Wiederholungsserie Sternaufgaben

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

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

*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.

**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?

*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 $Z_2 \to \operatorname{Aut}(N)$.

(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 $Z_2 \to \operatorname{Aut}(N)$ unter $\operatorname{Aut}(N)$ 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.

*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 $|S_i|/|S| = c_n/|\operatorname{Aut}(G_i)|$ 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?

*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 $a^n - a$.

*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.

*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.

*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.

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

**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 $\mathbb{F}_2[X]$.

*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?

*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.

*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.

*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.

*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 $\mathrm{Tr}(\varphi)$.

*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.

*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.