppenstrukturen auf X, und für jedes i sei S_i die Teilmenge der Gruppenstrukturen, für die X isomorph zu G_i wird. Zeige, dass $|S_i|/|S| = c_n/|\mathrm{Aut}(G_i)|$ ist mit einer nur von n abhängigen Zahl $c_n \in \mathbb{Q}^{>0}$.

Bemerkung: Der Quotient $|S_i|/|S|$ ist die Wahrscheinlichkeit, dass eine zufällig gewählte Gruppenstruktur auf X eine zu G_i isomorphe Gruppe liefert. Da X beliebig ist, können wir dies interpretieren als die Wahrscheinlichkeit, dass eine zufällig gewählte Gruppe der Ordnung n isomorph zu G_i ist.

(c) Bestimme die Wahrscheinlichkeiten für alle Gruppen der Ordnungen $\leqslant 8$. Welche sind jeweils die häufigsten?

(d) Zeige: Für jede abelsche Gruppe der Form $G = G' \times G''$ gilt

$$|\operatorname{Aut}(G)| \;\geqslant\; |\operatorname{Aut}(G')| \cdot |\operatorname{Hom}(G', G'')| \cdot |\operatorname{Hom}(G'', G')|.$$

(e) Folgere, dass unter allen abelschen Gruppen der Ordnung n die zyklische Gruppe die grösste Wahrscheinlichkeit hat.

**(f) Gilt das Entsprechende unter allen Gruppen der Ordnung n?

Lösung:

(a) Die zyklische Gruppe der Ordnung n zeigt, dass es mindestens eine Isomorphieklasse gibt. Andererseits sei G eine beliebige Gruppe der Ordnung n. Jede Bijektion $\varphi\colon X \to G$ liefert dann eine Gruppenstruktur auf X, für die X isomorph zu G wird. Da es überhaupt nur endlich viele Abbildungen $X \times X \to X$ gibt, existieren auch nur endlich viele Gruppenstrukturen auf X. Somit gibt es nur endlich viele Isomorphieklassen von Gruppen der Ordnung n.

(b) Nach Aufgabe 4 (c) von Serie 2 gilt $|S_i| = n!/|\operatorname{Aut}(G_i)|$. Nach (a) ist ausserdem $0 < |S| < \infty$. Folglich ist

$$\frac{|S_i|}{|S|} \;=\; \frac{n!}{|S| \cdot |\operatorname{Aut}(G_i)|}$$

und die gesuchte Aussage gilt mit $c_n := n!/|S|$.

Bemerkung: Da die Summe der Wahrscheinlichkeiten 1 ergeben muss, kann man c_n auch ausdrücken als

$$c_n \;=\; \left(\sum_{i=1}^{r} \frac{1}{|\operatorname{Aut}(G_i)|}\right)^{-1}. \tag{1}$$

(c) Für $n \in \{1, 2, 3, 5, 7\}$ ist jede Gruppe der Ordnung n zyklisch mit Wahrscheinlichkeit 1. In den übrigen Fällen haben wir:

- $n = 4$: Hier gibt es genau zwei Isomorphieklassen mit Repräsentanten $C_4 \cong \mathbb{Z}/4\mathbb{Z}$ und $C_2^2 \cong \mathbb{F}_2^2$. Die Gruppe $\operatorname{Aut}(\mathbb{Z}/4\mathbb{Z}) = (\mathbb{Z}/4\mathbb{Z})^\times$ hat Ordnung 2, und $\operatorname{Aut}(\mathbb{F}_2^2) \cong \mathrm{GL}_2(\mathbb{F}_2)$ hat die Ordnung $(2^2-1)(2^2-2) = 6$. Nach (1) ergibt sich $c_4 = (\frac{1}{2} + \frac{1}{6})^{-1} = \frac{3}{2}$ und daher

G_i	$\lvert\operatorname{Aut}(G_i)\rvert$	$\lvert S_i\rvert/\lvert S\rvert$
$\mathbb{Z}/4\mathbb{Z}$	2	$\frac{3}{4}$
$\mathbb{F}_2^2$	6	$\frac{1}{4}$

- $n = 6$: Hier gibt es wieder genau zwei Isomorphieklassen mit Repräsentanten $C_6 \cong \mathbb{Z}/6\mathbb{Z}$ und $D_3 \cong S_3$. Für diese gilt einerseits $|\operatorname{Aut}(\mathbb{Z}/6\mathbb{Z})| = |(\mathbb{Z}/6\mathbb{Z})^\times| = 2$. Andererseits besteht S_3 aus den drei Transpositionen (1 2) und (1 3) und (2 3), den zwei 3-Zykeln (1 2 3) und (3 2 1), sowie dem Einselement. Ein Automorphismus von S_3 muss (1 2) auf ein Element der Ordnung 2, also eine Transposition, und (1 2 3) auf ein Element der Ordnung 3, also einen 3-Zykel abbilden. Umgekehrt ist jeder Automorphismus durch diese Bilder bestimmt, weil (1 2) und (1 2 3) die S_3 erzeugen. Daher gibt es insgesamt höchstens $3 \cdot 2 = 6$ Automorphismen. Schliesslich ist die natürliche Abbildung $S_3 \to \operatorname{Aut}(S_3)$, $\sigma \mapsto \operatorname{int}(\sigma)$ injektiv, weil das Zentrum von S_3 trivial ist. Darum besitzt S_3 schon $|S_3| = 6$ innere Automorphismen, und zusammen folgt daraus $|\operatorname{Aut}(S_3)| = 6$. Nach (1) ergibt sich $c_6 = (\frac{1}{2} + \frac{1}{6})^{-1} = \frac{3}{2}$ und daher

G_i	$\lvert\operatorname{Aut}(G_i)\rvert$	$\lvert S_i\rvert/\lvert S\rvert$
$\mathbb{Z}/6\mathbb{Z}$	2	$\frac{3}{4}$
D_3	6	$\frac{1}{4}$

- $n = 8$: Hier wissen wir schon, dass es genau fünf Isomorphieklassen gibt. Wir lassen die Einzelrechnungen weg und erhalten $c_8 = \frac{42}{23}$ und

G_i	$\lvert\operatorname{Aut}(G_i)\rvert$	$\lvert S_i\rvert/\lvert S\rvert$
C_8	4	$\frac{21}{46}$
$C_2 \times C_4$	8	$\frac{21}{92}$
D_4	8	$\frac{21}{92}$
Q	24	$\frac{7}{92}$
$\mathbb{F}_2^3$	168	$\frac{1}{92}$

In jedem Fall hat die zyklische Gruppe C_n die höchste Wahrscheinlichkeit.

(d) Betrachte eine additiv geschriebene abelsche Gruppe der Form $G = G' \times G''$. Erstens induziert dann jedes $\gamma \in \operatorname{Aut}(G')$ einen Automorphismus $\Gamma_\gamma : (g', g'') \mapsto (\gamma(g'), g'')$ von G. Zweitens betrachte für jedes $\varphi \in \operatorname{Hom}(G', G'')$ die Abbildung

$$\Phi_\varphi \colon\ G' \times G'' \longrightarrow G' \times G'',\quad (g', g'') \mapsto (g', \varphi(g') + g'').$$

Direktes Nachrechnen zeigt, dass dies ein Homomorphismus ist. Weiter gilt $\Phi_{-\varphi} \circ \Phi_\varphi = \Phi_\varphi \circ \Phi_{-\varphi} = \mathrm{id}$, daher ist Φ_φ sogar ein Automorphismus von G. Drittens induziert jedes $\psi \in \operatorname{Hom}(G'', G')$ analog einen Automorphismus

$$\Psi_\psi \colon\ G' \times G'' \longrightarrow G' \times G'',\quad (g', g'') \mapsto (g' + \psi(g'), g'').$$

Betrachte nun den zusammengesetzten Automorphismus $\Theta := \Phi_\varphi \circ \Gamma_\gamma \circ \Psi_\psi$ von $G' \times G''$. Für diesen gilt $\Theta((g', 0)) = \big(\gamma(g'), \varphi(\gamma(g'))\big)$ für alle $g' \in G'$, also ist zuerst γ und dann auch φ bereits durch Θ bestimmt. Weiter ist $\Theta((0, g'')) = \big(\gamma(\psi(g'')), \varphi(\gamma(\psi(g''))) + g''\big)$ für alle $g'' \in G''$, also ist auch $\gamma \circ \psi$ und somit ψ selbst durch Θ bestimmt. Daher haben wir eine injektive Abbildung

$$\mathrm{Aut}(G') \times \mathrm{Hom}(G', G'') \times \mathrm{Hom}(G'', G') \longrightarrow \mathrm{Aut}(G),\ (\gamma, \varphi, \psi) \mapsto \Phi_\varphi \circ \Gamma_\gamma \circ \Psi_\psi.$$

Daraus folgt direkt die gewünschte Ungleichung

$$|\mathrm{Aut}(G)| \ \geqslant\ |\mathrm{Aut}(G')| \cdot |\mathrm{Hom}(G', G'')| \cdot |\mathrm{Hom}(G'', G')|.$$

(e) Nach (b) müssen wir zeigen, dass für jede abelsche Gruppe G der Ordnung n gilt:

$$|\mathrm{Aut}(G)| \leqslant |\mathrm{Aut}(C_n)| \quad \Longrightarrow \quad G \cong C_n. \tag{2}$$

Behauptung: Die Aussage (2) gilt, wenn n eine Primpotenz ist.

