Ralf Gerkmann, Mathematisches Institut der LMU München

Repetitorium zur Algbra

Inhaltsverzeichnis

1 Lineare Algebra

Hinweis: Diese Wiederholung beschränkt sich auf die Teile der Linearen Algebra, die seit dem Frühjahr 2020 Gegenstand von Staatsexamensaufgaben waren. In zukünftigen Aufgaben könnten aber durchaus noch andere Themen behandelt werden.

1.1 Dimensionssätze und lineare Gleichungssysteme

- *Dimensionssatz für Untervektorräume*
  Ist V ein K-Vektorraum und sind U, W endlich-dimensionale Untervektorräume von V, dann gilt

$$\dim(U+W) \quad = \quad \dim(U) + \dim(W) - \dim(U \cap W).$$

- *Dimensionssatz für lineare Abbildungen*
  Ist V ein endlich-dimensionaler und W ein beliebiger K-Vektorraum, dann gilt für jede lineare Abbildung $\phi : V \to W$ jeweils

$$\dim V \quad = \quad \dim \ker(\phi) + \dim \operatorname{im}(\phi).$$

  Dabei ist $\ker(\phi) = \{v \in V \mid \phi(v) = 0_W\}$ und $\operatorname{im}(\phi) = \phi(W) = \{\phi(v) \mid v \in V\}$.

- *Rang einer Matrix, Rangsatz*
  Der Zeilenraum einer Matrix $A \in \mathcal{M}_{m\times n,K}$ ist der Untervektorraum des K^n, der durch die Zeilen von A aufgespannt wird. Dessen Dimension wird der Zeilenrang der Matrix genannt. Ensprechend sind der Spaltenraum und der Spaltenrang von A definiert. Der Rangsatz besagt, dass Zeilen- und Spaltenrang stets übereinstimmen. Deshalb ist es gerechtfertigt, lediglich vom Rang $\operatorname{rg}(A)$ der Matrix A zu sprechen.

- *Lösungsraum homogener linearer Gleichungssysteme*
  Gegeben sei ein homogenes lineares Gleichungssystem $Ax = 0$ mit Koeffizientenmatrix $A \in \mathcal{M}_{m\times n,K}$. Die Lösungsmenge $\mathscr{L}$ dieses Systems ist ein Untervektorraum des K^n der Dimension $n - \operatorname{rg}(A)$.

- *Lösungsraum inhomogener linearer Gleichungssyteme*
  Gegeben sei ein inhomogenes lineares Gleichungssystem $Ax = b$ mit Koeffizientenmatrix $A \in \mathcal{M}_{m\times n,K}$ und erweiterter Koeffizientenmatrix $\tilde{A} = (A, b)$ in $\mathcal{M}_{m\times(n+1),K}$. Die Lösungsmenge $\mathscr{L}$ ist im Fall $\operatorname{rg}(A) < \operatorname{rg}(\tilde{A})$ leer. Ansonsten ist $\mathscr{L}$ ein affiner Unterraum des K^n der Dimension $n - \operatorname{rg}(A)$. Das LGS ist genau dann eindeutig lösbar, wenn $\operatorname{rg}(A) = n$ ist.

Aufgaben zum Thema: H22T2A1, F23T2A1, H23T2A4, F24T3A1

1.2 Eigenschaften der Determinante

- *Charakterisierung der Determinante*
  Die Determinantenfunktion $\det : \mathcal{M}_{n,K} \to K$ ist die eindeutig bestimmte Abbildung mit folgenden Eigenschaften:

  (i) Die Abbildung ist linear in jeder Zeile.

  (ii) Stimmen zwei Zeilen von $A \in \mathcal{M}_{n,K}$ überein, dann gilt $\det(A) = 0$.

(iii) Für die Einheitsmatrix $E \in \mathcal{M}_{n,K}$ gilt $\det(E) = 1$.

Mit anderen Worten, die Determinantenfunktion ist *multilinear*, *alternierend* und *normiert*.

- *Leibnizformel*
  Die Determinante kann durch folgende Summe über die Elemente der symmetrischen Gruppe berechnet werden.
  $$\det(A) \quad = \quad \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)}.$$
  Wichtige Spezialfälle dieser Gleichung sind die Formel $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ und die Sarrus-Regel für $n = 3$.

- *Berechnung der Determinante durch den Gauß-Algorithmus*
  Ist A eine quadratische Matrix in Zeilenstufenform, dann ist A insbesondere eine obere Dreiecksmatrix, und man kann $\det(A)$ durch Multiplikation der Elemente auf der Hauptdiagonalen berechnen. Eine beliebige quadratische Matrix A kann durch den Gauß-Algorithmus in eine Matrix $\tilde{A}$ in normierter Zeilenstufenform überführt werden, und es gilt dann $\det(\tilde{A}) = \mu \det(A)$ für ein $\mu \in K^\times$. Um den Faktor μ zu bestimmen, beachtet man folgende Regeln:
  - Bei jeder Zeilenvertauschung wechselt die Determinante das Vorzeichen.
  - Multipliziert man eine Zeile mit einem Wert $\lambda \in K^\times$, dann ändert sich die Determinante ebenfalls um den Faktor λ.
  - Die Addition des λ-fachen einer Zeile zu einer anderen Zeile hat keinen Einfluss auf die Determinante.

- *Determinante und Invertierbarkeit*
  Für alle $A \in \mathcal{M}_{n,K}$ gilt $\det(A) \neq 0 \Leftrightarrow \operatorname{rg}(A) = n \Leftrightarrow A$ ist invertierbar.

- *Laplace'scher Entwicklungssatz*
  Für jede Matrix $A \in \mathcal{M}_{n,K}$ und $i, j \in \{1, ..., n\}$ gilt
  $$\det(A) \quad = \quad \sum_{j=1}^{n} (-1)^{i+j} \det(A_{ij}) \quad = \quad \sum_{i=1}^{n} (-1)^{i+j} \det(A_{ij}).$$
  Dabei entsteht $A_{ij} \in \mathcal{M}_{n-1,K}$ aus A jeweils durch Entfernung der i-ten Zeile und der j-ten Spalte.

1.3 Darstellungsmatrizen

- *Darstellungsmatrix einer linearen Abbildung*
  Seien V, W zwei K-Vektorräume mit $n = \dim(V)$, $m = \dim(W)$, und sei $\phi : V \to W$ eine lineare Abbildung. Seien $\mathcal{A} = (v_1, ..., v_n)$ und $\mathcal{B} = (w_1, ..., w_m)$ geordnete Basen von V bzw. W. Dann bezeichnet man die eindeutig bestimmte Matrix $A = (a_{ij}) \in \mathcal{M}_{m \times n,K}$ mit
  $$\phi(v_j) \quad = \quad \sum_{i=1}^{m} a_{ij} w_i \qquad \text{für} \quad 1 \leq j \leq n$$
  als Darstellungsmatrix $\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$ von ϕ bezüglich der Basen $\mathcal{A}$ und $\mathcal{B}$. An der j-ten Spalte von A kann also jeweils das Bild des j-te Basisvektors v_j abgelesen werden.

- *Darstellungsmatrix einer Bilinearform*
  Sei V ein K-Vektorraum der endlichen Dimension n und $\mathcal{A} = (v_1, ..., v_n)$ eine geordnete Basis von V. Sei $b : V \times V \to K$ eine Bilinearform auf V. Dann wird die Matrix $A = (a_{ij}) \in \mathcal{M}_{n,K}$ mit den Einträgen $a_{ij} = b(v_i, v_j)$ die Darstellungsmatrix $\mathcal{M}_{\mathcal{A}}(b)$ von b bezüglich $\mathcal{A}$ genannt.

- *Anwendung von Darstellungsmatrizen auf Koordinatenvektoren*
  Seien V, W, ϕ, b, $\mathcal{A}$ und $\mathcal{B}$ wie in den letzten beiden Absätzen definiert. Dann gilt für alle $v, w \in V$ jeweils
  $$\Phi_{\mathcal{B}}(\phi(v)) = \mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi) \cdot \Phi_{\mathcal{A}}(v) \qquad \text{und} \quad b(v, w) = {}^{\mathrm{t}}\Phi_{\mathcal{A}}(v) \cdot \mathcal{M}_{\mathcal{A}}(b) \cdot \Phi_{\mathcal{A}}(w).$$
  Dabei bezeichnet $\Phi_{\mathcal{A}}(v) \in K^n$ den Koordinatenvektor von v bezüglich $\mathcal{A}$.

- *Äquivalenz von Matrizen*
  Zwei Matrizen $A, B \in \mathcal{M}_{m \times n,K}$ werden als äquivalent bezeichnet, wenn es Matrizen $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ mit $B = SAT$ gibt. Je zwei Darstellungsmatrizen einer linearen Abbildung $\phi : V \to W$ bezüglich unterschiedlicher geordneter Basen von V und W sind äquivalent zueinander.

- *Ähnlichkeit von Matrizen*
  Zwei Matrizen $A, B \in \mathcal{M}_{n,K}$ werden ähnlich genannt, wenn eine Matrix $T \in \mathrm{GL}_n(K)$ mit $B = TAT^{-1}$ existiert. Je zwei Darstellungsmatrizen eines Endomorphismus $\phi \in \mathrm{End}_K(V)$ bezüglich verschiedener geordneter Basen von V sind ähnlich zueinander.

- *Transformationsformel für lineare Abbildungen*
  Seien die Bezeichnungen wie im ersten Absatz dieses Abschnitts, $\mathcal{A}'$ eine weitere geordnete Basis von V und $\mathcal{B}'$ eine weitere geordnete Basis von W. Dann gilt
  $$\mathcal{M}_{\mathcal{B}'}^{\mathcal{A}'}(\phi) \quad = \quad \mathcal{T}_{\mathcal{B}'}^{\mathcal{B}} \cdot \mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi) \cdot \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$$
  wobei $\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$ die Matrix des Basiswechsels von $\mathcal{A}'$ nach $\mathcal{A}$ bezeichnet. Diese Matrix rechnet einen $\mathcal{A}'$-Koordinatenvektor von $v \in V$ in einen $\mathcal{A}$-Koordinatenvektor um.

- *Transformationsformel für Bilinearformen*
  Seien die Bezeichnungen wie im zweiten Absatz dieses Abschnitts, und es sei $\mathcal{A}'$ eine weitere geordnete Basis von V. Dann gilt
  $$\mathcal{M}_{\mathcal{A}'}(b) \quad = \quad {}^{\mathrm{t}}\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'} \cdot \mathcal{M}_{\mathcal{A}}(b) \cdot \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}.$$

1.4 Eigenwerte und Diagonalisierbarkeit

- *Eigenwerte und Eigenvektoren eines Endomorphismus*
  Sei $\phi \in \mathrm{End}_K(V)$, $v \in V$ und $\lambda \in K$. Man bezeichnet v als Eigenvektor von ϕ um Eigenwert λ, wenn $v \neq 0_V$ und $\phi(v) = \lambda v$ gilt. Ist $A \in \mathcal{M}_{n,K}$, so ist $v \in K^n$ ein Eigenvektor von A zum Eigenwert λ, wenn $v \neq 0_{K^n}$ und $Av = \lambda v$ gilt. Die Eigenwerte von ϕ bzw. A sind genau die Werte $\lambda \in K$, für die ein Eigenvektor existiert.

- *charakteristisches Polynom*
  Das charakteristische Polynom von $A \in \mathcal{M}_{n,K}$ ist das Polynom $\chi_A = \det(xE - A) \in K[x]$, wobei $E \in \mathcal{M}_{n,K}$ die Einheitsmatrix bezeichnet. Die Eigenwerte von A sind genau die Nullstellen von χ_A. Das charakteristische Polynom χ_ϕ eines Endomorphismus ϕ ist das charakteristische Polynom einer beliebigen Darstellungsmatrix des Endomorphismus.

- *Eigenraum und geometrische Vielfachheit eines Eigenwerts*
  Der Eigenraum eines Endomorphismus ϕ zum Eigenwert λ ist durch $\mathrm{Eig}(\phi, \lambda) = \{v \in V \mid \phi(v) = \lambda v\}$ definiert. Dessen Dimension wird die geometrische Vielfachheit von λ bezüglich ϕ genannt.

- *algebraische Vielfachheit eines Eigenwerts*
  Die algebraische Vielfachheit von λ bezüglich ϕ ist die Vielfachheit von λ als Nullstelle von χ_ϕ.

- *Diagonalisierbarkeit einer Matrix und eines Endomorphismus*
  Eine Matrix bezeichnet man als diagonalisierbar, wenn sie ähnlich zu einer zu einer Diagonalmatrix ist. Ein Endomorphismus $\phi \in \mathrm{End}_K(V)$ wird diagonalisierbar genannt, wenn eine geordnete Basis $\mathcal{A}$ von V existiert, so dass $\mathcal{M}_\mathcal{A}(\phi)$ eine Diagonalmatrix ist.

- *Diagonalisierbarkeitskriterium*
  Eine Matrix $A \in \mathcal{M}_{n,K}$ ist genau dann diagonalisierbar, wenn χ_A über K in Linearfaktoren zerfällt und für jeden Eigenwert λ von A die geometrische Vielfachheit mit der algebraischen Vielfachheit übereinstimmt. (Das Diagonalisierbarkeitskriterium für Endomorphismen hat dieselbe Formulierung.)

1.5 Die Jordansche Normalform

- *Minimalpolynom einer Matrix*
  Das Minimalpolynom μ_A von $A \in \mathcal{M}_{n,K}$ ist das eindeutig bestimmte, normierte Polynom $f \in K[x]$ minimalen Grades mit $f(A) = 0_{\mathcal{M}_{n,K}}$.

- *Satz von Cayley-Hamilton*
  Für jede Matrix $A \in \mathcal{M}_{n,K}$ gilt $\chi_A(A) = 0_{\mathcal{M}_{n,K}}$. Daraus folgt, dass das Minimalpolynom μ_A stets ein Teiler von χ_A ist. (Weil die Eigenwerte von A sind genau die Nullstellen von μ_A sind, ist μ_A außerdem ein Vielfaches des Produkts über $(x - \lambda)$, wobei λ die Eigenwerte von A durchläuft.)

- *Jordanmatrizen und Jordansche Normalform*
  Eine Matrix $J \in \mathcal{M}_{n,K}$, die auf der Hauptdiagonale den konstanten Wert $\lambda \in K$, auf der rechten Nebendiagonale den Wert 1 und ansonsten nur Nullen enthält, wird als Jordanmatrix zum Eigenwert λ bezeichnet. Eine Blockmatrix bestehend aus Jordanmatrizen entlang der Hauptdiagonalen wird Matrix in Jordanscher Normalform (JNF) genannt. Die Jordanmatrizen werden als *Jordanblöcke* der JNF bezeichnet.

- *Eigenschaften der Jordanschen Normalform*

  (i) Eine Matrix $A \in \mathcal{M}_{n,K}$ ist genau dann ähnlich zu einer Matrix in JNF, wenn χ_A in $K[x]$ in Linearfaktoren zerfällt.

  (iii) Je zwei Matrizen $J, J' \in \mathcal{M}_{n,K}$ in JNF sind genau dann ähnlich zueinander, wenn sie bis auf Reihenfolge dieselben Jordanblöcke enthalten.

  Im Folgenden sei $A \in \mathcal{M}_{n,K}$ und $J \in \mathcal{M}_{n,K}$ eine zu A ähnliche Matrix in JNF. Außerdem sei λ ein Eigenwert von A.

  (iv) Die geometrische Vielfachheit von λ bezüglich A ist gleich der Anzahl der Jordanblöcke von J zum Eigenwert λ.

  (v) Die algebraische Vielfachheit von λ bezüglich A ist die Summe der Größen aller Jordanblöcke von J zum Eigenwert λ.

  (vi) Die Vielfachheit von λ als Nullstelle von μ_A ist gleich der Größe des größten Jordanblocks.

1.6 Euklidische Vektorräume

- *Skalarprodukte*
  Ein Skalarprodukt auf einem $\mathbb{R}$-Vektorraum V ist eine symmetrische, positiv definite Bilinearform. Ein $\mathbb{R}$-Vektorraum mit einem Skalarprodukt wird als euklidischer Vektorraum bezeichnet. Ein Skalarprodukt auf einem $\mathbb{C}$-Vektorraum ist eine Sesquilinearform, die hermitesch und positiv definit ist.

- *Gram-Schmidt-Orthonormalisierung*
  Auf jedem endlich-dimensionalen euklidischen Vektorraum V existiert eine ON-Basis. Diese erhält man durch folgendes Verfahren: Zunächst wählt man einen Vektor $v \in V$ ungleich 0_V und normiert ihn. Ist ein orthonormales Tupel $(v_1, ..., v_m)$ mit $m < \dim(V)$ bereits konstruiert, dann wählt man einen Vektor $w \in V$ außerhalb von $U = \langle v_1, ..., v_m \rangle_{\mathbb{R}}$, bildet die Orthogonalprojektion $\pi_U(w)$, berechnet anschließend die Differenz $w - \pi_U(w)$ und normiert diese. Den Vektor v_{m+1}, den man auf diese Weise erhält, nimmt man zum bereits konstruierten Tupel hinzu.

- *orthogonale Endomorphismen*
  Sei (V, b) ein euklidischer Vektorraum und $\phi \in \mathrm{End}_K(V)$. Man bezeichnet ϕ als orthogonal, wenn $b(\phi(v), \phi(w)) = b(v, w)$ für alle $v, w \in V$ gilt. Typische Beispiele für orthogonale Endomorphimen sind Drehungen und Spiegelungen. Ein Endomorphismus ist genau dann orthogonal, wenn seine Darstellungsmatrix A bezüglich einer bliebigen ON-Basis $\mathcal{A}$ von V orthogonal ist, also ${}^{\mathrm{t}}AA = E$ gilt.

- *selbstadjungierte Endomorphismen*
  Sei (V, b) ein euklidischer Vektorraum und $\phi \in \mathrm{End}_K(V)$. Man bezeichnet ϕ als selbstadjungiert, wenn $b(\phi(v), w) = b(v, \phi(w))$ für alle $v, w \in v$ gilt. Ein Endomorphismus ist genau dann selbstadjungiert, wenn seine Darstellungsmatrix A bezüglich einer bliebigen ON-Basis $\mathcal{A}$ von V symmetrisch ist.

- *Satz über die Hauptachsentransformation*
  Zu jedem selbstadjungierte Endomorphismus auf einem endlich-dimensionalen euklidischen $\mathbb{R}$-Vektorraum existiert eine ON-Basis bestehend aus Eigenvektoren. Ist $A \in \mathcal{M}_{n,\mathbb{R}}$ eine symmetrische Matrix, dann existiert eine orthogonale Matrix T, so dass $D = {}^{\mathrm{t}}TAT$ eine Diagonalmatrix ist.

2 Gruppen

2.1 Grundbegriffe der Gruppentheorie, Beispiele

- *Gruppen*
  Eine Gruppe ist ein Paar $(G, \cdot)$ bestehend aus einer Menge G und einer assoziativen Verknüpfung, die folgende weitere Bedingungen erfüllt.

  (i) Es gibt ein Element $e_G \in G$ mit $g \cdot e_G = e_G \cdot g = g$.
  (Dieses Element ist eindeutig bestimmt. Man nennt e_G das *Neutralelement* der Gruppe.)

  (ii) Für jedes $g \in G$ existiert ein $h \in G$ mit $gh = hg = e_G$. (Dieses Element ist jeweils eindeutig bestimmt und wird mit g^{-1} bezeichnet.)

  Ist die Verknüpfung $\cdot$ darüber hinaus kommutativ, gilt also $gh = hg$ für alle $g, h \in G$, dann bezeichnet man $(G, \cdot)$ als *abelsche* oder *kommutative* Gruppe.

- *additive Schreibweise*
  Bei abelschen Gruppen wird häufig $+$ als Verknüpfungssymbol verwendet. In diesem Fall bezeichnet man das Neutralelement einer solchen Gruppe G mit 0_G, und das Inverse von $g \in G$ jeweils mit $-g$. Für $m \in \mathbb{N}$ ist dann mg eine abkürzende Schreibweise für die Verknüpfung $g + ... + g$ von m Exemplaren von g, und man setzt $(-m)g = -(gm)$.

- *wichtige Beispiele für abelsche Gruppen*

  (i) Ist R ein Ring (oder sogar ein Körper), dann ist $(R, +)$ eine abelsche Gruppe. Insbesondere sind $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ abelsche Gruppen, und $(\mathbb{Z}/n\mathbb{Z}, +)$ ist eine n-elementige abelsche Gruppe für jedes $n \in \mathbb{N}$.

  (ii) Für jeden K-Vektorraum V ist $(V, +)$ eine abelsche Gruppe. Beispielsweise bilden die $m \times n$-Matrizen über K mit der Addition von Matrizen jeweils eine Gruppe, für beliebige $m, n \in \mathbb{N}$.

  (iii) Für jeden Körper K kann die multiplikative Gruppe $K^\times$ gebildet werden. Unter anderem ist $\mathbb{F}_p^\times$ für jede Primzahl p eine $(p-1)$-elementige abelsche Gruppe.

  (iv) Die symmetrische Gruppe S_n ist abelsch für $n \leq 2$, und die alternierende Gruppe A_n ist abelsch für $n \leq 3$. Außerdem ist die *Kleinsche Vierergruppe* V_4 eine abelsche Gruppe.

  (v) Sind G und H abelsche Gruppen, dann auch $G \times H$ (mit der komponentenweisen Verknüpfung). Für alle $r \in \mathbb{N}$ und $m_1, ..., m_r \in \mathbb{N}$ ist $\mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$ eine endliche abelsche Gruppe.

2.2 Zyklische und abelsche Gruppen

2.3 Faktorgruppen und Homomorphiesatz

2.4 Gruppenoperationen und Sylowsätze

3 Ringe

3.1 Grundbegriffe der Ringtheorie, Beispiele

3.2 Faktorringe und Homomorphiesatz

3.3 Teilbarkeit und Irreduzibilität

3.4 Kongruenzrechnung

4 Körper

4.1 Endliche Körpererweiterungen

4.2 Normale und separable Erweiterungen

4.3 Endliche Körper

4.4 Kreisteilungspolynome und Kreisteilungskörper

5 Galoistheorie

5.1 Der Hauptsatz der Galoistheorie und seine Ergänzungen

5.2 Galoisgruppen spezieller Körpererweiterungen

5.3 Auflösbarkeit und Konstruktion mit Zirkel und Lineal

A Chronologische Sortierung der Aufgaben

Es fehlen noch die Lösungen zu den Prüfungsterminen Frühjahr 2023 (größtenteils), Herbst 2023, Frühjahr 2024, Frühjahr 2025 und Herbst 2025.

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

Frühjahr 2021

F21T1A1	F21T1A2	F21T1A3	F21T1A4	F21T1A5
F21T2A1	F21T2A2	F21T2A3	F21T2A4	F21T2A5
F21T3A1	F21T3A2	F21T3A3	F21T3A4	F21T3A5

Herbst 2021

H21T1A1	H21T1A2	H21T1A3	H21T1A4	H21T1A5
H21T2A1	H21T2A2	H21T2A3	H21T2A4	H21T2A5
H21T3A1	H21T3A2	H21T3A3	H21T3A4	H21T3A5

Frühjahr 2022

F22T1A1	F22T1A2	F22T1A3	F22T1A4	F22T1A5
F22T2A1	F22T2A2	F22T2A3	F22T2A4	F22T2A5
F22T3A1	F22T3A2	F22T3A3	F22T3A4	F22T3A5

Herbst 2022

H22T1A1	H22T1A2	H22T1A3	H22T1A4	H22T1A5
H22T2A1	H22T2A2	H22T2A3	H22T2A4	H22T2A5
H22T3A1	H22T3A2	H22T3A3	H22T3A4	H22T3A5

Frühjahr 2023

F23T1A1	F23T1A2	F23T1A3	F23T1A4	F23T1A5
F23T2A1	F23T2A2	F23T2A3	F23T2A4	F23T2A5
F23T3A1	F23T3A2	F23T3A3	F23T3A4	F23T3A5

Herbst 2023

H23T1A1	H23T1A2	H23T1A3	H23T1A4	H23T1A5
H23T2A1	H23T2A2	H23T2A3	H23T2A4	H23T2A5
H23T3A1	H23T3A2	H23T3A3	H23T3A4	H23T3A5

Frühjahr 2024

F24T1A1	F24T1A2	F24T1A3	F24T1A4	F24T1A5
F24T2A1	F24T2A2	F24T2A3	F24T2A4	F24T2A5
F24T3A1	F24T3A2	F24T3A3	F24T3A4	F24T3A5

Herbst 2024

H24T1A1	H24T1A2	H24T1A3	H24T1A4	H24T1A5
H24T2A1	H24T2A2	H24T2A3	H24T2A4	H24T2A5
H24T3A1	H24T3A2	H24T3A3	H24T3A4	H24T3A5

Frühjahr 2025

F25T1A1	F25T1A2	F25T1A3	F25T1A4	F25T1A5
F25T2A1	F25T2A2	F25T2A3	F25T2A4	F25T2A5
F25T3A1	F25T3A2	F25T3A3	F25T3A4	F25T3A5

B Sortierung nach Einzelthemen

0. Lineare Algebra

- Grundlagen
  H20T1A3, F21T2A2, H22T3A1, H22T3A4, F23T1A4, F23T1A5, F23T3A2, H23T2A4
- Lineare Gleichungssysteme
  H22T2A1, F23T2A1
- Ordnung linearer Gruppen
  F20T2A3, H21T3A2, F25T1A1, F25T2A5
- Berechnung von Determinanten
  F24T1A1
- Dimensionssätze
  F24T3A1
- Endomorphismen, charakteristisches Polynom, Eigenräume und Diagonalisierung
  F20T1A1, F21T1A2, F21T2A5, F23T2A1, F25T1A3
- Minimalpolynome und Satz von Cayley-Hamilton
  H21T3A3, F22T1A1, F25T3A1
- Jordansche Normalform
  F20T2A1
- euklidische Vektorräume H21T1A2

I. Gruppentheorie

- Elementare Gruppentheorie
  F20T2A4, F20T3A1, H22T1A1, H22T2A5, F23T1A1, H23T2A3, F24T1A2, F24T2A3, F24T3A3, H24T1A1, H24T3A1
- Elementordnungen und zyklische Gruppen
  H20T1A4, H21T2A1, F22T2A1, F24T2A4, F24T2A3
- abelsche Gruppen
  F23T3A3, F24T2A3, H24T3A1, F25T3A2
- symmetrische Gruppen
  H21T3A1, F22T1A3, H23T1A2
- Homomorphie- Isomorphie- und Korrespondenzsatz
  H22T1A1, H22T2A5, F23T1A1, F23T2A2, H23T3A1
- Gruppenoperationen
  F20T1A2, F20T3A3, H20T2A2, H22T1A1, F23T1A4, F23T3A1, H23T1A3, F25T1A4

- Satz von Cayley
  H20T3A2, H21T2A5, F22T1A3, F22T3A1
- Normalteiler und einfache Gruppen
  H24T2A3
- Auflösbarkeit
  F21T3A3, H22T2A5, H23T2A2, F24T3A3
- semidirekte Produkte
  F20T1A3, H21T1A4
- Sylowsätze
  F20T1A3, F20T2A3, F21T1A4, F22T2A2, F22T3A1, H22T3A3, F23T2A2, F23T3A3, H24T1A2, H24T2A3, F25T2A4

II. Ringtheorie

- Elementare Ringtheorie
  H20T1A2, H20T3A3, F21T2A3, H21T1A1, H22T2A2, F23T1A2, F23T1A4, F23T3A5, F24T2A4, F24T3A3, H24T1A3, F25T1A1
- Elementare Zahlentheorie
  H22T2A3
- Ideale und Faktorringe
  H20T3A4, F21T3A4, F22T1A4, F22T2A3, H22T3A4, H22T3A5, H23T1A4, H23T2A5, H23T3A5, F24T1A3, H24T1A4, H24T2A4
- Homomorphie- Isomorphie- und Korrespondenzsatz
  H20T2A4, F22T1A4, H22T3A4, F23T1A2, H23T1A1
- Kongruenzrechnung und Restklassenringe
  F20T1A5, F20T3A2, H20T1A1, H20T2A1, F22T1A2, F22T1A4, F22T3A2, H22T2A3, F23T2A1, H23T1A1, H23T3A4, F24T2A1, F24T2A2, H24T2A1, H24T2A2, H24T3A3, F25T2A1
- Chinesischer Restsatz
  H20T3A1, H22T1A2, H22T2A3, H23T1A1, H23T3A4, F24T3A2, H24T3A2
- Euklidische Ringe und Euklidischer Algorithmus
  H23T3A5, F24T3A1, H24T2A4, F25T3A5
- Hauptidealringe und faktorielle Ringe
  H22T3A2, F25T3A3
- Quadratische Zahlringe und Zerlegbarkeit von Elementen
  F21T1A1, F22T3A3, F23T2A3, F24T2A1, F24T3A1, F24T3A4, H24T1A3, H24T2A4
- Irreduzibilität von Polynomen
  F20T3A5, F21T3A1, H21T1A3, H22T2A4

III. Körpertheorie

- Teilkörper und Homomorphismen
  H24T1A4
- Algebraische Erweiterungen
  F21T1A3, F22T1A5, H22T1A4, H24T3A4
- Bestimmung von Minimalpolynomen
  F23T3A4, H23T3A2, H23T3A3, F24T1A5
- Erweiterungsgrade
  F21T2A1, F22T1A5, F22T2A5, F22T3A5, H22T1A4, H23T2A1, H23T3A3, F24T2A1, F24T2A5, F24T3A4, H24T2A5, F25T2A3
- Körperhomomorphismen und Fortsetzungssatz
  F22T3A5
- Zerfällungskörper
  F23T1A3, F23T2A4
- separable Körpererweiterungen
  H21T2A3
- endliche Körper
  H20T2A3, F21T3A5, H21T2A2, H21T3A4, F22T2A4, H22T3A4, F23T2A5, H23T1A5, F24T2A1

IV. Galoistheorie

- Nachweis von Galois-Erweiterungen
  F22T2A5, F22T3A5, H22T1A3, H22T2A4, H22T3A4, F23T1A3, H23T2A1, F24T1A5, H24T1A5, H24T2A5, H24T3A4
- Hauptsatz der Galoistheorie
  F20T3A4, H20T2A5, F21T2A4, H21T1A5, F22T2A5, F22T3A4, H22T1A3, F23T1A3, H24T2A5, F25T2A2
- Rechnen in Galoisgruppen und Bestimmung des Isomorphietyps
  H20T1A5, H20T3A5, F21T1A5, F21T3A2, H21T2A4, H22T1A4, H22T2A4, F23T1A3, F24T1A5, H24T2A5, H24T3A4, F25T1A5, F25T3A4
- Kreisteilungspolynome und Kreisteilungskörper
  F20T1A4, F20T2A2, F20T2A5, H21T3A5, F22T1A1, H22T1A5, H22T2A4, F23T3A4, H23T1A5, F24T1A4, F24T3A5, H24T3A5,
- Konstruktion mit Zirkel und Lineal
  F24T3A5

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 $\nu_{101} = 1$. 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 $a_1 \equiv 0 \bmod 4$ 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 $\mathrm{ord}(\zeta) \mid (2t)$ und $\mathrm{ord}(\zeta) \nmid t$ 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 $\mathrm{ord}(\zeta) \mid t$ 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 $\mathrm{ord}(\zeta) \mid 2t$. Würde auch $\mathrm{ord}(\zeta) \mid t$ 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 $\mathrm{ggT}(x^d + 1, dx^{d-1}) = 1$ und $\mathrm{ggT}(x^n + 1, nx^{n-1}) = 1$ 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 $\zeta \in \mathbb{C}^\times$, $\mathrm{ord}(\zeta) \mid (2d)$ und $\mathrm{ord}(\zeta) \nmid d$. Weil d ein Teiler von n ist, gilt auch $(2d) \mid (2n)$ und damit $\mathrm{ord}(\zeta) \mid (2n)$. Nehmen wir nun an, dass auch $\mathrm{ord}(\zeta) \mid n$ erfüllt ist. Dann ist $\mathrm{ord}(\zeta)$ insgesamt ein Teiler von $\mathrm{ggT}(2d, n) = \mathrm{ggT}(2d, dm) = d$, wobei im letzten Schritt verwendet wurde, dass m ungerade ist. Aber $\mathrm{ord}(\zeta) \mid d$ steht im Widerspruch zu unserer Voraussetzung. Es gilt also $\mathrm{ord}(\zeta) \mid (2n)$ und $\mathrm{ord}(\zeta) \mid n$. 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. (Korrektur!! Es kÃ¶nnte $d = n$ sein. m ungerade $\Rightarrow -1$ ist Nullstelle von $x^m + 1$.)

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.

Aufgabe F21T1A1

Seien $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ die Gauß'schen Zahlen und

$$N(a + bi) = a^2 + b^2$$

die übliche Norm. Für $\alpha, \beta \in \mathbb{Z}[i]$ ist α ein Teiler von β (Notation $\alpha \mid \beta$), falls $\beta = \gamma \cdot \alpha$ für ein $\gamma \in \mathbb{Z}[i]$ gilt. Zeigen Sie:

(a) $4 + 5i$ ist ein Teiler von $14 - 3i$

(b) $3 + 7i$ ist kein Teiler von $10 + 3i$

(c) Für $\alpha = a + bi \in \mathbb{Z}[i]$ gilt: $N(\alpha)$ ist gerade $\Leftrightarrow$ $1 + i$ teilt α.

Lösung:
zu (a) Es gilt

$$\frac{14 - 3i}{4 + 5i} \quad = \quad \frac{(14 - 3i)(4 - 5i)}{4 + 5i)(4 - 5i)} \quad = \quad \frac{41 - 82i}{4^2 + 5^2} \quad = \quad \tfrac{1}{41}(41 - 82i) \quad = \quad 1 - 2i.$$

Somit gilt in $\mathbb{Z}[i]$ die Gleichung $(1 - 2i)(4 + 5i) = 14 - 3i$, und somit ist $4 + 5i$ in $\mathbb{Z}[i]$ ein Teiler von $14 - 3i$.

zu (b) Allgemein gilt: Sind $\alpha, \beta \in \mathbb{Z}[i]$ und ist α ein Teiler von β in $\mathbb{Z}[i]$, dann ist $N(\alpha)$ ein Teiler von $N(\beta)$ in $\mathbb{Z}$. Denn auf Grund der Teiler-Eigenschaft existiert ein $\gamma \in \mathbb{Z}[i]$ mit $\beta = \gamma\alpha$, und aus der Multiplikativität der Norm folgt $N(\beta) = N(\gamma)N(\alpha)$. Hier ist $N(3 + 7i) = 3^2 + 7^2 = 9 + 49 = 58$ und $N(10 + 3i) = 10^2 + 3^2 = 109$. Aber 58 ist kein Teiler von 109 in $\mathbb{Z}$, somit ist $3 + 7i$ kein Teiler von $10 + 3i$ in $\mathbb{Z}[i]$.
Hinweis: Die Umkehrung der angegebenen Aussage ist im Allgemeinen falsch, d.h. aus $N(\alpha)|N(\beta)$ folgt im Allgemeinen nicht $\alpha \mid \beta$. Setzen wir beispielsweise $\alpha = 2 - i$ und $\beta = 2 + i$, dann ist $N(\alpha)$ ein Teiler von $N(\beta)$ wegen $N(\alpha) = N(\beta) = 5$. Aber α ist kein Teiler von β. Denn anderenfalls gäbe es ein $\gamma \in \mathbb{Z}[i]$ mit $\beta = \gamma\alpha$, und folglich wäre $\frac{\beta}{\alpha} = \gamma$ in $\mathbb{Z}[i]$ enthalten. Tatsächlich aber gilt

$$\frac{\beta}{\alpha} \quad = \quad \frac{2 + i}{2 - i} \quad = \quad \frac{(2 + i)^2}{(2 + i)(2 - i)} \quad = \quad \frac{3 + 4i}{2^2 + 1^2} \quad = \quad \tfrac{3}{5} + \tfrac{4}{5}i$$

und somit $\frac{\beta}{\alpha} \notin \mathbb{Z}[i]$.

zu (c) „$\Leftarrow$" Gilt $(1 + i) \mid \alpha$, dann ist $N(1 + i) = 2$ ein Teiler von $N(\alpha)$, und folglich ist $N(\alpha)$ gerade. „$\Rightarrow$" Ist $N(\alpha) = \alpha\bar{\alpha}$ gerade, dann ist gibt es ein $d \in \mathbb{N}$ mit $\alpha\bar{\alpha} = 2d = (1 + i)(1 - i)d$. Somit ist $1 + i$ ein Teiler von $\alpha\bar{\alpha}$ in $\mathbb{Z}[i]$. Weil $N(1 + i) = 2$ eine Primzahl ist, ist $1 + i$ laut Vorlesung in $\mathbb{Z}[i]$ irreduzibel. Weil $\mathbb{Z}[i]$ außerdem ein euklidischer Ring ist, muss $1 + i$ darüber hinaus ein Primelement sein. Aus $(1 + i) \mid \alpha\bar{\alpha}$ folgt somit $(1 + i) \mid \alpha$ oder $(1 + i) \mid \bar{\alpha}$.

Im Fall $(1 + i) \mid \alpha$ sind wir fertig. Betrachten wir nun den Fall $(1 + i) \mid \bar{\alpha}$. Dann gilt $\bar{\alpha} = \gamma(1 + i)$ für ein $\gamma \in \mathbb{Z}[i]$, und komplexe Konjugation auf beiden Seiten liefert $\alpha = \bar{\gamma}(1 - i) = \bar{\gamma} \cdot (-i) \cdot (1 + i)$. Dies zeigt, dass $1 + i$ auch in diesem Fall ein Teiler von α ist.

Aufgabe F21T1A2

Sei V ein K-Vektorraum und $f : V \to V$ eine K-lineare Abbildung. Es seien $m \geq 1$ und $a_0, ..., a_{m-1} \in K$ gegeben mit

$$f^m + a_{m-1}f^{m-1} + ... + a_1 f + a_0 \cdot \mathrm{id}_V = 0,$$

wobei m minimal gewählt ist (d.h. es gibt keine solche Relation mit kleinerem m). Zeigen Sie:

(a) Ist $a_0 = 0$, so ist f nicht invertierbar.

(b) Ist $a_0 \neq 0$, so ist f invertierbar.

Lösung:

zu (a) Dies ergibt sich aus einer kurzen Rechnung im (in der Regel nicht-kommutativen) Ring $\mathrm{End}_K(V)$. Nehmen wir an, dass f invertierbar ist und $a_0 = 0$ ist. Dann können wir die Gleichung $f^m + a_{m-1}f^{m-1} + ... + a_1 f = 0$ auf beiden Seiten von links mit f^{-1} multiplizieren und erhalten $f^{m-1} + a_{m-1}f^{m-2} + ... + a_1 \cdot \mathrm{id}_V = 0$. Aber diese Gleichung widerspricht der Minimalität von m.

zu (b) Auch dies kann durch eine Rechnung in $\mathrm{End}_K(V)$ gezeigt werden. Subtraktion von $a_0 \cdot \mathrm{id}_V$ und anschließende Multiplikation mit $-a_0^{-1}$ auf beiden Seiten der Gleichung liefert

$$(-a_0^{-1})f^m + (-\frac{a_{m-1}}{a_0})f^{m-1} + ... + (-\frac{a_2}{a_0})f^2 + (-\frac{a_1}{a_0})f \quad = \quad \mathrm{id}_V.$$

Es gilt also $f \circ g = \mathrm{id}_V$ mit $g = (-a_0^{-1})f^{m-1} + (-\frac{a_{m-1}}{a_0})f^{m-2} + ... + (-\frac{a_2}{a_0})f + (-\frac{a_{m-1}}{a_0}) \cdot \mathrm{id}_V$. Dies zeigt, dass f in $\mathrm{End}_K(V)$ invierterbar ist.

Aufgabe F21T1A3

Sei $K \subseteq L$ eine algebraische Körpererweiterung. Es sei $\alpha \in L$ mit $K(\alpha) = L$. Zu jedem Zwischenkörper E ist p_E das Minimalpolynom von α über E.

(a) Zeigen Sie, dass $[L : E] = \deg(p_E)$ für jeden Zwischenkörper E gilt.

(b) Seien E und F zwei Zwischenkörper mit $F \subseteq E$. Zeigen Sie, dass p_E ein Teiler von p_F in $E[x]$ ist.

(c) Sei E ein Zwischenkörper. Sei F der Zwischenkörper erzeugt von den Koeffizienten von p_E. Zeigen Sie, dass $p_E = p_F$ gilt. Folgern Sie daraus, dass $E = F$ ist.

Lösung:
zu (a) Für jeden Zwischenkörper E von $L|K$ gilt $L = E(\alpha)$. Denn wegen $E \subseteq L$ und $\alpha \in L$ gilt die Inklusion „$\supseteq$“; andererseits ist $L = K(\alpha)$ wegen $K \subseteq E \subseteq E(\alpha)$ und $\alpha \in E(\alpha)$ ein Teilkörper von $E(\alpha)$, also auch „$\subseteq$“ erfüllt. Da p_E das Minimalpolynom von α über E ist, gilt laut Vorlesung $[E(\alpha) : E] = \deg(p_E)$, somit auch $[L : E] = \deg(p_E)$.

zu (b) Laut Vorlesung ist das Minimalpolynom p_E ein Teiler jedes Polynoms $f \in E[x]$ mit $f(\alpha) = 0$. Dies wenden wir auf das Polynom $f = p_F$ an. Dieses Polynom liegt in $F[x]$, ist wegen $F \subseteq E$ also auch in $E[x]$ enthalten, und es erfüllt die Bedingung $p_F(\alpha) = 0$. Also ist p_E ein Teiler von p_F.

zu (c) Sei $m = \deg(p_E)$, und seien $a_0, .., a_m \in E$ die Koeffizienten von p_E. Dann gilt nach Definition (und wegen $K \subseteq E$ sowie $a_j \in E$ für $0 \leq j \leq m$) die Inklusion $F = K(a_0, ..., a_m) \subseteq E$. Nach Teil (b) gilt somit $p_E \mid p_F$. Andererseits gilt auch $p_E \in F[x]$, weil die Koeffizienten von p_E alle in F liegen, außerdem $p_E(\alpha) = 0$. Somit ist p_F auch ein Teiler von p_E.

Dies zeigt insgesamt, dass sich p_E und p_F nur um einen Faktor in $E^\times$ unterscheiden. Weil p_F und p_E als Minimalpolynome beide normiert sind, muss dieser Faktor gleich 1 sein. Daraus folgt $p_F = p_E$. Weil E und F beides Zwischenkörper von $L|K$ sind, gilt $L = F(\alpha) = E(\alpha)$, wie in Teil (a) gezeigt. Daraus folgt $[L : F] = [F(\alpha) : F] = \deg(p_F) = \deg(p_E) = [E(\alpha) : E] = [L : E]$. Mit der Gradformel, angewendet auf den Zwischenkörper E der Erweiterung $L|F$, erhalten wir

$$[E : F] \quad = \quad \frac{[L : F]}{[L : E]} \quad = \quad 1.$$

Aus $F \subseteq E$ und $[E : F] = 1$ wiederum folgt $F = E$.

Aufgabe F21T1A4

Gegeben sei die Gruppe der invertierbaren 3×3-Matrizen über dem Körper mit 2 Elementen

$$G = \mathrm{GL}_3(\mathbb{F}_2).$$

(a) Verifizieren Sie, dass G die Ordnung 168 hat.

(b) Bestimmen Sie eine 2-Sylowgruppe von G.
Hinweis: Betrachten Sie die Dreiecksmatrizen in G.

(c) Wieviele 2-Sylowgruppen hat G?
Hinweis: Betrachten Sie den Stabilisator einer 2-Sylowgruppe.

Lösung:
zu (a) Sei $A \in \mathcal{M}_{3,\mathbb{F}_2}$ eine 3×3-Matrix über $\mathbb{F}_2$, und seien $v_1, v_2, v_3 \in \mathbb{F}_2^3$ die Spaltenvektoren von A. Laut Vorlesung ist A genau dann invertierbar, also in G enthalten, wenn das Tupel (v_1, v_2, v_3) linear unabhängig ist. Dies wiederum ist genau dann der Fall, wenn $v_1 \in \mathbb{F}_2^3 \setminus \{0_{\mathbb{F}_2^3}\}$, $v_2 \in \mathbb{F}_2^3 \setminus \mathrm{lin}\{v_1\}$ und $v_3 \in \mathbb{F}_2^3 \setminus \mathrm{lin}\{v_1, v_2\}$ gilt. Für die Wahl von v_1 gibt es $|\mathbb{F}_2^3 \setminus \{0_{\mathbb{F}_2^3}\}| = 2^3 - 1 = 7$ Möglichkeiten, danach noch $|\mathbb{F}_2^3 \setminus \mathrm{lin}\{v_1\}| = 2^3 - 2^1 = 6$ Möglichkeiten für die Wahl von v_2 und nach Wahl von (v_1, v_2) noch $|\mathbb{F}_2^3 \setminus \mathrm{lin}\{v_1, v_2\}| = 2^3 - 2^2 = 4$ Möglichkeiten für v_3. Ingesamt gibt es also $7 \cdot 6 \cdot 4 = 168$ linear unabhängige Tupel, und somit gilt auch $|G| = 168$.

zu (b) Wegen $168 = 2^3 \cdot 3^1 \cdot 7^1$ sind die 2-Sylowgruppen von G genau die Untergruppen von G der Ordnung 8. Wir zeigen, dass

$$P \quad = \quad \left\{ \begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F}_2 \right\}$$

eine Untergruppe der Ordnung 8 von G ist. Zunächst ist klar, dass die Teilmenge P aus $2^3 = 8$ Elementen besteht, da es für die Wahl von $a, b, c \in \mathbb{F}_2$ in einer Matrix der angegeben Form jeweils zwei Möglichkeiten gibt. Die Gleichung

$$\begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} \bar{1} & a_1 & b_1 \\ \bar{0} & \bar{1} & c_1 \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \quad = \quad \begin{pmatrix} \bar{1} & a + a_1 & b + ac_1 + b_1 \\ \bar{0} & \bar{1} & c + c_1 \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

für $a, b, c, a_1, b_1, c_1 \in \mathbb{F}_2$ zeigt, dass das Produkt zweier Elemente aus P wiederum in P enthalten, die Teilmenge P unter der Verknüpfung von G also abgeschlossen ist. Zu zeigen ist noch die Abgeschlossenheit unter Inversenbildung. Sei dazu $A \in P$ vorgegeben. Als Element der endlichen Gruppe G besitzt A eine endliche Ordnung m. Die Gleichung $A^{m-1} \cdot A = A^m = E$ (wobei E die Einheitsmatrix bezeichnet) zeigt, dass $A^{m-1} = A^{-1}$ gilt, und auf Grund der Abgeschlossenheit von P unter der Verknüpfung von G ist A^{m-1} und somit auch A^{-1} in P enthalten. Insgesamt ist P also eine Untergruppe der Ordnung 8 von G und somit eine 2-Sylowgruppe.

zu (c) Der Stabilsator der 2-Sylowgruppe P aus Teil (b) unter der Operation von G auf der Menge der 2-Sylowgruppen durch Konjugation ist der Normalisator $N_G(P)$ von P in G, und die Anzahl der 2-Sylowgruppen ist durch $\nu_2 = (G : N_G(P))$ gegeben. Aus der Definition der Normalisators ergibt sich unmittelbar, dass $P \subseteq N_G(P)$ gilt. Wir zeigen, dass umgekehrt auch $N_G(P) \subseteq P$ erfüllt ist. Sei dazu $T \in N_G(P)$ vorgegeben, und bezeichnen wir die drei Spalten von T mit u, v, w. Auf Grund der

Invertierbarkeit von T ist $\mathcal{B} = (u, v, w)$ eine geordnete Basis $\mathbb{F}_2^3$, und laut Vorlesung ist T die Matrix des Basiswechsels $\mathcal{T}_{\mathcal{E}}^{\mathcal{B}}$ von $\mathcal{B}$ zur Einheitsbasis $\mathcal{E} = (e_1, e_2, e_3)$. Nach Definition des Normalisators gilt $TAT^{-1} \in P$ für alle $A \in P$. Dabei ist jeweils $TAT^{-1} = \mathcal{M}_{\mathcal{B}}(\phi_A)$, die Darstellungsmatrix der linearen Abbildung $\phi_A : \mathbb{F}_2^3 \to \mathbb{F}_2^3$, $v' \mapsto Av'$ bezüglich der Basis $\mathcal{B}$. Wegen $TAT^{-1} \in P$ für beliebiges gibt es jeweils $a, b, c \in \mathbb{F}_2$ mit

$$\mathcal{M}_{\mathcal{B}}(\phi_A) \quad = \quad TAT^{-1} \quad = \quad \begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}.$$

An der ersten und zweiten Spalte dieser Matrix kann abgelesen werden, dass jeweils $\phi_A(u) = u$ und $\phi_A(v) = au + v$ gilt; die Differenz $\phi_A(v) - v$ ist also jeweils in $\mathrm{lin}(u)$ enthalten. Wir betrachten nun in P speziell die Elemente

$$A_1 = \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \quad , \quad A_2 = \begin{pmatrix} \bar{1} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \quad \text{und} \quad A_3 = \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}.$$

Für den Vektor $u = (u_1, u_2, u_3)$ gilt nun insbesondere

$$\begin{pmatrix} u_1 + u_2 \\ u_2 \\ u_3 \end{pmatrix} = \phi_{A_1}(u) = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} u_1 + u_3 \\ u_2 \\ u_3 \end{pmatrix} = \phi_{A_2}(u) = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \quad ,$$

also $u_2 = u_3 = \bar{0}$. Für den Vektor $v = (v_1, v_2, v_3)$ liegt die Differenz

$$\begin{pmatrix} \bar{0} \\ v_3 \\ \bar{0} \end{pmatrix} \quad = \quad \begin{pmatrix} v_1 \\ v_2 + v_3 \\ v_3 \end{pmatrix} - \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \quad = \quad \phi_{A_3}(v) - v$$

in $\mathrm{lin}(u) \subseteq \mathrm{lin}(e_1)$, es gilt also $v_3 = \bar{0}$. Dies zeigt, dass die Matrix T die Form

$$T \quad = \quad \begin{pmatrix} u_1 & v_1 & w_1 \\ \bar{0} & v_2 & w_2 \\ \bar{0} & \bar{0} & w_3 \end{pmatrix}$$

hat. Weil T invertierbar ist, müssen die Diagonaleinträge u_1, v_2 und w_3 gleich $\bar{1}$ sein. Also ist T insgesamt in P enthalten. Damit ist die Gleichheit $N_G(P) = P$ nachgewiesen, und es folgt $\nu_2 = (G : N_G(P)) = (G : P) = \frac{|G|}{|P|} = \frac{168}{8} = 21$. Es gibt also genau 21 2-Sylowgruppen in G.

Aufgabe F21T1A5

Sei K ein Körper der Charakteristik 0 und $K(\alpha,\beta)|K$ eine endliche Galois-Erweiterung. Seien weiter $K(\alpha)|K$ und $K(\beta)|K$ Galois-Erweiterungen, sowie $K(\alpha)\cap K(\beta)=K$. Setze $G=\mathrm{Gal}(K(\alpha,\beta)|K(\alpha+\beta))$. Zeigen Sie:

(a) Für $\sigma\in G$ gilt: $\sigma(\alpha)-\alpha=\beta-\sigma(\beta)\in K$

(b) Es ist $K(\alpha+\beta)=K(\alpha,\beta)$.

Hinweis zu (b): Berechnen Sie zunächst $\sigma^j(\alpha)$ unter Verwendung von (a).

Lösung:
zu (a) Sei $\sigma\in G$. Als Automorphismus von $K(\alpha,\beta)$ ist σ verträglich mit der Addition. Außerdem wird das Element $\alpha+\beta$ auf sich selbst abgebildet, da σ nach Definition von G ein $K(\alpha+\beta)$-Automorphismus ist. Daraus folgt insgesamt $\alpha+\beta=\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$, was zu $\sigma(\alpha)-\alpha=\beta-\sigma(\beta)$ umgeformt werden kann.

Die Einschränkung $\sigma|_{K(\alpha)}$ kann als K-Homomorphismus $K(\alpha)\to K(\alpha,\beta)$ aufgefasst werden, somit auch aus K-Homomorphismus in einen algebraischen Abschluss von $K(\alpha,\beta)$. Weil $K(\alpha)|K$ als Galois-Erweiterung insbesondere normal ist, handelt es sich bei $\sigma|_{K(\alpha)}$ somit um einen K-Automorphismus von $K(\alpha)$. Es gilt also $\sigma(\alpha)\in K(\alpha)$ und $\sigma(\alpha)-\alpha\in K(\alpha)$. Genauso zeigt man, dass $\beta-\sigma(\beta)$ in $K(\beta)$ liegt. Insgesamt ist $\sigma(\alpha)-\alpha=\beta-\sigma(\beta)$ somit in $K(\alpha)\cap K(\beta)=K$ enthalten.

zu (b) Sei $\sigma\in G$. Wegen $\sigma(\alpha)-\alpha\in K$ gilt $\sigma^2(\alpha)-\sigma(\alpha)=\sigma(\sigma(\alpha)-\alpha)=\sigma(\alpha)-\alpha$, was zu $\sigma^2(\alpha)=2\sigma(\alpha)-\alpha$ umgeformt werden kann. Anwendung von σ auf beide Seiten liefert $\sigma^3(\alpha)=2\sigma^2(\alpha)-\sigma(\alpha)=2(2\sigma(\alpha)-\alpha)-\sigma(\alpha)=4\sigma(\alpha)-2\alpha-\sigma(\alpha)=3\sigma(\alpha)-2\alpha$. Wir beweisen nun durch vollständige Induktion, dass

$$\sigma^m(\alpha) \quad = \quad m\sigma(\alpha)-(m-1)\alpha \qquad \text{für alle } m\in\mathbb{N} \text{ gilt.}$$

Für $m=1$ ist die Gleichung wegen $\sigma^1(\alpha)=\sigma(\alpha)=1\cdot\sigma(\alpha)-(1-1)\alpha$ offenbar erfüllt. Sei nun $m\in\mathbb{N}$, und setzen wir die Gleichung voraus. Durch Anwendung von σ auf beide Seiten erhalten wir

$$\sigma^{m+1}(\alpha) \quad = \quad \sigma\left(m\sigma(\alpha)-(m-1)\alpha\right) \quad = \quad m\sigma^2(\alpha)-(m-1)\sigma(\alpha) \quad =$$
$$m(2\sigma(\alpha)-\alpha)-(m-1)\sigma(\alpha) \quad = \quad 2m\sigma(\alpha)-m\alpha-(m-1)\sigma(\alpha) \quad = \quad (m+1)\sigma(\alpha)-m\alpha \quad ,$$

wodurch die Gleichung für $m+1$ bewiesen ist.

Nach Voraussetzung ist $K(\alpha,\beta)|K$ und damit auch $K(\alpha,\beta)|K(\alpha+\beta)$ eine endliche Galois-Erweiterung. Daraus folgt, dass die Galois-Gruppe G dieser Erweiterung eine endliche Ordnung n besitzt, und somit $\sigma^n=\mathrm{id}_{K(\alpha,\beta)}$ gilt. Mit Hilfe der soeben bewiesenen Gleichung erhalten wir $\alpha=\mathrm{id}_{K(\alpha,\beta)}(\alpha)=\sigma^n(\alpha)=n\sigma(\alpha)-(n-1)\alpha$, was zu $n\alpha=n\sigma(\alpha)$ und $\alpha=\sigma(\alpha)$ umgestellt werden kann. Dieselbe Argumentation zeigt, dass auch $\sigma(\beta)=\beta$ gilt. Weil der K-Homomorphismus σ auf $K(\alpha,\beta)$ durch die Bilder von α und β bereits eindeutig festgelegt ist, folgt $\sigma=\mathrm{id}_{K(\alpha,\beta)}$. Weil σ als Element von G beliebig vorgegeben war, haben wir damit gezeigt, dass $\mathrm{Gal}(K(\alpha,\beta)|K(\alpha+\beta))=G=\{\mathrm{id}_{K(\alpha,\beta)}\}$ gilt. Da $K(\alpha,\beta)|K$ eine Galois-Erweiterung ist, folgt daraus $\mathrm{Gal}(K(\alpha,\beta)|K(\alpha+\beta))=[K(\alpha,\beta):K(\alpha+\beta)]=1$ und $K(\alpha,\beta)=K(\alpha+\beta)$.

Aufgabe F21T2A1

(a) Begründen Sie, dass die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 8 & 3 & 9 & 1 & 6 & 4 & 2 \end{pmatrix} \in S_9$$

in der alternierenden Gruppe A_9 liegt.

(b) Zeigen Sie, dass $\varphi(n)$ für $n \geq 3$ stets gerade ist - hierbei bezeichne φ die Eulersche φ-Funktion.

(c) Begründen Sie, dass in einem Integritätsbereich R aus $e^2 = e$, wobei $e \in R$, stets $e = 0$ oder $e = 1$ folgt.

(d) Bestimmen Sie den Körpergrad $[\mathbb{Q}(\sqrt[5]{7} \cdot e^{-2\pi i/5}) : \mathbb{Q}]$.

Lösung:
zu (a) Das Element σ besitzt die Darstellung $\sigma = (1\,7\,6)(2\,5\,9)(3\,8\,4)$ als Produkt disjunkte Zyklen. Bekanntlich hat für $n \in \mathbb{N}$ und $2 \leq k \leq n$ jeder k-Zykel in S_n das Signum $(-1)^{k-1}$. Daraus folgt $\operatorname{sgn}(\sigma) = \operatorname{sgn}((1\,7\,6)(2\,5\,9)(3\,8\,4)) = \operatorname{sgn}((1\,7\,6)) \cdot \operatorname{sgn}((2\,5\,9)) \cdot \operatorname{sgn}((3\,8\,4)) = (-1)^2 \cdot (-1)^2 \cdot (-1)^2 = 1$. Da A_9 genau aus den Elementen von S_9 mit positivem Signum besteht, folgt $\sigma \in A_9$.

zu (b) Sei $n \in \mathbb{N}$ mit $n \geq 3$ und $n = 2^e \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n (wobei $r \in \mathbb{N}_0$, $p_1, ..., p_r$ ungerade Primzahlen, $e \in \mathbb{N}_0$ und $e_1, ..., e_r \in \mathbb{N}$ sind). Auf Grund der Rechenregeln für die Eulersche φ-Funktion gilt

$$\varphi(n) \quad = \quad \varphi(2^e) \prod_{i=1}^{r} \varphi(p_i^{e_i}) \quad = \quad \varphi(2^e) \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1).$$

Wegen $n \geq 3$ gilt $e \geq 2$ oder $r \geq 1$. Im Fall $e \geq 2$ ist der Faktor $\varphi(2^e) = 2^{e-1}$ gerade, im Fall $r \geq 1$ ist $p_1^{e_1 - 1}(p_1 - 1)$ gerade. In beiden Fällen ist $\varphi(n)$ also eine gerade Zahl.

zu (c) Angenommen, es gilt $e^2 = e$ und $e \neq 0_R$. Die Gleichung kann zu $e(e - 1_R) = e^2 - e = 0_R$ umgestellt werden. Da R ein Integritätsbereich und e laut Annahme ungleich 0_R ist, kann die Kürzungsregel angewendet werden und liefert $e - 1_R = 0_R$, was wiederum zu $e = 1_R$ äquivalent ist.

zu (d) Sei $g = x^5 - 7 \in \mathbb{Q}[x]$ und $\alpha = \sqrt[5]{7} \cdot e^{-2\pi i/5}$. Dann gilt $g(\alpha) = g(\sqrt[5]{7} \cdot e^{-2\pi i/5}) = (\sqrt[5]{7} \cdot e^{-2\pi i/5})^5 - 7 = (\sqrt[5]{7})^5 \cdot (e^{-2\pi i/5})^5 - 7 = 7 \cdot e^{-2\pi i} - 7 = 7 \cdot 1 - 7 = 0$. Nach dem Eisenstein-Kriterium, angewendet auf die Primzahl $p = 7$, ist g in $\mathbb{Q}[x]$ irreduzibel, außerdem normiert. Insgesamt ist g also das Minimalpolynom von α über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \operatorname{grad}(g) = 5$.

Aufgabe F21T2A2

Sei K ein Körper und K^K die Menge aller Abbildungen $K \to K$. Es sei die Abbildung

$$\varphi : K[x] \to K^K \quad , \quad f \mapsto \varphi(f)$$

betrachtet, wobei $\varphi(f)(a) = f(a)$ für alle $a \in K$ gelte. Beweisen Sie:

(a) Genau dann ist φ injektiv, wenn K unendlich ist.

(b) Genau dann ist φ surjektiv, wenn K endlich ist.

Lösung:
zu (a) „⇒“ Angenommen, φ ist injektiv, der Körper K aber endlich. Dann ist K^K eine endliche Menge, denn für jedes $\alpha \in K^K$ ist der Definitionsbereich K von α endlich, und für jedes $c \in K$ gibt es jeweils nur endlich viele Möglichkeiten für das Bild $\alpha(c)$ (nämlich $|K|$ Stück). Dagegen ist $K[x]$ unendlich, da zum Beispiel die Polynome x^n mit $n \in \mathbb{N}_0$ alle verschieden sind. Es gibt aber keine injektive Abbildung von einer unendlichen in eine endliche Menge.

„⇐“ Bekanntlich sind $K[x]$ und K^K beides K-Vektorräume. Wir zeigen, dass durch φ eine lineare Abbildung gegeben ist. Seien dazu $f, g \in K[x]$ und $\lambda \in K$ vorgegeben. Dann gilt für alle $a \in K$ jeweils

$$\varphi(f+g)(a) \quad = \quad (f+g)(a) \quad = \quad f(a)+g(a) \quad = \quad \varphi(f)(a)+\varphi(g)(a) \quad = \quad (\varphi(f)+\varphi(g))(a) \quad ,$$

also $\varphi(f+g) = \varphi(f)+\varphi(g)$. Ebenso gilt für alle $a \in K$ jeweils $\varphi(\lambda f)(a) = (\lambda f)(a) = \lambda f(a) = \lambda\varphi(f)(a) = (\lambda\varphi(f))(a)$ und somit $\varphi(\lambda f) = \lambda\varphi(f)$. Damit ist die Linearität nachgewiesen.

Setzen wir nun voraus, dass K unendlich ist. Für die Injektivität von φ genügt es auf Grund der Linearität zu zeigen, dass $\ker(\varphi) = \{0_K\}$ gilt. Die Inklusion „⊇“ ist (ebenfalls auf Grund der Linearität) offensichtlich. Zum Nachweis von „⊆“ sei $f \in \ker(\varphi)$ vorgegeben. Dann ist $\varphi(f) \in K^K$ die Nullabbildung, es gilt also $\varphi(f)(a) = 0_K$ für alle $a \in K$. Da K unendlich ist, hat f also unendlich viele Nullstellen. Wäre $f \neq 0_K$ und $n = \mathrm{grad}(f) \in \mathbb{N}_0$, dann hätte f laut Vorlesung in K höchstens n Nullstellen. So aber muss f das Nullpolynom sein. Damit ist die Injektivität von φ nachgewiesen.

zu (b) „⇒“ Nehmen wir an, φ ist surjektiv, der Körper K aber unendlich. Sei $a \in K$ beliebig gewählt und $\alpha \in K^K$ gegeben durch $\alpha(a) = 1_K$ sowie $\alpha(c) = 0_K$ für alle $c \in K \setminus \{a\}$. Da φ laut Annahme surjektiv ist, existiert ein $f \in K[x]$ mit $\varphi(f) = \alpha$. Wegen $f(a) = \varphi(f)(a) = \alpha(a) = 1_K$ ist f nicht das Nullpolynom. Andererseits besitzt f wegen $f(c) = \varphi(f)(c) = \alpha(c) = 0_K$ für alle $c \in K \setminus \{a\}$ unendlich viele Nullstellen. Wie in Teil (a) gezeigt, folgt daraus, dass f das Nullpolynom ist, im Widerspruch zu unserer vorherigen Feststellung. Der Widerspruch zeigt, dass unsere Annahme falsch war und aus der Surjektivität von φ die Endlichkeit des Körpers K folgt.

„⇐“ Unter der Voraussetzung, dass K endlich ist, beweisen wir die Surjektivität von φ. Sei $q = |K|$, und seien $a_1, ..., a_q \in K$ die Elemente von K. Wir zeigen zunächst, dass für jedes $i \in \{1, ..., q\}$ jeweils ein Polynom $f_i \in K[x]$ mit $f_i(a_i) = 1_K$ und $f_i(a_j) = 0_K$ für alle $j \neq i$ gibt. Setzen wir zunächst $\tilde{f}_i = \prod_{j \neq i}(x - a_j)$, dann gilt $\tilde{f}_i(a_i) \neq 0_K$ und $\tilde{f}_i(a_j) = 0_K$ für $j \neq i$. Definieren wir nun $f_i = \tilde{f}_i(a_i)^{-1}\tilde{f}_i$, dann folgt $f_i(a_i) = 1_K$ und $f_i(a_j) = 0_K$, insgesamt also $f_i(a_j) = \delta_{ij}$ für $1 \leq j \leq n$ (wobei δ_{ij} wie üblich das Kronecker-Delta bezeichnet).

