Frühjahr 2020

F20T1A1	F20T1A2	F20T1A3	F20T1A4	F20T1A5
F20T2A1	F20T2A2	F20T2A3	F20T2A4	F20T2A5
F20T3A1	F20T3A2	F20T3A3	F20T3A4	F20T3A5

Herbst 2020

H20T1A1	H20T1A2	H20T1A3	H20T1A4	H20T1A5
H20T2A1	H20T2A2	H20T2A3	H20T2A4	H20T2A5
H20T3A1	H20T3A2	H20T3A3	H20T3A4	H20T3A5

Aufgabe F20T1A1

Sei K ein Körper und $V = K^{2\times 2}$ der K-Vektorraum der 2×2-Matrizen über K. Für $A, B \in K^{2\times 2}$ betrachten wir die Abbildung $\Phi : V \to V$, $X \mapsto AXB$. Zeigen Sie:

(a) Φ ist ein Endomorphismus von V.

(b) $\mathrm{Spur}(\Phi) = \mathrm{Spur}(A)\mathrm{Spur}(B)$

Lösung:
zu (a) Wir müssen überprüfen, dass durch Φ eine lineare Abbildung $V \to V$ gegeben ist, dass also $\Phi(X_1 + X_2) = \Phi(X_1) + \Phi(X_2)$ und $\Phi(\lambda X_1) = \lambda\Phi(X_1)$ für alle $X_1, X_2 \in V$ und $\lambda \in K$ gegeben ist. Beide Gleichungen ergeben sich unmittelbar aus den bekannten Rechenregeln für Matrizen. Es gilt

$$\Phi(X_1 + X_2) \quad = \quad A(X_1 + X_2)B \quad = \quad A(X_1B + X_2B) \quad = \quad AX_1B + AX_2B \quad = \quad \Phi(X_1) + \Phi(X_2)$$

und $\Phi(\lambda X_1) = A(\lambda X_1)B = A(\lambda(X_1B)) = \lambda(AX_1B) = \lambda\Phi(X_1)$.

zu (b) Für $1 \le i, j \le 2$ sei $B_{ij} \in K^{2\times 2}$ jeweils die Basismatrix mit dem Eintrag 1 an der Stelle (i, j) (bei der alle übrigen Einträge gleich null sind), also

$$B_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad , \quad B_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad , \quad B_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad , \quad B_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Wir berechnen die Spur von Φ, indem wir die Darstellungsmatrix von Φ bezüglich der geordneten Basis $(B_{11}, B_{12}, B_{21}, B_{22})$ des K-Vektorraums V bestimmen. Es gilt

$$\Phi(B_{11}) = AB_{11}B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ a_{21}b_{11} & a_{21}b_{12} \end{pmatrix}$$

$$\Phi(B_{12}) = AB_{12}B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{21} & b_{22} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{21} & a_{11}b_{22} \\ a_{21}b_{21} & a_{21}b_{22} \end{pmatrix}$$

$$\Phi(B_{21}) = AB_{21}B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ b_{11} & b_{12} \end{pmatrix} = \begin{pmatrix} a_{12}b_{11} & a_{12}b_{12} \\ a_{22}b_{11} & a_{22}b_{12} \end{pmatrix}$$

$$\Phi(B_{22}) = AB_{22}B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{12}b_{21} & a_{12}b_{22} \\ a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

Jede dieser Gleichungen liefert eine Spalte der Darstellungsmatrix; insgesamt ist die Darstellungsmatrix gegeben durch

$$\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{21} \\ a_{11}b_{12} & a_{11}b_{22} & a_{12}b_{12} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{21} & a_{22}b_{11} & a_{22}b_{21} \\ a_{21}b_{12} & a_{21}b_{22} & a_{22}b_{12} & a_{22}b_{22} \end{pmatrix}$$

Es gilt $\mathrm{Spur}(A) = a_{11} + a_{22}$ und $\mathrm{Spur}(B) = b_{11} + b_{22}$. Die Spur von Φ ist nach Definition gleich der Spur der Darstellungsmatrix, und für diese erhalten wir den Wert

$$a_{11}b_{11} + a_{11}b_{22} + a_{22}b_{11} + a_{22}b_{22} \quad = \quad (a_{11} + a_{22})(b_{11} + b_{22}) \quad = \quad \mathrm{Spur}(A)\mathrm{Spur}(B).$$

Aufgabe F20T1A2

Seien $R = \mathbb{Z}/15\mathbb{Z}$ und $f : R \to R$, $x \mapsto 7x$.

(a) Zeigen Sie, dass f bijektiv und damit eine Permutation von R ist.

(b) Bestimmen Sie die Fixpunkte von f.

(c) Bestimmen Sie die Anzahl der Bahnen der Operation von $\langle f \rangle$ auf R. Hier steht $\langle f \rangle$ für die von f erzeugte Untergruppe der Permutationen von R.

Lösung:
zu (a) Ist ist $\bar{7} \in R^\times$, und $\overline{13}$ ist das multiplikative Inverse von $\bar{7}$. Daraus folgt, dass $g : R \to \mathbb{R}$, $x \mapsto \overline{13}x$ die Umkehrabbildung von f ist, denn für alle $x \in R$ gilt $(g \circ f)(x) = g(f(x)) = g(\bar{7}x) = \overline{13}(\bar{7}x) = \overline{91}x = \bar{1}x = x$ und ebenso $(f \circ g)(x) = f(g(x)) = f(\overline{13}x) = \bar{7}(\overline{13}x) = \overline{91}x = \bar{1}x = x$. Die Existenz einer Umkehrabbildung zeigt, dass f bijektiv ist.

zu (b) Für $c \in \mathbb{R}$ ist $c + 15\mathbb{Z}$ genau dann ein Fixpunkt, wenn $7c \equiv c \bmod 15$ gilt, also genau dann, wenn 15 ein Teiler von $7c - c = 6c$ ist. Dies wiederum ist wegen $\mathrm{ggT}(3, 5) = 1$ genau dann der Fall, wenn 3 und 5 Teiler von $6c$ sind. Da 3 immer ein Teiler von $6c$ ist, dies dies wiederum äquivalent zur Teilbarkeit von $6c$ durch 5, wegen $\mathrm{ggT}(6, 5) = 1$ also zur Teilbarkeit von c durch 5. Es gilt $5 \mid c$ genau dann, wenn $c + 15\mathbb{Z} \in \{\bar{0}, \bar{5}, \overline{10}\}$ gilt. Also ist $\{\bar{0}, \bar{5}, \overline{10}\}$ die Fixpunktmenge von f.

zu (c) Jeder Fixpunkt bildet eine einelementige Bahn. Wegen $\bar{7}^2 = \overline{49} = \bar{4} \neq \bar{1}$ und $\bar{7}^4 = (\bar{7}^2)^2 = \bar{4}^2 = \overline{16} = \bar{1}$ ist $\bar{7}$ in der Einheitengruppe $R^\times$ ein Element der Ordnung 4. Zwei Bahnen der Operation sind deshalb gegeben durch

$$\langle f \rangle(\bar{1}) \quad = \quad \{f^n(\bar{1}) \mid n \in \mathbb{Z}\} \quad = \quad \{\bar{7}^n \cdot \bar{1} \mid n \in \mathbb{Z}\} \quad = \quad \{\bar{7}^n \mid 0 \leq n < 4\} \quad = \quad \{\bar{7}, \bar{4}, \overline{13}, \bar{1}\}$$

und

$$\langle f \rangle(\bar{2}) \quad = \quad \{f^n(\bar{2}) \mid n \in \mathbb{Z}\} \quad = \quad \{\bar{7}^n \cdot \bar{2} \mid n \in \mathbb{Z}\} \quad = \quad \{\bar{7}^n \cdot \bar{2} \mid 0 \leq n < 4\} \quad = \quad \{\overline{14}, \bar{8}, \overline{11}, \bar{2}\} \quad ,$$

eine weitere durch

$$\langle f \rangle(\bar{3}) \quad = \quad \{f^n(\bar{3}) \mid n \in \mathbb{Z}\} \quad = \quad \{\bar{7}^n \cdot \bar{3} \mid n \in \mathbb{Z}\} \quad = \quad \{\bar{7}^n \cdot \bar{3} \mid 0 \leq n < 4\} \quad = \quad \{\overline{21}, \overline{12}, \bar{9}, \bar{3}\}.$$

Insgesamt existieren also genau sechs Bahnen.

Aufgabe F20T1A3

(a) Geben Sie die Definition einer *auflösbaren Gruppe* an.

(b) Zeigen Sie: Jede Gruppe der Ordnung 2020 ist auflösbar.

(c) Geben Sie zwei nicht-isomorphe abelsche und zwei nicht-isomorphe nicht-abelsche Gruppen der Ordnung 2020 an (mit Begründung).

Lösung:

zu (a) Eine Gruppe G wird *auflösbar* genannt, wenn G eine abelsche Normalreihe besitzt. Darunter versteht man eine Kette $G = N_0 \supsetneq N_1 \supsetneq N_2 \supseteq ... \supsetneq N_r = \{e_G\}$ mit der Eigenschaft, dass die Untergruppe N_{i+1} jeweils ein Normalteiler von N_i und die FaktorN_i/N_{i+1} abelsch ist, für $0 \leq i < r$.

zu (b) Sei G eine Gruppe der Ordnung 2020. Für die Anzahl ν_{101} der 101-Sylowgruppen gilt auf Grund der Sylowsätze $\nu_{101} \mid 20$, also $\nu_{101} \in \{1, 2, 4, 5, 10, 20\}$, und außerdem $\nu_{101} \equiv 1 \bmod 101$. Wegen $a \not\equiv 1 \bmod 101$ für $a \in \{2, 4, 5, 10, 20\}$ folgt ν_{101}. Sei N die einzige 101-Sylowgruppe von G. Ebenfalls auf Grund der Sylowsätze handelt es sich um einen Normalteiler von G.

Laut Vorlesung ist G genau dann auflösbar, wenn N und G/N auflösbar sind. Wegen $2020 = 2^2 \cdot 5^1 \cdot 101^1$ gilt $|N| = 101^1 = 101$, und als Gruppe von Primzahlordnung ist N zyklisch, damit auch abelsch und auflösbar. Wegen $|G/N| = \frac{2020}{101} = 20$ genügt es zu zeigen, dass jede Gruppe der Ordnung 20 auflösbar ist; daraus ergibt sich auf Grund des soeben genannten Satzes dann die Auflösbarkeit von G.

Sei also H eine Gruppe der Ordnung 20 und μ_p für jede Primzahl p die Anzahl der p-Sylowgruppen von H. Es gilt $\mu_5 \mid 4$, also $\mu_5 \in \{1, 2, 4\}$, und außerdem $\mu_5 \equiv 1 \bmod 5$. Wegen $2 \not\equiv 1 \bmod 5$ und $4 \not\equiv 1 \bmod 5$ folgt $\mu_5 = 1$. Sei M die einzige 5-Sylowgruppe von H; dann gilt $M \trianglelefteq H$. Es gilt $|H| = 5$ und $|H/M| = \frac{|H|}{|M|} = \frac{20}{5} = 4$. Die Zahl 4 ist ein Primzahlquadrat, somit ist H/M eine abelsche und insbesondere auflösbare Gruppe. Auf Grund der Primzahlordnung ist H zyklisch, damit ebenfalls abelsch und auflösbar. Aus der Auflösbarkeit von M und H/M folgt die Auflösbarkeit von H.

zu (c) Sei $A = \mathbb{Z}/2020\mathbb{Z}$ und $B = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/1010\mathbb{Z}$. Die Gruppe A besitzt mit $\bar{1}$ ein Element der Ordnung 2020. Für alle $(\bar{b}, \bar{c}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/1010\mathbb{Z}$ gilt dagegen $1010(\bar{b}, \bar{c}) = (\overline{1010}\bar{b}, \overline{1010}\bar{c}) = (\bar{0}, \bar{0})$; dies zeigt, dass die Ordnung jedes Elements in B ein Teiler von 1010 ist und somit kein Element der Ordnung 2020 in B existiert. Folglich sind A und B zwei nicht zueinander isomorphe abelsche Gruppen.

Eine nicht-abelsche Gruppe der Ordnung 2020 konstruieren wir als äußeres semidirektes Produkt. In der Gruppe $\mathbb{Z}/100\mathbb{Z}$ ist $\overline{20}$ ein Element der Ordnung 5, folglich existiert laut Vorlesung ein nichttrivialer Homomorphismus $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$ gegeben durch $\phi(\bar{1}) = \overline{20}$. Außerdem gilt $\mathbb{Z}/100\mathbb{Z} \cong (\mathbb{Z}/101\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/101\mathbb{Z})$; sei $\iota : \mathbb{Z}/100\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/101\mathbb{Z})$ ein beliebig gewählter Isomorphismus und $\psi = \iota \circ \phi$. Das äußere semidirekte Produkt $C_1 = \mathbb{Z}/101\mathbb{Z} \rtimes_\psi \mathbb{Z}/5\mathbb{Z}$ ist dann eine nicht-abelsche Gruppe der Ordnung $101 \cdot 5 = 505$, und $C = \mathbb{Z}/4\mathbb{Z} \times C_1$ ist eine nicht-abelsche Gruppe der Ordnung $4 \cdot 505 = 2020$.

Eine weitere nicht-abelsche Gruppe der Ordnung 2020 ist Diedergruppe D_{1010}, die Symmetriegruppe des regelmäßigen 1010-Ecks. Diese ist laut Vorlesung ebenfalls nicht abelsch. Desweiteren sind C und D_{1010} nicht zueinander isomorph. Denn bekanntlich enthält die Diedergruppe D_n für alle $n \in \mathbb{N}$ nur Elemente der Ordnung 2 und solche, deren Ordnung ein Teiler von n ist. Anhand der Primfaktorzerlegung $1010 = 2 \cdot 5 \cdot 101$ können wir die Teiler von 1010 aufzählen. Die Gruppe D_{1010} enthält demnach nur Elemente der Ordnungen 1, 2, 5, 10, 101, 202, 505 und 1010, aber kein Element der Ordnung 4. Dagegen

ist $(\bar{1}, e_{C_1})$ offenbar ein Element der Ordnung 4 in C. Dies zeigt, dass C und D_{1010} nicht zueinander isomorph sind.

Aufgabe F20T1A4

Sei $\zeta \in \mathbb{C}$ eine primitive elfte Einheitswurzel und $K = \mathbb{Q}(\zeta)$.

(a) Zeigen Sie: K ist der Zerfällungskörper von $x^{11} - 1$ über $\mathbb{Q}$. Geben Sie den Isomorphietyp der Galois-Gruppe von $\mathrm{Gal}(K|\mathbb{Q})$ an.

(b) Zeigen Sie: Es gibt eine galoissche Körpererweiterung $\mathbb{Q} \subseteq L$ mit $[L : \mathbb{Q}] = 5$.

Lösung:
zu (a) Die Nullstellenmenge des Polynoms $f = x^{11} - 1$ ist gegeben durch $N = \{\zeta^k \mid 0 \leq k < 11\}$. Denn wegen $f(\zeta) = (\zeta^k)^{11} - 1 = (\zeta^{11})^k - 1 = 1 - 1 = 0$ ist jedes Element dieser Menge tatsächlich eine Nullstelle von f, und weil ζ eine primitive elfte Einheitswurzel ist, in der multiplikativen Gruppe $\mathbb{C}^\times$ also die Ordnung 11 besitzt, enthält N elf verschiedene Elemente. Weil ein Polynom vom Grad 11 über einem Körper nicht mehr als elf Nullstellen haben kann, muss N die genaue Nullstellenmenge von f sein.

Um nun zu zeigen, dass $K = \mathbb{Q}(\zeta)$ der Zerfällungskörper von f über $\mathbb{Q}$ ist, müssen wir die Gleichung $\mathbb{Q}(\zeta) = \mathbb{Q}(N)$ beweisen. Wegen $\zeta \in N$ gilt einerseits $\zeta \in \mathbb{Q}(N)$. Aus $\zeta \in \mathbb{Q}(\zeta)$ folgt auf Grund der Teilkörper-Eigenschaft von $\mathbb{Q}(\zeta)$ andererseits $\zeta^k \in \mathbb{Q}(\zeta)$ für $0 \leq k < 11$, also $N \subseteq \mathbb{Q}(\zeta)$. Aus $N \subseteq \mathbb{Q}(\zeta)$ und $\zeta \in \mathbb{Q}(N)$ folgt laut Vorlesung die behauptete Gleichheit.

Bezeichnet K_n den n-ten Kreisteilungskörper (mit $n \in \mathbb{N}$, $n \geq 2$), so ist die Erweiterung $K_n|\mathbb{Q}$ laut Vorlesung galoissch, und es gilt $\mathrm{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Somit gilt $\mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^\times$, und weil 11 eine Primzahl ist, gilt außerdem $(\mathbb{Z}/11\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z}$. Die Galois-Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist also zyklisch von Ordnung 10.

zu (b) Weil die Gruppe $G = \mathrm{Gal}(K|\mathbb{Q})$ zyklisch von Ordnung 10 ist, gibt es für jeden Teiler $d \in \mathbb{N}$ von 10 eine eindeutig bestimmte Untergruppe U_d von G von Ordnung d. Sei $L = K^{U_2}$ der Fixkörper der Untergruppe U_2. Nach den Ergänzungen zum Hauptsatz der Galoistheorie gilt dann $[L : \mathbb{Q}] = (G : U_2) = \frac{|G|}{|U_2|} = \frac{10}{2} = 5$. Weil G als zyklische Gruppe abelsch ist, sind sämliche Untergruppen von G Normalteiler, insbesondere die Untergruppe U_2. Daraus wiederum folgt laut Vorlesung, dass die Erweiterung $L|\mathbb{Q}$ eine Galois-Erweiterung ist.

Aufgabe F20T1A5

Ein n-Tupel $(a_1, a_2, ..., a_n)$ von ganzen Zahlen heiße *hübsch*, wenn $a_i a_j + 2$ eine Quadratzahl ist für alle $1 \leq i < j \leq n$. Zeigen Sie:

(a) Es gibt hübsche Tripel.

(b) Wenn ein Quadrupel hübsch ist, dann ist keine der Zahlen a_j $(j = 1, ..., 4)$ durch 4 teilbar.

(c) Es gibt keine hübschen Quadrupel.

Lösung:
zu (a) Das Tripel $(a_1, a_2, a_3) = (1, 2, 7)$ ist hübsch, denn $a_1 a_2 + 2 = 4$, $a_1 a_3 + 2 = 9$ und $a_2 a_3 + 2 = 16$ sind alles Quadratzahlen.

zu (b) Nehmen wir an, (a_1, a_2, a_3, a_4) ist ein hübsches Quadrupel mit der Eigenschaft, dass eines der Elemente a_i (mit $i \in \{1, 2, 3, 4\}$) durch 4 teilbar ist. Betrachten wir zunächst den Fall $i = 1$. Nach Voraussetzung ist $a_1 a_2 + 2$ eine Quadratzahl. Wegen $a_1 \equiv 0 mod 4$ gilt aber $a_1 a_2 + 2 \equiv 0 \cdot a_2 + 2 \equiv 2 \bmod 4$. Bekanntlich ist aber jede Quadratzahl kongruent zu 0 oder 1 modulo 4 (wegen $0^2 \equiv 0 \bmod 4$, $1^2 \equiv 1 \bmod 4$, $2^2 \equiv 0 \bmod 4$ und $3^2 \equiv 1 \bmod 4$). Der Widerspruch zeigt, dass die Annahme im Fall $i = 1$ falsch ist. Setzen wir nun $i > 1$ voraus. In diesem Fall ist $a_1 a_i + 2 \equiv a_1 \cdot 0 + 2 \equiv 2 \bmod 4$, andererseits ist auch $a_1 a_i + 2$ nach Voraussetzung eine Quadratzahl. Also führt die Annahme auch in diesem Fall zu einem Widerspruch.

zu (c) Angenommen, (a_1, a_2, a_3, a_4) ist ein hübsches Quadrupel. Nach (b) ist keine der vier Zahlen durch 4 teilbar. Da es abgesehen von $\bar{0}$ nur drei Restklassen modulo 4 gibt, müssen zwei der Zahlen a_i, a_j (mit $1 \leq i < j \leq j$) in derselben Restklasse modulo 4 liegen. Ist diese Restklasse $\bar{2}$, dann sind a_i, a_j beide gerade, und folglich gilt $a_i a_j + 2 \equiv 0 + 2 \equiv 2 \bmod 4$. Aber wie wir bereits in Teil (b) gesehen haben, ist dies unvereinbar mit der Annahme, dass $a_i a_j + 2$ eine Quadratzahl ist. Also muss entweder $a_i \equiv a_j \equiv 1 \bmod 4$ oder $a_i \equiv a_j \equiv 3 \bmod 4$ gelten. In beiden Fällen ist $a_i a_j + 2 \equiv 1 + 2 \equiv 3 \bmod 4$. Aber auch dies ist unmöglich, wenn $a_i a_j + 2$ ein Quadrat ist. Auch hier hat unsere Annahme also zu einem Widerspruch geführt.