Beweis: Nach dem Struktursatz für endliche abelsche Gruppen ist G isomorph zu $C_{p^{\nu_1}} \times \ldots \times C_{p^{\nu_r}}$ für eine Primzahl p und ganze Zahlen $\nu_1 \geqslant \ldots \geqslant \nu_r \geqslant 1$. Im Fall $r \leqslant 1$ ist G zyklisch und wir sind fertig. Andernfalls setzen wir $\nu := \nu_1$. Da wir G durch eine dazu isomorphe Gruppe ersetzen dürfen, können wir annehmen, dass $G = \mathbb{Z}/p^\nu\mathbb{Z} \oplus G'$ ist für eine additiv geschriebene Gruppe $G' \cong C_{p^{\nu_2}} \times \ldots \times C_{p^{\nu_r}}$. Nach Konstruktion gilt für diese dann $p^\nu G' = 0$ und $G' \neq 0$.

Erstens ist nun $\mathrm{Aut}(\mathbb{Z}/p^\nu\mathbb{Z}) \cong (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ und folglich

$$|\mathrm{Aut}(\mathbb{Z}/p^\nu\mathbb{Z})| \ =\ |(\mathbb{Z}/p^\nu\mathbb{Z})^\times| \ =\ (p-1)p^{\nu-1} \ \geqslant\ p^{\nu-1}. \tag{3}$$

Zweitens folgt aus $p^\nu G' = 0$, dass jedes $g' \in G'$ einen wohldefinierten Homomorphismus $\mathbb{Z}/p^\nu\mathbb{Z} \to G'$, $k + p^\nu\mathbb{Z} \mapsto kg'$ induziert. Somit gilt

$$|\mathrm{Hom}(\mathbb{Z}/p^\nu\mathbb{Z}, G')| \ \geqslant\ |G'|. \tag{4}$$

Auf analoge Weise implizieren $r \geqslant 2$ und $\nu_2 \geqslant 1$ die Ungleichung

$$|\mathrm{Hom}(\mathbb{Z}/p^{\nu_2}\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})| \ \geqslant\ p.$$

Durch Komposition mit der Projektion $G' \cong C_{p^{\nu_2}} \times \ldots \times C_{p^{\nu_r}} \twoheadrightarrow \mathbb{Z}/p^{\nu_2}\mathbb{Z}$ sowie der Injektion $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^\nu\mathbb{Z}$, $k + p\mathbb{Z} \mapsto p^{\nu-1}k + p^\nu\mathbb{Z}$ impliziert dies drittens die Ungleichung

$$|\mathrm{Hom}(G', \mathbb{Z}/p^\nu\mathbb{Z})| \ \geqslant\ p. \tag{4}$$

Durch Kombinieren von (3) bis (5) mit (d) folgt nun

$$|\operatorname{Aut}(G)| \;\geqslant\; p^{\nu-1} \cdot |G'''| \cdot p \;=\; p^{\nu} \cdot |G'''| \;=\; |G|.$$

Für die zyklische Gruppe der Ordnung $|G| = n$ gilt aber $\operatorname{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ und daher $|\operatorname{Aut}(C_n)| < n = |G|$. Also haben wir $|\operatorname{Aut}(G)| > |\operatorname{Aut}(C_n)|$ im Fall $r \geqslant 2$ und sind fertig. □

Behauptung: Die Aussage (2) gilt für alle natürlichen Zahlen $n \geqslant 1$.

Beweis: Nach dem Struktursatz für endliche abelsche Gruppen ist G isomorph zu einem Produkt von zyklischen Gruppen von Primpotenzordnung. Durch Zusammenfassen aller Faktoren zu derselben Primzahl erhalten wir eine Zerlegung $G = G_1 \times \ldots \times G_r$ mit abelschen Gruppen G_i der Ordnung $p_i^{\mu_i}$ für $\mu_i > 0$ und paarweise verschiedene Primzahlen $p_1, \ldots, p_r$. Jedes G_i ist dann die einzige p_i-Sylowgruppe von G. Für jeden Automorphismus γ von G ist auch $\gamma(G_i)$ eine p_i-Sylowgruppe von G und folglich gleich G_i. Somit induziert γ einen Automorphismus von G_i und ist umgekehrt durch diese bestimmt für alle i. Zusammen liefert dies einen natürlichen Isomorphismus

$$(\dagger_1) \qquad \operatorname{Aut}(G) \;\cong\; \operatorname{Aut}(G_1) \times \ldots \times \operatorname{Aut}(G_r).$$

Im Spezialfall der zyklischen Gruppe der Ordnung $n = p_1^{\mu_1} \cdots p_r^{\mu_r}$ haben wir $C_n \cong C_{p_1^{\mu_1}} \times \ldots \times C_{p_r^{\mu_r}}$ und folglich

$$(\dagger_2) \qquad \operatorname{Aut}(C_n) \;\cong\; \operatorname{Aut}(C_{p_1^{\mu_1}}) \times \ldots \times \operatorname{Aut}(C_{p_r^{\mu_r}}).$$

Für jedes i wissen wir nun nach (2) im Primpotenzfall bereits

$$|\operatorname{Aut}(G_i)| \;\geqslant\; |\operatorname{Aut}(C_{p_i^{\mu_i}})|,$$

mit Gleichheit nur im Fall $G_i \cong C_{p_i^{\mu_i}}$. Zusammen mit $(\dagger_1)$ und $(\dagger_2)$ folgt daraus

$$|\operatorname{Aut}(G)| \;\geqslant\; |\operatorname{Aut}(C_n)|,$$

mit Gleichheit nur im Fall $G \cong C_n$. Damit ist (2) allgemein bewiesen. □

Aliter: Für zusammengesetztes n verwende (d) und Induktion über die Anzahl der Faktoren.

(f) Besprechen Sie Ihre (Teil-)Ergebnisse mit Prof. Pink.

*42. Für jede ganze Zahl $n \geqslant 1$ sei Φ_n das n-te zyklotomische Polynom. Zeige:

(a) Für alle $m, n \geqslant 1$ und jedes $a \in \mathbb{Z}$ gilt

$$\operatorname{ggT}(a^m - 1, a^n - 1) \;\sim\; a^{\operatorname{ggT}(m,n)} - 1.$$

(b) Für alle $n \geqslant 2$ und $a \geqslant 2$ gilt $|\Phi_n(a)| > a - 1$.

(c) Für alle $n \geqslant 2$ und $a \geqslant 2$ ist $\Phi_n(a)$ kein Teiler von $a^n - a$.

Lösung:

(a) Sei $r := \mathrm{ggT}(m, n)$. Nach Ersetzen von (m, n, a) durch $(\frac{m}{r}, \frac{n}{r}, a^r)$ können wir ohne Beschränkung der Allgemeinheit $r = 1$ annehmen. Dann ist einerseits $\frac{a^m-1}{a-1} = 1 + a + \ldots a^{m-1} \in \mathbb{Z}$ und $\frac{a^n-1}{a-1} = 1 + a + \ldots a^{n-1} \in \mathbb{Z}$; also ist $d := \mathrm{ggT}(a^m - 1, a^n - 1)$ ein Vielfaches von $a - 1$. Umgekehrt ist nun $a^m \equiv 1 \equiv a^n$ modulo (d). Insbesondere ist die Restklasse von a modulo (d) ein Element der Einheitengruppe $(\mathbb{Z}/d\mathbb{Z})^\times$, und die Ordnung dieses Gruppenelements ist sowohl ein Teiler von m als auch von n. Wegen $\mathrm{ggT}(m, n) = 1$ ist diese Ordnung also gleich 1 und somit $a \equiv 1$ modulo (d). Daher ist d ein Teiler von $a - 1$, und insgesamt folgt daraus $d = a - 1$.

(b) Nach Definition des zyklotomischen Polynoms ist $\Phi_n(a) = \prod_\zeta (a - \zeta)$, wobei das Produkt über alle primitiven n-ten Einheitswurzeln ζ geht. Wegen $n \geqslant 2$ gilt für jede solche $\mathrm{Re}(\zeta) < 1$ und damit $\mathrm{Re}(a - \zeta) > a - 1 > 1$. Daraus folgt dann auch $|a - \zeta| > a - 1 > 1$ und daher $|\Phi_n(a)| > a - 1$.

(c) Nach (a) ist $\mathrm{ggT}(a^n-1, a^{n-1}-1) \sim a-1$. Wegen $\mathrm{ggT}(a^n-1, a) \sim \mathrm{ggT}(-1, a) \sim 1$ folgt daraus $\mathrm{ggT}(a^n - 1, a^n - a) \sim a - 1$. Nun ist aber $\Phi_n(a)$ ein Teiler von $a^n - 1$, und wegen (b) kein Teiler von $a - 1$. Also ist $\Phi_n(a)$ auch kein Teiler von $a^n - a$.

*43. *(Satz von Wedderburn)* Zeige: Jeder endliche Schiefkörper R ist kommutativ. Gehe dafür wie folgt vor:

(a) Das Zentrum $k := \{x \in R \mid \forall y \in R\colon xy = yx\}$ ist ein endlicher Körper. Setze $q := |k|$ und $n := \dim_k(R)$.

(b) Seien $C_1, \ldots, C_r$ die Konjugationsklassen der Gruppe $R^\times = R \smallsetminus \{0\}$ in $R \smallsetminus k$. Für jedes i ist dann $|C_i| = (q^n - 1)/(q^{n_i} - 1)$ für einen echten Teiler n_i von n.

(c) Folgere im Fall $n > 1$, dass $\Phi_n(q)$ ein Teiler von $q^n - q$ ist, im Widerspruch zur obigen Aufgabe 42.

Lösung: Siehe Chapter 6 von [Aigner-Ziegler: Proofs from the Book, Springer 2013]

`https://link.springer.com/book/10.1007/978-3-662-57265-8`

*44. Sei K ein Körper der Charakteristik 0 und sei X transzendent über K. Zeige, dass $K(X^2) \cap K(X^2 - X) = K$ ist.