Sei nun $\alpha \in K^K$ vorgegeben und $f = \sum_{i=1}^{q} \alpha(a_i) f_i$. Dann gilt für alle $1 \leq j \leq n$ jeweils

$$f(a_j) \quad = \quad \sum_{i=1}^{q} \alpha(a_i) f_i(a_j) \quad = \quad \sum_{i=1}^{q} \alpha(a_i)\delta_{ij} \quad = \quad \alpha(a_j) \quad ,$$

also $\varphi(f)(a) = f(a) = \alpha(a)$ für alle $a \in K$ und somit $\varphi(f) = \alpha$. Da K^K beliebig vorgegeben war, ist damit ist die Surjektivität von φ nachgewiesen.

Aufgabe F21T2A3

Sei R ein (nicht notwendig kommutativer) Ring mit 1. Ein Element $x \in R$ heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ mit $x^n = 0$ gibt.

(a) Zeigen Sie: Ist der Ring R kommutativ, und ist $u \in R$ eine Einheit sowie $x \in R$ nilpotent, so ist $u + x$ eine Einheit.

(b) Es sei R der Ring der 2×2-Matrizen über $\mathbb{Q}$. Geben Sie mit Begründung ein Beispiel für eine Einheit $u \in R$ und ein nilpotentes Element $x \in R$ an derart, dass $u + x$ keine Einheit ist.

Lösung:

zu (a) Wir zeigen durch vollständige Induktion, dass folgende Aussage für alle $n \in \mathbb{N}$ gilt: Ist u eine Einheit und $x \in R$ ein Element mit $x^n = 0$, dann ist $u + x$ eine Einheit. Für $n = 1$ ist diese Aussage offenbar erfüllt. Ist nämlich $x \in R$ ein Element mit $x^1 = 0$, dann ist $u + x = u + x^1 = u + 0 = u$ eine Einheit. Sei nun $n \in \mathbb{N}$ vorgegeben, und setzen wir die Aussage für dieses n voraus. Sei $x \in R$ ein Element mit $x^{n+1} = 0$ und $u \in R^\times$. Zu zeigen ist, dass es sich bei $u + x$ um eine Einheit handelt.

Setzen wir $y = -x^2$, dann gilt $(u + x)(u - x) = u^2 - x^2 = u^2 + y$. Das Element y erfüllt die Bedingung $y^n = 0$. Denn wegen $n \geq 1$ ist $n - 1 \geq 0$, und es folgt $y^n = (-x^2)^n = (-1)^n x^{2n} = (-1)^n x^{n-1} x^{n+1} = (-1)^n x^{n-1} \cdot 0 = 0$. Weil die Einheiten in R multiplikativ abgeschlossen sind, ist mit u auch u^2 eine Einheit. Auf Grund der Induktionsvoraussetzung ist also $(u + x)(u - x) = u^2 + y$ somit eine Einheit. Es gibt also ein $\varepsilon \in R$ mit $(u + x)(u - x)\varepsilon = 1$. Definieren wir $\varepsilon' = (u - x)\varepsilon \in R$, dann folgt $(u + x)\varepsilon' = 1$. Dies zeigt, dass auch $u + x$ eine Einheit ist. Der Induktionsschritt ist damit abgeschlossen.

zu (b) Seien zum Beispiel $u, x \in R$ gegeben durch

$$u = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Wegen $\det(u) = 1 \neq 0$ ist u eine invertierbare Matrix und somit eine Einheit in R. Außerdem ist

$$x^2 \quad = \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

und x somit nilpotent. Andererseits gilt

$$u + x \quad = \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad ,$$

aber wegen $\det(u + x) = 0$ ist $u + x$ nicht invertierbar und somit keine Einheit in R.

Aufgabe F21T2A4

(a) Zeigen Sie, dass die Galois-Gruppe einer galois'schen Körpererweiterung $L|K$ vom Grad 143 stets zyklisch ist.

(b) Sei $L|K$ eine galois'sche Körpererweiterung vom Grad 55 mit nichtabelscher Galois-Gruppe. Zeigen Sie: Es gibt genau einen echten Zwischenkörper M von $L|K$, so dass $M|K$ eine Galois-Erweiterung ist. Berechnen Sie den Grad $[M : K]$.

Lösung:
zu (a) Sei $G = \mathrm{Gal}(L|K)$, und für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Da $L|K$ eine endliche Galois-Erweiterung ist, gilt $|G| = [L : K] = 143 = 11 \cdot 13$. Auf Grund des 3. Sylowsatzes gilt $\nu_{13} \mid 11$, also $\nu_{13} \in \{1, 11\}$, andererseits aber auch $\nu_{13} \equiv 1 \bmod 13$. Wegen $11 \not\equiv 1 \bmod 13$ folgt $\nu_{13} = 1$. Ebenso gilt $\nu_{11} \mid 13$, also $\nu_{11} \in \{1, 13\}$, außerdem $\nu_{11} \equiv 1 \bmod 11$. Wegen $13 \equiv 2 \not\equiv 1 \bmod 11$ folgt $\nu_{11} = 1$.

Sei nun U die einzige 11- und N die einzige 13-Sylowgruppe von G. Wir zeigen, dass G ein inneres direktes Produkt von U und N ist. Wegen $\nu_{11} = \nu_{13} = 1$ folgt aus dem 2. Sylowsatz $U \trianglelefteq G$ und $N \trianglelefteq G$. Wegen $G = 11^1 \cdot 13^1$ ist (nach Definition der p-Sylowgruppen) $|U| = 11$ und $|N| = 13$, und aus $\mathrm{ggT}(|U|, |N|) = \mathrm{ggT}(11, 13) = 1$ folgt $U \cap N = \{\mathrm{id}_L\}$. Zu zeigen bleibt noch, dass das Komplexprodukt $H = UN$ mit G übereinstimmt. Wegen $N \trianglelefteq G$ ist H jedenfalls eine Untergruppe von G, und wegen $U \subseteq H$ und $N \subseteq H$ sind U und N beides Untergruppen von H. Nach dem Satz von Lagrange ist $|H|$ somit ein gemeinsames Vielfaches von $|U| = 11$ und $|N| = 13$. Es folgt $|H| \geq \mathrm{kgV}(11, 13) = 143 = |G|$, und wegen $H \subseteq G$ folgt daraus $G = H = UN$.

Der Nachweis, dass G ein inneres direktes Produkt von U und N ist, ist damit abgeschlossen, und laut Vorlesung folgt daraus $G \cong U \times N$. Als Gruppen von Primzahlordnung sind U und N zyklisch. Daraus folgt $U \cong \mathbb{Z}/11\mathbb{Z}$ und $N \cong \mathbb{Z}/13\mathbb{Z}$, und wir erhalten $G \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Wegen $\mathrm{ggT}(11, 13) = 1$ kann schließlich der Chinesische Restsatz angewendet werden, und wir erhalten $G \cong \mathbb{Z}/143\mathbb{Z}$. Damit ist gezeigt, dass es sich bei G um eine zyklische Gruppe handelt.

zu (b) Nach Voraussetzung ist $G = \mathrm{Gal}(L|K)$ eine nicht-abelsche Gruppe. Da $L|K$ eine endliche Galois-Erweiterung ist, gilt außerdem $|G| = [L : K] = 55$. Wiederum sei ν_p für jede Primzahl p die Anzahl der p-Sylowgruppen von G. Nach dem 3. Sylowsatz gilt $\nu_{11} \mid 5$, also $\nu_{11} \in \{1, 5\}$, außerdem $\nu_{11} \equiv 1 \bmod 11$. Wegen $5 \not\equiv 1 \bmod 11$ folgt $\nu_{11} = 1$. Ebenso gilt $\nu_5 \mid 11$, also $\nu_5 \in \{1, 11\}$. Wir betrachten zunächst den Fall $\nu_5 = 1$ und zeigen, dass in diesem Fall G eine abelsche Gruppe ist, im Widerspruch zur Voraussetzung. Sei dazu U die einzige 11- und N die einzige 5-Sylowgruppe. Wortwörtlich wie im im letzten Teil (wobei die Primzahl 13 lediglich durch die Primzahl 5 zu ersetzen ist) zeigt man, dass $G \cong U \times N$ gilt. Wegen $|G| = 5^1 \cdot 11^1$ ist $|U| = 11$ und $|N| = 5$. Die Gruppen U und N sind also beide von Primzahlordnung und als solche zyklisch, somit auch abelsch. Daraus folgt, dass auch $U \times N$ und G abelsche Gruppen sind, was der Voraussetzung widerspricht.

Der Fall $\nu_5 = 1$ ist durch den Widerspruch also ausgeschlossen, und es folgt $\nu_5 = 11$. Sei nun $M = L^U$, der Fixkörper der Untergruppe U von $G = \mathrm{Gal}(L|K)$. Nach dem Hauptsatz der Galoistheorie gilt dann $U = \mathrm{Gal}(L|M)$. Als einzige 11-Sylowgruppe ist U ein Normalteiler von G. Daraus folgt, dass $M|K$ eine Galois-Erweiterung ist. Außerdem gilt

$$[M : K] \quad = \quad (G : U) \quad = \quad \frac{|G|}{|U|} \quad = \quad \frac{55}{11} \quad = \quad 5.$$

Nehmen wir nun an, dass M' ein weiterer, von M verschiedener, echter Zwischenkörper von $L|K$ ist mit der Eigenschaft, dass $M'|K$ galoissch ist. Sei $V = \mathrm{Gal}(L|M')$. Wegen $K \subsetneq M' \subsetneq L$ gilt $\{\mathrm{id}_L\} \subsetneq V \subsetneq G$. Somit ist $|V|$ ein echter Teiler von $|G| = 55$ größer als 1. Die einzigen solchen Teiler sind 5 und 11. Betrachten wir zunächst den Fall $|V| = 11$. Dann ist V eine 11-Sylowgruppe von G, und wegen $\nu_{11} = 1$ folgt $V = U$. Mit dem Hauptsatz der Galois-Theorie erhalten wir $M' = L^V = L^U = M$, im Widerspruch zu unserer Annahme $M' \neq M$.

Betrachten wir nun die andere Möglichkeit, $|V| = 5$. Dann ist V eine 5-Sylowgruppe von G. Wegen $\nu_5 = 11 > 1$ kann V kein Normalteiler von G sein. Andererseits folgt aber aus der Annahme, dass $M'|K$ eine normale Teilererweiterung von $L|K$ ist, die Normalteiler-Eigenschaft von $V = \mathrm{Gal}(L|M')$. Dieser Widerspruch zeigt, dass auch der Fall $|V| = 5$ ausgeschlossen ist und somit kein Zwischenkörper $M' \neq M$ mit den angegebenen Eigenschaften existiert.

Aufgabe F21T2A5

(a) Sei K ein Körper, $n \geq 1$ eine natürliche Zahl und A eine beliebige $n \times n$-Matrix über K. Zeigen Sie: Es existiert eine endliche Körpererweiterung $L|K$ derart, dass A einen Eigenwert $\lambda \in L$ besitzt.

(b) Begründen Sie, dass $L = \mathbb{Q}[x]/(x^3+x+1)$ ein Körper ist. Zeigen Sie, dass $\alpha = [x]$ ein Eigenwert der linearen Abbildung $f : L^3 \to L^3$, $f(u, v, w) = (-w, u - w, v)$ ist, und geben Sie einen Eigenvektor zum Eigenwert α an.

Lösung:
zu (a) Sei $\chi_A \in K[x]$ das charakteristische Polynom von A und $f \in K[x]$ ein über K irreduzibler Faktor von A. Laut Vorlesung existiert eine endlich Körpererweiterung $L|K$, so dass f in L eine Nullstelle λ besitzt. Wegen $f \mid \chi_A$ ist λ auch eine Nullstelle von χ_A, und als Nullstelle des charakteristischen Polynoms von A ist $\lambda \in L$ ein Eigenwert von A.

zu (b) Das Polynom $g = x^3 + x + 1$ ist irreduzibel über $\mathbb{Q}$. Wäre es nämlich reduzibel, dann hätte es wegen $\text{grad}(g) = 3$ eine Nullstelle $r \in \mathbb{Q}$. Da g in $\mathbb{Z}[x]$ ist und normiert ist, müsste $r \in \mathbb{Z}$ gelten und r den konstanten Termin 1 von g teilen. Es müsste also $r \in \{\pm 1\}$ gelten. Aber wegen $g(-1) = -1 \neq 0$ und $g(1) = 3 \neq 0$ sind ± 1 keine Nullstellen von g; damit ist die Irreduzibilität von g nachgewiesen. Als Polynomring über einem Körper ist $\mathbb{Q}[x]$ ein Hauptidealring, und auf Grund der Irreduziblität von g ist das Hauptideal (g) ein maximales Ideal in $\mathbb{Q}[x]$. Daraus wiederum folgt, dass $L = \mathbb{Q}[x]/(g)$ ein Körper ist.

Seien e_1, e_2, e_3 die Einheitsvektoren in L^3. Es gilt $f(e_1) = f(1, 0, 0) = (0, 1, 0) = e_2$, $f(e_2) = f(0, 1, 0) = (0, 0, 1) = e_3$ und $f(e_3) = f(0, 0, 1) = (-1, -1, 0) = -e_1 - e_2$. Somit ist die Abbildung f gegeben durch $L^3 \mapsto L^3$, $v \mapsto Av$, wobei $A \in \mathcal{M}_{3\times 3,L}$ die Matrix mit den Spalten $e_2, e_3, -e_1 - e_2$ bezeichnet, also

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

Das charakteristische Polynom von f ist somit gleich dem charakteristischen Polynom von A, und dieses ist gegeben durch

$$\chi_A \quad = \quad \det(xE - A) \quad = \quad \det \begin{pmatrix} x & 0 & 1 \\ -1 & x & 1 \\ 0 & -1 & x \end{pmatrix} \quad = \quad x^3 + 0 + 1 - 0 - (-x) - 0 \quad = \quad x^3 + x + 1$$

wobei $E \in \mathcal{M}_{3\times 3,L}$ die Einheitsmatrix bezeichnet. Es gilt also $\chi_A = g$. Als Nullstelle von χ_A ist α ein Eigenwert von f. Die Eigenvektoren zum Eigenwert α sind genau die Elemente ungleich dem Nullvektor in $\text{Eig}(f, \alpha) = \text{Eig}(A, \alpha) = \ker(A - \alpha E)$. Wir bestimmen einen solchen Vektor durch Anwendung des Gauß-Algorithmus.

$$\begin{pmatrix} -\alpha & 0 & -1 \\ 1 & -\alpha & -1 \\ 0 & 1 & -\alpha \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & -\alpha & -1 \\ 0 & 1 & -\alpha \\ -\alpha & 0 & -1 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & -\alpha & -1 \\ 0 & 1 & -\alpha \\ 0 & -\alpha^2 & -\alpha - 1 \end{pmatrix} \quad \mapsto$$

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

Die beiden ersten Zeilen der umgeformten Matrix rechts entsprechen den Gleichungen $x_1 = (\alpha^2 + 1)x_3$ und $x_2 = \alpha x_3$. Dies zeigt, dass zum Beispiel $(\alpha^2 + 1, \alpha, 1)$ ein Eigenvektor zum Eigenwert λ ist. Wir überprüfen diese Ergebnis durch eine Proberechnung. Es gilt

$$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha^2 + 1 \\ \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ \alpha^2 \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha^3 + \alpha \\ \alpha^2 \\ \alpha \end{pmatrix} = \alpha \begin{pmatrix} \alpha^2 + 1 \\ \alpha \\ 1 \end{pmatrix} ,$$

wobei im vorletzten Schritt in der ersten Komponente des Vektors noch zu beachten ist, dass $\alpha^3 + \alpha = (\alpha^3 + \alpha + 1) - 1 = g(\alpha) - 1 = 0 - 1 = -1$ gilt.

Aufgabe F21T3A1

(a) Zeigen Sie, dass durch

$$K = \mathbb{F}_7[t]/(t^3 - 2)$$

ein Körper mit 343 Elementen gegeben wird.

(b) Bestimmen Sie das Minimalpolynom der komplexen Zahl $z = \pi + ei$ über $\mathbb{R}$.

(c) Zeigen oder widerlegen Sie, dass das Polynom

$$f = x^{2021} + 105x^{103} + 15x + 45$$

über folgenden Körpern irreduzibel ist:

(i) $K = \mathbb{Q}$

(ii) $K = \mathbb{R}$

(iii) $K = \mathbb{F}_2$

(iv) $K = \mathbb{Q}[t]/(f)$

(v) Begründen Sie, dass $\mathbb{Q}[t]/(f)$ ein Körper ist.

Lösung:
zu (a) Das Polynom $f = t^3 - \bar{2} = t^3 + \bar{5} \in \mathbb{F}_7[x]$ besitzt in $\mathbb{F}_7$ keine Nullstelle, denn es gilt $f(\bar{0}) = \bar{5} \neq \bar{0}$, $f(\bar{1}) = \bar{6} \neq \bar{0}$, $f(\bar{2}) = \overline{13} = \bar{6} \neq \bar{0}$, $f(\bar{3}) = \overline{32} = \bar{4} \neq \bar{0}$, $f(\bar{4}) = \overline{69} = \bar{6} \neq \bar{0}$, $f(\bar{5}) = f(-\bar{2}) = -\bar{3} = \bar{4} \neq \bar{0}$ und $f(\bar{6}) = f(-\bar{1}) = \bar{4} \neq \bar{0}$. Wegen $\text{grad}(f) = 3$ folgt daraus, dass f über $\mathbb{F}_7$ irreduzibel ist. Da $\mathbb{F}_7[t]$ als Polynomring über einem Körper ein Hauptidealring ist, ist jedes von einem irreduziblen Element erzeugte Ideal maximal. Also ist (f) ein maximales Ideal, und $K = \mathbb{F}_7[t]/(f)$ ist ein Körper. Aus der Vorlesung ist außerdem bekannt: Ist K ein Körper und $0 \neq g \in K[x]$ vom Grad n, dann bilden die Polynome vom Grad $\leq n - 1$ zusammen mit dem Nullpolynom ein Repräsentantensystem von $K[x]/(g)$. Insbesondere bilden die Polynome vom Grad ≤ 2 also ein Repräsentantensystem von $\mathbb{F}_7[t]/(f)$. Jedes dieser Polynome hat die Form $ax^2 + bx + c$ mit eindeutig bestimmten $a, b, c \in \mathbb{F}_7$. Für jeden der Koeffizienten gibt es also genau sieben Möglichkeiten, und $7^3 = 343$ mögliche Kombinationen. Dies zeigt, dass das Repräsentantensytem, und damit auch der Faktorring $K = \mathbb{F}_7[t]/(f)$, aus genau 343 Elementen besteht.

zu (b) Es gilt $z = \pi + ei \Rightarrow z - \pi = ei \Rightarrow (z - \pi)^2 = -e^2 \Rightarrow z^2 - 2\pi z + \pi^2 + e^2 = 0$. Dies zeigt, dass $\pi + ei$ eine Nullstelle des Polynoms $f = x^2 - 2\pi x + \pi^2 + e^2 \in \mathbb{R}[x]$ ist. Außerdem ist f normiert. Wäre f über $\mathbb{R}$ reduzibel, dann müsste wegen $\text{grad}(f) = 2$ die Nullstelle $\pi + ei$ in $\mathbb{R}$ liegen. Aber dies ist wegen $\text{Im}(\pi + ei) = e \neq 0$ nicht der Fall. Insgesamt ist damit gezeigt, dass f das Minimalpolynom von $\pi + ei$ über $\mathbb{R}$ ist.

zu (c)(i) Die Primzahl 5 teilt nicht den Leitkoeffizienten 1 von f, wegen $5 \bmod 105$, $5 \mid 15$, $5 \mid 45$ aber jeden anderen Koeffizienten des Polynoms, und 5^2 ist kein Teiler von $45 = 3^2 \cdot 5^1$. Also folgt die Irreduzibilität von f über $\mathbb{Z}$ aus dem Eisenstein-Kriterium. Nach dem Gauß'schen Lemma ist f damit auch irreduzibel über $\mathbb{Q}$.

zu (c)(ii) Aus der Analysis ist bekannt, dass jedes reelle Polynom ungeraden Grades mindestens eine reelle Nullstelle besitzt. Der Grad 2021 von f ist ungerade. Als Polynom vom Grad > 1 mit mindestens einer Nullstelle in $\mathbb{R}$ ist f über $\mathbb{R}$ reduzibel (also nicht irreduzibel).

zu (c)(iii) Es gilt $f(\bar{1}) = \bar{1}^{2021} + \overline{105} \cdot \bar{1}^{103} + \overline{15} \cdot \bar{1} + \overline{45} = \bar{1} + \overline{105} + \overline{15} + \overline{45} = \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{4} = \bar{0}$. Als Polynom vom Grad > 1, das in $\mathbb{F}_2$ eine Nullstelle besitzt, ist f über $\mathbb{F}_2$ reduzibel.

zu (c)(iv) Sei $\alpha = t + (f)$. Identifizieren wir $\mathbb{Q}$ mit einem Teilkörper von K durch die die injektive Abbildung $\mathbb{Q} \to K$, $a \mapsto a + (f)$, dann erhalten wir

$$\begin{aligned} f(\alpha) &= \alpha^{2021} + 105\alpha^3 + 15\alpha + 45 = (t + (f))^{2021} + 105(t + (f))^3 + 15(t + (f)) + (45 + (f)) \\ &= t^{2021} + 105t^3 + 15t + 45 + (f) = f + (f) = 0 + (f) = 0. \end{aligned}$$

Es handelt sich bei f also um ein Polynom in $K[x]$ vom Grad > 1, das mit α in K eine Nullstelle besitzt. Daraus folgt, dass f über K reduzibel ist.

zu (c)(v) Als Polynomring über einem Körper ist $\mathbb{Q}[t]$ ein Hauptidealring. Weil f nach Teil (c)(i) in $\mathbb{Q}[t]$ irreduzibel ist, ist das Hauptideal (f) in $\mathbb{Q}[t]$ ein maximales Ideal. Daraus folgt, dass der Faktorring $K = \mathbb{Q}[t]/(f)$ ein Körper ist.

Aufgabe F21T3A2

(a) Bestimmen Sie alle Nullstellen (mit Vielfachheiten) des Polynoms $f = x^4 + \bar{2}$ über $\mathbb{F}_3$.

(b) Bestimmen Sie die Galois-Gruppe von f über $\mathbb{F}_3$.

(c) Sei α eine Nullstelle von $g = x^4 + \bar{2}$ in einem algebraischen Abschluss von $\mathbb{F}_5$. Zeigen Sie, dass dann auch $\bar{2}\alpha$, $\bar{3}\alpha$ und $\bar{4}\alpha$ Nullstellen von g sind.

(d) Zeigen Sie, dass g über $\mathbb{F}_5$ irreduzibel ist.

(e) Berechnen Sie die Galois-Gruppe von g über $\mathbb{F}_5$.

Lösung:
zu (a) Es gilt $f(\bar{0}) = \bar{2} \neq \bar{0}$, $f(\bar{1}) = \bar{3} = \bar{0}$ und $f(\bar{2}) = \overline{18} = \bar{0}$. Die Ableitung von f ist $f' = \bar{4}x^3 = x^3$, und es gilt $f'(\bar{1}) = \bar{1} \neq \bar{0}$ und $f'(\bar{2}) = \bar{8} = \bar{2} \neq \bar{0}$. Insgesamt zeigt dies, dass $\bar{1}$ und $\bar{2}$ die einzigen Nullstellen von f in $\mathbb{F}_3$ sind, jeweils mit Vielfachheit 1.

zu (b) Aus Teil (a) folgt, dass f eine Zerlegung der Form $f = (x - \bar{1})(x - \bar{2})g$ besitzt, mit einem normierten, irreduziblen Polynom vom Grad 2. Sei $\mathbb{F}_3^{\text{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_3$ und $\alpha \in \mathbb{F}_3^{\text{alg}}$ eine Nullstelle von g. Da $x - \alpha$ ein Teiler von g in $\mathbb{F}_3(\alpha)[x]$ ist, existiert ein Polynom $h \in \mathbb{F}_3(\alpha)[x]$ vom Grad 1 mit $g = (x-\alpha)h$. Das Polynom g zerfällt über $\mathbb{F}_3(\alpha)$ also in Linearfaktoren, ebenso das Polynom f. Andererseits wird der Körper $\mathbb{F}_3(\alpha)$ über $\mathbb{F}_3$ durch die Nullstellen von f erzeugt, da α nicht nur eine Nullstelle von g, sondern auch eine Nullstelle von f ist.

Insgesamt handelt es sich bei $\mathbb{F}_3(\alpha)$ also um einen Zerfällungskörper von f über $\mathbb{F}_3$, und es folgt $\text{Gal}(f|\mathbb{F}_3) = \text{Gal}(\mathbb{F}_3(\alpha)|\mathbb{F}_3)$. Das Polynom g ist normiert, irreduzibel und hat α als Nullstelle. Es ist also das Minimalpolynom von α über $\mathbb{F}_3$, und folglich gilt $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \text{grad}(g) = 2$. Aus der Vorlesung ist bekannt, dass für jeden endlichen Körper F jede Erweiterung $E|F$ von einem endlichen Grad n galoissch ist, und dass jeweils $\text{Gal}(E|F) \cong \mathbb{Z}/n\mathbb{Z}$ gilt. Damit erhalten wir $\text{Gal}(f|\mathbb{F}_3) = \text{Gal}(\mathbb{F}_3(\alpha)|\mathbb{F}_3) \cong \mathbb{Z}/2\mathbb{Z}$.

zu (c) In $\mathbb{F}_5$ gilt $\bar{2}^4 = \overline{16} = \bar{1}$, $\bar{3}^4 = \overline{81} = \bar{1}$ und $\bar{4}^4 = (-\bar{1})^4 = \bar{1}$. Aus $g(\alpha) = \bar{0}$ folgt für alle $c \in \{\bar{2}, \bar{3}, \bar{4}\}$ also $g(c\alpha) = (c\alpha)^4 + \bar{2} = \bar{1} \cdot \alpha^4 + \bar{2} = g(\alpha) = \bar{0}$.

zu (d) Sei $h \in \mathbb{F}_5[x]$ das Minimalpolynom von α über $\mathbb{F}_5$ und $d = [\mathbb{F}_5(\alpha) : \mathbb{F}_5]$. Dann gilt $\text{grad}(h) = [\mathbb{F}_5(\alpha) : \mathbb{F}_5] = d$. Als d-dimensionaler $\mathbb{F}_5$-Vektorraum besteht $\mathbb{F}_5(\alpha)$ aus 5^d Elementen. Bezeichnen wir den in Teil (c) erwähnten algebraischen Abschluss, in dem α sich befindet, mit $\mathbb{F}_5^{\text{alg}}$, dann stimmt $\mathbb{F}_5(\alpha)$ also mit dem eindeutig bestimmten Zwischenkörper $\mathbb{F}_{5^d}$ von $\mathbb{F}_5^{\text{alg}}|\mathbb{F}_5$ mit 5^d Elementen überein. Die multiplikative Gruppe $\mathbb{F}_{5^d}^\times$ besteht aus $5^d - 1$ Elementen. Wegen $g(\bar{0}) = \bar{2} \neq \bar{0}$ ist $\alpha \neq \bar{0}$, und folglich ist α in $\mathbb{F}_{5^d}^\times$ enthalten.

Wegen $g \in \mathbb{F}_5[x]$ und $g(\alpha) = 0$ ist h ein Teiler von g, es gilt also $d = \text{grad}(h) \leq \text{grad}(g) = 4$ und somit $d \in \{1, 2, 3, 4\}$. Wegen $g(\alpha) = \bar{0}$ gilt außerdem $\alpha^4 = \bar{3} \neq \bar{1}$, $\alpha^8 = (\bar{3})^2 = \bar{9} = \bar{4} \neq \bar{1}$ und $\alpha^{16} = \bar{4}^2 = \bar{1}$. Dies zeigt, dass α in $\mathbb{F}_{5^d}^\times$ ein Element der Ordnung 16 ist. Nach dem Satz von Lagrange muss 16 also ein Teiler von $5^d - 1$ sein. Da 16 keine der Zahlen $5^1 - 1 = 4$, $5^2 - 1 = 24$, $5^3 - 1 = 124$ teilt, muss $d = 4$ sein. Aus $\text{grad}(h) = 4 = \text{grad}(g)$, $h \mid g$ und der Tatsache, dass h und g beide normiert sind, folgt $g = h$. Als Minimalpolynom eines über $\mathbb{F}_5$ algebraischen Elements ist g in $\mathbb{F}_5[x]$ irreduzibel.

zu (e) Nach Teil (c) sind $\alpha, \bar{2}\alpha, \bar{3}\alpha, \bar{4}\alpha$ alles Nullstellen von g in $\mathbb{F}_5^{\text{alg}}$. Da die Elemente $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ in $\mathbb{F}_5$ verschieden und $\alpha \neq \bar{0}$ ist, sind auch die vier angegebenen Nullstellen verschieden. Durch $x - c\alpha$ mit $c \in \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ sind also vier verschiedene Linearfaktoren von g in $\mathbb{F}_5^{\text{alg}}[x]$ gegeben, und wegen

$\mathrm{grad}(g) = 4$ folgt daraus $(x-\alpha)(x-\bar{2}\alpha)(x-\bar{3}\alpha)(x-\bar{4}\alpha)$. Dies zeigt, dass g über $\mathbb{F}_5(\alpha)$ in Linearfaktoren zerfällt. Andererseits wird $\mathbb{F}_5(\alpha)$ über $\mathbb{F}_5$ durch die Nullstellen von g erzeugt, da α eine Nullstelle von g ist. Insgesamt handelt es sich bei $\mathbb{F}_5(\alpha)$ also um den Zerfällungskörper von g über $\mathbb{F}_5$, und es folgt $\mathrm{Gal}(g|\mathbb{F}_5) = \mathrm{Gal}(\mathbb{F}_5(\alpha)|\mathbb{F}_5)$. Da g nach Teil (d) das Minimalpolynom von α über $\mathbb{F}_5$ ist, gilt $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = \mathrm{grad}(g) = 4$. Auf Grund des in Teil (b) erwähnten Satzes aus der Vorlesung folgt daraus $\mathrm{Gal}(g|\mathbb{F}_5) = \mathrm{Gal}(\mathbb{F}_5(\alpha)|\mathbb{F}_5) \cong \mathbb{Z}/4\mathbb{Z}$.

Aufgabe F21T3A3

Seien G eine endliche Gruppe und $\varphi : G \to H$ ein surjektiver Gruppenhomomorphismus auf eine weitere Gruppe H.

(a) Zeigen Sie, dass H auflösbar ist, wenn G auflösbar ist.

(b) Zeigen Sie, dass H entweder trivial oder einfach ist, wenn G einfach ist.

Lösung:
zu (a) Laut Vorlesung gilt: Ist G eine Gruppe und N ein Normalteiler von G, so ist G genau dann auflösbar, wenn die Gruppen N und G/N beide auflösbar sind. Setzen wir nun voraus, dass G auflösbar ist, und sei $N = \ker(\varphi)$. Da φ ein Epimorphismus von Gruppen ist, existiert nach dem Homomorphiesatz für Gruppen ein Isomorphismus $G/N \cong H$. Aus der Auflösbarkeit von G folgt nun die Auflösbarkeit von G/N, und wegen $G/N \cong H$ ist damit auch H auflösbar.

zu (b) Da G einfach ist, besitzt G genau zwei Normalteiler, nämlich $\{e\}$ und G. Bereits in Teil (a) haben wir festgestellt, dass $G/N \cong H$ gilt, mit $N = \ker(\varphi)$. Als Kern eines Gruppenhomomorphismus ist N ein Normalteiler von G. Es gilt also entweder $N = G$ oder $N = \{e\}$. Im ersten Fall folgt $H \cong G/G \cong \{e\}$, die Gruppe H ist also trivial. Im zweiten Fall gilt $H \cong G/\{e\} \cong G$. Da G einfach ist, folgt in dieser Situation aus $H \cong G$, dass auch H einfach ist.

Aufgabe F21T3A4

Sei R ein kommutativer Ring. Ein Element $a \in R$ heißt *nilpotent*, wenn $a^n = 0$ für ein $n \in \mathbb{N}$ gilt.

(a) Begründen Sie, warum in einem Körper K das einzige nilpotente Element a das Element $a = 0$ ist.

(b) Zeigen Sie, dass das *Nilradikal*

$$\mathfrak{n} = \{a \in R \mid a \text{ ist nilpotent } \}$$

ein Ideal ist.

(c) Zeigen Sie, dass das Nilradikal in jedem Primideal $\mathfrak{p}$ des Ringes R enthalten ist.

(d) Berechnen Sie das Nilradikal des (endlichen) Rings $\mathbb{Z}/\ell\mathbb{Z}$, wobei $\ell \geq 1$ eine natürliche Zahl ist.

Lösung:

zu (a) Sei K ein Körper und 0_K sein Nullelement. Wegen $0_K^1 = 0_K$ ist 0_K jedenfalls nilpotent. Sei nun $a \in K$ ein beliebiges nilpotentes Element. Dann gilt $a^n = 0_K$ für ein $n \in \mathbb{N}$; wir dürfen annehmen, dass n die kleinste natürliche Zahl mit dieser Eigenschaft ist. Es gilt dann $a^{n-1} \neq 0_K$, andererseits aber $a^{n-1} \cdot a = a^n = 0_K$. Weil K als Körper insbesondere ein Integritätsbereich ist, folgt daraus $a = 0_K$. Dies zeigt, dass es neben 0_K keine weiteren nilpotenten Elemente in K gibt.

zu (b) Zu zeigen ist, dass das Nullelement 0_R in $\mathfrak{n}$ enthalten ist, und dass für beliebige $a, b \in \mathfrak{n}$ und $r \in R$ auch $a+b$ und ra in $\mathfrak{n}$ liegen. Aus $0_R^1 = 0_R$ folgt unmittelbar $0_R \in \mathfrak{n}$. Seien nun $a, b \in \mathfrak{n}$ und $r \in R$ vorgegeben. Dann existieren $m, n \in \mathbb{N}$ mit $a^m = b^n = 0_R$. Es folgt $(ra)^m = r^m a^m = r^m \cdot 0_R = 0_R$ und somit $ra \in \mathfrak{n}$. Zum Nachweis von $a + b \in \mathfrak{n}$ dürfen wir nach eventueller Vertauschung von a und b die Ungleichung $m \leq n$ voraussetzen. Es gilt dann auch $a^n = a^m \cdot a^{n-m} = 0_R \cdot a^{n-m} = 0_R$. Auf Grund des Binomischen Lehrsatzes gilt

$$(a+b)^{2n} \quad = \quad \sum_{k=0}^{2n} \binom{2n}{k} a^{2n-k} b^k.$$

Für $0 \leq k \leq 2n$ gilt jeweils entweder $k \geq n$ oder $2n - k \geq n$. Im ersten Fall ist $b^k = b^n \cdot b^{k-n} = 0_R \cdot b^{k-n} = 0_R$, im zweiten $a^{2n-k} = a^n \cdot a^{n-k} = 0_R \cdot a^{n-k} = 0_R$. Daraus folgt, dass jeder einzelne Summand $\binom{2n}{k} a^{2n-k} b^k$ gleich null ist, also $(a+b)^{2n} = 0_R$ und damit $a + b \in \mathfrak{n}$ gilt.

zu (c) Sei $\mathfrak{p}$ ein beliebiges Primideal von R und $a \in \mathfrak{n}$. Dann gilt $a^n = 0_R$ für ein $n \in \mathbb{N}$, und da $\mathfrak{p}$ als Ideal von R das Nullelement 0_R enthält, folgt $a^n \in \mathfrak{p}$. Wir beweisen nun durch vollständige Induktion über n, dass für alle $n \in \mathbb{N}$ aus $a^n \in \mathfrak{p}$ jeweils $a \in \mathfrak{p}$ folgt. Für $n = 1$ ist dies unmittelbar klar. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für n voraus. Sei $a \in R$ ein Element mit $a^{n+1} \in \mathfrak{p}$. Aus $a^n \cdot a \in \mathfrak{p}$ folgt $a^n \in \mathfrak{p}$ oder $a \in \mathfrak{p}$, da $\mathfrak{p}$ ein Primideal ist. Im Fall $a \in \mathfrak{p}$ ist der Induktionsschritt bereits abgeschlossen. Im Fall $a^n \in \mathfrak{p}$ können wir die Induktionsvoraussetzung anwenden und erhalten ebenfalls $a \in \mathfrak{p}$.

zu (d) Sei $\ell = \prod_{i=1}^r p_i^{e_i}$ die Primfaktorzerlegung von ℓ, wobei $r \in \mathbb{N}_0$ ist und $p_1, ..., p_r$ verschiedene Primzahlen bezeichnen. Sei $\ell_0 = \prod_{i=1}^r p_i$. Wir zeigen, dass das Nilradikal $\mathfrak{n}$ von $\mathbb{Z}/(\ell)$ durch $\mathfrak{n} = (\ell_0 + \ell\mathbb{Z})$ gegeben ist. Zum Nachweis von „$\supseteq$“ sei $a + \ell Z \in (\ell_0 + \ell Z)$ vorgegeben, mit $a \in \mathbb{Z}$, und $e = \max\{e_1, ..., e_r\}$. Dann gibt es ein $m \in \mathbb{Z}$ mit $a + \ell Z = (m + \ell\mathbb{Z})(\ell_0 + \ell\mathbb{Z}) = m\ell_0 + \ell\mathbb{Z}$ und ein $s \in \mathbb{Z}$ mit $a = m\ell_0 + s\ell$. Mit ℓ ist auch a ein Vielfaches von ℓ_0, es gilt also $a = t\ell_0$ für ein $t \in \mathbb{Z}$. Außerdem ist

$$\ell_0^e \quad = \quad \left(\prod_{i=1}^r p_i\right)^e \quad = \quad \prod_{i=1}^r p_i^e \quad = \quad \left(\prod_{i=1}^r p_i^{e-e_i}\right)\left(\prod_{i=1}^r p_i^{e_i}\right) \quad = \quad \left(\prod_{i=1}^r p_i^{e-e_i}\right) \cdot \ell$$

ein Vielfaches von ℓ. Dies zeigt, dass auch a^e ein Vielfaches von ℓ ist. In $\mathbb{Z}/(\ell)$ gilt also $(a+\ell\mathbb{Z})^e = a^e + \ell\mathbb{Z} = 0 + \ell\mathbb{Z}$. Dies zeigt, dass $a + \ell\mathbb{Z}$ im Nilradikal $\mathfrak{n}$ von $\mathbb{Z}/(\ell)$ enthalten ist.

Zum Nachweis von „$\subseteq$“ setzen wir nun $a+\ell\mathbb{Z} \in \mathfrak{n}$ voraus, mit $a \in \mathbb{Z}$. Dann gilt $a^n+\ell Z = (a+\ell\mathbb{Z})^n = 0+\ell\mathbb{Z}$ für ein $n \in \mathbb{N}$. Somit ist a^n ein Vielfaches von ℓ. Für $i \in \{1, ..., r\}$ ist p_i jeweils ein Teiler von ℓ, damit auch von a^n und (da p_i eine Primzahl ist), auch von a. Insgesamt sind $p_1, ..., p_r$ also Primteiler von a. Somit ist auch deren Produkt ℓ_0 ein Teiler von a, es gilt also $a = s\ell_0$ und $a + \ell\mathbb{Z} = (s + \ell\mathbb{Z})(\ell_0 + \ell\mathbb{Z})$ für ein $s \in \mathbb{Z}$. Dies zeigt, dass $a + \ell\mathbb{Z}$ im Hauptideal $(\ell_0 + \ell\mathbb{Z})$ von $\mathbb{Z}/(\ell)$ enthalten ist.

Aufgabe F21T3A5

(a) Geben Sie mit Begründung eine mögliche Abbildungsmatrix des Frobenius-Homomorphismus

$$F : \mathbb{F}_{25} \to \mathbb{F}_{25} \ ,$$

aufgefasst als Endomorphismus des $\mathbb{F}_5$-Vektorraums $\mathbb{F}_{25}$, an.

(b) Bestimmen Sie die Anzahl der Unterkörper, die der endliche Körper $\mathbb{F}_{81}$ besitzt.

Lösung:
zu (a) Sei $\mathbb{F}_5^{\text{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_{25}$ (und damit insbesondere ein algebraischer Abschluss von $\mathbb{F}_5$). Sei $f = x^2 + \bar{2} \in \mathbb{F}_5[x]$ und $\alpha \in \mathbb{F}_5^{\text{alg}}$ eine Nullstelle von f. Dann ist f das Minimalpolynom von α über $\mathbb{F}_5$. Denn wegen $f(\bar{0}) = \bar{2} \neq \bar{0}$, $f(\bar{1}) = \bar{3} \neq \bar{0}$, $f(\bar{2}) = \bar{6} = \bar{1} \neq \bar{0}$, $f(\bar{3}) = \overline{11} = \bar{1} \neq \bar{0}$ und $f(\bar{4}) = \overline{18} = \bar{3} \neq \bar{0}$ besitzt f in $\mathbb{F}_5$ keine Nullstellen, ist wegen $\text{grad}(f) = 2$ somit über $\mathbb{F}_5$ irreduzibel. Außerdem ist f normiert, und es gilt $f(\alpha) = \bar{0}$. Auf Grund der Eigenschaft von f als Minimalpolynom gilt $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = \text{grad}(f) = 2$. Als 2-dimensionaler $\mathbb{F}_5$-Vektorraum besteht $\mathbb{F}_5(\alpha)$ aus $5^2 = 25$ Elementen. Aus der Vorlesung ist bekannt, dass die Erweiterung $\mathbb{F}_5^{\text{alg}}|\mathbb{F}_5$ für jedes $d \in \mathbb{N}$ genau einen Zwischenkörper $\mathbb{F}_{5^d}$ mit 5^d Elementen besitzt.

Es muss somit $\mathbb{F}_{25} = \mathbb{F}_5(\alpha)$ gelten. Da das Minimalpolynom f von α über $\mathbb{F}_5$ vom Grad 2 ist, ist laut Vorlesung durch $(1, \alpha)$ eine geordnete Basis von $\mathbb{F}_5(\alpha)$ als $\mathbb{F}_5$-Vektorraum gegeben. Wir bestimmen nun die Darstellungsmatrix des Frobenius-Endomorphismus $F : \mathbb{F}_{25} \to \mathbb{F}_{25}$, $\gamma \mapsto \gamma^5$ bezüglich dieser Basis. Die erste Spalte der Darstellungsmatrix ergibt sich durch die Rechung $F(\bar{1}) = \bar{1}^5 = \bar{1} = \bar{1} \cdot \bar{1} + \bar{0} \cdot \alpha$. Wegen $f(\alpha) = \bar{0}$ gilt $\alpha^2 = -\bar{2} = \bar{3}$. Die zweite Spalte der Darstellungsmatrix erhält man nun durch die Rechnung

$$F(\alpha) \quad = \quad \alpha^5 \quad = \quad \alpha^2 \cdot \alpha^2 \cdot \alpha \quad = \quad \bar{3} \cdot \bar{3} \cdot \alpha \quad = \quad \bar{9} \cdot \alpha \quad = \quad \bar{4} \cdot \alpha \quad = \quad \bar{0} \cdot \bar{1} + \bar{4} \cdot \alpha.$$

Insgesamt ist die Darstellungsmatrix von F bezüglich $(1, \alpha)$ also durch

$$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{4} \end{pmatrix} \qquad \text{gegeben.}$$

zu (b) In der Vorlesung wurde gezeigt: Ist p eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen und $\mathbb{F}_p^{\text{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$, dann gibt es für jedes $n \in \mathbb{N}$ genau einen Zwischenkörper $\mathbb{F}_{p^n}$ von $\mathbb{F}_p^{\text{alg}}|\mathbb{F}_p$ mit p^n Elementen. Dabei gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ für $m, n \in \mathbb{N}$ jeweils genau dann, wenn m ein Teiler von n ist. Insbesondere ist die Anzahl der Zwischenkörper von $\mathbb{F}_{p^n}|\mathbb{F}_p$ also gleich der Anzahl der natürlichen Teiler von n. Da $\mathbb{F}_p$ der Primkörper von $\mathbb{F}_{p^n}$ ist, ist dies zugleich auch die Anzahl der Unterkörper von $\mathbb{F}_{p^n}$. Die Zahl 4 besitzt in $\mathbb{N}$ genau drei Teiler (1, 2 und 4), somit hat der Körper $\mathbb{F}_{3^4} = \mathbb{F}_{81}$ genau drei Unterkörper (nämlich $\mathbb{F}_3 = \mathbb{F}_{3^1}$, $\mathbb{F}_9 = \mathbb{F}_{3^2}$ und $\mathbb{F}_{81} = \mathbb{F}_{3^4}$).

Aufgabe H21T1A1

Sei R ein kommutativer Ring (mit 1).

(a) Geben Sie die Definition des *größten gemeinsamen Teilers* (ggT) zweier Elemente $a, b \in R$ an.

(b) Begründen Sie, dass in einem faktoriellen Ring je zwei Elemente einen ggT haben.

(c) Begründen Sie, dass je zwei Elemente des Polynomrings $\mathbb{Q}[x, y]$ einen ggT haben.

(d) Zwei Elemente $a, b \in R$ heißen *teilerfremd*, wenn 1 ein ggT von a und b ist. Sie heißen *relativ prim*, wenn es $u, v \in R$ gibt mit $ua + vb = 1$. Zeigen Sie: Sind $a, b \in R$ relativ prim, dann sind sie auch teilerfremd.

(e) Geben Sie zwei Elemente $a, b \in \mathbb{Q}[x, y]$ an, die teilerfremd sind, aber nicht relativ prim.

Lösung:
zu (a) Ein Element $d \in R$ wird als *größter gemeinsamer Teiler* von a und b bezeichnet, wenn d ein gemeinsamer Teiler von a und b ist, also $d \mid a$ und $d \mid b$ gilt, und wenn $d' \mid d$ für jeden weiteren gemeinsamen Teiler d' von a und b erfüllt ist.

zu (b) Sei R ein faktorieller Ring und $P \subseteq R$ ein Repräsentantensystem der Primelemente von R (was bedeutet, dass P aus Primelementen besteht und jedes Primelement aus R zu genau einem Element aus P assoziiert ist). Aus der Vorlesung ist bekannt, dass jedes Element aus R dann eine eindeutige Darstellung der Form $\varepsilon \prod_{p \in P} p^{v_p}$ besitzt, mit $\varepsilon \in R^\times$, $v_p \in \mathbb{N}_0$ für alle $p \in P$ und $v_p = 0$ für alle bis auf endlich viele $p \in P$. Sind nun $a, b \in R$ zwei beliebige Elemente ungleich null und $a = \varepsilon \prod_{p \in P} p^{v_p}$, $b = \mu \prod_{p \in P} p^{w_p}$ die zugehörigen eindeutigen Darstellungen (mit $\varepsilon, \mu \in R^\times$), dann ist laut Vorlesung durch $\prod_{p \in P} p^{\min\{v_p, w_p\}}$ ein ggT von a und b gegeben.

zu (c) Nach Teil (b) genügt es zu zeigen, dass $\mathbb{Q}[x, y]$ ein faktorieller Ring ist. Laut Vorlesung ist jeder Polynomring über einem faktoriellen Ring wiederum faktoriell. Als Polynomring über einem Körper ist $\mathbb{Q}[x]$ ein Hauptidealring, somit insbesondere ein faktorieller Ring. Also ist auch $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$ faktoriell.

zu (d) Seien $a, b \in R$ relativ prim. Dann gibt es nach Definition $u, v \in R$ mit $ua + vb = 1$. Offenbar ist 1 ein gemeinsamer Teiler von a und b (denn es gilt $a = 1 \cdot a$ und $b = 1 \cdot b$). Sei nun d ein weiterer gemeinsamer Teiler von a und b. Dann ist d auch ein Teiler von ua und vb, und damit auch ein Teiler von $ua + vb = 1$. Damit ist nachgewiesen, dass 1 ein ggT von a und b ist, die Elemente a, b also teilerfremd sind.

zu (e) Sei $a = x$ und $b = y$. Wir zeigen zunächst, dass 1 ein größter gemeinsamer Teiler von a und b ist. Dass 1 ein gemeinsamer Teiler dieser beiden Elemente ist, ist wiederum offensichtlich. Sei nun $d \in \mathbb{Q}[x, y]$ ein weiterer gemeinsamer Teiler von a und b. Wegen $d \mid x$ existiert ein $u \in \mathbb{Q}[x, y]$ mit $x = ud$. Betrachten wir u und x als Polynome über dem Ring $\mathbb{Q}[x]$ in der Variablen y, so ist x ein Polynom vom Grad null, und aus der Gleichung $x = ud$ folgt, dass auch der Grad von u im Polynomring $\mathbb{Q}[x][y]$ gleich null ist. Dies bedeutet also, dass der Grad von u in der Variablen y gleich null ist. Ebenso folgt aus der Relation $d \mid y$, dass der Grad von d in der Variablen x gleich null ist. Somit ist das Polynom d insgesamt ein Konstante (wegen $ud = x \neq 0$ ungleich null), also eine Einheit in $\mathbb{Q}[x, y]$. Es folgt $d \mid 1$; also sind x und y tatsächlich teilerfremd in $\mathbb{Q}[x, y]$.

Nehmen wir nun an, dass x und y relativ prim sind. Dann gäbe es Polynome $u, v \in \mathbb{Q}[x, y]$ mit $ux+vy = 1$. Aber der konstante Term auf der linken Seite dieser Gleichung ist gleich 0, während der Termin auf der rechten Seite gleich 1 ist. Also kann eine solche Gleichung nicht gelten. Die Elemente x und y sind also nicht relativ prim zueinander.

Aufgabe H21T1A2

Sei V ein unendlich-dimensionaler $\mathbb{R}$-Vektorraum, auf dem eine positiv definite symmetrische Bilinearform $\langle \cdot, \cdot \rangle$ definiert ist. Wir schreiben $\|v\| = \sqrt{\langle v, v \rangle}$.

Es seien $v_1, ..., v_n \in V$. Zeigen Sie: Der Schwerpunkt $s = \frac{1}{n}(v_1 + ... + v_n)$ ist das eindeutig bestimmte Element $v \in V$, für das $\sum_{j=1}^{n} \|v - v_j\|^2$ minimal wird.

Hinweis: Schreiben Sie v als $v = s + w$.

Lösung:
Sei $v \in V$ beliebig vorgegeben und $w = v - s$. Wir beweisen die Gleichung

$$\sum_{j=1}^{n} \|v - v_j\|^2 \quad = \quad \sum_{j=1}^{n} \|s - v_j\|^2 + n\|w\|^2.$$

Daraus folgt unmittelbar, dass die Summe $\sum_{j=1}^{n} \|v - v_j\|^2$ genau dann minimal ist, wenn $w = 0$, also $v = s$ ist. Für $1 \leq j \leq n$ gilt jeweils

$$\begin{gathered} \|v - v_j\|^2 \quad = \quad \|s - v_j + w\|^2 \quad = \quad \langle s - v_j + w, s - v_j + w \rangle \quad = \\ \langle s - v_j, s - v_j \rangle + \langle s - v_j, w \rangle + \langle w, s - v_j \rangle + \langle w, w \rangle \quad = \quad \langle s - v_j, s - v_j \rangle + 2\langle s - v_j, w \rangle + \langle w, w \rangle \\ = \quad \|s - v_j\|^2 + \|w\|^2 + 2\langle s - v_j, w \rangle. \end{gathered}$$

Außerdem ist

$$\begin{gathered} \sum_{j=1}^{n} \langle s - v_j, w \rangle \quad = \quad \sum_{j=1}^{n} \langle s, w \rangle - \sum_{j=1}^{n} \langle v_j, w \rangle \quad = \quad n\langle s, w \rangle - \left\langle \sum_{j=1}^{n} v_j, w \right\rangle \quad = \\ n\langle s, w \rangle - \langle ns, w \rangle \quad = \quad n\langle s, w \rangle - n\langle s, w \rangle \quad = \quad 0. \end{gathered}$$

Insgesamt erhalten wir also

$$\begin{gathered} \sum_{j=1}^{n} \|v - v_j\|^2 \quad = \quad \sum_{j=1}^{n} \|s - v_j\|^2 + \sum_{j=1}^{n} \|w\|^2 + 2 \sum_{j=1}^{n} \langle s - v_j, w \rangle \quad = \\ \sum_{j=1}^{n} \|s - v_j\|^2 + n\|w\|^2 + 2 \cdot 0 \quad = \quad \sum_{j=1}^{n} \|s - v_j\|^2 + n\|w\|^2. \end{gathered}$$

Aufgabe H21T1A3

Sei K ein Körper. Für Polynome $f, g \in K[x]$ sei $f \circ g$ das Polynom $f(g(x))$. Beweisen oder widerlegen Sie durch ein Gegenbeispiel, ob folgende Aussage für alle Körper K richtig sind.

(a) $\forall f, g \in K[x] : (f \text{ irreduzibel} \Rightarrow f \circ g \text{ irreduzibel})$

(b) $\forall f, g \in K[x] : (f \circ g \text{ irreduzibel} \Rightarrow f \text{ irreduzibel})$

(c) $\forall f, g \in K[x] : (f \circ g \text{ irreduzibel} \Rightarrow g \text{ irreduzibel})$

Lösung:
zu (a) Diese Aussage ist falsch. Sei zum Beispiel $K = \mathbb{Q}$, $f = x$ und $g = x^2$. Dann ist f als lineares Polynom über einem Körper irreduzibel. Es gilt aber $f \circ g = f(x^2) = x^2$, und dieses Polynom ist reduzibel, denn $x^2 = x \cdot x$ ist eine Zerlegung in Nicht-Einheiten. (Die Einheiten im Ring $\mathbb{Q}[x]$ sind genau die konstanten Polynome ungleich null.)

zu (b) Diese Aussage ist wahr. Denn nehmen wir an, $f, g \in \mathbb{Q}[x]$ sind Polynome mit der Eigenschaft, dass $f \circ g$ irreduzibel, f aber nicht irreduzibel ist. Dann ist f entweder eine Einheit oder reduzibel. Im ersten Fall wäre f konstant. Dann wäre auch $f \circ g$ eine Konstante und somit eine Einheit in $\mathbb{Q}[x]$, insbesondere kein irreduzibles Element. Im zweiten Fall gäbe es eine Zerlegung $f = f_1 f_2$ von f in Nicht-Einheiten. Durch $f \circ g = f(g(x)) = (f_1 f_2)(g(x)) = f_1(g(x)) f_2(g(x)) = (f_1 \circ g) \cdot (f_2 \circ g)$ ist dann ebenfalls eine Zerlegung in Nicht-Einheiten gegeben. Da nämlich f_1 und f_2 keine Konstanten sind, können die Polynome $f_1 \circ g$ und $f_2 \circ g$ nur dann konstant sein, wenn g eine Konstante ist. Aber dann wäre auch $f \circ g$ konstant, im Widerspruch zur Voraussetzung, dass $f \circ g$ irreduzibel ist.

zu (c) Diese Aussage ist falsch. Sei zum Beispiel $K = \mathbb{Q}$, $f = x + 1$ und $g = x^2$. Dann ist $f \circ g = f(g(x)) = x^2 + 1$. Dieses Polynom ist irreduzibel, da es vom Grad 2 ist und keine rationale Nullstelle besitzt; wegen $(f \circ g)(a) = a^2 + 1 > 0$ für alle $a \in \mathbb{R}$ besitzt es noch nicht einmal eine Nullstelle in $\mathbb{R}$. Andererseits ist g irreduzibel, denn $x^2 = x \cdot x$ ist eine Zerlegung in Nicht-Einheiten.

Aufgabe H21T1A4

(a) Wir betrachten die additiven Gruppen $\mathbb{Z} \subseteq \mathbb{Q}$. Zeigen Sie: Die Faktorgruppe $\mathbb{Q}/\mathbb{Z}$ ist unendlich, aber jede endlich erzeugte Untergruppe von $\mathbb{Q}/\mathbb{Z}$ ist endlich.

(b) Sei $A = \{f : \mathbb{Z} \to \mathbb{Z}, x \mapsto ax + b \mid a = \pm 1, b \in \mathbb{Z}\}$. Zeigen Sie: A ist eine Gruppe mit der Hintereinanderschaltung von Abbildungen als Verknüpfung, und diese Gruppe ist isomorph zum semidirekten Produkt der (additiven) Gruppe $\mathbb{Z}$ mit der (multiplikativen) Gruppe $\{\pm 1\}$, wobei $\{\pm 1\}$ auf $\mathbb{Z}$ durch Multiplikation operiert.

Lösung:

zu (a) Um nachzuweisen, dass $\mathbb{Q}/\mathbb{Z}$ unendlich ist, zeigen wir, dass durch $2^{-n} + \mathbb{Z}$ mit $n \in \mathbb{N}$ unendlich viele verschiedene Elemente von $\mathbb{Q}/\mathbb{Z}$ gegeben sind. Wäre die Menge $\{2^{-n} + \mathbb{Z} \mid n \in \mathbb{N}\}$ endlich, dann gäbe es $m, n \in \mathbb{N}$, $m < n$ mit $2^{-m} + \mathbb{Z} = 2^{-n} + \mathbb{Z}$. Dies wäre gleichbedeutend mit $2^{-m} \in 2^{-n} + \mathbb{Z}$, also $2^{-m} = 2^{-n} + a$ für ein $a \in \mathbb{Z}$, was zu $a = 2^{-m} - 2^{-n}$ umgeformt werden kann. Im Fall $a = 0$ wäre $2^{-m} = 2^{-n}$ und $m = -\log_2(2^{-m}) = -\log_2(2^{-n}) = n$, im Widerspruch zur Voraussetzung. Im Fall $a \neq 0$ ist einerseits $|a| \geq 1$, andererseits aber $m \geq 1$ und somit $|2^{-m} - 2^{-n}| \leq 2^{-m} \leq \frac{1}{2} < 1$, was der Gleichung $a = 2^{-m} - 2^{-n}$ ebenfalls widerspricht.

Sei nun U eine endlich erzeugte Untergruppe von $\mathbb{Q}/\mathbb{Z}$ und $\{r_i + \mathbb{Z} \mid 1 \leq i \leq t\}$ ein endliches Erzeugendensystem von U, mit $r_i \in \mathbb{Q}$ für $1 \leq i \leq t$ und $t \in \mathbb{N}_0$. Wir schreiben $r_i = \frac{a_i}{b_i}$ mit $a_i \in \mathbb{Z}$ und $b_i \in \mathbb{N}$, für $1 \leq i \leq t$. Setzen wir $d = \mathrm{kgV}(b_1, ..., b_t)$, dann gelten $d_i = \frac{d}{b_i} \in \mathbb{N}$ und $r_i + \mathbb{Z} = a_i d_i \cdot (\frac{1}{d} + \mathbb{Z}) \in \langle \frac{1}{d} + \mathbb{Z} \rangle$ für $1 \leq i \leq t$. Aus $r_1 + \mathbb{Z}, ..., r_t + \mathbb{Z} \in \langle \frac{1}{d} + \mathbb{Z} \rangle$ folgt $U \subseteq \langle \frac{1}{d} + \mathbb{Z} \rangle$ (da $\{r_1 + \mathbb{Z}, ..., r_t + \mathbb{Z}\}$ ein Erzeugendensystem von U ist).

Um zu zeigen, dass U endlich ist, genügt es also nachzuweisen, dass die Gruppe $\langle \frac{1}{d} + \mathbb{Z} \rangle$ endlich ist. Dazu wiederum genügt es zu überprüfen, dass die Gruppe in der endlichen Menge $\{\frac{r}{d} + \mathbb{Z} \mid r \in \mathbb{Z}\ ,\ 0 \leq r < d\}$ enthalten ist. Jedes Element in $\langle \frac{1}{d} + \mathbb{Z} \rangle$ hat die Form $n \cdot (\frac{1}{d} + \mathbb{Z}) = \frac{n}{d} + \mathbb{Z}$, mit $n \in \mathbb{Z}$. Division von n durch d mit Rest liefert ein $q \in \mathbb{Z}$ und ein $r \in \{0, ..., d-1\}$ mit $n = qd + r$. Wegen $\frac{n}{d} - \frac{r}{d} = \frac{n-r}{d} = \frac{qd}{d} = q \in \mathbb{Z}$ gilt $\frac{n}{d} + \mathbb{Z} = \frac{r}{d} + \mathbb{Z}$. Das Element $\frac{n}{d} + \mathbb{Z}$ ist also tatsächlich in der angegebenen endlichen Menge enthalten.

zu (b) Für jedes $a \in \{\pm 1\}$ und jedes $b \in \mathbb{Z}$ sei $f_{a,b} : \mathbb{Z} \mapsto \mathbb{Z}$ die Abbildung gegeben durch $f(x) = ax + b$ für alle $x \in \mathbb{Z}$.

(i) Die Abbildung $f_{a,b} : \mathbb{Z} \to \mathbb{Z}$ ist für alle $a \in \{\pm 1\}$ und $b \in \mathbb{Z}$ jeweils bijektiv, es gilt also $A \subseteq \mathrm{Per}(\mathbb{Z})$.

(ii) Es ist A eine Untergruppe von $\mathrm{Per}(\mathbb{Z})$ (und somit insbesondere eine Gruppe).

(iii) Durch $\phi : \mathbb{Z} \to A$, $b \mapsto f_{1,b}$ und $\psi : \{\pm 1\} \to A$ sind injektive Homomorphismen definiert. Setzen wir $N = \phi(\mathbb{Z})$ und $U = \psi(\{\pm 1\})$, dann sind N und U also Untergruppen von A, und es gilt $\mathbb{Z} \cong N$ und $\{\pm 1\} \cong U$.

(iv) Bei A handelt es sich um ein inneres semidirektes Produkt von N und U. (Zusammen mit den Isomorphismen aus Teil (iii) folgt daraus, dass A isomorph zu einem semidirekten Produkt von $\mathbb{Z}$ und $\{\pm 1\}$ ist.)

(v) Es gilt $f_{a,0} \circ f_{1,b} \circ f_{a,0}^{-1} = f_{1,ab}$ für alle $a \in \{\pm 1\}$ und $b \in \mathbb{Z}$. (Daraus folgt, dass $\{\pm 1\}$ auf $\mathbb{Z}$ bei der Bildung des semidirekten Produkts durch Multiplikation operiert.)

zu (i) Sei $a \in \{\pm 1\}$ und $b \in \mathbb{Z}$. Wir zeigen, dass $f_{a,b} : \mathbb{Z} \to \mathbb{Z}$ bijektiv ist. Für alle $x, y \in \mathbb{Z}$ gilt die Äquivalenz $ax + b = y \Leftrightarrow ax = y - b \Leftrightarrow x = a^{-1}(y - b) \Leftrightarrow x = a^{-1}y + (-a^{-1})b \Leftrightarrow x = f_{a^{-1},-a^{-1}b}(y)$. Dies zeigt, dass $f_{a^{-1},-a^{-1}b}$ eine Umkehrabbildung von $f_{a,b}$ und $f_{a,b}$ somit bijektiv ist.

zu (ii) Das Neutralelement von $\mathrm{Per}(\mathbb{Z})$ ist die identische Abbildung $\mathrm{id}_\mathbb{Z}$, und für alle $x \in \mathbb{Z}$ gilt $\mathrm{id}_\mathbb{Z}(x) = x = 1 \cdot x + 0 = f_{1,0}(x)$. Wegen $1 \in \{\pm 1\}$ und $0 \in \mathbb{Z}$ ist $\mathrm{id}_\mathbb{Z} = f_{1,0}$ somit in A enthalten. Seien nun $f, g \in A$ vorgegeben. Dann gibt es $a, c \in \{\pm 1\}$ und $b, d \in \mathbb{Z}$ mit $f = f_{a,b}$ und $g = f_{c,d}$. Zu zeigen ist $f \circ g \in A$ und $f^{-1} \in A$. Wir haben bereits unter (i) festgestellt, dass die Umkehrabbildung von $f = f_{a,b}$ durch $f^{-1} = f_{a^{-1},-a^{-1}b}$ gegeben ist. Wegen $a \in \{\pm 1\}$ und $b \in \mathbb{Z}$ gilt $a^{-1} \in \{\pm 1\}$ und $-a^{-1}b \in \mathbb{Z}$, und dies zeigt, dass $f^{-1} = f_{a^{-1},-a^{-1}b}$ in A enthalten ist. Außerdem gilt für alle $x \in \mathbb{Z}$ jeweils

$$\begin{aligned}(f \circ g)(x) &= (f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx + d) = a(cx + d) + b \\ &= (ac)x + (ad + b) = f_{ac,ad+b}(x).\end{aligned}$$

Wegen $a, c \in \{\pm 1\}$ und $b, d \in \mathbb{Z}$ gilt $ac \in \{\pm 1\}$ und $ad + b \in \mathbb{Z}$, und damit folgt $f \circ g = f_{ac,ad+b} \in A$. Insgesamt ist die Untergruppen-Eigenschaft von A damit nachgewiesen.

zu (iii) Seien $b_1, b_2 \in \mathbb{Z}$ vorgegeben. Für alle $x \in \mathbb{Z}$ gilt $(f_{1,b_1} \circ f_{1,b_2})(x) = f_{1,b_1}(x + b_2) = (x + b_2) + b_1 = x + (b_1 + b_2) = f_{1,b_1+b_2}(x)$ und somit $\phi(b_1 + b_2) = f_{1,b_1+b_2} = f_{1,b_1} \circ f_{1,b_2} = \phi(b_1) \circ \phi(b_2)$. Also ist $\phi : \mathbb{Z} \to A$, $b \mapsto f_{1,b}$ ein Gruppenhomomorphismus. Zum Nachweis der Injektivität sei $b \in \ker(\phi)$ vorgegeben. Zu zeigen ist $b = 0$. Das Neutralelement in N ist die identische Abbildung, wegen $b \in \ker(\phi)$ gilt also $f_{1,b} = \phi(b) = \mathrm{id}_\mathbb{Z}$. Es folgt $b = 0 + b = f_{1,b}(0) = \mathrm{id}_\mathbb{Z}(0) = 0$.