Aufgabe F20T2A1

Für $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{C}$ seien a_0, a_1, a_2 die Koeffizienten des Polynoms

$$f(X) := (X - \lambda_1) \cdot (X - \lambda_2) \cdot (X - \lambda_3) = X^3 + a_2 X^2 + a_1 X + a_0 \in \mathbb{C}[x].$$

Ferner sei

$$A := \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix} \in \mathbb{C}^{3\times 3}$$

die sogenannte Begleitmatrix zu den gegebenen Zahlen. Zeigen Sie:

(a) Die Eigenwerte von A sind $\lambda_1, \lambda_2, \lambda_3$.

(b) Die Jordansche Normalform von A hat für jeden Eigenwert λ genau ein Jordan-Kästchen.

Lösung:
zu (a) Wir überprüfen, dass f mit dem charakteristischen Polynom χ_A von A übereinstimmt. Bezeichnen wir die Einheitsmatrix in $\mathbb{C}^{3\times 3}$ mit E, dann gilt

$$\chi_A \quad = \quad \det(xE - A) \quad = \quad \begin{pmatrix} x & 0 & a_0 \\ -1 & x & a_1 \\ 0 & -1 & x + a_2 \end{pmatrix} \quad =$$

$$x^2(x + a_2) + 0 + a_0 - 0 - (-a_1 x) - 0 \quad = \quad x^3 + a_2 x^2 + a_1 x + a_0.$$

Die Eigenwerte von A sind laut Vorlesung genau die Nullstellen von $\chi_A = f$, und die Zerlegung von f in Linearfaktoren zeigt, dass dies genau die Werte $\lambda_1, \lambda_2, \lambda_3$ sind.

zu (b) Wir zeigen zunächst, dass die Matrizen E, A, A^2 im $\mathbb{C}$-Vektorraum $\mathbb{C}^{3\times 3}$ ein linear unabhängiges System bilden. Die erste Spalte von E, A bzw. A^2 ist jeweils der Einheitsvektor e_1, e_2 bzw. e_3. Bei E und A kann dies direkt abgelesen werden, bei A^2 erhält man das Resultat durch Multiplikation der Matrix A mit ihrer ersten Spalte:

$$\begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad = \quad e_3.$$

(Es ist nicht notwendig, die Matrix A^2 vollständig zu berechnen.) Seien c_0, c_1, c_2 mit $c_0E + c_1A + c_2A^2 = 0$ vorgegeben. Durch Vergleich der ersten Spalten auf beiden Seiten erhält man $c_0e_1 + c_1e_2 + c_2e_3 = 0$, und daraus folgt $c_0 = c_1 = c_2 = 0$, weil $\{e_1, e_2, e_3\}$ ein linear unabhängiges System in $\mathbb{C}^3$ ist. Damit ist die linear Unabhängigkeit von $\{E, A, A^2\}$ nachgewiesen.

Aus der linearen Unabhängigkeit von $\{E, A, A^2\}$ folgt, dass das Minimalpolynom μ_A von A mindestens vom Grad 3 ist. Wäre nämlich μ_A vom Grad 1 oder 2, $\mu_A = c_2x^2 + c_1x + c_0$ mit $c_0, c_1, c_2 \in \mathbb{C}$, dann würde $c_2A^2 + c_1A + c_0 = \mu_A(A) = 0$ folgen, im Widerspruch zur linearen Unabhängigkeit. Nach dem Satz von Cayley-Hamilton gilt $\chi_A(A) = 0$; wegen $\operatorname{grad}(\mu_A) \geq 3 = \operatorname{grad}(\chi_A)$ folgt daraus $\mu_A = \chi_A$.

Sei nun $\lambda \in \mathbb{C}$ ein Eigenwert von A und $a \in \{1, 2, 3\}$ dessen algebraische Vielfachheit. Dann ist a zugleich die Vielfachheit von λ als Nullstelle von μ_A. Laut Vorlesung ist die algebraische Vielfachheit von λ die Summe der Größen sämtlicher Jordanblöcke zum Eigenwert λ in der Jordanschen Normalform. Die Vielfachheit von a als Nullstelle von μ_A ist dagegen die Größe des größten Jordanblocks zum Eigenwert λ. Da beide Werte gleich a sind, folgt daraus, dass nur ein Jordanblock zum Eigenwert λ existiert.

Aufgabe F20T2A2

Zeigen Sie:

(a) Ist $n = dm$ mit ungeradem $m \in \mathbb{N}$, so gilt die Teilbarkeitsrelation $(x^d + 1) \mid (x^n + 1)$.

(b) Das Polynom $x^n + 1$ ist genau dann über $\mathbb{Q}$ irreduzibel, wenn $n = 2^k$ für ein $k \in \mathbb{N}_0$ gilt.

Hinweise:

zu (a) Weisen Sie die Teilbarkeitsrelation anhand der Nullstellen nach. Die komplexen Nullstellen von $x^{2d} - 1$ sind genau die $2d$-ten Einheitswurzeln. Was bedeutet das für die Nullstellen von $x^d + 1$?

zu (b) Eine Implikationsrichtung kann aus Teil (a) abgeleitet werden. Für die andere Richtung denken Sie daran, dass Kreisteilungspolynome laut Vorlesung über $\mathbb{Q}$ irreduzibel sind.

Lösung:
zu (a) Wir zeigen: Für jedes $t \in \mathbb{N}$ ist $\zeta \in \mathbb{C}^\times$ genau dann eine Nullstelle von $x^t + 1$, wenn die Ordnung von ζ in $\mathbb{C}^\times$ zwar ein Teiler von $2t$, aber kein Teiler von t ist. „⇐“ Sei $\operatorname{ord}(\zeta) \mid (2t)$ und $\operatorname{ord}(\zeta) \nmid t$ vorausgesetzt. Wegen $(\zeta^t)^2 = \zeta^{2t} = 1$ ist ζ^t einerseits eine Nullstelle von $x^2 - 1$, also $\zeta^t \in \{\pm 1\}$, andererseits ist $\zeta^t = 1$ ausgeschlossen, da ansonsten $\operatorname{ord}(\zeta) \mid t$ gelten würde. Also gilt $\zeta^t = -1$, und somit ist ζ eine Nullstelle von $x^t + 1$ „⇒“ Sei $\zeta \in \mathbb{C}$ eine Nullstelle von $x^t + 1$. Dann gilt $\zeta^t = -1$ und $\zeta^{2t} = (-1)^2 = 1$, also $\zeta \in \mathbb{C}^\times$ und $\operatorname{ord}(\zeta) \mid 2t$. Würde auch $\operatorname{ord}(\zeta) \mid t$ gelten, dann würde daraus $\zeta^t = 1$ folgen, im Widerspruch zu $\zeta^t = -1$.

Seien nun $d, m, n \in \mathbb{N}$ wie angegeben. Die Polynome $x^d + 1$ und $x^n + 1$ haben wegen $\operatorname{ggT}(x^d + 1, dx^{d-1}) = 1$ und $\operatorname{ggT}(x^n + 1, nx^{n-1}) = 1$ nur einfache Nullstellen. Für den Nachweis der Teilbarkeitsrelation genügt es deshalb nachzuweisen, dass jede komplexe Nullstelle von $x^d + 1$ auch eine Nullstelle von $x^n + 1$ ist. Sei also $\zeta \in \mathbb{C}$ eine Nullstelle von $x^d + 1$. Wie im vorherigen Absatz gezeigt, gilt $\zeta \in \mathbb{C}^\times$, $\operatorname{ord}(\zeta) \mid (2d)$ und $\operatorname{ord}(\zeta) \nmid d$. Weil d ein Teiler von n ist, gilt auch $(2d) \mid (2n)$ und damit $\operatorname{ord}(\zeta) \mid (2n)$. Nehmen wir nun an, dass auch $\operatorname{ord}(\zeta) \mid n$ erfüllt ist. Dann ist $\operatorname{ord}(\zeta)$ insgesamt ein Teiler von $\operatorname{ggT}(2d, n) = \operatorname{ggT}(2d, dm) = d$, wobei im letzten Schritt verwendet wurde, dass m ungerade ist. Aber $\operatorname{ord}(\zeta) \mid d$ steht im Widerspruch zu unserer Voraussetzung. Es gilt also $\operatorname{ord}(\zeta) \mid (2n)$ und $\operatorname{ord}(\zeta) \mid n$. Wie oben gezeigt folgt daraus, dass ζ eine Nullstelle von $x^n + 1$ ist.

zu (b) „⇐“ Ist $n = 2^k$ für ein $k \in \mathbb{N}_0$, dann ist $x^n + 1$ das $2n$-te Kreisteilungspolynom und somit laut Vorlesung über $\mathbb{Q}$ irreduzibel. Bezeichnen wir nämlich für jedes $m \in \mathbb{N}$ mit $\Phi_m \in \mathbb{Z}[x]$ das m-te Kreisteilungspolynom, so gilt laut Vorlesung $x^{2n} - 1 = \prod_d \Phi_d$, wobei d die Teiler von $2n = 2^{k+1}$ durchläuft. Die Menge dieser Teiler besteht aus $2n$ und den Teilern von n, so dass die Gleichung in der Form $x^{2n} - 1 = \Phi_{2n} \cdot (x^n - 1)$ geschrieben werden kann. Daraus wiederum folgt

$$\Phi_{2n} \quad = \quad \frac{x^{2n} - 1}{x^n - 1} \quad = \quad x^n + 1.$$

„⇒“ Ist n keine Zweierpotenz, so gibt es eine Zerlegung $n = dm$ mit $d, m \in \mathbb{N}$, wobei $d > 1$ und ungerade ist. Nach Teil (a) wird $x^n + 1$ dann von $x^d + 1$ geteilt, mit $1 < d < n$. Daraus folgt, dass $x^n + 1$ in $\mathbb{Q}[x]$ reduzibel ist.

Aufgabe F20T2A3

Seien p eine Primzahl und $\mathbb{F}_p \subseteq \mathbb{F}_{p^k}$ eine Körpererweiterung vom Grad k über dem Körper $\mathbb{F}_p$. Betrachten Sie die Gruppe $G := \mathrm{GL}_2(\mathbb{F}_{p^k})$ der invertierbaren 2×2-Matrizen über $\mathbb{F}_{p^k}$. Zeigen Sie:

(a) Die Teilmenge $N := \{A \in G \mid \det(A) \in \mathbb{F}_p\}$ ist ein Normalteiler.

(b) Der Index des Normalteilers N ist teilerfremd zu p.

(c) Die p-Sylowgruppen von G sind genau die p-Sylowgruppen von N.

Lösung:
zu (a) Weil die Gruppe G aus den invertierbaren Matrizen über $\mathbb{F}_{p^k}$ besteht, gilt $\det(A) \neq \bar{0}$, also $\det(A) \in \mathbb{F}_{p^k}^\times$ für alle $A \in G$. Die Gruppe $\mathbb{F}_p^\times$ ist eine Untergruppe von $\mathbb{F}_{p^k}^\times$, denn es gilt $\bar{1} \in \mathbb{F}_p^\times$, und für alle $\bar{a}, \bar{b} \in \mathbb{F}_p^\times$ gilt auch $\bar{a}\bar{b} \in \mathbb{F}_p^\times$ und $\bar{a}^{-1} \in GFp^\times$. Darüber hinaus ist $\mathbb{F}_p^\times$ sogar ein Normalteiler von $\mathbb{F}_{p^k}^\times$, denn die Gruppe $\mathbb{F}_{p^k}^\times$ ist abelsch, und in einer abelschen Gruppe sind alle Untergruppen Normalteiler. Nun ist N nach Definition das Urbild des Normalteilers $\mathbb{F}_p^\times \trianglelefteq \mathbb{F}_{p^k}^\times$ unter dem Homomorphismus $\det : G \to \mathbb{F}_{p^k}^\times$, und laut Vorlesung ist jedes Urbild eines Normalteilers unter einem Gruppenhomomorphismus ebenfalls ein Normalteiler. Daraus folgt $N \trianglelefteq G$.

zu (b) Wir betrachten den Abbildung $\phi : G \to \mathbb{F}_{p^k}^\times/\mathbb{F}_p^\times$, $A \mapsto \det(A)\mathbb{F}_p^\times$. Als Komposition der Determinantenabbildung mit dem kanonischen Epimorphismus $\alpha \mapsto \alpha\mathbb{F}_p^\times$ handelt es sich um einen Gruppenhomomorphismus. Der Kern von ϕ ist gleich N, denn für alle A gilt die Äquivalenz

$$A \in \ker(\phi) \quad \Leftrightarrow \quad \phi(A) = e_{\mathbb{F}_{p^k}^\times/\mathbb{F}_p^\times} \quad \Leftrightarrow \quad \det(A)\mathbb{F}_p^\times = \mathbb{F}_p^\times \quad \Leftrightarrow \quad \det(A) \in \mathbb{F}_p^\times \quad \Leftrightarrow \quad A \in N.$$

Außerdem ist ϕ surjektiv, denn für vorgegebenes $\alpha\mathbb{F}_p^\times \in \mathbb{F}_{p^k}/\mathbb{F}_p^\times$ mit $\alpha \in \mathbb{F}_{p^k}^\times$ ist

$$C_\alpha \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \alpha \end{pmatrix}$$

wegen $\det(C_\alpha) = \alpha \neq \bar{0}$ eine invertierbare Matrix, also ein Element aus G, und es gilt $\phi(\alpha) = \det(C_\alpha)\mathbb{F}_p^\times = \alpha\mathbb{F}_p^\times$.

Damit sind alle Voraussetzungen des Homomorphiesatzes erfüllt, und wir erhalten einen Isomorphismus $G/N \cong \mathbb{F}_{p^k}^\times/\mathbb{F}_p^\times$. Es folgt

$$(G:N) \quad = \quad |G/N| \quad = \quad |\mathbb{F}_{p^k}^\times/\mathbb{F}_p^\times| \quad = \quad \frac{|\mathbb{F}_{p^k}^\times}{\mathbb{F}_p^\times} \quad = \quad \frac{p^k - 1}{p - 1} \quad = \quad \sum_{i=0}^{k-1} p^i.$$

Wegen $p^i \equiv 0 \bmod p$ für $1 \leq i \leq k-1$ folgt $(G:N) = \sum_{i=0}^{k-1} p^i \equiv 1 \bmod p$, insbesondere gilt $p \nmid (G:N)$. Weil p eine Primzahl ist, ist dies gleichbedeutend damit, dass p und $(G:N)$ teilerfremd sind.

zu (c) Sei P eine Untergruppe von G. Wir zeigen, dass P genau dann eine p-Sylowgruppe von G ist, wenn P eine p-Sylowgruppe von N ist. Dabei verwenden wir, dass allgemein eine Untergruppe P einer endlichen Gruppe G genau dann eine p-Sylowgruppe ist, wenn $|P|$ von p-Potenzordnung ist und $p \nmid (G:P)$ gilt. „$\Leftarrow$“ Weil P eine p-Sylowgruppe von N ist, gilt $p \nmid (N:P)$. Es gilt

$$(G:P) \quad = \quad \frac{|G|}{|P|} \quad = \quad \frac{|G|}{|N|} \cdot \frac{|N|}{|P|} \quad = \quad (G:N) \cdot (N:P).$$

Aus $p \nmid (G:N)$ und $p \nmid (N:P)$ folgt $p \nmid (G:P)$. Außerdem ist P (als p-Sylowgruppe von N) von p-Potenzordnung. Also ist P eine p-Sylowgruppe von G.

„⇒“ Sei P eine p-Sylowgruppe von G. Auf Grund des Ersten Isomorphiesatzes gilt $P/(N \cap P) \cong PN/N$. Weil P von p-Potenzordnung ist, gilt dasselbe für $P/(N \cap P)$ und damit auch für PN/N. Es handelt sich bei PN/N also um eine p-Untergruppe von G/N. Weil aber $|G/N| = (G : N)$ nach Teil (b) teilerfremd zu p ist, muss $PN/N = \{e_{G/N}\}$ sein, also $PN = N$ und somit $P \subseteq N$ gelten. Es ist P also eine p-Untergruppe von N. Wäre p ein Teiler von $(N : P)$, dann wäre p erst recht ein Teiler von $(G : P) = (G : N) \cdot (N : P)$. Aber dies ist nicht der Fall, weil P eine p-Sylowgruppe von G ist. Insgesamt ist damit gezeigt, dass P eine p-Sylowgruppe von N ist.

Aufgabe F20T2A4

(a) Sei $h : A \to G$ ein surjektiver Gruppenhomomorphismus einer abelschen Gruppe A in eine Gruppe G. Zeigen Sie, dass dann auch G abelsch ist.

(b) Sei p eine Primzahl, $p \neq 2$. Bestimmen Sie die Anzahl der Nullstellen des Polynoms $f(X) = x^2 + 2x + 1$ in $\mathbb{F}_{p^2}$ und in $\mathbb{Z}/p^2\mathbb{Z}$.

(c) Man zeige oder widerlege folgende Aussage: Für alle $a, b, c \in \mathbb{N}$ gilt $\mathrm{ggT}(a, b, c)\mathrm{kgV}(a, b, c) = abc$.

Lösung:
zu (a) Seien $u, v \in G$ vorgegeben. Zu zeigen ist $uv = vu$. Da h surjektiv ist, gibt es $a, b \in A$ mit $h(a) = u$ und $h(b) = v$. Weil A abelsch ist, gilt $ab = ba$. Auf Grund der Homomorphismus-Eigenschaft von h folgt $uv = h(a)h(b) = h(ab) = h(ba) = h(b)h(a) = vu$.

zu (b) Für alle $\alpha \in \mathbb{F}_{p^2}$ gilt die Äquivalenz

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \alpha^2 + 2\alpha + \bar{1} = \bar{0} \quad \Leftrightarrow \quad (\alpha + \bar{1})^2 = \bar{0} \quad \Leftrightarrow \quad \alpha + \bar{1} = \bar{0} \quad \Leftrightarrow \quad \alpha = -\bar{1}.$$

Dabei wurde im vorletzten Schritt verwendet, dass in jedem Körper K die Äquivalenz $\beta = 0_K \Leftrightarrow \beta^2 = 0_K$ für alle $\beta \in K$ gültig ist. (Im Fall $\beta = 0_K$ ist die Äquivalenz offensichtlich, im Fall $\beta \neq 0_K$ die Implikation „$\Rightarrow$“ ebenfalls, und „$\Leftarrow$“ erhält man durch $\beta = \beta^{-1}\beta^2 = \beta^{-1} \cdot 0_K = 0_K$.) Das Polynom f besitzt in $\mathbb{F}_{p^2}$ also genau eine Nullstelle.