Lösung: Die Erweiterungen $K(X)/K(X^2)$ und $K(X)/K(X^2 - X)$ haben Grad 2 und sind galoissch mit den jeweiligen nichttrivialen Galoisautomorphismen $\sigma(X) = -X$ und $\tau(X) = -X + 1$. Also ist $\sigma\tau$ ein Automorphismus von $K(X)$ über $K' :=$

$K(X^2) \cap K(X^2 - X)$ mit $\sigma(\tau(X)) = \sigma(-X + 1) = X + 1$. Für jede ganze Zahl $n > 0$ ist dann $(\sigma\tau)^n(X) = X + n$. Wegen $\mathrm{char}(K) = 0$ ist dies ungleich X und daher $(\sigma\tau)^n \neq \mathrm{id}$. Also ist $\sigma\tau$ ein Automorphismus von unendlicher Ordnung und somit auch $\mathrm{Aut}(K(X)/K')$ unendlich. Wäre aber $K' \neq K$, so enthielte K' ein transzendentes Element und $K(X)/K'$ wäre eine endliche Erweiterung. In diesem Fall wäre $|\mathrm{Aut}(K(X)/K')| \leqslant [K(X)/K'] < \infty$; Widerspruch.

*45. Sei F/K eine (nicht notwendigerweise algebraische) Körpererweiterung mit Zwischenkörpern K_1 und K_2, so dass F einen algebraischen Abschluss $\overline{K}_1$ von K_1 beziehungsweise $\overline{K}_2$ von K_2 enthält. Zeige oder widerlege:

(a) $\overline{K}_1 \cap \overline{K}_2$ ist ein algebraischer Abschluss von $K_1 \cap K_2$.

**(b) $\overline{K}_1\,\overline{K}_2$ ist ein algebraischer Abschluss von K_1K_2.

Lösung: (a) Die Aussage stimmt im allgemeinen nicht. Für ein Gegenbeispiel sei X transzendent über K, und sei F ein algebraischer Abschluss von $K(X)$. Dann ist $\overline{K}_1 := \overline{K}_2 := F$ auch ein algebraischer Abschluss der Unterkörper $K_1 := K(X^2)$ und $K_2 := K(X^2 - X)$. Nach der obigen Aufgabe 44 gilt aber $K_1 \cap K_2 = K$, sofern K die Charakteristik Null hat. Da F/K nicht algebraisch ist, ist $\overline{K}_1 \cap \overline{K}_2 = F$ dann kein algebraischer Abschluss von $K_1 \cap K_2$.

(b) Siehe Shreeram Abhyankar, "On the Compositum of Algebraically Closed Subfields", `http://repository.ias.ac.in/191/1/405.pdf`

*46. Sei K ein Körper und $L = K(t)$ der rationale Funktionenkörper über K in einer Variablen t.

(a) Zeige, dass für jeden Zwischenkörper $K \subsetneq K' \subset L$ die Erweiterung L/K' algebraisch und die Erweiterung K'/K transzendent ist.

(b) Sei $s = P(t)/Q(t) \in L$ für teilerfremde Polynome $P(X)$, $Q(X) \in K[X]$ mit $Q \neq 0$. Bestimme den Grad der Körpererweiterung $L/K(s)$ in Termen der Grade von P und Q.

(c) Zeige, dass die Körperautomorphismen von L, welche auf K die Identität sind, genau die Abbildungen der Form

$$L \to L,\ f(t) \mapsto f\Big(\frac{at + b}{ct + d}\Big)$$

sind für alle Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$.

Lösung: (a) Nimm ein beliebiges Element $s \in K' \smallsetminus K$, und schreibe $s = P(t)/Q(t)$ für teilerfremde Polynome $P(X)$, $Q(X) \in K[X]$ mit $Q \neq 0$. Dann ist t eine Nullstelle des Polynoms $F(X) := P(X) - s \cdot Q(X) \in K'[X]$.

Wir werden zeigen, dass dieses Polynom nicht identisch verschwindet. Sei dafür $b \in K$ der höchste nicht-verschwindende Koeffizient von $Q(X)$, und $a \in K$ der Koeffizient derselben Potenz von X in $P(X)$. Wenn $F(X)$ verschwindet, muss $a - sb = 0$ sein, also $s = a/b \in K$, im Widerspruch zur Annahme.

Da $F(X)$ nicht verschwindet, ist t algebraisch über K'. Wegen $s \in K(t)$ gilt nun $L = K(s,t) = K'(t)$. Nach einem Satz der Vorlesung ist also L/K' eine algebraische Erweiterung.

Wäre auch K'/K eine algebraische Erweiterung, so wäre nach einem Satz der Vorlesung ebenso L/K algebraisch. Aber $t \in L$ ist nicht algebraisch über K. Somit ist K'/K transzendent, wie zu zeigen war.

Insbesondere ist jedes Element von $L \smallsetminus K$ transzendent über K.

(b) Es ist $s \in K$ genau dann, wenn P und Q konstant sind, und in diesem Fall ist $[L/K(s)] = [L/K] = \infty$.

Sei also $s \notin K$ und P und Q nicht beide konstant. Die Überlegung in (a) zeigt dann genauer, daß $\deg(F) = \deg(Q)$ ist, falls $\deg(Q) \geqslant \deg(P)$ ist. In dem Fall $\deg(Q) < \deg(P)$ gilt dagegen offensichtlich $\deg(F) = \deg(P)$. Also ist $\deg(F)$ stets das Maximum der Grade von P und von Q. Wir werden zeigen, dass F irreduzibel in $K(s)[X]$ ist. Dann ist es bis auf einen Faktor in $K(s)^\times$ das Minimalpolynom von t über $K(s)$, und sein Grad ist gleich dem gesuchten Körpergrad $[L/K(s)]$.

Da s transzendent über K ist, können wir es für die folgende Überlegung als formale Unbestimmte auffassen. Nach Konstruktion liegt F in $K[s,X]$, was wir als Polynomring in zwei unabhängigen Variablen auffassen können. Dieser hat eindeutige Primfaktorzerlegung (siehe Algebra I). Es genügt daher zu beweisen, daß F als Element von $K[s,X]$ irreduzibel ist. Da F linear in s ist, kann es in $K[s,X]$ höchstens einen in s konstanten Faktor abspalten. Da aber P und Q als teilerfremd vorausgesetzt wurden, ist auch das nicht möglich.

(c) Betrachte zuerst eine beliebige Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. Dann ist $ct + d \neq 0$ und folglich $s := \frac{at+b}{ct+d} \in L$ wohldefiniert. Wegen $ad - bc \neq 0$ sind die Polynome $aX + b$ und $cX + d$ teilerfremd und mindestens eines hat den Grad 1. Nach Teil (b) ist daher $[K(t)/K(s)] = 1$ und somit $K(s) = K(t)$. Insbesondere ist s transzendent über K, und somit für jede rationale Funktion $f \in K(X)$ das Element $f(s) \in K(t)$ wohldefiniert. Also ist $K(t) \to K(t)$, $f(t) \mapsto f(s)$ ein wohldefinierter Körperhomomorphismus. Wegen $K(s) = K(t)$ ist dieser surjektiv und folglich bijektiv. Ausserdem ist er auf allen Konstanten in K die Identität. Dies zeigt die eine Richtung der Behauptung.

Für die andere Richtung betrachte einen beliebigen Automorphismus φ von L mit $\varphi|_K = \mathrm{id}_K$. Schreibe $s := \varphi(t) = P(t)/Q(t)$ wie in (b). Die Surjektivität von φ impliziert $L = K(s)$, also $[L/K(s)] = 1$, und aus (b) folgt, dass P und Q höchstens linear sind. Folglich ist $s = \frac{at+b}{ct+d}$ für gewisse $a, b, c, d \in K$. Wegen $L = K(s)$ ist s auch nicht konstant; daraus folgt $ad - bc \neq 0$. Da φ ein Körperhomomorphismus

mit $\varphi|_K = \mathrm{id}_K$ ist, folgt nun $\varphi(f(t)) = f(s)$ für alle $f \in K(X)$. Also hat φ die gesuchte Form.

**47. Der *Satz von Lüroth* besagt: Sei x transzendent über K, und sei $K \subsetneq L \subset K(x)$ ein Zwischenkörper. Dann ist $L = K(y)$ für ein $y \in L$. Beweise diesen Satz, oder lies einen Beweis und fasse das Wesentliche daran zusammen.

*48. Sei p eine Primzahl und sei $q = p^n$ für eine positive ganze Zahl n.

(a) Zeige: Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ teilt $X^q - X$ in $\mathbb{F}_p[X]$ genau dann, wenn sein Grad ein Teiler von n ist.

(b) Sei I_d die Menge der normierten, irreduziblen Polynome vom Grad d in $\mathbb{F}_p[X]$. Beweise die Gleichung
$$X^q - X = \prod_{d|n} \prod_{f \in I_d} f.$$

(c) Folgere daraus, dass gilt $\sum_{d|n} d|I_d| = q$.

(d) Bestimme die Anzahl der irreduziblen Polynome vom Grad 6, 7, 8 in $\mathbb{F}_2[X]$.

Lösungsskizze: Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$.

(a) Die Aussage ist invariant unter Multiplikation von f mit $\mathbb{F}_p^\times$; also können wir f als normiert annehmen. Dann ist f das Minimalpolynom über $\mathbb{F}_p$ von einem Element $a \in \overline{\mathbb{F}}_p$ und es gilt $d := \deg(f) = [\mathbb{F}_p(a)/\mathbb{F}_p]$. Nach Satz 6.7.1 (d) der Vorlesung gilt daher $\mathrm{Frob}_{p^d}(a) = a^{p^d} = a$.
Ist nun d ein Teiler von n, so folgt $a^{p^n} = \mathrm{Frob}_{p^n}(a) = (\mathrm{Frob}_{p^d})^{n/d}(a) = a$; also ist a eine Nullstelle des Polynoms $X^{p^n} - X$ und folglich f ein Teiler dieses Polynoms. Ist umgekehrt f ein Teiler von $X^{p^n} - X$, so liegt a in einem Zerfällungskörper dieses Polynoms; nach Satz 6.7.1 (e) der Vorlesung also in einer Erweiterung von $\mathbb{F}_p$ vom Grad n. Nach der Multiplikativität der Körpergrade ist dann $d = [k/\mathbb{F}_p]$ ein Teiler von n.