Seien nun $a_1, a_2 \in \{\pm 1\}$ vorgegeben. Für alle $x \in \mathbb{Z}$ gilt $(f_{a_1,0} \circ f_{a_2,0})(x) = f_{a_1,0}(a_2 x) = a_1(a_2 x) = (a_1 a_2)x = f_{a_1 a_2,0}(x)$ und somit $\psi(a_1 a_2) = f_{a_1 a_2,0} = f_{a_1,0} \circ f_{a_2,0} = \psi(a_1) \circ \psi(a_2)$. Also ist $\psi : \{\pm 1\} \to A$, $a \mapsto f_{a,0}$ ein Gruppenhomomorphismus. Um zu zeigen, dass ψ injektiv ist, sei $a \in \ker(\psi)$ vorgegeben. Zu zeigen ist $a = 1$. Das Neutralelement in U ist die identische Abbildung, wegen $a \in \ker(\psi)$ gilt also $f_{a,0} = \psi(a) = \mathrm{id}_\mathbb{Z}$. Es folgt $a = a \cdot 1 = f_{a,0}(1) = \mathrm{id}_\mathbb{Z}(1) = 1$.

Als Bilder von Gruppen unter Gruppenhomomorphismen sind $N = \phi(\mathbb{Z})$ und $U = \psi(\{\pm 1\})$ Untergruppen von A. Durch ϕ ist ein Isomorphismus $\mathbb{Z} \cong N$ gegeben, denn aufgefasst als Abbildung $\phi : \mathbb{Z} \to N$ ist ϕ surjektiv, außerdem (wie bereits oben gezeigt) injektiv und ein Homomorphismus. Aus demselben Grund ist durch ψ ein Isomorphismus $\{\pm 1\} \cong U$ definiert.

zu (iv) In Teil (iii) wurde bereits gezeigt, dass N und U Untergruppen von A sind. Zu zeigen bleibt, dass N ein Normalteiler von A ist und außerdem die Gleichungen $N \cap U = \{\mathrm{id}_\mathbb{Z}\}$ und $NU = A$ erfüllt sind. Zum Nachweis der Normalteiler-Eigenschaft seien $f \in A$ und $n \in N$ vorgegeben. Zu zeigen ist $f \circ n \circ f^{-1} \in N$. Auf Grund der Voraussetzungen gibt es $a \in \{\pm 1\}$ und $b, d \in \mathbb{Z}$ mit $f = f_{a,b}$ und $n = f_{1,d}$. Für alle $x \in \mathbb{Z}$ gilt

$$\begin{aligned}(f \circ n \circ f^{-1})(x) &= (f_{a,b} \circ f_{1,d} \circ f_{a,b}^{-1})(x) = (f_{a,b} \circ f_{1,d} \circ f_{a^{-1},-a^{-1}b})(x) = \\ &(f_{a,b} \circ f_{1,d})(a^{-1}x + (-a^{-1}b)) = f_{a,b}(a^{-1}x + (-a^{-1}b) + d) = \\ &a(a^{-1}x + (-a^{-1}b) + d) + b = x + (-b) + ad + b = x + ad\end{aligned}$$

und somit $f \circ n \circ f^{-1} = f_{1,ad} \in N$. In der Gleichung $N \cap U = \{\mathrm{id}_\mathbb{Z}\}$ ist die Inklusion „$\supseteq$“ offensichtlich (da N und U als Untergruppen von A beide das Neutralelement enthalten). Zum Nachweis von „$\subseteq$“ sei $f \in N \cap U$ vorgegeben. Wegen $f \in N$ gibt es ein $b \in Z$ mit $f = f_{1,b}$, und wegen $f \in U$ existiert ein $a \in \{\pm 1\}$ mit $f = f_{a,0}$. Es folgt $b = 0 + b = f_{1,b}(0) = f_{a,0}(0) = a \cdot 0 + 0 = 0$ und $a = a \cdot 1 + 0 = f_{a,0}(1) = f_{1,b}(1) = 1 + b = 1$. Ingesamt gilt also $f = f_{1,0}$. Wegen $f_{1,0}(x) = 1 \cdot x + 0 = x = \mathrm{id}_\mathbb{Z}(x)$ für alle $x \in \mathbb{Z}$ erhalten wir $f = \mathrm{id}_\mathbb{Z}$.

In der Gleichung $NU = A$ ist „$\subseteq$“ offensichtlich (weil N und U nach Definition Teilmengen von A sind). Zum Nachweis von „$\supseteq$“ sei $f \in A$ vorgegeben, $f = f_{a,b}$ mit $a \in \{\pm 1\}$ und $b \in \mathbb{Z}$. Für alle $x \in \mathbb{Z}$ gilt $(f_{1,b} \circ f_{a,0})(x) = f_{1,b}(ax + 0) = ax + b = f_{a,b}(x)$. Wegen $f_{1,b} = \phi(b) \in N$ und $f_{a,0} = \psi(a) \in U$ folgt $f = f_{a,b} = f_{1,b} \circ f_{a,0} \in NU$.

zu (v) Wir haben bereits unter (iv) nachgerechnet, dass $f_{a,b} \circ f_{1,d} \circ f_{a,b}^{-1} = f_{1,ad}$ für alle $a \in \{\pm 1\}$ und $b, d \in \mathbb{Z}$ gilt. Insbesondere gilt also $f_{a,0} \circ f_{1,b} \circ f_{a,0}^{-1} = f_{1,ab}$ für alle $a \in \{\pm 1\}$ und $b \in \mathbb{Z}$.

Aufgabe H21T1A5

Sei $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, wobei K eine galoissche Körpererweiterung von $\mathbb{Q}$ vom Grad 2021 ist. Zeigen Sie:

(a) Es gibt Zwischenkörper $\mathbb{Q} \subseteq L_j \subseteq K$, $j \in \{1, 2\}$, mit $[L_1 : \mathbb{Q}] = 43$ und $[L_2 : \mathbb{Q}] = 47$, die über $\mathbb{Q}$ galoissch sind.

(b) Sei $\alpha \in K$, so dass $K = \mathbb{Q}(\alpha)$ gilt, und sei f das Minimalpolynom von α über $\mathbb{Q}$. Dann zerfällt f über $\mathbb{R}$ in Linearfaktoren.

Lösung:
zu (a) Sei $G = \mathrm{Gal}(K|\mathbb{Q})$. Weil $K|\mathbb{Q}$ eine Galois-Erweiterung vom Grad 2021 ist, gilt $|G| = [K : \mathbb{Q}] = 2021 = 43 \cdot 47$. Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Auf Grund des 3. Sylowsatzes gilt $\nu_{47} \mid 43$, da 43 eine Primzahl ist also $\nu_{47} \in \{1, 43\}$, außerdem $\nu_{47} \equiv 1 \bmod 47$. Wegen $43 \not\equiv 1 \bmod 47$ folgt $\nu_{47} = 1$. Ebenso gilt $\nu_{43} \mid 47$, da 47 eine Primzahl ist also $\nu_{43} \in \{1, 47\}$, außerdem $\nu_{43} \equiv 1 \bmod 43$. Wegen $47 \equiv 4 \not\equiv 1 \bmod 43$ folgt $\nu_{43} = 1$.

Sei nun N_1 die einzige 47- und N_2 die einzige 43-Sylowgruppe, außerdem L_j jeweils der Fixkörper von N_j, also $L_j = K^{N_j}$ für $j = 1, 2$. Wegen $G = 43^1 \cdot 47^1$ gilt $|N_1| = 47$ und $|N_2| = 43$, nach Definition der p-Sylowgruppen. Auf Grund der Ergänzungen zum Hauptsatz der Galoistheorie gilt $[L_1 : \mathbb{Q}] = (G : N_1) = \frac{|G|}{|N_1|} = \frac{2021}{47} = 43$ und ebenso $[L_2 : \mathbb{Q}] = (G : N_2) = \frac{|G|}{|N_2|} = \frac{2021}{43} = 47$. Da N_1 als einzige 47-Sylowgruppe ein Normalteiler von G ist, liefert der zugehörige Fixkörper eine galoissche Teilerweiterung $L_1|\mathbb{Q}$ von $K|\mathbb{Q}$. Aus demselben Grund ist auch $L_2|\mathbb{Q}$ eine Galois-Erweiterung.

zu (b) Laut Angabe ist die Erweiterung $K|\mathbb{Q}$ galoissch, also insbesondere normal. Das Polynom f ist als Minimalpolynom von α über $\mathbb{Q}$ in $\mathbb{Q}[x]$ irreduzibel, außerdem besitzt es in $K = \mathbb{Q}(\alpha)$ eine Nullstelle (nämlich α). Weil $K|\mathbb{Q}$ normal ist, zerfällt f über K also in Linearfaktoren.

Weil f das Minimalpolynom von α ist, gilt außerdem $\mathrm{grad}(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 2021$. Weil f ein Polynom ungeraden Grades ist, besitzt es in $\mathbb{R}$ eine Nullstelle β. Weil f über K in Linearfaktoren zerfällt, enthält K alle Nullstellen von f, insbesondere die Nullstelle β. Es gilt also $\beta \in K$ und (da K eine Erweiterung von $\mathbb{Q}$ ist) somit auch $\mathbb{Q}(\beta) \subseteq K$. Da f (als Minimalpolynom von α über $\mathbb{Q}$) normiert und irreduzibel ist, folgt aus $f(\beta) = 0$, dass f auch das Minimalpolynom von β über $\mathbb{Q}$ ist. Es gilt also $[\mathbb{Q}(\beta) : \mathbb{Q}] = \mathrm{grad}(f) = [K : \mathbb{Q}]$. Zusammen mit $\mathbb{Q}(\beta) \subseteq K$ folgt daraus $K = \mathbb{Q}(\beta)$. Damit ist gezeigt, dass f auch über $\mathbb{Q}(\beta)$ in Linearfaktoren zerfällt. Wegen $\beta \in \mathbb{R}$ gilt $\mathbb{Q}(\beta) \subseteq \mathbb{R}$. Also zerfällt f erst recht über $\mathbb{R}$ in Linearfaktoren.

Aufgabe H21T2A1

Sei G eine Gruppe, und seien a, b, c Elemente aus G.

(a) Zeigen Sie, dass a und a^{-1} dieselbe Ordnung haben.

(b) Zeigen Sie, dass ab und ba dieselbe Ordnung haben.

(c) Zeigen Sie, dass abc und bca dieselbe Ordnung haben.

(d) Geben Sie Elemente a, b, c in der symmetrischen Gruppe S_3 an, so dass abc und bac nicht dieselbe Ordnung haben.

(e) Zeigen Sie, dass es in einer nichtkommutativen Gruppe G stets Elemente a, b, c gibt, so dass abc und bac nicht dieselbe Ordnung haben.

Lösung:
zu (a) Ist $\mathrm{ord}(a)$ unendlich, dann muss auch a^{-1} unendliche Ordnung haben. Denn ansonsten gäbe es ein $n \in \mathbb{N}$ mit $(a^{-1})^n = e$, wobei e das Neutralelement von G bezeichnet. Auf Grund der Potenzgesetze für Gruppenelemente würde dann $a^n = a^{-(-n)} = ((a^{-1})^n)^{-1} = e^{-1} = e$ gelten. Somit hätte auch a unendliche Ordnung, im Widerspruch zur Voraussetzung.

Somit können wir uns auf den Fall beschränken, dass $m = \mathrm{ord}(a)$ endlich ist. Sei $n = \mathrm{ord}(a^{-1})$. Wegen $(a^{-1})^m = a^{-m} = (a^m)^{-1} = e^{-1} = e$ ist $n = \mathrm{ord}(a^{-1})$ ein Teiler von m. Umgekehrt ist wegen $a^n = ((a^{-1})^n)^{-1} = e^{-1} = e$ auch $m = \mathrm{ord}(a)$ ein Teiler von n. Damit ist insgesamt $\mathrm{ord}(a) = m = n = \mathrm{ord}(a^{-1})$ nachgewiesen.

zu (b) Sei $\phi : G \to G$ gegeben durch die Konjugation mit a^{-1}, also durch $\phi(g) = a^{-1}ga$ für alle $g \in G$. Laut Vorlesung ist eine solche Abbildung ein Automorphismus von G. Außerdem ist bekannt, dass die Ordnung von Gruppenelementen unter Isomorphismen erhalten bleibt. Wegen $\phi(ab) = a^{-1}(ab)a = ba$ haben die Elemente also ab und ba dieselbe Ordnung.

zu (c) Sei ϕ wie in Aufgabenteil (b) definiert. Aus der Gleichung $\phi(abc) = a^{-1}(abc)a = bca$ ergibt sich wie in Teil (b), dass die Elemente abc und bca dieselbe Ordnung haben.

zu (d) Sei $a = (1\ 2)$, $b = (1\ 3)$ und $c = (1\ 2\ 3)$. Dann gilt $abc = (1\ 2) \circ (1\ 3) \circ (1\ 2\ 3) = (1\ 3\ 2) \circ (1\ 2\ 3) = \mathrm{id}$, andererseits $bac = (1\ 3) \circ (1\ 2) \circ (1\ 2\ 3) = (1\ 2\ 3) \circ (1\ 2\ 3) = (1\ 3\ 2)$. Es ist also einerseits $\mathrm{ord}(abc) = 1$, andererseits aber $\mathrm{ord}(bac) = 3$ (weil in S_n jeder k-Zykel von Ordnung k ist, für alle $n \in \mathbb{N}$ und $2 \leq k \leq n$).

zu (e) Ist G eine nichtkommutative Gruppe, dann gibt es Elemente a, b mit $ab \neq ba$. Sei $c = (ab)^{-1} = b^{-1}a^{-1}$. Dann ist einerseits $abc = (ab)(ab)^{-1} = e$ (wobei e wiederum das Neutralelement von G bezeichnet), andererseits $bac = (ba)(b^{-1}a^{-1})$. Hätten abc und bac dieselbe Ordnung, dann müsste wegen $\mathrm{ord}(abc) = \mathrm{ord}(e) = 1$ auch die Ordnung von bac gleich 1 sein, das Element bac also mit dem Neutralelement übereinstimmen. Aber daraus würde sich $(ba)(b^{-1}a^{-1}) = e \Rightarrow bab^{-1} = a \Rightarrow ba = ab$ ergeben, im Widerspruch zur Voraussetzung. Also haben die Elemente abc und bac verschiedene Ordnung.

Aufgabe H21T2A2

(a) Bestimmen Sie das Minimalpolynom m von $\sqrt[3]{2}$ über $\mathbb{Q}$. Zeigen Sie, dass m über $\mathbb{Q}[\sqrt[3]{2}]$ nicht in Linearfaktoren zerfällt.

(b) Sei $\mathbb{F}_5$ der endliche Körper mit fünf Elementen. Geben Sie einen Isomorphismus $\varphi : \mathbb{F}_5[\sqrt{2}] \to \mathbb{F}_5[\sqrt{3}]$ explizit an.

Lösung:

zu (a) Zunächst zeigen wir, dass $m = x^3 - 2$ gilt. Das Polynom $f = x^3 - 2$ liegt in $\mathbb{Q}[x]$, ist normiert, und es erfüllt die Bedingung $f(\sqrt[3]{2}) = 0$. Außerdem ist es nach dem Eisenstein-Kriterium (angewendet auf die Primzahl $p = 2$) irreduzibel über $\mathbb{Z}$ und damit nach dem Gauß'schen Lemma auch irreduzibel über $\mathbb{Q}$. Insgesamt handelt es sich also um das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, es gilt also $m = f = x^3 - 2$. Nun besitzt m neben $\sqrt[3]{2}$ auch die komplexe Nullstelle $\zeta\sqrt[3]{2}$, mit $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, denn es gilt $\zeta^3 = 1$ und somit $m(\zeta\sqrt[3]{2}) = (\zeta\sqrt[3]{2})^3 - 2 = \zeta^3(\sqrt[3]{2})^3 - 2 = 1 \cdot 2 - 2 = 0$. Würde m bereits über $\mathbb{Q}[\sqrt[3]{2}]$ in Linearfaktoren zerfallen, dann müssten alle komplexen Nullstellen von m in $\mathbb{Q}[\sqrt[3]{2}]$ liegen, insbesondere die Nullstelle $\zeta\sqrt[3]{2}$. Aber dies ist nicht der Fall, denn wegen $\sqrt[3]{2} \in \mathbb{R}$ gilt $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, aber andererseits hat $\zeta\sqrt[3]{2}$ den Imaginärteil $\frac{1}{2}\sqrt{3}\sqrt[3]{2}$ ungleich null und ist somit nicht in $\mathbb{R}$ enthalten.

zu (b) Das Polynom $f = x^2 - \bar{2} = x^2 + \bar{3} \in \mathbb{F}_5[x]$ ist das Minimalpolynom von $\sqrt{2}$ über $\mathbb{F}_5$. Denn wie die Rechnung $f(\bar{0}) = \bar{3} \neq \bar{0}$, $f(\bar{1}) = \bar{4} \neq \bar{0}$, $f(\bar{2}) = \bar{2} \neq \bar{0}$, $f(\bar{3}) = \bar{2} \neq \bar{0}$, $f(\bar{4}) = \bar{4} \neq \bar{0}$ zeigt, besitzt f in $\mathbb{F}_5$ keine Nullstellen; wegen $\operatorname{grad}(f) = 2$ folgt daraus die Irreduzibilität. Da f außerdem normiert ist und $f(\sqrt{2}) = (\sqrt{2})^2 - \bar{2} = \bar{2} - \bar{2} = \bar{0}$ gilt, ist f insgesamt das Minimalpolynom von $\sqrt{2}$ über $\mathbb{F}_5$. Laut Vorlesung existiert somit ein Isomorphismus $\phi : \mathbb{F}_5[x]/(f) \to \mathbb{F}_5[\sqrt{2}]$ gegeben durch $\phi(g + (f)) = g(\sqrt{2})$ für alle $g \in \mathbb{F}_5[x]$.

Im nächsten Schritt bestimmen wir eine Quadratwurzel aus $\bar{2}$ in $\mathbb{F}_5[\sqrt{3}]$. Für alle $a, b \in \mathbb{F}_5$ gilt die Äquivalenz

$$(a + b\sqrt{3})^2 = \bar{2} \quad \Leftrightarrow \quad a^2 + \bar{2}ab\sqrt{3} + (b\sqrt{3})^2 = \bar{2} \quad \Leftrightarrow \quad a^2 + \bar{3}b^2 + \bar{2}ab\sqrt{2} = \bar{2}.$$

Die letzte Gleichung ist zum Beispiel erfüllt, wenn wir $a = \bar{0}$ und $b = \bar{2}$ setzen. Tatsächlich ist $(\bar{2}\sqrt{3})^2 = \bar{2}^2 \cdot \bar{3} = \bar{4} \cdot \bar{3} = \overline{12} = \bar{2}$, d.h. das Element $\bar{2}\sqrt{3} \in \mathbb{F}_5[\sqrt{3}]$ ist eine Quadratwurzel aus $\bar{2}$.

Auf Grund der universellen Eigenschaft des Polynomrings gibt es einen eindeutig bestimmten Ringhomomorphismus $\psi : \mathbb{F}_5[x] \to \mathbb{F}_5[\sqrt{3}]$ mit $\psi|_{\mathbb{F}_5} = \mathrm{id}_{\mathbb{F}_5}$ und $\psi(x) = \bar{2}\sqrt{3}$, nämlich den Auswertungshomomorphismus gegeben durch $\psi(g) = g(\bar{2}\sqrt{3})$. Dieser Homomorphismus ist surjektiv, denn wegen $\psi|_{\mathbb{F}_5} = \mathrm{id}_{\mathbb{F}_5}$ ist der Teilring $\mathbb{F}_5$ im Bild enthalten, und wegen $\psi(\bar{3}x) = \bar{3} \cdot (\bar{2}\sqrt{3}) = \bar{6} \cdot \sqrt{3} = \sqrt{3}$ auch das Element $\sqrt{3}$, insgesamt also der komplette Ring $\mathbb{F}_5[\sqrt{3}]$. Darüber hinaus gilt $\ker(\psi) = (x^2 - \bar{2}) = (f)$. Denn die Rechung $\psi(f) = f(\bar{2}\sqrt{3}) = (\bar{2}\sqrt{3})^2 - \bar{2} = \bar{2} - \bar{2} = \bar{0}$ zeigt zunächst, dass das Hauptideal (f) im Kern enthalten ist. Weil $f = x^2 - \bar{2}$, wie oben gezeigt, ein in $\mathbb{F}_5[x]$ irreduzibles Polynom und $\mathbb{F}_5[x]$ als Polynomring über einem Körper ein Hauptidealring ist, handelt es sich bei (f) um ein maximales Ideal. Somit ist $\ker(\psi) \supsetneq (f)$ nur möglich, wenn $\ker(\psi) = (\bar{1})$ und ψ somit die Nullabbildung ist. Aber dies ist wegen $\psi|_{\mathbb{F}_5} = \mathrm{id}_{\mathbb{F}_5}$ nicht der Fall. Damit ist die angegebene Gleichung bewiesen.

Der Homomorphiesatz für Ringe zeigt nun, dass ψ einen Isomorphismus $\bar{\psi} : \mathbb{F}_5[x]/(f) \to \mathbb{F}_5[\sqrt{3}]$ induziert, gegeben durch $\bar{\psi}(g + (f)) = \psi(g) = g(\bar{2}\sqrt{3})$. Durch Komposition der beiden Isomorphismen $\phi^{-1} : \mathbb{F}_5[\sqrt{2}] \to \mathbb{F}_5[x]/(f)$ und $\bar{\psi} : \mathbb{F}_5[x]/(f) \to \mathbb{F}_5[\sqrt{3}]$ erhalten wir nun einen Isomorphismus $\alpha = \bar{\psi} \circ \phi^{-1}$. Dieser ist explizit gegeben durch $\alpha(g(\sqrt{2})) = (\bar{\psi} \circ \phi^{-1})(g(\sqrt{2})) = \bar{\psi}(g + (f)) = g(\bar{2}\sqrt{3})$ für alle $g \in \mathbb{F}_5[x]$, insbesondere ist $\alpha(\sqrt{2}) = \bar{2}\sqrt{3}$.

Aufgabe H21T2A3

Es sei $L|K$ eine Körpererweiterung vom Grad 2.

(a) Zeigen Sie, dass $L|K$ stets normal ist.

(b) Zeigen Sie, dass $L|K$ im Fall $\mathrm{char}(K) \neq 2$ stets separabel ist.

(c) Geben Sie (mit Begründung) jeweils ein Beispiel für eine separable und eine inseparable Körpererweiterung vom Grad 2 im Fall $\mathrm{char}(K) = 2$ an.

Hinweis für den zweiten Teil:
Betrachten Sie den rationalen Funktionenkörper $k(t)$ über einem Körper k.

Lösung:
zu (a) Sei $f \in K[x]$ ein über K irreduzibles Polynom, das in L eine Nullstelle α besitzt. Zu zeigen ist, dass f über L in Linearfaktoren zerfällt. Da $K(\alpha)$ ein Zwischenkörper von $L|K$ ist, gilt $2 = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$ auf Grund der Gradformel, also $[K(\alpha) : K] \mid 2$ und somit $[K(\alpha) : K] \in \{1, 2\}$. Da f irreduzibel über K und $\alpha \in L$ eine Nullstelle von f ist, folgt $\mathrm{grad}(f) = [K(\alpha) : K] \in \{1, 2\}$. Im Fall $\mathrm{grad}(f) = 1$ ist das Polynom f selbst linear und somit nichts zu zeigen. Im Fall $\mathrm{grad}(f) = 2$ ist $x - \alpha$ wegen $f(\alpha) = 0$ ein Teiler von f in $L[x]$, es existiert also ein $h \in K[x]$ mit $f = (x - \alpha)h$, und wegen $\mathrm{grad}(f) = 2$ muss $\mathrm{grad}(h) = 1$ gelten. Also zerfällt f auch in diesem Fall über L in Linearfaktoren.

zu (b) Sei $L|K$ eine Erweiterung mit $\mathrm{char}(K) \neq 2$ und $[L : K] = 2$. Zu zeigen ist, dass jedes Element aus L über K separabel ist. Sei also $\alpha \in L$ vorgegeben und $f \in K[x]$ das Minimalpolynom von α über K. Zu zeigen ist, dass es sich bei f um ein separables Polynom handelt, also $\mathrm{ggT}(f, f') = 1$ gilt. Auf Grund der Gradformel gilt $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K] = 2$. Daraus folgt $[K(\alpha) : K] \mid 2$ und somit $\mathrm{grad}(f) = [K(\alpha) : K] \in \{1, 2\}$. Im Fall $\mathrm{grad}(f) = 1$ ist f' die Ableitung eines normierten linearen Polynoms, also $f' = 1$ und $\mathrm{ggT}(f, f') = 1$ somit erfüllt.

Im Fall $\mathrm{grad}(f) = 2$ gibt es $a, b \in K$ mit $f = x^2 + ax + b$. Es gilt dann $f' = 2x + a$. In diesem Fall sind f und f' nur dann nicht teilerfremd, wenn f' ein Teiler von f und somit $-\frac{1}{2}a \in K$ eine Nullstelle von f ist. (Dabei ist zu beachten, dass in K wegen $\mathrm{char}(K) \neq 2$ die 2 nicht das Nullelement ist und somit $\frac{1}{2}$ in K existiert.) Aber dies würde der Tatsache widersprechen, dass f als Minimalpolynom von α über K irreduzibel ist. Also ist f auch in diesem Fall separabel.

zu (c) Sei $K = \mathbb{F}_2$ und $L = \mathbb{F}_4$, der Körper mit zwei bzw. vier Elementen. Da $\mathbb{F}_2$ der gemeinsame Primkörper von K und L ist, gilt $\mathrm{char}(K) = \mathrm{char}(L) = 2$. Wegen $4 = 2^2$ gilt laut Vorlesung $[L : K] = 2$. Außerdem ist bekannt, dass jede algebraische Erweiterung eines endlichen Körpers separabel ist. Weil L endlich ist, ist $L|K$ eine endliche und somit auch eine algebraisch und separable Erweiterung.

Sei nun $L = \mathbb{F}_2(t)$ der rationale Funktionenkörper über $\mathbb{F}_2$ und K der von t^2 über $\mathbb{F}_2$ erzeugte Teilkörper, also $K = \mathbb{F}_2(t^2)$. Wieder ist $\mathbb{F}_2$ der gemeinsame Primkörper von K und L, es gilt also auch hier $\mathrm{char}(K) = \mathrm{char}(L) = 2$. Wir zeigen nun, dass $f = x^2 - t^2 \in K[x]$ das Minimalpolynom von t über K ist. Das Polynom ist normiert, und es gilt $f(t) = t^2 - t^2 = 0$. Wäre es reduzibel, dann müsste wegen $\mathrm{grad}(f) = 2$ die Nullstelle t bereits in K enthalten sein. Aus der Vorlesung ist bekannt, dass die Elemente in K die Form $\frac{u(t^2)}{v(t^2)}$ haben, mit $u, v \in \mathbb{F}_2[x]$ und $v \neq \bar{0}$. Es gäbe also solche Polynome u, v mit $\frac{u(t^2)}{v(t^2)} = t$, was zu $u(t^2) = tv(t^2)$ umgeformt werden kann. Aber eine solche Gleichung in $\mathbb{F}_2[t]$ ist unmöglich, weil $\mathrm{grad}(u(t^2)) = 2 \cdot \mathrm{grad}(u)$ eine gerade, $\mathrm{grad}(tv(t^2)) = 2 \cdot \mathrm{grad}(v) + 1$ jedoch eine ungerade Zahl ist.

Dies zeigt, dass f irreduzibel und insgesamt tatsächlich das Minimalpolynom von t über K ist. Außerdem

gilt $L = K(t)$, denn wegen $\mathbb{F}_2 \subseteq K$ und $t \in K(t)$ gilt $L = \mathbb{F}_2(t) \subseteq K(t)$, und wegen $K \subseteq L$ und $t \in L$ andererseits auch $K(t) \subseteq L$. Es folgt $[L : K] = [K(t) : K] = \mathrm{grad}(f) = 2$. Aber die Erweiterung $L|K$ ist nicht separabel. Denn wegen $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, \bar{2}x) = \mathrm{ggT}(f, \bar{0}) = f$ sind f und f' nicht teilerfremd, das Polynom $f \in K[x]$ also nicht separabel und folglich (weil f das Minimalpolynom von t über K ist) das Element $t \in L$ nicht separabel über K.

Aufgabe H21T2A4

Zu betrachten seien die Körpererweiterungen $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ von $\mathbb{Q}$, wobei

$$\alpha = \sqrt{1+\sqrt{2}} \in \mathbb{R} \quad \text{und} \quad \beta = i\sqrt{\sqrt{2}-1} \in \mathbb{C} \text{ ist.}$$

(a) Bestimmen Sie jeweils das Minimalpolynom von α und β über $\mathbb{Q}$.

(b) Bestimmen Sie die Grade $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ und $[\mathbb{Q}(\beta) : \mathbb{Q}]$. Entscheiden Sie, ob die beiden Erweiterungen verschieden sind.

(c) Entscheiden und begründen Sie, ob die $\mathbb{Q}(\alpha)|\mathbb{Q}$ und $\mathbb{Q}(\beta)|\mathbb{Q}$ jeweils normal sind.

(d) Bestimmen Sie die Automorphismengruppen $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ und $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\beta))$.

Lösung:

zu (a) Zunächst bestimmen wir das Minimalpolynom von α über $\mathbb{Q}$. Die Rechnung

$$\alpha = \sqrt{1+\sqrt{2}} \quad \Rightarrow \quad \alpha^2 = 1+\sqrt{2} \quad \Rightarrow \quad \alpha^2 - 1 = \sqrt{2} \quad \Rightarrow \quad (\alpha^2-1)^2 = 2 \quad \Rightarrow$$
$$\alpha^4 - 2\alpha^2 + 1 = 2 \quad \Rightarrow \quad \alpha^4 - 2\alpha^2 - 1 = 0$$

zeigt, dass α eine Nullstelle von $f = x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$ ist. Wir zeigen, dass f über $\mathbb{Q}$ irreduzibel ist. Da f in $\mathbb{Z}[x]$ liegt und normiert ist, ist jede rationale Nullstelle von f ganzzahlig und ein Teiler des konstanten Terms -1. Die einzigen mögichen rationalen Nullstellen sind also ± 1. Es gilt aber $f(1) = f(-1) = 1-2-1 = -2 \neq 0$, also besitzt f keine rationale Nullstelle. Wäre f dennoch über $\mathbb{Q}$ reduzibel, dann auch über $\mathbb{Z}$. Es gäbe also zwei nicht-konstante Polynome $g, h \in \mathbb{Z}[x]$ mit $f = gh$. Da f normiert ist, können auch g und h normiert gewählt werden, und das Produkt der konstanten Terme von g und h muss -1 sein. Da $-1 = 1 \cdot (-1)$ bis auf Reihenfolge die einzige Zerlegung von -1 in ganzzahlige Faktoren ist, können wir nach eventueller Vertauschung von g und h davon ausgehen, dass der konstante Term von g gleich 1 und der konstante Term von h gleich -1 ist. Da f keine rationale Nullstelle besitzt, ist keiner der Faktoren g, h vom Grad 1. Es muss also $\mathrm{grad}(g) = \mathrm{grad}(h) = 2$ gelten. Insgesamt haben damit gezeigt, dass $g = x^2 + ax + 1$ und $h = x^2 + bx - 1$ ist, mit geeigneten $a, b \in \mathbb{Z}$. Weiter gilt

$$\begin{aligned} x^4 - 2x^2 - 1 &= f = gh = (x^2+ax+1)(x^2+bx-1) \\ &= x^4 + (a+b)x^3 + abx^2 + (-a+b)x - 1. \end{aligned}$$

Durch Koeffizientenvergleich erhalten wir $a + b = -a + b = 0$ und $ab = -2$. Die Addition der ersten beiden Gleichungen liefert $2b = 0$ und $b = 0$, woraus dann aber $ab = 0$, im Widerspruch zu $ab = -2$. Es gibt also keine Zerlegung von f der angegebenen Form, und insgesamt ist damit die Irreduzibilität von f nachgewiesen.

Nun bestimmen wir noch das Minimalpolynom von β über $\mathbb{Q}$. Es gilt

$$\beta = i\sqrt{\sqrt{2}-1} \quad \Rightarrow \quad \beta^2 = -(\sqrt{2}-1) = 1-\sqrt{2} \quad \Rightarrow \quad \beta^2 - 1 = -\sqrt{2} \quad \Rightarrow \quad (\beta^2-1)^2 = 2$$
$$\Rightarrow \quad \beta^4 - 2\beta^2 + 1 = 2 \quad \Rightarrow \quad \beta^4 - 2\beta^2 - 1 = 0.$$

Es gilt also auch $f(\beta) = 0$, und wie wir bereits oben festgestellt haben, ist f normiert und irreduzibel über $\mathbb{Q}$. Dies zeigt, dass f auch das Minimalpolynom von β über $\mathbb{Q}$ ist.

zu (b) Da f nach Teil (a) sowohl das Minimalpolynom von α als auch das Minimalpolynom von β ist, gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 4$ und ebenso $[\mathbb{Q}(\beta) : \mathbb{Q}] = \mathrm{grad}(f) = 4$. Es ist aber $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$, denn

wegen $\alpha \in \mathbb{R}$ gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$; andererseits ist $\mathbb{Q}(\beta)$ wegen $\sqrt{\sqrt{2}-1} \in \mathbb{R}$ und $\beta = i\sqrt{\sqrt{2}-1} \notin \mathbb{R}$ kein Teilkörper von $\mathbb{R}$.

zu (c) Angenommen, $\mathbb{Q}(\alpha)|\mathbb{Q}$ ist eine normale Erweiterung. Dann zerfällt jedes über $\mathbb{Q}$ irreduzible Polynom, das in $\mathbb{Q}(\alpha)$ eine Nullstelle hat, über $\mathbb{Q}(\alpha)$ in Linearfaktoren. Das Polynom $f = x^4 - 2x^2 - 1$ ist, wie wir in Teil (a) gesehen haben, über $\mathbb{Q}$ irreduzibel, und es besitzt in $\mathbb{Q}(\alpha)$ eine Nullstelle, nämlich α. Auf Grund unserer Annahme zerfällt f somit über $\mathbb{Q}(\alpha)$ in Linearfaktoren. Dies bedeutet, dass alle komplexen Nullstellen von f bereits in $\mathbb{Q}(\alpha)$ enthalten sind, unter anderem auch die Nullstelle β. Aber wie in Teil (b) gezeigt wurde, gilt einerseits $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, andererseits aber $\beta \notin \mathbb{R}$. Damit kann β auch kein Element von $\mathbb{Q}(\alpha)$ sein, und folglich ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ nicht normal.

Nehmen wir nun an, dass $\mathbb{Q}(\beta)|\mathbb{Q}$ eine normale Erweiterung ist. Da f auch in $\mathbb{Q}(\beta)$ eine Nullstelle besitzt, nämlich β, kommen wir erneut zu dem Ergebnis, dass f über $\mathbb{Q}(\beta)$ in Linearfaktoren zerfällt. Damit ist dann die Nullstelle α in $\mathbb{Q}(\beta)$ enthalten, und es folgt $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$. Zusammen mit dem Ergebnis $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [\mathbb{Q}(\beta) : \mathbb{Q}]$ aus Teil (b) folgt daraus $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Aber dies hätte $\beta \in \mathbb{Q}(\alpha)$ zur Folge, was wir bereits ausgeschlossen haben. Somit ist auch die Erweiterung $\mathbb{Q}(\beta)|\mathbb{Q}$ nicht normal.

zu (d) Zunächst zeigen wir, dass die vier komplexen Nullstellen von f durch $\pm\alpha, \pm\beta$ gegeben sind. Weil f nur Terme mit geraden Exponenten enthält, gilt neben $f(\alpha) = f(\beta) = 0$ auch $f(-\alpha) = f(\alpha) = 0$ und $f(-\beta) = f(\beta) = 0$. Desweiteren sind die Elemente $\pm\alpha, \pm\beta$ alle verschieden. Denn wegen $f(0) \neq 0$ gilt $\alpha, \beta \neq 0$ und somit $-\alpha \neq \alpha$, $-\beta \neq \beta$. Auch die Gleichungen $\beta = \pm\alpha$ und $-\beta = \pm\alpha$ sind ausgeschlossen, denn wie wir in Teil (b) gesehen haben, sind $\pm\alpha$ im Gegensatz zu $\pm\beta$ reelle Zahlen. Durch $\pm\alpha, \pm\beta$ sind also vier komplexe Nullstellen von f gegeben, und wegen $\operatorname{grad}(f) = 4$ kann es keine weiteren Nullstellen in $\mathbb{C}$ geben.

Weil die Erweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}$ von α erzeugt wird, ist jedes Element $\sigma \in \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ bereits durch das Bild $\sigma(\alpha)$ festgelegt. Außerdem muss σ aus $\mathbb{Q}$-Automorphismus die Nullstelle α von $f \in \mathbb{Q}[x]$ wiederum auf eine Nullstelle von f abbilden. Es gibt für $\sigma(\alpha)$ also nur die vier Möglichkeiten $\{\pm\alpha, \pm\beta\}$. Wie in Teil (c) gezeigt wurde, ist aber β kein Element von $\mathbb{Q}(\alpha)$, und daraus folgt auch $\beta \notin \mathbb{Q}(\alpha)$ (denn mit $-\beta$ wäre auch $\beta = -(-\beta)$ in $\mathbb{Q}(\alpha)$ enthalten). Im Fall $\sigma(\alpha) = \beta$ oder $\sigma(\alpha) = -\beta$ wäre σ also keine Abbildung $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ und erst recht kein Automorphismus.

Somit ist nur $\sigma(\alpha) \in \{\pm\alpha\}$ möglich, d.h. $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ besitzt nicht mehr als zwei Elemente. Weil f über $\mathbb{Q}$ irreduzibel ist und $\pm\alpha$ Nullstellen von f sind, liefert der Fortsetzungssatz einen $\mathbb{Q}$-Homomorphismus $\tau_1 : \mathbb{Q}(\alpha) \to \mathbb{C}$ mit $\tau_1(\alpha) = -\alpha$. Wegen $-\alpha = \tau_1(\alpha) \in \mathbb{Q}(\alpha)$ gilt $\tau_1(\alpha) \in \mathbb{Q}(\alpha)$ und damit auch $\tau_1(\mathbb{Q}(\alpha)) \subseteq \mathbb{Q}(\alpha)$ (da τ_1 ein $\mathbb{Q}$-Homomorphismus ist). Jeder Körperhomomorphismus ist injektiv, und als injektiver Endomorphismus des endlich-dimensionalen $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\alpha)$ ist τ_1 auch bijektiv. Damit ist insgesamt $\tau_1 \in \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ nachgewiesen. Ein weiterer $\mathbb{Q}$-Homomorphismus ist die Identität $\mathrm{id}_{\mathbb{Q}(\alpha)}$ (die wegen $\tau(\alpha) \neq \alpha$ von τ verschieden ist). Da es in $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ nicht mehr als zwei Elemente gibt, haben wir damit insgesamt $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\mathrm{id}_{\mathbb{Q}(\alpha)}, \tau_1\}$ gezeigt. Weil neben $\beta \notin \mathbb{Q}(\alpha)$ nach Teil (c) auch $\alpha \notin \mathbb{Q}(\beta)$ gilt, kann auf analoge Weise gezeigt werden, dass $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\beta)) = \{\mathrm{id}_{\mathbb{Q}(\beta)}, \tau_2\}$ gilt, wobei τ_2 den eindeutig bestimmten $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\beta)$ mit $\tau_2(\beta) = -\beta$ bezeichnet.

Aufgabe H21T2A5

(a) Sei G eine Gruppe und $\mathrm{Aut}(G)$ deren Automorphismengruppe. Zeigen Sie, dass folgende Abbildung wohldefiniert ist und einen Gruppenhomomorphismus darstellt.

$$c : G \to \mathrm{Aut}(G) \quad , \quad g \mapsto [c_g : x \mapsto gxg^{-1}]$$

(b) Bezeichne S_3 die symmetrische Gruppe des Grades 3. Beweisen Sie, dass die Automorphismengruppe $\mathrm{Aut}(S_3)$ zur Gruppe S_3 isomorph ist.

Lösung:
zu (a) Für den Nachweis, dass c eine wohldefinierte Abbildung ist, müssen wir zeigen, dass c_g für jedes $g \in G$ ein Element aus $\mathrm{Aut}(G)$ ist. Für jedes $g \in G$ ist $c_g : G \to G$, $x \mapsto gxg^{-1}$ ein Gruppenhomomorphismus, denn es gilt $c_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = c_g(h_1)c_g(h_2)$ für alle $h_1, h_2 \in G$. Außerdem ist c_g für jedes $g \in G$ bijektiv, denn durch c_g^{-1} ist jeweils eine Umkehrabbildung von c_g gegeben: Für alle $h \in G$ gilt $(c_{g^{-1}} \circ c_g)(h) = c_{g^{-1}}(c_g(h)) = c_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}g = ehe = h = \mathrm{id}_G(h)$ und ebenso $(c_g \circ c_{g^{-1}})(h) = c_g(g^{-1}h(g^{-1})^{-1}) = gg^{-1}hgg^{-1} = ehe = h = \mathrm{id}_G(h)$, also $c_{g^{-1}} \circ c_g = \mathrm{id}_G$ und $c_g \circ c_{g^{-1}} = \mathrm{id}_G$. Insgesamt ist c_g damit für jedes $g \in G$ ein Automorphismus von G.

Nun muss noch gezeigt werden, dass durch $G \to \mathrm{Aut}(G)$, $g \mapsto c_g$ ein Gruppenhomomorphismus gegeben ist. Seien $g_1, g_2 \in G$ vorgegeben. Für jedes $h \in G$ gilt $(c_{g_1} \circ c_{g_2})(h) = c_{g_1}(c_{g_2}(h)) = c_{g_1}(g_2hg_2^{-1}) = g_1(g_2hg_2^{-1})g_1^{-1} = (g_1g_2)h(g_1g_2)^{-1} = c_{g_1g_2}(h)$. Daraus folgt $c(g_1g_2) = c_{g_1g_2} = c_{g_1} \circ c_{g_2} = c(g_1) \circ c(g_2)$.

zu (b) Nach Teil (a) existiert ein Gruppenhomomorphismus $c : S_3 \to \mathrm{Aut}(S_3)$, $\sigma \mapsto [c_\sigma : \tau \mapsto \sigma\tau\sigma^{-1}]$. Wir zeigen, dass c injektiv und surjektiv ist. Zum Nachweis der Injektivität sei $\sigma \in \ker(c)$ vorgegeben. Zu zeigen ist $\sigma = \mathrm{id}$. Wegen $\sigma \in \ker(c)$ gilt $c_\sigma = c(\sigma) = \mathrm{id}_{S_3}$, also $\sigma\tau\sigma^{-1} = c_\sigma(\tau) = \mathrm{id}_{S_3}(\tau) = \tau$ für alle $\tau \in S_3$. Dies ist gleichbedeutend mit $\sigma\tau = \tau\sigma$ für alle $\tau \in S_3$, d.h. σ ist im Zentrum $Z(S_3)$ von S_3 enthalten. Aber wegen $(1\,2) \circ (1\,3) = (1\,3\,2) \neq (1\,2\,3) = (1\,3) \circ (1\,2)$ und $(1\,2) \circ (2\,3) = (1\,2\,3) \neq (1\,3\,2) = (2\,3) \circ (1\,2)$ sind die Transpositionen $(1\,2), (1\,3), (2\,3)$ keine Elemente des Zentrums, und die Ungleichungen $(1\,2\,3) \circ (1\,2) = (1\,3) \neq (2\,3) = (1\,2) \circ (1\,2\,3)$ und $(1\,3\,2) \circ (1\,2) = (2\,3) \neq (1\,3) = (1\,2) \circ (1\,3\,2)$ zeigen, dass $Z(S_3)$ auch keine 3-Zykel enthält. Es gilt also $Z(S_3) = \{\mathrm{id}\}$. Damit ist $\sigma = \mathrm{id}$ und die Injektivität von σ nachgewiesen. (Eventuell ist auch aus der Vorlesung bekannt, dass $Z(S_n)$ für $n \neq 2$ ein triviales Zentrum besitzt.)

Durch $\{(1\,2), (1\,2\,3)\}$ ist ein zweielementige Erzeugendensystem von S_3 definiert. Setzen wir nämlich $U = \langle (1\,2), (1\,2\,3) \rangle$, dann ist die Ordnung von U wegen $(1\,2) \in U$ ein Vielfaches von $\mathrm{ord}((1\,2)) = 2$ und wegen $(1\,2\,3) \in U$ auch ein Vielfaches von $\mathrm{ord}((1\,2\,3)) = 3$. Insgesamt ist $|U|$ also ein Vielfaches von $\mathrm{kgV}(2,3) = 6 = |S_3|$, und aus $U \subseteq S_3$ und $|U| \geq |S_3|$ folgt $U = S_3$. Weil die Gruppe S_3 von $\{(1\,2), (1\,2\,3)\}$ erzeugt wird, ist jedes $\phi \in \mathrm{Aut}(S_3)$ durch die Bilder $\phi((1\,2))$ und $\phi((1\,2\,3))$ bereits eindeutig festgelegt. Außerdem ist bekannt, dass ein Automorphismus jedes Gruppenelement jeweils auf ein Element gleicher Ordnung abbildet. Für $\phi((1\,2))$ kommen also nur die drei Transpositionen und für $\phi((1\,2\,3))$ nur die beiden 3-Zykel in Frage.

Dies zeigt, dass $|\mathrm{Aut}(S_3)|$ aus höchstens $3 \cdot 2 = 6$ Elementen besteht. Andererseits besitzt $\mathrm{Aut}(S_3)$ auf Grund der Injektivität von c eine zu S_3 isomorphe Untergruppe, nämlich $c(S_3)$. Wegen $|c(S_3)| = |S_3| = 6 \geq |\mathrm{Aut}(S_3)|$ und $c(S_3) \subseteq \mathrm{Aut}(S_3)$ muss $c(S_3) = \mathrm{Aut}(S_3)$ gelten. Durch c ist also ein Isomorphismus zwischen S_3 und $\mathrm{Aut}(S_3)$ definiert.

Aufgabe H21T3A1

Sei S_5 die symmetrische Gruppe auf $\{1,2,3,4,5\}$ und sei $A_5 \leq S_5$ die alternierende Gruppe. Zeigen Sie die folgenden Aussagen:

(a) Sei $U \leq S_5$ eine Untergruppe mit 3 oder 5 Elementen. Dann ist $U \leq A_5$.

(b) S_5 hat genau 10 Untergruppen der Ordnung 3

(c) S_5 hat genau 6 Untergruppen der Ordnung 5

Lösung:
zu (a) Sei zunächst U eine Untergruppe mit $|U| = 5$. Auf Grund der Primzahlordnung 5 ist U zyklisch, es gibt also ein Element $\sigma \in S_5$ mit $\text{ord}(\sigma) = 5$. Dieses Element ist ein 5-Zykel. Ist nämlich $(k_1, ..., k_r)$ der Zerlegungstyp von σ (mit $r, k_1, ..., k_r \in \mathbb{N}$, $k_1 \geq ... \geq k_r \geq 2$), dann gilt $k_1 + ... + k_r \leq 5$ und $\text{kgV}(k_1, ..., k_r) = \text{ord}(\sigma) = 5$. Auf Grund der letzten Gleichung teilt die 5 zumindest eine der Zykellängen $k_1, ..., k_r$; auf Grund der Ungleichung $k_1 + ... + k_r \leq 5$ ist dies nur für $r = 1$ und $k_1 = 5$ möglich. Da σ ein 5-Zykel ist, gilt $\text{sgn}(\sigma) = (-1)^{5-1} = (-1)^4 = 1$ und somit $\sigma \in A_5$. Daraus wiederum folgt $U = \langle\sigma\rangle \leq A_5$.

Betrachten wir nun den Fall $|U| = 3$. Auch 3 ist eine Primzahl, die Untergruppe U somit zyklisch, $U = \sigma$ für ein $\sigma \in S_5$ mit $\text{ord}(\sigma) = 3$. Sei $(k_1, ...k_r)$ wie oben der Zerlegungstyp von σ. Wegen $\text{kgV}(k_1, ..., k_r) = 3$ gilt $3 \mid k_i$ für ein $i \in \{1, ..., r\}$. Wegen $k_1 + ... + k_r \leq 5$ folgt daraus zunächst $r = 1$, $k_1 = 3$ oder $r = 2$, $k_1 = 3$, $k_2 = 2$. Im zweiten Fall wäre aber $\text{ord}(\sigma) = \text{kgV}(3, 2) = 6$, im Widerspruch zu $\text{ord}(\sigma) = 3$. Also bleibt $r = 1$, $k_1 = 3$ als einzige Möglichkeit, und σ ist ein 3-Zykel. Es folgt $\text{sgn}(\sigma) = (-1)^{3-1} = (-1)^2 = 1$ und $\sigma \in A_5$, und wiederum erhalten wir $U = \langle\sigma\rangle \leq A_5$.

zu (b) Wir haben bereits in Teil (a) festgestellt, dass jede Untergruppe der Ordnung 3 von S_5 zyklisch ist. Jede solche Gruppe enthält $\varphi(3) = 2$ Elemente der Ordnung 3, und umgekehrt ist jedes $\sigma \in S_5$ mit $\text{ord}(\sigma) = 3$ in genau einer zyklischen Untergruppe der Ordnung 3 enthalten, nämlich in $\langle\sigma\rangle$. Es gibt also doppelt so viele Elemente der Ordnung 3 wie Untergruppen der Ordnung 3. Die Anzahl der 3-Zykel in S_5 ist gleich $\binom{5}{3} \cdot (3-1)! = 10 \cdot 2 = 20$, denn für den Träger des 3-Zykels, eine dreielementige Teilmenge von $M_5 = \{1, 2, ..., 5\}$ gibt es $\binom{5}{3}$ Möglichkeiten, und nach Wahl des Trägers gibt es noch $(3-1)!$ Möglichkeiten für den 3-Zykel. Die Anzahl der Untergruppen der Ordnung 3 ist also gleich $\frac{1}{2} \cdot 20 = 10$.

zu (c) Aus Teil (a) wissen wir auch bereits, dass jede Untergruppe der Ordnung 5 zyklisch ist. Jede solche Gruppe enthält $\varphi(5) = 4$ Elemente der Ordnung 5, und umgekehrt ist jedes $\sigma \in S_5$ mit $\text{ord}(\sigma)$ in genau einer zyklischen Untergruppe der Ordnung 5 enthalten, nämlich in $\langle\sigma\rangle$. Es gibt also viermal so viele Elemente der Ordnund 5 wie Untergruppen der Ordnung 5. Die Anzahl der 5-Zykel in S_5 ist gleich $(5-1)! = 24$, denn der Träger eines 5-Zykels ist zwangsläufig die gesamte Menge $M_5 = \{1, 2, ..., 5\}$, und allgemein gibt es in S_n jeweils genau $(k-1)!$ k-Zykel mit festem Träger, für alle $k, n \in \mathbb{N}$ mit $2 \leq k \leq n$. Die Anzahl der Untergruppen der Ordnung 5 ist also gleich $\frac{1}{4} \cdot 24 = 6$.

Aufgabe H21T3A2

Es sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der endliche Körper mit p Elementen. Wir betrachten die Menge

$$G \quad = \quad \left\{ \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \;\middle|\; a \in \mathbb{F}_p^\times \;,\; b \in \mathbb{F}_p \right\}$$

von 2×2-Matrizen über dem Körper $\mathbb{F}_p$.

(a) Zeigen Sie, dass $G \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ ist.

(b) Zeigen Sie, dass G eine Gruppe ist.

(c) Bestimmen Sie alle Primzahlen p, für die G abelsch ist.

(d) Bestimmen Sie alle Primzahlen p, für die G zu einer symmetrischen Gruppe S_n isomorph ist.

Lösung:

zu (a) Für alle $a \in \mathbb{F}_p^\times$ und alle $b \in \mathbb{F}_p$ gilt

$$\det \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \quad = \quad a \cdot \bar{1} \quad = \quad a \quad \neq \quad \bar{0}.$$

Dies zeigt, dass die Matrix $\begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix}$ jeweils invertierbar ist, also in $\mathrm{GL}_2(\mathbb{F}_p)$ liegt.

zu (b) Wegen Teil (a) genügt es zu zeigen, dass G eine Untergruppe von $\mathrm{GL}_2(\mathbb{F}_p)$ ist. (Denn jede Untergruppe von $\mathrm{GL}_2(\mathbb{F}_p)$ ist insbesondere eine Gruppe.) Das Neutralelement von $\mathrm{GL}_2(\mathbb{F}_p)$ ist die Einheitsmatrix $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$, und wegen $\bar{1} \in \mathbb{F}_p^\times$ und $\bar{0} \in \mathbb{F}_p$ ist diese in G enthalten.
Seien nun $A_1, A_2 \in G$ vorgegeben. Dann gibt es $a_1, a_2 \in \mathbb{F}_p^\times$ und $b_1, b_2 \in \mathbb{F}_p$ mit

$$A_1 = \begin{pmatrix} a_1 & b_1 \\ \bar{0} & \bar{1} \end{pmatrix} \qquad \text{und} \qquad A_2 = \begin{pmatrix} a_2 & b_2 \\ \bar{0} & \bar{1} \end{pmatrix}.$$

Auf Grund der Gleichung

$$A_1 A_2 \quad = \quad \begin{pmatrix} a_1 & b_1 \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ \bar{0} & \bar{1} \end{pmatrix} \quad = \quad \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 \\ \bar{0} & \bar{1} \end{pmatrix}$$

und $a_1 a_2 \in \mathbb{F}_p^\times$, $a_1 b_2 + b_1 \in \mathbb{F}_p$ ist auch $A_1 A_2$ in G enthalten. Wegen

$$\begin{pmatrix} a_1 & b_1 \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} a_1^{-1} & -a_1^{-1} b_1 \\ \bar{0} & \bar{1} \end{pmatrix} \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$$

und $a_1^{-1} \in \mathbb{F}_p^\times$, $-a_1^{-1} b_1 \in \mathbb{F}_p$ ist auch $A_1^{-1} = \begin{pmatrix} a_1^{-1} & -a_1^{-1} b_1 \\ \bar{0} & \bar{1} \end{pmatrix}$ in G enthalten.

zu (c) Im Fall $p = 2$ gilt $|\mathbb{F}_p^\times| = 1$ und $|\mathbb{F}_p| = 2$. Jedes Element aus G ist durch die beiden Einträge $a \in \mathbb{F}_p^\times$ und $b \in \mathbb{F}_p$ eindeutig festgelegt. Daraus folgt $|G| = 1 \cdot 2 = 2$, und als Gruppe von Primzahlordnung ist G zyklisch, insbesondere abelsch. Sei nun p eine ungerade Primzahl. Dann gibt es ein $a \in \mathbb{F}_p^\times$ ungleich $\bar{1}$, und die Matrizen

$$A = \begin{pmatrix} a & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \qquad \text{und} \qquad T = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$$

sind beides Elemente von G. Wegen

$$AT = \begin{pmatrix} a & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} a & a \\ \bar{0} & \bar{1} \end{pmatrix} \qquad , \qquad TA = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} a & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} a & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$$

gilt aber $TA \neq AT$ wegen $a \neq \bar{1}$. Für jede ungerade Primzahl p ist die Gruppe G also nicht abelsch.

zu (d) Sei p eine beliebige Primzahl. Jedes Element der Gruppe G ist durch die Einträge $a \in \mathbb{F}_p^\times$ und $b \in \mathbb{F}_p$ eindeutig festgelegt. Da es für a jeweils $p-1$ und für b jeweils p Möglichkeiten gibt, gilt $|G| = p(p-1)$. Nehmen wir nun an, G ist isomorph zu S_n für ein $n \in \mathbb{N}$. Dann folgt $p(p-1) = |G| = |S_n| = n!$. Da der Primfaktor p in $n!$ vorkommt, muss $n \geq p$ gelten. Ist nun $p \geq 5$, dann ergibt sich der Widerspruch $n! \geq p! \geq p(p-1)(p-2) \geq p(p-1) \cdot 3 > p(p-1)$. Somit ist $G \cong S_n$ nur für $p \in \{2, 3\}$ möglich. In Teil (c) haben wir bereits festgestellt, dass G im Fall $p = 2$ zyklisch von Ordnung 2 ist, und dasselbe gilt auch für S_2. Da je zwei zyklische Gruppen derselben Ordnung isomorph sind, folgt $G \cong S_2$ für $p = 2$.

Um zu zeigen, dass G im Fall $p = 3$ zu S_3 isomorph ist, betrachten wir eine Operation von G auf einer geeigneten dreielementigen Menge. Sei $X = \{(c, \bar{1}) \mid c \in \mathbb{F}_3\} = \{(\bar{0}, \bar{1}), (\bar{1}, \bar{1}), (\bar{2}, \bar{1})\} \subseteq \mathbb{F}_3^2\}$. Für alle $a \in \mathbb{F}_3^\times$ und $b, c \in \mathbb{F}_3$ gilt

$$\begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} c \\ \bar{1} \end{pmatrix} = \begin{pmatrix} ac + b \\ \bar{1} \end{pmatrix} \in X.$$

Dies zeigt, dass durch $(A, v) \mapsto Av$ eine Abbildung $* : G \times X \to X$ definiert ist. Dabei handelt es sich um eine Gruppenoperation, denn es gilt $E * v = Ev = v$ für alle $v \in X$ (wobei E die Einheitsmatrix bezeichnet) und $A_1 * (A_2 * v) = A_1 * (A_2 v) = A_1(A_2 v) = (A_1 A_2)v = (A_1 A_2) * v$ für alle $A_1, A_2 \in G$ und $v \in X$. Laut Vorlesung liefert die Operation einen Gruppenhomomorphismus $\phi : G \to \mathrm{Per}(X)$, gegeben durch $\phi(A)(v) = A * v = Av$ für alle $A \in G$ und $v \in X$. Dieser Homomorphismus ist injektiv. Sei nämlich $A \in \ker(\phi)$ vorgegeben,

$$A = \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \qquad \text{mit} \quad a \in \mathbb{F}_3^\times \text{ und } b \in \mathbb{F}_3.$$

Dann gilt $\phi(A) = \mathrm{id}_X$ und $Av = \phi(A)(v) = \mathrm{id}_X(v) = v$ für alle $v \in X$. Aus den Gleichungen

$$\begin{pmatrix} b \\ \bar{1} \end{pmatrix} = \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} a + b \\ \bar{1} \end{pmatrix} = \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix}$$

folgt dann $b = \bar{0}$ und $a + b = \bar{1}$, also $a = \bar{1}$ und $b = \bar{0}$ und somit $A = E$.

Wegen $|X| = 3$ gilt $\mathrm{Per}(X) \cong S_3$ und $|\mathrm{Per}(X)| = |S_3| = 6 = |G|$. Aus dieser Gleichheit und der Injektivität von ϕ folgt, dass ϕ bijektiv ist. Also ist ϕ ein Isomorphismus, und es gilt $G \cong \mathrm{Per}(X) \cong S_3$ im Fall $p = 3$.

Aufgabe H21T3A3

Sei $L|K$ eine endliche Körpererweiterung und sei $\alpha \in L$. Zeigen Sie:

(a) Das Minimalpolynom f_α der K-linearen Abbildung $\varphi_\alpha : L \to L$, $x \mapsto \alpha x$, ist gleich dem Minimalpolynom g_α von α über K.

(b) Ist $L = K(\alpha)$, so stimmen das charakteristische Polynom und das Minimalpolynom von φ_α überein.

Lösung:
zu (a) Wir zeigen, dass für jedes Polynom $f \in K[x]$ genau dann $f(\alpha) = 0$ gilt, wenn die K-lineare Abbildung $f(\varphi_\alpha) : L \to L$ die Nullabbildung ist, also $f(\varphi_\alpha) = 0_{\mathrm{End}_K(L)}$ gilt. Nach Definition ist f_α das eindeutig bestimmte, normierte Polynom minimalen Grades mit $f_\alpha(\varphi_\alpha) = 0_{\mathrm{End}_K(L)}$, und g_α ist das eindeutig bestimmte, normierte Polynom minimalen Grades mit $g_\alpha(\alpha) = 0$. Aus der behaupteten Äquivalenz folgt also die Übereinstimmung von f_α und g_α.

Sei also $f \in K[x]$ vorgegeben, $f = a_n x^n + ... + a_1 x + a_0$ mit $n \in \mathbb{N}$ und $a_0, ..., a_n \in K$. Ist $f(\alpha) = 0$, dann folgt $\sum_{k=0}^{n} a_k \alpha^k = 0$. Für alle $\beta \in L$ erhalten wir

$$\begin{aligned} f(\varphi_\alpha)(\beta) &= \left(\sum_{k=0}^{n} a_k \varphi_\alpha^k\right)(\beta) = \sum_{k=0}^{n} a_k \varphi_\alpha^k(\beta) = \sum_{k=0}^{n} a_k \alpha^k \beta \\ &= f(\alpha) \cdot \beta = 0 \cdot \beta = 0 \quad , \end{aligned}$$

wobei im dritten Schritt verwendet wurde, dass $\varphi_\alpha(\beta) = \alpha\beta$ und $\varphi_\alpha^k(\beta) = \alpha^k \beta$ für alle $k \in \mathbb{N}_0$ gilt. Aus $f(\varphi_\alpha)(\beta) = 0$ für alle $\beta \in L$ folgt $f(\varphi_\alpha) = 0_{\mathrm{End}_K(L)}$. Setzen wir nun diese Gleichung umgekehrt voraus, dann gilt insbesondere

$$\begin{aligned} 0 = 0_{\mathrm{End}_K(L)}(1) = f(\varphi_\alpha)(1) &= \left(\sum_{k=0}^{n} a_k \varphi_\alpha^k\right)(1) = \sum_{k=0}^{n} (a_k \varphi_\alpha^k)(1) \\ &= \sum_{k=0}^{n} a_k \alpha^k \cdot 1 = \sum_{k=0}^{n} a_k \alpha^k = f(\alpha) \quad , \end{aligned}$$

also $f(\alpha) = 0$. Damit ist die behauptete Äquivalenz insgesamt bewiesen.

zu (b) Aus der Linearen Algebra ist bekannt, dass für jeden Endomorphismus eines endlichdimensionalen K-Vektorraums V das Minimalpolynom stets ein Teiler des charakteristischen Polynoms ist. Außerdem ist der Grad des charakteristischen Polynoms immer gleich der Dimension von V.

Das Minimalpolynom f_α von φ_α ist also ein Teiler des charakteristischen Polynoms χ_{φ_α} von φ_α. Da $L|K$ eine endliche Erweiterung ist, und $K(\alpha)$ wegen $\alpha \in L$ ein Zwischenkörper von $L|K$, ist auch $n = [K(\alpha) : K]$ endlich. Aus der allgemeinen Aussage zum Grad des charakteristischen Polynoms folgt $\mathrm{grad}(\chi_{\varphi_\alpha}) = \dim_K K(\alpha) = [K(\alpha) : K] = n$, wobei $\dim_K K(\alpha)$ die Dimension von $K(\alpha)$ als K-Vektorraum bezeichnet. Nach Teil (a), und weil g_α das Minimalpolynom von α ist, gilt andererseits $n = [K(\alpha) : K] = \mathrm{grad}(g_\alpha) = \mathrm{grad}(f_\alpha)$. Da f_α ein Teiler von χ_{φ_α} ist, die beiden Polynome aber andererseits denselben Grad haben, stimmen sie überein.

Aufgabe H21T3A4

Es sei $\mathbb{F}_2$ der Körper mit zwei Elementen und $f = x^4 + x + \bar{1} \in \mathbb{F}_2[x]$.

(a) Zeigen Sie, dass f irreduzibel ist.

(b) Sei $K = \mathbb{F}_2[x]/(f) = \mathbb{F}_2(\alpha)$ mit $\alpha = \bar{x}$ die durch Adjunktion einer Nullstelle von f entstandene algebraische Körpererweiterung von $\mathbb{F}_2$. Zeigen Sie, dass α ein Erzeuger der multiplikativen Gruppe $K^\times$ ist.

(c) Zeigen Sie: In $K[x]$ gilt $f = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$.