Im Ring $\mathbb{Z}/p^2\mathbb{Z}$ ist diese Äquivalenz aber falsch, weshalb hier anders vorgegangen werden muss. Sei $a \in \mathbb{Z}$ und $\bar{a}$ das Bild von a in $\mathbb{Z}/p^2\mathbb{Z}$. Es gilt die Äquivalenz

$$\begin{aligned} f(\bar{a}) = \bar{0} \quad &\Leftrightarrow \quad \bar{a}^2 + 2\bar{a} + \bar{1} = \bar{0} \quad \Leftrightarrow \quad (\bar{a} + \bar{1})^2 = \bar{0} \quad \Leftrightarrow \quad p^2 \mid (a+1)^2 \quad \Leftrightarrow \quad p \mid (a+1) \\ &\Leftrightarrow \quad \exists\, k \in \mathbb{Z} : a + 1 = kp \quad \Leftrightarrow \quad a \in -1 + p\mathbb{Z} \quad \Leftrightarrow \quad \bar{a} \in \{-\bar{1} + \bar{p}\bar{k} \mid k \in \mathbb{Z}\} \\ &\Leftrightarrow \quad \bar{a} \in \{-\bar{1} + \bar{p}\bar{k} \mid 0 \leq k < p\}. \end{aligned}$$

Im vierten Schritt ist die Implikation „$\Leftarrow$“ erfüllt, denn aus $a+1 = kp$ für ein $k \in \mathbb{Z}$ folgt $(a+1)^2 = k^2p^2$. Ebenso gilt „$\Rightarrow$“, denn wäre $a+1$ teilerfremd zu p, dann würde dies auch für $(a+1)^2$ gelten. Im letzten Schritt haben wir verwendet, dass für $k, \ell \in \mathbb{Z}$ die Elemente $-\bar{1} + \bar{p}\bar{k}$ und $-\bar{1} + \bar{p}\bar{\ell}$ in $\mathbb{Z}/p^2\mathbb{Z}$ genau dann übereinstimmen, wenn $-1 + pk \equiv -1 + p\ell \bmod p^2$ gilt, was zu $pk \equiv p\ell \bmod p^2$ und $k \equiv \ell \bmod p$ äquivalent ist. Damit $-\bar{1} + \bar{p}\bar{k}$ alle Elemente von $\mathbb{Z}/p^2\mathbb{Z}$ durchläuft, genügt es also, für k alle Elemente aus einem Repräsentantensystem von $\mathbb{Z}/p\mathbb{Z}$ einzusetzen, zum Beispiel $\{0, 1, ..., p-1\}$. Zugleich sind diese Elemente dann alle verschieden. Das Polynom f hat also in $\mathbb{Z}/p^2\mathbb{Z}$ genau p Nullstellen.

zu (c) Diese Aussage ist im Allgemeinen falsch. Setzt man zum Beispiel $a = 5$, $b = 5^2$, $c = 5^3$, dann gilt $\mathrm{ggT}(a, b, c) = 5$, $\mathrm{kgV}(a, b, c) = 5^3$ und somit $\mathrm{ggT}(a, b, c)\mathrm{kgV}(a, b, c) = 5^4$, andererseits aber $abc = 5 \cdot 5^2 \cdot 5^3 = 5^6$. (Im Gegensatz dazu ist die Gleichung $\mathrm{ggT}(a, b)\mathrm{kgV}(a, b) = ab$ für beliebige $a, b \in \mathbb{N}$ richtig. Man beweist diese Gleichung leicht, indem man die Primfaktorzerlegung von a und b betrachtet und die Formeln für die Primfaktorzerlegung von ggT und kgV aus der Vorlesung verwendet.)

Aufgabe F20T2A5

Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $x^8 - 2$. Sei ferner $\zeta := \exp(\frac{2\pi i}{8}) \in \mathbb{C}$. Zeigen Sie:

(a) Es gilt $\sqrt{2} \in \mathbb{Q}(\zeta)$.

(b) Die Körpererweiterung $\mathbb{Q} \subseteq L$ hat den Grad $[L : \mathbb{Q}] = 16$.

(c) Die Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$ ist nicht abelsch und hat einen Normalteiler der Ordnung 4 mit $N \cong \mathbb{Z}/4\mathbb{Z}$.

Lösung:
zu (a) Es gilt $\zeta = \exp(\frac{\pi i}{4}) = \cos(\frac{1}{4}\pi) + i\sin(\frac{1}{4}\pi)$, $\zeta^{-1} = \exp(-\frac{\pi i}{4}) = \cos(\frac{1}{4}\pi) - i\sin(\frac{1}{4}\pi)$, und somit $\cos(\frac{1}{4}\pi) = \frac{1}{2}(\zeta + \zeta^{-1}) \in \mathbb{Q}(\zeta)$. Auf Grund des Additionstheorems des Kosinus gilt $0 = \cos(\frac{1}{2}\pi) = \cos(\frac{1}{4}\pi)^2 - \sin(\frac{1}{4}\pi)^2$, also $\cos(\frac{1}{4}\pi)^2 = \sin(\frac{1}{4}\pi)^2$. Es folgt $2\cos(\frac{1}{4}\pi)^2 = \cos(\frac{1}{4}\pi)^2 + \sin(\frac{1}{4}\pi)^2 = 1$, $\cos(\frac{1}{4}\pi)^2 = \frac{1}{2}$, und wegen $\cos(\alpha) > 0$ für $-\frac{1}{2}\pi < \alpha < \frac{1}{2}\pi$ folgt $\frac{1}{\sqrt{2}} = \cos(\frac{1}{4}\pi) \in \mathbb{Q}(\zeta)$. Damit ist auch der Kehrwert $\sqrt{2}$ in $\mathbb{Q}(\zeta)$ enthalten.

zu (b) Wir zeigen zunächst, dass $L = \mathbb{Q}(\sqrt[8]{2}, i)$ gilt. Die Menge der komplexen Nullstellen von $f = x^8 - 2$ ist durch $N = \{\zeta^k \sqrt[8]{2} \mid 0 \leq k < 8\}$ gegeben. Denn wegen $f(\zeta^k \sqrt[8]{2}) = (\zeta^k \sqrt[8]{2})^8 - 2 = (\zeta^8)^k \cdot 2 - 2 = 1^k \cdot 2 - 2 = 0$ sind tatsächlich alle Elemente von N Nullstellen von f. Da es sich bei ζ um eine primitive achte Einheitswurzel handelt, sind die Elemente ζ^k mit $0 \leq k < 8$ alle verschieden, und wegen $\sqrt[8]{2} \neq 0$ gilt dasselbe für $\zeta^k \sqrt[8]{2}$ mit $0 \leq k < 8$. Da andererseits ein Polynom vom Grad 8 über einem Körper nie mehr als acht Nullstellen besitzt, ist N genau die Menge der komplexen Nullstellen von f. Der Zerfällungskörper L von f über $\mathbb{Q}$ in $\mathbb{C}$ ist also durch $L = \mathbb{Q}(N)$ gegeben.

Zu zeigen bleibt $\mathbb{Q}(N) = \mathbb{Q}(\sqrt[8]{2}, i)$. Wir haben bereits in Teil (a) gesehen, dass $\cos(\frac{1}{4}\pi) = \frac{1}{\sqrt{2}}$ und $\sin(\frac{1}{4}\pi)^2 = \cos(\frac{1}{4}\pi)^2$ gilt. Wegen $\sin(\alpha) > 0$ für $0 < \alpha < \pi$ ist somit auch $\sin(\frac{1}{4}\pi) = \frac{1}{\sqrt{2}}$. Es folgt $\zeta = \cos(\frac{1}{4}\pi) + i\sin(\frac{1}{4}\pi) = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$. Aus $\sqrt[8]{2}, i \in \mathbb{Q}(\sqrt[8]{2}, i)$ folgt $\sqrt{2} = (\sqrt[8]{2})^4 \in \mathbb{Q}(\sqrt[8]{2}, i)$ und $\zeta = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \in \mathbb{Q}(\sqrt[8]{2}, i)$. Wir erhalten weiter $\zeta^k \sqrt[8]{2} \in \mathbb{Q}(\sqrt[8]{2}, i)$ für $0 \leq k < 8$ und somit $N \subseteq \mathbb{Q}(\sqrt[8]{2}, i)$. Aus $\sqrt[8]{2} \in N \subseteq \mathbb{Q}(N)$ und $\zeta\sqrt[8]{2} \in N \subseteq \mathbb{Q}(N)$ folgt andererseits $\zeta = \frac{\sqrt[8]{2}\zeta}{\sqrt[8]{2}} \in \mathbb{Q}(N)$ und $i = \zeta^2 \in \mathbb{Q}(N)$. Insgesamt gilt also $\{\sqrt[8]{2}, i\} \subseteq \mathbb{Q}(N)$. Aus den beiden Inklusionen $\{\sqrt[8]{2}, i\} \subseteq \mathbb{Q}(N)$ und $N \subseteq \mathbb{Q}(\sqrt[8]{2}, i)$ folgt die Gleichung $\mathbb{Q}(N) = \mathbb{Q}(\sqrt[8]{2}, i)$. Insgesamt ist der Beweis von $L = \mathbb{Q}(\sqrt[8]{2}, i)$ damit abgeschlossen.

Nun bestimmen wir den Erweiterungsgrad $[L : \mathbb{Q}]$. Das Polynom $f = x^8 - 2$ ist in $\mathbb{Q}[x]$ irreduzibel nach dem Eisenstein-Kriterium, angewendet auf die Primzahl $p = 2$. Außerdem ist es normiert und hat $\sqrt[8]{2}$ als Nullstelle. Insgesamt ist f damit das Minimalpolynom von $\sqrt[8]{2}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = \mathrm{grad}(f) = 2$. Das Polynom $g = x^2 + 1$ ist normiert und hat i als Nullstelle. Wäre es über $\mathbb{Q}(\sqrt[8]{2})$ reduzibel, dann müssten wegen $\mathrm{grad}(g) = 2$ die beiden Nullstellen $\pm i$ in $\mathbb{Q}(\sqrt[8]{2})$ liegen. Aber dies ist unmöglich, denn es gilt $\mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{R}$, während die Zahlen $\pm i$ nicht reell sind. Also ist g das Minimalpolynom von i über $\mathbb{Q}(\sqrt[8]{2})$, und es folgt

$$[L : \mathbb{Q}(\sqrt[8]{2})] \quad = \quad [\mathbb{Q}(\sqrt[8]{2})(i) : \mathbb{Q}(\sqrt[8]{2})] \quad = \quad \mathrm{grad}(f) \quad = \quad 2.$$

Mit der Gradformel erhalten wir $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[8]{2})] \cdot [\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 2 \cdot 8 = 16$.

zu (c) Wäre G abelsch, dann müsste jede Untergruppe von G Normalteiler sein. Insbesondere wäre $\mathrm{Gal}(L|\mathbb{Q}(\sqrt[8]{2}))$ ein Normalteiler von G, und nach den Ergänzungen zum Hauptsatz der Galoistheorie würde sich daraus ergeben, dass $\mathbb{Q}(\sqrt[8]{2})|\mathbb{Q}$ eine Galois-Erweiterung ist, insbesondere eine normale Erweiterung. Aber dies ist nicht der Fall. Denn das Polynom $f = x^8 - 2$ ist über $\mathbb{Q}$ irreduzibel und hat

in $\mathbb{Q}(\sqrt[8]{2})$ eine Nullstelle. Wäre die Erweiterung normal, dann müsste f über $\mathbb{Q}(\sqrt[8]{2})$ bereits in Linearfaktoren zerfallen, also alle komplexen Nullstellen bereits in $\mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{R}$ liegen. Aber f besitzt auch nicht-reelle Nullstellen in $\mathbb{C}$, beispielsweise $\zeta\sqrt[8]{2}$. Dies zeigt, dass G nicht-abelsch ist.

Für den Beweis der zweiten Aussage zeigen wir zunächst, dass es in G ein Element σ mit $\mathrm{ord}(\sigma) = 8$ gibt. Der erste Schritt ist die Konstruktion eines solchen Elements. Nach dem Fortsetzungssatz, angewendet auf das irreduzible Polynom $f \in \mathbb{Q}[x]$ und die beiden Nullstellen $\sqrt[8]{2}$ und $\zeta\sqrt[8]{2}$, existiert ein $\mathbb{Q}$-Homomorphismus $\tilde{\sigma} : \mathbb{Q}(\sqrt[8]{2}) \to \mathbb{C}$ mit $\sigma(\sqrt[8]{2}) = \zeta\sqrt[8]{2}$. Nochmalige Anwendung dieses Satzes, diesmal auf das über $\mathbb{Q}(\sqrt[8]{2})$ irreduzible Polynom $g = x^2 + 1$, liefert eine Fortsetzung $\sigma : L \to \mathbb{C}$ von $\tilde{\sigma}$ mit $\sigma(i) = i$. Es gilt also $\sigma(\sqrt[8]{2}) = \zeta\sqrt[8]{2}$ und $\sigma(i) = i$. Da die Erweiterung $L|\mathbb{Q}$ normal ist, handelt es sich bei σ sogar um einen $\mathbb{Q}$-Automorphismus von L, also um ein Element von G.

Aus $\sigma(\sqrt[8]{2}) = \zeta\sqrt[8]{2}$ folgt $\sigma(\sqrt[2]{8}) = \sigma((\sqrt[8]{2})^4) = \sigma(\sqrt[8]{2})^4 = (\zeta\sqrt[8]{2})^4 = \zeta^4(\sqrt[8]{2})^4 = (-1)\sqrt{2} = -\sqrt{2}$ und

$$\sigma(\zeta) \quad = \quad \sigma(\tfrac{1}{\sqrt{2}} + \tfrac{i}{\sqrt{2}}) \quad = \quad \tfrac{1}{\sigma(\sqrt{2})} + \tfrac{\sigma(i)}{\sigma(\sqrt{2})} \quad = \quad -\tfrac{1}{\sqrt{2}} - \tfrac{i}{\sqrt{2}} \quad = \quad -\zeta.$$

Wir erhalten weiter

$$\sigma^2(\sqrt[8]{2}) = \sigma(\sigma(\sqrt[8]{2})) = \sigma(\zeta\sqrt[8]{2}) = \sigma(\zeta)\sigma(\sqrt[8]{2}) = (-\zeta)(\zeta\sqrt[8]{2}) = -i\sqrt[8]{2}$$

$$\sigma^4(\sqrt[8]{2}) = \sigma^2(\sigma^2(\sqrt[8]{2})) = \sigma^2(-i\sqrt[8]{2}) = -\sigma^2(i)\sigma^2(\sqrt[8]{2}) = (-i)(-i)\sqrt[8]{2} = -\sqrt[8]{2}$$

$$\sigma^8(\sqrt[8]{2}) = \sigma^4(\sigma^4(\sqrt[8]{2})) = \sigma^4(-\sqrt[8]{2}) = -\sigma^4(\sqrt[8]{2}) = -(-\sqrt[8]{2}) = \sqrt[8]{2}.$$

Aus $\sigma^8(\sqrt[8]{2}) = \sqrt[8]{2}$ und $\sigma^8(i) = i$ folgt $\sigma^8 = \mathrm{id}$, denn wegen $L = \mathbb{Q}(\sqrt[8]{2}, i)$ ist jedes Element aus G durch die Bilder von $\sqrt[8]{2}$ und i festgelegt. Aus $\sigma^4(\sqrt[8]{2}) \neq \sqrt[8]{2}$ folgt andererseits $\sigma^4 \neq \mathrm{id}$. Damit ist $\mathrm{ord}(\sigma) = 8$ nachgewiesen.

Sei nun $N = \mathrm{Gal}(L|\mathbb{Q}(\zeta))$. Als Kreisteilungserweiterung ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine normale Erweiterung, und nach den Ergänzungen zum Hauptsatz der Galoistheorie gilt somit $N \trianglelefteq G$. Darüber hinaus gilt $G/N \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$, außerdem $|G| = |\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 16$. Es folgt

$$\frac{16}{|N|} \quad = \quad \frac{|G|}{|N|} \quad = \quad |G/N| \quad = \quad |(\mathbb{Z}/8\mathbb{Z})^\times| \quad = \quad \varphi(8) \quad = \quad 4.$$

Es folgt $|N| = \frac{16}{4} = 4$. Bekanntlich sind die einzigen Gruppen der Ordnung 4 bis auf Isomorphie durch $\mathbb{Z}/4\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})^2$ gegeben.

Nehmen wir an, es ist $N \cong (\mathbb{Z}/2\mathbb{Z})^2$. Weil es in $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ nur Elemente der Ordnung 1 und 2 gibt, gilt für jedes $\tau \in G$ jeweils $\tau^2 N = (\tau N)^2 = e_{G/N} = N$ und somit $\tau^2 \in N$. Weil auch in $N \cong (\mathbb{Z}/2\mathbb{Z})^2$ nur Elemente der Ordnung 1 und 2 existieren, folgt daraus weiter $\tau^4 = (\tau^2)^2 = \mathrm{id}_L$. Aus der Annahme folgt also, dass in G nur Elemente existieren, deren Ordnungen Teiler von 4 sind, im Widerspruch dazu, dass es in G ein Element der Ordnung 8 gibt. Somit bleibt $N \cong \mathbb{Z}/4\mathbb{Z}$ als einzige Möglichkeit.

Aufgabe F20T3A1

Seien G und G' Gruppen und $f : G \to G'$ ein Gruppenhomomorphismus.

(a) Definieren Sie den Begriff *Normalteiler*.

(b) Sei K der Kern von f, und sei $H \subseteq G$ eine Untergruppe. Zeigen Sie, dass

$$f^{-1}(f(H)) = HK = \{hk \mid h \in H, k \in K\} \qquad \text{ist.}$$

(c) Sei G eine Gruppe, und seien H und K Normalteiler in G mit der Eigenschaft $H \cap K = \{e_G\}$. Zeigen Sie, dass $kh = hk$ gilt für alle $h \in H$ und $k \in K$.

(d) Geben Sie ein Beispiel (U, G) mit einer Gruppe G und einer Untergruppe U von G, die kein Normalteiler ist.

Lösung:
zu (a) Ein *Normalteiler* einer Gruppe G ist eine Untergruppe N mit der Eigenschaft, dass $gN = Ng$ für alle $g \in G$ erfüllt ist.

zu (b) „$\subseteq$“ Sei $g \in f^{-1}(f(H))$ vorgegeben. Dann ist $f(g) \in f(H)$, also $f(g) = f(h)$ für ein $h \in H$. Es folgt $f(h^{-1}g) = f(h^{-1})f(g) = f(h)^{-1}f(g) = e_{G'}$ und somit $h^{-1}g \in K$. Dies wiederum bedeutet $g = h(h^{-1}g) \in HK$. „$\supseteq$“ Sei $g \in HK$, also $g = hk$ für ein $h \in H$ und ein $k \in K$. Dann folgt $f(g) = f(hk) = f(h)f(k) = f(h) \cdot e_{G'} = f(h) \in f(H)$ und somit $g \in f^{-1}(f(H))$.

zu (c) Seien $h \in H$ und $k \in K$ vorgegeben. Die Gleichung $kh = hk$ ist äquivalent zu $khk^{-1}h^{-1} = e_G$. Wegen $H \trianglelefteq G$ ist $khk^{-1} \in H$ und $khk^{-1}h^{-1} = (khk^{-1})h^{-1} \in H$. Wegen $K \trianglelefteq G$ gilt auch $hk^{-1}h^{-1} \in K$ und $khk^{-1}h^{-1} = k(hk^{-1}h^{-1}) \in K$. Insgesamt ist damit nachgewiesen, dass $khk^{-1}h^{-1}$ in $H \cap K = \{e_G\}$ enthalten ist. Also gilt $khk^{-1}h^{-1} = e_G$.

zu (d) Sei G die symmetrische Gruppe S_3 und $U = \langle(1\ 2)\rangle = \{\mathrm{id}, (1\ 2)\}$. Dann gilt einerseits $(1\ 3)U = \{(1\ 3)\circ\mathrm{id}, (1\ 3)\circ(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$, andererseits $U(1\ 3) = \{\mathrm{id}\circ(1\ 3), (1\ 2)\circ(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\}$. Es gilt also $(1\ 3)U \neq U(1\ 3)$, was zeigt, dass U kein Normalteiler von S_3 ist.

Aufgabe F20T3A2

Berechnen Sie die letzten beiden Ziffern der Zahl

$$2018^{(2019^{2020})}.$$

Gehen Sie dazu wie folgt vor:

(a) Berechnen Sie die Klasse von $2018^{(2019^{2020})}$ in $\mathbb{Z}/25\mathbb{Z}$.

(b) Zeigen Sie, dass $[2018^{(2019^{2020})}] = 0$ in $\mathbb{Z}/4\mathbb{Z}$ gilt.

(c) Schließen Sie die Berechnung mit Hilfe des Chinesischen Restsatzes ab.