(b) Nach (a) sind die Faktoren auf der rechten Seite genau die normierten irreduziblen Faktoren der linken Seite. Wegen $\frac{d}{dX}(X^q - X) = -1 \in \mathbb{F}_p^\times$ ist die linke Seite aber separabel und hat deshalb keine mehrfachen irreduziblen Faktoren. Da sie ausserdem normiert ist, folgt die Gleichheit.

(c) Vergleiche den Grad auf der rechten und linken Seite in (b).

(d) Nach (c) gilt $2^6 = |I_1| + 2|I_2| + 3|I_3| + 6|I_6|$. Die irreduziblen Polynome vom Grad $\leqslant 3$ können wir schnell abzählen und finden $|I_6| = \frac{64-2-2\cdot1-3\cdot2}{6} = 9$.
Analog gilt $2^7 = |I_1| + 7|I_7|$ und daher $|I_7| = \frac{128-2}{7} = 18$.
Nach (c) gilt $2^8 = |I_1| + 2|I_2| + 4|I_4| + 8|I_8|$ und $2^4 = |I_1| + 2|I_2| + 4|I_4|$ und daher $2^8 - 2^4 = 8|I_8|$, also $|I_8| = \frac{256-16}{8} = 30$.

*49. Für welche Werte von $k \geqslant 1$ ist die Körpererweiterung $\mathbb{F}_7(X)/\mathbb{F}_7(X^k)$

(a) separabel?

(b) normal?

(c) galoissch?

Lösung: Mit der Variablen X ist auch $Y := X^k$ transzendent über $\mathbb{F}_7$. Sodann ist X eine Nullstelle des normierten Polynoms $f(T) := T^k - Y$. Nach dem Eisensteinkriterium für das Primelement Y ist $f(T)$ aber irreduzibel in $\mathbb{F}_7(Y)[T]$. Daher ist f das Minimalpolynom von X über $\mathbb{F}_7(Y)$.

(a) Die Körpererweiterung ist genau dann separabel, wenn f separabel ist. Da f irreduzibel ist, ist dies äquivalent dazu, dass $\frac{df}{dT} = kT^{k-1}$ nicht verschwindet. Dies ist genau dann der Fall, wenn k nicht durch 7 teilbar ist.

(b) Das Polynom $f(T)$ hat genau die Nullstellen ζX für alle k-ten Einheitswurzeln ζ in einem algebraischen Abschluss von $\mathbb{F}_7(X)$. Also ist die Erweiterung normal genau dann, wenn alle diese ζ schon in $\mathbb{F}_7(X)$ liegen. Nun ist aber jedes solche ζ algebraisch über $\mathbb{F}_7$. Nach der obigen Aufgabe 46 (a) ist aber jedes Element von $\mathbb{F}_7(X) \smallsetminus \mathbb{F}_7$ transzendent über $\mathbb{F}_7$. Somit brauchen wir genau, dass alle k-ten Einheitswurzeln in $\mathbb{F}_7$ liegen.

Schreibe $k = \ell \cdot 7^n$ mit $7 \nmid \ell$. Dann gilt $X^k - 1 = (X^\ell - 1)^{7^n}$ über $\mathbb{F}_7$, also ist jede k-te Einheitswurzel in L schon eine ℓ-te Einheitswurzel. Dagegen ist $X^\ell - 1$ separabel über $\mathbb{F}_7$, also ist die Gruppe der ℓ-ten Einheitswurzeln in einem algebraischen Abschluss von $\mathbb{F}_7$ zyklisch der Ordnung ℓ. Weil $\mathbb{F}_7^\times$ zyklisch der Ordnung 6 ist, folgt daraus, dass $\mathbb{F}_7$ genau dann alle k-ten Einheitswurzeln enthält, wenn ℓ ein Teiler von 6 ist.

Insgesamt ist die Körpererweiterung also normal genau für

$$k \in \big\{7^n, 2 \cdot 7^n, 3 \cdot 7^n, 6 \cdot 7^n \;\big|\; n \geqslant 0\big\}.$$

(c) Nach (a) und (b) ist die Erweiterung genau dann normal und separabel, wenn $k \in \{1, 2, 3, 6\}$ ist.

*50. Zeige, dass die Substitutionen $t \mapsto 1/t$ und $t \mapsto 1 - t$ eine endliche Untergruppe G der Automorphismengruppe des rationalen Funktionenkörpers $L := \mathbb{Q}(t)$ erzeugen. Bestimme den Fixkörper $K := L^G$ in der Form $K = \mathbb{Q}(s)$ sowie das Minimalpolynom von t über K.

Lösung: Die Menge der Substitutionen

$$t \mapsto t, \quad t \mapsto \frac{1}{t}, \quad t \mapsto 1 - t, \quad t \mapsto \frac{1}{1-t}, \quad t \mapsto 1 - \frac{1}{t}, \quad t \mapsto \frac{t}{t-1}$$

wird von $t \mapsto 1/t$ und $t \mapsto 1 - t$ erzeugt und ist unter Komposition und Inversenbildung abgeschlossen, also ist G genau die Menge der von diesen Substitutionen

induzierten Automorphismen von L; insbesondere ist $|G| = 6$. (Man überprüft übrigens leicht, dass G nicht kommutativ und daher isomorph zu S_3 ist.)

Nach Konstruktion ist das Polynom $f(X) := \prod_{\sigma\in G}(X - \sigma(t))$ invariant unter G, also liegen seine Koeffizienten in K. Explizite Rechnung liefert

$$\begin{aligned} f(X) &= (X-t)(X-\tfrac{1}{t})(X-(1-t))(X-\tfrac{1}{1-t})(X-(1-\tfrac{1}{t}))(X-\tfrac{t}{t-1}) \\ &= X^6 - 3X^5 - sX^4 + (2s+5)X^3 - sX^2 - 3X + 1 \end{aligned}$$

mit

$$s \;:=\; \frac{t^6 - 3t^5 + 5t^3 - 3t + 1}{t^2(1-t)^2} \;\in\; K.$$

Nach der obigen Aufgabe 46 (b) ist $[L/\mathbb{Q}(s)]$ das Maximum von Zählergrad und Nennergrad von s, also gleich 6. Nach Satz 7.1.5 der Vorlesung ist andererseits $[L/K] = |G| = 6$. Wegen $\mathbb{Q}(s) \subset K$ folgt daraus $K = \mathbb{Q}(s)$. Schliesslich ist t eine Nullstelle des normierten Polynoms $f \in K[X]$ vom Grad $6 = [L/K] = [K(t)/K]$; also ist f das Minimalpolynom von t über K.

*51. Sei m ungerade, und sei K ein Körper der Charakteristik 0, der alle m-ten Einheitswurzeln enthält. Sei f ein irreduzibles Polynom der Form

$$f(X) = X^{2m} - 2aX^m + 1 \in K[X].$$

Zeige:

(a) Jeder Stammkörper L von f über K ist bereits ein Zerfällungskörper.

(b) Die Galoisgruppe $\mathrm{Gal}(L/K)$ ist isomorph zur Diedergruppe D_m.

(c) Bestimme alle Zwischenkörper von L/K.

Lösung: (a) Seien α eine Nullstelle von f in einem algebraischen Abschluss $\overline{K}$ von K und $\zeta_m \in K$ eine primitive m-te Einheitswurzel. Wegen $f(\zeta_m^i\alpha) = f(\alpha) = 0$ ist

$$A \;:=\; \left\{\zeta_m^i\alpha \;\middle|\; 0 \leqslant i \leqslant m-1\right\} \;\subset\; K(\alpha)$$

eine Teilmenge der Menge der Nullstellen von f. Wegen $f(0) = 1 \neq 0$ ist $\alpha \neq 0$, und weil ζ_m eine primitive m-te Einheitswurzel ist, folgt $|A| = m$. Weiter gilt $f(\alpha^{-1}) = \alpha^{-2m} - 2a\alpha^{-m} + 1 = \alpha^{-2m}f(\alpha) = 0$. Also ist auch α^{-1} eine Nullstelle von f, und daher genauso jedes Element von

$$A' \;:=\; \left\{\zeta_m^i\alpha^{-1} \;\middle|\; 0 \leqslant i \leqslant m-1\right\} \;\subset\; K(\alpha).$$

Diese Menge hat ebenfalls die Kardinalität $|A'| = m$. Ausserdem sind die Mengen A und A' disjunkt: Denn andernfalls existiert ein $0 \leqslant i \leqslant m-1$ mit $\alpha^{-1} = \zeta_m^i\alpha$. Daraus folgt $\alpha^2 = \zeta_m^{-i}$ und folglich $\alpha^{2m} = 1$, also ist α eine Nullstelle des Polynoms $X^{2m} - 1$. Nach Voraussetzung ist f das Minimalpolynom von α über K, also ist f

dann ein Teiler von $X^{2m}-1$. Aus Gradgründen muss somit $f(X) = X^{2m}-1$ sein, was aber wegen der konstanten Koeffizienten nicht der Fall ist. Somit sind A und A' disjunkt.

Insgesamt folgt nun $|A \cup A'| = 2m$; also ist $A \cup A'$ genau die Nullstellenmenge von f. Wegen $A \cup A' \subset K(\alpha)$ ist der Stammkörper $K(\alpha)$ von f auch schon ein Zerfällungskörper. Damit ist die Aussage bewiesen.