Lösung:
zu (a) Wegen $f(\bar{0}) = \bar{1} \neq \bar{0}$ und $f(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$ besitzt f in $\mathbb{F}_2$ keine Nullstelle. Ist f dennoch reduzibel in $\mathbb{F}_2[x]$, dann muss das Polynom wegen $\operatorname{grad}(f) = 4$ das Produkt zweier irreduzibler Polynome vom Grad 2 sein. Das einzige irreduzible Polynom vom Grad 2 über $\mathbb{F}_2$ ist bekanntlich $x^2 + x + \bar{1}$. Es gilt aber

$$(x^2 + x + \bar{1})(x^2 + x + \bar{1}) \quad = \quad x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + \bar{1} \quad = \quad x^4 + x^2 + \bar{1} \quad \neq \quad f.$$

Also ist f irreduzibel über $\mathbb{F}_2$.

zu (b) Da f normiert und irreduzibel über $\mathbb{F}_2$ ist und α als Nullstelle besitzt, ist f das Minimalpolynom von α über $\mathbb{F}_2$. Daraus folgt $[K : \mathbb{F}_2] = \operatorname{grad}(f) = 4$. Es ist K also ein vierdimensionaler $\mathbb{F}_2$-Vektorraum und besteht als solcher aus $2^4 = 16$ Elementen. Die multiplikative Gruppe $K^\times = K \setminus \{0\}$ enthält somit $16 - 1 = 15$ Elemente. Wegen $f(\bar{0}) \neq \bar{0}$ ist α ungleich null, also in $K^\times$ enthalten. Das Element α ist genau dann ein Erzeuger von $K^\times$, wenn es ein Element der Ordnung 15 ist. Wegen $|K^\times| = 15$ ist $\operatorname{ord}(\alpha)$ jedenfalls ein Teiler von 15. Es gilt $\operatorname{ord}(\alpha) = 15$ genau dann, wenn $\alpha^3 \neq \bar{1}$ und $\alpha^5 \neq \bar{1}$ gilt. Die Gleichung $\alpha^3 = \bar{1}$ ist ausgeschlossen, denn ansonsten wäre α eine Nullstelle des Polynoms $x^3 - \bar{1}$. Weil das Minimalpolynom von α aber vom Grad 4 ist, existiert kein Polynom ungleich null mit einem kleineren Grad als 4, das α als Nullstelle hat. Nehmen wir nun an, es gilt $\alpha^5 = \bar{1}$. Wegen $\alpha^4 + \alpha + \bar{1} = f(\alpha) = \bar{0}$ gilt $\alpha^4 = -\bar{1} - \alpha = \bar{1} + \alpha$. Aus $\alpha^4 \cdot \alpha = \alpha^5 = \bar{1}$ folgt also $\alpha^2 + \alpha = (\alpha + \bar{1}) \cdot \alpha = \bar{1} = -\bar{1}$ und somit $\alpha^2 + \alpha + \bar{1} = \bar{0}$. Es wäre α also eine Nullstelle von $x^2 + x + \bar{1}$, was wiederum ausgeschlossen ist, weil das Minimalpolynom von α vom Grad 4 ist.

zu (c) Das Polynom $g = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) \in K[x]$ ist vom Grad 4, normiert, und besitzt α als Nullstelle. Wenn wir zeigen können, dass g darüber hinaus in $\mathbb{F}_2[x]$ enthalten ist, dann ist g insgesamt das Minimalpolynom von α über $\mathbb{F}_2$, und aus der Eindeutigkeit des Minimalpolynoms folgt $g = f$. Sei $\varphi : K \to K$ der Frobenius-Automorphismus definiert durch $\varphi(\gamma) = \gamma^2$ für alle $\gamma \in K$. Aus der Vorlesung ist bekannt, dass jedes $\gamma \in K$ genau dann in $\mathbb{F}_2$ liegt, wenn $\varphi(\gamma) = \gamma$ gilt. Wir können γ zu einem Automorphismus des Polynomrings $K[x]$ fortsetzen, indem wir γ auf die Koeffizienten der Polynome anwenden. Bemerken wir noch, dass wegen $|K^\times| = 15$ und $\alpha \in K^\times$ die Gleichungen $\alpha^{15} = \bar{1}$ und $\alpha^{16} = \alpha$ gelten, so erhalten wir

$$\begin{aligned} \varphi(g) \quad &= \quad (x - \varphi(\alpha))(x - \varphi(\alpha^2))(x - \varphi(\alpha^4))(x - \varphi(\alpha^8)) \quad = \\ (x-\alpha^2)(x-(\alpha^2)^2)(x-(\alpha^4)^2)(x-(\alpha^8)^2) \quad &= \quad (x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16}) \\ = \quad (x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^1) \quad &= \quad g. \end{aligned}$$

Alle Koeffizienten von g bleiben also unter der Anwendung von φ unverändert. Sie liegen also in $\mathbb{F}_2$, und damit gilt tatsächlich $g \in \mathbb{F}_2[x]$.

Aufgabe H21T3A5

Seien m und n zwei positive ganze Zahlen mit $\mathrm{ggT}(m,n) = 1$. Für jede positive ganze Zahl a sei $\zeta_a = e^{2\pi i/a} \in \mathbb{C}$; ζ_a ist eine primitive a-te Einheitswurzel. Beweisen Sie die folgenden Aussagen:

(a) $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$

(b) $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$

(c) $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$

Lösung:
zu (a) Zu zeigen ist $\zeta_m, \zeta_n \in \mathbb{Q}(\zeta_{mn})$ und $\zeta_{mn} \in \mathbb{Q}(\zeta_m, \zeta_n)$. Die ersten Aussage ist wegen $\zeta_m = e^{2\pi i/m} = (e^{2\pi i/(mn)})^n = \zeta_{mn}^n \in \mathbb{Q}(\zeta_{mn})$ und $\zeta_n = e^{2\pi i/n} = (e^{2\pi i/(mn)})^m = \zeta_{mn}^m \in \mathbb{Q}(\zeta_{mn})$ offenbar erfüllt. Für die zweite Aussage bemerken wir zunächst, dass wegen $\mathrm{ggT}(m,n) = 1$ und auf Grund des Lemmas von Bézout ganze Zahlen a, b mit $am + bn = 1$ existieren. Es folgt $\frac{1}{mn} = \frac{a}{n} + \frac{b}{m}$ und

$$\zeta_{mn} \quad = \quad e^{2\pi i/(mn)} \quad = \quad e^{2\pi i \cdot (\frac{a}{n} + \frac{b}{m})} \quad = \quad e^{2\pi i a/n} e^{2\pi i b/m} \quad = \quad \zeta_n^a \zeta_m^b.$$

Dies zeigt, dass ζ_{mn} in $\mathbb{Q}(\zeta_m, \zeta_n)$ enthalten ist.

zu (b) Laut Vorlesung gilt $[\mathbb{Q}(\zeta_\ell) : \mathbb{Q}] = \varphi(\ell)$ für alle $\ell \in \mathbb{N}$, wobei φ die Eulersche φ-Funktion bezeichnet. Weil m und n teilerfremd sind, gilt $\varphi(mn) = \varphi(m)\varphi(n)$. Zusammen mit dem Ergebnis aus Teil (a) erhalten wir

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] \quad = \quad \varphi(mn) \quad = \quad \varphi(m)\varphi(n) \quad = \quad [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

zu (c) Aus der Vorlesung ist bekannt, dass $\mathbb{Q}(\zeta_\ell)|\mathbb{Q}$ für jedes $\ell \in \mathbb{N}$ eine Galois-Erweiterung ist, und dass ferner ein Isomorphismus $\psi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)|\mathbb{Q})$ mit $\psi(a + \ell\mathbb{Z}) = \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, \ell) = 1$ existiert, wobei $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)|\mathbb{Q})$ jeweils den Automorphismus bezeichnet, der durch $\sigma_a(\zeta_\ell) = \zeta_\ell^a$ eindeutig bestimmt ist.

Sei nun $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{mn})|\mathbb{Q})$. Auf Grund des Hauptsatzes der Galoistheorie genügt es zu zeigen, dass die Untergruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_{mn})|\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))$ mit ganz G übereinstimmt, denn dann stimmen die zugehörigen Fixkörper $\mathbb{Q}$ bzw. $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$ überein. Sei also $\sigma \in G$ vorgegeben; zu zeigen ist $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{mn})|\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))$. Für ein vorgegebenes $\gamma \in \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$ muss also die Gleichung $\sigma(\gamma) = \gamma$ bewiesen werden.

Auf Grund der oben angebenen Beschreibung der Elemente von G existiert ein $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, mn) = 1$ und $\sigma(\zeta_{mn}) = \zeta_{mn}^a$. Nach dem

Chinesischen Restsatzes existiert ein Isomorphismus $\phi : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\phi(c + mn\mathbb{Z}) = (c + m\mathbb{Z}, c + n\mathbb{Z})$ für alle $c \in \mathbb{Z}$. Seien $b, c \in \mathbb{Z}$ Repräsentanten der Urbilder $b + mn\mathbb{Z} = \phi^{-1}(a + m\mathbb{Z}, 1 + n\mathbb{Z})$ und $c + mn\mathbb{Z} = \phi^{-1}(1 + m\mathbb{Z}, a + n\mathbb{Z})$. Auf Grund der Definition von ϕ gilt $b \equiv a \bmod m$, $b \equiv 1 \bmod n$, $c \equiv 1 \bmod m$ und $c \equiv a \bmod n$. Es gibt also $r, s, t, u \in \mathbb{Z}$ mit $b = a + rm = 1 + sn$ und $c = 1 + tm = a + un$. Wegen $\phi(bc + mn\mathbb{Z}) = \phi(b + mn\mathbb{Z})\phi(c + mn\mathbb{Z}) = (a + m\mathbb{Z}, 1 + n\mathbb{Z})(1 + m\mathbb{Z}, a + n\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z}) = \phi(a + mn\mathbb{Z})$ und der Bijektivität von ϕ gilt auch $bc + mn\mathbb{Z} = a + mn\mathbb{Z}$, also $bc \equiv a \bmod (mn)$ und somit $a = bc + vmn$ für ein $v \in \mathbb{Z}$.

Seien nun die Elemente $\rho, \tau \in G$ gegeben durch $\rho(\zeta_{mn}) = \zeta_{mn}^b$ und $\tau(\zeta_{mn}) = \zeta_{mn}^c$. Dann gilt

$$(\rho \circ \tau)(\zeta_{mn}) \quad = \quad \rho(\tau(\zeta_{mn})) \quad = \quad \rho(\zeta_{mn}^c) \quad = \quad \rho(\zeta_{mn})^c \quad = \quad (\zeta_{mn}^c)^b \quad = \quad \zeta_{mn}^{bc} \quad =$$
$$\zeta_{mn}^{a - vmn} \quad = \quad \zeta_{mn}^a (\zeta_{mn}^{mn})^{-v} \quad = \quad \zeta_{mn}^a \cdot 1^{-v} \quad = \quad \zeta_{mn}^a \quad = \quad \sigma(\zeta_{mn}).$$

Weil jedes Element aus G durch das Bild von ζ_{mn} eindeutig festgelegt ist, folgt daraus $\sigma = \rho \circ \tau$. Nun gilt außerdem

$$\begin{aligned}\rho(\zeta_n) &= \rho(\zeta_{mn}^m) = \rho(\zeta_{mn})^m = (\zeta_{mn}^b)^m = \zeta_{mn}^{bm} = \zeta_n^b = \zeta_n^{1+sn} = \\ &\zeta_n \cdot (\zeta_n^n)^s = \zeta_n \cdot 1^s = \zeta_n.\end{aligned}$$

Dies zeigt, dass ζ_n im Fixkörper $\mathbb{Q}(\zeta_{mn})^{\langle\rho\rangle}$ enthalten ist, also auch $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})^{\langle\rho\rangle}$ gilt. Wegen $\gamma \in \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})^{\langle\rho\rangle}$ folgt $\rho(\gamma) = \gamma$. Genauso beweist man auch die Gleichung $\tau(\gamma) = \gamma$. Denn zunächst gilt

$$\begin{aligned}\tau(\zeta_m) &= \tau(\zeta_{mn}^n) = \tau(\zeta_{mn})^n = (\zeta_{mn}^c)^n = \zeta_{mn}^{cn} = \zeta_m^c = \zeta_m^{1+tm} = \\ &\zeta_m \cdot (\zeta_m^m)^t = \zeta_m \cdot 1^t = \zeta_m.\end{aligned}$$

Das Element ζ_m liegt also im Fixkörper von $\langle\tau\rangle$, es gilt somit $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{mn})^{\langle\tau\rangle}$. Wegen $\gamma \in \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{mn})^{\langle\tau\rangle}$ folgt $\tau(\gamma) = \gamma$. Insgesamt erhalten wir nun $\sigma(\gamma) = (\rho \circ \tau)(\gamma) = \rho(\tau(\gamma)) = \rho(\gamma) = \gamma$, wie gewünscht.

Aufgabe F22T1A1

Sei $A \in \mathcal{M}_{2,\mathbb{Q}}$ eine 2×2-Matrix mit rationalen Einträgen, so dass A^n die Einheitsmatrix I_2 ist für ein $n \geq 1$. Sei $m_A \in \mathbb{Q}[x]$ das Minimalpolynom von A. Zeigen Sie:

(a) Der Grad von m_A ist höchstens 2.

(b) Das Polynom m_A ist ein Teiler von $x^n - 1$ in $\mathbb{Q}[x]$.

(c) Wählt man $n \geq 1$ minimal mit $A^n = I_2$, dann ist $n \in \{1, 2, 3, 4, 6\}$.
Hinweis: Betrachten Sie geeeignete Kreisteilungspolynome.

Lösung:
zu (a) Laut Vorlesung ist jedes Polynom $f \in \mathbb{Q}[x]$ mit $f(A) = 0_{\mathcal{M}_{2,\mathbb{Q}}}$ ein Vielfaches vom Minimalpolynom m_A. Nach dem Satz von Cayley-Hamilton erfüllt das charakteristische Polynom c_A von A die Bedingung $c_A(A) = 0_{\mathcal{M}_{2,\mathbb{Q}}}$, es gilt also $m_A \mid c_A$. Der Grad von c_A stimmt mit der Zeilenanzahl (oder der Spaltenanzahl von A überein, ist also gleich 2. Aus $m_A \mid c_A$ folgt somit $\text{grad}(m_A) \leq 2$.

zu (b) Das Polynom $f = x^n - 1 \in \mathbb{Q}[x]$ erfüllt ebenfalls die Bedingung $f(A) = A^n - I_2 = I_2 - I_2 = 0_{\mathcal{M}_{2,\mathbb{Q}}}$. Daraus folgt, dass m_A ein Teiler von f ist.

zu (c) Sei $n \in \mathbb{N}$ minimal mit $A^n = I_2$. Nach Teil (b) ist das Minimalpolynom $m_A \in \mathbb{Q}[x]$ von A ein Teiler von $x^n - 1$. Weil die irreduziblen Faktoren von $x^n - 1$ in $\mathbb{Q}[x]$ laut Vorlesung die Kreisteilungspolynome Φ_d sind, wobei $d \in \mathbb{N}$ die Teiler von n durchläuft, muss m_A ein Produkt dieser Kreisteilungspolynome sein. Setzen wir $f = x^n - 1$, dann gilt $\text{ggT}(f, f') = \text{ggT}(x^n - 1, nx^{n-1}) = 1$. Das Polynom f besitzt also keine mehrfahren komplexen Nullstellen, und wegen $m_A \mid f$ gilt dasselbe für m_A. Die irreduziblen Faktoren von m_A sind also alle verschieden. Da nach Teil (a) außerdem die Ungleichung $\text{grad}(m_A) \leq 2$ gilt, muss m_A entweder selbst ein Kreisteilungspolynom vom Grad 1 oder 2, oder ein Produkt zweier verschiedener Kreisteilungspolynome vom Grad 1 sein.

Die einzigen linearen Kreisteilungspolynome sind $\Phi_1 = x - 1$ und $\Phi_2 = x + 1$. Im Fall $m_A = \Phi_1$ ist $n = 1$. Im Fall $m_A = \Phi_2$ ist $A + I_2 = 0$, also $A = -I_2 \neq I_2$ und $A^2 = (-I_2)^2 = I_2$, woraus $n = 2$ folgt. Im Fall $m_A = (x - 1)(x + 1) = x^2 - 1$ gilt ebenfalls $n = 2$. Die einzige verbleibende Möglichkeit ist $m_A = \Phi_d$, wobei $d \in \mathbb{N}$ mit $\varphi(d) = \text{grad}(\Phi_d) = 2$ ist. Ist $d = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von d (mit $r \in \mathbb{N}$, Primzahlen $p_1, ..., p_r$ und Exponenten $e_1, ..., e_r \in \mathbb{N}$), dann folgt $\prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = \varphi(d) = 2$. Dies zeigt, dass $p_i \leq 3$ für alle i gilt, es ist also $d = 2^{e_1} 3^{e_2}$ mt $e_1, e_2 \in \mathbb{N}_0$ und $(e_1, e_2) \neq (0, 0)$. Im Fall $e_1 > 0$, $e_2 = 0$ ist $d = 2^{e_1}$ und $2^{e_1 - 1} = \varphi(d) = 2$, also $e_1 = 2$ und $n = 4$. Im Fall $e_1 = 0$ und $e_2 > 0$ ist $d = 3^{e_1}$ und $2 \cdot 3^{e_2 - 1} = \varphi(d) = 2$, also $e_2 = 1$ und $n = 3$. Im Fall $e_1, e_2 > 0$ schließlich erhalten wir $2^{e_1 - 1} \cdot 2 \cdot 3^{e_2 - 1} = 2^{e_1} 3^{e_2 - 1} = \varphi(d) = 2$, was nur für $(e_1, e_2) = (1, 1)$ und $n = 6$ möglich ist. Insgesamt ist damit $n \in \{1, 2, 3, 4, 6\}$ nachgewiesen.

Aufgabe F22T1A2

(a) Bestimmen Sie die letzten drei Ziffern von 7^{404404}.

(b) Es sei φ die Eulersche φ-Funktion. Zeigen Sie, dass $\varphi(n^2) = n\varphi(n)$ für alle $n \in \mathbb{N}$ gilt.

(c) Es sei p eine Primzahl mit $p \notin \{2, 5\}$. Zeigen Sie, dass p eine der Zahlen 9, 99, 999, 9999, ... teilt.

Lösung:
zu (a) Die letzten drei Ziffern einer natürlichen Zahl in Dezimaldarstellung hängen nur von der Restklasse der Zahl modulo 1000 ab. Es genügt deshalb, das Bild von $n = 7^{404404}$ in $\mathbb{Z}/1000\mathbb{Z}$ zu bestimmen. Mit 7 ist auch n teilerfremd zu 1000, also ist $\bar{n} = n + 1000\mathbb{Z}$ ein Element von $(\mathbb{Z}/1000\mathbb{Z})^\times$. Die Ordnung der primen Restklassengruppe $(\mathbb{Z}/1000\mathbb{Z})^\times$ ist $\varphi(1000) = \varphi(8)\varphi(125) = 4 \cdot 100$. Daraus folgt $7^{400} = 1$. Wegen $404404 \equiv 4 \bmod 400$ existiert ein $m \in \mathbb{N}$ mit $404404 = 400m + 4$. Damit erhalten wir $\bar{n} = \bar{7}^{404404} = \bar{7}^{400m+4} = (\bar{7}^{400})^m \cdot \bar{7}^4 = \bar{1}^m \cdot \bar{7}^4 = \overline{49}^2 = \overline{2401} = \overline{401}$. Dies zeigt, dass 4, 0 und 1 die letzten drei Ziffern von n sind.

zu (b) Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_r$ und $e_1, ..., e_r \in \mathbb{N}$. Dann gilt

$$\begin{aligned}\varphi(n^2) &= \varphi\left(\prod_{i=1}^{r} p_i^{2e_i}\right) = \prod_{i=1}^{r} \varphi(p_i^{2e_i}) = \prod_{i=1}^{r} p_i^{2e_i-1}(p_i-1) = \prod_{i=1}^{r} p_i^{e_i} p_i^{e_i-1}(p_i-1) \\ &= \prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{i=1}^{r} p_i^{e_i-1}(p_i-1) = \prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{i=1}^{r} \varphi(p_i^{e_i}) = n\varphi(n).\end{aligned}$$

zu (c) Als Primzahl ungleich 2 und 5 ist p teilerfremd zu 10. Dies zeigt, dass $\overline{10} = 10 + p\mathbb{Z}$ in der primen Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Da es sich dabei um eine endliche Gruppe handelt, besitzt das Element $\overline{10}$ eine endliche Ordnung. Es existiert also ein $m \in \mathbb{N}$ mit $\overline{10}^m = \bar{1}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Daraus wiederum folgt $10^m \equiv 1 \bmod p$, was zu $p \mid (10^m - 1)$ äquivalent ist. Die Primzahl p ist also ein Teiler von $10^m - 1 = 99....99$, der Zahl, deren Dezimaldarstellung aus genau m-mal der Ziffer „9“ besteht.

Beispiel: Sei $p = 61$. Dann hat $\overline{10} = 10 + 61\mathbb{Z}$ in $(\mathbb{Z}/61\mathbb{Z})^\times$ die Ordnung 60. Dies zeigt, dass 61 ein Teiler von

$$10^{60} - 1 = 999999999999999999999999999999999999999999999999999999999999 \quad \text{ist.}$$

Aufgabe F22T1A3

Man betrachte die symmetrische Gruppe S_4 des Grades 4 und

$$V \quad = \quad \{\mathrm{id}\ ,\ (1\ 2)(3\ 4)\ ,\ (1\ 3)(2\ 4)\ ,\ (1\ 4)(2\ 3)\} \quad \subseteq \quad S_4.$$

(a) Zeigen Sie, dass V ein zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ isomorpher Normalteiler in S_4 ist.

(b) Zeigen Sie, dass S_4/V zu S_3 isomorph ist.

(c) Beweisen Sie, dass S_4 keinen Normalteiler der Ordnung 8 hat.

(d) Bestimmen Sie alle Untergruppen und alle Normalteiler der Faktorgruppe S_4/V.

Lösung:
zu (a) Zunächst zeigen wir, dass V eine Untergruppe von S_4 ist. Das Neutralelement id von S_4 ist in V enthalten. Seien nun $\sigma, \tau \in V$ vorgegeben; zu zeigen ist $\sigma \circ \tau \in V$ und $\sigma^{-1} \in V$. Wie man leicht überprüft, gilt $\rho^2 = \mathrm{id}$ für alle $\rho \in V$. Daraus folgt, dass jedes Element in V sein eigenes Inverses ist und insbesondere $\sigma^{-1} = \sigma$ in V liegt. Ist $\sigma = \mathrm{id}$, dann folgt $\sigma \circ \tau = \tau$, und dieses Element ist in V enthalten. Ist $\tau = \mathrm{id}$, dann gilt $\sigma \circ \tau = \sigma$ und somit ebenfalls $\sigma \circ \tau \in V$. Im Fall $\sigma, \tau \neq \mathrm{id}$ zeigt die folgende Verknüpfungstabelle, dass $\sigma \circ \tau$ in V enthalten ist.

$\circ$	$(1\ 2)(3\ 4)$	$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$
$(1\ 2)(3\ 4)$	id	$(1\ 4)(2\ 3)$	$(1\ 3)(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$	id	$(1\ 2)(3\ 4)$
$(1\ 4)(2\ 3)$	$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$	id

Als Gruppe der Primzahlquadratordnung 4 ist V abelsch. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist V isomorph zu einem direkten Produkt zyklischer Gruppen, also isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Da jedes Element in V sein eigenes Inverses ist, gibt es in V nur Elemente der Ordnung 1 und 2, und folglich ist V isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Nun zeigen wir noch, dass V ein Normalteiler von S_4 ist. Laut Vorlesung sind zwei Elemente in S_4 genau dann zueinander konjugiert, wenn sie denselben Zerlegungstyp besitzen. Die drei Elemente $\neq \mathrm{id}$ in V sind die einzigen Doppeltranspositionen in S_4, also die einzigen Elemente vom Zerlegungstyp $(2,2)$. Seien nun $\sigma \in S_4$ und $\tau \in V$ vorgegeben; zu zeigen ist $\sigma \circ \tau \circ \sigma^{-1} \in V$. Ist $\tau \in V \setminus \{\mathrm{id}\}$, dann ist mit τ auch das zu τ konjugierte Element $\sigma \circ \tau \circ \sigma^{-1}$ eine Doppeltransposition, und es folgt $\sigma \circ \tau \circ \sigma^{-1} \in V$. Im Fall $\tau = \mathrm{id}$, ist $\sigma \circ \tau \circ \sigma^{-1}$ gleich id und somit ebenfalls in V enthalten.

zu (b) Sei $X = V \setminus \{\mathrm{id}\}$. Wie wir in Teil (a) gesehen haben, ist mit $\sigma \in S_4$ und $\tau \in X$ auch $\sigma \circ \tau \circ \sigma^{-1}$ wieder in X enthalten. Durch $(\sigma, \tau) \mapsto \sigma \circ \tau \circ \sigma^{-1}$ ist also eine Abbildung $\cdot : S_4 \times X \to X$ definiert. Dabei handelt es sich um eine Gruppenoperation von S_4 auf X. Sind nämlich $\sigma_1, \sigma_2 \in S_4$ und $\tau \in X$ vorgegeben, dann gilt $\mathrm{id} \cdot \tau = \tau \circ \mathrm{id} \circ \tau^{-1} = \tau \circ \tau^{-1} = \mathrm{id}$ und

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot \tau) \quad &= \quad \sigma_1 \cdot (\sigma_2 \circ \tau \circ \sigma_2^{-1}) \quad = \quad \sigma_1 \circ (\sigma_2 \circ \tau \circ \sigma_2^{-1}) \circ \sigma_1^{-1} \quad = \\ &(\sigma_1 \circ \sigma_2) \circ \tau \circ (\sigma_1 \circ \sigma_2)^{-1} \quad = \quad (\sigma_1 \circ \sigma_2) \cdot \tau. \end{aligned}$$

Laut Vorlesung erhält man durch die Operation einen Gruppenhomomorphismus $\phi : S_4 \to \mathrm{Per}(X)$, definiert durch $\phi(\sigma)(\tau) = \sigma \cdot \tau = \sigma \circ \tau \circ \sigma^{-1}$. Dabei ist V im Kern von ϕ enthalten, denn weil V abelsch ist, gilt für alle $\sigma, \tau \in V$ jeweils $\phi(\sigma)(\tau) = \sigma \circ \tau \circ \sigma^{-1} = \sigma \circ \sigma^{-1} \circ \tau$, und somit $\phi(\sigma) = \mathrm{id}_X$ für alle $\sigma \in V$. Somit induziert ϕ einen Homomorphismus $\bar{\phi} : S_4/V \to \mathrm{Per}(X)$.

Wenn wir zeigen können, dass $\bar{\phi}$ surjektiv ist, dass folgt daraus direkt, dass $S_4/V \cong S_3$ gilt. Denn wegen $|X| = 3$ gilt $\mathrm{Per}(X) \cong S_3$ und somit $|\mathrm{Per}(X)| = |S_3| = 6$. Ebenso ist $|S_4/V| = (S_4 : V) = \frac{|S_4|}{|V|} = \frac{24}{4} = 6$, und als surjektive Abbildung zwischen gleichmächtigen Mengen ist $\bar{\phi}$ auch bijektiv. Insgesamt ist $\bar{\phi}$ also ein Isomorphismus, und es folgt $S_4/V \cong \mathrm{Per}(X) \cong S_3$.

Beweisen wir also noch die Surjektivität von $\bar{\phi}$. Das Element $(1\ 2\ 3) \in S_4$ ist ein Element der Ordnung 3, also muss die Ordnung von $\bar{\phi}((1\ 2\ 3))$ gleich 1 oder 3 sein. Wegen $\phi((1\ 2\ 3))((1\ 2)(3\ 4)) = (1\ 2\ 3) \circ (1\ 2)(3\ 4) \circ (1\ 2\ 3)^{-1} = (1\ 2\ 3) \circ (1\ 2)(3\ 4) \circ (1\ 3\ 2) = (1\ 4)(2\ 3) \neq (1\ 2)(3\ 4)$ ist $\phi((1\ 2\ 3)) \neq \mathrm{id}$ und somit ein Element der Ordnung 3 in $\mathrm{Per}(X)$. Ebenso zeigt die Rechung $\bar{\phi}((1\ 2))((1\ 3)(2\ 4)) = (1\ 2) \circ (1\ 3)(2\ 4) \circ (1\ 2)^{-1} = (1\ 2) \circ (1\ 3)(2\ 4) \circ (1\ 2) = (1\ 4)(2\ 3) \neq (1\ 3)(2\ 4)$, dass $\phi((1\ 2))$ in $\mathrm{Per}(X)$ ein Element der Ordnung 2 ist. Die Ordnung des Bildes $\mathrm{im}(\bar{\phi})$ muss also ein gemeinsames Vielfaches von 2 und 3 sein. Aus $|\mathrm{im}(\bar{\phi})| \geq \mathrm{kgV}(2,3) = 6 = |\mathrm{Per}(X)|$ und $\mathrm{im}(\bar{\phi}) \subseteq \mathrm{Per}(X)$ folgt $\mathrm{im}(\bar{\phi}) = \mathrm{Per}(X)$ und somit die Surjektivität von $\bar{\phi}$.

Anmerkung:
Setzt man als bekannt voraus, dass S_3 bis auf Isomorphie die einzige nicht-abelsche Gruppe der Ordnung 6 ist, kommt man schneller zum Ziel. Wie oben zeigt man zunächst, dass auch die Faktorgruppe S_4/V von Ordnung 6 ist. Anschließend überprüft man noch, dass S_4/V nicht-abelsch ist, zum Beispiel, indem man nachrechnet, dass

$$(1\ 2)V \cdot (1\ 3)V \quad \neq \quad (1\ 3)V \cdot (1\ 2)V$$

gilt. Das Element auf der linken Seite ist gleich $((1\ 2) \circ (1\ 3))V = (1\ 3\ 2)V$, das auf der rechten Seite ist gleich $((1\ 3) \circ (1\ 2))V = (1\ 2\ 3)V$. Wären die Elemente gleich dann müsste $(1\ 3\ 2)^{-1} \circ (1\ 2\ 3)$ in V liegen. Tatsächlich aber gilt $(1\ 3\ 2)^{-1} \circ (1\ 2\ 3) = (1\ 2\ 3) \circ (1\ 2\ 3) = (1\ 3\ 2) \notin V$.

zu (c) Wegen $|S_4| = 24 = 2^3 \cdot 3$ sind die Untergruppen der Ordnung 8 genau die 2-Sylowgruppen von S_4. Gäbe es eine 2-Sylowgruppe, die Normalteiler ist, so wäre dies laut Zweitem Sylowsatz die einzige 2-Sylowgruppe. Nun ist bekanntlich die Diedergruppe D_4 eine Untergruppe der Ordnung 8 von S_4, und diese enthält zwei Elemente der Ordnung 4. Wäre dies die einzige Untergruppe der Ordnung 8, dann gäbe es also nur zwei Elemente der Ordnung 4 in S_4. Offensichtlich gibt es aber mehr als zwei solche Elemente, zum Beispiel (1 2 3 4), (1 4 3 2) und (1 3 2 4).

zu (d) Nach Teil (b) ist S_4/V isomorph zu S_3. Bekanntlich besitzt S_3 genau drei verschiedene Untergruppen der Ordnung 2 und genau je eine Untergruppe der Ordnung 1, 3 und 6. Dabei sind die drei Untergruppen der Ordnung 2 keine Normalteiler, die übrigen drei Gruppen sind Normalteiler. Auf Grund der Isomorphie besitzt S_4/V die gleiche Untergruppenstruktur.

Das Neutralelement von S_4/V ist $e_{S_4/V} = V$, und offenbar ist $\{V\}$ die eindeutig bestimmte Untergruppe der Ordnung 1 von S_4/V. Ebenso ist S_4/V die eindeutig bestimmte Untergruppe der Ordnung 6 von S_4/V. Wir betrachten in S_4/V nun die Elemente $g_1 = (1\ 2)V$, $g_2 = (1\ 3)V$, $g_3 = (1\ 4)V$ und $h = (1\ 2\ 3)V$. Wegen $(1\ 2), (1\ 3), (1\ 4) \notin V$ gilt $g_1 \neq e_{S_4/V}$, $g_2 \neq e_{S_4/V}$ und $g_3 \neq e_{S_4/V}$. Andererseits gilt $g_1^2 = (1\ 2)^2V = \mathrm{id}V = e_{S_4/V}$, also ist g_1 in S_4/V ein Element der Ordnung 2. Ebenso zeigen die Gleichungen $g_2^2 = (1\ 3)^2V = \mathrm{id}V = e_{S_4/V}$ und $g_3^2 = (1\ 4)^2V = \mathrm{id}V = e_{S_4/V}$, dass auch g_2 und g_3 Elemente der Ordnung 2 in S_4/V sind.

Durch $\langle g_1 \rangle = \{e_{S_4/V}, g_1\}$, $\langle g_2 \rangle = \{e_{S_4/V}, g_2\}$ und $\langle g_3 \rangle = \{e_{S_4/V}, g_3\}$ sind also Untergruppen von S_4/V der Ordnung 2 gegeben. Würden zwei davon übereinstimmen, dann wären auch zwei der Elemente g_1, g_2, g_3 identisch. Aus $g_1 = g_2$ würde $(1\ 2)V = (1\ 3)V$ und $(1\ 2)^{-1} \circ (1\ 3) \in V$ folgen. Aber dies ist wegen $(1\ 2)^{-1} \circ (1\ 3) = (1\ 2) \circ (1\ 3) = (1\ 3\ 2) \notin V$ nicht der Fall. Ebenso zeigen die Rechnungen $(1\ 2)^{-1} \circ (1\ 4) = (1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin V$ und $(1\ 3)^{-1} \circ (1\ 4) = (1\ 3) \circ (1\ 4) = (1\ 4\ 3) \notin V$, dass $g_1 \neq g_3$ und $g_2 \neq g_3$ gilt. Also sind $\langle g_1 \rangle$, $\langle g_2 \rangle$ und $\langle g_3 \rangle$ die drei Untergruppen der Ordnung 2 von S_4/V.

Es gilt $h = (1\ 2\ 3)V \neq e_{S_4/V}$ wegen $(1\ 2\ 3) \notin V$, $h^2 = (1\ 2\ 3)^2 V = (1\ 3\ 2)V \neq e_{S_4/V}$ wegen $(1\ 3\ 2) \notin V$ und $h^3 = (1\ 2\ 3)^3 V = \mathrm{id}V = e_{S_4/V}$. Also ist $\mathrm{ord}(h) = 3$, und $\langle h \rangle$ ist eine Untergruppe der Ordnung 3 von S_4/V. Insgesamt sind

$$\{V\} \quad , \quad \langle g_1 \rangle \quad , \quad \langle g_2 \rangle \quad , \quad \langle g_3 \rangle \quad , \quad \langle h \rangle \quad \text{und} \quad S_4/V$$

also die sechs Untergruppen von S_4/V, und $\{V\}$, $\langle h \rangle$, S_4/V sind die drei Normalteiler.

Aufgabe F22T1A4

(a) Bestimmen Sie alle Ideale des Rings $R = \mathbb{Z}/2022\mathbb{Z}$. Bestimmen Sie darunter alle Primideale in R.

(b) Bestimmen Sie alle idempotenten Elemente des Rings R, d.h. alle Elemente $a \in R$ mit $a^2 = a$.

(c) Bestimmen Sie die Anzahl der Nullteiler in R.

(d) Bestimmen Sie ein $n \in \mathbb{N}$ mit $n < 2022$ und $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2022\mathbb{Z})^\times$.

Lösung:
zu (a) Sei $\pi : \mathbb{Z} \to \mathbb{Z}/2022\mathbb{Z}$ der kanonische Epimorphismus und $I = (2022)$. Nach dem Korrespondenzsatz der Ringtheorie ist durch $J \mapsto \pi(J)$ eine Bijektion gegeben zwischen den Idealen J von $\mathbb{Z}$ mit $J \supseteq I$ und den Idealen von $\mathbb{Z}/2022\mathbb{Z}$. Die Ideale von $\mathbb{Z}$ haben alle die Form (n) mit $n \in \mathbb{N}_0$, und es gilt $(n) \supseteq I$ genau dann, wenn 2022 in (n) liegt, was wiederum genau dann der Fall ist, wenn n ein Teiler von 2022 ist. An der Primfaktorzerlegung $2022 = 2 \cdot 3 \cdot 337$ liest man ab, dass 2022 genau acht Teiler in $\mathbb{N}_0$ besitzt, nämlich 1, 2, 3, 6, 337, 674, 1011 und 2022. Die Ideale von $\mathbb{Z}/2022\mathbb{Z}$ sind somit gegeben durch $(\bar{1})$, $(\bar{2})$, $(\bar{3})$, $(\bar{6})$, $(\overline{337})$, $(\overline{674})$, $(\overline{1011})$ und $(\overline{2022}) = (\bar{0}) = \{\bar{0}\}$.

Wir zeigen, dass allgemein gilt: Ist R ein Ring, I ein Ideal von R und $\pi : R \to R/I$ der kanonische Epimorphismus, so ist ein Ideal J von R mit $J \supseteq I$ genau dann ein Primideal, wenn $\pi(J)$ ein Primideal in R/I ist. Ist J ein Primideal, dann gilt zunächst $1_R + I \notin \pi(J)$, denn ansonsten wäre 1_R in $\pi^{-1}(\pi(J)) = J$ enthalten. Sind $a + I, b + I \in R/I$ mit $a, b \in R$ und $(a + I)(b + I) \in \pi(J)$, dann folgt $ab + I \in \pi(J)$ und $ab \in J$. Weil J ein Primideal ist, folgt $a \in J$ oder $b \in J$, und daraus wiederum $a + I \in \pi(J)$ oder $b + I \in \pi(J)$. Also ist $\pi(J)$ ein Primideal in R/I. Setzen wir dies nun umgekehrt voraus, dann ist $1_R \notin J$, denn ansonsten wäre $1_{R/I} = \pi(1_R) \in \pi(J)$. Seien nun $a, b \in R$ mit $ab \in J$. Dann folgt $\pi(a)\pi(b) = \pi(ab) \in \pi(J)$, und daraus wiederum $\pi(a) \in \pi(J)$ oder $\pi(b) \in \pi(J)$, weil $\pi(J)$ ein Primideal ist. Wegen $\pi^{-1}(\pi(J)) = J$ folgt daraus wiederum $a \in J$ oder $b \in J$. Dies zeigt, dass J ein Pprimideal in J ist.

Bekanntlich sind die Primideale in $\mathbb{Z}$ genau das Nullideal und die Ideale der Form (p), wobei p die Primzahlen durchläuft. Die einzigen Primideale, die (2022) enthalten, sind also (2), (3) und (337). Die soeben bewiesene Aussage zeigt, dass $(\bar{2})$, $(\bar{3})$ und $(\overline{337})$ somit die Primideale von $\mathbb{Z}/2022\mathbb{Z}$ sind.

zu (b) Weil $2022 = 2 \cdot 3 \cdot 337$ gilt und die Zahlen 2, 3 und 337 paarweise teilerfremd sind, gilt $\mathbb{Z}/2022\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$ nach dem Chinesischen Restsatz. Ein Element $(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$ ist genau dann idempotent, wenn $(\bar{a}^2, \bar{b}^2, \bar{c}^2) = (\bar{a}, \bar{b}, \bar{c})^2 = (\bar{a}, \bar{b}, \bar{c})$ gilt, was wiederum zu $\bar{a}^2 = \bar{a}$, $\bar{b}^2 = \bar{b}$ und $\bar{c}^2 = \bar{c}$ ist. Nun ist in einem Körper K für jedes $\alpha \in K$ die Gleichung $\alpha^2 = \alpha$ äquivalent zu $\alpha(\alpha - 1_K) = 0_K$ und damit zu $\alpha \in \{0_K, 1_K\}$. Weil 2, 3 und 337 Primzahlen sind, sind $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/337\mathbb{Z}$ Körper. Also sind die Gleichungen $\bar{a}^2 = \bar{a}$, $\bar{b}^2 = \bar{b}$, $\bar{c}^2 = \bar{c}$ äquivalent zu $\bar{a} \in \{\bar{0}, \bar{1}\}$, $\bar{b} \in \{\bar{0}, \bar{1}\}$, $\bar{c} \in \{\bar{0}, \bar{1}\}$. Insgesamt zeigt dies, dass in $\mathbb{Z}/2022\mathbb{Z}$ genau acht idempotente Elemente existieren, nämlich die Urbilder von

$$(\bar{0}, \bar{0}, \bar{0}), (\bar{0}, \bar{0}, \bar{1}), (\bar{0}, \bar{1}, \bar{0}), (\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{0}, \bar{0}), (\bar{1}, \bar{0}, \bar{1}), (\bar{1}, \bar{1}, \bar{0}), (\bar{1}, \bar{0}, \bar{1})$$

unter dem Isomorphismus $\mathbb{Z}/2022\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$. Wir rechnen diese acht Urbilder nun aus. Das Urbild von $(\bar{0}, \bar{0}, \bar{0})$ ist das eindeutig bestimmte Element $a + 2022\mathbb{Z}$ mit $a \equiv 0 \bmod 2$, $a \equiv 0 \bmod 3$ und $a \equiv 0 \bmod 337$, und dies ist offenbar $0 + 2022\mathbb{Z}$. Genauso sieht man, dass $1 + 2022\mathbb{Z}$ das Urbild von $(\bar{1}, \bar{1}, \bar{1})$ ist.

Das Urbild $a + 2022\mathbb{Z}$ von $(\bar{0}, \bar{0}, \bar{1})$ erfüllt $a \equiv 0 \bmod 2$, $a \equiv 0 \bmod 3$ und $a \equiv 1 \bmod 337$, was äquivalent ist zu $a \equiv 0 \bmod 6$ und $a \equiv 1 \bmod 337$. Die letzte Bedingung zeigt, dass a die Form $1 + 337k$ mit $k \in \mathbb{Z}$ haben muss. Wegen $337 \equiv 1 \bmod 6$ erfüllt $1 + 337 \cdot 5 = 1686$ auch die Bedingung $1686 \equiv 0 \bmod 6$. Also ist $1686 + 2022\mathbb{Z}$ das Ubild von $(\bar{0}, \bar{0}, \bar{1})$.

Das Urbild $a + 2022\mathbb{Z}$ von $(\bar{0}, \bar{1}, \bar{0})$ erfüllt $a \equiv 0 \bmod 2$, $a \equiv 1 \bmod 3$ und $a \equiv 0 \bmod 337$, was äquivalent ist zu $a \equiv 0 \bmod 674$ und $a \equiv 1 \bmod 3$. Es gilt $674 \equiv 2 \bmod 3$, also $1348 \equiv 2 \cdot 674 \equiv 4 \equiv 1 \bmod 3$. Also ist $1348 + 2022\mathbb{Z}$ das Urbild von $(\bar{0}, \bar{1}, \bar{0})$. Durch analoge Rechnungen sieht man, dass die Urbilder von $(\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{0}, \bar{0}), (\bar{1}, \bar{0}, \bar{1})$ und $(\bar{1}, \bar{1}, \bar{0})$ durch $1012 + 2022\mathbb{Z}$, $1011 + 2022\mathbb{Z}$, $675 + 2022\mathbb{Z}$ und $337 + 2022\mathbb{Z}$ gegeben sind. Die idempotenten Elemente von $\mathbb{Z}/2022\mathbb{Z}$ sind also $a + 2022\mathbb{Z}$ mit $a \in \{0, 1, 337, 675, 1011, 1012, 1348, 1686\}$.

zu (c) Weil $\mathbb{Z}/2022\mathbb{Z}$ ein endlicher Ring ist, ist jedes Element entweder Einheit oder Nullteiler. Laut Vorlesung hat die Einheitengruppe $(\mathbb{Z}/2022\mathbb{Z})^\times$ die Ordnung $\varphi(2022) = \varphi(2)\varphi(3)\varphi(337) = 1 \cdot 2 \cdot 336 = 772$. Die Zahl der Nullteiler ist also gegeben durch $|\mathbb{Z}/2022\mathbb{Z}| - |(\mathbb{Z}/2022\mathbb{Z})^\times| = 2022 - 772 = 1350$.

zu (d) Sei $n = 1011$; diese Zahl besitzt die Primfaktorzerlegung $3 \cdot 337$. Wegen $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ und dem Chinesischen Restsatz gilt

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times \quad &\cong \quad (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/337\mathbb{Z})^\times \quad \cong \quad \{\bar{1}\} \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/337\mathbb{Z})^\times \\ &\cong \quad (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/337\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/2022\mathbb{Z})^\times.\end{aligned}$$

Aufgabe F22T1A5

Für jedes $n \in \mathbb{N}$ sei $a_n = \sqrt[2^n]{2}$. Weiter seien $A = \{a_n \mid n \in \mathbb{N}\}$ und $K = \mathbb{Q}(A)$. Zeigen Sie:

(a) $[\mathbb{Q}(a_n) : \mathbb{Q}] = 2^n$ für jedes $n \in \mathbb{N}$

(b) $[K : \mathbb{Q}] = \infty$

(c) $K = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(a_n)$

(d) K ist eine algebraische Erweiterung von $\mathbb{Q}$

Lösung:
zu (a) Das Polynom $f_n = x^{2^n} - 2 \in \mathbb{Z}[x]$ ist normiert, nach dem Eisenstein-Kriterium (angewendet auf die Primzahl 2) über $\mathbb{Q}$ irreduzibel, und es gilt $f_n(a_n) = (\sqrt[2^n]{2})^{2^n} - 2 = 2 - 2 = 0$. Somit ist f_n das Minimalpolynom von a_n über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(a_n) : \mathbb{Q}] = \operatorname{grad}(f_n) = 2^n$.

zu (b) Nehmen wir an, der Grad $m = [K : \mathbb{Q}]$ wäre endlich. Wegen $a_n \in A \subseteq \mathbb{Q}(A) = K$ ist $\mathbb{Q}(a_n)$ für jedes $n \in \mathbb{N}$ ein Zwischenkörper von $K|\mathbb{Q}$. Mit der Gradformel und dem Ergebnis von Teil (a) erhalten wir

$$m \quad = \quad [K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(a_n)] \cdot [\mathbb{Q}(a_n) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(a_n)] \cdot 2^n$$

für alle $n \in \mathbb{N}$. Die Zahl $m \in \mathbb{N}$ wäre also durch 2^n teilbar für jedes $n \in \mathbb{N}$, was offenbar unmöglich ist.

zu (c) „$\supseteq$“ Wie bereits in Teil (b) festgestellt, ist $\mathbb{Q}(a_n)$ für jedes $n \in \mathbb{N}$ ein Zwischenkörper von $K|\mathbb{Q}$. Insbesondere gilt also $\mathbb{Q}(a_n) \subseteq K$ für alle $n \in \mathbb{N}$, und damit auch $\bigcup_{n\in\mathbb{N}} \mathbb{Q}(a_n) \subseteq K$. „$\subseteq$“ Sei $L = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(a_n)$. Für jedes $m \in \mathbb{N}$ gilt $a_m \in \mathbb{Q}(a_m) \subseteq L$ und damit $A = \{a_m \mid m \in \mathbb{N}\} \subseteq L$.

Außerdem ist L ein Zwischenkörper der Erweiterung $\mathbb{R}|\mathbb{Q}$. Zum Nachweis der Teilkörper-Eigenschaft stellen wir zunächst fest, dass 1 in $\mathbb{Q}(a_1) \subseteq L$ enthalten ist. Seien nun $\alpha, \beta \in L$ vorgegeben. Dann gibt es nach Definition von L natürliche Zahlen m, n mit $\alpha \in \mathbb{Q}(a_m)$ und $\beta \in \mathbb{Q}(a_n)$. Nach eventueller Vertauschung von α und β können wir $m \leq n$ annehmen. Wegen $a_m = \sqrt[2^m]{2} = 2^{2^{-m}} = 2^{2^{-n}\cdot 2^{n-m}} = (2^{2^{-n}})^{2^{n-m}} = (\sqrt[2^n]{2})^{2^{n-m}} = a_n^{2^{n-m}} \in \mathbb{Q}(a_n)$ gilt $\mathbb{Q}(a_m) \subseteq \mathbb{Q}(a_n)$. Aus $\alpha \in \mathbb{Q}(a_m) \subseteq \mathbb{Q}(a_n)$ und $\beta \in \mathbb{Q}(a_n)$ sowie der Teilkörper-Eigenschaft von $\mathbb{Q}(a_n)$ folgt nun, dass auch $\alpha - \beta$ und $\alpha\beta$ in $\mathbb{Q}(a_n)$ und wegen $\mathbb{Q}(a_n) \subseteq L$ damit auch in L enthalten sind. Im Fall $\alpha \neq 0$ erhält man ebenso $\alpha^{-1} \in \mathbb{Q}(a_m)$ und damit $\alpha^{-1} \in L$. Damit ist der Nachweis der Teilkörper-Eigenschaft von L abgeschlossen. Außerdem gilt $\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq L$.

Somit ist L tatsächlich ein Zwischenkörper von $\mathbb{R}|\mathbb{Q}$. Da außerdem, wie bereits festgestellt, $A \subseteq L$ gibt, erhalten wir insgesamt $K = \mathbb{Q}(A) \subseteq L$.

zu (d) Es genügt zu zeigen, dass jedes $\alpha \in K$ algebraisch über $\mathbb{Q}$ ist. Sei also $\alpha \in K$ vorgegeben. Auf Grund des Ergebnisses von Teil (c) gilt $\alpha \in \mathbb{Q}(a_n)$ für ein $n \in \mathbb{N}$. Nach Teil (a) ist $\mathbb{Q}(a_n)|\mathbb{Q}$ eine endliche Erweiterung, und jede endliche Erweiterung ist laut Vorlesung algebraisch. Daraus folgt, dass alle Elemente aus $\mathbb{Q}(a_n)$ algebraisch über $\mathbb{Q}$ sind, insbesondere auch das Element α.

alternative Lösung:
Wie wir in Teil (a) festgestellt haben, ist a_n für jedes $n \in \mathbb{N}$ jeweils eine Nullstelle des Polynoms $f_n = x^{2^n} - 1 \in \mathbb{Q}[x]$ und somit algebraisch über $\mathbb{Q}$. Die Menge A besteht also aus Elementen, die algebraisch über $\mathbb{Q}$ sind. Laut Vorlesung ist jede Körpererweiterung, die von Elementen erzeugt wird, die über dem Grundkörper algebraisch sind, selbst eine algebraische Erweiterung. Wegen $K = \mathbb{Q}(A)$ ist die Erweiterung $K|\mathbb{Q}$ somit algebraisch. (Vom Aufgabensteller war aber wohl nicht vorgesehen, dass man dieses Resultat verwendet. Es wird eventuell nicht in jeder Algebra-Vorlesung behandelt.)

Aufgabe F22T2A1

Gegeben sei die komplexe 2×2-Matrix

$$A \quad = \quad \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix}.$$

Berechnen Sie die Matrix A^{2022}.

Lösung:
Es gilt

$$A^2 = \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{und} \quad A^4 = (A^2)^2 = (-E) = E \quad ,$$

wobei E die 2×2-Einheitsmatrix bezeichnet. Daraus folgt $A^{2022} = A^{4 \cdot 505 + 2} = (A^4)^{505} \cdot A^2 = E^{505} \cdot A^2 = A^2 = -E$.

Aufgabe F22T2A2

(a) Geben Sie eine nicht-abelsche Gruppe der Ordnung 100 an.

(b) Zeigen Sie mit Hilfe der Sylowsätze, dass jede Gruppe der Ordnung 100 auflösbar ist.

(c) Zeigen Sie, dass eine Gruppe der Ordnung 100 genau dann abelsch ist, wenn es in G lediglich eine 2-Sylowgruppe gibt.

Lösung:
zu (a) Laut Vorlesung ist die Diedergruppe D_n für alle $n \in \mathbb{N}$ mit $n \geq 3$ eine nicht-abelsche Gruppe der Ordnung $2n$. Also ist D_{50} eine nicht-abelsche Gruppe der Ordnung 100.

zu (b) Sei G eine Gruppe der Ordnung $100 = 2^2 \cdot 5^2$, und es sei ν_5 die Anzahl der 5-Sylowgruppen von G. Auf Grund des Dritten Sylowsatzes gilt $\nu_5 \mid 2^2$, also $\nu_5 \in \{1, 2, 4\}$, außerdem $\nu_5 \equiv 1 \bmod 5$. Wegen $2, 4 \not\equiv 1 \bmod 5$ folgt daraus $\nu_5 = 1$. Sei N die einzige 5-Sylowgruppe von G. Auf Grund des Zweiten Sylowsatzes ist N ein Normalteiler von G. Als Gruppe der Primzahlpotenzordnung 5^2 ist N eine auflösbare Gruppe. Auch die Ordnung der Faktorgruppe G/N ist eine Primzahlpotenz, nämlich $|G/N| = (G : N) = \frac{|G|}{|N|} = \frac{100}{25} = 2^2$. Somit ist auch G/N auflösbar. Aus der Auflösbarkeit von N und G/N folgt die Auflösbarkeit von G. (Als Gruppen von Primzahlquadratordnung sind N und G/N sogar abelsch, aber daraus folgt natürlich nicht, dass G abelsch sein muss.)

zu (c) Wieder sei G eine Gruppe der Ordnung 100, und für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Bereits in Teil (b) haben wir gesehen, dass G genau eine 5-Sylowgruppe N besitzt, und dass $N \trianglelefteq G$ gilt. Laut Vorlesung besitzt G für jede Primzahl p mindestens eine p-Sylowgruppe. Wir bezeichnen mit U eine beliebige 2-Sylowgruppe und beweisen nun die angegebene Äquivalenz.

„$\Rightarrow$“ Ist G abelsch, dann ist jede Untergruppe von G ein Normalteiler, insbesondere auch die 2-Sylowgruppe U. Aus $U \trianglelefteq G$ folgt auf Grund des Zweiten Sylowsatzes $\nu_2 = 1$. „$\Leftarrow$“ Aus $\nu_2 = 1$ folgt mit dem Zweiten Sylowsatz umgekehrt auch $U \trianglelefteq G$. Wir zeigen nun, dass G ein inneres direktes Produkt von N und U ist. Die Bedingung $N, U \trianglelefteq G$ haben wir bereits verifiziert. Auf Grund der Teilerfremdheit von $|N| = 25$ und $|U| = 4$ gilt $N \cap U = \{e\}$. Für den Nachweis der Gleichung $G = NU$ stellen wir zunächst fest, dass NU wegen $N, U \trianglelefteq G$ eine Untergruppe von G ist (sogar ein Normalteiler). Aus $N \subseteq NU$ folgt mit dem Satz von Lagrange, dass $|N| = 25$ ein Teiler von $|NU|$ ist. Aus $U \subseteq NU$ folgt ebenso $4 \mid |NU|$. Insgesamt ist $|NU|$ damit ein Vielfaches von $\mathrm{kgV}(25, 4) = 100$; insbesondere gilt $|NU| \geq 100 = |G|$. Wegen $NU \subseteq G$ folgt daraus $NU = G$.

Insgesamt ist G also tatsächlich ein inneres direktes Produkt von N und U. Laut Vorlesung folgt daraus $G \cong N \times U$. Als Gruppen von Primzahlquadratordnung sind N und U abelsch. Also ist auch $N \times U$, und auf Grund der Isomorphie auch G, eine abelsche Gruppe.

Aufgabe F22T2A3

Sei $n \in \mathbb{N}$ und R ein kommutativer Ring (mit Einselement). Betrachten Sie für $a, b \in R$ das Ideal $I = (a, b) \subseteq R$.

(a) Zeigen Sie: Aus $a^n = b^n = 0$ folgt $I^{2n} = (0)$.

(b) Nehmen Sie an, dass $2 = 1 + 1$ eine Einheit von R ist und dass $c^2 = 0$ für alle $c \in I$ gilt. Zeigen Sie, dass dann $ab = 0$ folgt.

(c) Geben Sie einen kommutativen Ring R mit Elementen $a, b \in R$ an, für welche $a^2 = b^2 = 0$ und $ab \neq 0$ gilt. Begründen Sie, dass diese beiden Bedingungen für den von Ihnen angegebenen Ring erfüllt sind.
Hinweis: Betrachten Sie $R = \mathbb{Q}[x, y]/I$ für ein geeignetes Ideal I.

Lösung:
zu (a) Wir zeigen durch vollständige Induktion, dass $S_m = \{a^{n-j}b^j \mid 0 \leq j \leq m\}$ für jedes $m \in \mathbb{N}$ ein Erzeugendensystem des Ideals I^m ist. Dass $S_1 = \{a, b\}$ das Ideal $I^1 = I$ erzeugt, gilt laut Angabe. Sei nun $m \in \mathbb{N}$, und setzen wir $I^m = (S_m)$ voraus. Wegen $I^{m+1} = I^m \cdot I$, $I^m = (S_m)$ und $I = (a, b)$ ist laut Vorlesung $S = \{cd \mid c \in S_m, d \in \{a, b\}\}$ ein Erzeugendensystem von I^{m+1}. Diese Menge stimmt mit S_{m+1} überein, denn es gilt

$$\begin{aligned} S &= \{a^{m-j}b^j \cdot a \mid 0 \leq j \leq m\} \cup \{a^{m-j}b^j \cdot b \mid 0 \leq j \leq m\} \\ &= \{a^{m+1-j}b^j \mid 0 \leq j \leq m\} \cup \{a^{(m+1)-(j+1)}b^{j+1} \cdot b \mid 0 \leq j \leq m\} \\ &= \{a^{m+1-j}b^j \mid 0 \leq j \leq m\} \cup \{a^{(m+1)-j}b^j \cdot b \mid 1 \leq j \leq m+1\} \\ &= \{a^{m+1-j}b^j \mid 0 \leq j \leq m+1\} = S_{m+1}. \end{aligned}$$

Setzen wir nun voraus, dass $a^n = b^n = 0$ für ein $n \in \mathbb{N}$ gilt. Für $0 \leq j \leq n$ gilt dann $2n - j \geq n$ und somit $a^{2n-j} \cdot b^j = a^n \cdot a^{n-j} \cdot b^j = 0 \cdot a^{n-j} \cdot b^j = 0$, und für $n < j \leq 2n$ erhalten wir $a^{2n-j} \cdot b^j = a^{2n-j} \cdot b^{j-n} \cdot b^n = a^{2n-j} \cdot b^{j-n} \cdot 0 = 0$. Insgesamt gilt damit $S_{2n} = \{0\}$, und es folgt $I^{2n} = (S_{2n}) = (0)$.

zu (b) Auf Grund der Voraussetzungen gilt $2ab = 0 + 2ab + 0 = a^2 + 2ab + b^2 = (a + b)^2 = 0$. Weil 2 in R eine Einheit ist, folgt daraus $ab = 2^{-1}(2ab) = 2^{-1} \cdot 0 = 0$.

zu (c) Wir betrachten im Polynomring $\mathbb{Q}[x, y]$ das Ideal $I = (x^2, y^2)$ und setzen $R = \mathbb{Q}[x, y]/I$. Es sei $a = x + I$ und $b = y + I$. Wegen $x^2 \in I$ gilt $a^2 = x^2 + I = I = 0_R$, und aus $y^2 \in I$ folgt ebenso $b^2 = y^2 + I = I = 0_R$. Nehmen wir nun an, dass auch $ab = 0_R$ gilt. Dann folgt $xy + I = (x + I)(y + I) = ab = 0_R = I$ und damit $xy \in I$. Nach Definition des Ideals I würden dann Polynome $f, g \in \mathbb{Q}[x, y]$ existieren mit der Eigenschaft, dass die Gleichung $xy = x^2 f + y^2 g$ erfüllt ist. Aber das ist ausgeschlossen, denn stellt man f und g auf der rechten Seite als Summe von Monomen dar, dann kommt weder in $x^2 f$ noch in $y^2 g$ ein Monom vor, dass genau einmal durch x und genau einmal durch y teilbar ist.

Aufgabe F22T2A4

Sei p eine Primzahl und $n \in \mathbb{N}$. Seien $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ endliche Körper mit p bzw. p^n Elementen.

(a) Sei zunächst $n = 2$. Zeigen Sie: Für jedes $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ gilt $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$.

(b) Bestimmen Sie die Anzahl der Elemente $a \in \mathbb{F}_{p^2}$ mit $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$.

(c) Sei jetzt $n = 6$. Zeigen Sie, dass die Anzahl der Elemente $a \in \mathbb{F}_{p^6}$ mit $\mathbb{F}_{p^6} = \mathbb{F}_p(a)$ genau $p^6 - p^3 - p^2 + p$ beträgt.

(d) Bestimmen Sie die Anzahl der irreduziblen, normierten Polynome $f \in \mathbb{F}_p[x]$ vom Grad 6.

Lösung:
zu (a) Sei $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ vorgegeben. Wegen $a \in \mathbb{F}_{p^2}$ ist $\mathbb{F}_p(a)$ ein Zwischenkörper von $\mathbb{F}_{p^2}|\mathbb{F}_p$. Laut Vorlesung sind die Zwischenkörper dieser Erweiterung durch $\mathbb{F}_{p^d}$ gegeben, wobei $d \in \mathbb{N}$ die Teiler von 2 durchläuft. Es ist somit nur $\mathbb{F}_p(a) = \mathbb{F}_p$ oder $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ möglich. Im Fall $\mathbb{F}_p(a) = \mathbb{F}_p$ wäre $a \in \mathbb{F}_p$, im Widerspruch zur Voraussetzung. Also muss $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ gelten.

zu (b) Zunächst zeigen wir, dass umgekehrt aus $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$ auch $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ folgt. Auf Grund der Gleichung muss offenbar $a \in \mathbb{F}_{p^2}$ gelten. Wäre $a \in \mathbb{F}_p$, dann würde $\mathbb{F}_p(a) = \mathbb{F}_p \subsetneq \mathbb{F}_{p^2}$ folgen. Also ist a in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ enthalten. Zusammen mit dem Ergebnis aus Teil (a) folgt, dass die Elemente $a \in \mathbb{F}_{p^2}$ mit $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ genau die Elemente der Menge $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ sind. Die Anzahl der Elemente in dieser Menge ist gegeben durch $|\mathbb{F}_{p^2} \setminus \mathbb{F}_p| = |\mathbb{F}_{p^2}| - |\mathbb{F}_p| = p^2 - p$.

zu (c) Zunächst beweisen wir für alle $a \in \mathbb{F}_{p^6}$ die Äquivalenz

$$\mathbb{F}_p(a) = \mathbb{F}_{p^6} \quad \Leftrightarrow \quad a \notin \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}.$$

„$\Rightarrow$“ (durch Kontraposition) Ist $a \in \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}$, dann folgt $a \in \mathbb{F}_{p^2}$ oder $a \in \mathbb{F}_{p^3}$. Im ersten Fall erhalten wir $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^2} \subsetneq \mathbb{F}_{p^6}$, im zweiten $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^3} \subsetneq \mathbb{F}_{p^6}$. In beiden Fällen gilt also $\mathbb{F}_p(a) \neq \mathbb{F}_{p^6}$.

„$\Leftarrow$“ Wegen $a \in \mathbb{F}_{p^6}$ ist $\mathbb{F}_p(a)$ ein Zwischenkörper von $\mathbb{F}_{p^6}|\mathbb{F}_p$. Die Zwischenkörper dieser Erweiterung sind gegeben durch $\mathbb{F}_{p^d}$, wobei $d \in \mathbb{N}$ die Teiler von 6 durchläuft, also $d \in \{1, 2, 3, 6\}$ gilt. Im Fall $\mathbb{F}_p(a) = \mathbb{F}_p$ oder $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ wäre $a \in \mathbb{F}_{p^2}$, im Widerspruch zur Voraussetzung. Im Fall $\mathbb{F}_p(a) = \mathbb{F}_{p^3}$ wäre $a \in \mathbb{F}_{p^3}$, was der Voraussetzung ebenfalls widerspricht. Also muss $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$ gelten.

Aus der soeben bewiesenen Äquivalenz folgt, dass die Anzahl der Elemente $a \in \mathbb{F}_{p^6}$ mit $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$ mit der Anzahl der Elemente in $\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ übereinstimmt. Zunächst bestimmen wir $|\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}|$. Es ist $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}$ ein gemeinsamer Teilkörper von $\mathbb{F}_{p^2}$ und $\mathbb{F}_{p^3}$, also von der Form $\mathbb{F}_{p^d}$ mit $d \in \mathbb{N}$ und $d \mid 2, 3$. Es folgt $d = 1$ und $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} = \mathbb{F}_p$. Damit erhalten wir

$$|\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| \quad = \quad |\mathbb{F}_{p^2}| + |\mathbb{F}_{p^3}| - |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}| \quad = \quad |\mathbb{F}_{p^2}| + |\mathbb{F}_{p^3}| - |\mathbb{F}_p| \quad = \quad p^2 + p^3 - p.$$

Die gesuchte Elementezahl ist somit $|\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| = |\mathbb{F}_{p^6}| - |\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| = p^6 - (p^2 + p^3 - p) = p^6 - p^2 - p^3 + p$.

zu (d) Sei L ein algebraischer Abschluss von $\mathbb{F}_{p^6}$ (und somit zugleich ein algebraischer Abschluss von $\mathbb{F}_p$). Jedes irreduzible, normierte Polynom $f \in \mathbb{F}_p[x]$ vom Grad 6 ist laut Vorlesung separabel, besitzt also laut Vorlesung sechs verschiedene Nullstellen in L. Bezeichnet a eine solche Nullstelle, dann ist f das Minimalpolynom von a über $\mathbb{F}_p$. Daraus folgt $[\mathbb{F}_(a) : \mathbb{F}_p] = \text{grad}(f) = 6$ und somit $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$, denn laut Vorlesung ist $\mathbb{F}_{p^6}|\mathbb{F}_p$ die eindeutig bestimmte Teilerweiterung von $L|\mathbb{F}_p$ vom Grad 6. Wäre

$a \in \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}$, dann würde $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^2}$ oder $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^3}$ und somit $[\mathbb{F}_p(a) : \mathbb{F}_p] \leq [\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$ oder $[\mathbb{F}_p(a) : \mathbb{F}_p] \leq [\mathbb{F}_{p^3} : \mathbb{F}_p] = 3$ folgen, im Widerspruch zu $[\mathbb{F}_p(a) : \mathbb{F}_p] = 6$. Insgesamt haben wir damit gezeigt, dass f genau 6 verschiedene Nullstellen in $\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ besitzt.