Lösung:
zu (a) Laut Vorlesung gilt $|\mathbb{Z}/25\mathbb{Z}^\times| = \varphi(25) = 20$, und in $\mathbb{Z}/20\mathbb{Z}^\times$ gilt

$$[2019]^{2020} \quad = \quad [19]^{2020} \quad = \quad [-1]^{2020} \quad = \quad ([-1]^2)^{1010} \quad = \quad [1]^{1010} \quad = \quad 1.$$

Es folgt $2019^{2020} \equiv 1 \bmod 20$; es existiert also ein $k \in \mathbb{Z}$ mit $2019^{2020} = 1 + 20k$. Wegen $|\mathbb{Z}/25\mathbb{Z}^\times| = 20$ gilt $\bar{c}^{20} = \bar{1}$ für alle $\bar{c} \in (\mathbb{Z}/25\mathbb{Z})^\times$. Wegen $5 \nmid 2018$ folgt $\mathrm{ggT}(2018, 25) = 1$, also ist die Klasse $[2018]$ von 2018 in $\mathbb{Z}/25\mathbb{Z}$ in $(\mathbb{Z}/25\mathbb{Z})^\times$ enthalten. Daraus wiederum folgt

$$[2018^{(2019^{2020})}] \quad = \quad [2018^{1+20k}] \quad = \quad [2018] \cdot ([2018]^{20})^k \quad = \quad [2018] \cdot [1]^k \quad = \quad [2018] \quad = \quad [18].$$

zu (b) Für alle $k \geq 2$ gilt $4 \mid 2^k$ und somit $[2]^k = [0]$ in $\mathbb{Z}/4\mathbb{Z}$, und es ist $2019^{2020} \geq 2019 \geq 2$. Wegen $2018 \equiv 2 \bmod 4$ folgt $[2018]^{(2019^2020)} = [2]^{(2019^{2020})} = [0]$ in $\mathbb{Z}/4\mathbb{Z}$.

zu (c) Laut Chinesischem Restsatz existiert ein (eindeutig bestimmter) Ringhisomorphismus $\phi : \mathbb{Z}/100\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ mit $\phi(c + 100\mathbb{Z}) = (c + 4\mathbb{Z}, c + 25\mathbb{Z})$ für alle $c \in \mathbb{Z}$. Daraus folgt: Sind $c_1, c_2 \in \mathbb{Z}$ mit $c_1 \equiv c_2 \bmod 4$ und $c_1 \equiv c_2 \equiv c_2 \bmod 25$, dann folgt $c_1 \equiv c_2 \bmod 100$. Denn auf Grund der Voraussetzung gilt

$$\phi(c_1 + 100\mathbb{Z}) \quad = \quad (c_1 + 4\mathbb{Z}, c_1 + 25\mathbb{Z}) \quad = \quad (c_2 + 4\mathbb{Z}, c_2 + 25\mathbb{Z}) \quad = \quad \phi(c_2 + 100\mathbb{Z}).$$

Aus der Injektivität von ϕ folgt $c_1 + 100\mathbb{Z} = c_2 + 100\mathbb{Z}$, und dies wiederum ist gleichbedeutend mit $c_1 \equiv c_2 \bmod 100$.

Es gibt gibt genau vier Zahlen $c \in \mathbb{Z}$ mit $0 \leq c < 100$ mit $c \equiv 18 \bmod 25$, nämlich 18, 43, 68 und 93. Nur eine dieser Zahlen erfüllt auch die Bedingung $c \equiv 0 \bmod 4$, nämlich 68. Sei nun $c_1 = 2018^{(2019^{2020})}$ und $c_2 = 68$. Nach Teil (a) gilt $c_1 \equiv 18 \equiv 68 \equiv c_2 \bmod 25$, und nach Teil (b) gilt $c_1 \equiv 0 \equiv 68 \equiv c_2 \bmod 4$. Wie soeben ausgeführt, folgt daraus $c_1 \equiv c_2 \bmod 100$, also $c_1 \equiv 68 \bmod 100$. Dies bedeutet, dass die letzten beiden Ziffern der Zahl c_1 durch 6 und 8 gegeben sind.

Aufgabe F20T3A3

Sei p eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen und $V = \mathbb{F}_p^n$ für $n \in \mathbb{N}$. Weiter sei $G \leq \mathrm{GL}_n(\mathbb{F}_p)$ eine Gruppe, deren Ordnung eine Potenz von p ist. Man zeige, dass es einen Vektor $0 \neq v \in \mathbb{F}_p^n$ gibt mit $gv = v$ für alle $g \in G$.
(Hinweis: $|V \setminus \{0\}|$ ist nicht durch p teilbar.)

Lösung:
Bekanntlich ist durch $\cdot : \mathrm{GL}_n(\mathbb{F}_p) \times V \to V$, $(A, v) \mapsto Av$ eine Gruppenoperation von $\mathrm{GL}_n(\mathbb{F}_p)$ auf V definiert, und durch Einschränkung der Abbildung auf $G \times V$ erhalten wir eine Operation von G auf V. Es sei $F \subseteq V$ die Fixpunktmenge dieser Operation und $R \subseteq V$ ein Repräsentantensystem der Bahnen mit mehr als einem Element. Laut Bahngleichung gilt

$$p^n \quad = \quad |V| \quad = \quad |F| + \sum_{v \in R} (G : G_v)$$

mit $(G : G_v) > 1$ für alle $v \in R$. Nach Voraussetzung gibt es außerdem $|G| = p^e$ für ein $e \in \mathbb{N}$. Betrachten wir nun zunächst den Fall $e = 0$. Dann ist $G = \{E\}$ mit der Einheitsmatrix E, und für einen beliebig gewählten Vektor $v \in V \setminus \{0\}$ gilt $Ev = v$, also $gv = v$ für alle $g \in G$.

Ist dagegen $e > 0$, dann ist nicht nur $|G|$, sondern auch $(G : G_v)$ für jedes $v \in R$ eine p-Potenz größer als 1. Daraus folgt, dass $\sum_{v \in R}$ durch p teilbar ist. Weil auch p^n ein Vielfaches von p ist, ergibt sich aus der Bahngleichung, dass dasselbe auch für $|F|$. Außerdem ist $|F|$ positv, denn wegen $A \cdot 0 = 0$ für alle $A \in G$ ist der Nullvektor auf jeden Fall in G enthalten. Ingesamt gilt damit $|F| \geq p > 1$, insbesondere gibt es ein $v \in F \setminus \{0\}$. Wegen $v \in F$ ist $Av = v$ für alle $A \in G$ erfüllt.

Aufgabe F20T3A4

Seien K ein Körper und $L|K$ eine endliche Galoiserweiterung.

(a) Wir betrachten Zwischenkörper M und M' von $L|K$ und ein Element σ in $\mathrm{Gal}(L|K)$. Zeigen Sie die Äquivalenz der folgenden beiden Aussagen.

(i) $\sigma(M) = M'$

(ii) $\sigma\mathrm{Gal}(L|M)\sigma^{-1} = \mathrm{Gal}(L|M')$

(b) Seien L der Zerfällungskörper eines irreduziblen Polynoms f in $K[x]$ und α und β Nullstellen von f in L. Zeigen Sie, dass die Galoisgruppen $\mathrm{Gal}(L|K(\alpha))$ und $\mathrm{Gal}(L|K(\beta))$ zueinander isomorph sind.

(c) Zeigen Sie, dass man in (b) die Voraussetzung, dass f irreduzibel ist, nicht weglassen kann.

Lösung:
zu (a) „⇒“ Wir zeigen, dass M' der Fixkörper der Untergruppe $U = \sigma\mathrm{Gal}(L|M)\sigma^{-1}$ von $G = \mathrm{Gal}(L|K)$ ist; dann folgt Gleichung (ii) aus dem Hauptsatz der Galoistheorie. Sei $\alpha \in L$ vorgegeben. Weil $\sigma : L \to L$ bijektiv ist, existiert ein $\beta \in L$ mit $\sigma(\beta) = \alpha$. Es gilt nun die Äquivalenz

$$\begin{gathered}\alpha \in L^U \quad \Leftrightarrow \quad \forall\, \tau \in U : \tau(\alpha) = \alpha \quad \Leftrightarrow \quad \forall\, \tau \in \mathrm{Gal}(L|M) : (\sigma \circ \tau \circ \sigma^{-1})(\alpha) = \alpha \quad \Leftrightarrow \\ \forall\, \tau \in \mathrm{Gal}(L|M) : (\sigma \circ \tau \circ \sigma^{-1})(\sigma(\beta)) = \sigma(\beta) \quad \Leftrightarrow \quad \forall\, \tau \in \mathrm{Gal}(L|M) : \sigma(\tau(\beta)) = \sigma(\beta) \quad \Leftrightarrow \\ \forall\, \tau \in \mathrm{Gal}(L|M) : \tau(\beta) = \beta \quad \Leftrightarrow \quad \beta \in L^{\mathrm{Gal}(L|M)} \quad \Leftrightarrow \quad \beta \in M \quad \Leftrightarrow \quad \sigma(\beta) \in \sigma(M) \quad \Leftrightarrow \quad \alpha \in M'.\end{gathered}$$

Dabei wurde im fünften Schritt erneut die Bijektivität von σ verwendet, und im siebten (drittletzten) der Hauptsatz der Galoistheorie. Die Äquivalenz zeigt, dass tatsächlich $M' = L^U$ gilt.

„⇐“ Sei $M'' = \sigma(M)$. Wie wir unter „⇒“ gezeigt haben, ist M'' der Fixkörper von $\sigma\mathrm{Gal}(L|M)\sigma^{-1}$, auf Grund der Voraussetzung also von $\mathrm{Gal}(L|M')$. Nach dem Hauptsatz der Galoistheorie gilt $L^{\mathrm{Gal}(L|M')} = M'$. Aus Aus $M'' = L^{\mathrm{Gal}(L|M')}$ und $L^{\mathrm{Gal}(L|M')} = M'$ folgt $M' = M'' = \sigma(M)$.

zu (b) Auf Grund des Fortsetzungssatzes, angewendet auf das irreduzible Polynom f, existiert ein Element $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Weil σ ein K-Homomorphismus ist, gilt $\sigma(K(\alpha)) = K(\sigma(\alpha)) = K(\beta)$. Nach Teil (a) folgt daraus $\mathrm{Gal}(L|K(\beta)) = \sigma\mathrm{Gal}(L|K(\alpha))\sigma^{-1}$. Die Untergruppen $\mathrm{Gal}(L|K(\alpha))$ und $\mathrm{Gal}(L|K(\beta))$ sind also konjugiert zueinander; daraus folgt, dass sie isomorph sind.

zu (c) Sei $f = x(x^2+1) = x^3 + x \in \mathbb{Q}[x]$. Die Nullstellenmenge dieses Polynoms ist $N = \{0, i, -i\}$, somit ist $L = \mathbb{Q}(N)$ der Zerfällungskörper von f. Aus $i \in N \subseteq \mathbb{Q}(N)$ und $N = \{0, i, -i\} \subseteq \mathbb{Q}(i)$ folgt $\mathbb{Q}(N) = \mathbb{Q}(i)$. Die Erweiterung $L|\mathbb{Q}$ ist normal, da L Zerfällungskörper des Polynoms f über $\mathbb{Q}$ ist. Als normale Erweiterung ist $L|\mathbb{Q}$ insbesondere algebraisch, und jede algebraische Erweiterung von $\mathbb{Q}$ ist wegen $\mathrm{char}(\mathbb{Q}) = 0$ separabel. Insgesamt ist $L|\mathbb{Q}$ also eine Galois-Erweiterung.

Wir bestimmen die Ordnung der Galois-Gruppe $G = \mathrm{Gal}(f|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(i)|\mathbb{Q})$. Das Polynom $g = x^2 + 1$ ist normiert, irreduzibel und hat i als Nullstelle. Es ist g also das Minimalpolynom von i über $\mathbb{Q}$, und folglich gilt $[L : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = \mathrm{grad}(g) = 2$. Da $L|Q$ eine Galois-Erweiterung ist, erhalten wi r $|G| = |\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 2$.

Betrachten wir nun die beiden Nullstellen $\alpha = 0$ und $\beta = i$ von f. Dann ist $\mathbb{Q}(\alpha) = Q$ und $\mathbb{Q}(\beta) = L$. Es folgt $|\mathrm{Gal}(L|\mathbb{Q}(\alpha))| = [L : \mathbb{Q}(\alpha)] = [L : \mathbb{Q}] = 2$ und $|\mathrm{Gal}(L|\mathbb{Q}(\beta))| = [L : \mathbb{Q}(\beta)] = [L : L] = 1$. Als Gruppen unterschiedlicher Ordnung können $\mathrm{Gal}(L|\mathbb{Q}(\alpha))$ und $\mathrm{Gal}(L|\mathbb{Q}(\beta))$ nicht isomorph sein.

Aufgabe F20T3A5

Wir betrachten das Polynom $f_1 := x^5 + 10x + 5$ in $\mathbb{Q}[x]$ und definieren induktiv Polynome $f_n(x) := f_1(f_{n-1}(x))$ für $n \in \mathbb{N}$ mit $n \geq 2$. Zeigen Sie, dass die Polynome f_n für alle $n \in \mathbb{N}$ irreduzibel sind. Zeigen Sie dazu folgende Zwischenschritte durch Induktion nach n:

(a) f_n liegt in $\mathbb{Z}[x]$, und die Klasse von f_n in $\mathbb{Z}/5\mathbb{Z}[x]$ ist durch x^{5^n} gegeben.

(b) Zeigen Sie, dass die Klasse von $f_n(0)$ in $\mathbb{Z}/25\mathbb{Z}$ nicht verschwindet.

Lösung:
zu (a) Für alle $n \in \mathbb{N}$ sei $\bar{f}_n$ jeweils das Bild von $f_n \in \mathbb{Z}[x]$ in $\mathbb{Z}/5\mathbb{Z}[x]$. Wir beweisen nun die angegebene Aussage durch vollständige Induktion nach n. Das Polynom f_1 ist nach Definition in $\mathbb{Z}[x]$ enthalten und das Bild von f_1 in $\mathbb{Z}/5\mathbb{Z}[x]$ ist gegeben durch $\bar{f}_1 = x^5 + \overline{10}x + \bar{5} = x^5 = x^{5^1}$. Damit ist die Aussage für $n = 1$ bewiesen. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für n voraus. Dann gilt also $f_n \in \mathbb{Z}[x]$ und $\bar{f}_n = x^{5^n}$. Allgemein gilt: Setzt man in ein Polynom $f \in \mathbb{Z}[x]$ ein Polynom $g \in Z[x]$ ein, dann ist $f(g(x))$ wiederum in $\mathbb{Z}[x]$ enthalten. Daraus folgt $f_{n+1}(x) = f_1(f_n(x)) \in \mathbb{Z}[x]$. Betrachten wir auf beiden Seiten dieser Gleichung das Bild in $\mathbb{Z}/5\mathbb{Z}[x]$, so erhalten wir $\bar{f}_{n+1}(x) = \bar{f}_1(\bar{f}_n(x)) = \bar{f}_n(x)^5 + \overline{10}\bar{f}_n(x) + \bar{5} = \bar{f}_n(x)^5 = (x^{5^n})^5 = x^{5^{n+1}}$. Damit ist die Aussage für $n + 1$ bewiesen.

zu (b) Hier beweisen wir durch vollständige Induktion über n, dass $f_n(0)$ jeweils zwar durch 5, aber nicht durch 25 teilbar ist. Daraus ergibt sich unmittelbar, dass das Bild von $f_n(0)$ in $\mathbb{Z}/25\mathbb{Z}$ ungleich null ist. Für $n = 1$ ist die Aussage wegen $f_1(0) = 5$, $5 \mid 5$ und $25 \nmid 5$ offenbar erfüllt. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für n voraus. Dann gilt laut Annahme $5 \mid f_n(0)$ und $25 \nmid f_n(0)$. Nach Definition ist $f_{n+1}(x) = f_1(f_n(x))$ und somit $f_{n+1}(0) = f_1(f_n(0)) = f_n(0)^5 + 10f_n(0) + 5$. Wegen $5 \mid f_n(0)$ ist $f_n(0)^5$ durch 5^5 und somit erst recht durch 25 teilbar. Aus $5 \mid f_n(0)$ und $5 \mid 10$ folgt auch $25 \mid 10f_n(0)$. Damit gilt insgesamt $f_{n+1}(0) \equiv 5 \bmod 25$. Dies zeigt, dass auch $f_{n+1}(0)$ zwar durch 5, aber nicht durch 25 teilbar ist.

Die Irreduzibilität von f_n für alle $n \in \mathbb{N}$ folgt nun aus dem Eisenstein-Kriterium. Um nachzuweisen, dass die Voraussetzungen dieses Kriteriums jeweils erfüllt sind, zeigen wir noch durch vollständige Induktion, dass x^{5^n} jeweils der Leitterm von f_n, das Polynom also insbesondere normiert ist. Für f_1 ist dies offenbar erfüllt, der Leitterm ist x^5. Sei nun $n \in \mathbb{N}$, und setzen wir voraus, dass x^{5^n} der Leitterm von f_n ist. Es ist $f_{n+1} = f_n^5 + 10f_n + 5$. Nach Induktionsvoraussetzung ist f_n vom Grad 5^n, also ist f_n^5 vom Grad $5 \cdot 5^n = 5^{n+1}$ und $10f_n$ vom Grad 5^n. Der Leitterm von f_{n+1} ist also gleich dem Leitterm von f_n^5, und dieser ist durch $(x^{5^n})^5 = x^{5^{n+1}}$ gegeben.

Jedes f_n ist also normiert vom Grad 5^n, x^{5^n} ist der Leitterm und 1 der Leitkoeffizient. Weil das Bild von f_n in $\mathbb{Z}/5\mathbb{Z}[x]$ nach Teil (a) gleich x^{5^n} ist, sind alle übrigen Koeffizienten von f_n durch 5 teilbar. Nach Teil (b) ist der konstante Termn $f_n(0)$ aber nicht durch 25 teilbar. Also sind tatsächlich alle Voraussetzungen des Eisenstein-Kriteriums erfüllt.

Aufgabe H20T1A1

(a) Entscheiden Sie, ob es eine Potenz von 7 gibt, die mit den Ziffern 11 endet, und begründen Sie Ihre Entscheidung.

(b) Ermitteln Sie die kleinste Potenz von 7, die auf 001 endet.

(c) Bestimmen Sie die letzten vier Ziffern von 7^{2020}.

Lösung:
zu (a) Eine Potenz 7^n mit $n \in \mathbb{N}$ endet genau dann auf die Ziffern 11, wenn $7^n \equiv 11 \bmod 100$ gilt. Dies wiederum ist genau dann der Fall, wenn in $\mathbb{Z}/100\mathbb{Z}$ die Gleichung $\bar{7}^n = \overline{11}$ erfüllt ist. Wegen $\mathrm{ggT}(7, 100) = 1$ ist $\bar{7}$ ein Element der primen Restklassengruppe $(\mathbb{Z}/100\mathbb{Z})^\times$. Wäre $\bar{7}^n = \overline{11}$ für ein $n \in \mathbb{N}_0$ erfüllt, dann müsste $\overline{11}$ in der von $\bar{7}$ erzeugten Untergruppe $\langle\bar{7}\rangle$ von $(\mathbb{Z}/100\mathbb{Z})^\times$ liegen.

Es gilt $\bar{7}^2 = \overline{49} \neq \bar{1}$ und $\bar{7}^4 = (\overline{49})^2 = \overline{2401} = \bar{1}$. Dies zeigt, dass $\bar{7}$ in $(\mathbb{Z}/100\mathbb{Z})^\times$ ein Element der Ordnung 4 ist und folglich $\langle\bar{7}\rangle = \{\bar{7}^0, \bar{7}^1, \bar{7}^2, \bar{7}^3\} = \{\bar{1}, \bar{7}, \overline{49}, \overline{43}\}$ gilt. Insbesondere ist $\overline{11}$ nicht in $\langle\bar{7}\rangle$ enthalten, und folglich gibt es keine Potenz von 7, die auf die Ziffern 11 endet.

zu (b) Eine Potenz 7^n mit $n \in \mathbb{N}$ endet genau dann auf die Ziffern 001, wenn $7^n \equiv 1 \bmod 1000$ gilt. Dies wiederum ist genau dann der Fall, wenn in $\mathbb{Z}/1000\mathbb{Z}$ die Gleichung $\bar{7}^n = \bar{1}$ erfüllt ist. Wegen $\mathrm{ggT}(7, 1000) = 1$ ist $\bar{7}$ ein Element der Gruppe $(\mathbb{Z}/1000\mathbb{Z})^\times$, und das kleinste $n \in \mathbb{N}$ mit $\bar{7}^n = \bar{1}$ ist die Ordnung von $\bar{7}$ in dieser Gruppe.