(b) Die Diedergruppe D_m ist von einer Spiegelung s der Ordnung 2 und einer Drehung t der Ordnung m erzeugt mit der Relation $sts^{-1} = t^{-1}$. Wir zeigen, dass $\Gamma := \mathrm{Gal}(L/K)$ von zwei Elementen σ und τ mit den entsprechenden Eigenschaften erzeugt wird. Daraus folgt dann die gewünschte Isomorphie $\Gamma \cong D_m$.

Sei $L = K(\alpha)$ der oben gefundene Zerfällungskörper von f. Als Zerfällungskörper eines Polynoms ist L/K normal. Wegen $\mathrm{char}(K) = 0$ ist L/K separabel. Folglich ist L/K galoissch und es gilt

$$|\Gamma| = [L/K] = \deg(f) = 2m.$$

Da f irreduzibel ist, operiert Γ transitiv auf der Menge der Nullstellen $A \cup A'$. Wegen $L = K(\alpha)$ ist ausserdem jedes Element von Γ bereits durch seine Wirkung auf α bestimmt. Somit existieren eindeutige $\sigma, \tau \in \Gamma$ mit $\sigma(\alpha) = \alpha^{-1}$ und $\tau(\alpha) = \zeta_m \alpha$. Dann ist $\sigma^2(\alpha) = \alpha$ und somit $\sigma^2 = \mathrm{id}$; wegen $\sigma(\alpha) \neq \alpha$ hat σ daher die Ordnung 2. Weiter gilt $\tau^i(\alpha) = \zeta_m^i \alpha$ für jedes $i \in \mathbb{Z}$, und dieses ist gleich α genau dann, wenn $m|i$ ist. Somit ist $\tau^i = \mathrm{id}$ genau dann, wenn $m|i$ ist; also hat τ die Ordnung m. Ausserdem gilt

$$\tau\sigma\tau(\alpha) = \tau\sigma(\alpha^{-1}) = \tau(\zeta_m^{-1}\alpha^{-1}) = \zeta_m^{-1}\alpha = \sigma^{-1}(\alpha),$$

woraus $\tau\sigma\tau = \sigma^{-1}$ folgt. Damit erzeugen σ und τ eine zu D_m isomorphe Untergruppe $\langle \sigma, \tau \rangle < \Gamma$. Wegen $|D_m| = 2m = |\Gamma|$ folgt aus der Inklusion schliesslich die gewünschte Gleichheit.

(c) Jede Untergruppe ungerader Ordnung von Γ ist enthalten in der zyklischen Untergruppe $\langle \tau \rangle$ der Ordnung m, also gleich $\langle \tau^k \rangle$ für einen Teiler $k|m$. Wegen

$$\tau^k(\alpha^{m/k}) = \tau^k(\alpha)^{m/k} = (\zeta_m^k \alpha)^{m/k} = \zeta_m^m \alpha^{m/k} = \alpha^{m/k}$$

liegt $\alpha^{m/k}$ in dem zu $\langle \tau^k \rangle$ gehörenden Zwischenkörper $L^{\langle \tau^k \rangle}$. Also gilt $K(\alpha^{m/k}) \subset L^{\langle \tau^k \rangle}$. Betrachte andererseits das Polynom $X^{m/k} - \alpha^{m/k} \in K(\alpha^{m/k})[X]$. Da α eine Nullstelle dieses Polynoms ist, hat sein Minimalpolynom über $K(\alpha^{m/k})$ den Grad $\leqslant m/k$, und es folgt

$$[L/K(\alpha^{m/k})] = [K(\alpha^{m/k})(\alpha)/K(\alpha^{m/k})] \leqslant m/k = |\langle \tau^k \rangle| = [L/L^{\langle \tau^k \rangle}].$$

Wegen $K(\alpha^{m/k}) \subset L^{\langle \tau^k \rangle}$ folgt daraus

$$(*) \qquad L^{\langle \tau^k \rangle} = K(\alpha^{m/k}).$$

Jede Untergruppe gerader Ordnung $\Delta < \Gamma$ enthält ein Element der Ordnung 2. Da m ungerade ist, bilden die Elemente der Ordnung 2 von Γ genau die Konjugationsklasse der Spiegelung σ. Nach Konjugation von Δ betrachten wir daher zuerst den Fall $\sigma \in \Delta$. Dann ist weiter $\Delta \cap \langle\tau\rangle = \langle\tau^k\rangle$ für einen Teiler $k|m$, und folglich $\Delta = \langle\tau^k, \sigma\rangle$ der Ordnung $2k$.

Der zugehörige Fixkörper L^Δ ist dann in dem bereits bekannten Fixkörper $L^{\langle\tau^k\rangle} = K(\alpha^{m/k})$ enthalten, und es gilt $[L^{\langle\tau^k\rangle}/L^\Delta] = [\Delta : \langle\tau^k\rangle] = 2$. Um L^Δ zu bestimmen, suchen wir also ein Element von $K(\alpha^{m/k})$, das zusätzlich invariant unter $\sigma\colon \alpha \mapsto \alpha^{-1}$ ist und dabei möglichst nichttrivial ist. Dafür nehmen wir $\beta_k := \alpha^{m/k} + \alpha^{-m/k}$. Dieses Element ist offenbar invariant unter Δ, also gilt $K(\beta_k) \subset L^\Delta$. Da $\alpha^{m/k}$ eine Nullstelle des Polynoms $X^2 - \beta_k X + 1 \in K(\beta_k)[X]$ ist, folgt wie oben

$$[K(\alpha^{m/k})/K(\beta_k)] \leqslant 2 = [K(\alpha^{m/k})/L^\Delta].$$

Wegen $K(\beta_k) \subset L^\Delta$ folgt daraus $K(\beta_k) = L^\Delta$.

Schliesslich hat jede Untergruppe gerader Ordnung die Form ${}^\gamma\Delta$ für ein $\Delta = \langle\tau^k, \sigma\rangle$ wie oben und ein $\gamma \in \Gamma$. Wegen $\sigma \in \Delta$ gilt ${}^{\gamma\sigma}\Delta = {}^\gamma\Delta$; nach etwaigem Ersetzen von γ durch $\gamma\sigma$ können wir also oBdA $\gamma = \tau^i$ annehmen für ein $0 \leqslant i < m$. Nach Teil (c) des Hauptsatzes der Galoistheorie ist der entsprechende Fixkörper dann

$$(**) \qquad L^{({}^{\tau^i}\Delta)} = \tau^i(L^\Delta) = \tau^i(K(\beta_k)) = K(\tau^i(\beta_k)) = K\big((\zeta_m^i\alpha)^{m/k} + (\zeta_m^i\alpha)^{-m/k}\big).$$

Mit $(*)$ und $(**)$ haben wir alle Zwischenkörper von L/K bestimmt.

*52. In dieser Aufgabe beweisen wir den Fundamentalsatz für die Algebra mit Hilfe von Galoistheorie. Sei $K/\mathbb{R}$ eine endliche Körpererweiterung.

(a) Nimm an, $K/\mathbb{R}$ sei galoissch. Zeige, dass ein Körperturm $K = K_n/\ldots/K_0/\mathbb{R}$ existiert, sodass $[K_0/\mathbb{R}]$ ungerade ist und für jedes $0 \leqslant i \leqslant n-1$ die Erweiterung K_{i+1}/K_i den Grad 2 hat.

(b) Zeige, dass $\mathbb{R}$ keine nichttriviale Erweiterung von ungeradem Grad hat.

(c) Zeige, dass jede Erweiterung von $\mathbb{R}$ vom Grad 2 isomorph zu $\mathbb{C}$ ist.

(d) Zeige, dass $\mathbb{C}$ keine Erweiterung vom Grad 2 hat.

(e) Folgere, dass K entweder $\mathbb{R}$ oder $\mathbb{C}$ ist.

Lösung: (a) Set $G := \mathrm{Gal}(K/\mathbb{R})$. Write $|G| = 2^n m$ with an odd integer m. By Sylow, there exists a subgroup $G_0 < G$ of order $|G_0| = 2^n$. By the Galois correspondence, there is then an intermediate field K_0 such that

$$[K_0/\mathbb{R}] = [G : G_0] = m = \text{odd}.$$

Next, since G_0 is a p-group for $p = 2$, it is solvable and possesses a chain of subgroups $1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0$ with successive indices $[G_i : G_{i+1}] = 2$. By

the Galois correspondence, this chain corresponds to a chain of intermediate fields $K = K_n \supset \ldots \supset K_0$ with $[K_{i+1} : K_i] = 2$.

(b) Suppose that $[K/\mathbb{R}]$ is odd. Take any element $\alpha \in K$ and let $f \in \mathbb{R}[X]$ be its minimal polynomial over $\mathbb{R}$. Then $\deg(f) = [\mathbb{R}(\alpha)/\mathbb{R}]$ divides $[K/\mathbb{R}]$ and is therefore also odd. By the Intermediate Value Theorem f then has a zero $\beta \in \mathbb{R}$. Thus $(X - \beta)$ divides f in $\mathbb{R}[X]$; but since f is already irreducible over $\mathbb{R}$ by assumption, we must have $f(X) = X - \beta$. Thus $\alpha = \beta \in \mathbb{R}$. This shows that every element of K already lies in $\mathbb{R}$; hence $K = \mathbb{R}$.

(c) If $[K/\mathbb{R}] = 2$, we have $K = \mathbb{R}(\alpha)$ for some element $\alpha \in K \setminus \mathbb{R}$. After a linear substitution we may assume that $\alpha^2 \in \mathbb{R}$. The minimal polynomial of α over $\mathbb{R}$ is then $X^2 - \alpha^2$. As this is irreducible over $\mathbb{R}$, we must have $\alpha^2 < 0$, because otherwise it would have a real zero. Let β be the positive real square root of $|\alpha^2|$. Then $K = \mathbb{R}(\alpha) = \mathbb{R}(\frac{\alpha}{\beta})$ with $(\frac{\alpha}{\beta})^2 = \frac{\alpha^2}{\beta^2} = -1$. Thus $K \cong \mathbb{C}$ over $\mathbb{R}$ with $\frac{\alpha}{\beta} \leftrightsquigarrow i$.