Umgekehrt gilt für jedes $a \in \mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$, wie in Teil (c) gezeigt, jeweils $\mathbb{F}_{p^6} = \mathbb{F}_p(a)$. Bezeichnet $f \in \mathbb{F}_p[x]$ das Minimalpolynom von a über $\mathbb{F}_p$, dann folgt $\operatorname{grad}(f) = [\mathbb{F}_p(a) : \mathbb{F}_p] = [\mathbb{F}_{p^6} : \mathbb{F}_p] = 6$. Außerdem ist f normiert, irreduzibel, und es gilt $f(a) = 0$. Also ist jedes $a \in \mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ Nullstelle von einem normierten, irreduziblen Polynom vom Grad 6 in $\mathbb{F}_p[x]$.

Insgesamt ist damit gezeigt, dass die Anzahl der Elemente in $\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ sechsmal so groß ist wie die Anzahl der normierten, irreduziblen Polynome vom Grad 6. Mit dem Ergebnis von Teil (c) kommen wir zu dem Schluss, dass es genau $\frac{1}{6}(p^6 - p^2 - p^3 + p)$ solche Polynome gibt.

Aufgabe F22T2A5

Betrachten Sie die Teilkörper $K_1 = \mathbb{Q}(\sqrt{3})$ und $K_2 = \mathbb{Q}(\sqrt{6})$ von $\mathbb{C}$.

(a) Zeigen Sie: Für das Kompositum $L = K_1K_2$ gilt $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(b) Beweisen Sie: $K_1 \cap K_2 = \mathbb{Q}$

(c) Bestimmen Sie den Grad der Körpererweiterung $L|\mathbb{Q}$.

(d) Zeigen Sie, dass $L|\mathbb{Q}$ galoissch ist und bestimmen Sie die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ bis auf Isomorphie.

(e) Bestimmen Sie sämtliche Zwischenkörper der Erweiterung $L|\mathbb{Q}$.

Lösung:
zu (a) Nach Definition ist das Kompositum gleich $K_1(K_2)$, also die von K_2 erzeugte Erweiterung des Körpers K_1. Zu zeigen ist, dass $K_1(K_2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ gilt. Für die Inklusion „$\supseteq$“ muss gezeigt werden, dass $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\}$ in $K_1(K_2)$ gezeigt werden, denn daraus folgt, dass $K_1(K_2)$ ein Erweiterungskörper von $\mathbb{Q}$ ist, der $\{\sqrt{2}, \sqrt{3}\}$ enthält, und $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist nach Definition der kleinste Erweiterungskörper von $\mathbb{Q}$ mit dieser Eigenschaft. Offenbar gilt $\mathbb{Q} \subseteq K_1 \subseteq K_1(K_2)$, und wegen $\sqrt{3} \in K_1$ ist $\sqrt{3}$ auch in $K_1(K_2)$ enthalten. Desweiteren gilt $\sqrt{6} \in K_2$, somit auch $\sqrt{6} \in K_1(K_2)$, und mit $\sqrt{3}$ und $\sqrt{6}$ ist auch $\sqrt{2} = \frac{\sqrt{6}}{\sqrt{3}}$ im Teilkörper $K_1(K_2)$ enthalten.

Für die Inklusion „$\subseteq$“ muss $K_1 \cup K_2 \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ nachgewiesen werden. Wegen $\{\sqrt{3}\} \subseteq \{\sqrt{2}, \sqrt{3}\}$ ist $K_1 = \mathbb{Q}(\sqrt{3})$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ enthalten. Für die Inklusion $K_2 = \mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ genügt es auf Grund der Teilkörper-Eigenschaft von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ zu zeigen, dass $\mathbb{Q} \cup \{\sqrt{6}\} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ gilt. Die Inklusion $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist erfüllt, weil $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nach Definition ein Erweiterungskörper von $\mathbb{Q}$ ist, und mit $\sqrt{2}$ und $\sqrt{3}$ ist auch das Produkt $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ enthalten.

zu (b) Die Inklusion „$\supseteq$“ ist wegen $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) = K_1$ und $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{6}) = K_2$ erfüllt. Für die Inklusion „$\subseteq$“ bemerken wir zunächst, dass $K_1 \cap K_2$ ein Zwischenkörper von $K_1|\mathbb{Q}$ ist. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$ für jede quadratfreie Zahl $m \in \mathbb{Z} \setminus \{0, 1\}$, insbesondere also $[K_1 : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Auf Grund der Gradformel gilt

$$2 \quad = \quad [K_1 : \mathbb{Q}] \quad = \quad [K_1 : K_1 \cap K_2] \cdot [K_1 \cap K_2 : \mathbb{Q}] \quad ,$$

daraus folgt $[K_1 \cap K_2 : \mathbb{Q}] \in \{1, 2\}$. Im Fall $[K_1 \cap K_2 : \mathbb{Q}] = 2$ wäre $[K_1 : K_1 \cap K_2] = K_1$ und somit $K_1 = K_1 \cap K_2$, was zu $K_1 \subseteq K_2$ äquivalent ist. Daraus wiederum würde folgen, dass $\sqrt{3}$ in $K_2 = \mathbb{Q}(\sqrt{6})$ enthalten ist. Aus der Vorlesung aber ist bekannt, dass für zwei verschiedene, quadratfreie Zahlen $m, n \in \mathbb{Z}\setminus\{0, 1\}$ jeweils $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$ gilt. Also muss $[K_1 \cap K_2 : \mathbb{Q}] = 1$ gelten, woraus $K_1 \cap K_2 = \mathbb{Q}$ folgt.

zu (c) Bereits in Teil (b) wurde festgestellt, dass $[K_1 : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ gilt. Das Polynom $f = x^2 - 2 \in \mathbb{Q}(\sqrt{3})[x]$ ist normiert, und es erfüllt $f(\sqrt{2}) = 0$. Wäre es über $\mathbb{Q}(\sqrt{3})$ reduzibel, dann müssten wegen $\mathrm{grad}(f) = 2$ die beiden Nullstellen $\pm\sqrt{2}$ in $\mathbb{Q}(\sqrt{3})$ liegen. Weil aber 2 und 3 zwei verschiedene, quadratfreie Zahlen in $\mathbb{Z} \setminus \{0, 1\}$ sind, gilt $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. Also ist f in $\mathbb{Q}(\sqrt{3})[x]$ irreduzibel, insgesamt das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}(\sqrt{3})$. Daraus folgt

$$[L : \mathbb{Q}(\sqrt{3})] \quad = \quad [\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})] \quad = \quad \mathrm{grad}(f) = 2$$

und $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

zu (d) Wir zeigen, dass L ein Zerfällungskörper des Polynoms $g = (x^2 - 2)(x^2 - 3)$ über $\mathbb{Q}$ ist. Daraus folgt, dass $L|\mathbb{Q}$ eine normale und insbesondere eine algebraische Erweiterung ist. Zu zeigen ist $\mathbb{Q}(N) = L$, also $\mathbb{Q}(N) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, wobei N die Menge der komplexen Nullstellen von g bezeichnet. Diese Menge ist gegeben durch $N = \{\pm\sqrt{2}, \pm\sqrt{3}\}$, es ist also $\mathbb{Q}(\{\pm\sqrt{2}, \pm\sqrt{3}\}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ nachzuweisen. Die Inklusion „$\supseteq$“ ist wegen $\{\sqrt{2}, \sqrt{3}\} \subseteq N$ erfüllt. Mit $\sqrt{2}$ und $\sqrt{3}$ sind auch $-\sqrt{2}, -\sqrt{3}$ im Teilkörper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ von $\mathbb{R}$ enthalten. Somit ist auch die Inklusion „$\subseteq$“ gültig.

Als algebraische Erweiterung von $\mathbb{Q}$ ist $L|\mathbb{Q}$ wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel, insgesamt eine Galois-Erweiterung. Weil $L|\mathbb{Q}$ eine Galois-Erweiterung ist, ist die Ordnung der Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$ durch $|G| = [L : \mathbb{Q}] = 4$ gegeben. Als Gruppe von Primzahlquadratordnung ist G abelsch, und als endliche abelsche Gruppe ist G isomorph zu einem äußeren direkten Produkt zyklischer Gruppen. Damit gilt entweder $G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wäre G zyklisch, also $G \cong \mathbb{Z}/4\mathbb{Z}$, dann gäbe es in G zu jedem Teiler der Gruppenordnung genau eine Untergruppe der entsprechenden Ordnung, insbesondere genau eine Untergruppe U der Ordnung 2, die in G zugleich vom Index 2 ist, wegen $(G : U) = \frac{|G|}{|U|} = \frac{4}{2} = 2$. Daraus wiederum folgt laut Galoistheorie, dass es genau einen Zwischenkörper M von $L|\mathbb{Q}$ mit $[M : \mathbb{Q}] = 2$ gibt.

Nach Teil (a) sind die Elemente $\sqrt{2}, \sqrt{3}, \sqrt{6}$ in L enthalten. Daraus folgt, dass $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$ Zwischenkörper von $L|\mathbb{Q}$ sind. Da es sich bei 2, 3 und 6 um verschiedene quadratfreie Zahlen in $\mathbb{Z} \setminus \{0, 1\}$ handelt, sind diese Zwischenkörper alle vom Grad 2 über $\mathbb{Q}$ und voneinander verschieden. Es gibt also mehr als einen Zwischenkörper von $L|\mathbb{Q}$ vom Grad 2 über $\mathbb{Q}$. Also ist G nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$, sondern zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

zu (e) Nach dem Hauptsatz der Galoistheorie stimmt die Anzahl der Zwischenkörper von $L|\mathbb{Q}$ mit der Anzahl der Untergruppen von $G = \mathrm{Gal}(L|\mathbb{Q})$ überein, wegen der Isomorphie also auch mit der Anzahl der Untergruppen von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Nach dem Satz von Lagrange ist die Ordnung jeder Untergruppe ein Teiler von $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$, also gleich 1, 2 oder 4. Die einzige Untergruppe der Ordnung 1 ist $\{(\bar{0}, \bar{0})\}$, und die einzige Untergruppe der Ordnung 4 ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Jede Untergruppe der Ordnung 2 ist zyklisch, wird also von einem Element der Ordnung 2 erzeugt. Daraus folgt, dass $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ genau drei Untergruppen der Ordnung 2 besitzt, nämlich $\langle(\bar{1}, \bar{0})\rangle$, $\langle(\bar{0}, \bar{1})\rangle$ und $\langle(\bar{1}, \bar{1})\rangle$. Insgesamt haben $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und G also genau fünf Untergruppen, und dementsprechend hat die Erweiterung $L|\mathbb{Q}$ genau fünf Zwischenkörper.

Wie bereits in Teil (d) festgestellt wurde, gibt es drei verschiedene Zwischenkörper vom Grad 2 über $\mathbb{Q}$, nämlich $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$. Hinzu kommen der Zwischenkörper $\mathbb{Q}$ mit $[\mathbb{Q} : \mathbb{Q}] = 1$ und der Zwischenkörper L mit $[L : \mathbb{Q}] = 4$. Damit haben wir alle fünf Zwischenkörper von $L|\mathbb{Q}$ bestimmt.

Aufgabe F22T3A1

Gegeben sei die Gruppe $G = \mathrm{GL}_2(\mathbb{F}_2)$ der invertierbaren 2×2-Matrizen mit Einträgen im Körper $\mathbb{F}_2$.

(a) Listen Sie alle Elemente von G auf.

(b) Zeigen Sie, dass die natürliche Operation von G auf dem Vektorraum $\mathbb{F}_2^2$ einen Isomorphismus $\varphi : G \to \mathrm{Bij}(\mathbb{F}_2^2 \setminus \{0\})$ induziert. (Hierbei bezeichne $\mathrm{Bij}(M)$ die Gruppe der Bijektionen auf einer Mengen M.) Zeigen Sie insbesondere, dass G isomorph ist zu S_3, der symmetrischen Gruppe über 3 Elementen.

(c) Zeigen Sie, dass eine Gruppe der Ordnung 30 höchstens 6 Untergruppen der Ordnung 5 haben kann.

Lösung:
zu (a) Eine 2×2-Matrix über $\mathbb{F}_2$ ist genau dann invertierbar, liegt also in G, wenn die beiden Spaltenvektoren v und w linear unabhängig sind. Die Ordnung von G ist also gleich der Anzahl der Paare (v, w) mit linear unabhängigen $v, w \in \mathbb{F}_2^2$. Für v kann jeder Vektor aus $\mathbb{F}_2^2 \setminus \{(\bar{0}, \bar{0}\}$ gewählt werden; hierfür gibt es genau drei Möglichkeiten. Ist v bereits gewählt, so ist (v, w) genau dann linear unabhängig, wenn $w \in \mathbb{F}_2^2 \setminus \mathrm{lin}(v)$ gilt. Da $\mathrm{lin}(v)$ aus zwei Elementen besteht (nämlich v und dem Nullvektor), stehen für w jeweils $2^2 - 2 = 2$ Elemente zur Auswahl. Insgesamt ist damit gezeigt, dass die Ordnung von G gleich $2 \cdot 3 = 6$ ist. Offenbar sind die sechs Matrizen in der Menge

$$\left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix} \right\}$$

alle invertierbar, denn die Determinante jeder Matrix ist gleich $\bar{1}$. Also enthält diese Menge genau die Elemente der Gruppe G.

zu (b) Die natürliche Operation von G auf $\mathbb{F}_2^2$ ist gegeben durch $G \times \mathbb{F}_2^2 \to \mathbb{F}_2^2$, $(A, v) \mapsto Av$. Setzen wir $X = \mathbb{F}_2^2 \setminus \{0\}$, dann erhalten wir durch Einschränkung eine Abbildung $\cdot : G \times X \to \mathbb{F}_2^2$. Für alle $A \in G$ und $v \in X$ ist $Av \neq 0_{\mathbb{F}_2^2}$, also $Av \in X$, denn auf Grund der Invertierbarkeit von A besteht der Kern der linearen Abbildung $\mathbb{F}_2^2 \to \mathbb{F}_2^2$, $v \mapsto Av$ nur aus dem Nullvektor. Also kann $\cdot$ als Abbildung $G \times X \to X$ betrachtet werden.

Wir zeigen, dass durch diese Abbildung eine Gruppenoperation definiert ist. Für alle $v \in X$ und alle $A, B \in G$ gilt $E \cdot v = Ev = v$ und $A \cdot (B \cdot v) = A \cdot (Bv) = A(Bv) = (AB)v = (AB) \cdot v$, wobei E die 2×2-Einheitsmatrix über $\mathbb{F}_2$, also das Neutralelement von G, bezeichnet.

Also ist $\cdot$ tatsächlich eine Gruppenoperation von G auf X. Laut Vorlesung existiert somit ein Gruppenhomomorphismus $\phi : G \to \mathrm{Bij}(X)$ mit $\phi(A)(v) = A \cdot v = Av$ für alle $v \in X$. Zu zeigen ist, dass es sich bei ϕ um einen Isomorphismus handelt. Ist $A \in \ker(\phi)$, dann gilt $Ae_1 = \phi(A)(e_1) = \mathrm{id}_X(e_1) = e_1$. Die erste Spalte von A ist also der erste Einheitsvektor e_1. Genauso zeigt man, dass die zweite Spalte von A gleich e_2 ist. Insgesamt gilt also $A = E$. Damit ist nachgewiesen, dass ϕ injektiv ist. Aus $|X| = |\mathbb{F}_2^2 \setminus \{0_{\mathbb{F}_2^2}\}| = 2^2 - 1 = 3$ folgt außerdem $\mathrm{Bij}(X) \cong S_3$ und somit $|\mathrm{Bij}(X)| = |S_3| = 3! = 6 = |G|$. Als injektive Abbildung zwischen gleichmächtigen endlichen Mengen ist ϕ auch surjektiv, insgesamt ein Isomorphismus. Also ist G isomorph zu $\mathrm{Bij}(X)$, und damit auch zu S_3.

zu (c) Sei G eine Gruppe der Ordnung $30 = 2 \cdot 3 \cdot 5$, und sei ν_5 die Anzahl der 5-Sylowgruppen von G. Auf Grund des Dritten Sylowsatzes gilt $\nu_5 \mid 6$. Es kann also in G höchstens sechs 5-Sylowgruppen geben. Wegen $5^1 \mid 30$, $5^2 \nmid 30$ sind die 5-Sylowgruppen von G genau die Untergruppen der Ordnung 5.

Aufgabe F22T3A2

(a) Bestimmen Sie $a, b \in \mathbb{Z}$ so, dass $(1 + 2\mathbb{Z}) \cap (2 + 3\mathbb{Z}) \cap (3 + 5\mathbb{Z}) = a + b\mathbb{Z}$.

(b) Bestimmen Sie sämtliche ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $221x + 39y = 26$.

(c) Sei $n \geq 2$ und nehmen wir an, dass $p = 2^n + 1$ eine Primzahl ist. Zeigen Sie, dass eine Restklasse $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ genau dann die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ erzeugt, wenn a kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist.

Lösung:
zu (a) Eine Zahl $z \in \mathbb{Z}$ liegt genau dann in $(1 + 2\mathbb{Z}) \cap (2 + 3\mathbb{Z}) \cap (3 + 5\mathbb{Z})$, wenn sie die Kongruenzen $z \equiv 1 \bmod 2$, $z \equiv 2 \bmod 3$ und $z \equiv 3 \bmod 5$ erfüllt. Wegen $23 \equiv 1 \bmod 2$, $23 \equiv 2 \bmod 3$ und $23 \equiv 3 \bmod 5$ (und weil Kongruenzrelationen Äquivalenzrelationen, also insbesondere transitiv, sind), ist dies äquivalent zu $z \equiv 23 \bmod n$ für $n \in \{2, 3, 5\}$, also zu $n \mid (z - 23)$ für $n \in \{2, 3, 5\}$. Wegen $\mathrm{kgV}(2, 3, 5) = 30$ ist dies äquivalent zu $30 \mid (z - 23)$, also zu $z \equiv 23 \bmod 30$ und somit zu $z \in 23 + 30\mathbb{Z}$. Die Zahlen $a = 23$ und $b = 30$ haben also die gewünschte Eigenschaft.

zu (b) Für alle $(x, y) \in \mathbb{Z}^2$ ist die Gleichung $221x + 39y = 26$ äquivalent zu $17x + 3y = 2$. Dies wiederum ist äquivalent zu $(17x \equiv 2 \bmod 3) \wedge (y = \frac{1}{3}(2 - 17x))$. Die Kongruenz ist äquivalent zur Gleichung $(2 + 3\mathbb{Z})(x + 2\mathbb{Z}) = 2 + 3\mathbb{Z}$ in $\mathbb{Z}/3\mathbb{Z}$, somit auch zu $x + 2\mathbb{Z} = 1 + 3\mathbb{Z}$, auf Grund der Invertierbarkeit von $2 + 3\mathbb{Z}$ in diesem Ring. Dies wiederum ist äquivalent zur Aussage, dass $x = 1 + 3z$ für ein $z \in \mathbb{Z}$ gilt. Die Menge der ganzzahligen Lösungen der Gleichung ist also gegeben durch $\{(1 + 3z, \frac{1}{3}(2 - 17(1 + 3z))) \mid z \in \mathbb{Z}\}$, was zu $\{(1 + 3z, -5 - 17z) \mid z \in Z\}$ vereinfacht werden kann.

zu (c) Da p eine Primzahl ist, handelt es sich bei $\mathbb{Z}/p\mathbb{Z}$ um einen Körper, und deshalb gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$. Somit gilt $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1 = 2^n$. Laut Vorlesung ist die multiplikative Gruppe eines endlichen Körpers zyklisch, es existiert also ein $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $(\mathbb{Z}/p\mathbb{Z})^\times = \langle c \rangle$. Sei $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ beliebig vorgegeben. Dann existiert ein $j \in \{0, ..., p - 2\}$ mit $a = c^j$.

„$\Leftarrow$“ Ist a kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$, dann muss j ungerade sein, denn wäre j gerade, $j = 2k$ für ein $k \in \mathbb{N}_0$, dann würde $a = c^{2k} = (c^k)^2$ folgen im Widerspruch zur Voraussetzung, dass a kein Quadrat ist. Als ungerade Zahl ist j teilerfremd zur Gruppenordnung 2^n. Daraus folgt laut Vorlesung, dass c und $a = c^j$ dieselbe Ordnung haben. Es gilt also $\mathrm{ord}(a) = 2^n = |(\mathbb{Z}/p\mathbb{Z})^\times|$, und daraus folgt $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$.

„$\Rightarrow$“ Wenn a ein Quadrat ist, $a = b^2$ für ein $b \in \mathbb{Z}/p\mathbb{Z}$, dann ist mit a auch b ungleich $\bar{0}$, also eine Einheit. Weil 2 ein Teiler der Gruppenordnung 2^n ist, gilt $\mathrm{ord}(a) = \mathrm{ord}(b^2) \leq \frac{1}{2}\mathrm{ord}(b) = \frac{1}{2}|(\mathbb{Z}/p\mathbb{Z})^\times|$. Wegen $\mathrm{ord}(a) < |(\mathbb{Z}/p\mathbb{Z})^\times|$ kann a kein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ sein.

Aufgabe F22T3A3

Es sei $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ der Ring der ganzen Gauß'schen Zahlen.

(a) Bestimmen Sie die Einheitengruppe von R. Führen Sie einen expliziten und vollständigen Beweis der Korrektheit Ihres Ergebnisses.

(b) Zeigen Sie, dass zwei Elemente $w, z \in R$ genau dann assoziiert sind, wenn $w^4 = z^4$ gilt.

(c) Es sei $(1-i)$ das von dem Element $1-i$ erzeugte Ideal von R. Bestimmen Sie das Ideal $(1-i) \cap \mathbb{Z}$.

Lösung:
zu (a) Sei $N : \mathbb{C} \to \mathbb{R}_+$ die Normfunktion gegeben durch $N(z) = z\bar{z} = |z|^2$ für alle $z \in \mathbb{C}$. Diese Funktion ist multiplikativ, denn für alle $z, w \in \mathbb{C}$ gilt $N(zw) = |zw|^2 = (|z||w|)^2 = |z|^2|w|^2 = N(z)N(w)$. Die Einschränkung von N auf $\mathbb{Z}[i]$ nimmt nur Werte in $\mathbb{N}_0$ an, denn für alle $a, b \in \mathbb{Z}$ gilt $N(a + ib) = |a + ib|^2 = a^2 + b^2 \in \mathbb{N}_0$. Ist nun $\varepsilon = a + ib$ eine Einheit in $\mathbb{Z}[i]$, mit $a, b \in \mathbb{Z}$, dann gilt $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$, und wegen $N(\varepsilon), N(\varepsilon^{-1}) \in \mathbb{N}_0$ folgt daraus $a^2 + b^2 = N(\varepsilon) = 1$. Die Lösungsmenge der Gleichung $a^2 + b^2 = 1$ in $\mathbb{Z}^2$ ist $L = \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$. Aus $(a, b) \in L$ wiederum folgt $\varepsilon = a + ib \in \{1, -1, i, -i\}$. Damit ist $\mathbb{Z}[i]^\times \subseteq \{\pm 1, \pm i\}$ nachgewiesen. Andererseits zeigen die Gleichungen $1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i) = 1$, dass alle vier Elemente der Menge $\{\pm 1, \pm i\}$ Einheiten sind. Also ist die Einheitengruppe von $\mathbb{Z}[i]$ durch $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ gegeben.

zu (b) Sind $z, w \in \mathbb{Z}[i]$ zueinander assoziiert, dann existiert ein $\varepsilon \in \mathbb{Z}[i]^\times$ mit $w = \varepsilon z$. Nach Teil (a) ist ε damit in der Menge $\{\pm 1, \pm i\}$ enthalten, und wegen $1^4 = (-1)^4 = i^4 = (-i)^4 = 1$ folgt $\varepsilon^4 = 1$. Damit wiederum erhalten wir $w^4 = \varepsilon^4 z^4 = 1 \cdot z^4 = z^4$. Setzen wir umgekehrt $w^4 = z^4$ voraus, dann gilt entweder $w = z = 0$ oder $w, z \neq 0$. Im ersten Fall sind w und z wegen $0 = 1 \cdot 0$ zueinander assoziiert. Ansonsten kann die Gleichung $z^4 = w^4$ zu $(\frac{w}{z})^4 - 1 = 0$ umgeformt werden. Die einzigen komplexen Nullstellen des Polynoms $x^4 - 1$ sind $\pm 1, \pm i$, also die Einheiten von $\mathbb{Z}[i]$. Dies zeigt, dass $w = \frac{w}{z} \cdot z = \varepsilon z$ für ein $\varepsilon \in \mathbb{Z}[i]^\times$ erfüllt, die Elemente w, z also zueinander assoziiert sind.

zu (c) Wir zeigen, dass $(1 - i) \cap Z = 2\mathbb{Z}$ gilt. Als Urbild des Ideals $(1 - i)$ unter dem Inklusionshomomorphismus $\mathbb{Z} \to \mathbb{Z}[i]$, $a \mapsto a$ ist $(1 - i)$ ein Ideal in $\mathbb{Z}$, und dieses enthält 2 wegen $2 \in \mathbb{Z}$ und $2 = (1 + i)(1 - i) \in (1 - i)$. Aus $2 \in (1 - i) \cap Z$ und der Idealeigenschaft von $(1 - i) \cap \mathbb{Z}$ folgt $2\mathbb{Z} \subseteq (1 - i) \cap Z$. Sei nun umgekehrt $a \in (1 - i) \cap \mathbb{Z}$ vorgegeben. Dann gilt $a = \gamma \cdot (1 - i)$ für ein $\gamma \in \mathbb{Z}[i]$. Wegen $a^2 = N(a) = N(\gamma)N(1 - i) = 2N(\gamma)$ ist a^2 gerade. Damit ist auch a gerade, also $a \in 2\mathbb{Z}$.

Aufgabe F22T3A4

Es sei K ein Teilkörper von $\mathbb{C}$, so dass $K|\mathbb{Q}$ eine Galois-Erweiterung vom Grad 4 mit zyklischer Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist. Zeigen Sie, dass dann $i \notin K$ gilt.
Hinweis: Nehmen Sie an, dass $i \in K$ gilt und betrachten Sie $K|\mathbb{Q}(i)$.

Lösung:
Sei $G = \mathrm{Gal}(K|\mathbb{Q})$, und nehmen wir an, es gilt $i \in K$. Dann ist $\mathbb{Q}(i)$ ein Zwischenkörper von $K|\mathbb{Q}$. Weil -1 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, ist $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ eine Erweiterung von $\mathbb{Q}$ vom Grad 2. Laut Galoistheorie ist $U = \mathrm{Gal}(K|\mathbb{Q}(i))$ damit eine Untergruppe vom Index 2, und wegen $|U| = \frac{|G|}{(G:U)} = \frac{4}{2} = 2$ ist diese auch von Ordnung 2. Weil G zyklisch ist, gibt es für jeden Teiler der Gruppenordnung 4 genau eine Untergruppe der Ordnung 4. Daraus folgt, dass U die einzige Untergruppe der Ordnung 2 in G ist.

Sei nun $\rho : K \to \mathbb{C}$ die Einschränkung der komplexen Konjugation $z \mapsto \bar{z}$ auf K. Diese Abbildung ist ein $\mathbb{Q}$-Homomorphismus, und weil $K|\mathbb{Q}$ als Galois-Erweiterung insbesondere normal ist, sogar ein $\mathbb{Q}$-Automorphismus von K, also ein Element der Galoisgruppe G. Für alle $\alpha \in K$ gilt $\rho^2(\alpha) = \rho(\bar{\alpha}) = \bar{\bar{\alpha}} = \alpha$, also $\rho^2 = \mathrm{id}_K$. Wegen $i \in K$ und $\rho(i) = -i \neq i$ ist andererseits $\rho \neq \mathrm{id}_K$. Also ist $\rho \in G$ ein Element der Ordnung 2. Weil U die einzige Untergruppe der Ordnung 2 in G ist, muss $\langle \rho \rangle = U$ und insbesondere $\rho \in U$ gelten. Aber wegen $U = \mathrm{Gal}(K|\mathbb{Q}(i))$ folgt daraus $\rho(i) = i$, im Widerspruch zu $\rho(i) = -i$. Also ist die Annahme $i \in K$ falsch, und es folgt $i \notin K$.

Aufgabe F22T3A5

Es sei $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$.

(a) Bestimmen Sie den Grad der Körpererweiterung $K|\mathbb{Q}$.

(b) Entscheiden und begründen Sie, ob es einen $\mathbb{Q}$-Homomorphismus $\varphi : K \to \mathbb{C}$ mit $\varphi(\sqrt[3]{2}) = \sqrt{3}$ gibt.

(c) Entscheiden und begründen Sie, ob die Erweiterung $K|\mathbb{Q}$ galoissch ist.

Lösung:

zu (a) Das Polynom $f = x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 2), es ist normiert und erfüllt $f(\sqrt[3]{2}) = 0$. Also ist f das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \operatorname{grad}(f) = 3$. Weil 3 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, gilt laut Vorlesung $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Das Polynom $g = x^2 - 3 \in \mathbb{Q}(\sqrt[3]{2})[x]$ ist normiert und erfüllt $g(\sqrt{3}) = 0$. Wäre es in $\mathbb{Q}(\sqrt[3]{2})[x]$ reduzibel, dann müsste die Nullstelle $\sqrt{3}$ von g wegen $\operatorname{grad}(g) = 2$ in $\mathbb{Q}(\sqrt[3]{2})$ liegen. Es wäre dann $\mathbb{Q}(\sqrt{3})$ ein Zwischenkörper von $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$, und die Gradformel würde

$$3 \quad = \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] \cdot 2$$

liefern. Es gilt aber $2 \nmid 3$, und somit ist g in $\mathbb{Q}(\sqrt[3]{2})[x]$ irreduzibel. Somit ist g das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt[3]{2})$, und es folgt $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = \operatorname{grad}(g) = 2$. Schließlich ist das Polynom $h = x^2 + 1 \in \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$ normiert und erfüllt $h(i) = 0$. Wäre es über $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ reduzibel, dann müsste wegen $\operatorname{grad}(h) = 2$ die Nullstelle i in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ liegen. Aber dies ist wegen $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) \subseteq \mathbb{R}$ und $i \notin \mathbb{R}$ nicht der Fall. Also ist h in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$ irreduzibel, insgesamt das Minimalpolynom von h über $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. Daraus folgt

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})] \quad = \quad \operatorname{grad}(h) \quad = \quad 2.$$

Mit der Gradformel erhalten wir nun

$$\begin{aligned}[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : \mathbb{Q}] \quad &= \quad [[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})] \cdot [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \\ &= \quad 2 \cdot 2 \cdot 3 \quad = \quad 12.\end{aligned}$$

zu (b) Nehmen wir an, ein $\mathbb{Q}$-Homomorphismus φ wie angegeben existiert. Ist $f \in \mathbb{Q}[x]$ und $\alpha \in \mathbb{C}$ eine Nullstelle von f, dann muss laut Vorlesung $\varphi(\alpha)$ eine Nullstelle desselben Polynoms sein. Da nun $\sqrt[3]{2}$ eine Nullstelle von $f = x^3 - 2$ ist, müsste auch $\varphi(\sqrt[3]{2}) = \sqrt{3}$ eine Nullstelle von f sein. Tatsächlich gilt aber $f(\sqrt{3}) \neq 0$, denn die komplexen Nullstellen von f sind $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$ mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, insbesondere ist $\sqrt[3]{2}$ die einzige reelle Nullstelle. Also existiert kein $\mathbb{Q}$-Homomorphismus $\varphi : K \to \mathbb{C}$ mit $\varphi(\sqrt[3]{2}) = \sqrt{3}$.

Anmerkung:

In der Orginalfassung der Aufgabenstellung war von einem $\mathbb{Q}$-Automorphismus $K \to \mathbb{C}$ die Rede. Das ist natürlich nicht sinnvoll, denn bei einem Automorphismus (egal ob von Körpern, Ringen, Gruppen oder Vektorräumen) müssen Definitions- und Wertebereich stets übereinstimmen.

zu (c) Wir zeigen, dass die Erweiterung $K|\mathbb{Q}$ normal ist, indem wir nachweisen, dass es sich bei K um den Zerfällungskörper des Polynoms $g = (x^3 - 2)(x^2 + 1) \in \mathbb{Q}[x]$ über $\mathbb{Q}$ handelt. Wie bereits in Teil (b) festgestellt, ist $\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$ mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ die Menge der komplexen Nullstellen von $x^3 - 2$, und $\pm i$ sind die komplexen Nullstellen von $x^2 + 1$. Daraus folgt, dass $N = \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}, i, -i\}$ die Nullstellenmenge von g ist. Zu zeigen ist also

$$\mathbb{Q}(N) \quad = \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i).$$

„$\subseteq$“ Es genügt, $N \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ nachzuweisen. mit $\sqrt{3}$ und i ist auch $\sqrt{-3} = i\sqrt{3}$ in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ enthalten, damit auch $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ und ζ^2. Da auch $\sqrt[3]{2}$ und $\pm i$ in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ liegen, folgt insgesamt $N = \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}, i, -i\} \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$.

„$\supseteq$“ Zu zeigen ist $\{\sqrt[3]{2}, \sqrt{3}, i\} \subseteq \mathbb{Q}(N)$. Wegen $\sqrt[3]{2}, i \in N$ gilt $\sqrt[3]{2}, i \in \mathbb{Q}(N)$. Mit $\sqrt[3]{2} \in \mathbb{Q}(N)$ und $\zeta\sqrt[3]{2} \in \mathbb{Q}(N)$ gilt auch $\zeta = \frac{\zeta\sqrt[3]{2}}{\sqrt[3]{2}} \in \mathbb{Q}(N)$ und damit auch $\sqrt{-3} = 2\zeta + 1 \in \mathbb{Q}(N)$. Aus $\sqrt{-3} \in \mathbb{Q}(N)$ und $i \in N \subseteq \mathbb{Q}(N)$ folgt $\sqrt{3} = (-i)\sqrt{-3} \in \mathbb{Q}(N)$. Damit ist die Inklusion $\{\sqrt[3]{2}, \sqrt{3}, i\} \subseteq \mathbb{Q}(N)$ vollständig nachgewiesen.

Als normale Erweiterung ist $K|\mathbb{Q}$ insbesondere algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch separabel. Insgesamt ist $K|\mathbb{Q}$ also tatsächlich eine Galois-Erweiterung.

Aufgabe H22T1A1

Gegeben sei die Gruppe

$$G \quad = \quad \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathcal{M}_{2,\mathbb{Q}} \;\middle|\; a, b, c \in \mathbb{Q}, ac \neq 0 \right\}$$

der invertierbaren oberen 2×2-Dreiecksmatrizen über $\mathbb{Q}$. Ferner seien

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \;\middle|\; c = a \right\} \qquad \text{und} \qquad U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \;\middle|\; b = 0 \right\}.$$

(a) Zeigen Sie, dass H ein Normalteiler von G ist und dass durch

$$\varphi : G/H \to \mathbb{Q}^\times \quad \text{mit} \quad \varphi\left(\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right] \right) = \frac{a}{c}$$

ein wohldefinierter Gruppenisomorphismus gegeben ist.

(b) Zeigen Sie, dass U eine Untergruppe von G, aber kein Normalteiler ist.

(c) Betrachten Sie die Operation von U auf H durch Konjugation. Geben Sie ein Repräsentantensystem der Bahnen dieser Gruppenoperation an.

Lösung:

zu (a) Wir beweisen die Existenz des angegebenen Isomorphismus durch Anwendung des Homomorphiesatzes für Gruppen. Sei $\hat{\varphi} : G \to \mathbb{Q}^\times$ gegeben durch

$$\hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) \quad = \quad \frac{a}{c} \qquad \text{für} \quad a, c \in \mathbb{Q}^\times \text{ und } b \in \mathbb{Q}.$$

Diese Abbildung ist ein Gruppenhomomorphismus, denn für alle $a, a_1, c, c_1 \in \mathbb{Q}^\times$ und alle $b, b_1 \in \mathbb{Q}$ gilt

$$\hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \right) \quad = \quad \hat{\varphi}\left(\begin{pmatrix} aa_1 & ab_1 + bc_1 \\ 0 & cc_1 \end{pmatrix} \right) \quad = \quad \frac{aa_1}{cc_1}(aa_1)(cc_1) \quad = \quad \frac{a}{c} \cdot \frac{a_1}{c_1}$$

$$= \quad \hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) \hat{\varphi}\left(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \right).$$

Für alle $a, c \in \mathbb{Q}^\times$ und $b \in \mathbb{Q}$ gilt die Äquivalenz

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \ker(\hat{\varphi}) \quad \Leftrightarrow \quad \hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = 1 \quad \Leftrightarrow \quad \frac{a}{c} = 1 \quad \Leftrightarrow \quad c = a \quad \Leftrightarrow \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in H.$$

Dies zeigt, dass $H = \ker(\hat{\varphi})$ gilt. Als Kern eines Gruppenhomomorphismus $G \to \mathbb{Q}^\times$ ist H ein Normalteiler von G. Darüber hinaus ist $\hat{\varphi}$ surjektiv. Ist nämlich $a \in \mathbb{Q}^\times$ vorgegeben, dann gilt

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in G \text{ wegen } a \cdot 1 = a \neq 0 \quad \text{und außerdem} \quad \hat{\varphi}\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right) = a \cdot 1 = a.$$

Damit ist nachgewiesen, dass $\hat{\varphi}$ die Voraussetzungen des Homomorphiesatzes erfüllt. Auf Grund des Satzes existiert ein wohldefinierter Isomorphismus $G/H \to \mathbb{Q}^\times$ gegeben durch

$$\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right] \quad \mapsto \quad \hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = ac$$

für alle $a, c \in \mathbb{Q}^\times$ und $b \in \mathbb{Q}$. Dieser stimmt offenbar mit der in der Aufgabenstellung angegebenen Abbildung überein.

zu (b) Zunächst zeigen wir, dass U eine Untergruppe von G ist. Das Neutralelement von G ist die Einheitsmatrix E_2, und diese ist offenbar in U enthalten (setze $a = c = 1$. Seien nun $A, A_1 \in U$ vorgegeben. Dann sind auch AA_1 und A^{-1} in U enthalten. Denn wegen $A, A_1 \in U$ gibt es $a, a_1, c, c_1 \in \mathbb{Q}^\times$ mit

$$A = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \quad \text{und} \quad A_1 = \begin{pmatrix} a_1 & 0 \\ 0 & c_1 \end{pmatrix} \quad ,$$

und es folgt

$$AA_1 = \begin{pmatrix} aa_1 & 0 \\ 0 & cc_1 \end{pmatrix} \in U \quad \text{und} \quad A^{-1} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} \in U$$

wegen $aa_1, cc_1 \in \mathbb{Q}^\times$. Wäre U ein Normalteiler, dann wäre wegen

$$B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in U \quad \text{und} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$$

auch TBT^{-1} in U enthalten. Tatsächlich aber gilt

$$\begin{aligned} TBT^{-1} &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \notin U. \end{aligned}$$

zu (c) Um zu erkennen, welche Gestalt die Bahnen der Gruppenoperation haben, wenden wir ein beliebiges Element der Gruppe U auf ein beliebiges Element der Menge H an. Für alle $a, a_1, c \in \mathbb{Q}^\times$ und $b_1 \in \mathbb{Q}$ gilt

$$\begin{aligned} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} &= \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} \\ &= \begin{pmatrix} aa_1 & ab_1 \\ 0 & ca_1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} a_1 & ab_1c^{-1} \\ 0 & a_1 \end{pmatrix}. \end{aligned}$$

Ist $b_1 = 0$, dann besteht die Bahn also nur aus der Diagonalmatrix a_1E_2, ansonsten durchläuft der Eintrag rechts oben alle Elemente aus $\mathbb{Q}^\times$. Dies führt uns zu der Behauptung, dass die Teilmenge $R \subseteq H$ gegeben durch

$$R = \left\{ \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} \;\middle|\; a_1 \in \mathbb{Q}^\times \;,\; \varepsilon_1 \in \{0, 1\} \right\}$$

ein Repräsentantensystem der Bahnen der Operation ist. Bezeichnet $\mathcal{B}$ die Menge der Bahnen, so müssen wir nachweisen, dass die Abbildung $\phi : R \to \mathcal{B}$, $A \mapsto U(A)$ surjektiv und injektiv ist. Zum Nachweis der Surjektivität sei $U(A) \in \mathcal{B}$ vorgegeben, mit

$$A = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \in H \quad , \quad a_1 \in \mathbb{Q}^\times,\ b_1 \in \mathbb{Q}.$$

Ist $b_1 = 0$, dann liegt A selbst bereits in R, und es gilt $\phi(A) = U(A)$. Betrachten wir nun den Fall $b_1 \neq 0$. Dann gilt

$$\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix} \in R \quad \text{und} \quad \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \in U$$

wegen $a_1 \in \mathbb{Q}^\times$ und $1, b_1 \in \mathbb{Q}^\times$, und außerdem

$$\begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b_1^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} aa_1 & 1 \\ 0 & a_1 b_1^{-1} \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix}.$$

Es folgt

$$\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix} \in U\left(\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\right)$$

und somit

$$\phi\left(\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix}\right) = U\left(\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix}\right) = U\left(\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\right).$$

Damit ist der Nachweis der Surjektivität abgeschlossen.

Zum Nachweis der Injektivität seien

$$\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}, \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} \in R \quad \text{mit} \quad \phi\left(\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix}\right)$$

vorgegeben, wobei $a, a_1 \in \mathbb{Q}^\times$ und $\varepsilon, \varepsilon_1 \in \{0, 1\}$ sind. Nach Definition der Abbildung ϕ folgt

$$U\left(\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}\right) = U\left(\begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix}\right) \qquad \text{und} \qquad \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} \in U\left(\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}\right).$$

Es gibt also ein Element

$$\begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \in U \qquad \text{mit} \qquad \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \cdot \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}$$

und $a_2, c_2 \in \mathbb{Q}^\times$. Es gilt also

$$\begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \cdot \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix}^{-1} =$$

$$\begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} \begin{pmatrix} a_2^{-1} & 0 \\ 0 & c_2^{-1} \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} aa_2^{-1} & \varepsilon c_2^{-1} \\ 0 & ac_2^{-1} \end{pmatrix} = \begin{pmatrix} a & a_2 \varepsilon c_2^{-1} \\ 0 & a \end{pmatrix}$$

Durch Vergleich der Einträge erhalten wir $a_1 = a$ und $\varepsilon_1 = a_2 \varepsilon c_2^{-1}$. Wieder unterscheiden wir zwei Fälle. Ist $\varepsilon = 0$, dann folgt $\varepsilon_1 = 0$ und somit insgesamt

$$\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} = \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix}.$$

Ist $\varepsilon = 1$, dann folgt $\varepsilon_1 = a_2 \varepsilon c_2^{-1} \neq 0$, wegen $\varepsilon_1 \in \{0, 1\}$ also $\varepsilon_1 = 1$. Dies zeigt, dass die beiden Elemente aus R auch in diesem Fall übereinstimmen.

Aufgabe H22T1A2

Sei R der Faktorring $\mathbb{Q}[x]/(x^2-7x+12)$.

(a) Zeigen Sie, dass R als Ring isomorph zu $\mathbb{Q}\times\mathbb{Q}$ ist.

(b) Geben Sie explizit einen Ringisomorphismus $\varphi:\mathbb{Q}\times\mathbb{Q}\to R$ an.

(c) Bestimmen Sie alle Zahlen $a\in\mathbb{Q}$, so dass die Restklasse von $x+a$ in R eine Einheit ist, und finden Sie jeweils das dazu inverse Element.

Lösung:
zu (a) Die p-q-Formel liefert für das Polynom $f=x^2-7x+12$ die Nullstellen 3 und 4. Die Polynome $x-3$ und $x-4$ sind als Polynome vom Grad 1 irreduzibel, und da sie nicht zueinander assoziiert sind, sind sie teilerfremd. Der Chinesische Restsatz kann somit angewendet werden und liefert einen Isomorphismus

$$\bar{\phi}: R=\mathbb{Q}[x]/(f)\to\mathbb{Q}[x]/(x-3)\times\mathbb{Q}[x]/(x-4)\quad,\quad g+(f)\mapsto(g+(x-3),g+(x-4))$$

von Ringen. Für jedes $a\in\mathbb{Q}$ sei $\rho_a:\mathbb{Q}[x]\to g$, $g\mapsto g(a)$ der Auswertungshomomorphismus an der Stelle a. Dieser ist surjektiv, denn für vorgegebenes $c\in\mathbb{Q}$ gilt $\rho_a(c)=c(a)=c$. Es gilt $\ker(\rho_a)=(x-a)$, auf Grund der Äquivalenz

$$g\in\ker(\rho_a)\quad\Leftrightarrow\quad\rho_a(g)=0\quad\Leftrightarrow\quad g(a)=0\quad\Leftrightarrow\quad(x-a)\mid g\quad\Leftrightarrow\quad g\in(x-a)$$

für alle $g\in\mathbb{Q}[x]$. Der Homomorphiesatz für Ringe ist also anwendbar und liefert für jedes $a\in\mathbb{Q}$ einen Isomorphismus $\bar{\rho}_a:\mathbb{Q}[x]/(x-a)\to\mathbb{Q}$, $g+(x-a)\mapsto g(a)$. Durch $(g+(x-3),g+(x-4))\mapsto(g(3),g(4))$ ist somit ein Isomorphismus $\psi:\mathbb{Q}[x]/(x-3)\times\mathbb{Q}[x]/(x-4)\to\mathbb{Q}\times\mathbb{Q}$ definiert, und insgesamt ist $\bar{\phi}\circ\psi$ ein Isomorphismus zwischen R und $\mathbb{Q}\times\mathbb{Q}$.

zu (b) Die Gleichung $1\cdot(x-3)+(-1)\cdot(x-4)=1$ kann zu $1+(3-x)=4-x$ umgestellt werden und liefert wegen $\bar{\phi}(4-x+(f))=((4-x)+(x-3),(4-x)+(x-4))=(1+(x-3),0+(x-4))$ ein Urbild von $(1+(x-3),0+(x-4))\in\mathbb{Q}[x]/(x-3)\times\mathbb{Q}[x]/(x-4)$ bezüglich $\bar{\phi}$. Ebenso überprüft man, dass der Isomorphismus $\bar{\phi}$ das Element $x-3+(f)$ auf $(0+(x-3),1+(x-4))$ abbildet. Für alle $h_1,h_2\in\mathbb{Q}[x]$ gilt

$$\begin{aligned}\bar{\phi}((4-x)h_1+(x-3)h_2+(f)) &= \bar{\phi}(h_1+(f))\bar{\phi}(4-x+(f))+\bar{\phi}(h_2+(f))\bar{\phi}(x-3+(f))\\ &= (h_1+(x-3),h_1+(x-4))(1+(x-3),0+(x-4))+\\ &\quad(h_2+(x-3),h_2+(x-4))(0+(x-3),1+(x-4)) =\\ &\quad(h_1+(x-3),0+(x-4))+(0+(x-3),h_2+(x-4)) = (h_1+(x-3),h_2+(x-4)).\end{aligned}$$

Dies zeigt, dass die Umkehrabbildung von $\bar{\phi}$ durch $\bar{\phi}^{-1}(h_1+(x-3),h_2+(x-4))=(4-x)h_1+(x-3)h_2+(f)$ gegeben ist. Die Umkehrabbildung von ψ ist offenbar gegeben durch $\psi^{-1}(c,d)=(c+(x-3),d+(x-4))$ für alle $(c,d)\in\mathbb{Q}\times\mathbb{Q}$, denn es gilt jeweils $\psi(c+(x-3),d+(x-4))=(c(3),d(4))=(c,d)$. Die Abbildung $\bar{\phi}^{-1}\circ\psi^{-1}$ ist ein Isomorphismus $\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}[x]/(f)$, und dieser ist explizit gegeben durch

$$\begin{aligned}(\bar{\phi}^{-1}\circ\psi^{-1})(c,d) &= \bar{\phi}^{-1}(c+(x-3),d+(x-4)) = c(4-x)+d(x-3)+(f)\\ &= (d-c)x+4c-3d+(f)\end{aligned}$$

für alle $c,d\in\mathbb{Q}$.

zu (c) Sei $a \in \mathbb{Q}$. Da es sich bei $\psi \circ \bar{\phi}$ um einen Isomorphismus von Ringen handelt, ist das Element $x-a+(f)$ genau dann eine Einheit in R, wenn $(\psi \circ \bar{\phi})(x-a+(f)) = \psi(x-a+(x-3), x-a+(x-4)) = (3-a, 4-a)$ eine Einheit in $\mathbb{Q}$ ist. Wegen $(\mathbb{Q} \times \mathbb{Q})^\times = \mathbb{Q}^\times \times \mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}) \times (\mathbb{Q} \setminus \{0\})$ ist dies genau dann der Fall, wenn $3-a \neq 0$ und $4-a \neq 0$ gilt, also genau dann, wenn $a \notin \{3, 4\}$ gilt.

Das Inverse von $(\psi \circ \bar{\phi})(x-a+(f)) = (3-a, 4-a)$ in $\mathbb{Q} \times \mathbb{Q}$ ist $(\frac{1}{3-a}, \frac{1}{4-a})$. Das Inverse von $x-a+(f)$ in R ist somit gegeben durch

$$\begin{aligned}(\psi \circ \bar{\phi})^{-1}(\tfrac{1}{3-a}, \tfrac{1}{4-a}) &= (\bar{\phi}^{-1} \circ \psi^{-1})(\tfrac{1}{3-a}, \tfrac{1}{4-a}) = \bar{\phi}^{-1}\left(\tfrac{1}{3-a} + (x-3), \tfrac{1}{4-a} + (x-4)\right) \\ &= \frac{4-x}{3-a} + \frac{x-3}{4-a} + (f).\end{aligned}$$

Anmerkung:
Dass dieses Element tatsächlich das Inverse von $x-a+(f)$ ist, kann auch durch eine direkte Rechnung überprüft werden: Wegen $(4-a)(3-a) = f(a)$ gilt

$$\begin{aligned}\left(\frac{4-x}{3-a} + \frac{x-3}{4-a} + (f)\right) \cdot (x-a+(f)) &= \left(\frac{(4-x)(4-a)+(x-3)(3-a)}{f(a)} + (f)\right) \cdot (x-a+(f)) \\ &= \big(f(a)^{-1}((16-4x-4a+ax)+(3x-9-ax+3a)) + (f)\big) \cdot (x-a+(f)) \\ = \big(f(a)^{-1}(-x+7-a)+(f)\big) \cdot (x-a+(f)) &= f(a)^{-1}(-x+7-a)(x-a)+(f) \\ = f(a)^{-1}(-x^2+7x+a(a-7))+(f) &= f(a)^{-1}(-x^2+7x+a(a-7)+f)+(f)) \\ = f(a)^{-1}(-x^2+7x+a(a-7)+x^2-7x+12)+(f) &= f(a)^{-1}(a(a-7)+12)+(f) \\ = f(a)^{-1}(a^2-7a+12)+(f) = f(a)^{-1}f(a)+(f) &= 1+(f) = 1_R.\end{aligned}$$

Aufgabe H22T1A3

(a) Sei $L|K$ eine endliche Galois-Erweiterung und sei $a \in L$. Zeigen Sie, dass a genau dann ein primitives Element für $L|K$ ist, wenn die Elemente $\sigma(a)$ für alle $\sigma \in \mathrm{Gal}(L|K)$ paarweise verschieden sind.

(b) Beweisen Sie, dass $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ eine Galois-Erweiterung ist und bestimmen Sie die Elemente der Galois-Gruppe.

(c) Zeigen Sie, dass für alle $q \in \mathbb{Q} \setminus \{0\}$ das Element $a = \sqrt{3} + qi$ ein primitives Element der Galois-Erweiterung $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ ist.

Lösung:
zu (a) „⇒“ Nach Voraussetzung gilt $L = K(a)$. Daraus folgt, dass jedes Element $\sigma \in \mathrm{Gal}(L|K)$ durch das Bild $\sigma(a)$ bereits eindeutig bestimmt ist. Sind also $\sigma, \tau \in \mathrm{Gal}(L|K)$ mit $\sigma(a) = \tau(a)$, dann folgt $\sigma = \tau$. Setzen wir umgekehrt $\sigma \neq \tau$ voraus, dann muss also $\sigma(a) \neq \tau(a)$ gelten.

„⇐“ Auf Grund der Voraussetzung folgt für jedes $\sigma \in \mathrm{Gal}(L|K)$ aus $\sigma(a) = a = \mathrm{id}_L(a)$ bereits $\sigma = \mathrm{id}_L$. Ist nun $\sigma \in \mathrm{Gal}(L|K(a))$, dann gilt $\sigma(\gamma) = \gamma$ für alle $\gamma \in K(a)$, insbesondere also $\sigma(a) = a$ und somit $\sigma = \mathrm{id}_L$. Es gilt also $\mathrm{Gal}(L|K(a)) = \{\mathrm{id}_L\} = \mathrm{Gal}(L|L)$. Nach dem Hauptsatz der Galoistheorie ist $M \mapsto \mathrm{Gal}(L|M)$ eine bijektive Korrespondenz zwischen den Zwischenkörpern von $L|K$ und den Untergruppen von $\mathrm{Gal}(L|K)$. Aus der Gleichheit $\mathrm{Gal}(L|K(a)) = \mathrm{Gal}(L|L)$ folgt also $L = K(a)$, d.h. a ist ein primitives Element der Erweiterung $L|K$.

zu (b) Die Elemente $\sqrt{3}$ und i sind Nullstellen des Polynoms $f = (x^2 - 3)(x^2 + 1) \in \mathbb{Q}[x]$ und somit algebraisch über $\mathbb{Q}$. Daraus folgt, dass $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ eine algebraische Körpererweiterung ist. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ als algebraische Erweiterung auch separabel. Darüber hinaus ist die Erweiterung normal. Um dies zu zeigen, weisen wir nach, dass $\mathbb{Q}(\sqrt{3}, i)$ in $\mathbb{C}$ der Zerfällungskörper von f über $\mathbb{Q}$ ist. Offenbar sind die Elemente der Menge $N = \{\pm\sqrt{3}, \pm i\}$ Nullstellen von f, und wegen $\mathrm{grad}(f) = 4 = |N|$ kann es keine weiteren geben. Somit ist $\mathbb{Q}(N)$ der Zerfällungskörper von f über $\mathbb{Q}$. Wegen $\sqrt{3}, i \in N$ gilt $\mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(N)$. Umgekehrt enthält $\mathbb{Q}(\sqrt{3}, i)$ neben $\sqrt{3}$ und i auch $-\sqrt{3}$ und $-i$ (weil $\mathbb{Q}(\sqrt{3}, i)$ als Teilkörper von $\mathbb{C}$ abgeschlossen unter der Bildung von Negativen ist). Es gilt also $N \subseteq \mathbb{Q}(\sqrt{3}, i)$, und weil $\mathbb{Q}(\sqrt{3}, i)$ ein Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ ist, folgt daraus auch $\mathbb{Q}(N) \subseteq \mathbb{Q}(\sqrt{3}, i)$, insgesamt also $\mathbb{Q}(N) = \mathbb{Q}(\sqrt{3}, i)$.

Also handelt es sich bei $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ tatsächlich um eine Galois-Erweiterung. Sei G die zugehörige Galois-Gruppe; laut Vorlesung ist die Ordnung dieser Gruppe durch $|G| = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$ gegeben. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, weil 3 eine quadratfreie ganze Zahl ungleich $0, 1$ ist. Das Polynom $g = x^2 + 1$ ist normiert und hat i als Nullstelle. Wäre es über $\mathbb{Q}(\sqrt{3})$ reduzibel, dann wären wegen $\mathrm{grad}(g)$ die beiden Nullstellen $\pm i$ in $\mathbb{Q}(\sqrt{3})$ enthalten. Aber dies ist unmöglich, denn wegen $\sqrt{3} \in \mathbb{R}$ gilt einerseits $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, andererseits aber $\pm i \in \mathbb{C} \setminus \mathbb{R}$. Also ist g über $\mathbb{Q}(\sqrt{3})$ irreduzibel, insgesamt das Minimalpolynom von i über $\mathbb{Q}(\sqrt{3})$. Es folgt

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] \quad = \quad [\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})] \quad = \quad \mathrm{grad}(g) \quad = \quad 2 \quad ,$$

und mit der Gradformel erhalten wir $|G| = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Weil das Polynom g über $\mathbb{Q}(\sqrt{3})$ irreduzibel ist, und weil $\pm i$ Nullstellen von g sind, existiert auf Grund des Fortsetzungssatzes ein Element $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}(\sqrt{3}))$ mit $\tau(i) = -i$. Insbesondere ist τ ein Element der Gruppe G, mit $\tau(\sqrt{3}) = \sqrt{3}$ und $\tau(i) = -i$. Das Polynom $h = x^2 - 3$ ist irreduzibel über $\mathbb{Q}(i)$. Wäre es nämlich reduzibel, dann würden die beiden Nullstellen $\pm\sqrt{3}$ bereits in $\mathbb{Q}(i)$ liegen, und daraus würde $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(i)$ folgen. Da -1 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, ergäbe sich daraus $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}] = 2$. Aber dies steht Widerspruch zu unserer Feststellung $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$ von oben. Da $\pm\sqrt{3}$ Nullstellen von h sind, liefert der Fortsetzungssatz ein Element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}(i))$ mit $\sigma(\sqrt{3}) = -\sqrt{3}$, also ein Element $\sigma \in G$ mit $\sigma(\sqrt{3}) = -\sqrt{3}$ und $\sigma(i) = i$.

Neben $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}$, σ und τ ist $\sigma \circ \tau$ ein weiteres Element der Gruppe G. Dieses stimmt mit keinem der drei anderen Elemente überein, denn es gilt einerseits $(\sigma \circ \tau)(i) = \sigma(-i) = -\sigma(i) = -i$ und somit $\sigma \circ \tau \neq \mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}, \sigma$ (wegen $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}(i) = \sigma(i) = i$), andererseits aber auch $(\sigma \circ \tau)(\sqrt{3}) = \sigma(\sqrt{3}) = -\sqrt{3}$ und somit $\sigma \circ \tau \neq \tau$ (wegen $\tau(\sqrt{3}) = \sqrt{3}$). Wegen $|G| = 4$ ist damit insgesamt $G = \{\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}, \sigma, \tau, \sigma \circ \tau\}$ nachgewiesen.

zu (c) Sei $q \in \mathbb{Q} \setminus \{0\}$ und $a = \sqrt{3} + iq$. Nach Teil (b) sind $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}$, σ, τ und $\sigma \circ \tau$ die Elemente von $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q})$, und es gilt $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}(a) = \sqrt{3} + iq$, $\sigma(a) = -\sqrt{3} + iq$, $\tau(a) = \sqrt{3} - iq$ und $(\sigma \circ \tau)(a) = \sigma(\sqrt{3} - iq) = -\sqrt{3} - iq$. Je zwei dieser komplexen Zahlen unterscheiden sich im Real- oder Imaginärteil. Die vier Bilder von a unter den Elementen der Galois-Gruppe sind also paarweise verschieden. Nach Teil (a) folgt daraus, dass a ein primitives Element der Erweiterung $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ ist.

Aufgabe H22T1A4

Betrachten Sie das Polynom $f = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$. Es sei $Z \subseteq \mathbb{C}$ sein Zerfällungskörper in $\mathbb{C}$ und $\alpha \in Z$ eine Nullstelle.

(a) Dividieren Sie das Polynom f durch $x^2 - \alpha^2 \in \mathbb{Q}(\alpha)[x]$, ohne die Nullstelle exiplizit zu berechnen.

(b) Zeigen Sie, dass die Gleichung $(\alpha^3 + 3\alpha)^2 = -(5 + \alpha^2)$ gilt.

(c) Zeigen Sie, dass $[Z : \mathbb{Q}] = 4$ und $\mathrm{Gal}(Z|\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ gilt.

Lösung:
zu (a) Entsprechend der Vorgehensweise bei der Polynomdivision berechnen wir zunächst die Differenz $f - x^2(x^2 - \alpha^2) = f - x^4 + \alpha^2 x^2 = (5 + \alpha^2)x^2 + 5$ und subtrahieren anschließend $(5 + \alpha^2)(x^2 - \alpha^2)$. Wir erhalten

$$\begin{aligned}(5 + \alpha^2)x^2 + 5 - (5 + \alpha^2)(x^2 - \alpha^2) &= 5x^2 + \alpha^2 x^2 + 5 - 5x^2 - \alpha^2 x^2 + 5\alpha^2 + \alpha^4 = \\ 5 + 5\alpha^2 + \alpha^4 &= f(\alpha) = 0.\end{aligned}$$

Insgesamt gilt also

$$f - x^2(x^2 - \alpha^2) - (5 + \alpha^2)(x^2 - \alpha^2) = 0$$

was zu $f = (x^2 + \alpha^2 + 5)(x^2 - \alpha^2)$ umgeformt werden kann.

zu (b) Das Polynom $f \in \mathbb{Z}[x]$ ist auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 5) irreduzibel über $\mathbb{Z}$ und damit auch über $\mathbb{Q}$. Außerdem ist es normiert, und es gilt $f(\alpha) = 0$. Insgesamt handelt es sich also um das Minimalpolynom von α über $\mathbb{Q}$. Laut Vorlesung folgt daraus, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 4$ und $\mathcal{B} = \{1, \alpha, \alpha^2, \alpha^3\}$ eine Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum ist. Die Elemente $(\alpha^3 + 3\alpha)^2$ und $-(5 + \alpha)^2$ stimmen also genau dann überein, wenn ihre Darstellung als Linearkombination von $\mathcal{B}$ übereinstimmt.

Nun gilt einerseits $-(5 + \alpha^2) = (-5) + (-1)\alpha^2$. Um auch $(\alpha^3 + 3\alpha)^2$ als Linearkombination von $\mathcal{B}$ darzustellen, formen wir die Gleichung $\alpha^4 + 5\alpha^2 + 5 = f(\alpha) = 0$ zunächst zu $\alpha^4 = -5 - 5\alpha^2$ um. Wir erhalten dann $\alpha^6 = \alpha^2 \cdot \alpha^4 = \alpha^2(-5 - \alpha^2) = -5\alpha^2 - 5\alpha^4 = -5\alpha^2 + 25 + 25\alpha^2 = 20\alpha^2 + 25$. Es folgt

$$(\alpha^3 + 3\alpha)^2 = \alpha^6 + 6\alpha^4 + 9\alpha^2 = 20\alpha^2 + 25 - 30\alpha^2 - 30 + 9\alpha^2 = (-5) + (-1)\alpha^2.$$

Also stimmen die Elemente tatsächlich überein.

zu (c) Bereits in Teil (b) wurde nachgewiesen, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ ist. Nun zeigen wir noch, dass $\mathbb{Q}(\alpha)$ mit dem Zerfällungskörper Z von f über $\mathbb{Q}$ übereinstimmt und erhalten somit die gewünschte Gleichung $[Z : \mathbb{Q}] = 4$. Nach Definition gilt $Z = \mathbb{Q}(N)$, wobei N die Menge der komplexen Nullstellen von f bezeichnet. Zu zeigen ist also $\mathbb{Q}(\alpha) = \mathbb{Q}(N)$. Wegen $f(\alpha) = 0$ gilt $\alpha \in N$ und somit $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(N)$. Für die umgekehrte Inklusion genügt es, $N \subseteq \mathbb{Q}(\alpha)$ zu Überprüfen. Die Zerlegung

$$f = (x^2 + \alpha^2 + 5)(x^2 - \alpha^2)$$

aus Teil (a) zeigt, dass $\pm\alpha$ in N liegen.

Aus der Gleichung $(\alpha^3+3\alpha)^2 = -(5+\alpha^2)$ aus Teil (b) folgt, dass auch $\pm(3\alpha+\alpha^3)$ Nullstellen von f sind, denn es gilt

$$\begin{aligned} f(3\alpha+\alpha^3) &= ((3\alpha+\alpha^3)^2+\alpha^2+5)((3\alpha+\alpha^3)^2-\alpha^2) = \\ (-(5+\alpha^2)+\alpha^2+5)((3\alpha+\alpha^3)^2-\alpha^2) &= 0\cdot((3\alpha+\alpha^3)^2-\alpha^2) = 0 \quad , \end{aligned}$$

und ebenso erhält man $f(-3\alpha-\alpha^3)=0$. Die Elemente $\pm\alpha$ und $\pm(3\alpha+\alpha^3)$ sind paarweise verschieden, denn wie in Teil (b) gezeigt wurde, ist $\mathcal{B}=\{1,\alpha,\alpha^2,\alpha^3\}$ eine vierelementige Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum, und für beliebige $b_0,b_1,b_2,b_3\in\mathbb{Q}$ und $c_0,c_1,c_2,c_3\in\mathbb{Q}$ gilt somit

$$b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3 = c_0+c_1\alpha+c_2\alpha^2+c_3\alpha^3$$

dann und nur dann, wenn $b_j=c_j$ für $0\le j\le 3$ erfüllt ist. Da f als Polynom vom Grad 4 nicht mehr als vier komplexe Nullstellen besitzen kann, muss $N=\{\pm\alpha,\pm(3\alpha+\alpha^3)\}$ gelten. Dies zeigt, dass N tatsächlich in $\mathbb{Q}(\alpha)$ enthalten ist.