Auf Grund des Chinesischen Restsatzes und wegen $\mathrm{ggT}(8, 125) = 1$ existiert ein Isomorphismus $\phi : (\mathbb{Z}/1000\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/125\mathbb{Z})^\times$ gegeben durch $a + 1000\mathbb{Z} \mapsto (a + 8\mathbb{Z}, a + 125\mathbb{Z})$. Die Ordnung von $\bar{7}$ in $(\mathbb{Z}/1000\mathbb{Z})^\times$ stimmt also mit der Ordnung von $(\bar{7}, \bar{7})$ in $(\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/125\mathbb{Z})^\times$ überein.

Es ist $(\mathbb{Z}/125\mathbb{Z})^\times$ eine Gruppe der Ordnung $\varphi(125) = 100$, wobei φ die Eulersche φ-Funktion bezeichnet. Die Ordnung von $\bar{7} \in (\mathbb{Z}/125\mathbb{Z})^\times$ muss somit ein Teiler von 100 sein. Es gilt $\bar{7}^2 = \overline{49}$, $\bar{7}^4 = \overline{49}^2 = \overline{26}$, $\bar{7}^8 = \overline{26}^2 = \overline{51}$, $\bar{7}^{10} = \bar{7}^8 \cdot \bar{7}^2 = \overline{51} \cdot \overline{49} = \overline{124} = -\bar{1}$ und $\bar{7}^{20} = (-\bar{1})^2 = \bar{1}$. Dies zeigt, dass $\bar{7}$ in $(\mathbb{Z}/125\mathbb{Z})^\times$ die Ordnund 20 hat. In $(\mathbb{Z}/8\mathbb{Z})^\times$ gilt $\bar{7}^2 = \overline{49} = \bar{1}$ und somit ebenfalls $\bar{7}^{20} = (\bar{7}^2)^{10} = \bar{1}^{10} = \bar{1}$. Insgesamt ist 20 damit die kleinste natürliche Zahl n mit der Eigenschaft $(\bar{7}, \bar{7})^n = (\bar{1}, \bar{1})$ in $(\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/125\mathbb{Z})^\times$. Folglich ist 20 auch die Ordnung von $\bar{7}$ in $(\mathbb{Z}/1000\mathbb{Z})^\times$. Die kleinste Potenz von 7, die auf 001 endet, ist somit $7^{20} = 79.792.266.297.612.001$.

(Die Anwendung des Chinesischen Restsatzes ist hier nicht unbedingt notwendig. Es entstehen beim Rechnen in $\mathbb{Z}/125\mathbb{Z}$ lediglich nicht ganz so große Zahlen wie in $\mathbb{Z}/1000\mathbb{Z}$.)

zu (c) An den letzten vier Stellen der Zahl 7^{20} kann abgelesen werden, dass in $\mathbb{Z}/10000\mathbb{Z}$ die Gleichung $\bar{7}^{20} = \overline{2001}$ gilt, und es ist $\bar{7}^{100} = (\bar{7}^{20})^5 = \overline{2001}^5 = \bar{1}$. Daraus folgt $\bar{7}^{2020} = \bar{7}^{100 \cdot 20 + 20} = (\bar{7}^{100})^{20} \cdot \bar{7}^{20} = \bar{1}^{20} \cdot \overline{2001} = \overline{2001}$. Die letzten vier Ziffern von 7^{2020} sind also 2001.

Aufgabe H20T1A2

(a) Begründen Sie für jeden der folgenden vier Ringe $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{F}_2[x]/(x^2)$ und $\mathbb{F}_2[x]/(x^2+x+\bar{1})$, ob er ein Körper ist.

(b) Zeigen Sie, dass die vier Ringe aus Teilaufgabe (a) paarweise nicht isomorph sind.

Lösung:
zu (a) Die Ringe $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2 \times \mathbb{F}_2$ und $\mathbb{F}_2[x]/(x^2)$ sind keine Körper. Denn Körper sind Integritätsbereiche, was bedeutet, dass in ihnen kein von Null verschiedener Nullteiler existiert. Die Gleichungen $\bar{2} \cdot \bar{2} = \bar{0} = 0_{\mathbb{Z}/4\mathbb{Z}}$ in $\mathbb{Z}/4\mathbb{Z}$, $(\bar{1}, \bar{0}) \cdot (\bar{0}, \bar{1}) = (\bar{0}, \bar{0}) = 0_{\mathbb{F}_2 \times \mathbb{F}_2}$ in $\mathbb{F}_2 \times \mathbb{F}_2$ und $(x + (x^2)) \cdot (x + (x^2)) = x^2 + (x^2) = (x^2) = 0_{\mathbb{F}_2[x]/(x^2)}$ sowie die Ungleichungen $\bar{2} \neq 0_{\mathbb{Z}/4\mathbb{Z}}$, $(\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \neq 0_{\mathbb{F}_2 \times \mathbb{F}_2}$ und $x + (x^2) \neq 0_{\mathbb{F}_2[x]/(x^2)}$ zeigen aber, dass es in den drei genannten Ringen solche Elemente gibt.

Der Ring $\mathbb{F}_2[x]/(f)$ mit $f = x^2 + x + \bar{1}$ dagegen ist ein Körper. Denn als Polynomring über einem Körper ist $\mathbb{F}_2[x]$ laut Vorlesung ein Hauptidealring. Jedes irreduzible Element in einem Hauptidealring erzeugt ein maximales Ideal, und der entsprechende Faktorring ist dann ein Körper. Das Element f ist irreduzibel in $\mathbb{F}_2[x]$, denn es ist $\operatorname{grad}(f) = 2$, und wegen $f(\bar{0}) = \bar{1} \neq \bar{0}$ und $f(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$ hat f in $\mathbb{F}_2$ keine Nullstellen. Folglich ist (f) in $\mathbb{F}_2[x]$ ein maximales Ideal, und $\mathbb{F}_2[x]/(f)$ ist ein Körper.

zu (b) Aus Teil (a) folgt, dass $\mathbb{F}_2[x]/(f)$ zu keinem der drei anderen Ringe isomorph ist (denn ein Ring, der isomorph zu einem Körper ist, ist selbst ein Körper).

Der Ring $\mathbb{Z}/4\mathbb{Z}$ ist weder zu $\mathbb{F}_2 \times \mathbb{F}_2$ noch zu $\mathbb{F}_2[x]/(x^2)$ isomorph. Denn wegen $4 \cdot \bar{1} = \bar{0}$ und $2 \cdot \bar{1} = \bar{2} \neq \bar{0}$ in $\mathbb{Z}/4\mathbb{Z}$ ist $\bar{1}$ in der Gruppe $(\mathbb{Z}/4\mathbb{Z}, +)$ ein Element der Ordnung 4, und folglich die Charakteristik von $\mathbb{Z}/4\mathbb{Z}$ gleich 4. Andererseits folgt aus $1_{\mathbb{F}_2 \times \mathbb{F}_2} = (\bar{1}, \bar{1}) \neq 0_{\mathbb{F}_2 \times \mathbb{F}_2}$ und $2 \cdot 1_{\mathbb{F}_2 \times \mathbb{F}_2} = (\bar{2}, \bar{2}) = (\bar{0}, \bar{0})$, dass $\mathbb{F}_2 \times \mathbb{F}_2$ von Charakteristik 2 ist. Auch $\mathbb{F}_2[x]/(x^2)$ ist von Charakteristik 2, denn es gilt $1_{\mathbb{F}_2[x]/(x^2)} = \bar{1} + (x^2) \neq 0_{\mathbb{F}_2[x]/(x^2)}$ und $2 \cdot 1_{\mathbb{F}_2[x]/(x^2)} = \bar{2} + (x^2) = (x^2) = 0_{\mathbb{F}_2[x]/(x^2)}$.

Schließlich sind auch $\mathbb{F}_2[x]/(x^2)$ und $\mathbb{F}_2 \times \mathbb{F}_2$ nicht zueinander isomorph. Denn der Ring $\mathbb{F}_2[x]/(x^2)$ enthält wegen $x + (x^2) \neq 0_{\mathbb{F}_2[x]/(x^2)}$ und $(x + (x^2))^2 = x^2 + (x^2) = (x^2) = 0_{\mathbb{F}_2[x]/(x^2)}$ ein von Null verschiedenes Element, dessen Quadrat gleich Null ist. Wären die beiden Ringe isomorph, dann müsste es auch in $\mathbb{F}_2 \times \mathbb{F}_2$ ein solches Element geben. Aber aus $(a, b)^2 = (\bar{0}, \bar{0})$ folgt für $a, b \in \mathbb{F}_2$ jeweils $(a^2, b^2) = (\bar{0}, \bar{0})$, also $a^2 = b^2 = \bar{0}$, somit $a = b = \bar{0}$ und $(a, b) = (\bar{0}, \bar{0}) = 0_{\mathbb{F}_2 \times \mathbb{F}_2}$. Dies zeigt, dass in $\mathbb{F}_2 \times \mathbb{F}_2$ kein Element ungleich Null existiert, dessen Quadrat gleich Null ist.

Aufgabe H20T1A3

Sei $V = \mathcal{M}_{2,\mathbb{Q}}$ der $\mathbb{Q}$-Vektorraum der 2×2-Matrizen über $\mathbb{Q}$, und sei $\phi : V \to V$ die Linksmultiplikation mit der Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(a) Zeigen Sie, dass ϕ eine $\mathbb{Q}$-lineare Abbildung ist.

(b) Bestimmen Sie das charakteristische Polynom von ϕ.

(c) Bestimmen Sie das Minimalpolynom von ϕ.

Lösung:

zu (a) Sei A die in der Aufgabenstellung angegebene Matrix. Nach Definition der Abbildung ϕ und auf Grund der bekannten Rechenregeln für Matrizen gilt für alle $B, C \in \mathcal{M}_{2,\mathbb{Q}}$ und alle $\lambda \in \mathbb{Q}$ jeweils $\phi(B + C) = A(B + C) = AB + AC = \phi(B) + \phi(C)$ und $\phi(\lambda B) = A(\lambda B) = \lambda(AB) = \lambda\phi(B)$. Damit ist die $\mathbb{Q}$-Linearität von ϕ nachgewiesen.

zu (b) Aus der Linearen Algebra ist bekannt, dass durch $\mathcal{B} = (B_{11}, B_{12}, B_{21}, B_{22})$ mit den Matrizen

$$B_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad , \quad B_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad , \quad B_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad , \quad B_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

eine geordnete Basis von $V = \mathcal{M}_{2,\mathbb{Q}}$ gegeben ist. Die Bilder dieser Basiselemente unter ϕ sind gegeben durch

$$\phi(B_{11}) = AB_{11} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = 0 \cdot B_{11} + 0 \cdot B_{12} + 1 \cdot B_{21} + 0 \cdot B_{22}$$

$$\phi(B_{12}) = AB_{12} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0 \cdot B_{11} + 0 \cdot B_{12} + 0 \cdot B_{21} + 1 \cdot B_{22}$$

$$\phi(B_{21}) = AB_{21} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1 \cdot B_{11} + 0 \cdot B_{12} + 0 \cdot B_{21} + 0 \cdot B_{22}$$

$$\phi(B_{22}) = AB_{22} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0 \cdot B_{11} + 1 \cdot B_{12} + 0 \cdot B_{21} + 0 \cdot B_{22}$$

Jede Gleichung liefert eine Spalte in der Darstellungsmatrix $M = M_{\mathcal{B}}(\phi)$ des Endomorphismus ϕ bezüglich der Basis $\mathcal{B}$. Es ist

$$M = M_{\mathcal{B}}(\phi) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Als charakteristisches Polynom von ϕ erhalten wir (durch Entwicklung der Matrix $xE_4 - M$ zur ersten

Spalte)

$$\chi_\phi \quad = \quad \chi_M \quad = \quad \det(xE_4 - M) \quad = \quad \det \begin{pmatrix} x & 0 & -1 & 0 \\ 0 & x & 0 & -1 \\ -1 & 0 & x & 0 \\ 0 & -1 & 0 & x \end{pmatrix} \quad =$$

$$x \det \begin{pmatrix} x & 0 & -1 \\ 0 & x & 0 \\ -1 & 0 & x \end{pmatrix} + (-1) \det \begin{pmatrix} 0 & -1 & 0 \\ x & 0 & -1 \\ -1 & 0 & x \end{pmatrix} \quad =$$

$$x \cdot (x^3 - x) + (-1) \cdot ((-1) - (-x^2)) \quad = \quad x^4 - 2x^2 + 1 \quad = \quad (x^2 - 1)^2.$$

zu (c) Aus der Linearen Algebra ist bekannt, dass das Minimalpolynom μ_ϕ stets ein Teiler der charakteristischen Polynoms χ_ϕ ist. Darüber hinaus ist μ_ϕ ein normierter Teiler jedes Polynoms $f \in \mathbb{Q}[x]$ mit $f(\phi) = 0$ bzw. $f(M) = 0$. Die Gleichung

$$M^2 - E_4 \quad = \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

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

zeigt, dass μ_ϕ ein Teiler von $x^2 - 1 = (x - 1)(x + 1)$ ist. Die einzigen normierten Teiler dieses Polynoms sind $x^2 - 1$, $x - 1$ und $x + 1$. Wegen $M \neq \pm E_4$ ist weder $M - E_4 = 0$ noch $M + E_4 = 0$, also stimmt μ_ϕ weder mit $x - 1$ noch mit $x + 1$ überein. Somit ist $\mu_\phi = x^2 - 1$ die einzige verbleibende Möglichkeit.

Aufgabe H20T1A4

Sei G eine Gruppe und sei H die Untergruppe von G, die aus allen Produkten von Elementen der Form g^2 mit $g \in G$ besteht.

(a) Bestimmen Sie H im Fall der alternierenden Gruppe $G = A_4$.

(b) Bestimmen Sie H im Fall der symmetrischen Gruppe $G = S_4$.

(c) Zeigen Sie $H \neq G$, falls G eine Untergruppe von Index 2 besitzt.

Lösung:
zu (a) Jeder 3-Zykel $(i\ \ j\ \ k)$ ist in H enthalten, denn es gilt $(i\ \ k\ \ j) \in A_4$ somit $(i\ \ j\ \ k) = (i\ \ k\ \ j)(i\ \ k\ \ j) = (i\ \ k\ \ j)^2 \in H$. Die Gleichungen $(1\ \ 2\ \ 3)(1\ \ 2\ \ 4) = (1\ \ 3)(2\ \ 4)$, $(1\ \ 3\ \ 4)(1\ \ 3\ \ 2) = (1\ \ 4)(2\ \ 3)$ und $(1\ \ 3)(2\ \ 4) \circ (1\ \ 4)(2\ \ 3) = (1\ \ 2)(3\ \ 4)$ zeigen, dass auch die drei Doppeltranspositionen in H enthalten sind. Als Untergruppe von G enthält H auch id, das Neutralelement. Insgesamt ist damit $H = A_4 = G$ nachgewiesen.

zu (b) Für jedes $g \in G$ gilt $\operatorname{sgn}(g) \in \{\pm 1\}$ und somit $\operatorname{sgn}(g^2) = \operatorname{sgn}(g)^2 = 1$. Da H aus Produkten von Elementen dieser Form besteht, haben alle Elemente von H positives Signum, es gilt also $H \subseteq A_4$. Andererseits enthält H insbesondere alle Produkte von Elementen der Form g^2 mit $g \in A_4$, und diese Gruppe stimmt nach Teil (a) mit A_4 überein. Insgesamt gilt also $H = A_4$ auch in diesem Fall.

zu (c) Sei N eine Untergruppe von G vom Index 2. Laut Vorlesung ist N dann ein Normalteiler von G, und somit kann die Faktorgruppe G/N gebildet werden. Für alle $g \in G$ gilt $g^2N = (gN)^2 = N$ und somit $g^2 \in N$, wobei im zweiten Schritt verwendet wurde, dass G/N eine Gruppe der Ordnung $(G : N) = 2$ ist und $gN \in G/N$ somit ein Element der Ordnung 1 oder 2 sein muss. Aus $g^2 \in N$ für alle $g \in G$ folgt $H \subseteq N$, wegen $N \subsetneq G$ also auch $H \subsetneq G$.

Aufgabe H20T1A5

Sei $\omega = \frac{1}{2}(1 - \sqrt{-3})$.

(a) Zeigen Sie, dass ω eine primitive sechste Einheitswurzel ist.

(b) Entscheiden Sie, ob $\mathbb{Q}(\omega, \sqrt[3]{5})$ eine galoissche Körpererweiterung von $\mathbb{Q}(\sqrt[3]{5})$ ist.

(c) Entscheiden Sie, ob $\mathbb{Q}(\omega, \sqrt[6]{2})$ eine galoissche Körpererweiterung von $\mathbb{Q}$ ist.

(d) Finden Sie galoissche Körpererweiterungen $L|K$ und $K|\mathbb{Q}$, so dass $L|\mathbb{Q}$ nicht galoissch ist.
Hinweis: Betrachten Sie $\sqrt[4]{2}$.

Lösung:
zu (a) Zu zeigen ist, dass es sich bei ω um ein Element der Ordnung 6 in der multiplikativen Gruppe $\mathbb{C}^\times$ handelt. Dies ist genau dann der Fall, wenn $\omega^2, \omega^3 \neq 1$ und $\omega^6 = 1$ gilt. Tatsächlich gilt $\omega^2 = \frac{1}{4}(1 - \sqrt{-3})^2 = \frac{1}{4}(1 - 2\sqrt{-3} + (-3)) = -\frac{1}{2} - \frac{1}{2}\sqrt{-3} \neq 1$, $\omega^3 = \omega^2 \cdot \omega = (-\frac{1}{2} - \frac{1}{2}\sqrt{-3})(\frac{1}{2} - \frac{1}{2}\sqrt{-3}) = -\frac{1}{4} - \frac{1}{4}\sqrt{-3} + \frac{1}{4}\sqrt{-3} - \frac{3}{4} = -1$ und $\omega^6 = (\omega^3)^2 = (-1)^2 = 1$.

zu (b) Wir zeigen zunächst, dass $[\mathbb{Q}(\omega, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] = 2$ gilt. Als primitive sechste Einheitswurzel ist ω eine Nullstelle des sechsten Kreisteilungspolynoms $\Phi_6 = x^2 - x + 1$, außerdem ist Φ_6 normiert. Wäre Φ_6 über $\mathbb{Q}(\sqrt[3]{5})$ reduzibel, dann wäre wegen $\operatorname{grad}(\Phi_6) = 2$ die Nullstelle ω des Polynoms in $\mathbb{Q}(\sqrt[3]{5})$ enthalten. Aber dies ist wegen $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$ und $\omega \in \mathbb{C} \setminus \mathbb{R}$ nicht der Fall. Insgesamt ist Φ_6 damit das Minimalpolynom von ω über $\mathbb{Q}(\sqrt[3]{5})$, und wir erhalten

$$[\mathbb{Q}(\omega, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] \quad = \quad [\mathbb{Q}(\sqrt[3]{5})(\omega) : \mathbb{Q}(\sqrt[3]{5})] \quad = \quad \operatorname{grad}(\Phi_6) \quad = \quad 2 \quad ,$$

wie gewünscht. Laut Vorlesung ist jede Körpererweiterung vom Grad 2 normal, insbesondere algebraisch. Wegen $\operatorname{char}(\mathbb{Q}(\sqrt[3]{5})) = 0$ ist jede algebraische Erweiterung von $\mathbb{Q}(\sqrt[3]{5})$ auch separabel. Insgesamt ist $\mathbb{Q}(\omega, \sqrt[3]{5})|\mathbb{Q}(\sqrt[3]{5})$ also tatsächlich eine Galois-Erweiterung.

zu (c) Die Menge der komplexen Nullstellen des Polynoms $f = x^6 - 2$ ist gegeben durch $N = \{\omega^k \sqrt[6]{2} \mid 0 \leq k < 6\}$. Denn für $k \in \{0, ..., 5\}$ gilt jeweils $f(\omega^k \sqrt[6]{2}) = (\omega^k \sqrt[6]{2})^6 - 2 = (\omega^6)^k (\sqrt[6]{2})^6 - 2 = 1^k \cdot 2 - 2 = 0$. Da ω eine primitive sechste Einheitswurzel ist, sind die Elemente $\omega^0, \omega^1, ..., \omega^5$ alle verschieden, wegen $\sqrt[6]{2} \neq 0$ auch die Produkte $\omega^k \sqrt[6]{2}$ mit $0 \leq k < 6$. Da ein Polynom vom Grad 6 über einem Körper nicht mehr als sechs Nullstellen besitzen kann, haben wir damit tatsächlich alle komplexen Nullstellen von f bestimmt.