(d) If $[K/\mathbb{C}] = 2$, we have $K = \mathbb{C}(\alpha)$ for some element $\alpha \in K \setminus \mathbb{C}$. After a linear substitution we may assume that $\alpha^2 \in \mathbb{C}$. The minimal polynomial of α over $\mathbb{R}$ is then $X^2 - \alpha^2$. But every complex number has a square root in $\mathbb{C}$; so this polynomial is reducible over $\mathbb{C}$; contradiction.

(e) Suppose first that $K/\mathbb{R}$ is Galois, and let $K = K_n/\ldots/K_0/\mathbb{R}$ be as in (a). Then $K_0 = \mathbb{R}$ by (b). If $n = 0$, it follows that $K = \mathbb{R}$. Otherwise (c) implies that $K_1 \cong \mathbb{C}$, and (d) implies by induction that $K_i = K_1$ for all $1 \leqslant i \leqslant n$. Thus $K = K_n \cong \mathbb{C}$.

For general K let L be a Galois closure of $K/\mathbb{R}$. Then the preceding case shows that $L \cong \mathbb{R}$ or $\mathbb{C}$; hence the same follows for K.

*53. Sei L/K eine endliche Körpererweiterung vom Grad m. Für jedes $\alpha \in L$ ist die *Spur* $\mathrm{Tr}_{L/K}(\alpha)$ definiert als Spur der K-linearen Abbildung $\mu_\alpha \colon L \to L$, $x \mapsto \alpha x$. Zeige:

(a) Ist $X^n + \sum_{k=0}^{n-1} a_k X^k$ das Minimalpolynom von $\alpha \in L$ über K, so gilt für die Spur $\mathrm{Tr}_{L/K}(\alpha) = -\frac{m}{n} a_{n-1}$.

(b) Die Spur induziert eine K-lineare Abbildung $\mathrm{Tr}_{L/K} \colon L \to K$.

(c) Ist L/K separabel und $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_m\}$ für einen algebraischen Abschluss $\overline{K}$ von K, so gilt $\mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_m(\alpha)$.

(d) Ist L/K separabel, so ist die Spurabbildung $\mathrm{Tr}_{L/K} \colon L \to K$ surjektiv.

(e) Benutze dies, um den zu der Untergruppe $\{1, 2, 4\} < \mathbb{F}_7^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_7)/\mathbb{Q})$ gehörenden Zwischenkörper explizit zu konstruieren.

(*f) Zeige allgemein: Für jede Primzahl p und jede Untergruppe $H < \mathbb{F}_p^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ und jede primitive p-te Einheitswurzel ζ gilt

$$\mathbb{Q}(\mu_p)^H = \mathbb{Q}\Big(\sum_{h \in H} \zeta^h\Big).$$

Beachte: Die Spur einer quadratischen Matrix ist definiert als die Summe ihrer Diagonaleinträge. Als minus der zweithöchste Koeffizient des charakteristischen Polynoms ist sie invariant unter Ähnlichkeit. (Vergleiche Lineare Algebra I Wiederholungsserie Aufgabe 4.) Für jeden Endomorphismus φ eines endlich dimensionalen K-Vektorraums mit Basis B ist die Spur der Darstellungsmatrx ${}_B[\varphi]_B$ folglich unabhängig von B, hängt also nur von φ ab, und heisst die *Spur von* φ, englisch trace, geschrieben $\mathrm{Tr}(\varphi)$.

Lösungsskizze: (a) Da α den Grad n über K hat, ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine Basis von $K(\alpha)$ über K. Sei ausserdem $(\beta_1, \ldots, \beta_{m/n})$ eine Basis von L über $K(\alpha)$. Wie im Beweis der Multiplikativität des Körpergrads ist dann

$$(\beta_1, \alpha\beta_1, \ldots, \alpha^{n-1}\beta_1, \beta_2, \ldots, \alpha^{n-1}\beta_{m/n})$$

eine Basis von L über K. Bezüglich dieser hat die Darstellungsmatrix von μ_α die Blockform

$$\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & B \end{pmatrix} \quad \text{für} \quad B := \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & \vdots & -a_1 \\ 0 & \ddots & 0 & \vdots \\ \vdots & \ddots & 1 & -a_{n-2} \\ 0 & \cdots & 0 & -a_{n-1} \end{pmatrix} \in M_{n\times n}(K).$$

Somit ist $\mathrm{Tr}_{L/K}(\alpha) = \frac{m}{n}\,\mathrm{Tr}(B) = -\frac{m}{n}a_{n-1}$.

(b) Sei $\mathrm{VHom}_K(L, L)$ die Menge aller K-Vektorraumhomomorphismen $L \to L$. Dann gilt $\mathrm{VHom}_K(L, L) \cong \mathrm{Mat}_{m\times m}(K)$. Die Abbildungen $\mathrm{Tr}\colon \mathrm{Mat}_{m\times m}(K) \to K$ und $\mu\colon L \to \mathrm{VHom}_K(L, L)$ sind K-linear, also auch ihre Verknüpfung.

(c) Die Bilder von α unter den Einbettungen $\sigma_1, \ldots, \sigma_m$ sind gerade die verschiedenen Nullstellen $\alpha_1, \ldots, \alpha_n$ des Minimalpolynoms von α. Sei $\mathrm{Hom}_K(K(\alpha), \overline{L}) = \{\tau_1, \ldots, \tau_n\}$. Jedes τ_i hat genau $[L/K(\alpha)] = m/n$ Fortsetzungen auf L. Das impliziert für jedes $1 \leqslant j \leqslant n$, dass $|\{1 \leqslant i \leqslant m : \sigma_i(\alpha) = \alpha_j\}| = m/n$ ist. Nach dem Satz von Vieta ist $\alpha_1 + \cdots + \alpha_n = -a_{n-1}$, und somit ist $\sigma_1(\alpha) + \cdots + \sigma_m(\alpha) = \frac{m}{n}(\alpha_1 + \cdots + \alpha_n) = -\frac{m}{n}a_{n-1} = \mathrm{Tr}_{L/K}(\alpha)$ nach (a).

(d) Wegen (b) genügt es, zu zeigen, dass $\mathrm{Tr}_{L/K}$ ungleich null ist. Wir nehmen zuerst an, die Erweiterung L/K sei galoissch. Dann sind $\sigma_1, \ldots, \sigma_m$ die Elemente der Galoisgruppe von L/K und somit linear unabhängig, also ist $\mathrm{Tr}_{L/K}$ ungleich null. Sei nun M die normale Hülle von L/K. Mit (c) können wir zeigen, dass $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ gilt. Da $\mathrm{Tr}_{M/K} \neq 0$ ist, folgt $\mathrm{Tr}_{L/K} \neq 0$.

(e) Sei ζ eine primitive siebte Einheitswurzel. Dann ist $t := \zeta + \zeta^2 + \zeta^4$ die Summe aller Konjugierten von ζ unter der Untergruppe $\{1, 2, 4\}$ und liegt folglich im zugehörigen Fixkörper $\mathbb{Q}(\mu_7)^H$. Da die Untergruppe Index 2 hat, hat dieser Fixkörper Grad 2 über $\mathbb{Q}$. Wenn er also nicht schon von t erzeugt ist, so liegt t schon in $\mathbb{Q}$. In diesem Fall ist t gleich seinem Konjugierten unter einem der restlichen Elemente von $\mathbb{F}_7^\times$, also gleich $\zeta^3 + \zeta^5 + \zeta^6$. Es gibt viele Wege zu zeigen, dass dies nicht der Fall ist: elementare Trigonometrie, Analysis, Algebra, Zahlentheorie … Siehe (f).

(f) Als Summe aller Konjugierten von ζ unter H liegt $\sum_{h\in H}\zeta^h$ im Fixkörper $\mathbb{Q}(\mu_p)^H$. Genauer ist es nach (c) gleich der Spur von ζ unter der Körpererweiterung $\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p)^H$. Für die Gleichheit $\mathbb{Q}(\mu_p)^H = \mathbb{Q}(\sum_{h\in H}\zeta^h)$ bleibt daher nur noch zu zeigen, dass $\sum_{h\in H}\zeta^h$ nicht schon in einem kleineren Körper liegt. Dafür genügt es zu zeigen, dass es verschieden ist von allen seinen Konjugierten unter Elementen von $\mathbb{F}_p^\times \smallsetminus H$.

Betrachte also ein $n \in \mathbb{F}_p^\times \smallsetminus H$. Das entsprechende Konjugierte von $\sum_{h\in H}\zeta^h$ ist dann $\sum_{h\in H}\zeta^{hn}$. Wäre es gleich $\sum_{h\in H}\zeta^h$, so hätten wir also die Gleichung $\sum_{h\in H}\zeta^{hn} - \sum_{h\in H}\zeta^h = 0$. Für jedes $i \in \mathbb{F}_p^\times$ sei $\overline{i}$ sein eindeutiger Repräsentant in $\{1,\ldots,p-1\}$, und betrachte das Polynom

$$P(X) \;:=\; \sum_{h\in H} X^{\overline{hn}} - \sum_{h\in H} X^{\overline{h}} \;\in\; \mathbb{Z}[X].$$

Dann ist ζ eine Nullstelle von P. Andererseits ist ζ eine Nullstelle des p-ten Kreisteilungspolynoms

$$\Phi_p(X) \;:=\; X^{p-1} + \ldots + X + 1 \;\in\; \mathbb{Z}[X].$$

Letzteres ist irreduzibel und muss folglich P teilen. Aber P hat Grad $\leqslant p-1 = \deg(\Phi_p)$ und ist zusätzlich durch X teilbar. Folglich muss $P = 0$ sein. Aber da H und Hn nichtleer und disjunkt sind, ist $P \neq 0$, Widerspruch.