Als Zerfällungskörper des Polynoms $f\in\mathbb{Q}[x]$ über $\mathbb{Q}$ ist Z ein normaler Erweiterungskörper von $\mathbb{Q}$. Insbesondere ist die Erweiterung $Z|\mathbb{Q}$ algebraisch, und wegen $\mathrm{char}(\mathbb{Q})=0$ somit auch separabel. Insgesamt handelt es sich bei $Z|\mathbb{Q}$ um eine Galois-Erweiterung, und laut Vorlesung folgt daraus $|\mathrm{Gal}(f|\mathbb{Q})| = \mathrm{Gal}(Z|\mathbb{Q}) = [Z:\mathbb{Q}] = 4$. Für den Isomorphismus $\mathrm{Gal}(f|\mathbb{Q})\cong\mathbb{Z}/4\mathbb{Z}$ genügt es somit zu zeigen, dass in $\mathrm{Gal}(f|\mathbb{Q})$ ein Element der Ordnung 4 existiert. Weil f irreduzibel ist und α und $3\alpha+\alpha^3$ Nullstellen von f sind, existiert auf Grund des Fortsetzungssatzes ein Element $\sigma\in\mathrm{Gal}(f|\mathbb{Q})$ mit $\sigma(\alpha)=3\alpha+\alpha^3$. Wegen $|\mathrm{Gal}(f|\mathbb{Q})|=4$ ist nur $\mathrm{ord}(\sigma)\in\{1,2,4\}$ möglich. Um zu zeigen, dass $\mathrm{ord}(\sigma)=4$ gilt, genügt es somit $\sigma^2\neq\mathrm{id}_Z$ nachzuweisen, und hierfür wiederum ist $\sigma^2(\alpha)\neq\alpha$ hinreichend. Mit Hilfe der Gleichungen $\alpha^4=-5-5\alpha^2$, $\alpha^6=20\alpha^2+25$ und $(3\alpha+\alpha^3)^2=-5-\alpha^2$ aus Teil (b) erhalten wir

$$\begin{aligned} (3\alpha+\alpha^3)^3 &= (3\alpha+\alpha^3)^2(3\alpha+\alpha^3) = (-5-\alpha^2)(3\alpha+\alpha^3) = -15\alpha-3\alpha^3-5\alpha^3-\alpha^5 \\ &= -15\alpha-8\alpha^3-\alpha^4\alpha = -15\alpha-8\alpha^3+(5+5\alpha^2)\alpha \\ &= -15\alpha-8\alpha^3+5\alpha+5\alpha^3 = -10\alpha-3\alpha^3 \end{aligned}$$

und somit

$$\begin{aligned} \sigma^2(\alpha) &= \sigma(\sigma(\alpha)) = \sigma(3\alpha+\alpha^3) = 3\sigma(\alpha)+\sigma(\alpha)^3 = 3(3\alpha+\alpha^3)+(3\alpha+\alpha^3)^3 \\ &= 9\alpha+3\alpha^3-10\alpha-3\alpha^3 = -\alpha. \end{aligned}$$

Also gilt tatsächlich $\sigma^2(\alpha)\neq\alpha$.

Aufgabe H22T1A5

Sei $\Phi_n \in \mathbb{Q}[x]$ das n-te Kreisteilungspolynom über $\mathbb{Q}$. Zeigen Sie:

(a) Es gilt $x^n - 1 = (x-1)h$ mit einem Polynom $h \in \mathbb{Q}[x]$ mit $h(1) = n$.

(b) Ist $n = p^k$ für eine Primzahl p und $k \geq 1$, so gilt $\Phi_n(1) = p$.

(c) Hat n mindestens zwei Primzahlen $p \neq q$ als Teiler, so ist $\Phi_n(1) = 1$.

Lösung:
zu (a) Bekanntlich gilt $x^n - 1 = (x-1)h$ mit $h = \sum_{k=0}^{n-1} x^k$, und es ist $h(1) = \sum_{k=0}^{n-1} 1^k = \sum_{k=0}^{n-1} 1 = n$.

zu (b) Laut Vorlesung ist das Kreisteilungspolynom zu einer Primzahlpotenz p^k (mit $k \geq 1$) gegeben durch $\Phi_{p^k} = \sum_{j=0}^{p-1} x^{jp^{k-1}}$. Folglich gilt $\Phi_{p^k}(1) = \sum_{j=0}^{p-1} 1^{jp^{k-1}} = \sum_{j=0}^{p-1} 1 = p$.

zu (c) Wir beweisen die folgenden beiden Aussagen.

(i) Ist $n \in \mathbb{N}$ und sind p, q zwei verschiedene Primteiler von n, dann gilt $\Phi_n(1) \mid n$, aber $p \nmid \Phi_n(1)$ und $q \nmid \Phi_n(1)$.

(ii) Es gilt $\Phi_n(1) > 0$ für alle $n \in \mathbb{N}$ mit $n \geq 2$.

Aus Teil (i) folgt, dass $\Phi_n(1)$ keine Primteiler hat, sobald n mindestens zwei verschiedene Primteiler besitzt, in diesem Fall also $\Phi_n(1) \in \{\pm 1\}$ gilt. Zusammen mit (ii) folgt dann $\Phi_n(1) = 1$, wie gewünscht.

zu (i) Aus der Vorlesung ist bekannt, dass $x^n - 1 = \prod_{d|n} \Phi_d$ gilt, wobei d die Teiler von n in $\mathbb{N}$ durchläuft. Nach Teil (a) existiert ein Polynom $h_n \in \mathbb{Z}[x]$ mit $x^n - 1 = (x-1)h_n$ und $h_n(1) = n$. Wir erhalten

$$(x-1)h_n \quad = \quad x^n - 1 \quad = \quad (x-1) \prod_{\substack{d \mid n \\ d \neq 1}} \Phi_d \quad ,$$

und die Anwendung der Kürzungsregel im Integritätsbereich $\mathbb{Q}[x]$ liefert $h_n = \prod_{d|n, d\neq 1} \Phi_d = \Phi_n \cdot \prod_{d|n, d\neq 1, n} \Phi_d$. Dies zeigt, dass $\Phi_n(1)$ ein Teiler von $h_n(1) = n$ ist. Seien nun $a, b \in \mathbb{N}$ so gewählt, dass $n = p^a q^b m$ gilt, mit einem zu p und q teilerfremden m, und setzen wir $S = \{d \in \mathbb{N} \mid d \mid n, d \nmid p^a, d \nmid q^b, d \neq n\}$. Dann können wir das Polynom h_n in der Form

$$h_n \quad = \quad \prod_{k=1}^{a} \Phi_{p^k} \cdot \prod_{\ell=1}^{b} \Phi_{q^\ell} \cdot \Phi_n \cdot r$$

mit $r = \prod_{d \in S} \Phi_d \in \mathbb{Z}[x]$ schreiben. Mit Hilfe der Ergebnisse von Teil (a) und (b) erhalten wir

$$p^a q^b m \quad = \quad n \quad = \quad h_n(1) \quad = \quad p^a \cdot q^b \cdot \Phi_n(1) \cdot r(1)$$

und somit $m = \Phi_n(1) \cdot r(1)$. Es folgt $\Phi_n(1) \mid m$. Wegen $\mathrm{ggT}(m, pq) = 1$ ergibt sich daraus wiederum $p \nmid \Phi_n(1)$ und $q \nmid \Phi_n(1)$.

zu (ii) Diese Aussage beweisen wir durch vollständige Induktion über n. Für $n = 2$ ist sie offenbar erfüllt, denn es gilt $\Phi_2 = x + 1$ und $\Phi_2(1) = 1 + 1 = 2 > 0$. Sei nun $n \in \mathbb{N}$ mit $n > 2$, und setzen wir die Aussage für natürliche Zahlen kleiner als n voraus. Wie oben gezeigt, gilt $h_n = \Phi_n \cdot \prod_{d|n, d\neq 1, n} \Phi_d$ und somit auch $h_n(1) = \Phi_n(1) \cdot \prod_{d|n, d\neq 1, n} \Phi_d(1)$. Es ist $h_n(1) = n > 0$, und nach Induktionsvoraussetzung gilt $\Phi_d(1) > 0$ für alle Teiler $d \in \mathbb{N}$ von n mit $d \neq 1, n$. Auf Grund der obigen Gleichung muss somit auch $\Phi_n(1) > 0$ gelten.

Aufgabe H22T2A1

Eine *affine Ebene* in $\mathbb{R}^3$ ist die Menge aller Punkte $(x, y, z) \in \mathbb{R}^3$, die eine Gleichung der Form $ax + by + cz + d = 0$ erfüllen mit fest vorgegebenen Zahlen $a, b, c, d \in \mathbb{R}$ und $(a, b, c) \neq (0, 0, 0)$.

(a) Für $j = 1, 2, 3, 4$ seien vier Punkte $P_j = (x_j, y_j, z_j) \in \mathbb{R}^3$ gegeben. Zeigen Sie, dass P_1, P_2, P_3, P_4 genau dann in einer affinen Ebene liegen, wenn gilt

$$\begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{vmatrix} = 0.$$

(b) Sei $C = \{(t, t^2, t^3) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}$, und sei $E \subseteq \mathbb{R}^3$ eine affine Ebene. Zeigen Sie, dass $C \cap E$ höchstens drei Elemente hat.

Lösung:
zu (a) Seien $a, b, c, d \in \mathbb{R}$ mit $(a, b, c) \neq (0, 0, 0)$. Es liegen P_1, P_2, P_3, P_4 genau dann auf der Ebene

$$E_{a,b,c,d} = \{(x, y, z) \in \mathbb{R}^3 \mid ax + by + cz + d = 0\} ,$$

wenn $ax_j + by_j + cz_j + d = 0$ für $j = 1, 2, 3, 4$ gilt. Die Punkte liegen also genau dann auf einer affinen Ebene, wenn das linearen Gleichungssystem

$$x_j a + y_j b + z_j c + d = 0 \quad (1 \leq j \leq 4)$$

eine Lösung $(a, b, c, d) \in \mathbb{R}^4$ mit $(a, b, c) \neq (0, 0, 0)$ besitzt. Dies ist genau dann der Fall, wenn das lineare Gleichungssystem $Ax = 0_{\mathbb{R}^4}$ mit der Matrix

$$A = \begin{pmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{pmatrix}$$

eine Lösung dieser Form besitzt. Wir zeigen, dass dies genau dann der Fall ist, wenn $\det A = 0$ gilt.

„⇒“ Existiert eine Lösung der angegebenen Form, dann ist insbesondere $\ker A \neq \{0_{\mathbb{R}^4}\}$ und $\dim \ker A \geq 1$. Mit dem Dimensionssatz für lineare Abbildungen folgt daraus $4 - \operatorname{rg}(A) \geq 1$, was zu $\operatorname{rg}(A) < 4$ und $\det A = 0$ äquivalent ist. „⇐“ Aus $\det A = 0$ folgt $\operatorname{rg}(A) < 4$, was auf Grund der Dimensionssatzes zu $\dim \ker A \geq 1$ und $\ker A \neq \{0_{\mathbb{R}^4}\}$ äquivalent ist. Sei $(a, b, c, d) \in \mathbb{R}^4$ ein Element des Kerns ungleich null. Wäre $(a, b, c) = (0, 0, 0)$, dann würde wegen

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ d \end{pmatrix} = \begin{pmatrix} d \\ d \\ d \\ d \end{pmatrix}$$

auch $d = 0$ und somit $(a, b, c, d) = (0, 0, 0, 0)$ folgen, im Widerspruch zur Voraussetzung. Also ist (a, b, c, d) eine Lösung des LGS mit $(a, b, c) \neq (0, 0, 0)$.

zu (b) Sei $p \in \mathbb{R}^3$ und $E = E_{a,b,c}$ eine affine Ebene. Dann gilt die Äquivalenz

$$\begin{aligned} p \in E \cap C \quad &\Leftrightarrow \quad p \in E \text{ und } p \in C \quad \Leftrightarrow \quad p \in E \text{ und } \exists\, t \in \mathbb{R} : p = (t, t^2, t^3) \\ &\Leftrightarrow \quad \exists\, t \in \mathbb{R} : p = (t, t^2, t^3) \text{ und } at + bt^2 + ct^3 + d = 0. \end{aligned}$$

Also gilt $p \in E \cap C$ genau dann, wenn ein $t \in \mathbb{R}$ mit $p = (t, t^2, t^3)$ existiert, das Nullstelle des Polynoms $f_{a,b,c} = cx^3 + bx^2 + ax + d \in \mathbb{R}[x]$ ist. Wegen $(a, b, c) \neq (0, 0, 0)$ ist $f_{a,b,c}$ nicht das Nullpolynom. Da es als Polynom ungleich null vom Grad ≤ 3 höchstens drei Nullstellen besitzt (und jeder Schnittpunkt $p \in \mathbb{R}^3$ durch die zugehörige Nullstelle $t \in \mathbb{R}$ eindeutig festgelegt ist) gibt es höchstens drei Schnittpunkte von E und C.

Aufgabe H22T2A2

Sei K ein Körper, sei $K[x]$ der Polynomring über K in einer Unbestimmten, und sei $L = K(x)$ der Quotientenkörper von $K[x]$. Sei weiter

$$R \quad = \quad \left\{ \frac{a}{b} \;\middle|\; a, b \in K[x] \ , \ \mathrm{ggT}(a,b) = 1 \ , \ b(0) \neq 0 \right\} \quad \subseteq \quad L.$$

Zeigen Sie:

(a) Die Menge R ist ein Teilring von L.

(b) Sei I ein Ideal von R. Dann ist $I \cap K[x]$ ein Ideal von $K[x]$.

(c) Der Ring R ist ein Hauptidealring.

Lösung:
zu (a) Zu überprüfen ist, dass $1_{K(x)} \in R$ gilt, und dass mit $u, v \in R$ auch $u - v$ und uv in R liegen. Da K ein Teilring von $K[x]$ und $K[x]$ ein Teilring von $K(x)$ ist, ist K ein Teilring von $K(x)$. Sei $a = b = 1_K$. Dann gilt $a, b \in K[x]$ und $b(0_K) = 1_K \neq 0_K$, außerdem $\mathrm{ggT}(a,b) = \mathrm{ggT}(1_K, 1_K) = 1_K$. Insgesamt erhalten wir $1_{K(x)} = 1_K = \frac{1_K}{1_K} \in R$.

Seien $u, v \in R$. Dann gibt es $a_1, a_2, b_1, b_2 \in K[x]$ mit $u = \frac{a_1}{b_1}$, $v = \frac{a_2}{b_2}$ und $b_1(0_K) \neq 0_K$, $b_2(0_K) \neq 0_K$. Es folgt

$$uv \quad = \quad \frac{a_1 a_2}{b_1 b_2} \quad \text{mit} \quad a_1 a_2, b_1 b_2 \in K[x] \quad \text{und} \quad (b_1 b_2)(0_K) = b_1(0_K) b_2(0_K) \neq 0 \quad ,$$

da $b_1(0_K), b_2(0_K) \neq 0_K$ und K ein Körper ist. Sei nun $d \in R$ ein größter gemeinsamer Teiler von $a_1 a_2$ und $b_1 b_2$. Dann gibt es teilerfremde $a_3, b_3 \in K[x]$ mit $a_1 a_2 = d a_3$ und $b_1 b_2 = d b_3$. Es folgt

$$uv \quad = \quad \frac{a_1 a_2}{b_1 b_2} \quad = \quad \frac{d a_3}{d b_3} \quad = \quad \frac{a_3}{b_3}$$

und außerdem $b_3(0_K) \neq 0$, da ansonsten $(b_1 b_2)(0_K) = d(0_K) b_3(0_K)$ gleich 0_K wäre. Insgesamt ist damit $uv \in R$ nachgewiesen. Ebenso gilt

$$u - v \quad = \quad \frac{a_1}{b_1} - \frac{a_2}{b_2} \quad = \quad \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}$$

mit $a_1 b_2 - a_2 b_1 \in K[x]$, $b_1 b_2 \in K[x]$ und $(b_1 b_2)(0_K) \neq 0_K$. Sei $d' \in R$ ein größter gemeinsamer Teiler von $a_1 b_2 - a2 b_1$ und $b_1 b_2$. Dann gibt es teilerfremde $a_4, b_4 \in K[x]$ mit $a_1 b_2 - a2 b_1 = d' a_4$ und $b_1 b_2 = d' b_4$. Es folgt

$$u - v \quad = \quad \frac{a_1 b_2 - a_2 b_1}{b_1 b_2} \quad = \quad \frac{d' a_4}{d' b_4} \quad = \quad \frac{a_4}{b_4}.$$

Dabei ist $b_4(0_K) \neq 0$, da ansonsten $(b_1 b_2)(0_K) = d'(0_K) b_4(0_K)$ gleich 0_K wäre. Insgesamt zeigt dies, dass auch $u - v$ in R liegt.

zu (b) Sei I ein Ideal in R. Zu zeigen ist, dass $I \cap K[x]$ ein Ideal in $K[x]$ ist. Wir betrachten dazu die Abbildung $\phi : K[x] \to K(x)$, $f \mapsto \frac{f}{1_K}$. Für jedes $f \in K[x]$ gilt $\mathrm{ggT}(f, 1_K) = 1_K$ und $1_K(0_K) = 1_K \neq 0_K$, also $f = \frac{f}{1} \in R$. Dies zeigt, dass ϕ als Abbildung $K[x] \to R$ aufgefasst werden kann. Diese Abbildung ist ein Ringhomomorphismus, denn es gilt $\phi(1_{K[x]}) = \phi(1_K) = \frac{1_K}{1_K} = 1_R$ und für alle $f, g \in K[x]$ außerdem

$$\phi(f+g) \quad = \quad \frac{f+g}{1_K} \quad = \quad \frac{f}{1_K} + \frac{g}{1_K} \quad = \quad \phi(f) + \phi(g)$$

und

$$\phi(fg) \quad = \quad \frac{fg}{1_K} \quad = \quad \frac{f}{1_K} \cdot \frac{g}{1_K} \quad = \quad \phi(f)\phi(g).$$

Es ist $I \cap K[x] = \phi^{-1}(I)$, denn für alle $f \in K[x]$ gilt die Äquivalenz

$$f \in \phi^{-1}(I) \quad = \quad \phi(f) \in I \quad = \quad \frac{f}{1_K} \in I \quad = \quad f \in I \quad = \quad f \in I \cap K[x].$$

Als Urbild eines Ideals in R unter einem Ringhomomorphismus $K[x] \to R$ ist $I \cap K[x]$ ein Ideal in $K[x]$.

zu (c) Wir müssen überprüfen, dass R ein Integritätsbereich und jedes Ideal in R ein Hauptideal ist. Ersteres ist der Fall, weil R nach Teil (a) Teilring eines Körpers, nämlich $K(x)$, ist. Für den Nachweis der zweiten Aussage sei I ein Ideal in R. Nach Teil (b) ist $I \cap K[x]$ ein Ideal in $K[x]$. Da es sich bei $K[x]$ (als Polynomring über einem Körper) um einen Hauptidealring handelt, existiert ein $f \in K[x]$ mit $I \cap K[x] = fK[x]$. (Wir verwenden die Notation $fK[x]$ an Stelle der üblichen Schreibweise (f) für das von f erzeugte Ideal, um deutlich zu machen, dass hier das Erzeugnis von f im Ring $K[x]$ gemeint ist.) Wir zeigen nun, dass auch I ein Hauptideal ist, indem wir die Gleichung

$$I \quad = \quad fR \qquad \text{überprüfen.}$$

„$\supseteq$“ Es gilt $f \in K[x] \cap I$, damit insbesondere $f \in I$. Weil I ein Ideal in R ist, folgt daraus $fR \subseteq I$. „$\subseteq$“ Sei $u \in I$ vorgegeben. Dann liegt u insbesondere in R, es gibt also $a, b \in K[x]$ mit $u = \frac{a}{b}$, $b(0_K) \neq 0_K$ und $\mathrm{ggT}(a, b) = 1_K$. Das Element $bu = a$ ist dann in $K[x] \cap I$ enthalten. Wegen $K[x] \cap I = fK[x]$ existiert ein $r \in K[x]$ mit $bu = a = rf$. Sei $d \in K[x]$ ein größter gemeinsamer Teiler von b und r. Dann gibt es teilerfremde Elemente $b_1, r_1 \in K[x]$ mit $b = db_1$ und $r = dr_1$, und es folgt $db_1u = dr_1f$. Weil $K[x]$ ein Integritätsbereich ist, dann die Kürzungsregel angewendet werden, und wir erhalten $b_1u = r_1f$. Es folgt $u = f\frac{r_1}{b_1}$, wegen $\frac{r_1}{b_1} \in R$ also $u \in fR$.

Aufgabe H22T2A3

(a) Es ist $337 = 2\cdot 3\cdot 5\cdot 11+7 = 13\cdot 17+2^2\cdot 29$. Erklären Sie, dass daraus folgt, dass 337 eine Primzahl ist.

(b) Sei p eine Primzahl und $n \geq 1$. Zeigen Sie, dass die Gleichung $x^n = \bar{1}$ in $\mathbb{F}_p$ genau $\mathrm{ggT}(n, p-1)$ verschiedene Lösungen besitzt.

(c) Ermitteln Sie alle positiven ganzen Zahlen n, für die die Gleichung $x^n = 1$ im Ring $\mathbb{Z}/2022\mathbb{Z}$ genau n Lösungen hat.

Lösung:

zu (a) Wäre 337 keine Primzahl, dann gäbe es einen Primteiler p von 337 mit $p \leq \sqrt{337}$. Wegen $\sqrt{337} < 19$ ist 17 die größte Primzahl $\leq \sqrt{337}$. Es genügt deshalb zu zeigen, dass 337 keinen Primteiler ≤ 17 besitzt, mit anderen Worten, die Zahlen 2, 3, 5, 7, 11, 13 und 17 müssen als Teiler von 337 ausgeschlossen werden. Wäre eine der Zahlen $2, 3, 5$ oder 11 ein Teiler von 337, dann müsste diese Zahl auf Grund der Gleichung $337 = 2\cdot 3\cdot 5\cdot 11+7$ auch ein Teiler von 7 sein, was aber unmöglich ist, da es sich um eine von 7 verschiedene Primzahl handelt. Ebenso zeigt die Gleichung, dass 7 kein Teiler von 337 ist. Denn andernfalls wäre 7 auch ein Teiler von $2\cdot 3\cdot 5\cdot 11$, was nicht der Fall ist, denn die einzigen Primteiler dieses Produkts sind 2, 3, 5 und 11. Wären 13 oder 17 Teiler von 337, dann müsste 13 oder 17 auf Grund der Gleichung $337 = 13\cdot 17+2^2\cdot 29$ auch Teiler von $2^2\cdot 29$ sein, was ebenfalls nicht erfüllt ist, denn die einzigen Primteiler dieser Zahl sind 2 und 29. Insgesamt wird 337 also von keiner Primzahl $p \leq 17$ geteilt.

zu (b) Wegen $\bar{0}^n = \bar{0} \neq \bar{1}$ ist jede Lösung von $x^n = \bar{1}$ in $\mathbb{F}_p$ auch in $\mathbb{F}_p^\times$ enthalten. Die Ordnung jedes Elements $\alpha \in \mathbb{F}_p^\times$ ist auf jeden Fall ein Teiler von $|\mathbb{F}_p^\times| = p-1$. Darüber hinaus gilt die Äquivalenz

$$\alpha^n = \bar{1} \quad\Leftrightarrow\quad \mathrm{ord}(\alpha) \mid n \quad\Leftrightarrow\quad \mathrm{ord}(\alpha) \mid n \wedge \mathrm{ord}(\alpha) \mid (p-1) \quad\Leftrightarrow\quad \mathrm{ord}(\alpha) \mid \mathrm{ggT}(n, p-1) = 1$$
$$\Leftrightarrow\quad \alpha^{\mathrm{ggT}(n,p-1)} = \bar{1}.$$

Allgemein gilt: Ist G eine zyklische Gruppe der Ordnung m, $g \in G$ ein erzeugendes Element und d ein Teiler von m, dann ist $\langle g^d\rangle$ die eindeutig bestimmte Untergruppe von G mit Ordnung $\frac{m}{d}$, und jedes Element h mit $h^{m/d} = e_G$ ist in dieser Untergruppe enthalten. Daraus folgt, dass es in G genau $\frac{m}{d}$ Elemente h gibt, die die Gleichung $h^{m/d} = e_G$ erfüllen. Wenden wir dies auf $G = \mathbb{F}_p^\times$, $m = p-1$ und $d = \frac{p-1}{\mathrm{ggT}(n,p-1)}$ an, so kommen wir zu dem Ergebnis, dass in $\mathbb{F}_p^\times$ genau $\mathrm{ggT}(n, p-1)$ Elemente α mit $\alpha^{\mathrm{ggT}(n,p-1)} = \bar{1}$ gibt, auf Grund der Äquivalenz also ebenso viele Elemente α mit $\alpha^n = \bar{1}$.

zu (c) Die Primfaktorzerlegung von 2022 ist gegeben durch $2\cdot 3\cdot 337$. Auf Grund des Chinesischen Restsatzes existiert also ein Isomorphismus

$$\phi : \mathbb{Z}/2022\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$$

von Ringen. Seien $a \in \mathbb{Z}/2022\mathbb{Z}$ und $(b, c, d) = \phi(a)$. Dann gilt für jedes $n \in \mathbb{N}$ auf Grund der Bijektivität von ϕ die Äquivalenz

$$a^n = \bar{1} \quad\Leftrightarrow\quad \phi(a^n) = \phi(\bar{1}) \quad\Leftrightarrow\quad \phi(a)^n = (\bar{1}, \bar{1}, \bar{1}) \quad\Leftrightarrow\quad (b^n, c^n, d^n) = (\bar{1}, \bar{1}, \bar{1})$$
$$\Leftrightarrow\quad b^n = \bar{1} \ \wedge\ c^n = \bar{1} \ \wedge\ d^n = \bar{1}.$$

Definieren wir für jedes $m \in \mathbb{N}$ die Menge $\mathcal{L}_m = \{a \in \mathbb{Z}/m\mathbb{Z} \mid a^n = \bar{1}\}$, dann ist durch ϕ also eine Bijektion zwischen $\mathcal{L}_{2022}$ und $\mathcal{L}_2 \times \mathcal{L}_3 \times \mathcal{L}_{337}$ gegeben. Nach Teil (b) gilt $|\mathcal{L}_p| = \mathrm{ggT}(n, p-1)$ für jede Primzahl p. Insgesamt erhalten wir also

$$\begin{aligned} |\mathcal{L}_{2022}| &= |\mathcal{L}_2 \times \mathcal{L}_3 \times \mathcal{L}_{337}| = |\mathcal{L}_2| \cdot |\mathcal{L}_3| \cdot |\mathcal{L}_{337}| = \mathrm{ggT}(n,1) \cdot \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336) \\ &= \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336). \end{aligned}$$

Gesucht werden also alle $n \in \mathbb{N}$ mit der Eigenschaft $n = \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336)$. Die Primfaktorzerlegung von 336 ist $2^4 \cdot 3 \cdot 7$. Weil $\mathrm{ggT}(n,2)$ ein Teiler von 2 und $\mathrm{ggT}(n,2)$ ein Teiler von 336 ist, kann $n = \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336)$ also nur dann erfüllt sein, wenn n ein Teiler von $2^5 \cdot 3 \cdot 7$ ist, also die Form $n = 2^a \cdot 3^b \cdot 7^c$ mit $0 \le a \le 5$ und $b, c \in \{0,1\}$ hat. Weiter gilt die Äquivalenz

$$\begin{aligned} \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336) = n &\quad\Leftrightarrow\quad 2^{\min\{a,1\}} \cdot 2^{\min\{a,4\}} \cdot 3^{\min\{b,1\}} \cdot 7^{\min\{c,1\}} = 2^a \cdot 3^b \cdot 7^c \\ &\Leftrightarrow\quad 2^{\min\{a,1\}+\min\{a,4\}} \cdot 3^{\min\{b,1\}} \cdot 7^{\min\{c,1\}} = 2^a \cdot 3^b \cdot 7^c \\ &\Leftrightarrow\quad \min\{a,1\} + \min\{a,4\} = a \ \wedge\ \min\{b,1\} = b \ \wedge\ c = \min\{c,1\} \\ &\overset{b,c\in\{0,1\}}{\Leftrightarrow}\quad \min\{a,1\} + \min\{a,4\} = a \quad\overset{a\in\{0,1,\ldots,5\}}{\Leftrightarrow}\quad a \in \{0,5\} \\ \Leftrightarrow\quad n \in \{2^a \cdot 3^b \cdot 7^c \mid a \in \{0,5\}, b, c \in \{0,1\}\} &\quad\Leftrightarrow\quad n \in \{1,3,7,21,32,96,224,672\}. \end{aligned}$$

Es gibt also genau acht natürliche Zahlen n mit der Eigenschaft, dass die Gleichung $x^n = \bar{1}$ genau n Lösungen in $\mathbb{Z}/2022\mathbb{Z}$ besitzt.

Aufgabe H22T2A4

Sei $f = x^6 + 3 \in \mathbb{Q}[x]$, sei $\alpha \in \mathbb{C}$ eine Nullstelle von f, und sei $K = \mathbb{Q}(\alpha) \subseteq \mathbb{C}$. Zeigen Sie:

(a) Das Polynom f ist über $\mathbb{Q}$ irreduzibel.

(b) Die Zahl $\zeta = \frac{1}{2}(1 + \alpha^3) \in K$ ist eine primitive sechste Einheitswurzel.

(c) Der Körper K ist eine Galois-Erweiterung von $\mathbb{Q}$.

(d) Die Galois-Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist nicht abelsch.

Lösung:
zu (a) Auf Grund des Eisenstein-Kriteriums, angewendet auf die Primzahl $p = 3$, ist f irreduzibel in $\mathbb{Z}[x]$, und auf Grund des Gauß'schen Lemmas auch in $\mathbb{Q}[x]$.

zu (b) Zu zeigen ist, dass es sich bei ζ um ein Element der Ordnung 6 in der multiplikativen Gruppe $\mathbb{C}^\times$ handelt. Dafür müssen wir überprüfen, dass $\zeta^2 \neq 1$, $\zeta^3 \neq 1$ und $\zeta^6 = 1$ gilt. Zunächst bemerken wir, dass wegen $f(\alpha) = 0$ die Gleichung $\alpha^6 = -3$ gilt. Da f normiert und über $\mathbb{Q}$ irreduzibel ist und $f(\alpha) = 0$ gilt, handelt es sich bei f um das Minimalpolynom von α über $\mathbb{Q}$. Laut Vorlesung folgt daraus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 6$, und $\{1, \alpha, ..., \alpha^5\}$ ist eine 6-elementige Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum. Dies bedeutet, dass zwei Elemente $\sum_{j=0}^5 b_j\alpha^j$ und $\sum_{j=0}^5 c_j\alpha^j$ mit $b_j, c_j \in \mathbb{Q}$ für $0 \leq j \leq 5$ genau dann übereinstimmen, wenn $b_j = c_j$ für $0 \leq j \leq 5$ gilt.

Die Rechnungen $\zeta^2 = \frac{1}{4}(1 + \alpha^3)^2 = \frac{1}{4}(1 + 2\alpha^3 + \alpha^6) = \frac{1}{4}(1 + 2\alpha^3 + (-3)) = -\frac{1}{2} + \frac{1}{2}\alpha^3$ und $\zeta^3 = \zeta \cdot \zeta^2 = \frac{1}{2}(1 + \alpha^3) \cdot \frac{1}{2}(-1 + \alpha^3) = \frac{1}{4}(-1 - \alpha^3 + \alpha^3 + \alpha^6) = \frac{1}{4}(-1 - 3) = -1$ zeigen also, dass ζ^2 und ζ^3 ungleich 1 sind. Andererseits gilt $\zeta^6 = (\zeta^3)^2 = (-1)^2 = 1$.

zu (c) Die Erweiterung $K|\mathbb{Q}$ ist algebraisch, weil das Element α als Nullstelle des Polynoms $0 \neq f \in \mathbb{Q}[x]$ algebraisch über $\mathbb{Q}$ ist und weil K der vom algebraischen Element α erzeugte Zwischenkörper der Erweiterung $\mathbb{C}|\mathbb{Q}$ ist. Wegen $\mathrm{char}(K|\mathbb{Q}) = 0$ ist diese algebraische Erweiterung auch separabel. Nun zeigen wir noch, dass $K|\mathbb{Q}$ normal ist, indem wir nachweisen, dass K in $\mathbb{C}$ mit dem Zerfällungskörper von f über $\mathbb{Q}$ übereinstimmt. Wegen $f(0) \neq 0$ ist $\alpha \neq 0$. Weil ζ nach Teil (b) eine primitive sechste Einheitswurzel ist, sind die Elemente ζ^j für $0 \leq j \leq 5$ paarweise verschieden, und wegen $\alpha \neq 0$ gilt dasselbe für die Elemente $\zeta^j\alpha$ mit $0 \leq j \leq 5$. Für diese j gilt jeweils $f(\zeta^j\alpha) = (\zeta^j\alpha)^6 + 3 = (\zeta^6)^j\alpha^6 + 3 = \alpha^6 + 3 = f(\alpha) = 0$, die Elemente sind also Nullstellen von f. Wegen $\mathrm{grad}(f) = 6$ kann es keine weiteren Nullstellen geben.

Dies zeigt, dass durch $N = \{\zeta^j\alpha \mid 0 \leq j \leq 5\}$ die Menge aller komplexen Nullstellen von f gegeben und $\mathbb{Q}(N)$ somit der Zerfällungskörper von f über $\mathbb{Q}$ ist. Wegen $\alpha \in N$ gilt $K = \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(N)$. Andererseits liegen die Elemente $\zeta^j\alpha$ für $0 \leq j \leq 5$ wegen $\zeta = \frac{1}{2}(1 + \alpha^3)$ alle in $K = \mathbb{Q}(\alpha)$. Aus $N \subseteq K$ folgt $\mathbb{Q}(N) \subseteq K$, insgesamt also $\mathbb{Q}(N) = K$.

zu (d) *1. Möglichkeit: Angabe einer nicht-normalen Teilerweiterung*
Wäre die Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ abelsch, dann wäre jede Untergruppe von $\mathrm{Gal}(K|\mathbb{Q})$ ein Normalteiler. Nach den Sätzen der Galoistheorie würde daraus folgen, dass jeder Zwischenkörper M von $K|\mathbb{Q}$ normal über $\mathbb{Q}$ ist.

Wir führen die Annahme zu einem Widerspruch, indem wir zeigen, dass es sich bei $M = \mathbb{Q}(\sqrt[3]{3})$ um einen Zwischenkörper von $K|\mathbb{Q}$ handelt, der nicht normal über $\mathbb{Q}$ ist. Wegen $\alpha^6 = -3$ gilt $(\alpha^2)^3 = -3$, das Element α^2 ist also eine Nullstelle des Polynoms $g = x^3 + 3 \in \mathbb{Q}[x]$. Weil ζ eine primitive sechste Einheitswurzel ist, ist ζ^2 eine primitive dritte Einheitswurzel. Die Elemente 1, ζ^2, ζ^4 sind somit paarweise

verschieden, und wegen $\alpha^2 \neq 0$ gilt dasselbe für die Elemente α^2, $\zeta^2\alpha^2$ und $\zeta^4\alpha^2$. Diese drei Elemente sind die komplexen Nullstellen des Polynoms g, denn es gilt $g(\zeta^{2j}\alpha^2) = (\zeta^{2j})^3(\alpha^2)^3 + 3 = (\zeta^6)^j\alpha^6 + 3 = 1^j \cdot (-3) + 3 = 0$ für $j = 0, 1, 2$. Da offenbar $-\sqrt[3]{3} \in \mathbb{R}$ eine Nullstelle von g ist, stimmt diese mit einem der drei Elemente α^2, $\zeta^2\alpha^2$ und $\zeta^4\alpha^2$ überein.

Es gilt also $\sqrt[3]{3} \in K$, und somit ist $M = \mathbb{Q}(\sqrt[3]{3})$ tatsächlich ein Zwischenkörper von $K|\mathbb{Q}$. Auf Grund des Eisenstein-Kriteriums (angwendet auf die Primzahl 3) und des Gauß'schen Lemmas ist das Polynom g irreduzibel über g, und es besitzt in M die Nullstelle $\sqrt[3]{3}$. Wäre $M|\mathbb{Q}$ eine normale Erweiterung, dann müsste g über M in Linearfaktoren zerfallen und somit auch die beiden anderen komplexen Nullstellen in M liegen. Aber dies ist nicht der Fall. Denn wegen $\sqrt[3]{3} \in \mathbb{R}$ ist M ein Teilkörper von $\mathbb{R}$. Die beiden von $\sqrt[3]{3}$ verschiedenen Nullstellen des Polynoms g sind aber $\zeta^2\sqrt[3]{3}$ und $\zeta^4\sqrt[3]{3}$, und diese sind nicht reell, weil die beiden primitiven dritten Einheitswurzeln, also die Elemente der Menge $\{\zeta^2, \zeta^4\} = \{-\frac{1}{2} \pm \sqrt{1}2\sqrt{-3}\}$, nicht in $\mathbb{R}$ liegen. Also ist $M|\mathbb{Q}$ keine normale Erweiterung.

2. Möglichkeit: direkter Nachweis der Nicht-Kommutativität
Nach Teil (a) ist f irreduzibel über $\mathbb{Q}$, und wie in Teil (c) festgestellt wurde, sind unter anderen $\pm\alpha$ und $\zeta^2\alpha$ Nullstellen von f in K. Auf Grund des Fortsetzungssatzes gibt es somit Elemente $\sigma, \tau \in \mathrm{Gal}(K|\mathbb{Q})$ mit $\sigma(\alpha) = -\alpha$ und $\tau(\alpha) = \zeta\alpha$. In Teil (b) hatten wir nachgerechnet, dass $\zeta^2 = -\frac{1}{2} + \frac{1}{2}\alpha^3$ und $\zeta^3 = -1$ gilt. Wegen $\zeta = \frac{1}{2}(1 + \alpha^3)$ erhalten wir damit

$$\sigma(\zeta) \quad = \quad \sigma(\tfrac{1}{2}(1+\alpha^3)) \quad = \quad \tfrac{1}{2}(1+\sigma(\alpha)^3) \quad = \quad \tfrac{1}{2}(1+(-\alpha)^3) \quad = \quad \tfrac{1}{2}(1-\alpha^3) \quad = \quad -\zeta^2$$

und ebenso

$$\tau(\zeta) \quad = \quad \tau(\tfrac{1}{2}(1+\alpha^3)) \quad = \quad \tfrac{1}{2}(1+\tau(\alpha)^3) \quad = \quad \tfrac{1}{2}(1+(\zeta\alpha)^3) \quad = \quad \tfrac{1}{2}(1-\alpha^3) \quad = \quad -\zeta^2.$$

Damit erhalten wir einerseits

$$(\sigma \circ \tau)(\alpha) \quad = \quad \sigma(\tau(\alpha)) \quad = \quad \sigma(\zeta\alpha) \quad = \quad \sigma(\zeta)\sigma(\alpha) \quad = \quad (-\zeta^2)(-\alpha) \quad = \quad \zeta^2\alpha$$

andererseits aber

$$(\tau \circ \sigma)(\alpha) \quad = \quad \tau(\sigma(\alpha)) \quad = \quad \tau(-\alpha) \quad = \quad -\tau(\alpha) \quad = \quad -\zeta\alpha \quad = \quad \zeta^4\alpha.$$

Weil ζ nach Teil (b) eine primitive sechste Einheitswurzel ist, gilt $\zeta^2 \neq \zeta^4$ und somit auch $(\sigma \circ \tau)(\alpha) \neq (\tau \circ \sigma)(\alpha)$ und $\sigma \circ \tau \neq \tau \circ \sigma$. Dies zeigt, dass die Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ tatsächlich nicht kommutativ ist.

Aufgabe H22T2A5

Sei G eine Gruppe der Ordnung 2022.

(a) Nennen Sie vier paarweise nicht isomorphe Beispiele von Gruppen der Ordnung 2022 und begründen Sie, dass die Gruppen paarweise nicht isomorph sind.

(b) Zeigen Sie, dass G auflösbar ist.

(c) Beweisen Sie, dass G einen Normalteiler vom Index 2 besitzt.

Lösung:
zu (a) Sei $G_1 = \mathbb{Z}/2022\mathbb{Z}$, $G_2 = D_{1011}$ (die Diedergruppe mit $2 \cdot 1011 = 2022$ Elementen), $G_3 = S_3 \times \mathbb{Z}/337\mathbb{Z}$ und $G_4 = \mathbb{Z}/3\mathbb{Z} \times D_{337}$. Weil S_3, D_{337} und D_{1011} nicht-abelsche Gruppen sind, gilt dasselbe für G_2, G_3 und G_4. Weil die Gruppe G_1 abelsch ist, ist sie zu keiner der drei anderen Gruppen isomorph. Die Gruppe D_{1011} besitzt genau 1011 Elemente der Ordnung 2. (Dies sind die Spiegelungen in der Symmetriegruppe des regelmäßigen 1011-Ecks. Es gibt keine Drehung von Ordnung 2, weil 1011 ungerade ist.)

Wir zeigen nun, dass G_3 genau drei und G_4 genau 337 Elemente der Ordnung 2 besitzt. Weil die Anzahlen der Elemente der Ordnung 2 in den drei Gruppen G_2, G_3, G_4 nicht übereinstimmen, sind auch diese paarweise nicht-isomorph. Für jedes Element $(\sigma, a) \in G_3$ (mit $\sigma \in S_3$ und $a \in \mathbb{Z}/337\mathbb{Z}$) gilt die Äquivalenz

$$\begin{aligned}\operatorname{ord}(\sigma,a) = 2 \quad &\Leftrightarrow \quad (\sigma,a)^2 = e_{G_3} \ \wedge \ (\sigma,a) \neq e_{G_3} \quad \Leftrightarrow \quad (\sigma^2, \bar{2}a) = (\mathrm{id}, \bar{0}) \ \wedge \ (\sigma,a) \neq (\mathrm{id},\bar{0}) \\ &\Leftrightarrow \quad (\sigma^2, a) = (\mathrm{id},\bar{0}) \ \wedge \ (\sigma,a) \neq (\mathrm{id},\bar{0}) \quad \Leftrightarrow \quad a = \bar{0} \ \wedge \ \sigma \in \{(1\ 2), (2\ 3), (1\ 3)\} \\ &\Leftrightarrow \quad (\sigma,a) \in \{((1\ 2),\bar{0}), ((2\ 3),\bar{0}), ((1\ 3),\bar{0})\}.\end{aligned}$$

Dabei wurde im dritten Schritt verwendet, dass $\bar{2}$ wegen $\mathrm{ggT}(2, 337) = 1$ in $\mathbb{Z}/337\mathbb{Z}$ invertierbar ist und somit $\bar{2}a = \bar{0}$ äquivalent zu $a = \bar{0}$ ist. Im vierten Schritt haben wir verwendet, dass die Elemente $\sigma \in S_3$ mit $\sigma^2 = \mathrm{id}$ und $\sigma \neq \mathrm{id}$ durch $(1\ 2), (2\ 3), (1\ 3)$ gegeben sind. Insgesamt zeigt die Rechnung, dass es in G_3 tatsächlich genau drei Elemente der Ordnung 2 gibt.

Für alle $(a, \sigma) \in G_4$ mit $a \in \mathbb{Z}/3\mathbb{Z}$ und $\sigma \in D_{337}$ gilt die Äquivalenz

$$\begin{aligned}&\operatorname{ord}(a,\sigma) = 2 \quad \Leftrightarrow \quad (a,\sigma)^2 = (\bar{0},\mathrm{id}) \ \wedge \ (a,\sigma) = (\bar{0},\mathrm{id}) \quad \Leftrightarrow \quad (\bar{2}a, \sigma^2) = (\bar{0},\mathrm{id}) \ \wedge \ (a,\sigma) = (\bar{0},\mathrm{id}) \\ &\Leftrightarrow \quad (a,\sigma^2) = (\bar{0},\mathrm{id}) \ \wedge \ (a,\sigma) = (\bar{0},\mathrm{id}) \quad \Leftrightarrow \quad a = \bar{0} \ \wedge \ \sigma^2 = \mathrm{id} \ \wedge \ \sigma \neq \mathrm{id} \quad \Leftrightarrow \quad a = \bar{0} \ \wedge \ \operatorname{ord}(\sigma) = 2.\end{aligned}$$

In D_{337} gibt es genau 337 Elemente der Ordnung 2. Also zeigt die Rechnung, dass es ebenso viele Elemente der Ordnung 2 in G_4 gibt.

zu (b) Sei G eine Gruppe der Ordnung $2022 = 2 \cdot 3 \cdot 337$. (Die Zahl 337 ist eine Primzahl.) Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Auf Grund des Dritten Sylowsatzes gilt $\nu_{337} \mid 2 \cdot 3$, also $\nu_{337} \in \{1, 2, 3, 6\}$. Außerdem gilt $\nu_{337} \equiv 1 \bmod 337$. Wegen $2, 3, 6 \not\equiv 1 \bmod 337$ folgt $\nu_{337} = 1$. Sei N die einzige 337-Sylowgruppe von G. Wegen $\nu_{337} = 1$ gilt $N \trianglelefteq G$. Laut Vorlesung ist G auflösbar, wenn N und G/N beide auflösbar sind. Die Gruppe N ist auf Grund der Primzahlordnung $|N| = 337$ zyklisch, damit auch abelsch und auflösbar. Es bleibt zu zeigen, dass G/N eine auflösbare Gruppe ist.

Auf Grund des Satzes von Lagrange gilt $|G/N| = (G : N) = \frac{|G|}{|N|} = \frac{2022}{337} = 6$. Sei $\bar{P}$ ein beliebige 3-Sylowgruppe von $\bar{G} = G/N$. Dann gilt $|\bar{P}| = 3$ und $(\bar{G} : \bar{P}) = \frac{6}{3} = 2$. Als Untergruppe vom Index 2 ist $\bar{P}$ ein Normalteiler von $\bar{G}$. Als Gruppen der Primzahlordnungen $|\bar{P}| = 3$ und $|\bar{G}/\bar{P}| = (\bar{G} : \bar{P}) = 2$ sind $\bar{P}$ und $\bar{G}/\bar{P}$ beide zyklisch und damit auch auflösbar. Dies zeigt, dass auch $\bar{G}$ eine auflösbare Gruppe ist.

zu (c) In Teil (b) wurde gezeigt, dass G einen Normalteiler N von Ordnung 337 besitzt. Sei $\pi_N : G \to G/N$ der kanonische Epimorphismus. Aus der Korrespondenzsatz für Gruppen folgt: Ist $\bar{U}$ eine Untergruppe von G/N vom Index $d \in \mathbb{N}$, dann ist $U = \pi_N^{-1}(\bar{U})$ eine Untergruppe vom Index d von G mit $U \supseteq N$. In Teil (b) haben wir auch gezeigt, dass in G/N eine Untergruppe $\bar{P}$ vom Index 2 existiert. Also ist $P = \pi_N^{-1}(\bar{P})$ eine Untergruppe vom Index 2 von G. Wegen $(G : P) = 2$ handelt es sich darüber hinaus um einen Normalteiler.

Aufgabe H22T3A1

Gegeben sei eine endliche Körpererweiterung $L|K$. Weiterhin sei $\mathrm{Tr}_{L|K} : L \to K$ die Abbildung, die jeden Element $a \in L$ die Spur der Multiplikation $m_a : L \to L$, $b \mapsto ab$ zuordnet. Dabei ist die *Spur* einer K-linearen Abbildung $\varphi : L \to L$ definiert als die Summe der Hauptdiagonalelemente einer Darstellungsmatrix.

(a) Zeigen Sie, dass $\mathrm{Tr}_{L|K}$ eine K-lineare Abbildung ist.

(b) Nun sei $\{a_1, ..., a_n\}$ eine K-Basis von L. Beweisen Sie, dass sich die *Diskriminante* $\Delta_{L|K}(a_1, ..., a_n) = \det(\mathrm{Tr}(\alpha_i\alpha_j)_{ij})$ um einen Faktor aus $(K^\times)^2$ ändert, wenn man die Basis wechselt.

(c) Seien $p, q \in \mathbb{Q}$ so gewählt, dass $f = x^2 + px + q$ ein irreduzibles Polynom ist. Finden Sie $\Delta_{L|K}(1, \alpha)$ für $K = \mathbb{Q}$ und $L = K[x]/(f)$, wobei α die Restklasse von x in L bezeichne.

Lösung:
zu (a) Sei $n = [L : K] = \dim_K L$ und $\mathcal{B} = (\alpha_1, ..., \alpha_n)$ eine geordnete Basis von L als K-Vektorraum. Für jedes $\phi \in \mathrm{End}_K(L)$ sei $\mathcal{M}_\mathcal{B}(\phi)$ die Darstellungsmatrix von ϕ bezüglich $\mathcal{B}$. Für jede Matrix $A = (a_{ij}) \in \mathcal{M}_{n,K}$ sei $\mathrm{Tr}(A) = \sum_{i=1}^n a_{ii}$ die Spur. Nach Definition gilt $\mathrm{Tr}_{L|K}(a) = \mathrm{Tr}(\mathcal{M}_\mathcal{M}(m_a))$ für alle $a \in L$. Für den Nachweis, dass $\mathrm{Tr}_{L|K} : L \to K$ eine lineare Abbildung ist, genügt es zu überprüfen

(1) Die Abbildung $L \to \mathrm{End}_K(L)$, $a \mapsto m_a$ ist linear.

(2) Die Abbildung $\mathrm{End}_K(L) \to \mathcal{M}_{n,K}$, $\phi \mapsto \mathcal{M}_\mathcal{B}(\phi)$ ist linear.

(3) Die Abbildung $\mathrm{Tr} : \mathcal{M}_{n,K} \to K$, $A \mapsto \mathrm{Tr}(A)$ ist linear.

zu (1) Seien $a, a' \in L$ und $\lambda \in K$ vorgegeben. Zu überprüfen sind die beiden Gleichungen $m_{a+a'} = m_a + m_{a'}$ und $m_{\lambda a} = \lambda m_a$ in $\mathrm{End}_K(L)$. Sei dazu b ein beliebiges Element aus L. Es gilt

$$m_{a+a'}(b) \quad = \quad (a + a')b \quad = \quad ab + a'b \quad = \quad m_a(b) + m_{a'}(b) \quad = \quad (m_a + m_{a'})(b)$$

und ebenso $m_{\lambda a}(b) = (\lambda a)b = \lambda(ab) = \lambda m_a(b) = (\lambda m_a)(b)$. Damit sind die beiden Gleichungen in $\mathrm{End}_K(L)$ verifziert.

zu (2) Laut Vorlesung gilt: Sind V, W zwei K-Vektorräume der endlichen Dimensionen $n = \dim V$ und $m = \dim W$, ist $\mathcal{A}$ eine geordnete Basis von V und $\mathcal{B}$ eine geordnete Basis von W, dann ist durch $\mathrm{Hom}_K(V, W) \to \mathcal{M}_{m\times n,K}$, $\phi \mapsto \mathcal{M}_\mathcal{B}^\mathcal{A}(\phi)$ ein Isomorphismus von K-Vektorräumen definiert, insbesondere eine linearen Abbildung. Anwendung dieser Aussage auf $V = W = L$ und die Basis $\mathcal{B}$ liefert die angegebene Behauptung.

zu (3) Seien $A = (a_{ij})$ und $B = (b_{ij})$ Elemente des K-Vektorraums $\mathcal{M}_{n,K}$, und sei $\lambda \in K$. Dann gilt

$$\mathrm{Tr}(A + B) \quad = \quad \sum_{i=1}^n (a_{ii} + b_{ii}) \quad = \quad \sum_{i=1}^n a_{ii} + \sum_{i=1}^n b_{ii} \quad = \quad \mathrm{Tr}(A) + \mathrm{Tr}(B)$$

und ebenso $\mathrm{Tr}(\lambda A) = \sum_{i=1}^n (\lambda a_{ii}) = \lambda \sum_{i=1}^n a_{ii} = \lambda \mathrm{Tr}(A)$.

zu (b) Diese Aussage beweisen wir durch Anwendung des Satzes vom Basiswechsel für Bilinearformen. Zunächst überprüfen wir, dass durch $b : L \times L \to K$, $(\alpha, \beta) \mapsto \mathrm{Tr}_{L|K}(\alpha\beta)$ eine Bilinearform auf L definiert ist. Seien $\alpha, \alpha', \beta, \beta' \in L$ und $\lambda \in K$ vorgegeben. Dann gilt

$$\begin{aligned}
b(\alpha+\alpha',\beta) &= \mathrm{Tr}_{L|K}((\alpha+\alpha')\beta) = \mathrm{Tr}_{L|K}(\alpha\beta+\alpha'\beta) = \mathrm{Tr}_{L|K}(\alpha\beta)+\mathrm{Tr}_{L|K}(\alpha'\beta) = b(\alpha,\beta)+b(\alpha',\beta)\\
b(\alpha,\beta+\beta') &= \mathrm{Tr}_{L|K}(\alpha(\beta+\beta')) = \mathrm{Tr}_{L|K}(\alpha\beta+\alpha\beta') = \mathrm{Tr}_{L|K}(\alpha\beta')+\mathrm{Tr}_{L|K}(\alpha\beta') = b(\alpha,\beta)+b(\alpha,\beta')\\
b(\lambda\alpha,\beta) &= \mathrm{Tr}_{L|K}(\lambda\alpha\beta) = \lambda\mathrm{Tr}_{L|K}(\alpha\beta) = \lambda b(\alpha,\beta)\\
b(\alpha,\lambda\beta) &= \mathrm{Tr}_{L|K}(\lambda\alpha\beta) = \lambda\mathrm{Tr}_{L|K}(\alpha\beta) = \lambda b(\alpha,\beta).
\end{aligned}$$

Also ist durch b tatsächlich eine Bilinearform auf dem K-Vektorraum L definiert. Seien $\mathcal{A} = (\alpha_1, ..., \alpha_n)$ und $\mathcal{A}' = (\alpha'_1, ..., \alpha'_n)$ zwei geordnete Basen von L. Dann sind die Darstellungsmatrizen von b bezüglich $\mathcal{A}$ und $\mathcal{A}'$ gegeben durch

$$\mathcal{M}_{\mathcal{A}}(b) = (\mathrm{Tr}_{L|K}(\alpha_i\alpha_j))_{ij} \qquad \text{und} \qquad \mathcal{M}_{\mathcal{A}'}(b) = (\mathrm{Tr}_{L|K}(\alpha'_i\alpha'_j))_{ij}.$$

Nach dem Satz vom Basiswechsel für Bilinearformen gilt

$$\mathcal{M}_{\mathcal{A}'}(b) = {}^{\mathrm{t}}\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'} \cdot \mathcal{M}_{\mathcal{A}}(b) \cdot \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$$

wobei $\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$ die Matrix des Basiswechsels von $\mathcal{A}'$ nach $\mathcal{A}$ bezeichnet. Sei $c = \det \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'} \in K$. Weil die Matrix $\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$ invertierbar ist, liegt $c \in K^\times$. Die zu beweisende Aussage aus der Aufgabenstellung ergibt sich nun durch die Rechnung

$$\begin{aligned}
\Delta_{L|K}(\mathcal{A}') &= \det\left(\mathrm{Tr}_{L|K}(\alpha'_i\alpha'_j)\right) = \det \mathcal{M}_{\mathcal{A}'}(b) = \det\left({}^{\mathrm{t}}\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}\mathcal{M}_{\mathcal{A}'}(b)\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}\right)\\
&= (\det \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'})^2 \cdot \det \mathcal{M}_{\mathcal{A}}(b) = c^2 \det\left(\mathrm{Tr}_{L|K}(\alpha_i\alpha_j)\right) = c^2\Delta_{L|K}(\mathcal{A}).
\end{aligned}$$

zu (c) Wir berechnen die Darstellungsmatrizen A_β von m_β bezüglich der Basis $\mathcal{B} = (1, \alpha)$ des K-Vektorraums L, für $\beta \in \{1, \alpha, \alpha^2\}$. Zur Vorbereitung berechnen wir

$$\begin{aligned}
\alpha^2 &= (x+(f))^2 = x^2+(f) = x^2 - f + (f) = x^2 - (x^2+px+q) + (f)\\
&= -px - q + (f) = (-p+(f))(x+(f)) - (q+(f)) = -p\alpha - q\\
\alpha^3 &= \alpha\cdot\alpha^2 = \alpha(-p\alpha - q) = -p\alpha^2 - q\alpha = -p(-p\alpha-q) - q\alpha = (p^2-q)\alpha + pq
\end{aligned}$$

Nun gilt $m_1(1) = 1 \cdot 1 = 1 \cdot 1 + 0 \cdot \alpha$, $m_1(\alpha) = \alpha = 0 \cdot 1 + 1 \cdot \alpha$. Dies liefert die Darstellungsmatrix

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und $\mathrm{Tr}_{L|\mathbb{Q}}(1) = \mathrm{Tr}(A_1) = 1 + 1 = 2$. Die Gleichungen $m_\alpha(1) = \alpha = 0 \cdot 1 + 1 \cdot \alpha$ und $m_\alpha(\alpha) = \alpha^2 = (-q) \cdot 1 + (-p) \cdot \alpha$ liefern die Darstellungsmatrix

$$A_\alpha = \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

und $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha) = \mathrm{Tr}(A_\alpha) = 0 + (-p) = -p$. Die Gleichungen $m_{\alpha^2}(1) = \alpha^2 = (-q) \cdot 1 + (-p) \cdot \alpha$ und $m_{\alpha^2}(\alpha) = \alpha^3 = (pq) \cdot 1 + (p^2 - q) \cdot \alpha$ liefern schließlich die Darstellungsmatrix

$$A_{\alpha^2} = \begin{pmatrix} -q & pq \\ -p & p^2-q \end{pmatrix}$$

und $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha^2) = \mathrm{Tr}(A_{\alpha^2}) = (-q) + (p^2 - q) = p^2 - 2q$.

Für die Diskriminante erhalten wir nun

$$\begin{aligned}\Delta_{L|\mathbb{Q}}(1,\alpha) &= \det\begin{pmatrix}\mathrm{Tr}_{L|\mathbb{Q}}(1) & \mathrm{Tr}_{L|\mathbb{Q}}(\alpha)\\ \mathrm{Tr}_{L|\mathbb{Q}}(\alpha) & \mathrm{Tr}_{L|\mathbb{Q}}(\alpha^2)\end{pmatrix} = \det\begin{pmatrix}2 & -p\\ -p & p^2-2q\end{pmatrix}\\ &= 2(p^2-2q)-(-p)^2 = p^2-4q.\end{aligned}$$

Aufgabe H22T3A2

(a) Geben Sie eine vollständige Definition des kleinsten gemeinsamen Vielfachen zweier ganzer Zahlen an.

(b) Beweisen Sie mit Hilfe Ihrer Definition aus (a), dass für $a, b, c, d \in \mathbb{Z}$ die folgende Formel gilt:

$$\mathrm{kgV}(\mathrm{kgV}(a,b), \mathrm{kgV}(c,d)) \ , \ \mathrm{kgV}(\mathrm{kgV}(a,c), \mathrm{kgV}(b,d)).$$

Lösung:
zu (a) Seien $a, b \in \mathbb{Z}$. Dann ist $\mathrm{kgV}(a,b)$ die eindeutig bestimmte Zahl $d \in \mathbb{N}_0$ mit den folgenden beiden Eigenschaften.

(i) $a \mid d$ und $b \mid d$

(ii) Für alle $d' \in \mathbb{N}_0$ folgt aus $a \mid d'$ und $b \mid d'$ jeweils $d \mid d'$.

Damit ist die Zahl eindeutig bestimmt. Erfüllen nämlich d und d' aus $\mathbb{N}_0$ beide die Bedingungen (i) und (ii), dann gilt $d \mid d'$ und $d' \mid d$, und wegen $d, d' \in \mathbb{N}_0$ folgt daraus $d = d'$.

zu (b) Seien $a, b, c, d \in \mathbb{Z}$ vorgegeben, und sei $r = \mathrm{kgV}(\mathrm{kgV}(a,b), \mathrm{kgV}(c,d))$. Wir zeigen, dass r die definierenden Bedingungen (i) und (ii) des kgV von $\mathrm{kgV}(a,c)$ und $\mathrm{kgV}(b,d)$ erfüllt. Es gilt $\mathrm{kgV}(a,b) \mid r$ und $\mathrm{kgV}(c,d) \mid r$. Daraus wiederum folgt $a \mid r$, $b \mid r$, $c \mid r$ und $d \mid r$. Aus $a \mid r$ und $c \mid r$ folgt $\mathrm{kgV}(a,c) \mid r$, und aus $b \mid r$ und $d \mid r$ folgt ebenso $\mathrm{kgV}(b,d) \mid r$. Damit ist Bedingung (i) verifiziert.

Sei nun $s \in \mathbb{N}_0$ mit $\mathrm{kgV}(a,c) \mid s$ und $\mathrm{kgV}(b,d) \mid s$. Dann folgt $a \mid s$, $c \mid s$, $b \mid s$ und $d \mid s$. Aus $a \mid s$ und $b \mid s$ folgt $\mathrm{kgV}(a,b) \mid s$. Aus $c \mid s$ und $d \mid s$ folgt $\mathrm{kgV}(c,d) \mid s$. Aus $\mathrm{kgV}(a,b) \mid s$ und $\mathrm{kgV}(c,d) \mid s$ wiederum folgt $r \mid s$, auf Grund von Bedingung (ii) für das kleinste gemeinsame Vielfache von $\mathrm{kgV}(a,b)$ und $\mathrm{kgV}(c,d)$. Damit ist Bedingung (ii) für das kleinste gemeinsame Vielfache von $\mathrm{kgV}(a,c)$ und $\mathrm{kgV}(b,d)$ nachgewiesen.

Anmerkung:

Für $a, b \in \mathbb{Z}$ gilt $\mathrm{kgV}(a,b) = 0$ genau dann, wenn $a = 0$ oder $b = 0$ ist. Ist nämlich $a = 0$ und setzen wir und setzen wir $d = \mathrm{kgV}(a,b)$, so gilt $a \mid d$, also $d = ka$ für ein $k \in \mathbb{Z}$. Es folgt $d = k \cdot 0 = 0$. Ebenso folgt aus $b = 0$, dass $\mathrm{kgV}(a,b) = 0$ ist. Sind andererseits a und b beide ungleich null, dann ist $|ab| \in \mathbb{N}$ ein gemeinsames Vielfaches von a und b. Also muss $d = \mathrm{kgV}(a,b)$ ein Teiler von $|ab|$ sein. Dies ist nur möglich, wenn d ungleich null ist, denn 0 ist kein Teiler einer ganzen Zahl ungleich 0.

Weder in Teil (a) noch in Teil (b) ist es notwendig, die Situation, dass eine der Zahlen a, b, c, d gleich 0 ist, als Sonderfall zu betrachten.

Aufgabe H22T3A3

Seien p, q, r Primzahlen mit $p < q < r$, und sei G eine Gruppe der Ordnung pqr. Für $i \in \{p, q, r\}$ bezeichne ν_i die Anzahl der verschiedenen i-Sylowgruppen von G. Beweisen Sie:

(a) Besitzt G keine normale Sylowgruppe, so gilt $\nu_p \geq q$ und $\nu_q \geq r$ und $\nu_r = pq$.

(b) Die Gruppe G besitzt eine normale Sylowgruppe.

(c) Eine Gruppe der Ordnung 2022 ist nicht einfach.

Lösung:
zu (a) Nach dem Dritte Sylowsatz gilt $\nu_p \mid (qr)$, also $\nu_p \in \{1, q, r, qr\}$. Da G keine normale p-Sylowgruppe besitzt, ist $\nu_p = 1$ ausgeschlossen. Wegen $r > q$ und $qr > q$ folgt aus $\nu_p \in \{q, r, qr\}$ direkt $\nu_p \geq q$.

Ebenso gilt $\nu_q \mid (pr)$ auf Grund des Dritten Sylowsatzes, also $\nu_q \in \{1, p, r, pr\}$. Da es keine normale q-Sylowgruppe in G gibt, gilt $\nu_q \neq 1$. Nehmen wir an, es ist $\nu_q = p$. Wegen $\nu_q \equiv 1 \bmod q$ folgt dann $p \equiv 1 \bmod q$, also $q \mid (p-1)$ und insbesondere $q < p$. Aber dies steht zur Voraussetzung $q > p$ im Widerspruch. Also gilt $\nu_q \in \{r, pr\}$, und wegen $pr > r$ folgt $\nu_q \geq r$.

Eine erneute Anwendung des Dritten Sylowsatzes liefert $\nu_r \mid (pq)$, also $\nu_r \in \{1, p, q, pq\}$. Da G keine normale r-Sylowgruppe besitzt, gilt $\nu_r \neq 1$. Aus $\nu_r = p$ oder $\nu_r = q$ würde $p \equiv 1 \bmod r$ oder $q \equiv 1 \bmod r$ folgen, also auch $r|(p-1)$ oder $r|(q-1)$ bzw. $r < p$ oder $r < q$, im Widerspruch zu den Voraussetzungen $r > q > p$. Also ist $\nu_r = pq$ die einzige verbleibende Möglichkeit.

zu (b) Nehmen wir an, G besitzt keine normale Sylowgruppe. Nach Teil (a) gilt dann $\nu_p \geq q$, $\nu_q \geq r$ und $\nu_r = pq$. Wegen $|G| = p^1 \cdot q^1 \cdot r^1$ sind die p- bzw. q- bzw. r-Sylowgruppen genau die Untergruppen der Ordnung p bzw. q bzw. r von G. Jedes Element $g \in G$ der Ordnung r liegt genau in einer r-Sylowgruppe von G, nämlich $\langle g \rangle$. Umgekehrt ist jede r-Sylowgruppe als Untergruppe der Primzahlordnung r zyklisch und enthält somit genau $\varphi(r) = r - 1$ Elemente der Ordnung $r - 1$. Insgesamt zeigt dies, dass die Anzahl der Elemente der Ordnung r in G genau $(r-1)$-mal so groß ist wie die Anzahl ν_r der r-Sylowgruppen. Es gibt also genau $pq(r-1)$ Elemente der Ordnung r in G.