Somit ist $\mathbb{Q}(N)$ der Zerfällungskörper von f in $\mathbb{C}$ über $\mathbb{Q}$. Laut Vorlesung folgt daraus, dass die Erweiterung $\mathbb{Q}(N)|\mathbb{Q}$ normal ist. Als algebraische Erweiterung ist sie wegen $\operatorname{char}(\mathbb{Q}) = 0$ auch separabel. Insgesamt handelt es sich also bei $\mathbb{Q}(N)|\mathbb{Q}$ um eine Galois-Erweiterung. Schließlich gilt noch $\mathbb{Q}(N) = \mathbb{Q}(\omega, \sqrt[6]{2})$. Die Inklusion „$\subseteq$“ folgt aus der Tatsache, dass mit ω und $\sqrt[6]{2}$ auch $\omega^k \sqrt[6]{2}$ für $0 \leq k < 6$ in $\mathbb{Q}(\omega, \sqrt[6]{2})$ liegt, also $N \subseteq \mathbb{Q}(\omega, \sqrt[6]{2})$ gilt. Für die Inklusion „$\supseteq$“ bemerken wir, dass mit $\sqrt[6]{2}, \omega\sqrt[6]{2} \in N \subseteq \mathbb{Q}(N)$ auch $\omega = \frac{\omega \sqrt[6]{2}}{\sqrt[6]{2}}$ in $\mathbb{Q}(N)$ liegt. Es gilt also $\{\omega, \sqrt[6]{2}\} \subseteq \mathbb{Q}(N)$. Damit ist die Gleichung $\mathbb{Q}(N) = \mathbb{Q}(\omega, \sqrt[6]{2})$ bewiesen, und folglich ist auch $\mathbb{Q}(\omega, \sqrt[6]{2})|\mathbb{Q}$ eine Galois-Erweiterung.

zu (d) Sei $K = \mathbb{Q}(\sqrt[6]{})$ und $L = \mathbb{Q}(\sqrt[4]{2})$. Zunächst zeigen wir, dass $[K : \mathbb{Q}] = [L : \mathbb{Q}] = 2$ gilt. Da laut Vorlesung Erweiterungen vom Grad 2 immer normal sind, folgt daraus, dass $K|\mathbb{Q}$ und $L|K$ normale Erweiterungen sind. Als endliche Erweiterungen sind diese auch algebraisch, und wegen $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(K) = 0$ darüber hinaus separabel. Insgesamt handelt es sich damit also um Galois-Erweiterungen.

Zum Nachweis der angegebenen Erweiterungsgrade sei $f = x^2 - 2$ und $g = x^4 - 2$. Beide Polynome sind normiert und außerdem irreduzibel über $\mathbb{Z}$, auf Grund des Eisenstein-Kriteriums angewendet auf die Primzahl $p = 2$. Nach dem Gauß'schen Lemma sind sie somit auch irreduzibel über $\mathbb{Q}$. Wegen $f(\sqrt{2}) = 0$ ist f insgesamt das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$, und es folgt $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \text{grad}(f) = 2$. Wegen $g(\sqrt[4]{2}) = 0$ ist g das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$, und es folgt $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \text{grad}(g) = 4$. Wegen $\sqrt{2} = (\sqrt[4]{2})^2 \in L$ ist $K = \mathbb{Q}(\sqrt{2})$ ein Zwischenkörper von $L|\mathbb{Q}$. Auf Grund der Gradformel gilt somit $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$, und wir erhalten $[L : K] = \frac{[L:\mathbb{Q}]}{[K:\mathbb{Q}]} = \frac{4}{2} = 2$.

Nun zeigen wir noch, dass die Erweiterung $L|\mathbb{Q}$ nicht normal ist, und somit erst recht eine galois'sche Erweiterung. Wäre sie normal, dann müsste jedes Polynom, das über $\mathbb{Q}$ irreduzibel ist und in L eine Nullstelle besitzt, über L bereits in Linearfaktoren zerfallen. Wie oben gezeigt, ist das Polynom $g = x^4 - 2$ irreduzibel über $\mathbb{Q}$, und es besitzt in L die Nullstelle $\sqrt[4]{2}$. Würde es über L in Linearfaktoren zerfallen, dann müssten sämtliche komplexen Nullstellen von g bereits in L liegen, insbesondere auch die Nullstelle $i\sqrt[4]{2}$. Aber dies ist nicht der Fall, denn einerseits gilt $L = \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ wegen $\sqrt[4]{2} \in \mathbb{R}$, andererseits aber $i\sqrt[4]{2} \notin \mathbb{R}$.

Aufgabe H20T2A1

(a) Bestimmen Sie das $a \in \{0, 1, ..., 6\}$ mit $3^{2020} \equiv a \bmod 7$.
Hinweis: Benutzen Sie den kleinen Satz von Fermat.

(b) Zeigen Sie, dass die Diedergruppe $D_4 = \{\sigma^k \delta^\ell \mid k \in \{0, 1\}, \ell \in \{0, 1, 2, 3\}\}$ mit 8 Elementen (es gilt $\sigma^2 = e = \delta^4$ und $\sigma\delta\sigma^{-1} = \delta^{-1}$) nicht isomorph zur Quaternionengruppe $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ (es gilt $i^2 = j^2 = k^2 = ijk = -1$) ist.

(c) Bestimmen Sie eine zu $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2,\mathbb{R}}$ ähnliche Diagonalmatrix D sowie eine invertierbare Matrix S mit $D = S^{-1}AS$.

(d) Bestimmen Sie alle erzeugenden Elemente der Einheitengruppe $(\mathbb{Z}/11\mathbb{Z})^\times$.

Lösung:
zu (a) Die Gruppe $(\mathbb{Z}/7\mathbb{Z})^\times$ hat $\varphi(7) = 6$ Elemente, und $\bar{3} = 3 + 7\mathbb{Z}$ ist wegen $\mathrm{ggT}(3, 7) = 1$ in dieser Gruppe enthalten. Auf Grund des kleinen Satzes von Fermat folgt $\bar{3}^6 = 1$. Wegen $2020 \equiv 220 \equiv 40 \equiv 4 \bmod 6$ gibt es ein $n \in \mathbb{Z}$ mit $2020 = 6n+4$. Es gilt also $\bar{3}^{2020} = \bar{3}^{6n+4} = (\bar{3}^6)^n \cdot \bar{3}^4 = \bar{1}^n \cdot \bar{3}^4 = \overline{81} = \overline{11} = \bar{4}$ in $(\mathbb{Z}/7\mathbb{Z})^\times$. Daraus wiederum folgt $3^{2020} \equiv 4 \bmod 7$.

zu (b) Wären die beiden Gruppen isomorph, dann müsste es in beiden Gruppen gleich viele Elemente der Ordnung 2 geben. Für $\alpha \in \{\pm i, \pm j, \pm k\}$ gilt jeweils $\alpha^2 = -1 \neq 1$. Diese Elemente sind also nicht von Ordnung 2. Die einzigen verbleibenden Elemente sind ± 1. Das Neutralelement 1 hat die Ordnung 1; wegen $-1 \neq 1$ und $(-1)^2 = 1$ ist -1 also das einzige Element der Ordnung 2 in Q. Andererseits ist bekannt, dass für jedes $n \in \mathbb{N}$ mit $n \geq 3$ die $2n$-elementige Diedergruppe mindestens n Elemente der Ordnung 2 besitzt (die „Spiegelungen“). Daraus folgt, dass in D_4 mindestens vier Elemente der Ordnung 2 existieren. Somit kann D_4 nicht zu Q isomorph sein. (Tatsächlich gibt es in D_4 noch ein fünftes Element der Ordnung 2, die 180°-Drehung δ^2.)

zu (c) Das charakteristische Polynom von A ist gegeben durch

$$\begin{aligned} \chi_A &= \det(xE - A) = \det \begin{pmatrix} x-1 & 2 \\ 2 & x-1 \end{pmatrix} = (x-1)^2 - 4 \\ &= (x^2 - 2x + 1) - 4 = x^2 - 2x - 3. \end{aligned}$$

wobei $E \in \mathcal{M}_{2,\mathbb{R}}$ die Einheitsmatrix bezeichnet. Mit Hilfe der p-q-Formel findet man die Nullstellen -1 und 3. Also sind dies die beiden Eigenwerte von A, und foglich ist

$$D = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix}$$

eine zu A ähnliche Diagonalmatrix. Durch die Rechnung

$$A + E = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

findet man den Eigenvektor $(1, -1)$ zum Eigenwert -1. Genauso erhält man durch

$$A - 3E = \begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$$

den Eigenvektor $(1,1)$ zum Eigenwert 1. Trägt man die beiden Eigenvektoren als Spalten in eine Matrix

$$S \quad = \quad \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

ein, so erhält man eine Matrix mit $D = S^{-1}AS$. Tatsächlich gilt

$$S^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \text{ und } S^{-1}AS = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 & 3 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix} = D.$$

zu (d) Da $p = 11$ eine Primzahl ist, handelt es sich laut Vorlesung bei $(\mathbb{Z}/11\mathbb{Z})^\times$ um eine zyklische Gruppe der Ordnung $11-1 = 10$. Die einzigen Primteiler von 10 sind 2 und 5. Nach einem Kriterium aus der Vorlesung ist $\bar{2}$ wegen $\bar{2}^{10/2} = \bar{2}^5 = \overline{32} = \overline{10} \neq \bar{1}$ und $\bar{2}^{10/5} = \bar{2}^2 = \bar{4} \neq \bar{1}$ ein Element der Ordnung 10, also ein erzeugendes Element der Gruppe. Allgemein gilt: Ist $n \in \mathbb{N}$, G eine zyklische Gruppe der Ordnung n und $g \in G$ ein erzeugendes Element, dann besitzt G genau $\varphi(n)$ erzeugende Elemente (wobei φ die Eulersche φ-Funktion bezeichnet), und diese sind gegeben durch g^k mit $0 \leq k < n$ und $\mathrm{ggT}(k,n) = 1$. Wegen $\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4$ besitzt $(\mathbb{Z}/11\mathbb{Z})^\times$ also insgesamt vier erzeugende Elemente, und diese sind gegeben durch $\bar{2}^1 = \bar{2}$, $\bar{2}^3 = \bar{8}$, $\bar{2}^7 = \overline{128} = \bar{7}$ und $\bar{2}^9 = \overline{512} = \overline{72} = \bar{6}$ (denn 1, 3, 7 und 9 sind genau die zu 10 teilerfremden ganzen Zahlen k mit $0 \leq k < 10$).

Aufgabe H20T2A2

Sei G eine Gruppe, die auf einer Menge S operiert. Dann heißt die Operation transitiv, falls es zu jedem Paar von Elementen $s, s' \in S$ ein $g \in G$ mit $gs = s'$ gibt. Zeigen Sie:

(a) Die übliche Operation von $\mathrm{GL}_2(\mathbb{R})$ auf $\mathbb{R}^2 \setminus \{0\}$ ist transitiv.
Hinweis: Betrachten Sie die Bahn von $v = (1, 0)$.

(b) Sei G eine endliche Gruppe mit $|G| \geq 3$. Dann ist die Operation von G auf $G \setminus \{e\}$ nicht transitiv.

Lösung:
zu (a) Laut Vorlesung ist die Operation einer Gruppe G auf einer Menge S genau dann transitiv, wenn ein Element $s \in S$ existiert, dessen Bahn $G(s)$ mit S übereinstimmt. Setzen wir $G = \mathrm{GL}_2(\mathbb{R})$ und $S = \mathbb{R}^2 \setminus \{0\}$, so genügt es also zu zeigen, dass für $v = (1, 0) \in S$ die Gleichung $G(v) = S$ erfüllt ist. Die Inklusion „$\subseteq$“ ist offensichtlich erfüllt, da jede Bahn einer Operation von G auf S in S enthalten ist. Zum Beweis der Inklusion „$\supseteq$“ sei $w = (a, b) \in S$ vorgegeben. Wegen $w \neq (0, 0)$ gilt $a \neq 0$ oder $b \neq 0$. Im ersten Fall ist die Matrix

$$A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

wegen $\det(A) = a \neq 0$ ein Element von G mit

$$Av \quad = \quad \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad = \quad \begin{pmatrix} a \\ b \end{pmatrix} \quad = \quad w.$$

Im zweiten Fall setzen wir

$$A = \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}.$$

Auch diese Matrix ist wegen $\det(A) = -b \neq 0$ ein Element von G, und es gilt

$$Av \quad = \quad \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad = \quad \begin{pmatrix} a \\ b \end{pmatrix} \quad = \quad w.$$

In beiden Fällen ist w also in der Bahn $G(v)$ enthalten.

zu (b) Nehmen wir an, dass G auf $G \setminus \{e\}$ transitiv operiert, und sei $h \in G \setminus \{e\}$ ein beliebiges Element. Auf Grund der Transitivität ist die Bahn von h dann durch $G(h) = G \setminus \{e\}$ gegeben. Bezeichnet G_h den Stabilisator von h, dann gilt auf Grund der Beziehung zwischen Bahnlänge und Stabilisator $\frac{|G|}{|G_h|} = (G : G_h) = |G(h)| = |G \setminus \{e\}| = |G| - 1$. Setzen wir $n = |G|$, dann zeigt die Gleichung, dass $n - 1$ ein Teiler von n ist. Es gibt also ein $d \in \mathbb{N}$ mit $d(n - 1) = n$. Aber die Umformung zeigt, dass dann $d = \frac{n}{n-1} = 1 + \frac{1}{n-1}$ eine ganze Zahl sein müsste, was nur für $n = 2$ der Fall ist. Dies steht im Widerspruch zur Voraussetzung $n = |G| \geq 3$.

Aufgabe H20T2A3

Sei p eine Primzahl, $n \in \mathbb{N}$ und $f \in \mathbb{F}_p[x]$ irreduzibel vom Grad n. Man bestimmen diejenigen $m \in \mathbb{N}$, für die f über $\mathbb{F}_{p^m}$ in Linearfaktoren zerfällt.

Lösung:
Sei $m \in \mathbb{N}$. Wir zeigen, dass f genau dann über $\mathbb{F}_{p^m}$ in Linearfaktoren zerfällt, wenn m ein Vielfaches von n ist. Mit $\mathbb{F}_p^{\text{alg}}$ bezeichnen wir einen algebraischen Abschluss von $\mathbb{F}_{p^m}$ (der zugleich ein algebraischer Abschluss des Primkörpers $\mathbb{F}_p$ von $\mathbb{F}_{p^m}$ ist).

„$\Rightarrow$“ Wenn f über $\mathbb{F}_{p^m}$ in Linearfaktoren zerfällt, dann besitzt f insbesondere eine Nullstelle $\alpha \in \mathbb{F}_{p^m}$. Da f in $\mathbb{F}_p[x]$ irreduzibel vom Grad n ist, stimmt f bis auf eine Konstante ungleich null mit dem Minimalpolynom von α über $\mathbb{F}_p$ überein, und es gilt $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \text{grad}(f) = n$. Als n-dimensionaler $\mathbb{F}_p$-Vektorraum besteht der Körper $\mathbb{F}_p(\alpha)$ aus p^n Elementen; er stimmt also mit dem eindeutig bestimmten p^n-elementigen Zwischenkörper $\mathbb{F}_{p^n}$ von $\mathbb{F}_p^{\text{alg}}|\mathbb{F}_p$ überein. Aus $\alpha \in \mathbb{F}_{p^m}$ folgt, dass $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ ein Teilkörper von $\mathbb{F}_{p^m}$ ist. Dies ist laut Vorlesung genau dann der Fall, wenn m ein Vielfaches von n ist.

„$\Leftarrow$“ Hier setzen wir voraus, dass $m = dn$ für ein $d \in \mathbb{N}$ gilt. Zu zeigen ist, dass f über $\mathbb{F}_{p^m}$ in Linearfaktoren zerfällt. Sei α eine Nullstelle von f in $\mathbb{F}_p^{\text{alg}}$. Wie im Beweis von „$\Rightarrow$“ zeigt man, dass $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$ gilt. Insbesondere ist α in $\mathbb{F}_{p^n}$ enthalten. Da n ein Teiler von m ist, gilt $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$; es gilt somit auch $\alpha \in \mathbb{F}_{p^m}$. Aus der Vorlesung ist bekannt: Ist $E|F$ eine Erweiterung bestehend aus endlichen Körpern F und E, dann ist $E|F$ normal. Also ist auch $\mathbb{F}_{p^m}|\mathbb{F}_p$ eine normale Erweiterung. Dies bedeutet, dass jedes über $\mathbb{F}_p$ irreduzible Polynom, das in $\mathbb{F}_{p^m}$ eine Nullstelle besitzt, über $\mathbb{F}_{p^m}$ in Linearfaktoren zerfällt. Das Polynom f ist laut Voraussetzung irreduzibel, und α ist eine Nullstelle dieses Polynoms in $\mathbb{F}_{p^m}$. Also zerfällt f über $\mathbb{F}_{p^m}$ in Linearfaktoren.

Aufgabe H20T2A4

Sei k ein Körper und $G = \langle g \rangle$ eine von g erzeugte zyklische Gruppe der Ordnung $n \geq 2$. Der Gruppenring kG ist die Menge aller Summen $\sum_{i=0}^{n-1} \alpha_i g^i$ ($\alpha_i \in K$). Fakt: Die Menge kG ist bezüglich der Operationen

$$\left(\sum_{i=0}^{n-1} \alpha_i g^i\right) + \left(\sum_{i=0}^{n-1} \beta_i g^i\right) \quad = \quad \sum_{i=0}^{n-1} (\alpha_i + \beta_i) g^i$$

$$\left(\sum_{i=0}^{n-1} \alpha_i g^i\right) \cdot \left(\sum_{i=0}^{n-1} \beta_i g^i\right) \quad = \quad \sum_{k=0}^{n-1} \gamma_k g^k \quad , \quad \gamma_k = \sum_{i+j \equiv k \bmod n} \alpha_i \beta_j$$

ein assoziativer, kommutativer Ring mit Einselement $1_{kG} = 1_k \cdot 1_G$. Zeigen Sie:

(a) Es gibt einen surjektiven Ringhomomorphismus $\phi : k[x] \to kG$.

(b) $kG \cong k[x]/(x^n - 1_k)$

(c) kG ist kein Integritätsbereich

Lösung:

zu (a) Allgemein gilt: Ist $\phi_0 : R \to S$ ein Ringhomomorphismus und $s \in S$, dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\phi : R[x] \to S$ mit $\phi|_R = \phi_0$ und $\phi(x) = s$. Die Abbildung $\phi_0 : k \to kG$ gegeben durch $\phi_0(c) = c \cdot 1_G$ für alle $c \in k$ ist ein Ringhomomorphismus, denn es gilt $\phi_0(1_k) = 1_k \cdot 1_G = 1_{kG}$, $\phi_0(c+d) = (c+d) \cdot 1_G = c \cdot 1_G + d \cdot 1_G = \phi_0(c) + \phi_0(d)$ und $\phi_0(cd) = (cd) \cdot 1_G = (c \cdot 1_G) \cdot (d \cdot 1_G) = \phi_0(c) \cdot \phi_0(d)$ für alle $c, d \in k$.