*54. Als Vorbereitung zeige:

(a) Sei H eine Untergruppe einer endlichen Gruppe G, so dass jede Konjugationsklasse von G ein Element von H enthält. Dann ist $H = G$.
(*Hinweis:* Zähle die Elemente von $\bigcup_{g\in G} gHg^{-1}$.)

(b) Jede Untergruppe von S_n, welche den Stabilisator einer Ziffer enthält, ist gleich diesem Stabilisator oder gleich S_n.

(c) Für je zwei natürliche Zahlen $d > 0$ und $k \geqslant 0$ existiert ein N, so dass für jede Primzahl $p > N$ mindestens k verschiedene normierte irreduzible Polynome vom Grad d in $\mathbb{F}_p[X]$ existieren.

Sodann zeige für jede natürliche Zahl $n \geqslant 1$:

(d) Es gibt ein separables Polynom vom Grad n über $\mathbb{Q}$ mit Galoisgruppe S_n.

(e) Es gibt eine Erweiterung vom Grad n von $\mathbb{Q}$, die keine echten Zwischenkörper besitzt.

Lösung:

(a) Nach Voraussetzung ist $\bigcup_{g\in G} gHg^{-1} = G$. Dabei hängt die Untergruppe gHg^{-1} nur von der Nebenklasse gH ab. Für Repräsentanten $g_1,\ldots,g_n$ dieser

Nebenklassen gilt also $\bigcup_{i=1}^{n} g_i H g_i^{-1} = G$. Nun enthalten aber alle $g_i H g_i^{-1}$ das Einselement von G; somit enthält die linke Seite höchstens $1 + n \cdot (|H| - 1)$ Elemente. Wegen $n = [G : H]$ gilt also $1 + [G : H] \cdot (|H| - 1) \geqslant |G|$. Mit $[G : H] \cdot |H| = |G|$ folgt daraus $1 \geqslant [G : H]$ und damit $H = G$.

(b) Sei $H < S_n$ eine Untergruppe, die den Stabilisator $\mathrm{Stab}_{S_n}(k)$ einer Ziffer k enthält. Falls H nicht gleich diesem Stabilisator ist, so existiert ein Element $\sigma \in H \smallsetminus \mathrm{Stab}_{S_n}(k)$, das heisst, mit $\sigma(k) \neq k$. Sei nun $g \in S_n$ beliebig. Im Fall $g(k) = k$ gilt dann $g \in \mathrm{Stab}_{S_n}(k) < H$. Im Fall $g(k) = \sigma(k)$ liegt $\sigma^{-1}g$ in $\mathrm{Stab}_{S_n}(k) < H$ und daher auch $g = \sigma(\sigma^{-1}g)$ in H. Andernfalls ist $\tau := (g(k)\ \sigma(k))$ eine Transposition in $\mathrm{Stab}_{S_n}(k) < H$ und $\sigma^{-1}\tau g \in \mathrm{Stab}_{S_n}(k) < H$ und daher auch $g = \tau^{-1}\sigma(\sigma^{-1}\tau g)$ in H. In allen Fällen gilt daher $g \in H$ und somit $H = S_n$.

(c) Sei p eine beliebige Primzahl. Für jede ganze Zahl $d \geqslant 1$ sei I_d die Menge der normierten irreduziblen Polynome vom Grad d in $\mathbb{F}_p[X]$. Nach der obigen Aufgabe 48 (c) gilt dann $\sum_{e|d} e|I_e| = p^d$. Insbesondere gilt $d|I_d| \leqslant p^d$; also auch $e|I_e| \leqslant p^e$ für alle $e \geqslant 1$, und es folgt $d|I_d| \geqslant\ p^d - \sum_{e|d,\ e<d} p^e$. Für festes d ist diese rechte Seite ein normiertes Polynom in p. Für jede reelle Konstante k existiert daher eine Zahl N, so dass die rechte Seite $\geqslant dk$ ist für alle $p > N$. Für jede solche Primzahl p ist dann $|I_d| \geqslant k$, wie gewünscht.

(d) Seien $\sigma_1, \ldots, \sigma_m$ Repräsentanten aller Konjugationsklassen von S_n. Wähle eine Zahl N, für welche die Aussage (c) für alle $d, k \leqslant n$ gilt, sowie Primzahlen $N < p_1 < \ldots < p_m$. Für jedes $1 \leqslant i \leqslant m$ wähle ein normiertes Polynom $f_i \in \mathbb{F}_{p_i}[X]$ wie folgt:

Sei $\sum'_{d \geqslant 1} k_d d = n$ die zu σ_i gehörende Partition von n. Für jedes d mit $k_d > 0$ gilt dann $d, k_d \leqslant n$, und nach (c) existieren somit k_d paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_{p_i}[X]$. Das Produkt aller dieser für alle d ist ein separables normiertes Polynom $f_i \in \mathbb{F}_{p_i}[X]$ vom Grad n, für das die Grade der irreduziblen Faktoren genau der Partition von σ_i entsprechen.

Schreibe nun jedes dieser Polynome in der Form $f_i = X^n + \sum_{j=0}^{n-1} a_{ij} X^j$ mit $a_{ij} \in \mathbb{F}_{p_i}$. Da die Primzahlen $p_1, \ldots, p_m$ paarweise verschieden sind, existiert nach dem Chinesischen Restsatz für jedes j eine ganze Zahl a_j mit der Restklasse $a_j + p_i\mathbb{Z} = a_{ij}$ für alle i. Dann ist $f := X^n + \sum_{j=0}^{n-1} a_i X^j$ ein normiertes Polynom vom Grad n in $\mathbb{Z}[X]$ mit $f \bmod (p_i) = f_i$ für alle i.

Da jedes f_i separabel ist, ist dann auch f separabel. Sei $\Gamma < S_n$ seine Galoisgruppe über $\mathbb{Q}$ für irgendeine Numerierung der Nullstellen von f. Nach Satz 7.9.4 der Vorlesung enthält dann Γ für jedes i eine Permutation mit derselben zugehörigen Partition wie für σ_i. Diese Permutation ist also konjugiert zu σ_i. Da $\sigma_1, \ldots, \sigma_m$ Repräsentanten aller Konjugationsklassen von S_n waren, erfüllt also $\Gamma < S_n$ die Voraussetzung in (a) und es folgt $\Gamma = S_n$.

(e) Sei $L/\mathbb{Q}$ ein Zerfällungskörper des Polynoms f aus (d); dann ist $L/\mathbb{Q}$ galoissch mit $\mathrm{Gal}(L/\mathbb{Q}) = S_n$. Sei K ein Zwischenkörper, der dem Stabilisator

einer Ziffer entspricht. (Das ist ein Stammkörper von f über $\mathbb{Q}$.) Jeder Zwischenkörper K' von $K/\mathbb{Q}$ entspricht dann einer Untergruppe von S_n, die diesen Stabilisator enthält. Nach (b) ist diese Untergruppe gleich dem Stabilisator oder gleich S_n, und nach der Galoiskorrespondenz ist folglich $K' = K$ oder $K' = \mathbb{Q}$. Damit ist $K/\mathbb{Q}$ eine Erweiterung vom Grad n, die keine echten Zwischenkörper besitzt.

*55. Sei K ein Körper der Charakteristik $\neq 2$ mit festgewählten Elementen a und t. Definiere die *Iterierten* des Polynoms $f(X) := X^2 + a \in K[X]$ durch $f_0(X) := X$ und $f_{n+1}(X) := f_n(f(X))$ für alle $n \geqslant 0$. Ziel dieser Aufgabe ist, etwas über die Galoisgruppe des Polynoms $F_n(X) := f_n(X) - t$ herauszufinden.

Dazu schreiben wir einen Zerfällungskörper von F_n über K in der Form $K_n = K(t_{n,1}, \ldots, t_{n,2^n})$ mit $F_n(X) = (X - t_{n,1}) \cdots (X - t_{n,2^n})$, wobei wir die Nullstellen so numerieren, dass $f(t_{n,2i-1}) = f(t_{n,2i}) = t_{n-1,i}$ ist für alle $1 \leqslant i \leqslant 2^{n-1}$.

Die einzige Nullstelle der Ableitung $f'(X) = 2X$ ist der *kritische Punkt* 0 *von* f. Die Menge $A := \{f_n(0) \mid n \geqslant 1\}$ heisst die *postkritische Bahn von* f. Zeige:

(a) Die Menge A ist genau dann unendlich, wenn die Elemente $f_n(0)$ für alle $n \geqslant 1$ paarweise verschieden sind.

(b) Ist $t \notin A$, so ist das Polynom $F_n(X)$ separabel für jedes $n \geqslant 0$.

(c) Die Bedingung $t \notin A$ gilt insbesondere dann, wenn eines der Elemente a oder t in einem Unterkörper $k \subset K$ liegt und das andere transzendent über k ist.

Im folgenden setzen wir stets $t \notin A$ voraus. Zeige:

(d) Mit der gewählten Numerierung der Nullstellen von F_n wird $G_n := \mathrm{Gal}(K_n/K)$ eine Untergruppe der Gruppe $P_n < S_{2^n}$ aus der obigen Aufgabe 38.

Für jedes $n \geqslant 1$ sei nun $p_n := \prod_{i=1}^{2^{n-1}} t_{n,2i-1}$. Zeige:

(e) Die Untergruppe $G_n \cap [P_n, P_n]$ entspricht dem Zwischenkörper $K(p_1, \ldots, p_n)$.

(f) Es gilt $G_n = P_n$ genau dann, wenn $[K(p_1, \ldots, p_n)/K] = 2^n$ ist.

(g) Für jedes $n \geqslant 1$ gilt $p_n^2 = r_n$ mit

$$r_n := \begin{cases} t - f_1(0) & \text{falls } n = 1, \\ f_n(0) - t & \text{falls } n \geqslant 2. \end{cases}$$

(h) Sei nun $K = k(t)$ mit $a \in k$ und t transzendent über k, und sei A unendlich. Folgere $G_n = P_n$ für alle $n \geqslant 0$.