Genauso folgt aus $\nu_p \geq q$, dass es in G mindestens $(p-1)q$ Elemente der Ordnung p, und aus $\nu_q \geq r$, dass es in G mindestens $(q-1)r$ Elemente der Ordnung q gibt. Insgesamt enthält G also mindestens $pq(r-1) + (p-1)q + (q-1)r$ Elemente ungleich dem Neutralelement. Wegen $|G| = pqr$ folgt

$$pq(r-1) + (p-1)q + (q-1)r + 1 \leq pqr \quad \Leftrightarrow \quad -pq + (p-1)q + (q-1)r + 1 \leq 0 \quad \Leftrightarrow$$
$$-q + (q-1)r + 1 \leq 0 \quad \Leftrightarrow \quad qr + 1 \leq q + r \quad \Leftrightarrow \quad q(r-1) + 1 \leq r.$$

Wegen $q \geq 3$ folgt daraus $3(r-1) + 1 \leq r$, was zu $3r + 1 \leq r + 3$ und $r \leq 1$ umgeformt werden kann. Aber dies steht im Widerspruch dazu, dass r eine Primzahl ist. Dies zeigt, dass es in G eine normale Sylowgruppe geben muss.

zu (c) Sei G eine Gruppe der Ordnung $2022 = 2 \cdot 3 \cdot 337$. Die Zahl 337 ist eine Primzahl, also ist $|G| = pqr$ mit den Primzahlen $p = 2 < q = 3 < r = 337$ erfüllt. Nach Teil (b) besitzt G also eine normale p-, q- oder r-Sylowgruppe. Wegen $1 < p, q, r < |G|$ handelt es sich dabei um einen nichttrivialen Normalteiler von G. Dies zeigt, dass G keine einfache Gruppe ist.

Aufgabe H22T3A4

Sei $K = \mathbb{Z}[x]/(x^5+2, x^4+x^3+x^2+x+1)$.

(a) Beweisen Sie, dass $3 \in (x^5+2, x^4+x^3+x^2+x+1)$ gilt.

(b) Zeigen Sie, dass K ein Körper ist.

(c) Beweisen Sie, dass K eine Galois-Erweiterung seines Primkörpers $\mathbb{F}_3$ ist, und bestimmen Sie die Galoisgruppe von $K|\mathbb{F}_3$.

(d) Sei α die Restklasse von x in K. Zeigen Sie, dass $\{1, \alpha, \alpha^2, \alpha^3\}$ eine $\mathbb{F}_3$-Basis von K ist, und bestimmen Sie die Darstellungsmatrizen der Elemente der Galoisgruppe $\mathrm{Gal}(K|\mathbb{F}_3)$ bezüglich dieser Basis.

Lösung:
zu (a) Setzen wir $I = (f, g)$ mit $f = x^5+2$ und $g = x^4+x^3+x^2+x+1$, dann ist auch $(x-1)g = x^5-1$ in I enthalten, und damit auch $3 = (x^5+2) - (x^5-1) = f + (1-x)g$.

zu (b) Wir beweisen zunächst mit Hilfe des Homomorphiesatzes für Ringe, dass $K = \mathbb{Z}[x]/I$ isomorph zu $\mathbb{F}_3[x]/(\bar{f})$ ist, wobei $\bar{f}$ das Bild von f in $\mathbb{F}_3[x]$ bezeichnet. Auf Grund der universellen Eigenschaft gibt es einen eindeutig bestimmten Ringhomomorphismus $\pi_1 : \mathbb{Z}[x] \to \mathbb{F}_3[x]$, $h \mapsto \bar{h}$ der den kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{F}_3$ auf $\mathbb{Z}[x]$ fortsetzt und dabei $x \in \mathbb{Z}[x]$ auf $x \in \mathbb{F}_3[x]$ abbildet. Dabei entsteht das Polynom $\bar{h} \in \mathbb{F}_3[x]$ jeweils durch Anwendung des kanonischen Epimorphismus auf die Koeffizienten von h. Diese Abbildung ist surjektiv. Ist nämlich $\bar{h} = \sum_{i=0}^{m} \bar{a}_i x^i$ mit $m \in \mathbb{N}_0$ und $\bar{a}_0, ..., \bar{a}_m \in \mathbb{F}_3$ und ist $a_i \in \mathbb{Z}$ jeweils ein Urbild von $\bar{a}_i \in \mathbb{F}_3$ für $0 \le i \le m$, dann ist durch $h = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ offenbar ein Element mit $\pi_1(h) = \bar{h}$ gegeben.

Bezeichnen wir den kanonischen Epimorphismus $\mathbb{F}_3[x] \to \mathbb{F}_3[x]/(\bar{f})$ mit π_2, dann ist durch $\pi_2 \circ \pi_1$ ein Ringhomomorphismus $\mathbb{Z}[x] \to \mathbb{F}_3[x]/(\bar{f})$ gegeben. Als Komposition zweier surjektiver Abbildungen ist dieser ebenfalls surjektiv. Außerdem gilt $\ker(\pi_2 \circ \pi_1) = I$, denn für alle $h \in \mathbb{Z}[x]$ gilt die Äquivalenz

$$\begin{gathered}
h \in \ker(\pi_2 \circ \pi_1) \quad \Leftrightarrow \quad (\pi_2 \circ \pi_1)(h) = 0_{\mathbb{F}_3[x]/(\bar{g})} \quad \Leftrightarrow \quad \pi_2(\bar{h}) = \bar{0} + (\bar{g}) \quad \Leftrightarrow \quad \bar{h} + (\bar{g}) = \bar{0} + (\bar{g}) \\
\Leftrightarrow \quad \bar{h} \in (\bar{g}) \quad \Leftrightarrow \quad \exists\, \bar{u} \in \mathbb{F}_3[x] : \bar{h} = \bar{u} \cdot \bar{g} \quad \Leftrightarrow \quad \exists\, u \in \mathbb{Z}[x] : h \equiv ug \bmod (3) \\
\Leftrightarrow \quad \exists\, u, v \in \mathbb{Z}[x] : h = ug + 3v \quad \Leftrightarrow \quad \exists\, u, v \in \mathbb{Z}[x] : h = ug + v(f + (1-x)g) \\
\Leftrightarrow \quad \exists\, u, v \in \mathbb{Z}[x] : h = vf + (u + (1-x)v)g \quad \Leftrightarrow \quad \exists\, u', v' \in \mathbb{Z}[x] : h = u'f + v'g \\
\Leftrightarrow \quad h \in (f, g) \quad \Leftrightarrow \quad h \in I.
\end{gathered}$$

(Im drittletzten Schritt erhält man die Richtung „⇒“ mit $u' = v$, $v' = u + (1-x)v$, und die Richtung „⇐“ mit $v = u'$, $u = v' - (1-x)u'$.) Auf Grund des Homomorphiesatzes für Ringe existiert also ein Isomorphismus $\bar{\phi} : K \to \mathbb{F}_3[x]/(\bar{f})$, gegeben durch $\bar{\phi}(h + I) = \bar{h} + (\bar{f})$ für alle $h \in \mathbb{Z}[x]$. Auf Grund der Isomorphie genügt es zu zeigen, dass $\mathbb{F}_3[x]/(\bar{f})$ ein Körper ist. Als Polynomring über einem Körper ist $\mathbb{F}_3[x]$ ein Hauptidealring. In einem solchen Ring sind die von irreduziblen Elementen erzeugte Hauptideale maximale Ideale. Ist $\bar{f}$ also irreduzibel, dann ist $(\bar{f})$ ein maximales Ideal in $\mathbb{F}_3[x]$, und daraus wiederum folgt, dass $\mathbb{F}_3[x]/(\bar{f})$ ein Körper ist.

Für den Nachweis der Irreduzibilität stellen wir zunächst fest, dass $\bar{f} \in \mathbb{F}_3[x]$ im Körper $\mathbb{F}_3$ keine Nullstelle besitzt, denn es ist $f(\bar{0}) = \bar{1} \neq \bar{0}$, $f(\bar{1}) = \bar{5} = \bar{2} \neq \bar{0}$ und $f(\bar{2}) = \overline{16} + \bar{8} + \bar{4} + \bar{2} + \bar{1} = \overline{31} = \bar{1} \neq \bar{0}$. Wäre $\bar{f}$ dennoch reduzibel, dann müsste $\bar{f}$ Produkt zweier irreduzibler Polynome $\bar{g}, \bar{h} \in \mathbb{F}_3[x]$ vom Grad 2 sein. Man kann durch direktes Nachrechnen überprüfen, dass keine Zerlegung von f der Form

$$x^4 + x^3 + x^2 + x + \bar{1} \quad = \quad (x^2 + ax + b)(x^2 + cx + d)$$

mit $a, b, c, d \in \mathbb{F}_3$ existiert. Wir wählen hier aber einen anderen Weg: Sei α eine Nullstelle von $\bar{g}$ in einem algebraischen Abschluss $\mathbb{F}_3^{\text{alg}}$ von $\mathbb{F}_3$. Weil $\bar{g}$ das Minimalpolynom von α über $\mathbb{F}_3$ ist, gilt $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \text{grad}(\bar{g}) = 2$. Als zweidimensionaler $\mathbb{F}_3$-Vektorraum besteht $\mathbb{F}_3(\alpha)$ aus $3^2 = 9$ Elementen, stimmt also mit dem Zwischenkörper $\mathbb{F}_9$ von $\mathbb{F}_3^{\text{alg}}|\mathbb{F}_3$ überein. Wegen $\bar{f}(\bar{0}) \neq \bar{0}$ und $\bar{f} = \bar{g} \cdot \bar{h}$ gilt auch $\bar{g}(\bar{0}) \neq \bar{0}$. Daraus folgt $\alpha \in \mathbb{F}_9^\times$. Wegen $|\mathbb{F}_9^\times| = 9 - 1 = 8$ ist die Ordnung $\text{ord}(\alpha)$ von α in der multiplikativen Gruppe $\mathbb{F}_9^\times$ ein Teiler von 8. Andererseits ist α als Nullstelle von $\bar{f}$ auch eine Nullstelle von $x^5 - \bar{1} = (x - \bar{1})\bar{f}$. Es gilt also $\alpha^5 = \bar{1}$; wegen $\alpha \neq \bar{1}$ folgt daraus $\text{ord}(\alpha) = 5$. Weil aber 5 kein Teiler von 8 ist, hat unsere Annahme, das Polynom $\bar{f}$ sei reduzibel in $\mathbb{F}_3[x]$, zu einem Widerspruch geführt.

zu (c) Wie wir bereits in Teil (b) festgestellt haben, ist K isomorph zu $\mathbb{F}_3[x]/(\bar{f})$. Weil $\bar{f}$ ein irreduzibles Polynom vom Grad 4 ist, ist dieser Körper wiederum isomorph zu $\mathbb{F}_{81}$, dem eindeutig bestimmten Zwischenkörper von $\mathbb{F}_3^{\text{alg}}|\mathbb{F}_3$ mit $3^4 = 81$ Elementen. Für jedes $m \in \mathbb{N}$ gilt $[\mathbb{F}_{3^m} : \mathbb{F}_3] = m$, insbesondere also $[\mathbb{F}_{81} : \mathbb{F}_3] = 4$. Laut Vorlesung ist jede endliche Erweiterung $E|F$ bestehend aus endlichen Körpern E und F eine Galois-Erweiterung. Die Galoisgruppe $G = \text{Gal}(E|F)$ ist jeweils zyklisch von Ordnung $[E : F]$ und wird vom Frobenius-Automorphismus $\varphi_q : E \to E$, $\gamma \mapsto \gamma^q$ erzeugt, wobei $q = |F|$ ist. Insbesondere ist $\text{Gal}(K|\mathbb{F}_3) = \text{Gal}(\mathbb{F}_{81}|\mathbb{F}_3)$ also die vierelementige Gruppe $\langle \varphi_3 \rangle = \{\text{id}_K, \varphi_3, \varphi_3^2, \varphi_3^3\}$, mit $\varphi_3 : K \to K$, $\gamma \mapsto \gamma^3$.

zu (d) Die Darstellungmatrix der Abbildung id_V auf einem n-dimensionalen $\mathbb{F}_3$-Vektorraum V bezüglich einer beliebigen Basis ist immer die Einheitsmatrix $E_n \in \mathcal{M}_{n,\mathbb{F}_3}$. Somit ist E_4 die Darstellung von id_K. Für die Darstellungsmatrix von φ_3 bemerken wir zunächst, dass $\alpha = x + (\bar{f})$ laut Vorlesung eine Nullstelle von $\bar{f}$ ist und somit $\alpha^4 = -\bar{1} - \alpha - \alpha^2 - \alpha^3 = \bar{2} + \bar{2}\alpha + \bar{2}\alpha^2 + \bar{2}\alpha^3$ gilt. Wie wir bereits in Teil (b) festgestellt haben, ist $\alpha^5 = \bar{1}$ und somit $\alpha^6 = \alpha$. Damit erhalten wir $\varphi_3(\bar{1}) = \bar{1}$, $\varphi_3(\alpha) = \alpha^3 = \bar{0} + \bar{0} \cdot \alpha + \bar{0} \cdot \alpha^2 + \bar{1} \cdot \alpha^3$, $\varphi_3(\alpha^2) = \varphi_3(\alpha)^2 = (\alpha^3)^2 = \alpha^6 = \alpha = \bar{0} + \bar{1} \cdot \alpha + \bar{0} \cdot \alpha^2 + \bar{0} \cdot \alpha^3$ und $\varphi_3(\alpha^3) = \varphi_3(\alpha)^3 = (\alpha^3)^3 = \alpha^9 = \alpha^5 \cdot \alpha^4 = \alpha^4 = \bar{2} + \bar{2}\alpha + \bar{2}\alpha^2 + \bar{2}\alpha^3$. Jede dieser Gleichungen liefert eine Spalte der Darstellungsmatrix $A \in \mathcal{M}_{4,\mathbb{F}_3}$, insgesamt ist diese gegeben durch

$$A \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} & \bar{2} \\ \bar{0} & \bar{0} & \bar{1} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} & \bar{2} \end{pmatrix}.$$

Die Darstellungsmatrizen von φ_3^2 bzw. φ_3^3 sind gegeben durch

$$A^2 = \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} & \bar{0} \\ \bar{0} & \bar{2} & \bar{0} & \bar{0} \\ \bar{0} & \bar{2} & \bar{0} & \bar{1} \\ \bar{0} & \bar{2} & \bar{1} & \bar{0} \end{pmatrix} \qquad \text{bzw.} \qquad A^3 = \begin{pmatrix} \bar{1} & \bar{0} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} & \bar{0} \end{pmatrix}.$$

Aufgabe H22T3A5

Sei R ein kommutativer Ring mit Einselement, und sei I der Durchschnitt der maximalen Ideale von R.

(a) Zeigen Sie, dass I ein Ideal von R ist.

(b) Beweisen Sie, dass ein Element $a \in R$ genau dann in I liegt, wenn für alle $b \in R$ das Element $ab-1$ eine Einheit von R ist.

Lösung:
zu (a) Wir müssen überprüfen, dass $0_R \in I$ gilt, und dass mit $a, b \in I$ und $r \in R$ auch die Elemente $a+b$ und ra in I enthalten sind. Das Nullelement 0_R ist in jedem Ideal des Rings R enthalten, insbesondere in jedem maximalen Ideal, und damit auch im Durchschnitt I aller maximalen Ideale.

Die Elemente a und b sind in jedem maximalen Ideal $\mathfrak{m}$ von R enthalten (weil I der Durchschnitt aller maximalen Ideale ist). Weil $\mathfrak{m}$ ein Ideal ist, liege auch die Elemente $a+b$ und ra jeweils in $\mathfrak{m}$. Weil I der Durchschnitt aller maximalen Ideale $\mathfrak{m}$ von R ist, zeigt dies, dass $a+b$ und ra auch in I enthalten sind.

zu (b) Die Implikation „$\Rightarrow$“ beweisen wir durch Kontraposition. Sei $a \in R$, und nehmen wir an, dass $ab - 1_R$ für ein $b \in R$ keine Einheit von R ist. Zu zeigen ist, dass a dann nicht im Durchschnitt aller maximalen Ideale von R liegt. Aus $ab - 1_R \notin R^\times$ folgt, dass das Hauptideal $(ab - 1_R)$ nicht das Einheitsideal ist. Sei $\mathfrak{m}$ ein maximales Ideal mit $\mathfrak{m} \supseteq (ab-1_R)$ und nehmen wir an, dass a im Durchschnitt aller maximalen Ideale liegt. Dann gilt insbesondere $a \in \mathfrak{m}$, und damit auch $ab \in \mathfrak{m}$. Aus $ab - 1_R \in \mathfrak{m}$ folgt dann $1_R - ab \in \mathfrak{m}$ und $1_R = (1_R - ab) + ab \in \mathfrak{m}$. Aber dies ist unmöglich, denn da $\mathfrak{m}$ ein maximales Ideal von R ist, gilt $1_R \notin \mathfrak{m}$.

„$\Leftarrow$“ Nehmen wir an, dass $ab - 1_R$ für alle $b \in R$ eine Einheit ist, a aber nicht in I liegt. Dann existiert ein maximales Ideal $\mathfrak{m}$ mit $a \notin \mathfrak{m}$, und auf Grund der Maximalität von $\mathfrak{m}$ muss $(a) + \mathfrak{m} = (1_R)$ gelten. Insbesondere ist also das Einselement 1_R in $(a) + \mathfrak{m}$ enthalten. Es gibt also ein $b \in R$ und ein $m \in \mathfrak{m}$ mit $1_R = ab + m$. Auf Grund unserer Annahme ist $-m = ab - 1_R$ eine Einheit. Aber dies ist unmöglich, denn $-m$ liegt auch in $\mathfrak{m}$, und im maximalen Ideal $\mathfrak{m}$ sind keine Einheiten enthalten.

Aufgabe F23T1A1

(a) Es sei $(A, \cdot)$ eine abelsche Gruppe. Zeigen Sie, das die Abbildung $\phi : A \to A$, $a \mapsto a^{-1}$ ein Gruppenhomomorphismus ist.

(b) Geben Sie ein Gegenbeispiel an, welches zeigt, dass die entsprechende Aussage für beliebige Gruppen im Allgemeinen falsch ist.

(c) Mit A_4 werde die alternierende Gruppe über vier Buchstaben bezeichnet. Bestimmen Sie diejenigen $n \in \mathbb{N}_0$, für die es einen surjektiven Gruppenhomomorphismus $\phi : A_4 \to \mathbb{Z}/(n)$ gibt.

Lösung:
zu (a) Seien $a, b \in A$. Dann gilt $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$.

zu (b) Wir betrachten in der symmetrischen Gruppe S_3 die beiden Elemente $\sigma = (1\ 2)$ und $\tau = (1\ 3)$. Für die Abbildung $\phi : S_3 \to S_3$, $\rho \mapsto \rho^{-1}$ gilt dann $\phi(\sigma\circ\tau) = \phi((1\ 2)\circ(1\ 3)) = \phi((1\ 3\ 2)) = (1\ 3\ 2)^{-1} = (1\ 2\ 3)$, aber $\phi(\sigma) \circ \phi(\tau) = (1\ 2)^{-1} \circ (1\ 3)^{-1} = (1\ 2) \circ (1\ 3) = (1\ 3\ 2)$, und somit $\phi(\sigma \circ \tau) \neq \phi(\sigma) \circ \phi(\tau)$.

zu (c) Allgemein gilt: Ist $n \in \mathbb{N}$, $\phi : G \to H$ ein Gruppenhomomorphismus und $g \in G$ ein Element der Ordnung n, dann ist $\mathrm{ord}(\phi(g))$ ein Teiler von n. In A_4 gibt es bekanntlich nur Elemente der Ordnung 1 (das Neutralelement id), der Ordnung 3 (die 3-Zykel) und der Ordnung 2 (die Doppeltranspositionen). In $\mathbb{Z}/(n)$ ist $1 + n\mathbb{Z}$ ein Element der Ordnung n. Ist $\phi : A_4 \to \mathbb{Z}/(n)$ ein surjektiver Homomorphismus, dann gibt es ein Element $\sigma \in A_4$ mit $\phi(\sigma) = 1 + n\mathbb{Z}$. Auf Grund der Vorbemerkung muss $\mathrm{ord}(\sigma)$ ein Vielfaches von n sein. Wegen $\mathrm{ord}(\sigma) \in \{1, 2, 3\}$ ist dies nur für $n \in \{1, 2, 3\}$ möglich.

Die Gruppe $\mathbb{Z}/(1)$ besteht aus nur einem Element (nämlich $0+1\mathbb{Z}$). Daraus folgt, dass für jede Gruppe G ein surjektiver Homomorphismus $\phi : G \to \mathbb{Z}/(1)$ existiert, der durch $g \mapsto 0+1\mathbb{Z}$ gegeben ist. Insbesondere gibt es einen surjektiven Homomorphismus $A_4 \to \mathbb{Z}/(1)$.

Aus der Vorlesung ist bekannt, dass die Kleinsche Vierergruppe V_4 ein Normalteiler von A_4 (und S_4) ist. Die Faktorgruppe A_4/V_4 ist eine Gruppe der Ordnung $(A_4 : V_4) = |A_4|/|V_4| = \frac{12}{4} = 3$. Als Gruppe der Primzahlordnung 3 ist A_4/V_4 zyklisch, und weil zwei zyklische Gruppen derselben Ordnung zyklisch sind, existiert ein Isomorphismus $\bar{\phi} : A_4/V_4 \to \mathbb{Z}/(3)$. Bezeichnet $\pi : A_4 \to A_4/V_4$ den kanonischen Epimorphismus, dann erhalten wir durch $\phi = \bar{\phi} \circ \pi$ einen surjektiven Homomorphismus $A_4 \to \mathbb{Z}(3)$.

Nehmen wir nun an, dass ein surjektiver Homomorphismus $\phi : A_4 \to \mathbb{Z}/(2)$ existiert. Sei $N = \ker(\phi)$. Auf Grund des Homomorphiesatzes für Gruppen gilt $A_4/N \cong \mathbb{Z}/(2)$. Es folgt

$$\frac{12}{|N|} \quad = \quad \frac{|A_4|}{|N|} \quad = \quad |A_4/N| \quad = \quad |\mathbb{Z}/(2)| \quad = \quad 2$$

und somit $|N| = 6$. Es wäre N also eine Untergruppe der Ordnung 6 von A_4. Aber aus der Vorlesung ist bekannt, dass in A_4 keine solche Untergruppe existiert. Die einzigen $n \in \mathbb{N}$, für die ein surjektiver Homomorphismus $\phi : A_4 \to \mathbb{Z}/(n)$ existiert, sind also 1 und 3.

Aufgabe F23T1A2

(a) Geben Sie die Definition von *Nullteilerfreiheit* eines kommutativen Rings an.

(b) Bestimmen Sie alle Nullteiler und Einheiten sowie die Inklusionen aller Ideale des kommutativen Rings $\mathbb{Z}/(27)$.

Lösung:
zu (a) Ein kommutativer R wird als *nullteilerfrei* bezeichnet, wenn für alle $a, b \in R$ aus $ab = 0_R$ jeweils $a = 0_R$ oder $b = 0_R$ folgt. Ist R darüber hinaus ein Ring mit 1 und gilt außerdem $1_R \neq 0_R$, dann spricht man von einem *Integritätsbereich*. (Die erste Bedingung besagt genau genommen, dass es in R mit eventueller Ausnahme der 0_R keine Nullteiler in R gibt. Die Bezeichnung „nullteilerfrei“ ist so gesehen ein wenig irreführend. Wir hatten die Bezeichnung deshalb in der Vorlesung auch nicht verwendet.)

zu (b) Ist $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, 27) = 1$, was zu $\mathrm{ggT}(a, 3) = 1$ äquivalent ist, dann ist $a+27\mathbb{Z}$ laut Vorlesung eine Einheit in $\mathbb{Z}/(27)$. Die Einheiten in $\mathbb{Z}/(27)$ sind also gegeben durch

$$\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}, \overline{10}, \overline{11}, \overline{13}, \overline{14}, \overline{16}, \overline{17}, \overline{19}, \overline{20}, \overline{22}, \overline{23}, \overline{25}, \overline{26}.$$

Ist die Bedingung $\mathrm{ggT}(a, 3) = 1$ nicht erfüllt, dann ist a ein Vielfaches von 3. In diesem Fall ist $a + 27\mathbb{Z}$ in $\mathbb{Z}/(27)$ ein Nullteiler, denn es ist $9 + 27\mathbb{Z} \neq \bar{0}$ und $(a + 27\mathbb{Z})(9 + 27\mathbb{Z}) = 9a + 27\mathbb{Z} = 0 + 27\mathbb{Z} = \bar{0}$, weil $9a$ ein Vielfaches von 27 ist. (Man kann leicht zeigen, dass in einem endlichen Ring jedes Element entweder eine Einheit oder ein Nullteiler ist.) Also sind

$$\bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}$$

die Nullteiler in $\mathbb{Z}/(27)$.

Jedes Ideal in $\mathbb{Z}$ hat bekanntlich die Form (n) mit $n \in \mathbb{N}_0$, und für $m, n \in \mathbb{N}$ gilt $(m) \supseteq (n)$ genau dann, wenn m ein Teiler von n ist. Die Ideale, die (27) als Teilmenge enthalten, sind also genau die Ideale der Form (m), wobei $m \in \mathbb{N}$ die Teiler von 27 durchläuft. Dies sind 1, 3, 9 und 27. Auf Grund des Korrespondenzsatzes für Ringe existiert eine bijektive Korrespondenz zwischen diesen Idealen von $\mathbb{Z}$ und den Idealen von $\mathbb{Z}/(27)$, und diese ist gegeben durch $(m) \mapsto (m + 27\mathbb{Z})$. Die Inklusion bleibt unter dieser Korrespondenz erhalten, d.h. für zwei Teiler $m, n \in \mathbb{N}$ von 27 gelten die Äquivalenzen

$$m \mid n \quad \Leftrightarrow \quad (m) \supseteq (n) \quad \Leftrightarrow \quad (m + 27\mathbb{Z}) \supseteq (n + 27\mathbb{Z}).$$

Das Hauptideal $(27 + 27\mathbb{Z}) = (\bar{0}) = \{\bar{0}\}$ ist in jedem der Ideale $(27 + 27\mathbb{Z})$, $(9 + 27\mathbb{Z})$, $(3 + 27\mathbb{Z})$ und $(1+27\mathbb{Z})$ enthalten. Das Hauptideal $(9+27\mathbb{Z})$ liegt in $(9+27\mathbb{Z})$, $(3+27\mathbb{Z})$ und $(1+27\mathbb{Z})$. Das Hauptideal $(3 + 27\mathbb{Z})$ ist enthalten in $(3 + 27\mathbb{Z})$ und $(1 + 27\mathbb{Z})$, und es gilt offenbar $(1 + 27\mathbb{Z}) \subseteq (1 + 27\mathbb{Z})$. Darüber hinaus gibt es keine Inklusionsbeziehungen zwischen den Idealen von $\mathbb{Z}/(27)$.

Aufgabe F23T1A3

(a) Zeigen Sie, dass jeder irreduzible Faktor von $f = x^4 - 25 \in \mathbb{Q}[x]$ separabel über $\mathbb{Q}$ ist.

(b) Bestimmen Sie ein primitives Element eines Zerfällungskörpers L von f über $\mathbb{Q}$ und die Dimension von L über $\mathbb{Q}$.

(c) Berechnen Sie die Automorphismengruppe von L über $\mathbb{Q}$.

(d) Bestimmen Sie alle Zwischenkörper $\mathbb{Q} \subseteq K \subseteq L$ und ihre Inklusionen.

Lösung:
zu (a) Jeder irreduzible Faktor von $x^4 - 25$ in $\mathbb{Q}[x]$ ist insbesondere ein irreduzibles Polynom in $\mathbb{Q}[x]$. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist laut Vorlesung jedes irreduzible Polynom über $\mathbb{Q}$ separabel.

zu (b) Die Zerlegung $f = (x^2 - 5)(x^2 + 5) = (x - \sqrt{5})(x + \sqrt{5})(x - i\sqrt{5})(x + i\sqrt{5})$ zeigt, dass $N = \{\pm\sqrt{5}, \pm i\sqrt{5}\}$ die Menge der komplexen Nullstellen von f über $\mathbb{Q}$ und $\mathbb{Q}(N)$ somit der Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$ ist. Wir zeigen, dass

$$\mathbb{Q}(N) \quad = \quad \mathbb{Q}(i + \sqrt{5})$$

gilt und $i + \sqrt{5}$ somit ein primitives Element von L über $\mathbb{Q}$ ist. Wegen $\sqrt{5}, i\sqrt{5} \in N$ gilt erst recht $\sqrt{5}, i\sqrt{5} \in \mathbb{Q}(N)$ und somit auch $i = \frac{i\sqrt{5}}{\sqrt{5}} \in \mathbb{Q}(N)$ und $i + \sqrt{5} \in \mathbb{Q}(N)$. Dadurch ist „$\supseteq$“ nachgewiesen. Für den Nachweis von „$\subseteq$“ bemerken wir, dass mit $i + \sqrt{5}$ auch $(i + \sqrt{5})^{-1} = \frac{1}{6}(i - \sqrt{5})$ in $\mathbb{Q}(i + \sqrt{5})$ enthalten ist, damit auch die Elemente $i - \sqrt{5}$, $i = \frac{1}{2}(i + \sqrt{5}) + \frac{1}{2}(i - \sqrt{5})$, $\sqrt{5} = (i + \sqrt{5}) - i$, $i\sqrt{5}$, $-\sqrt{5}$ und $-i\sqrt{5}$. Insgesamt gilt also $N \subseteq \mathbb{Q}(i + \sqrt{5})$ und damit auch $\mathbb{Q}(N) \subseteq \mathbb{Q}(i + \sqrt{5})$.

Sei nun $L = \mathbb{Q}(N)$. Die Dimension von L als $\mathbb{Q}$-Vektorraum ist nach Definition nichts anderes als der Erweiterungsgrad $[L : \mathbb{Q}]$. Wie wir bereits gesehen, erhält der Körper $\mathbb{Q}(i, \sqrt{5})$ die Menge N, und umgekehrt gilt $N \subseteq \mathbb{Q}(i, \sqrt{5})$. Es gilt also $L = \mathbb{Q}(i, \sqrt{5})$. Das Polynom $g = x^2 - 5$ ist normiert, besitzt $\sqrt{5}$ als Nullstelle und ist auf Grund des Eisenstein-Kriteriums in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel. Es handelt sich also um das Minimalpolynom $\mu_{\sqrt{5},\mathbb{Q}}$ von $\sqrt{5}$ über $\mathbb{Q}$, und daraus folgt $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = \mathrm{grad}(g) = 2$. Das Polynom $h = x^2 + 1$ liegt in $\mathbb{Q}[x]$ und damit auch in $\mathbb{Q}(\sqrt{5})[x]$, es ist normiert, und es besitzt i als Nullstelle. Wäre es über $\mathbb{Q}(\sqrt{5})$ reduzibel, dann wären wegen $\mathrm{grad}(h) = 2$ die beiden Nullstellen $\pm i$ in $\mathbb{Q}(\sqrt{5})$ enthalten. Aber dies ist wegen $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$ und $\pm i \notin \mathbb{R}$ nicht der Fall. Es gilt also $h = \mu_{i,\mathbb{Q}(\sqrt{5})}$ und $[L : \mathbb{Q}(\sqrt{5})] = [\mathbb{Q}(\sqrt{5})(i) : \mathbb{Q}(\sqrt{5})] = \mathrm{grad}(h) = 2$. Mit der Gradformel erhalten wir

$$[L : \mathbb{Q}] \quad = \quad [L : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \quad = \quad 2 \cdot 2 \quad = \quad 4.$$

zu (c) Die Erweiterung $L|\mathbb{Q}$ ist normal, weil L der Zerfällungskörper von f über $\mathbb{Q}$ ist, damit auch algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist jede algebraische Erweiterung von $\mathbb{Q}$ auch separabel. Insgesamt ist $L|\mathbb{Q}$ damit eine Galois-Erweiterung, und laut Vorlesung folgt daraus $|\mathrm{Aut}_{\mathbb{Q}}(L)| = |\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 4$. Für jedes $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(L)$ ist mit $\sqrt{5}$ auch $\sigma(\sqrt{5})$ eine Nullstelle von $x^2 - 5$, es gilt also $\sigma(\sqrt{5}) = \varepsilon_1\sqrt{5}$ für ein $\varepsilon_1 \in \{\pm 1\}$. Ebenso ist mit i auch $\sigma(i)$ eine Nullstelle von $x^2 + 1$ und somit $\sigma(i) = \varepsilon_2 i$ für ein $\varepsilon_2 \in \{\pm 1\}$. Wegen $L = \mathbb{Q}(\sqrt{5}, i)$ ist σ durch die Bilder $\sigma(\sqrt{5})$ und $\sigma(i)$ eindeutig bestimmt. Wegen $|\mathrm{Aut}_{\mathbb{Q}}(L)| = 4$ existiert für jedes Paar $(\varepsilon_1, \varepsilon_2) \in \{\pm 1\}^2$ genau ein $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(L)$ mit $\sigma(\sqrt{5}) = \varepsilon_1\sqrt{5}$ und $\sigma(i) = \varepsilon_2 i$. Insgesamt gilt also

$$\mathrm{Aut}_{\mathbb{Q}}(L) \quad = \quad \{\sigma_{+1,+1} \ , \ \sigma_{+1,+1} \ , \ \sigma_{-1,+1} \ , \ \sigma_{+1,-1}\} \quad ,$$

wobei jedes $\sigma_{\varepsilon_1,\varepsilon_2}$ jeweils durch $\sigma(\sqrt{5}) = \varepsilon_1\sqrt{5}$ und $\sigma(i) = \varepsilon_2 i$ festgelegt ist.

zu (d) Zunächst bestimmen wir die Anzahl der Zwischenkörper von $L|\mathbb{Q}$. Nach dem Hauptsatz der Galoistheorie stimmt diese überein mit der Anzahl der Untergrupppen von $\mathrm{Gal}(L|\mathbb{Q})$. Als Gruppe der Ordnung $|\mathrm{Gal}(L|\mathbb{Q})| = [L:\mathbb{Q}] = 4$ ist $\mathrm{Gal}(L|\mathbb{Q})$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Jedes Element in $\mathrm{Gal}(L|\mathbb{Q})$ ist von Ordnung 1 oder 2. Denn für alle $(\varepsilon_1,\varepsilon_2) \in \{\pm 1\}^2$ gilt $\sigma^2_{\varepsilon_1,\varepsilon_2}(\sqrt{5}) = \sigma_{\varepsilon_1,\varepsilon_2}(\varepsilon_1\sqrt{5}) = \varepsilon_1\sigma_{\varepsilon_1,\varepsilon_2}(\sqrt{5}) = \varepsilon_1^2\sqrt{5} = \sqrt{5}$, und ebenso erhält man $\sigma^2_{\varepsilon_1,\varepsilon_2}(i) = i$. Weil jedes Element von $\mathrm{Gal}(L|\mathbb{Q})$ durch die Bilder von $\sqrt{5}$ und i eindeutig bestimmt ist, folgt daraus $\sigma^2_{\varepsilon_1,\varepsilon_2} = \mathrm{id}_L$. Weil also in $\mathrm{Gal}(L|\mathbb{Q})$ keine Elemente der Ordnung 4 existieren, muss $\mathrm{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ gelten.

Die Ordnung jeder Untergruppe ist ein Teiler von 4, also gleich 1, 2 oder 4. Die Untergruppen der Ordnung 2 sind zyklisch, werden also durch ein Element der Ordnung 2 erzeugt. In $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ gibt es genau drei Elemente der Ordnung 2 (nämlich $(\bar{1},\bar{0})$, $(\bar{0},\bar{1})$ und $(\bar{1},\bar{1})$, und diese drei Elemente liefern drei verschiedene Untergruppen der Ordnung 2. Daneben gibt es noch die Untergruppe $\{(\bar{0},\bar{0})\}$ der Ordnung 1 und die Untergruppe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ der Ordnung 4. Insgesamt besitzt also $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ genau fünf Untergruppen, und dasselbe gilt für $\mathrm{Gal}(L|\mathbb{Q})$. Die Erweiterung $L|\mathbb{Q}$ besitzt also genau fünf Zwischenkörper. Es ist $\mathbb{Q}$ ein Zwischenkörper von $L|\mathbb{Q}$ mit $[\mathbb{Q}:\mathbb{Q}] = 1$, und L ist ein Zwischenkörper mit $[L:\mathbb{Q}] = 4$. Außerdem sind $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(i\sqrt{5}) = \mathbb{Q}(\sqrt{-5})$ drei verschiedene Zwischenkörper vom Grad 2 über $\mathbb{Q}$, denn aus der Vorlesung ist bekannt, dass $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}] = 2$ für jede quadratfreie Zahl $d \in \mathbb{Z}\setminus\{0,1\}$ gilt, und dass verschiedene quadratfreie Zahlen jeweils unterschiedliche Zwischenkörper liefern. Insgesamt haben wir damit alle fünf Zwischenkörper der Erweiterung $L|\mathbb{Q}$ bestimmt.

Aufgabe F23T1A4

(a) Zeigen Sie, dass die Charakteristik eines endlichen Körpers eine Primzahl ist.

(b) Zeigen Sie, dass die Anzahl der Elemente eines endlich-dimensionalen Vektorraums V über einem endlichen Körper K eine Potenz der Charakteristik von K ist.

(c) Sei K ein endlicher Körper mit q Elementen; die Charakteristik von K sein ungleich 2. Berechnen Sie die Mächtigkeit der Bahn des Elements

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(K)$$

unter der Operation von $\mathrm{GL}_2(K)$ durch Konjugation.

Lösung:

zu (a) Sei K ein endlicher Körper und nehmen wir an, dass $\mathrm{char}(K)$ keine Primzahl ist. Dann gilt $\mathrm{char}(K) \in \{0, 1\}$, oder es gibt $m, n \in \mathbb{N}$ mit $\mathrm{char}(K) = mn$ und $m, n > 1$. Im Fall $\mathrm{char}(K) = 0$ wären durch $m \cdot 1_K$ mit $m \in \mathbb{N}$ unendlich viele verschiedene Elemente gegeben, was der Endlichkeit von K widerspricht. Im Fall $\mathrm{char}(K) = 1$ wäre K ein Nullring (also 0_K das einzige Element von K), was bei einem Körper ausgeschlossen ist. Nehmen wir nun an, es existieren $m, n \in \mathbb{N}$ mit den angegebenen Eigenschaften. Dann würde $m \cdot 1_K \neq 0_K$ und $n \cdot 1_K \neq 0_K$, andererseits aber $(m \cdot 1_K) \cdot (n \cdot 1_K) = (mn) \cdot 1_K = 0_K$ gelten. Es wäre also $m \cdot 1_K$ ein Nullteiler ungleich 0_K, was ebenfalls im Widerspruch zur Körpereigenschaft stehen würde.

zu (b) Nach Teil (a) ist $p = \mathrm{char}(K)$ eine Primzahl. Sei P der Primkörper von K und $d = \dim(V)$ (mit $d \in \mathbb{N}_0$). Laut Vorlesung gilt $p = \mathrm{char}(K) = |P|$. Weil K endlich ist, muss auch der Erweiterungsgrad $n = [K : P]$ endlich sein. Als P-Vektorraum ist K isomorph zu P^n, woraus $|K| = |P|^n = p^n$ folgt. Außerdem ist V als K-Vektorraum isomorph zu K^d. Damit erhalten wir $|V| = |K|^d = (p^n)^d = p^{nd}$. Dies zeigt, dass $|V|$ eine Primzahlpotenz ist.

zu (c)

Aufgabe F23T1A5

Seien K ein Körper und $f : V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen K-Vektorräumen V und W. Seien

$$V^* = \mathrm{Hom}_K(V, K) \quad \text{und} \quad W^* = \mathrm{Hom}_K(W, K)$$

die Dualräume, sowie $f^* : W^* \to V^*$, $\varphi \mapsto \varphi \circ f$, die duale Abbildung.

(a) Sei $v_1, ..., v_n$ eine K-Basis von V. Zeigen Sie, dass f genau dann injektiv ist, wenn $f(v_1), ..., f(v_n)$ linear unabhängig sind.

(b) Zeigen Sie: Ist f injektiv, dann ist f^* surjektiv.

(c) Zeigen Sie: Ist f^* surjektiv, dann ist f injektiv.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T2A1

(a) Es seien $a, b \in \mathbb{Z}$. Zeigen Sie: $7 \mid (10a + b) \Leftrightarrow 7 \mid (a - 2b)$.

(b) Bestimmen Sie, für welche $r \in \mathbb{R}$ das folgende lineare Gleichungssystem (i) keine, (ii) genau eine, (iii) unendlich viele Lösungen hat.

$$\begin{array}{rcrcrcl} rx & + & y & + & z & = & 1 \\ x & + & ry & + & z & = & 1 \\ x & + & y & + & rz & = & 1 \end{array}$$

(c) Geben Sie ein externes direktes Produkt zyklischer Gruppen an, das isomorph ist zur Einheitengruppe $(\mathbb{Z}/40\mathbb{Z})^\times$.
Hinweis: Hauptsatz über endliche abelsche Gruppen

(d) Bestimmen Sie eine Orthonormalbasis des $\mathbb{R}^3$ aus Eigenvektoren des Endomorphismus

$$\varphi : \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \quad , \quad \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} x - 2z \\ 0 \\ -2x + 4z \end{pmatrix}.$$

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T2A2

Es sei G eine Gruppe der Ordnung 30. Es bezeichnen U_3 und U_5 jeweils eine 3- und eine 5-Sylowgruppe von G. Zeigen Sie:

(a) Mindestens eine der Gruppen U_3 und U_5 ist ein Normalteiler von G.

(b) Ist U_3 normal, so hat G/U_3 eine Untergruppe vom Index 2. Ist U_5 normal, so hat G/U_5 eine Untergruppe vom Index 2.

(c) Die Gruppe G hat eine Untergruppe U_{15} vom Index 2.

(d) Zeigen Sie, dass alle 3-Sylowgruppen und alle 5-Sylowgruppen von G in U_{15} enthalten sind.

(e) Folgern Sie, dass G genau eine 3-Sylowgruppe und genau eine 5-Sylowgruppe hat.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T2A3

Es sei $R = \{x + y\sqrt{-31} \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Begründen Sie, dass R ein Ring ist.

(b) Zeigen Sie, dass R nicht faktoriell ist.
Hinweis: Beachten Sie $32 = (1 + \sqrt{-31})(1 - \sqrt{-31})$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T2A4

Seien p und q zwei Primzahlen. Bestimmen Sie den Zerfällungskörper des Polynoms $x^p - q \in K[x]$ für die Grundkörper $K = \mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T2A5

Es sei $\mathbb{F}_{625}$ der endliche Körper mit 625 Elementen mit Primkörper P. Bestimmen Sie die Anzahl der Elemente $a \in \mathbb{F}_{625}$ mit $P(a) = \mathbb{F}_{625}$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T3A1

Es seien G die multiplikative Gruppe $(\mathbb{R}^+, \cdot)$ und $X = \mathbb{R}^3$ der dreidimensionale $\mathbb{R}$-Vektorraum mit skalarer Multiplikation $\mathbb{R} \times X \to X$, $(\lambda, x) \mapsto \lambda x$. Weiter sei die folgende Abbildung gegeben:

$$\cdot : G \times X \to X \quad , \quad (g, x) \mapsto g \cdot x = gx.$$

(Das ist die skalare Multiplikation, eingeschränkt auf $G \times X$.)

(a) Zeigen Sie, dass $\cdot$ eine Operation von G auf X ist.

(b) Bestimmen Sie die Menge F der Fixpunkte der Operation.

(c) Zeigen Sie, dass $R = \{x \in \mathbb{R}^3 \mid \|x\| = 1\} \cup \{0\}$ ein Repräsentantensystem der Bahnen der Operation ist.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T3A2

Es seien $n \in \mathbb{N}$ und V der $\mathbb{R}$-Vektorraum $\mathcal{M}_{n,\mathbb{R}}$ der reellen $n \times n$-Matrizen. Für $A \in V$ sei ${}^{\mathrm{t}}A$ die zu A transponierte Matrix. Weiter seien

$$U = \{A \in V \mid {}^{\mathrm{t}}A = A\} \quad \text{und} \quad W = \{A \in V \mid {}^{\mathrm{t}}A = -A\}.$$

Zeigen Sie:

(a) Die Teilmengen U und W sind Untervektorräume von V.

(b) Es gilt $V = U \oplus W$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T3A3

Bestimmen Sie bis auf Isomorphie alle Gruppen der Ordnung $2023 = 7 \cdot 17^2$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T3A4

Es sei $\zeta \in \mathbb{C}$ eine primitive 7-te Einheitswurzel, und es seien $a = \zeta + \zeta^{-1}$ und $b = \zeta + \zeta^2 + \zeta^4$.

(a) Geben Sie einen konkreten Isomorphismus zwischen der Einheitengruppe von $\mathbb{Z}/7\mathbb{Z}$ und der Galoisgruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$ an.

(b) Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galois'sch sind, und bestimmen Sie die zugehörigen Galois-Gruppen bis auf Isomorphie.

(c) Bestimmen Sie die Minimalpolynome von a und b über $\mathbb{Q}$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F23T3A5

Für einen kommutativen Ring R definieren wir $S(R) = \{r_1^2 + r_2^2 \mid r_1, r_2 \in R\}$.

(a) Zeigen Sie: Sind $r, r' \in S(R)$, dann gilt auch $rr' \in S(R)$.

(b) Bekanntlich sind die normierten irreduziblen Polynome in $\mathbb{R}[x]$ genau die Polynome der Form $x - r$ oder $(x - a)^2 + b^2$ mit $r, a \in \mathbb{R}$, $b \in \mathbb{R}^+$.
Zeigen Sie: $S(\mathbb{R}[x]) = \{f \in \mathbb{R}[x] \mid \forall\, \xi \in \mathbb{R} : f(\xi) \geq 0\}$

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T1A1

(a) Sei $n \geq 1$ eine natürliche Zahl und $p \neq 2$ eine Primzahl. Zeigen Sie:

$$p \mid (1 + 2 + ... + (n-1) + n) \quad \Leftrightarrow \quad p \mid n \text{ oder } p \mid (n+1).$$

(b) Bestimmen Sie die Anzahl der Elemente der Einheitengruppe $(\mathbb{Z}[x]/(2, x^3 + x^2 + x))^\times$ des angegebenen Quotientenrings.

(c) Bestimmen Sie mit Hilfe des Chinesischen Restsatzes und unter vollständiger Angabe des Lösungswegs die kleinste natürliche Zahl $n \geq 1$, die die Kongruenzen $n \equiv 1 \mod 3$, $n \equiv 2 \mod 5$ und $n \equiv 0 \mod 8$ erfüllt.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T1A2

Im Folgenden sei S_n die symmetrische Gruppe.

(a) Sei $\sigma \in S_n$ ein Produkt $\sigma = \zeta_1 \cdot ... \cdot \zeta_m$ von paarweise disjunkten Zyklen ζ_j der Längen ℓ_j. Zeigen Sie, dass die Ordnung von σ gleich dem kleinsten gemeinsamen Vielfachen von $\ell_1, ..., \ell_m$ ist.

(b) Bestimmen Sie die maximale Ordnung eines Elements (i) der S_6; (ii) der S_7.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T1A3

(a) Sei G eine einfache Gruppe mit $|G| > 2$, die auf der endlichen Menge X operiere, und $\rho : G \to \Sigma(X) \cong S_n$ (mit $n = |X|$) der zugehörige Homomorphismus in die symmetrische Gruppe von X. Zeigen Sie, dass $\rho(G)$ in der alternierenden Gruppe A_n enthalten ist.

(b) Sei G eine nicht-abelsche einfache Gruppe, $H \subseteq G$ eine Untergruppe sowie $n = (G : H) \geq 2$. Zeigen Sie, dass G isomorph zu einer Untergruppe von A_n ist, und dass $n \geq 5$ gilt.

(c) Zeigen Sie, dass keine endliche einfache Gruppe der Ordnung 80 existiert.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T1A4

Sei R ein kommutativer Ring (mit 1). Sei weiter $I \subseteq R$ ein Ideal. Wir definieren das *Radikal* von I als

$$\mathrm{rad}(I) \quad = \quad \{r \in R \mid r^n \in I \text{ für ein } n \in \mathbb{N}\}.$$

Zeigen Sie:

(a) Die Teilmenge $\mathrm{rad}(I) \subseteq R$ ist ebenfalls ein Ideal von R.

(b) Ist I ein Primideal, dann gilt $\mathrm{rad}(I) = I$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T1A5

(a) Zeigen Sie, dass der Kreisteilungskörper $\mathbb{Q}(\zeta_8)$ genau drei quadratische Teilkörper besitzt, d.h. Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_8)$ mit $[K : \mathbb{Q}] = 2$.

(b) Bestimmen Sie in Teil (a) drei Elemente $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$ so, dass die Zwischenkörper $K_i = \mathbb{Q}(\sqrt{\alpha_i})$ genau die quadratischen Teilkörper sind.

(c) Zeigen Sie, dass das Polynom $x^4 + x + \bar{1} \in \mathbb{F}_2[x]$ irreduzibel ist.

(d) Nach Teil (c) gilt $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ für ein $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\alpha^4 + \alpha + \bar{1} = \bar{0}$. Bestimmen Sie die Grade $[\mathbb{F}_2(\beta) : \mathbb{F}_2]$ in den beiden Fällen $\beta = \alpha + \bar{1}$ und $\beta = \alpha^3 + \bar{1}$.

Lösung:

zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T2A1

Sei $\omega \in \mathbb{C}$ eine primitive dritte Einheitswurzel.

(a) Zeigen Sie, dass $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ eine Galois-Erweiterung ist.

(b) Bestimmen Sie den Grad $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$ dieser Erweiterung.

(c) Sei G die Menge der invertierbaren 2×2-Matrizen der Form $\begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix}$ mit Einträgen in $\mathbb{F}_3$. Zeigen Sie, dass G eine Untergruppe der Gruppe der invertierbaren 2×2-Matrizen über $\mathbb{F}_3$ ist, und geben Sie einen Isomorphismus $G \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)|\mathbb{Q})$ an.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe H23T2A2

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

(b) Bestimmen Sie alle endlichen einfachen auflösbaren Gruppen.

Lösung:
zu (a) zu (b)

Aufgabe H23T2A3

(a) Seien G_1 und G_2 endliche Gruppen und $|G_1|$ teilerfremd zu $|G_2|$. Sei weiter $H \subseteq G_1 \times G_2$ eine Untergruppe. Zeigen Sie, dass es Untergruppen $H_1 \subseteq G_1$ und $H_2 \subseteq G_2$ gibt mit $H = H_1 \times H_2$.

(b) Geben Sie zwei Gruppen G_1 und G_2 an sowie eine Untergruppe $H \subseteq G_1 \times G_2$, so dass H nicht von der Form $H_1 \times H_2$ für zwei Untergruppen $H_1 \subseteq G_1$ und $H_2 \subseteq G_2$ ist.

(c) Sei G eine endliche Gruppe der Ordnung n mit folgenden Eigenschaften.

(i) Für jeden Teiler $k > 0$ von n gibt es eine Untergruppe U von G der Ordnung k.

(ii) Die Gruppe G ist nicht abelsch.

Zeigen Sie, dass G nicht einfach ist.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T2A4

Es seien $x = (x_1, x_2, x_3, x_4)$, $y = (y_1, y_2, y_3, y_4)$, $z = (z_1, z_2, z_3, z_4) \in \mathbb{R}^4$ beliebig und

$$f : \mathbb{R}^4 \longrightarrow \mathbb{R} \quad , \quad (u_1, u_2, u_3, u_4) \mapsto \det \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ u_1 & u_2 & u_3 & u_4 \end{pmatrix}.$$

(a) Zeigen Sie, dass f eine lineare Abbildung ist.

(b) Zeigen Sie, dass x, y, z Elemente des Kerns von f sind.

(c) Zeigen Sie, dass der Kern von f genau dann der von x, y, z aufgespannte Untervektorraum ist, wenn diese Vektoren linear unabhängig sind.

(d) Bestimmen Sie den Kern von f in dem Fall, dass x, y, z linear abhängig sind.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T2A5

Sei R ein kommutativer Ring mit 1.

(a) Sei $x \in R$ ein Element mit $x^m = 0$ für ein $m > 0$. Zeigen Sie, dass dann $1 + x \in R$ multiplikativ invertierbar ist.

(b) Sei $I \subseteq R$ ein Ideal. Zeigen Sie, dass dann auch

$$\sqrt{I} \quad = \quad \{x \in R \mid x^m \in I0 \text{ für ein } m > 0\}$$

ein Ideal in R ist.

(c) Zeigen Sie, dass $N(R) = \{x \in R \mid x^m = 0 \text{ für ein } m > 0\}$ ein Ideal in R ist.

(d) Geben Sie ein Beispiel für einen (nicht kommutativen) Ring R' an, in dem $N(R') \subseteq R'$ (wie in Teil (c)) kein (Links-)Ideal ist.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T3A1

Sei G eine Gruppe und H eine Untergruppe von G.

(a) Geben Sie die Definition des *Index* $(G : H)$ an. (Die Gruppe G braucht nicht endlich zu sein.)

(b) Zeigen Sie, dass $(G : H)$ ein Teiler von 168 ist, wenn H der Kern eines Homomorphismus $f : G \to \mathrm{GL}_3(\mathbb{F}_2)$ in die Gruppe der invertierbaren 3×3-Matrizen über dem Körper $\mathbb{F}_2$ ist.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T3A2

Es seien $\alpha = \sqrt{\sqrt{12}+3}$, $\beta = i\sqrt{\sqrt{12}-3} \in \mathbb{C}$ und $L = \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{C}$.

(a) Bestimmen Sie das Minimalpolynom $f = m_{\alpha,\mathbb{Q}}$ von α über $\mathbb{Q}$, und zeigen Sie, dass auch β eine Nullstelle von f ist.

(b) Begründen Sie, warum $L|\mathbb{Q}$ eine Galois-Erweiterung ist.

(c) Zeigen Sie, dass $L = \mathbb{Q}(\alpha, i)$ gilt, und bestimmen Sie den Grad $[L : \mathbb{Q}]$.

(d) Zeigen Sie, dass die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ einen Normalteiler der Ordnung 2 enthält.

Lösung:

zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T3A3

Sei L ein Zerfällungskörper des Polynoms $f = x^4 - x^3 + 2x^2 - 2$ über $\mathbb{Q}$. Bestimmen Sie

(a) für eine Nullstelle $1 \neq \alpha \in L$ von f das Minimalpolynom von α über $\mathbb{Q}$,

(b) den Grad $[L : \mathbb{Q}]$.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T3A4

(a) Sei p eine ungerade Primzahl und $n \geq 1$. Zeigen Sie, dass die Gleichung $x^2 = \bar{1}$ in $R = \mathbb{Z}/p^n\mathbb{Z}$ genau zwei Lösungen hat.

(b) Bestimmen Sie alle Lösungen der Gleichung $x^2 = \bar{1}$ im Ring $\mathbb{Z}/2023\mathbb{Z}$.
Hinweis: $2023 = 7 \cdot 17^2$

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe H23T3A5

Seien $R \neq 0$ ein kommutativer Ring und $F, G \in R[x]$ Polynome, wobei G als normiert angenommen sei. Dann (das sollen Sie nicht beweisen) existieren eindeutig bestimmte $A, B \in R[x]$ so, dass gelten $F = AG + B$ und $\deg(B) < \deg(G)$ (hierbei ist $\deg(0) = -\infty$). (Das ist Division mit Rest durch ein normiertes Polynom.)

(a) Seien $f : R \to S \neq 0$ ein Ringhomomorphismus und $f[x] : R[x] \to S[x]$ der Ringhomomorphismus, der auf $R \subseteq R[x]$ mit f übereinstimmt und außerdem $f[x](x) = x$ erfüllt. Zeigen Sie, dass in $S[x]$ gilt $f[x](F) = f[x](A) \cdot f[x](G) + f[x](B)$, und dass diese Gleichung die Division mit Rest von $f[x](F)$ durch $f[x](G)$ ist.

(b) Zeigen Sie, dass genau ein Ideal $I \subseteq R$ existiert, so dass für jeden Ringhomomorphismus $f : R \to S \neq 0$ äquivalent sind:

  (i) $f[x](G)$ teilt $f[x](F)$ in $S[x]$

  (ii) $f(I) = 0$

(c) Bestimmen Sie das Ideal $I \subseteq R$ aus Teil (b) in den beiden folgenden Fällen:

  (i) $R = \mathbb{Z}$, $F = x^3 - 1$, $G = x^2 + 1$

  (ii) $R = \mathbb{Z}[y]$, $F = x^2 + y$, $G = x - 1$

Lösung:

zu (a) zu (b) zu (c) zu (d)

Aufgabe F24T1A1

Sei $n > 0$ und $M_n = (m_{ij})$ die reelle $n \times n$-Matrix mit $m_{ij} = 0$, falls $j < i - 1$ oder $j > i + 1$, $m_{ij} = 1$, falls $j = i - 1$, $m_{ij} = 3$, falls $j = i$, und $m_{ij} = 2$, falls $j = i + 1$. Also ist beispielsweise

$$M_5 = \begin{pmatrix} 3 & 2 & 0 & 0 & 0 \\ 1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix}.$$

Sei d_n die Determinante von M_n.

(a) Berechnen Sie d_1 und d_2.

(b) Zeigen Sie, dass für alle $n \geq 3$ gilt $d_n = 3d_{n-1} - 2d_{n-2}$.

(c) Zeigen Sie, dass $d_n = 2^{n+1} - 1$ gilt.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe F24T1A2

(a) Bestimmen Sie alle $n \in \{1, 2, 3, ...\}$, für die die Gruppe $\mathbb{Z}/n\mathbb{Z}$ außer der Identität keinen weiteren Gruppenautomorphismus besitzt.

(b) Sei nun G eine endliche Gruppe der Ordnung ≥ 2 mit der Eigenschaft, dass die Identität der einzige Gruppenautomorphismus ist. Zeigen Sie, dass G eine abelsche Gruppe ist.

(c) Zeigen Sie, dass $G \cong \mathbb{Z}/2\mathbb{Z}$ gilt.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe F24T1A3

(a) Sei R ein kommutativer Ring. Ein Element $x \in R$ heißt *nilpotent*, falls es ein $k \in \{1, 2, 3, ...\}$ gibt mit $x^k = 0$. Sei $I \subseteq R$ ein Primideal und $x \in R$ nilpotent. Zeigen Sie: $x \in I$

(b) Sei $I = (1 + i)$ das von $1 + i$ erzeugte Ideal im Ring $\mathbb{Z}[i]$. Zeigen Sie, dass der Ring $\mathbb{Z}[i]/I$ genau zwei Elemente hat.

(c) Seien R ein Integritätsbereich und $a, b, c \in R$. Zeigen Sie: Erzeugen a und b in R das Einheitsideal und ist a ein Teiler von bc, so ist a ein Teiler von c.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe F24T1A4

Sei p eine Primzahl mit der Eigenschaft, dass $p-1 = p_1 \cdot ... \cdot p_n$ das Produkt der paarweise verschiedenen Primzahlen $p_1, ..., p_n$ ist.

(a) Zeigen Sie, dass es genau 2^n verschiedene Untergruppen in $G = (\mathbb{Z}/p\mathbb{Z})^\times$ gibt.

(b) Sei $\zeta_p \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Bestimmen Sie die Anzahl der Zwischenkörper in der Erweiterung $\mathbb{Q}(\zeta_p)|\mathbb{Q}$.

Lösung:
zu (a) zu (b)

Aufgabe F24T1A5

Sei $\alpha = \sqrt{10 - 5\sqrt{2}} \in \mathbb{R}$.

(a) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}$.

(b) Zeigen Sie, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine Galois-Erweiterung ist.

(c) Zeigen Sie, dass die Galois-Gruppe von $\mathbb{Q}(\alpha)|\mathbb{Q}$ zu $\mathbb{Z}/4\mathbb{Z}$ isomorphi ist.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe F24T2A1

(a) Bestimmen Sie eine Zerlegung des Elements $z = 29 \in \mathbb{Z}[i]$ in Primelemente.

(b) Es sei $p > 3$ eine Primzahl. Zeigen Sie, dass es in der multiplikativen Gruppe $\mathbb{F}_{p^2}^{\times}$ ein Element a der Ordnung 12 gibt.

(c) Entscheiden Sie, ob $\overline{437} \in \mathbb{Z}/911\mathbb{Z}$ invertierbar ist. Bestimmen Sie gegebenenfalls das Inverse.

(d) Entscheiden Sie begründet, ob $\mathbb{R}$ eine algebraische Erweiterung vom Grad 4 hat.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F24T2A2

Es sei $N = a_{n-1}a_{n-2}\cdots a_1a_0$ mit $a_i \in \{0, 1, ..., 9\}$, $a_{n-1} \neq 0$ die dezimale Zifferndarstellung einer Zahl N.

(a) Die *Wechselsumme* von N ist durch

$$W(N) \quad = \quad \sum_{i=0}^{n-1} (-1)^i a_i$$

gegeben. (Beispiel: $W(123456) = 6 - 5 + 4 - 3 + 2 - 1$)

(b) Wir nennen N *palindromisch*, wenn die Ziffernzahl n gerade ist und

$$a_{n-1}a_{n-2}\cdots a_1a_0 \quad = \quad N \quad = \quad a_0a_1\cdots a_{n-2}a_{n-1}$$

gilt. (Beispiel: 493394 ist palindromisch.)
Bestimmen Sie alle palindromischen Primzahlen.

(c) Sei die Folge $(U_n)_{n\in\mathbb{N}}$ mit $U_1 = 1$, $U_2 = 11$, $U_3 = 111$, $U_4 = 1111$, gegeben. Zeigen Sie

(i) Im Fall $k \mid n$ gilt $U_k \mid U_n$.

(ii) Ist $n = k \cdot \ell$ mit $k, \ell \in \{2, 3, 4, ...\}$, so ist U_n keine Primzahl.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F24T2A3

(a) Entscheiden Sie und begründen Sie, ob es eine Gruppe gibt, die außer dem neutralen Element vier Elemente der Ordnung 5, sechs Elemente der Ordnung 2 und keine weiteren Elemente enthält.

(b) Entscheiden und begründen Sie, ob es eine abelsche Gruppe ist, die nur Elemente mit den Ordnungen 1, 2 und 4 enthält, wobei die Anzahl der Elemente durch

Ordnung	1	2	4
Anzahl	1	3	12

gegeben ist. Entscheiden Sie begründet, ob die abelsche Gruppe durch diese Angabe bis auf Isomorphie eindeutig bestimmt ist.

(c) Beweisen oder widerlegen Sie die folgende Aussage: Ist G eine endliche Gruppe und d ein Teiler der Gruppenordnung $|G|$, so hat G eine Untergruppe U mit $|U| = d$.

Lösung:

zu (a) Eine Gruppe mit diesen Eigenschaften existiert nicht. Denn nehmen wir an, dass es sich bei G um eine solche Gruppe handelt. Die Gesamtzahl der Gruppenelemente, also die Ordnung von G, ist gleich $1 + 4 + 6 = 11$. Nach dem Satz von Lagrange ist $\text{ord}(g)$ für jedes $g \in G$ also ein Teiler von 11, also $\text{ord}(g) \in \{1, 11\}$ für alle $g \in G$. Somit kann es in G keine Elemente der Ordnung 2 oder 5 geben, im Widerspruch zur Annahme.

zu (b) Nehmen wir an, G ist eine Gruppe mit diesen Eigenschaften. Dann ist $|G| = 1 + 3 + 12 = 16$. Nach dem Hauptsatz über endliche abelsche Gruppen gibt es ein $r \in \mathbb{N}$ und $d_1, ..., d_r \in \mathbb{N}$, $d_1 \geq d_2 \geq ... \geq d_r \geq 2$ mit

$$G \quad \cong \quad \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$$

und $d_1 \cdot d_2 \cdot ... \cdot d_r = 16$. Wegen $d_j \mid 16$ gilt jeweils $d_j \in \{2, 4, 8, 16\}$. Da es in G keine Elemente der Ordnung 8 oder 16 gibt, ist jeweils nur $d_j \in \{2, 4\}$ möglich. Die einzigen Möglichkeiten für solche Produkte sind $4 \cdot 4$ oder $4 \cdot 2 \cdot 2$. Also gilt

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{oder} \quad G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

In $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$ gibt es wegen $2 \cdot (\bar{2}, \bar{0}, \bar{0}) = 2 \cdot (\bar{0}, \bar{1}, \bar{0}) = 2 \cdot (\bar{0}, \bar{0}, \bar{1}) = 2 \cdot (\bar{2}, \bar{1}, \bar{0}) = (\bar{0}, \bar{0}, \bar{0})$ (und weil keines dieser Elemente mit dem Neutralelement $(\bar{0}, \bar{0}, \bar{0})$ übereinstimmt) mehr als drei Elemente der Ordnung 2. Also bleibt $G \cong (\mathbb{Z}/4\mathbb{Z})^2$ also einzige Möglichkeit. Wir überprüfen nun, dass es in $(\mathbb{Z}/4\mathbb{Z})^2$ tatsächlich genau drei Elemente der Ordnung 2 und genau 12 Elemente der Ordnung 4 gibt.