Also existiert ein eindeutig bestimmter Ringhomomorphismus $\phi : k[x] \to kG$ mit $\phi|_k = \phi_0$ und $\phi(x) = 1_k \cdot g^1$. Zu zeigen bleibt, dass ϕ surjektiv ist. Wir zeigen zunächst durch vollständige Induktion, dass $(1_k \cdot g^1)^i = 1_k \cdot g^i$ für $0 \leq i \leq n-1$ gilt. Für $i = 0$ ist die Gleichung erfüllt, denn es gilt $(1_k \cdot g^1)^0 = 1_{kG} = 1_k \cdot 1_G = 1_k \cdot g^0$. Setzen wir nun die Gleichung für ein $i \in \{0, ..., n-2\}$ voraus. Es sei $\alpha_i = \beta_1 = 1_k$ und $\alpha_j = 0_k$ für alle $j \in \{0, ..., n-1\} \setminus \{i\}$, $\beta_j = 0$ für $j = 0$ und $2 \leq j \leq n-1$. Definieren wir $\gamma_\ell = \sum_{u+v \equiv \ell \bmod n} \alpha_u \beta_v$ für $0 \leq \ell \leq n-1$, dann ist $\alpha_u \beta_v \neq 0_k$ nur für das Paar $(u, v) = (i, 1)$. Daraus folgt $\gamma_{i+1} = \alpha_i \beta_1 = 1_k$ und $\gamma_\ell = 0_k$ für $\ell \in \{0, ..., n-1\} \setminus \{i+1\}$, und wir erhalten

$$(1_k \cdot g^1)^{i+1} \quad = \quad (1_k \cdot g^1)^i \cdot (1_k \cdot g^1) \quad = \quad \left(\sum_{u=0}^{n-1} \alpha_u g^u\right) \left(\sum_{v=0}^{n-1} \beta_v g^v\right) \quad = \quad \sum_{\ell=0}^{n-1} \gamma_\ell g^\ell \quad = \quad 1_k \cdot g^{i+1}.$$

Zum Nachweis der Surjektivität von ϕ sei nun $\gamma = \sum_{i=0}^{n-1} \alpha_i g^i$ ein beliebig vorgegebenes Element, mit $\alpha_0, ..., \alpha_{n-1} \in k$. Setzen wir $f = \sum_{i=0}^{n-1} \alpha_i x^i$, dann gilt

$$\phi(f) \quad = \quad \phi\left(\sum_{i=0}^{n-1} \alpha_i x^i\right) \quad = \quad \sum_{i=0}^{n-1} \phi(\alpha_i) \cdot \phi(x)^i \quad = \quad \sum_{i=0}^{n-1} \phi_0(\alpha_i) \cdot (1_k \cdot g)^i \quad =$$

$$\sum_{i=0}^{n-1} (\alpha_i \cdot 1_G) \cdot (1_k \cdot g)^i \quad = \quad \sum_{i=0}^{n-1} \alpha_i g^i \quad = \quad \gamma.$$

Damit ist die Surjektivität von ϕ nachgewiesen.

zu (b) In Teil (a) haben wir einen surjektiven Ringhomomorphismus $\phi : k[x] \to kG$ definiert. Wenn außerdem $\ker(\phi) = (x^n - 1_k)$, dann induziert ϕ nach dem Homomorphiesatz für Ringe einen Isomorphismus $k[x]/(x^n - 1_k) \cong k_G$. Zum Nachweis der Inklusion „$\supseteq$“ beweisen wir zunächst die Gleichung $(1_k \cdot g)^n = 1_{kG}$. Bereits gezeigt wurde die Gleichung $(1_k \cdot g)^{n-1} = 1_k \cdot g^{n-1}$. Wir definieren nun $\alpha_i = 0_k$ für $0 \leq i \leq n-2$, $\alpha_{n-1} = 1_k$, $\beta_1 = 1_k$ und $\beta_j = 0_k$ für alle $j \in \{0, ..., n-1\} \setminus \{1\}$, und $\gamma_\ell = \sum_{u+v \equiv \ell \bmod n} \alpha_u \beta_v$

für $0 \leq \ell \leq n-1$. Das einzige Paar (u,v) mit $\alpha_u \beta_v \neq 0_k$ ist dann $(n-1,1)$, und es gilt $(n-1)+1 \equiv 0 \bmod n$. Daraus folgt $\gamma_0 = \alpha_{n-1}\beta_1 = 1_k$ und $\gamma_\ell = 0_k$ für $1 \leq \ell \leq n-1$. Wir erhalten

$$\begin{aligned}(1_k \cdot g^1)^n &= (1_k \cdot g^1)^{n-1} \cdot (1_k \cdot g^1) = \left(\sum_{u=0}^{n-1} \alpha_u g^u\right)\left(\sum_{v=0}^{n-1} \beta_v g^v\right) = \sum_{\ell=0}^{n-1} \gamma_\ell g^\ell = \\ 1_k \cdot g^0 &= 1_k \cdot 1_G = 1_{kG}.\end{aligned}$$

Wegen $\phi(x^n - 1_k) = \phi(x)^n - \phi(1_k) = (1_k \cdot g)^n - 1_{kG} = 1_{kG} - 1_{kG} = 0_{kG}$ ist $x^n - 1_k$ im Kern von ϕ enthalten, und weil $\ker(\phi)$ ein Ideal in $k[x]$ ist, gilt $(x^n - 1_k) \subseteq \ker(\phi)$. Zum Nachweis der Inklusion „$\subseteq$“ sei nun umgekehrt $f \in \ker(\phi)$. Durch Division von f durch $x^n - 1_k$ mit Rest erhalten wir Polynome $q, r \in k[x]$ mit $f = q \cdot (x^n - 1_k) + r$, wobei $r = 0_k$ oder $\operatorname{grad}(r) < n$ gilt. Schreiben wir $r = \sum_{\ell=0}^{n-1} a_\ell x^\ell$ mit $a_0, a_1, ..., a_{n-1} \in k$, dann folgt

$$\begin{aligned}0_{kG} = \phi(f) &= \phi(q(x^n - 1_k) + r) = \phi(q) \cdot \phi(x^n - 1_k) + \phi(r) = \\ &\phi(q) \cdot 0_{kG} + \phi\left(\sum_{\ell=0}^{n-1} a_\ell x^\ell\right) = \sum_{\ell=0}^{n-1} a_\ell g^\ell.\end{aligned}$$

Daraus folgt $a_\ell = 0_k$ für $0 \leq \ell < n$, was wiederum $r = 0_k$ zur Folge hat. Es gilt also $f = q \cdot (x^n - 1_k)$. Dies zeigt, dass f im Hauptideal $(x^n - 1_k)$ enthalten ist, womit der Nachweis der Inklusion abgeschlossen ist.

zu (c) Im Faktorring $k[x]/(x^n - 1_k)$ sind die Elemente $x - 1_k + (x^n - 1_k)$ und $\sum_{\ell=0}^{n-1} x^\ell + (x^n - 1_k)$ ungleich null, denn die Polynome $x - 1_k$ und $\sum_{\ell=0}^{n-1} x^\ell$ sind auf Grund ihrer Grade keine Vielfachen von $x^n - 1_k$. Andererseits gilt

$$\begin{aligned}(x - 1_k + (x^n - 1_k)) \cdot \left(\sum_{\ell=0}^{n-1} x^\ell + (x^n - 1_k)\right) &= (x - 1_k)\left(\sum_{\ell=0}^{n-1} x^\ell\right) + (x^n - 1_k) \\ = x^n - 1_k + (x^n - 1_k) &= 0_{k[x]/(x^n - 1_k)}.\end{aligned}$$

Dies zeigt, dass $k[x]/(x^n - 1_k)$ kein Integritätsbereich ist. Wegen $k[x]/(x^n - 1_k) \cong kG$ ist auch kG kein Integritätsbereich.

Aufgabe H20T2A5

Sei K ein Körper der Charakteristik 0 und sei p eine Primzahl. Angenommen, p teilt den Grad jeder endlichen Körpererweiterung $L|K$ mit $K \subsetneq L$. Zeigen Sie, dass dann der Grad jeder endlichen Körpererweiterung von K eine Potenz von p ist.
Hinweis: Zeigen Sie, dass es eine endliche Galoiserweiterung $E|K$ mit $K \subseteq L \subseteq E$ gibt, und verwenden Sie die Sylowsätze.

Lösung:
Sei $L|K$ eine endliche Körpererweiterung, und nehmen wir an, dass $[L : K]$ keine p-Potenz ist. Dann existiert eine von p verschiedene Primzahl q, die $[L : K]$ teilt. Wegen $\mathrm{char}(K) = 0$ ist $L|K$ separabel. Somit kann der Satz vom primitiven Element angewendet werden, und demnach existiert ein Element $\gamma \in L$ mit $L = K(\gamma)$. Sei $f \in K[x]$ das Minimalpolynom von γ über K, L^{alg} ein algebraischer Abschluss von L und M der Zerfällungskörper von f über K, der durch Adjunktion aller Nullstellen von f in L^{alg} an K existiert. Weil γ eine Nullstelle von f in $L \subseteq L^{\mathrm{alg}}$ ist, gilt $\gamma \in M$ und $L = K(\gamma) \subseteq M$.

Als Zerfällungskörper eines Polynoms $f \in K[x]$ über K ist $M|K$ eine normale Erweiterung. Wegen $\mathrm{char}(K) = 0$ ist diese Erweiterung auch separabel, insgesamt also eine Galois-Erweiterung. Sei $G = \mathrm{Gal}(M|K)$ die zugehörige Galois-Gruppe. Dann gilt $|G| = [M : K]$. Da L ein Zwischenkörper von $M|K$ ist, liefert die Gradformel die Gleichung $[M : K] = [M : L] \cdot [L : K]$. Da die Primzahl q ein Teiler von $[L : K]$ ist, ist sie auch ein Teiler von $[M : K]$ und $|G|$. Schreiben wir $|G| = p^r \cdot m$ mit $r \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $p \nmid m$, dann ist q ein Teiler von m.

Sei nun P eine p-Sylowgruppe von G und $L_1 = M^P$ der zugehörige Fixkörper. Auf Grund der Ergänzungen zum Hauptsatz der Galoistheorie gilt dann $[L_1 : K] = (G : P) = \frac{n}{p^r} = m$. Wegen $q \mid m$ gilt $[L_1 : K] > 1$; es handelt sich bei $L_1|K$ also um eine endliche Körpererweiterung mit $L_1 \supsetneq K$. Aber der Grad $[L_1 : K] = m$ wird von p nicht geteilt, im Widerspruch zu den Voraussetzungen. Unsere Annahme, dass $[L : K]$ keine p-Potenz ist, war also falsch.

Aufgabe H20T3A1

Es sei $f = x^4 + ax + 2 \in \mathbb{Z}[x]$.

(a) Bestimmen Sie alle $a \in \mathbb{Z}$, für die f eine rationale Nullstelle besitzt.

(b) Zeigen Sie, dass f für kein $a \in \mathbb{Z}$ in zwei quadratische Faktoren aus $\mathbb{Z}[x]$ zerfällt.

(c) Beweisen Sie: Der Restklassenring $\mathbb{Q}[x]/(f)$ ist, abhängig von a, entweder ein Körper oder isomorph zu einem direkten Produkt $K_1 \times K_2$ von zwei Körpern, die die Grade 1 bzw. 3 über $\mathbb{Q}$ haben und geben Sie an, für welche Werte von a die jeweiligen Fälle eintreten.

Lösung:

zu (a) Da es sich bei f ein um normiertes, ganzzahliges Polynom handelt, ist jede rationale Nullstelle ganzzahlig und ein Teiler des konstanten Terms. Die einzigen möglichen Nullstellen sind also $\pm 1, \pm 2$. Es gilt $f(1) = 3 + a$, $f(-1) = 3 - a$, $f(2) = 18 + 2a$, $f(-2) = 18 - 2a$. Außerdem gelten die Äquivalenzen $3 + a = 0 \Leftrightarrow a = -3$, $3 - a = 0 \Leftrightarrow a = 3$, $18 + 2a = 0 \Leftrightarrow a = -9$, $18 - 2a = 0 \Leftrightarrow a = 9$. Das Polynom f besitzt also genau dann eine rationale Nullstelle, wenn $a \in \{\pm 3, \pm 9\}$ gilt, und diese rationale Nullstelle ist dann auch ganzzahlig.

zu (b) Nehmen wir an, dass f ein Produkt zweier Faktoren $g, h \in \mathbb{Z}[x]$ ist. Weil f normiert ist, ist das Produkt der Leitkoeffizienten von g und h gleich 1. Daraus folgt, dass entweder beide Leitkoeffizienten gleich 1 oder beide gleich -1 sind. Nach eventueller Ersetzung von g und h durch $-g$ bzw. $-h$ können wir davon ausgehen, dass g und h beide normiert sind. Es gibt also $b, c, r, s \in \mathbb{Z}$ mit $g = x^2 + bx + r$ und $h = x^2 + cx + s$. Wir erhalten

$$x^4 + ax + 2 \quad = \quad f \quad = \quad gh \quad = \quad (x^2 + bx + r)(x^2 + cx + s) \quad = \\ x^4 + (b + c)x^3 + (r + s + bc)x^2 + (bs + cr)x + rs.$$

Koeffizientenvergleich liefert $b + c = r + s + bc = 0$, $bs + cr = a$ und $rs = 2$. Einsetzen von $c = -b$ in die letzten drei Gleichungen liefert $r + s = c^2$, $b(s - r) = a$ und $rs = 2$. Auf Grund der Gleichung $rs = 2$ gibt es für das Paar (r, s) nur die vier Möglichkeiten $(1, 2)$, $(2, 1)$, $(-1, -2)$ und $(-2, -1)$. Die Summe $r + s$ ist in diesen vier Fällen entweder 3 oder -3. Da aber beides keine Quadrate in $\mathbb{Z}$ sind, kann die Gleichung $r + s = c^2$ nicht gelten. Dies zeigt, dass keine Zerlegung von f in der angegebenen Form existiert.

zu (c) Betrachten wir zunächst den Fall $a \notin \{\pm 3, \pm 9\}$. Nach Teil (a) besitzt das Polynom f in diesem Fall keine rationale Nullstelle. Ist f das Polynom dennoch reduzibel in $\mathbb{Q}[x]$, dann ist es nach dem Gauß'schen Lemma auch reduzibel in $\mathbb{Z}[x]$. Es gibt also in $\mathbb{Z}[x]$ eine Zerlegung von f in zwei Nicht-Einheiten g, h. Da f normiert und somit insbesondere primitiv ist, ist keines der Polynome g, h eine Konstante. Da f keine rationale Nullstelle besitzt, muss es sich bei g und h um Polynome vom Grad 2 handeln. Aber in Teil (b) wurde gezeigt, dass eine solche Zerlegung nicht existiert.

Also ist f über $\mathbb{Q}$ irreduzibel. Als Polynomring über einem Körper ist $\mathbb{Q}[x]$ ein Hauptidealring. Daraus folgt, dass jedes Hauptideal, das von einem irreduziblen Element erzeugt wird, maximal ist. Also ist (f) ein maximales Ideal in $\mathbb{Q}[x]$, und folglich ist $\mathbb{Q}[x]/(f)$ ein Körper.

Betrachten wir nun den Fall $a \in \{\pm 3, \pm 9\}$. Wie in Teil (a) gezeigt, besitzt f dann eine Nullstelle $r \in \mathbb{Z}$. Es gibt also ein Polynom $g \in \mathbb{Q}[x]$ mit $\text{grad}(g) = 3$ und $f = (x - r)g$. Nehmen wir an, dass f, eventuell mit Vielfachheiten, mindestens zwei rationale Nullstellen besitzt. Nach Teil (a) müssten diese Nullstellen r, s dann beide ganzzahlig sein. Es wäre dann $(x - r)(x - s)$ ein Teiler von f in $\mathbb{Z}[x]$; das Polynom würde also

in zwei Faktoren vom Grad 2 zerfallen. Aber dies wurde in Teil (b) ausgeschlossen. Folglich besitzt f mit Vielfachheiten genau eine rationale Nullstelle, und g besitzt keine rationale Nullstelle. Wegen $\operatorname{grad}(g) = 3$ folgt daraus, dass g in $\mathbb{Q}[x]$ irreduzibel ist. Als Polynom vom Grad 1 ist $x - r$ ebenfalls irreduzibel.

Als voneinander verschiedene, normierte irreduzible Polynome sind $x-r$ und g teilerfremd. Folglich sind auch die Hauptideale $(x-r)$ und (g) in $\mathbb{Q}[x]$ teilerfremd. Durch Anwendung des Chinesischen Restsatzes erhalten wir einen Isomorphismus $\mathbb{Q}[x]/(f) \cong \mathbb{Q}[x]/(x-r) \times \mathbb{Q}[x]/(g)$. Da $x-r$ und g irreduzibel sind, sind (wie bereits oben bemerkt) die Hauptideale $(x - r)$ und (g) maximal, und die Faktorringe $\mathbb{Q}[x]/(x - r)$ und $\mathbb{Q}[x]/(g)$ sind Körper. Also ist $\mathbb{Q}[x]/(f)$ isomorph zu einem direkten Produkt zweier Körper. Aus der Vorlesung ist bekannt: Ist $h \in \mathbb{Q}[x]$ irreduzibel und $\alpha \in \mathbb{C}$ eine Nullstelle von h, dann ist $\mathbb{Q}(\alpha)$ zum Faktorring $\mathbb{Q}[x]/(h)$ isomorph. Das Polynom h stimmt bis auf eine Konstante ungleich null mit dem Minimalpolynom von α über $\mathbb{Q}$ überein. Daraus folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \operatorname{grad}(h)$, und folglich ist auch $\mathbb{Q}[x]/(h)$ ein Erweiterungskörper vom Grad $\operatorname{grad}(h)$ über $\mathbb{Q}$. Insbesondere sind also $\mathbb{Q}[x]/(x - r)$ und $\mathbb{Q}[x]/(g)$ Erweiterungen von $\mathbb{Q}$ vom Grad 1 bzw. 3.

Aufgabe H20T3A2

Es sei U eine Untergruppe einer endlichen einfachen Gruppe G vom Index $n = (G : U) \geq 3$.

(a) Zeigen Sie, dass G isomorph zu einer Untergruppe der S_n ist.
Hinweis: Betrachten Sie eine geeignete Operation von G.

(b) Zeigen Sie, dass $|G|$ ein Teiler von $\frac{1}{2}n!$ ist.

(c) Begründen Sie, ob die alternierende Gruppe A_5 eine Untergruppe der Ordnung 15 besitzt.

Lösung:
zu (a) Wir betrachten die Operation $*$ von G auf der Menge G/U der Linksnebenklassen von U gegeben durch $g * (hU) = (gh)U$ für alle $g, h \in G$. Laut Vorlesung existiert ein Homomorphismus $\phi : G \to \mathrm{Per}(G/U)$ gegeben durch $\phi(g)(hU) = g * (hU) = (gh)U$ für alle $g, h \in G$. Als Kern eines Gruppenhomomorphismus ist $N = \ker(\phi)$ ein Normalteiler von G. Da G laut Angabe einfach ist, sind nur die beiden Fälle $N = \{e\}$ und $N = G$ möglich. Betrachten wir zunächst den Fall $N = G$. Dann gilt $\phi(g) = \mathrm{id}_{G/U}$ für alle $g \in G$. Wegen $(G : U) \geq 3$ gibt es in G/U insbesondere zwei verschiedene Elemente h_1U und h_2U, mit $h_1, h_2 \in G$, und es ist $(h_2h_1^{-1}) * (h_1U) = (h_2h_1^{-1}h_1)U = h_2U$. Aus $\phi(h_2h_1^{-1}) = \mathrm{id}_{G/U}$ folgt aber andererseits $(h_2h_1^{-1}) * (h_1U) = \phi(h_2h_1^{-1})(h_1U) = \mathrm{id}_{G/U}(h_1U) = h_1U \neq h_2U$. Der Widerspruch zeigt, dass die Annahme $N = G$ falsch war.

Also muss $\ker(\phi) = N = \{e\}$ gelten, und folglich ist ϕ injektiv. Durch ϕ ist somit ein Isomorphismus zwischen G und $\phi(G)$ definiert. Folglich ist G isomorph zur Untergruppe $\phi(G)$ von $\mathrm{Per}(G/U)$. Wegen $|G/U| = (G : U) = n$ ist $\mathrm{Per}(G/U)$ isomorph zu S_n. Also ist G isomorph zu einer Untergruppe von S_n.

zu (b) Nach Teil (a) existiert ein Isomorphismus zwischen G und einer Untergruppe V von S_n. Durch Komposition dieses Isomorphismus mit der Inklusionsabbildung $V \hookrightarrow S_n$ erhalten wir einen injektiven Homomorphismus $\psi : G \to S_n$. Wir zeigen, dass $\psi(G) \subseteq A_n$ gilt. Daraus folgt, dass G isomorph zur Untergruppe $\psi(G)$ von A_n ist, und nach dem Satz von Lagrange ist $|G| = |\psi(G)|$ somit ein Teiler von $|A_n| = \frac{1}{2}n!$.