Bemerkung: Im allgemeinen ist es nicht einfach zu entscheiden, wann $G_n = P_n$ ist.

Lösung: Zunächst bemerken wir, dass die Nullstellen auf die beschriebene Weise numeriert werden können, weil jede Faktorisierung $F_{n-1}(X) = \prod_{i=1}^{2^{n-1}}(X - t_{n-1,i})$ die Faktorisierung

$$(*) \qquad F_n(X) \;=\; F_{n-1}(f(X)) \;=\; \prod_{i=1}^{2^{n-1}}(X^2+a-t_{n-1,i}) \;=\; \prod_{i=1}^{2^{n-1}}(X-t_{n,2i-1})(X-t_{n,2i})$$

ermöglicht mit $f(t_{n,2i-1}) = f(t_{n,2i}) = t_{n-1,i}$ für alle $1 \leqslant i \leqslant 2^{n-1}$.

(a) Sind die $f_n(0)$ paarweise verschieden für alle $n \geqslant 1$, so ist A unendlich. Sei umgekehrt $f_n(0) = f_m(0)$ für gewisse $n > m \geqslant 1$. Aus der Konstruktion der Iterierten folgt dann $f_{r+n}(0) = f_r(f_n(0)) = f_r(f_m(0)) = f_{r+m}(0)$ für alle $r \geqslant 0$. Damit ist $A = \{f_1(0), \ldots, f_{n-1}(0)\}$ eine endliche Menge.

(b) Offenbar ist $F_0(X) = X - t$ separabel. Ist $F_{n-1}(X)$ separabel für ein $n \geqslant 1$, so sind seine Nullstellen $t_{n-1,i}$ paarweise verschieden. Nach Konstruktion sind dann auch die Werte $f(t_{n,2i-1}) = f(t_{n,2i})$ paarweise verschieden für alle i. Somit sind die Nullstellen von $F_n(X)$ paarweise verschieden, ausser dass $t_{n,2i-1} = t_{n,2i}$ sein kann für gewisse i. Wegen der Formel für $f(X)$, und da $-1 \neq 1$ ist in K, tritt dies aber nur im Fall $t_{n,2i-1} = t_{n,2i} = 0$ auf. Dann ist aber $0 = F_n(0) = f_n(0) - t$ und somit $t = f_n(0) \in A$, im Widerspruch zur Annahme. Durch Induktion folgt daher, dass jedes $F_n(X)$ separabel ist.

(c) Liegt a in einem Unterkörper $k \subset K$, so liegt jedes Element $f_n(0)$ von A ebenfalls in k. Ist daher t transzendent über k, so folgt direkt $t \notin A$.

Sei andererseits a transzendent über einem Unterkörper $k \subset K$. Dann können wir in $k[a]$ rechnen wie in einem Polynomring über k und finden $f_1(0) = a$ und $f_2(0) = a^2 + a$ und durch Induktion, dass $f_n(0)$ für jedes $n \geqslant 1$ ein normiertes Polynom vom Grad 2^{n-1} in $k[a]$ ist. Insbesondere ist $f_n(0)$ dann ebenfalls transzendent über k. Ist daher t schon in k, so folgt ebenfalls $t \notin A$.

(d) Nach Voraussetzung und (b) ist $F_n(X)$ separabel. Die Numerierung der Nullstellen liefert damit eine eindeutige Einbettung $G_n := \mathrm{Gal}(K_n/K) \hookrightarrow S_{2^n}$ gemäss der Formel $\tau(t_{n,i}) = t_{n,\tau i}$ für alle $1 \leqslant i \leqslant 2^n$. Wir identifizieren G_n mit seinem Bild. Offenbar gilt dann $G_0 = \{1\} = S_{2^0}$.

Sei nun $n \geqslant 1$ mit $G_{n-1} < P_{n-1}$. Die Konstruktion liefert eine Einbettung $K_{n-1} \hookrightarrow K_n$ und somit einen surjektiven Homomorphismus $\pi_n \colon G_n \twoheadrightarrow G_{n-1}$. Jedes Element $\tau \in G_n$ operiert damit auf den Nullstellen $t_{n-1,1}, \ldots, t_{n-1,2^{n-1}}$ von $F_{n-1}(X)$ durch ein Element $\sigma \in G_{n-1}$. Die gewählte Numerierung der Nullstellen impliziert dann, dass die Permutation $\rho := \tau \cdot j(\sigma)^{-1} \in S_n$ jedes Paar $\{2i-1, 2i\}$ invariant lässt und daher in der Untergruppe Q_n liegt. Ausserdem ist schon $\sigma \in P_{n-1}$ nach Induktionsvoraussetzung. Insgesamt folgt daraus $\tau = \rho \cdot j(\sigma) \in Q_n \cdot j(P_{n-1}) = P_n$ und damit $G_n < P_n$.

(e) Für jedes Element $\tau = \rho \cdot j(\sigma) \in P_n$ mit $\rho \in Q_n$ und $\sigma \in P_{n-1}$ und jedes $1 \leqslant i \leqslant 2^{n-1}$ gilt

$$\tau(2i-1) \;=\; \begin{cases} 2\sigma(i)-1 & \text{falls } \rho(2\sigma(i)-1) = 2\sigma(i)-1, \\ 2\sigma(i) & \text{falls } \rho(2\sigma(i)-1) = 2\sigma(i). \end{cases}$$

Im Fall $\tau \in G_n$ bedeutet dies

$$\tau(t_{n,2i-1}) \;=\; t_{n,\tau(2i-1)} \;=\; \begin{cases} t_{n,2\sigma(i)-1} & \text{falls } \rho(2i-1) = 2i-1, \\ t_{n,2\sigma(i)} = -t_{n,2\sigma(i)-1} & \text{falls } \rho(2i-1) = 2i. \end{cases}$$

Für das Element $p_n := \prod_{i=1}^{2^{n-1}} t_{n,2i-1}$ folgt daraus $\tau(p_n) = \operatorname{sgn}(\rho) \cdot p_n$. Nach der Definition von $\chi_{n,n}$ bedeutet dies $\tau(p_n) = \chi_{n,n}(\tau) \cdot p_n$. Die induktive Konstruktion von $\chi_{n,m}$ impliziert dann

$$\tau(p_m) \;=\; \chi_{n,m}(\tau) \cdot p_m$$

für alle $n \geqslant m \geqslant 1$. Nach der Definition von $\underline{\chi}_n$ ist also

$$\begin{aligned} \operatorname{Kern}(\underline{\chi}_n | G_n) \;&=\; \big\{ \tau \in G_n \;\big|\; \tau(p_m) = p_m \text{ für alle } 1 \leqslant m \leqslant n \big\} \\ &=\; \operatorname{Gal}(K_n / K(p_1, \ldots, p_n)). \end{aligned}$$

Nach Aufgabe 38 (e) ist aber $\operatorname{Kern}(\underline{\chi}_n | G_n) = G_n \cap [P_n, P_n]$. In der Galoiskorrespondenz entspricht diese Untergruppe daher dem Zwischenkörper $K(p_1, \ldots, p_n)$.

(f) Nach Aufgabe 38 (f) gilt $G_n = P_n$ genau dann, wenn die Einschränkung $\underline{\chi}_n | G_n \colon G_n \to \{\pm 1\}^n$ surjektiv ist. Nach der Rechnung in (e) beschreibt diese Einschränkung aber genau die Operation von $G_n = \operatorname{Gal}(K_n/K)$ auf den Elementen $p_1, \ldots, p_n$. Somit ist ihr Bild $\underline{\chi}_n(G_n)$ natürlich isomorph zu der Galoisgruppe $\operatorname{Gal}(K(p_1, \ldots, p_n)/K)$. Ihre Ordnung ist daher gleich dem Körpergrad $[K(p_1, \ldots, p_n)/K]$. Somit ist $\underline{\chi}_n | G_n \colon G_n \to \{\pm 1\}^n$ genau dann surjektiv, wenn $[K(p_1, \ldots, p_n)/K] = 2^n$ ist.

(g) Für alle $n \geqslant 1$ und $1 \leqslant i \leqslant 2^{n-1}$ gilt nach Konstruktion $t_{n,2i} = -t_{n,2i-1}$. Die Definition von p_n impliziert daher

$$p_n^2 \;=\; \prod_{i=1}^{2^{n-1}} t_{n,2i-1}^2 \;=\; (-1)^{2^{n-1}} \cdot \prod_{i=1}^{2^{n-1}} (0 - t_{n,2i-1})(0 - t_{n,2i})$$

Mit $(*)$ folgt daraus

$$p_n^2 \;=\; (-1)^{2^{n-1}} \cdot F_n(0) \;=\; (-1)^{2^{n-1}} \cdot (f_n(0) - t) \;=:\; r_n.$$

(h) Da A unendlich ist, sind die Elemente $f_n(0)$ paarweise verschieden für alle $n \geqslant 1$. Wegen $a \in k$ liegen alle diese schon in k. Da t transzendent über k ist, können wir in $k[t]$ rechnen wie in einem Polynomring über k und schliessen, dass $r_1 = t - f_1(0)$ und $r_n = f_n(0) - t$ für alle $n \geqslant 2$ paarweise inäquivalente irreduzible Elemente von $k[t]$ sind. Wegen $K = k(t)$ erzeugen die Elemente $r_1, \ldots, r_n$ daher eine Untergruppe der Ordnung 2^n von $K^\times/(K^\times)^2$. Nach (g) und Aufgabe 35 der Wiederholungsserie Algebra II folgt daraus $[K(p_1, \ldots, p_n)/K] = 2^n$. Nach (f) folgt daraus schliesslich $G_n = P_n$.