Nehmen wir an, dass $\psi(G)$ keine Teilmenge von A_n ist. Durch Komposition von ψ mit der Signumsabbildung $\mathrm{sgn} : S_n \to \{\pm 1\}$ erhalten wir einen Homomorphismus $\alpha = \mathrm{sgn} \circ \psi : G \to \{\pm 1\}$. Wegen $\psi(G) \not\subseteq A_n$ existiert ein $g \in G$ mit $\alpha(g) = (\mathrm{sgn} \circ \psi)(g) = -1$, außerdem gilt $\alpha(e) = (\mathrm{sgn} \circ \psi)(e) = \mathrm{sgn}(\mathrm{id}) = 1$ (wobei e das Neutralelement von G bezeichnet). Der Homomorphismus α ist also surjektiv. Nach dem Homomorphiesatz für Gruppen induziert α einen Isomorphismus $G/\ker(\alpha) \cong \{\pm 1\}$. Dabei ist $\ker(\alpha)$ ein Normalteiler von G, und wegen $(G : \ker(\alpha)) = |G/\ker(\alpha)| = |\{\pm 1\}| = 2$ gilt $\ker(\alpha) \subsetneq G$. Da G laut Angabe einfach ist, muss also $\ker(\alpha) = \{e\}$ gelten. Damit wäre α injektiv, die Gruppe G also isomorph zu einer Untergruppe von $\{\pm 1\}$. Daraus würde $|G| \in \{1, 2\}$ folgen. Aber wegen $|G| = (G : U)|U|$ würde daraus auch $(G : U) \in \{1, 2\}$ folgen, im Widerspruch zur Voraussetzung $(G : U) \geq 3$.

zu (c) Laut Vorlesung ist jede Gruppe der Ordnung 15 zyklisch. (Dies wurde aus den Sylowsätzen abgeleitet.) Wenn in A_5 eine Untergruppe der Ordnung 15 existieren würde, dann auch ein Element der Ordnung 15. Aber selbst in S_5 gibt es kein solches Element. Sei nämlich $\sigma \in S_5$ ein beliebiges nichttriviales Element, vom Zerlegungstyp $(k_1, ..., k_r)$ mit $r \in \mathbb{N}$, $k_1 \geq ... \geq k_r \geq 2$ und $k_1 + ... + k_r \leq 5$. Wäre $\mathrm{ord}(\sigma) = 15$, dann würde daraus $\mathrm{kgV}(k_1, ..., k_r) = 15$ folgen. Dies würde bedeuten, dass mindestens eine der Zahlen k_i durch 3 und eine der Zahlen k_j durch 5 teilbar ist. Aber dies ist wegen $k_1 + ... + k_r \leq 5$ unmöglich, denn im Fall $i \neq j$ wäre $k_1 + ... + k_r \geq 8$, um im Fall $i = j$ wäre k_i sogar durch 15 teilbar, also $k_1 + ... + k_r \geq 15$. Also gibt es in S_5 kein Element der Ordnung 15.

Aufgabe H20T3A3

Sei R ein Ring mit 1, und seien $a, b \in R$. Es gelte $ab = 1$ und $ba \neq 1$. Insbesondere ist R also nicht kommutativ. Ein Element $x \in R$ heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ gibt mit $x^n = 0$. Ein Element $x \in R$ heißt *idempotent*, falls $x^2 = x$ gilt.

(a) Zeigen Sie, dass das Element $1 - ba$ idempotent ist.

(b) Zeigen Sie, dass das Element $b^n(1 - ba)$ für $n \geq 1$ nilpotent ist.

(c) Zeigen Sie, dass es unendlich viele nilpotente Elemente in R gibt.

Lösung:
zu (a) Es gilt $(1-ba)^2 = (1-ba)(1-ba) = 1-ba-ba+(ba)(ba) = 1-2ba+b(ab)a = 1-2ba+b\cdot 1\cdot a = 1-2ba+ba = 1-ba$.

zu (b) Sei $n \in \mathbb{N}$. Dass das Element $b^n(1-ba)$ nilpotent ist, ergibt sich durch die Rechnung

$$\begin{aligned}(b^n(1-ba))^2 &= b^n(1-ba)b^n(1-ba) = (b^n - b^{n+1}a)(b^n - b^{n+1}a) = \\ b^{2n} - b^{n+1}ab^n - b^{2n+1}a + b^{n+1}ab^{n+1}a &= b^{2n} - b^{n+1}(ab)b^{n-1} - b^{2n+1}a + b^{n+1}(ab)b^n a = \\ b^{2n} - b^{n+1}\cdot 1\cdot b^{n-1} - b^{2n+1}a + b^{n+1}\cdot 1\cdot b^n a &= b^{2n} - b^{2n} - b^{2n+1}a + b^{2n+1}a = 0.\end{aligned}$$

zu (c) Nach Teil (b) ist $b^n(1-ba)$ für jedes $n \in \mathbb{N}$ nilpotent. Es genügt also zu zeigen, dass diese Elemente voneinander verschieden sind. Nehmen wir an, es gibt $m, n \in \mathbb{N}$ mit $m < n$ und $b^m(1-ba) = b^n(1-ba)$. Ein einfacher Induktionsbeweis zeigt, dass $a^\ell b^\ell = 1$ gilt. Denn für $\ell = 1$ gilt diese Gleichung laut Angabe, und setzen wir sie für ein $\ell \in \mathbb{N}$ voraus, dann folgt $a^{\ell+1}b^{\ell+1} = a(a^\ell b^\ell)b = a\cdot 1\cdot b = ab = 1$. Multiplizieren wir die Gleichung von oben auf beiden Seiten von links mit a^m, dann erhalten wir $a^m b^m(1-ba) = a^m b^m b^{n-m}(1-ba)$. Wie soeben gezeigt, folgt daraus $1 - ba = b^{n-m}(1-ba)$. Multiplizieren wir diese Gleichung ein weiteres Mal von links mit a, dann folgt

$$\begin{aligned}a(1-ba) = ab^{n-m}(1-ba) &\Rightarrow a-(ab)a = abb^{n-m-1}(1-ba) \Rightarrow \\ a-a = b^{n-m-1}(1-ba) &\Rightarrow b^{n-m-1}(1-ba) = 0 \Rightarrow a^{n-m-1}b^{n-m-1}(1-ba) = 0 \\ &\Rightarrow 1-ba = 0 \Rightarrow ba = 1\end{aligned}$$

im Widerspruch zur Voraussetzung in der Angabe. Also gilt $b^m(1-ba) = b^n(1-ba)$, und folglich besteht die Menge $\{b^n(1-ba) \mid n \in \mathbb{N}\}$ aus unendlich vielen nilpotenten Elementen.

Aufgabe H20T3A4

Es sei $\mathbb{F}_3$ der Körper mit 3 Elementen. Sei I das von x^2+1 im Polynomring $R=\mathbb{F}_3[x]$ erzeugte Ideal.

(a) Zeigen Sie, dass $K=R/I$ ein Körper ist, und ermitteln Sie die Anzahl der Elemente von K.

(b) Geben Sie eine Formel an für das multiplikative Inverse des Elements $ax+b+I$ in R/I für $a,b\in\mathbb{F}_3$, falls es existiert.

(c) Geben Sie einen Erzeuger an für die multiplikative Gruppe $K^\times$.

Lösung:
zu (a) Das Polynom $f=x^2+\bar{1}\in\mathbb{F}_3[x]$ besitzt wegen $f(\bar{0})=\bar{1}\neq\bar{0}$, $f(\bar{1})=\bar{2}\neq\bar{0}$ und $f(\bar{2})=\bar{5}=\bar{2}\neq\bar{0}$ in $\mathbb{F}_3$ keine Nullstelle. Wegen $\operatorname{grad}(f)=2$ ist es somit irreduzibel in $R=\mathbb{F}_3[x]$. Als Polynomring über einem Körper ist R ein Hauptidealring, und somit ist jedes Hauptideal, das von einem irreduziblen Element erzeugt wird, ein maximales Ideal. Folglich ist $I=(f)$ ein maximales Ideal in R, und daraus wiederum folgt, dass $K=R/I$ ein Körper ist. Aus der Vorlesung ist bekannt, dass für jeden Körper k und jedes Polynom $g\in k[x]$ vom Grad $n=\operatorname{grad}(g)\geq 1$ die Polynome vom Grad $\leq n-1$ zusammen mit dem Nullpolynom ein Repräsentantensystem von $k[x]/(g)$ bilden. Wenden wir dies auf $k=\mathbb{F}_3$ und $g=f$ an, so kommen wir zu dem Ergebnis, dass die Polynome der Form $ax+b$ mit $a,b\in\mathbb{F}_3$ ein Repräsentantensystem von $K=R/I$ bilden. Da es für jeden der Koeffizienten a,b jeweils drei Möglichkeiten gibt, existieren insgesamt neun solche Polynome, und folglich besteht auch $K=R/I$ aus neun Elementen.

zu (b) Da die Polynome der Form $ax+b$ mit $a,b\in\mathbb{F}_3$ ein Repräsentantensystem von $K=R/I$ bilden, sind durch $ax+b+I$ mit $a,b\in\mathbb{F}_3$ die neun verschiedenen Elemente von K gegeben. Da es sich bei K um einen Körper handelt, ist das Nullelement $\bar{0}\cdot x+\bar{0}+I=\bar{0}+I$ das einzige Element in K, das kein multiplikatives Inverses besitzt. Seien nun $a,b\in\mathbb{F}_3$ mit $(a,b)\neq(\bar{0},\bar{0})$. Wegen $x^2+\bar{1}\in I$ gilt $x^2+\bar{1}+I=\bar{0}+I$, was zu $x^2+I=-\bar{1}+I$ umgeformt werden kann. Für alle $c,d\in\mathbb{F}_3$ gilt

$$\begin{aligned}(ax+b+I)(cx+d+I) &= acx^2+bcx+adx+bd+I &=\\ (ac+I)(x^2+I)+((ad+bc)x+bd+I) &= (ac+I)(-\bar{1}+I)+((ad+bc)x+bd+I) &=\\ (-ac+I)+((ad+bc)x+bd+I) &= (bd-ac)+(ad+bc)x+I.\end{aligned}$$

Das Einselement von K ist $\bar{1}+I$, und es gilt $(bd-ac)+(ad+bc)x+I=\bar{1}+I$ genau dann, wenn die Gleichungen $bd-ac=\bar{1}$ und $ad+bc=\bar{0}$ erfüllt sind. Betrachten wir zunächst den Fall, dass $a\neq\bar{0}$ ist. Dann kann $ad+bc=\bar{0}$ umgestellt werden zu $d=-a^{-1}bc$. Durch Einsetzen in die Gleichung $bd-ac=\bar{1}$ erhält man $c=\frac{(-a)}{a^2+b^2}$, $d=\frac{b}{a^2+b^2}$. Das multiplikative Inverse von $ax+b+I$ ist also in diesem Fall gegeben durch

$$\frac{(-a)}{a^2+b^2}x+\frac{b}{a^2+b^2}+I.$$

Betrachten wir nun den Fall $a=\bar{0}$. Wegen $(a,b)\neq(\bar{0},\bar{0})$ ist dann $b\neq\bar{0}$, und die beiden Gleichungen von oben vereinfachen sich zu $bd=\bar{1}$ und $bc=\bar{0}$. Wir erhalten in diesem Fall $d=b^{-1}$ und $c=\bar{0}$, somit ist $(ax+b+I)^{-1}=cx+d+I=b^{-1}+I$. Dies zeigt, dass die Gleichung

$$(ax+b+I)^{-1} = \frac{(-a)}{a^2+b^2}x+\frac{b}{a^2+b^2}+I$$

für das multiplikative Inverse auch in dieser Situation gültig ist.

zu (c) Da K ein Körper bestehend aus neun Elementen ist, gilt $|K^\times|=|K\setminus\{\bar{0}\}|=|K|-1=9-1=8$. Sei $\alpha=x+\bar{1}+I$. Dann gilt $\alpha^2=(x+\bar{1})^2+I=x^2+\bar{2}x+\bar{1}+I=(-\bar{1})+\bar{2}x+\bar{1}+I=\bar{2}x+I$, $\alpha^4=(\alpha^2)^2=(\bar{2}x+I)^2=\bar{4}x^2+I=-\bar{1}+I$ und $\alpha^8=(\alpha^4)^2=(-\bar{1})^2+I=\bar{1}+I=1_K$. Wegen $\alpha^4\neq 1_K$ und $\alpha^8=1_K$ ist α ein Element der Ordnung 8.

Aufgabe H20T3A5

Gegeben ist das Polynom $f = x^3 - 3x^2 + 3x - 6 \in \mathbb{Q}[x]$. Weiter sei $\zeta = e^{2\pi i/3} \in \mathbb{C}$ eine primitive dritte Einheitswurzel.

(a) Zeigen Sie, dass f irreduzibel über $\mathbb{Q}$ ist.

(b) Zeigen Sie, dass $a_k = 1 + \zeta^k \sqrt[3]{5}$ für $k = 0, 1, 2$ die drei verschiedenen komplexen Nullstellen von f sind.

(c) Zeigen Sie, dass $L = \mathbb{Q}(\sqrt[3]{5}, \zeta) \subseteq \mathbb{C}$ ein Zerfällungskörper von f ist.

(d) Zeigen Sie, dass die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q})$ isomorph zur symmetrischen Gruppe S_3 ist.

Lösung:

zu (a) Es gilt $3 \nmid 1$, $3 \mid (-3)$, $3 \mid 3$, $3 \mid (-6)$, aber $3^2 \nmid (-6)$. Das Eisenstein-Kriterium, angewendet auf die Primzahl 3, zeigt somit, dass f in $\mathbb{Z}[x]$ irreduzibel ist. Auf Grund des Gauß'schen Lemmas ist f damit auch irreduzibel über $\mathbb{Q}$.

zu (b) Sei $g = f(x+1) = (x+1)^3 - 3(x+1)^2 + 3(x+1) - 6 = (x^3 + 3x^2 + 3x + 1) - (3x^2 + 6x + 3) + (3x + 3) - 6 = x^3 - 5$. Dann ist $\zeta^k \sqrt[3]{5}$ für $k = 0, 1, 2$ eine Nullstelle von g, denn es gilt jeweils $g(\zeta^k \sqrt[3]{5}) = (\zeta^k \sqrt[3]{5})^3 - 5 = (\zeta^3)^k \cdot 5 - 5 = 1^k \cdot 5 - 5 = 0$. Da ζ eine primitive Einheitswurzel ist, sind die Elemente $1, \zeta, \zeta^2$ verschieden, wegen $\sqrt[3]{5} \neq 0$ also auch die Elemente $\zeta^k \sqrt[3]{5}$, $k = 0, 1, 2$. Da g als Polynom dritten Grades nicht mehr als drei komplexe Nullstellen hat, ist $\{\zeta^k \sqrt[3]{5} \mid k = 0, 1, 2\}$ somit die genaue Nullstellenmenge von g. Da für jedes $\alpha \in \mathbb{C}$ die Äquivalenz $g(\alpha) = 0 \Leftrightarrow f(1 + \alpha) = 0$ gilt, ist $N = \{1 + \zeta^k \sqrt[3]{5} \mid k = 0, 1, 2\} = \{a_k \mid k = 0, 1, 2\}$ die dreielementige Nullstellenmenge von f.

zu (c) Da $N = \{a_k \mid k = 0, 1, 2\}$ die Menge der komplexen Nullstellen von f ist, ist $\mathbb{Q}(N)$ ein Zerfällungskörper von f. Zu zeigen ist also $\mathbb{Q}(N) = \mathbb{Q}(\sqrt[3]{5}, \zeta)$. Die Inklusion „$\subseteq$“ ist erfüllt, weil mit $\sqrt[3]{5}$ und ζ auch die Elemente $a_k = 1 + \zeta^k \sqrt[3]{5}$ mit $k \in \{0, 1, 2\}$ in $\mathbb{Q}(\sqrt[3]{5}, \zeta)$ liegen. Es gilt also $N \subseteq \mathbb{Q}(\sqrt[3]{5}, \zeta)$, und daraus folgt auch $\mathbb{Q}(N) \subseteq \mathbb{Q}(\sqrt[3]{5}, \zeta)$. Zum Nachweis von „$\supseteq$“ bemerken wir zunächst, dass mit $a_0 = 1 + \sqrt[3]{5}$ auch das Element $a_0 - 1 = \sqrt[3]{5}$ in $\mathbb{Q}(N)$ liegt. Aus $a_1 = 1 + \zeta \sqrt[3]{5} \in \mathbb{Q}(N)$ folgt $\zeta \sqrt[3]{5} \in \mathbb{Q}(N)$, und aus $\sqrt[3]{5}, \zeta \sqrt[3]{5} \in \mathbb{Q}(N)$ folgt $\zeta = \frac{\zeta \sqrt[3]{5}}{\sqrt[3]{5}} \in \mathbb{Q}(N)$. Insgesamt gilt also $\{\sqrt[3]{5}, \zeta\} \subseteq \mathbb{Q}(N)$, und daraus folgt $\mathbb{Q}(\sqrt[3]{5}, \zeta) \subseteq \mathbb{Q}(N)$.

zu (d) Die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q})$ stimmt mit der Galoisgruppe $\mathrm{Gal}(f|\mathbb{Q})$ des Polynoms f überein, weil L Zerfällungskörper von f ist. Da f drei verschiedene komplexe Nullstellen besitzt, ist diese Gruppe laut Vorlesung isomorph zu einer Untergruppe von S_3. Da $L|\mathbb{Q}$ eine endliche Galois-Erweiterung ist, gilt außerdem $|\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}]$.

Wir bestimmen deshalb den Erweiterungsgrad $[L : \mathbb{Q}]$. Das Polynom $g = x^3 - 5$ ist irreduzibel über $\mathbb{Z}$, da das Eisenstein-Kriterium auf die Primzahl 5 angewendet werden kann. Nach dem Gauß'schen Lemma ist g auch irreduzibel über $\mathbb{Q}$. Außerdem ist g normiert, und es gilt $g(\sqrt[3]{5}) = 0$. Somit ist g das Minimalpolynom von $\sqrt[3]{5}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = \mathrm{grad}(g) = 3$. Wäre das dritte Kreisteilungspolynom $h = x^2 + x + 1$ über $\mathbb{Q}(\sqrt[3]{5})$ reduzibel, dann müssten wegen $\mathrm{grad}(h) = 2$ die beiden komplexen Nullstellen ζ und ζ^2 in $\mathbb{Q}(\sqrt[3]{5})$ liegen. Aber dies ist nicht der Fall, denn wegen $\sqrt[3]{5} \in \mathbb{R}$ gilt $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$, aber die Zahlen $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ und $\zeta^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$ sind nicht reell. Also ist h über $\mathbb{Q}(\sqrt[3]{5})$ irreduzibel, außerdem normiert, und es gilt $h(\zeta) = 0$. Somit ist h das Minimalpolynom von ζ über $\mathbb{Q}(\sqrt[3]{5})$. Wir erhalten

$$[L : \mathbb{Q}(\sqrt[3]{5})] \quad = \quad [\mathbb{Q}(\sqrt[3]{\ })(\zeta) : \mathbb{Q}(\sqrt[3]{5})] \quad = \quad \mathrm{grad}(h) \quad = \quad 2 \quad ,$$

und die Gradformel liefert $[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[3]{5})] \cdot [\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}] = 2 \cdot 3 = 6$. Somit ist auch $|\mathrm{Gal}(L|\mathbb{Q})| = 6$. Wie oben bemerkt, ist $\mathrm{Gal}(L|\mathbb{Q})$ isomorph zu einer Untergruppe U von S_3. Diese muss ebenfalls von Ordnung 6 sein, und wegen $|S_3| = 6$ folgt daraus $U = S_3$. Damit ist insgesamt gezeigt, dass $\mathrm{Gal}(L|\mathbb{Q})$ isomorph zu S_3 ist.