Die drei Elemente $(\bar{0}, \bar{2})$, $(\bar{2}, \bar{0})$ und $(\bar{2}, \bar{2})$ sind von Ordnung 2, denn keines von ihnen stimmt mit dem Neutralelement $(\bar{0}, \bar{0})$ überein, aber wenn man sie mit 2 multipliziert, dann erhält man $(\bar{0}, \bar{0})$. Sei nun $(a, b) \in (\mathbb{Z}/4\mathbb{Z})^2$ ein beliebiges Element der Ordnung 2. Dann gilt $(2\bar{a}, 2\bar{b}) = (\bar{0}, \bar{0})$; dies ist nur möglich, wenn $a, b \in \{\bar{0}, \bar{2}\}$ erfüllt ist. Weil (a, b) ungleich dem Neutralelement ist (dies ist von Ordnung 1), muss $(a, b) \in \{(\bar{0}, \bar{2}), (\bar{2}, \bar{0}), (\bar{2}, \bar{2})\}$ gelten. Nun gibt es G neben den Elementen der Ordnung 2 und dem Neutralelement noch 12 weitere Elemente, wegen $|G| - 3 - 1 = 16 - 3 - 1 = 12$. Ist (c, d) ein solches Element, dann gilt $4 \cdot (c, d) = (4\bar{c}, 4\bar{d}) = (\bar{0}, \bar{0})$, also $\text{ord}((c, d)) \mid 4$ und somit $\text{ord}((c, d)) \in \{1, 2, 4\}$. Da wir die Ordnungen 1 und 2 ausgeschlossen hatten, muss (c, d) ein Element der Ordnung 4 sein. Dies zeigt, dass es in G genau 12 Elemente der Ordnung 4 gibt.

zu (c) Diese Aussage ist im Allgemeinen falsch, denn bekanntlich ist die alternierende Gruppe A_4 von Ordnung 12, diese enthält aber keine Untergruppe der Ordnung 6, obwohl 6 ein Teiler von 12 ist. Um

dies nachzuweisen, nehmen wir an, U wäre eine Untergruppe mit $|U| = 6$. Da 3 ein Primteiler von $|U|$ ist, existiert nach dem Lemma von Cauchy ein $\sigma \in U$ mit $\mathrm{ord}(\sigma) = 3$. Die Elemente der Ordnung 3 in A_4 sind genau die 3-Zykel; es gibt somit drei verschiedene Zahlen i, j, k in $M_4 = \{1, 2, 3, 4\}$ mit $\sigma = (i\ j\ k)$. Ebenso existiert in U ein Element τ mit $\mathrm{ord}(\tau) = 2$, und wegen $\tau \in A_4$ ist dies eine Doppeltransposition. Sei ℓ das eindeutig bestimmte Element in $M_4 \setminus \{i, j, k\}$. Die folgenden Gleichungen zeigen, dass die Untergruppe U *alle* Doppeltranspositionen enthält, sobald zumindest *eine* Doppeltransposition in U liegt:

$$(i\ j\ k)^{-1} \circ (i\ j)(k\ \ell) \circ (i\ j\ k) = (k\ j\ i) \circ (i\ j)(k\ \ell) \circ (i\ j\ k) = (i\ k)(j\ \ell)$$

$$(i\ j\ k) \circ (i\ j)(k\ \ell) \circ (i\ j\ k)^{-1} = (i\ j\ k) \circ (i\ j)(k\ \ell) \circ (k\ j\ i) = (i\ \ell)(j\ k).$$

Also enthält U mindestens $(i\ j\ k)$, das Inverse $(i\ j\ k)^{-1} = (i\ k\ j)$, die drei Doppeltransposition, die Identität, und außerdem noch das Element

$$(i\ j)(k\ \ell) \circ (i\ j\ k) \circ (i\ j)(k\ \ell) \quad = \quad (i\ \ell\ j).$$

Damit wäre dann $|U| \geq 7$, im Widerspruch zu $|U| = 6$.

Aufgabe F24T2A4

(a) Entscheiden Sie begründet, ob ein Ring R existiert, der unendlich viele Einheiten $u \in R^\times$ endlicher multiplikativer Ordnung hat.

(b) Entscheiden Sie begründet, ob ein Ring R existiert, der unendlich viele Einheiten endlicher additiver Ordnung hat.

(c) Entscheiden Sie begründet, ob ein Ring R existiert, der nur endlich viele Einheiten hat und in dem die multiplikative Ordnung einer Einheit $u \in R^\times$ unendlich ist.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe F24T2A5

Es seien $a_1, ..., a_n \in \mathbb{Q}$ und das Polynom $f \in \mathbb{Q}[x]$ vom Grad $2n$ durch

$$f \quad = \quad x^{2n} + a_1 x^{2n-1} + ... + a_{n-1} x^{n+1} + a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + 1$$

gegeben. Sei K der Zerfällungskörper von K über $\mathbb{Q}$. Zeigen Sie:

(a) Ist r eine Nullstelle von f, so ist auch $\frac{1}{r}$ eine Nullstelle von f.

(b) Es ist $|\mathrm{Gal}(K|\mathbb{Q})| \leq 2^n \cdot n!$.

Lösung:
zu (a) zu (b)

Aufgabe F24T3A1

(a) Es sei $\mathbb{F}_3$ der endliche Körper mit drei Elementen. Bestimmen Sie die Anzahl der Elemente des Kerns U der linearen Abbildung

$$\varphi : \mathbb{F}_3^3 \to \mathbb{F}_3^2 \quad , \quad v \mapsto \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{2} & \bar{1} & \bar{2} \end{pmatrix} v.$$

(b) Bestimmen Sie eine Zerlegung des Polynoms $f = 2x^3 + 4x^2 - 2x$ über $\mathbb{Z}$ in irreduzible Faktoren.

(c) Bestimmen Sie ein $f \in \mathbb{R}[x]$ mit $(f) = (x^2 - 1, x^3 - 1)$ und begründen Sie, warum Ihre Wahl diese Gleichheit erfüllt.

(d) Zeigen Sie, dass das Element $2 \in \mathbb{Z}[\sqrt{-13}]$ irreduzibel ist.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F24T3A2

(a) Ermitteln Sie die Anzahl der Lösungen der folgenden Gleichungen in $\mathbb{Z}/8\mathbb{Z}$.

$$x^5 = \bar{0}, \quad x^5 = \bar{1}, \quad x^5 = \bar{2}, \quad x^5 = \bar{3}$$

(b) Ermitteln Sie die Anzahl der Lösungen der folgenden Gleichungen in $\mathbb{Z}/2024\mathbb{Z}$. $(2024 = 8 \cdot 11 \cdot 23)$

$$x^5 = \bar{0}, \quad x^5 = \bar{1}, \quad x^5 = \bar{2}, \quad x^5 = \bar{3}$$

(c) Bestimmen Sie, wieviele fünfte Potenzen es in $\mathbb{Z}/2024\mathbb{Z}$ gibt.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F24T3A3

Für eine Primzahl p sei $\mathbb{F}_p$ der endliche Körper mit $|\mathbb{F}_p| = p$; weiter sei

$$R \quad = \quad \left\{ \begin{pmatrix} a & b \\ \bar{0} & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{F}_p \right\}$$

(a) Zeigen Sie, dass R ein Teilring des Rings der 2×2-Matrizen ist.

(b) Zeigen Sie, dass die Einheitengruppe $R^\times$ im Fall $p \neq 2$ nicht einfach ist.

(c) Nun sei $p = 257$. Entscheiden Sie begründet, ob die Einheitengruppe $R^\times$ in diesem Fall auflösbar ist.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe F24T3A4

(a) Seien K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Begründen Sie, warum die Ordnung der Galoisgruppe von f über K durch den Grad von f teilbar ist.

(b) Geben Sie ein Beispiel an, wieso die Aussage im Allgemeinen falsch wird, wenn f nicht mehr als irreduzibel vorausgesetzt wird.

(c) Begründen Sie, warum es zu jeder natürlichen Zahl $n \geq 1$ eine Galois-Erweiterung $E|F$ von Körpern E,F gibt, deren Galoisgruppe die Ordnung n hat.

(d) Zeigen Sie, dass die Aussage (c) im Allgemeinen falsch wird, wenn der Körper F fest vorgegeben wird.

Lösung:
zu (a) zu (b) zu (c) zu (d)

Aufgabe F24T3A5

(a) Geben Sie eine explizite Darstellung der primitiven fünften Einheitswurzeln mithilfe von Quadratwurzeln an. (Tipp: Wenn $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + \bar{1} = \bar{0}$ ist, welche Polynomgleichung erfüllt dann $\beta = \alpha + \alpha^{-1}$?)

(b) Folgern Sie aus Ihrer Lösung der Teilaufgabe (a) eine Konstruktionsvorschrift eines regelmäßigen Fünfecks mit Zirkel und Lineal.

(c) Geben Sie eine Konstruktionsvorschrift eines regelmäßigen Zwanzigecks mit Zirkel und Lineal an.

Lösung:
zu (a) zu (b) zu (c)

Aufgabe H24T1A1

Sei H die Menge aller reellen 2×2-Matrizen der Form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{mit } a^2 + b^2 \neq 0.$$

(a) Zeigen Sie, dass H eine Untergruppe der Gruppe $\mathrm{GL}_2(\mathbb{R})$ der invertierbaren reellen 2×2-Matrizen ist.

(b) Seien $A, B, C \in H$. Zeigen Sie, dass die Gleichung $AYB = C$ eine eindeutige Lösung Y in H hat.

(c) Lösen Sie die Gleichung

$$\begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix} Y \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}.$$

Lösung:

zu (a) Das Nentralelement von $\mathrm{GL}_2(\mathbb{R})$ ist die Einheitsmatrix E. Es muss also gezeigt werden, dass E in H liegt, und dass für alle $A, B \in H$ auch $AB \in H$ und $A^{-1} \in H$ erfüllt ist. Offenbar gilt $E \in H$, denn E kommt dadurch zu Stande, dass man in der Matrix der angegebenen Form $a = 1$ und $b = 0$ setzt (und es ist $1^2 + 0^2 = 1 \neq 0$). Seien nun $A, B \in H$ vorgegeben. Dann gibt es Paare $(a, b), (c, d) \in \mathbb{R}^2$ mit $a^2 + b^2 \neq 0$, $c^2 + d^2 \neq 0$.

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{und} \qquad B = \begin{pmatrix} c & d \\ -d & b \end{pmatrix}.$$

Es ist dann

$$AB \quad = \quad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \quad = \quad \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}$$

Wegen $\det(A) = a^2 + b^2 \neq 0$ und $\det(B) = c^2 + d^2 \neq 0$ muss auch $\det(AB) = \det(A)\det(B)$ ungleich null sein. Es gilt also $(ac - bd)^2 + (ad + bc)^2 \neq 0$. Damit ist insgesamt $AB \in H$ nachgewiesen. Weiter gilt

$$A^{-1} \quad = \quad \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ -(-\frac{b}{a^2+b^2}) & \frac{a}{a^2+b^2} \end{pmatrix} \quad = \quad \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$$

mit $u = \frac{a}{a^2+b^2}$, $v = \frac{b}{a^2+b^2}$. Aus $\det(A) \neq 0$ folgt $\det(A^{-1}) \neq 0$ und somit $u^2 + v^2 \neq 0$. Dies zeigt, dass auch A^{-1} in H liegt.

zu (b) Wegen $A, B \in H$ sind A und B invertierbar. Sei $Y_1 = A^{-1}CB^{-1}$. Wegen $A, B, C \in H$ und der Untergruppen-Eigenschaft ist auch Y_1 in H enthalten, und Y_1 ist eine Lösung der angegebenen Gleichung, denn es gilt

$$AY_1B \quad = \quad A(A^{-1}CB^{-1})B \quad = \quad ECE \quad = \quad C.$$

Bezeichnet $Y_1' \in H$ eine beliebige Lösung der Gleichung, dann folgt $Y_1' = A^{-1}(AY_1'B)B^{-1} = A^{-1}CB^{-1} = A^{-1}(AY_1B)B^{-1} = Y_1$. Dies zeigt, dass Y_1 die einzige Lösung der Gleichung ist.

zu (c) Nach Teil (b) erhalten wir eine Lösung der Gleichung durch

$$Y_1 \quad = \quad \begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix}^{-1} \quad = \quad \tfrac{1}{25} \begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix} \cdot \tfrac{1}{40} \begin{pmatrix} 6 & -2 \\ 2 & 6 \end{pmatrix}$$

$$= \quad \tfrac{1}{1000} \begin{pmatrix} 13 & 9 \\ -9 & 13 \end{pmatrix} \begin{pmatrix} 6 & -2 \\ 2 & 6 \end{pmatrix} \quad = \quad \tfrac{1}{1000} \begin{pmatrix} 96 & 28 \\ -28 & 96 \end{pmatrix} \quad = \quad \tfrac{1}{250} \begin{pmatrix} 24 & 7 \\ -7 & 24 \end{pmatrix}$$

Wir überprüfen die Korrektheit der Lösung.

$$\begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix} Y_1 \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix} = \tfrac{1}{250} \begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} 24 & 7 \\ -7 & 24 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix}$$

$$= \tfrac{1}{250} \begin{pmatrix} 75 & 100 \\ -100 & 75 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix} = \tfrac{1}{250} \begin{pmatrix} 250 & 750 \\ -750 & 250 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}.$$

Aufgabe H24T1A2

Sei G eine Gruppe der Ordnung 2024 ($= 2^3 \cdot 11 \cdot 23$). Zeigen Sie:

(a) G hat einen Normalteiler H der Ordnung 23.

(b) H operiert transitiv durch Konjugation auf den Untergruppen der Ordnung 11.

(c) G hat einen Normalteiler der Ordnung 253.

(d) G ist auflösbar.

Lösung:
zu (a) Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Auf Grund der Sylowsätze gilt $\nu_{23} \mid 2^3 \cdot 11$, also $\nu_{23} \in \{1, 2, 4, 8, 11, 22, 44, 88\}$, außerdem $\nu_{23} \equiv 1 \bmod 23$. Wegen $2, 4, 8, 11, 22 \not\equiv 1 \bmod 23$, $44 \equiv 21 \not\equiv 1 \bmod 23$ und $88 \equiv 19 \not\equiv 1 \bmod 23$ folgt $\nu_{23} = 1$. Wiederum auf Grund der Sylowsätze ist die einzige 23-Sylowgruppe H ein Normalteiler von G, und wegen $|G| = 2^3 \cdot 11^1 \cdot 23^1$ gilt $|H| = 23$.

zu (b) Sei $\bullet$ die Operation der Gruppe H operiert auf der Menge $\mathcal{M}_{11}$ den Untergruppen von G der Ordnung 11 durch Konjugation. Für beliebiges $U \in \mathcal{M}_{11}$ ist die Bahnlänge $|H(U)|$ ein Teiler von 23, also (da 23 eine Primzahl ist) entweder $|H(U)| = 1$ oder $|H(U)| = 23$. Im zweiten Fall ist die Operation transitiv; nehmen wir also an, es gilt $|H(U)| = 1$ und somit $H(U) = \{U\}$.

Aus dieser Annahme folgt $hUh^{-1} = h \bullet U = U$ für alle $h \in H$, d.h. H ist ist im Normalisator $N_G(U)$ von U enthalten. Somit ist $|H| = 23$ nach dem Satz von Lagrange ein Teiler von $|N_G(U)|$. Wegen $U \subseteq N_G(U)$ ist auch $|U| = 11$ ein Teiler von $|N_G(U)|$. Insgesamt ist also $\mathrm{kgV}(11, 23) = 253$ ein Teiler von $|N_G(U)|$, und insbesondere $|N_G(U)| \geq 253$. Weil G auf der Menge der 11-Sylowgruppen transitiv operiert, $N_G(U)$ der Stabilisator von U bezüglich dieser Operation und $\nu_{11} = |G(U)|$ die Bahnlänge ist, gilt $\nu_{11} = (G : N_G(U))$, und wir erhalten

$$\nu_{11} \quad = \quad \frac{|G|}{|N_G(U)|} \quad = \quad \frac{2024}{|N_G(U)|} \quad \leq \quad \frac{2024}{253} \quad = \quad 8.$$

Auf Grund der Sylowsätze gilt außerdem $\nu_{11} \mid (2^3 \cdot 23)$, insgesamt folgt aus der Annahme also $\nu_{11} \mid 8$ und $\nu_{11} \in \{1, 2, 4, 8\}$. Zusammen mit $\nu_{11} \equiv 1 \bmod 11$ und $2, 4, 8 \not\equiv 1 \bmod 11$ folgt $\nu_{11} = 1$. Die Menge $\mathcal{M}_{11}$ ist dann einelementig. Wegen $\{U\} = H(U) \subseteq \mathcal{M}_{11}$ folgt daraus $\mathcal{M}_{11} = H(U)$, d.h. die Operation von H auf $\mathcal{M}_{11}$ ist auch in diesem Fall transitiv.

zu (c) Sei $\bar{G} = G/H$; dies ist eine Gruppe der Ordnung $|\bar{G}| = (G : H) = \frac{|G|}{|H|} = \frac{2024}{23} = 88$. Für jede Primzahl p sei $\bar{\nu}_p$ die Anzahl der p-Sylowgruppen von $\bar{G}$. Auf Grund der Sylowsätze gilt $\bar{\nu}_{11} \mid 8$, also $\bar{\nu}_1 1 \in \{1, 2, 4, 8\}$, und $\bar{\nu}_{11} \equiv 1 \bmod 11$. Wegen $2, 4, 8 \not\equiv 1 \bmod 11$ folgt $\bar{\nu}_{11} = 1$. Sei $\bar{N}$ die einzige 11-Sylowgruppe von $\bar{G}$ und $N = \pi^{-1}(\bar{N})$ das Urbild von $\bar{N}$ unter dem kanonischen Epimorphismus $\pi : G \to \bar{G}$. Wegen dem Zweiten Sylowsatz ist $\bar{N}$ ein Normalteiler von $\bar{G}$, und auf Grund des Korrespondenzsatzes gilt $N \trianglelefteq G$.

Sei nun $M = NH$, das Komplexprodukt von N und H. Mit N und H ist auch M ein Normalteiler von G. Darüber hinaus ist M ein inneres direktes Produkt von N und H. Denn wegen $\mathrm{ggT}(|N|, |H|) = \mathrm{ggT}(11, 23) = 1$ gilt $N \cap H = \{e_G\}$, und wegen $N, H \trianglelefteq G$ sind N und H auch Normalteiler von M. Weil M ein inneres direktes Produkt von N und H ist, gilt $M \cong N \times H$ und $|M| = |N| \cdot |H| = 11 \cdot 23 = 253$. Insgesamt ist M also ein Normalteiler von G der Ordnung 253.

zu (d) Wegen $M \trianglelefteq G$ genügt es zu zeigen, dass M und G/M auflösbare Gruppen sind. Wegen $|G/M| = (G : M) = \frac{|G|}{|M|} = \frac{2024}{253} = 8 = 2^3$ ist G/M eine Gruppe von Primzahlpotenzordnung und also solche auflösbar. Nun beweisen wir noch die Auflösbarkeit von M. Als Normalteiler von G ist $H \subseteq M$ auch ein Normalteiler von M. Als Gruppe von Primzahlordnung ist $|H| = 23$ zyklisch und damit auch auflösbar. Auch die Faktorgruppe M/H ist wegen $|M/H| = (M : H) = \frac{|M|}{|H|} = \frac{253}{23} = 11$ von Pirmzahlordnung und damit auflösbar. Aus der Auflösbarkeit von H und M/H folgt die Auflösbarkeit von M.

Aufgabe H24T1A3

Sei K ein Körper und sei

$$R \quad = \quad \left\{ \sum_{i=0}^{n} a_i x^i \in K[x] \;\middle|\; a_1 = 0 \right\}.$$

(a) Zeigen Sie, dass R ein Teilring (mit Eins) des Polynomrings $K[x]$ über K ist.

(b) Entscheiden Sie begründet, ob $f = x^3 \in R$ irreduzibel ist, und ob $f = x^3 \in R$ prim ist.

(c) Entscheiden Sie begründet, ob R ein faktorieller Ring ist.

(d) Geben Sie ein $a \in R$ an, so dass das Ideal (x^3, a) von R kein Hauptideal ist, und begründen Sie Ihre Wahl.

Lösung:
zu (a) Zu zeigen ist, dass $1 \in R$ gilt, und dass für alle $f, g \in R$ auch $f - g \in R$ und $fg \in R$ erfüllt sind. Offenbar ist 1 tatsächlich in R enthalten, denn dieses Element hat die Form $\sum_{i=0}^{n} a_i x^i$ mit $n = 1$, $a_0 = 1$ und $a_1 = 0$. Seien nun $f, g \in R$ vorgegeben, $f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{j=0}^{n} b_j x^j$ mit $m, n \in \mathbb{N}$, $a_0, ..., a_m, b_1, ..., b_n \in K$ und $a_1 = b_1 = 0$. Setzen wir $r = \max\{m, n\}$, $a_i = 0$ für alle $i \in \mathbb{N}$ mit $i > m$ und $b_j = 0$ für alle $j \in \mathbb{N}$ mit $j > n$ und anschließend $c_j = a_j - b_j$ für alle $j \in \mathbb{N}_0$, dann gilt $f - g = \sum_{j=0}^{r} c_j x^j$ sowie $c_1 = a_1 - b_1 = 0 - 0 = 0$. Dies zeigt, dass $f - g$ in R enthalten ist.

Weiter gilt $fg = \sum_{j=0}^{m+n} d_j x^j$ mit $d_j = \sum_{i=0}^{j} a_{j-i} b_i$. Insbesondere ist $d_1 = a_1 b_0 + a_0 b_1 = 0 \cdot b_0 + a_0 \cdot 0 = 0$. Dies zeigt, dass fg in R enthalten ist.

zu (b) Um zu zeigen, dass x^3 tatsächlich irreduzibel ist, überprüfen wir, dass $x^3 \neq 0$ und $x^3 \notin R^\times$ gilt, und dass für alle $f, g \in R$ aus $x^3 = fg$ jeweils $f \in R^\times$ oder $g \in R^\times$ folgt. Die Ungleichung $x^3 \neq 0$ ist offensichtlich erfüllt. Wäre x^3 in R eine Einheit, dann gäbe es ein $f \in R$ mit $x^3 \cdot f = 1$. Insbesondere wäre x^3 dann eine Einheit im Polynomring $K[x]$. Aus der Vorlesung ist aber bekannt, dass im Polynomring $K[x]$ die Menge der Einheiten mit $K^\times$ übereinstimmt. Somit wäre x^3 in $K[x]$ eine Konstante (ungleich null), was offensichtlich nicht der Fall ist.

Seien nun $f, g \in R$ mit $x^3 = fg$ gegeben und nehmen wir an, dass weder f noch g in R eine Einheit ist. Dann gilt auch $f, g \notin K[x]^\times$, also $f, g \notin K^\times$. Denn wäre $f \in K^\times$, dann wäre auch der Kehrwert f^{-1} in R enthalten, und wegen $f \cdot f^{-1} = 1$ wäre f in R eine Einheit. Ebenso kann $g \in K^\times$ ausgeschlossen werden. Aus $f, g \notin K[x]^\times$ folgt $\mathrm{grad}(f), \mathrm{grad}(g) > 0$. Wegen $\mathrm{grad}(f) + \mathrm{grad}(g) = \mathrm{grad}(fg) = \mathrm{grad}(x^3) = 3$ können wir, nach eventueller Vertauschung von f und g, $\mathrm{grad}(f) = 1$ und $\mathrm{grad}(g) = 2$ annehmen. Als Polynom vom Grad 1 ist f in $K[x]$ ein irreduzibles Element. Weil $K[x]$ ein faktorieller Ring ist, muss f als Teiler von x^3 in $K[x]$ zu einem der irreduziblen Faktoren von x^3 assoziiert sein. Bis auf Assoziierte ist x der einzige irreduzible Faktor von x^3 (mit Vielfachheit 3). Es gilt folglich $f = cx$ für ein $c \in K^\times$. Schreiben wir nun f in der Form $f = \sum_{j=0}^{n} a_j x^j$ mit $n \in \mathbb{N}$ und $a_0, ..., a_n \in K$, dann folgt $a_1 = c \neq 0$. Dies zeigt, dass f nicht in R enthalten ist, im Widerspruch zur Annahme. Der Nachweis der Irreduzibilität von x^3 ist damit abgeschlossen.

Die Gleichung $x^3 \cdot x^3 = x^2 \cdot x^4$ zeigt, dass x^3 in R ein Teiler von $x^2 \cdot x^4$ ist. Wäre x^3 in R ein Primelement, dann müsste x^3 folglich ein Teiler von x^2 oder von x^4 sein. Im ersten Fall würde $x^2 = f \cdot x^3$ für ein $f \in R$ gelten, und daraus würde $2 = \mathrm{grad}(x^2) = \mathrm{grad}(f) + \mathrm{grad}(x^3) \geq 3$ folgt, im Widerspruch zu $2 < 3$. Im zweiten Fall wäre $x^4 = f \cdot x^3$ für ein $f \in R$. Da $K[x]$ ein Integritätsbereich ist, dürfen wir auf $x \cdot x^3 = f \cdot x^3$ die Kürzungsregel anwenden und erhalten $f = x$. Aber wie bereits oben festgestellt, ist kein Polynom der Form cx mit $c \in K^\times$ in R enthalten. Also ist x^3 kein Primelement in R.

zu (c) Laut Vorlesung stimmt in einem faktoriellen Ring die Menge der irreduziblen Elemente mit der Menge der Primelemente überein. Da x^3 nach Teil (b) irreduzibel, aber nicht prim ist, kann R kein faktorieller Ring sein.

zu (d) Offenbar ist x^2 in R enthalten; wir zeigen, dass $I = (x^3, x^2)$ kein Hauptideal in R ist. Nehmen wir an, dass $(x^3, x^2) = (f)$ für ein $f \in R$ gilt. Wegen $x^3, x^2 \in (f)$ gibt es dann $g, h \in R$ mit $x^3 = fg$ und $x^2 = fh$. Auf Grund der Eindeutigkeit der Primfaktorzerlegung in $K[x]$ ist f entweder eine Einheit oder assoziiert zu einem Produkt von Primfaktoren von x^2 in $K[x]$. Da x bis auf Assoziierte der einzige Primfaktor ist, muss also $f = cx^m$ gelten, für ein $c \in K^\times$ und $m \in \{0, 1, 2\}$. Der Fall $m = 1$ ist ausgeschlossen, denn aus $x^2 = cx \cdot h$ würde dann $c^{-1}x = h \in R$ folgen, im Widerspruch zu unserer Feststellung aus Teil (b). Ebenso ist $m = 2$ unmöglich, denn dann wäre $x^3 = cx^2 \cdot g$ und $c^{-1}x = g \in R$. Also bleibt nur $m = 0$ und $f = c \in K^\times$. Aber dann wäre f auch eine Einheit in R und $I = (f)$ in R das Einheitsideal, also insbesondere $1 \in (x^3, x^2)$. Dies ist ebenfalls unmöglich, denn jedes Element u in (x^3, x^2) hat die Form $u = x^3 \cdot v + x^2 \cdot w$ mit $v, w \in R$, und somit $u(0) = 0^3 \cdot v(0) + 0^2 \cdot w(0) = 0 \neq 1$.

Aufgabe H24T1A4

(a) Sei $K|\mathbb{Q}$ eine Körpererweiterung. Zeigen Sie, dass jeder Körperautomorphismus von K ein $\mathbb{Q}$-Automorphismus ist.

(b) Sei K eine endliche Körpererweiterung von $\mathbb{Q}$ und sei $\varphi : K \to K$ ein Körperhomomorphismus. Zeigen Sie, dass φ bijektiv ist.

(c) Geben Sie eine Körpererweiterung K von $\mathbb{Q}$ und einen Körperhomomorphismus $\varphi : K \to K$ an, der nicht bijektiv ist. Begründen Sie dabei Ihre Aussagen.

Lösung:
zu (a) Sei $\sigma : K \to K$ ein Körperautomorphismus. Dann ist σ insbesondere ein Ringhomomorphismus, und somit $\sigma(0) = 0$ und $\sigma(1) = 1$. Durch vollständige Induktion folgt daraus $\sigma(m) = m$ für alle $m \in \mathbb{N}_0$. Denn für $m \in \{0, 1\}$ haben wir die Gleichung gerade überprüft, und setzen wir sie für ein $m \in \mathbb{N}_0$ voraus, dann erhalten wir durch die Homomorphismus-Eigenschaft auch $\sigma(m + 1) = \sigma(m) + \sigma(1) = m + 1$.

Aus der Vorlesung ist bekannt, dass σ als Körperhomomorphismus auch die Gleichung $\sigma(-\alpha) = -\sigma(\alpha)$ für alle $\alpha \in K$ erfüllt, also insbesondere $\sigma(-1) = -\sigma(1) = -1$, und darüber hinaus $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}$ für alle $\alpha \in K^\times$. Sei nun $r \in \mathbb{Q}$ beliebig vorgegeben. Dann gibt es ein $\varepsilon \in \{\pm 1\}$, ein $m \in \mathbb{N}_0$ und ein $n \in \mathbb{N}$ mit $r = \varepsilon \cdot m \cdot n^{-1}$. Die Homomorphismus-Eigenschaft von σ liefert

$$\sigma(r) \quad = \quad \sigma(\varepsilon \cdot m \cdot n^{-1}) \quad = \quad \sigma(\varepsilon) \cdot \sigma(m) \cdot \sigma(n^{-1}) \quad = \quad \varepsilon \cdot m \cdot \sigma(n)^{-1} \quad = \quad \varepsilon \cdot m \cdot n^{-1} \quad = \quad r.$$

Dies zeigt, dass durch σ ein $\mathbb{Q}$-Homomorphismus $K \to K$ gegeben ist. Als Körperautomorphismus ist σ außerdem bijektiv, insgesamt also ein $\mathbb{Q}$-Automorphismus von K.

zu (b) Aus der Vorlesung ist bekannt, dass Körperhomomorphismen stets injektiv sind. Insbesondere ist $\varphi : K \to K$ also eine injektive Abbildung. Da für alle $c \in \mathbb{Q}$ und alle $\alpha, \beta \in K$ auch $\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta)$ und $\varphi(c\alpha) = \varphi(c)\varphi(\alpha) = c\varphi(\alpha)$ gilt (wobei wir im letzten Schritt das Ergebnis aus Teil (a) verwendet haben, dass jeder Körperhomomorphismus $K \to K$ ein $\mathbb{Q}$-Homomorphismus ist), ist φ darüber hinaus ein Endomorphismus des $\mathbb{Q}$-Vektorraums K. Nun ist $n = \dim K = [K : \mathbb{Q}]$ laut Angabe eine (endliche) natürliche Zahl. Der Dimensionssatz für lineare Abbildungen liefert

$$n \quad = \quad \dim \ker(\varphi) + \dim \operatorname{im}(\varphi) \quad ,$$

wobei $\ker(\varphi)$ den Kern und $\operatorname{im}(\varphi)$ das Bild der linearen Abbildung φ bezeichnet. Da φ injektiv ist, gilt $\dim \ker(\varphi) = \dim\{0\} = 0$ und somit $\dim \operatorname{im}(\varphi) = n-0 = n$. Aus $\operatorname{im}(\varphi) \subseteq K$ und $\dim \operatorname{im}(\varphi) = n = \dim K$ folgt $\operatorname{im}(\varphi) = K$. Also ist φ auch surjektiv, insgesamt eine bijektive Abbildung.

zu (c) Sei $K = \mathbb{Q}(t)$ der rationale Funktionenkörper über $\mathbb{Q}$, also der Quotientenkörper des Polynomrings $\mathbb{Q}[t]$. Auf Grund der universellen Eigenschaft des Polynomrings gibt es einen Ringhomomorphismus $\psi : \mathbb{Q}[t] \to \mathbb{Q}(t)$ mit $\psi(c) = c$ für alle $c \in \mathbb{Q}$ und $\psi(t) = t^2$. Ein beliebiges Element $f \in \mathbb{Q}[t]$ wird durch ψ offenbar auf das Polynom $f(t^2)$ abgebildet. Dies zeigt insbesondere, dass ψ die Elemente aus $\mathbb{Q}[t] \setminus \{0\}$ auf Einheiten des Rings $\mathbb{Q}(t)$ abbildet, denn $\mathbb{Q}(t)$ ist ein Körper, und die Einheiten in $\mathbb{Q}(t)$ sind somit genau die Elemente ungleich null. Auf Grund der universellen Eigenschaft des Quotientenkörpers existiert damit ein Ringhomomorphismus $\varphi : \mathbb{Q}(t) \to \mathbb{Q}(t)$ mit $\varphi(f/g) = \psi(f)\psi(g)^{-1}$ für alle $f \in \mathbb{Q}[t]$ und $g \in \mathbb{Q}[t] \setminus \{0\}$. Als Ringhomomorphismus zwischen Körpern ist φ ein Körperhomomorphismus.

Wir zeigen nun, dass φ nicht surjektiv, und damit auch nicht bijektiv ist. Wäre φ surjektiv, dann gäbe es ein Element $u \in \mathbb{Q}(t)$ mit $\varphi(u) = t$. Schreiben wir $u = f/g$ mit $f \in \mathbb{Q}[t]$ und $g \in \mathbb{Q}[t] \setminus \{0\}$, dann folgt

$$t \quad = \quad \varphi(u) \quad = \quad \varphi(f/g) \quad = \quad \psi(f)\psi(g)^{-1} \quad = \quad \frac{f(t^2)}{g(t^2)}$$

und somit $tg(t^2) = f(t^2)$. Aber der Grad des Polynoms $tg(t^2)$ ist ungerade, und der Grad von $f(t^2)$ ist gerade, wodurch eine solche Gleichung ausgeschlossen ist.

Aufgabe H24T1A5

(a) Zeigen Sie: Ist $L|K$ eine Körpererweiterung von Grad 2 und ist $\mathrm{char}(K) \neq 2$, so ist $L|K$ eine Galois-Erweiterung.

(b) Geben Sie begründet eine Körpererweiterung $L|K$ vom Grad 2 an, die nicht galois'sch ist.

(c) Geben Sie für jedes $n \in \mathbb{N}$ mit $n \geq 3$ eine Körpererweiterung $K|\mathbb{Q}$ vom Grad n an, die nicht galois'sch ist, und geben Sie für Ihre Beispiele die Anzahl der Körperautomorphismen von K an. Begründen Sie dabei Ihre Aussagen.

Lösung:
zu (a) Sei $L|K$ eine Körpererweiterung mit $[L : K] = 2$. Dann ist $L|K$ normal. Ist nämlich $f \in K[x]$ ein über K irreduzibles Polynom mit einer Nullstelle $\alpha \in L$, dann ist $K(\alpha)$ ein Zwischenkörper von $L|K$, und folglich

$$2 \quad = \quad [L : K] \quad = \quad [L : K(\alpha)] \cdot [K(\alpha) : K] \quad = \quad [L : K(\alpha)] \cdot \mathrm{grad}(f).$$

Daraus folgt $\mathrm{grad}(f) \in \{1, 2\}$. Wegen $f(\alpha) = 0$ ist $x-\alpha$ ein Teiler von f in $L[x]$. Es gilt also $f = (x-\alpha)\cdot g$ für ein $g \in L[x]$. Wegen $\mathrm{grad}(f) \in \{1, 2\}$ gilt $\mathrm{grad}(g) \in \{0, 1\}$. Dies zeigt, dass f über L in Linearfaktoren zerfällt. Damit ist insgesamt nachgewiesen, dass $L|K$ eine normale Erweiterung ist. (Das Resultat, dass jede Körpererweiterung vom Grad 2 normal ist, wird meistens in der Vorlesung behandelt. Aus der Aufgabenstellung geht nicht klar hervor, ob man das hier benutzen darf. Normalerweise dürfen alle Ergebnisse aus der Vorlesung verwendet werden.)

Nun muss noch gezeigt werden, dass $L|K$ separabel ist, denn daraus folgt insgesamt, dass es sich bei $L|K$ um eine Galois-Erweiterung handelt. Dafür wiederum genügt es zu zeigen, dass jedes $\alpha \in L \setminus K$ separabel über K ist. Sei also α ein solches Element und $f \in K[x]$ das Minimalpolynom von α über K. Da f als Minimalpolynom irreduzibel über K ist, folgt $\mathrm{grad}(f) \in \{1, 2\}$ aus der Rechnung von oben. Im Fall $\mathrm{grad}(f) = 1$ wäre $x - \alpha = f \in K[x]$ und somit $\alpha \in K$. Also muss $\mathrm{grad}(f) = 2$ sein, d.h. $f = x^2 + ax + b$ für geeignete $a, b \in K$. Wäre α nicht separabel über K, dann wäre $f \in K[x]$ kein separables Polynom. Es wäre dann α eine doppelte Nullstelle von f und damit auch eine Nullstelle von $f' = 2x + a$. Wegen $\mathrm{char}(K) \neq 2$ ist aber $2 \neq 0$ in K. Aus $2\alpha + a = f'(\alpha) = 0$ würde dann $\alpha = -\frac{1}{2}a \in K$ folgen, erneut im Widerspruch zu $\alpha \notin K$.

zu (b) Sei $L = \mathbb{F}_2(t)$ der rationale Funktionenkörper über $\mathbb{F}_2$, also der Quotientenkörper des Polynomrings $\mathbb{F}_2[t]$, und $K = \mathbb{F}_2(t^2)$. Dann gilt $K(t) = \mathbb{F}_2(t^2, t) = \mathbb{F}_2(t) = L$. Um zu zeigen, dass $[L : K] = 2$ ist, genügt es zu überprüfen, dass $f = x^2 - t^2 \in K[x]$ das Minimalpolynom von t über K ist, denn darauf folgt $[L : K] = [K(t) : K] = \mathrm{grad}(f) = 2$. Offenbar ist f normiert, und es gilt $f(t) = t^2 - t^2 = 0$. Nehmen wir nun an, f wäre über K reduzibel. Wegen $\mathrm{grad}(f) = 2$ wäre die Nullstelle t von f dann in K enthalten. Es gäbe dann Polynome $u, v \in \mathbb{F}_2[t]$ mit $v \neq 0$ und $t = u(t^2)/v(t^2)$ (weil jedes Element aus K in dieser Form dargestellt werden kann). Daraus würde $tv(t^2) = u(t^2)$ folgen, aber eine solche Gleichung ist ausgeschlossen, weil der Polynomgrad von $u(t^2)$ gerade und der von $tv(t^2)$ ungerade ist, vgl. H24T1A4 (c). Also ist f über K irreduzibel.

zu (c) Für jedes $n \in \mathbb{N}$ mit $n \geq 3$ sei $\alpha_n = \sqrt[n]{2} \in \mathbb{R}^+$ und $K_n = \mathbb{Q}(\alpha_n)$. Wir zeigen, dass jeweils $[K_n : \mathbb{Q}] = n$ gilt, und dass die Erweiterung $K_n|\mathbb{Q}$ nicht normal, und damit auch nicht galois'sch ist. Das Polynom $f_n = x^n - 2 \in \mathbb{Q}[x]$ ist normiert, hat α_n als Nullstelle, und nach dem Eisenstein-Kriterium (angewendet auf die Primzahl $p = 2$) ist es in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel. Es handelt sich also um das

Minimalpolynom von α_n über $\mathbb{Q}$, und daraus folgt $[K_n : \mathbb{Q}] = [\mathbb{Q}(\alpha_n) : \mathbb{Q}] = \text{grad}(f_n) = n$, für alle $n \in \mathbb{N}$.

Nehmen wir nun an, dass $K_n|\mathbb{Q}$ eine normale Erweiterung ist. Weil f_n über $\mathbb{Q}$ irreduzibel ist und mit α_n in K_n eine Nullstelle besitzt, müsste f_n über K_n in Linearfaktoren zerfallen. Dies würde bedeuten, dass alle komplexen Nullstellen von f_n bereits in K_n enthalten sind. Wegen $\alpha_n \in \mathbb{R}$ gilt $K_n \subseteq \mathbb{R}$; laut unserer Annahme wären also alle Nullstellen reell. Bezeichnet ζ_n die primitive n-te Einheitswurzel $e^{2\pi i/n}$, dann ist auch $\alpha'_n = \zeta_n\alpha_n$ eine komplexe Nullstelle von f_n, wegen $f_n(\alpha'_n) = (\zeta_n\alpha_n)^n - 2 = \zeta_n^n\alpha_n^n - 2 = 1 \cdot 2 - 2 = 0$. Laut Annahme wäre also $\alpha'_n \in \mathbb{R}$, und wegen $\alpha_n \in \mathbb{R}^+$ würde auch $\zeta_n = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ in $\mathbb{R}$ liegen. Es wäre dann $\sin(\frac{2\pi}{n}) = 0$. Aber aus $n \geq 3$ folgt $0 < \frac{2\pi}{n} < \pi$ und $\sin(\frac{2\pi}{n}) > 0$. Unsere Annahme hat also zu einem Widerspruch geführt, und folglich ist die Erweiterung $K_n|\mathbb{Q}$ nicht normal.

Sei nun $G_n = \text{Aut}(K_n)$; wir zeigen, dass für ungerades n jeweils $|G_n| = 1$ gilt, und $|G_n| = 2$ für gerades n. Aus der Vorlesung (oder durch Aufgabe H24T1A4) ist bekannt, dass $\text{Aut}(K_n) = \text{Aut}_{\mathbb{Q}}(K_n) = \text{Hom}_{\mathbb{Q}}(K_n)$ gilt. Auf Grund des Fortsetzungssatzes und wegen $K_n = \mathbb{Q}(\alpha_n)$ stimmt die Anzahl der Elemente von $\text{Hom}_{\mathbb{Q}}(K_n)$ mit der Anzahl der Nullstellen des Minimalpolynoms $\mu_{\alpha_n,\mathbb{Q}} = f_n$ in K_n überein.

Zunächst überprüfen wir, dass die Menge der Nullstellen von f_n in $\mathbb{C}$ durch $N_n = \{\zeta_n^k\alpha_n \mid 0 \leq k < n\}$ gegeben ist. Weil ζ_n in $\mathbb{C}^\times$ ein Element der Ordnung n ist, sind die Elemente ζ_n^k mit $0 \leq k < n$ alle verschieden. Wegen $\alpha_n \neq 0$ folgt daraus, dass N_n aus n verschiedenen Elementen besteht, und wegen $f_n(\zeta_n^k\alpha_n) = (\zeta_n^k\alpha_n)^n - 2 = (\zeta_n^n)^k\alpha_n^n - 2 = 1^k \cdot 2 - 1 = 0$ sind dies alles Nullstellen von f_n. Die Anzahl der komplexen Nullstellen von f_n ist mit Vielfachheiten genau gleich $\text{grad}(f_n) = n$; dies zeigt, dass N_n tatsächlich genau die Menge der komplexen Nullstellen von f_n ist.

Als nächstes ermitteln wir, viele der komplexen Nullstellen jeweils in K_n liegen; wie oben gezeigt, ist dies dann die gesuchte Anzahl $|G_n|$. Für jedes $n \in \mathbb{N}$ mit $n \geq 3$ und $0 \leq k < n$ gilt jeweils

$$\zeta_n^k\alpha_n \quad = \quad \alpha_n \cos(\frac{2\pi k}{n}) + i\alpha_n \sin(\frac{2\pi k}{n}).$$

Die Nullstellen der Sinusfunktion sind bekanntlich genau die ganzzahligen Vielfachen von π. Ist also $\frac{2k}{n}$ keine ganze Zahl, dann ist $\zeta_n^k\alpha_n$ also nicht reell, und erst recht gilt $\zeta_n^k\alpha_n \notin K_n$. Wegen $k \in \mathbb{Z}$ und $0 \leq k < n$ ist $\frac{2k}{n} \in \mathbb{Z}$ nur für $k \in \{0, \frac{1}{2}n\}$ möglich. Ist n ungerade, dann $\frac{2k}{n} \in \mathbb{Z}$ also nur für $k = 0$ erüllt, und somit $|G_n| \leq 1$. Ist n gerade, so gilt $\frac{2k}{n} \in \mathbb{Z}$ genau für $k \in \{0, \frac{1}{2}n\}$, also ist hier $|G_n| \leq 2$. Andererseits gilt für $k = 0$ jeweils $\zeta_n^k\alpha_n = \alpha_n \in K_n$, und für n gerade, $k = \frac{1}{2}n$ ist $\zeta_n^k = \cos(\pi) + i\sin(\pi) = -1$ und ebenfalls $\zeta_n^k\alpha_n = -\alpha_n \in K_n$. Es ist also tatsächlich $|G_n| = 1$ für ungerades und $|G_n| = 2$ für gerades n, wie oben angegeben.

Aufgabe H24T2A1

Sei R ein Ring und eine Folge $(a_n)_{n\geq 0}$ von Elementen von R rekursiv definiert wie folgt:

$$a_0 = a_1 = 1, \quad a_{n+2} = 2a_{n+1} + a_n.$$

(a) Sei $\alpha \in R$ mit $\alpha^2 = 2$. Zeigen Sie, dass dann für alle $n \geq 0$ gilt

$$2a_n \quad = \quad (1+\alpha)^n + (1-\alpha)^n.$$

(b) Sei p eine ungerade Primzahl, so dass es ein $\alpha \in R = \mathbb{F}_p$ (der Körper mit p Elementen) gibt mit $\alpha^2 = \bar{2}$. Zeigen Sie, dass die Folge $(a_n)_{n\geq 1}$ periodisch ist mit einer minimalen Periode, die $p-1$ teilt.

(c) Bestimmen Sie die kleinste Zahl $k > 0$, so dass für $R = \mathbb{F}_7$ gilt $a_{n+k} = a_n$ für alle $n \geq 0$.

(d) Zeigen Sie, dass es für $R = \mathbb{Z}$ keine ganzen Zahlen $m, n \geq 0$ mit der Eigenschaft $a_n = m^6 + 4$ gibt.

Lösung:
zu (a) Wir beweisen die Gleichung durch vollständige Induktion für alle $n \in \mathbb{N}_0$. Es gilt sowohl $(1+\alpha)^0 + (1-\alpha)^0 = 1 + 1 = 2 = 2 \cdot a_0$ als auch $(1+\alpha)^1 + (1-\alpha)^1 = 2 = 2 \cdot a_1$, also ist die Gleichung für $n \in \{0, 1\}$ erfüllt. Sei nun $n \in \mathbb{N}_0$ vorgegeben, und setzen wir die Gleichung für alle Werte $m \in \mathbb{N}_0$ mit $m < n$ voraus. Dann erhalten wir einerseits

$$2a_n \quad = \quad 4a_{n-1} + 2a_{n-2} \quad = \quad 2(1+\alpha)^{n-1} + 2(1-\alpha)^{n-1} + (1+\alpha)^{n-2} + (1-\alpha)^{n-2} \quad =$$
$$(1+\alpha)^{n-2} \cdot (2(1+\alpha)+1) + (1-\alpha)^{n-2} \cdot (2(1-\alpha)+1) \quad = \quad (1+\alpha)^{n-2} \cdot (3+2\alpha) + (1-\alpha)^{n-2} \cdot (3-2\alpha)$$

und wegen $\alpha^2 = 2$ andererseits

$$(1+\alpha)^n + (1-\alpha)^n \quad = \quad (1+\alpha)^{n-2} \cdot (1+\alpha)^2 + (1-\alpha)^{n-2} \cdot (1-\alpha)^2 \quad =$$
$$(1+\alpha)^{n-2} \cdot (1+2\alpha+\alpha^2) + (1-\alpha)^{n-2} \cdot (1-2\alpha+\alpha^2) \quad = \quad (1+\alpha)^{n-2} \cdot (3+2\alpha) + (1-\alpha)^{n-2} \cdot (3-2\alpha) \quad ,$$

insgesamt also $2a_n = (1+\alpha)^n + (1-\alpha)^n$.

zu (b) Vorweg bemerken wir: Ist $k \in \mathbb{N}$ die minimale Periode der Folge $(a_n)_{n\geq 0}$ und $\ell \in \mathbb{N}$ eine beliebige Periode (also eine Zahl mit $a_{n+\ell} = a_n$ für alle $n \in \mathbb{N}_0$, dann muss ℓ ein Vielfaches von k sein. Denn nehmen wir an, dies ist nicht der Fall. Durch Division mit Rest erhalten wir $q, r \in \mathbb{N}_0$ mit $0 < r < k$, so dass $\ell = qk + r$ erfüllt ist. Für jedes $n \in \mathbb{N}_0$ gilt dann $a_{n+r} = a_{n+\ell-qk} = a_{n+\ell} = a_n$. Somit wäre r eine noch kürzere Periode, im Widerspruch zur Minimalität von k.

Da p ungerade ist, ist $\bar{2}$ in $\mathbb{F}_p$ invertierbar. Nach Teil (a) gilt somit $a_n = \bar{2}^{-1}(\bar{1}+\alpha)^n + \bar{2}^{-1}(\bar{1}-\alpha)^n$ für alle $n \in \mathbb{N}_0$. Wegen $\alpha^2 = \bar{2}$ und $p \geq 3$ ist $\alpha \neq \bar{1}$ und somit $\bar{1} - \alpha \in \mathbb{F}_p^\times$. Ebenso ist $\bar{1} + \alpha \in \mathbb{F}_p^\times$ enthalten, denn andernfalls wäre $\alpha = -\bar{1}$ und $\bar{2} = \alpha^2 = \bar{1}$, was in $\mathbb{F}_p$ (wegen $p > 1$) ausgeschlossen ist.

Zunächst betrachten wir den Fall, dass auch das Element $\bar{1} + \alpha$ in $\mathbb{F}_p^\times$ liegt. Wegen $|\mathbb{F}_p^\times| = p - 1$ gilt dann $(\bar{1}+\alpha)^{p-1} = \bar{1}$ und $(\bar{1}-\alpha)^{p-1} = \bar{1}$, und wir erhalten für alle $n \in \mathbb{N}_0$ jeweils

$$a_{n+p} \quad = \quad \bar{2}^{-1}(\bar{1}+\alpha)^{n+p} + \bar{2}^{-1}(\bar{1}-\alpha)^{n+p} \quad = \quad \bar{2}^{-1}(\bar{1}+\alpha)^n \cdot (\bar{1}+\alpha)^p + \bar{2}^{-1}(\bar{1}-\alpha)^n \cdot (\bar{1}-\alpha)^p$$
$$= \quad \bar{2}^{-1}(\bar{1}+\alpha)^n \cdot \bar{1} + \bar{2}^{-1}(\bar{1}-\alpha)^n \cdot \bar{1} \quad = \quad a_n.$$

Also ist $p-1$ eine Periode der Folge $(a_n)_{n\geq 0}$, und die minimale Periode ist, wie oben festgestellt wurde, ein Teiler davon.

zu (c) Nach Teil (b) ist die minimale Periode k ein Teiler von 6, also $k \in \{1, 2, 3, 6\}$. In $\mathbb{F}_7$ gilt $a_0 = a_1 = \bar{1}$, und die Rekursionsformel liefert $a_2 = \bar{3}$, $a_3 = \bar{0}$, $a_4 = \bar{3}$, $a_5 = \bar{6}$, $a_6 = a_7 = \bar{1}$. Wegen $a_1 \neq a_2$, $a_1 \neq a_3$ und $a_1 \neq a_4$ ist $k \in \{1, 2, 3\}$ ausgeschlossen. Also ist die minimale Periode gleich 6. (Dass $a_{n+6} = a_n$ für alle $n \in \mathbb{N}_0$ gilt, lässt sich natürlich wegen $a_6 = a_0$ und $a_7 = a_1$ auch mit Hilfe der Rekursionsformel durch vollständige Induktion beweisen.)

zu (d) Nehmen wir an, dass es $m, n \in \mathbb{N}_0$ mit $a_n = m^6 + 4$ gibt. Sei $(b_n)_{n\geq 0}$ die entsprechende Folge in $\mathbb{F}_7$. Wegen $b_0 = a_0 + 7\mathbb{Z}$, $b_1 = a_1 + 7\mathbb{Z}$ und auf Grund der Rekursionsformeln $a_{n+2} = 2a_{n+1} + a_n$, $b_{n+2} = \bar{2}b_{n+1} + b_n$ liefert ein einfacher Induktionsbeweis $b_n = a_n + 7\mathbb{Z}$ für alle $n \in \mathbb{N}_0$. Insbesondere wäre also $b_n = \bar{m}^6 + \bar{4}$, mit $\bar{m} = m + 7\mathbb{Z}$. Wir unterscheiden nun zwei Fälle. Ist $\bar{m} = \bar{0}$, dann ist $b_n = \bar{4}$; andernfalls liegt $\bar{m}$ in $\mathbb{F}_7^\times$, und weil dies eine Gruppe der Ordnung 6 ist, folgt $b_n = \bar{m}^6 + \bar{4} = \bar{1} + \bar{4} = \bar{5}$. Aber anhand der Werte $b_0, ..., b_5$, die wir unter (c) berechnet haben, und auf Grund der Periodenlänge $\bar{6}$ der Folge $(b_n)_{n\geq 0}$, ist erkennbar, dass weder $\bar{4}$ noch $\bar{5}$ in der Folge vorkommt. Die Annahme hat also zu einem Widerspruch geführt.

Aufgabe H24T2A2

(a) Bestimmen Sie die ganze Zahl $a \in \{0, ..., 82\}$ mit $50^{247} \equiv a \bmod 83$.

(b) Der Satz von Wilson besagt, dass $(p-1)! \equiv -1 \bmod p$ für jede Primzahl p gilt. Bestimmen Sie hiermit die ganze Zahl $a \in \{0, ..., 100\}$ mit $98! \equiv a \bmod 101$.
Hinweis: Sie dürfen den Satz von Wilson ohne Beweis benutzen.

(c) Im Folgenden bezeichne φ die Eulersche φ-Funktion. Beweisen oder widerlegen Sie:

(i) für alle $m, n \in \mathbb{N}$ mit $n > m$ gilt $\varphi(n) > \varphi(m)$;

(ii) für alle $n \in \mathbb{N}$ gilt $\varphi(2n) \geq \varphi(n)$;

(iii) für alle $n \in \mathbb{N}$ gilt $\varphi(n) \mid \varphi(n^2)$.

Lösung:
zu (a) Weil 83 eine Primzahl ist, gilt $c^{82} \equiv 1 \bmod 83$ für alle $c \in \mathbb{Z}$ mit $83 \nmid c$, nach dem Kleinen Satzes von Fermat. Wegen $83 \nmid 50$ erhalten wir mit Hilfe der Rechenregeln für Kongruenzen

$$50^{247} \equiv 50^{3 \cdot 82+1} \equiv (50^{82})^3 \cdot 50 \equiv 1^3 \cdot 50 \equiv 50 \bmod 83.$$

Also ist $a = 50$ die gesuchte Zahl.

zu (b) Die Zahl 101 ist eine Primzahl, und im Körper $\mathbb{F}_{101}$ gilt $\bar{2} \cdot \overline{50} = \overline{100} = -\bar{1}$, also $(-\bar{2})^{-1} = \overline{50}$ und $\overline{99}^{-1} = (-\bar{2})^{-1} = \overline{50}$. Daraus folgt $50 \cdot 99 \equiv 1 \bmod 101$, und mit der Kongruenz $100! \equiv -1 \bmod 101$ aus dem Satz von Wilson erhalten wir

$$98! \equiv 1 \cdot (98!) \equiv 50 \cdot 99 \cdot 98! \equiv 50 \cdot 99! \equiv 50 \cdot (-1) \cdot (-1) \cdot 99! \equiv 50 \cdot (-1) \cdot 100 \cdot 99! \equiv 50 \cdot (-1) \cdot 100!$$
$$\equiv 50 \cdot (-1) \cdot (-1) \equiv 50 \bmod 101.$$

Also ist auch hier $a = 50$ die Lösung.

zu (c) (i) Die Aussage ist falsch, denn es ist $6 > 3$, aber $\varphi(6) = 2 = \varphi(3)$.

zu (c) (ii) Diese Aussage ist richtig. Für den Nachweis stellen wir eine beliebige Zahl $n \in \mathbb{N}$ in der Form $n = 2^r \cdot m$ dar, wobei $r \in \mathbb{N}_0$ und $m \in \mathbb{N}$ ungerade ist. Ist $r = 0$, dann sind 2 und n teilerfremd, und es folgt $\varphi(2n) = \varphi(2)\varphi(n) = 1 \cdot \varphi(n) \geq \varphi(n)$. Ansonsten gilt $\varphi(2n) = \varphi(2^{r+1}m) = \varphi(2^{r+1}) \cdot \varphi(m) = 2^r \cdot \varphi(m) \geq 2^{r-1} \cdot \varphi(m) = \varphi(2^r)\varphi(m) = \varphi(n)$, also ist die Ungleichung hier ebenfalls erfüllt.

zu (c) (iii) Auch diese Aussage ist richtig. Sei $n \in \mathbb{N}$ vorgegeben und $n = \prod_{j=1}^{r} p_j^{e_j}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, r verschiedenen Primzahlen $p_1, ..., p_r$ und $e_1, ..., e_r \in \mathbb{N}$. Dann gilt

$$\varphi(n) \quad = \quad \prod_{j=1}^{r} \varphi(p_j^{e_j}) \quad = \quad \prod_{j=1}^{r} p_j^{e_j-1}(p_j - 1)$$

und

$$\varphi(n^2) \quad = \quad \prod_{j=1}^{r} \varphi(p_j^{2e_j}) \quad = \quad \prod_{j=1}^{r} p_j^{2e_j-1}(p_j - 1).$$

Für $1 \leq j \leq r$ gilt jeweils $2e_j - 1 = e_j + e_j - 1 \geq e_j + 1 - 1 = e_j \geq e_j - 1$. Der Faktor $p_j^{e_j-1}(p_j - 1)$ ist also jeweils ein Teiler des Faktors $p_j^{2e_j-1}(p_j - 1)$, und somit ist $\varphi(n)$ ein Teiler von $\varphi(n^2)$.

Aufgabe H24T2A3

(a) Es sei $n \in \mathbb{N}$ und es sei G eine einfache Untergruppe der symmetrischen Gruppe S_n mit $|G| > 2$. Zeigen Sie, dass G bereits eine Untergruppe der alternierenden Gruppe A_n ist.

(b) Sei G eine einfache Gruppe der Ordnung 90. Zeigen Sie, dass G zu einer Untergruppe der alternierenden Gruppe A_6 isomorph ist.

(c) Zeigen Sie, dass es keine einfache Gruppe der Ordnung 90 gibt.

Lösung:

zu (a) Aus der Vorlesung ist bekannt, dass durch die Signumsfunktion ein Homomorphismus $\operatorname{sgn} : S_n \to \{\pm 1\}$ gegeben ist. Sei $\varphi : G \to \{\pm 1\}$ dessen Einschränkung auf die Untergruppe G von S_n. Nehmen wir an, dass G keine Teilmenge von A_n ist. Dann existiert ein $\sigma \in G$ mit $\varphi(\sigma) = \operatorname{sgn}(\sigma) = -1$. Setzen wir $N = \ker(\varphi)$, dann ist N (als Kern eines Homomorphismus) ein Normalteiler von G. Wegen $\varphi(\sigma) \neq 1$ ist $\sigma \notin N$ und somit $N \subsetneq G$. Aber auch $N = \{\mathrm{id}\}$ ist ausgeschlossen. Denn in diesem Fall wäre φ injektiv und somit $|\varphi(G)| = |G| > 2$, was aber wegen $\varphi(G) \subseteq \{\pm 1\}$ und $|\{\pm 1\}| = 2$ unmöglich ist. Insgesamt gilt unter unserer Annahme von oben also $\{\mathrm{id}\} \subsetneq N \subsetneq G$. Aber dies steht im Widerspruch zur Voraussetzung, dass G einfach ist. Also ist G in A_n enthalten.

zu (b) Wir erhalten diesen Isomorphismus, indem wir die Gruppe G auf ihren 5-Sylowgruppen operieren lassen. Die Primfaktorzerlegung der Zahl 90 ist gegeben durch $90 = 2 \cdot 3^2 \cdot 5$. Für die Anzahl ν_5 der 5-Sylowgruppen gilt nach dem Dritten Sylowsatz $\nu_5 \mid 18$, also $\nu_5 \in \{1, 2, 3, 6, 9, 18\}$, und außerdem $\nu_5 \equiv 1 \bmod 5$. Wegen $2, 3 \not\equiv 1 \bmod 5$, $9 \equiv 4 \not\equiv 1 \bmod 5$ und $18 \equiv 3 \not\equiv 1 \bmod 5$ folgt $\nu_5 \in \{1, 6\}$. Im Fall $\nu_5 = 1$ wäre die einzige 5-Sylowgruppe, die wir mit P bezeichnen, auf Grund des Zweiten Sylowsatzes ein Normalteiler von G, und wegen $1 < |P| = 5 < |G|$ wäre $\{e\} \subsetneq P \subsetneq G$. Dies würde der Einfachheit von G widersprechen. Also muss $\nu_5 = 6$ gelten.

Sei X die Menge der 5-Sylowgruppen von G. Laut Vorlesung liefert die Operation von G auf X einen Homomorphismus $\varphi : G \to \operatorname{Per}(X)$, der durch $\varphi(g)(P) = g \cdot P = gPg^{-1}$ für alle $g \in G$ und $P \in X$ definiert ist, wobei $\cdot$ die Operation von G auf X durch Konjugation bezeichnet. Wir zeigen, dass dieser Homomorphismus injektiv ist. Angenommen, dies ist nicht der Fall. Dann ist $N = \ker(\varphi)$ ein Normalteiler von G mit $\{e\} \subsetneq N$, für den außerdem $N \subsetneq G$ gilt. Denn andernfalls wäre $\varphi(g) = \mathrm{id}_X$ für alle $g \in G$, also $gPg^{-1} = \varphi(g)(P) = \mathrm{id}_X(P) = P$ für alle $g \in G$ und $P \in X$, also jede 5-Sylowgruppe ein Normalteiler von G. Dies würde laut Zweiten Sylowsatz aber $\nu_5 = 1$ implizieren, im Widerspruch zu $\nu_5 = 6$. So also erhalten wir $\{e\} \subsetneq N \subsetneq G$, was der Einfachheit von G widerspricht. Damit ist die Injektivität von φ nachgewiesen.

Wegen $|X| = \nu_5 = 6$ existiert ein Isomorphismus $\iota : \operatorname{Per}(X) \to S_6$. Durch $\psi = \iota \circ \varphi$ ist dann ein injektiver Homomorphismus $G \to S_6$ definiert, und G ist somit isomorph zur Untergruppe $\psi(G)$ von S_6. Wegen $|G| = 90 > 2$ können wir das Ergebnis aus Teil (a) anwenden und kommen zu dem Ergebnis, dass G sogar isomorph zu einer Untergruppe von A_6 ist.

zu (c) Nehmen wir an, dass G eine einfache Gruppe der Ordnung 90 ist. Nach Teil (b) ist G isomorph zu einer Untergruppe von A_6. Wir können an Stelle von G somit auch diese Untergruppe betrachten und somit direkt $G \leq A_6$ annehmen. Es ist $|A_6| = \frac{1}{2} \cdot 6! = \frac{1}{2} \cdot 720 = 360$ und somit $(A_6 : G) = \frac{|A_6|}{|G|} = \frac{360}{90} = 4$. Laut Vorlesung liefert die Operation von G auf der Menge A_6/G der vierelementigen Linksnebenklassen von G in A_6 einen Homomorphismus $\varphi : A_6 \to \operatorname{Per}(A_6/G)$ gegeben durch $\varphi(\sigma)(\tau G) = (\sigma\tau)G$ für alle $\sigma, \tau \in A_6$. Wegen $|A_6/G| = (A_6 : G) = 4$ existiert außerdem ein Isomorphismus $\iota : \operatorname{Per}(A_6/G) \to S_4$, so dass wir durch $\psi = \iota \circ \varphi$ einen Homomorphismus $A_6 \to S_4$ erhalten.

Sei $N = \ker(\psi)$. Laut Vorlesung ist die Gruppe A_6 einfach und somit nur $N = \{\mathrm{id}\}$ oder $N = A_6$ möglich. Im Fall $N = A_6$ wäre $\psi(\sigma) = \mathrm{id}$ und somit auch $\varphi(\sigma) = \mathrm{id}_{A_6/G}$ für alle $\sigma \in A_6$. Aber dann würde $\sigma G = (\sigma \circ \mathrm{id})G = \varphi(\sigma)(\mathrm{id}\, G) = \varphi(\sigma)(G) = \mathrm{id}_{A_6/G}(G) = G$ und $\sigma \in G$ für alle $\sigma \in A_6$ gelten. Aber dies ist wegen $(A_6 : G) = 4 > 1$ offenbar nicht der Fall. Betrachten wir nun die Möglichkeit $N = \{\mathrm{id}\}$. Dann wäre ψ injektiv und A_6 somit isomorph zur Untergruppe $\psi(A_6)$ von S_4. Aber auch dies ist wegen $|A_6| = 360 > 24 = |S_4|$ unmöglich. Unsere Annahme, dass eine einfache Gruppe der Ordnung 90 existiert, hat also zu einem Widerspruch geführt.

Aufgabe H24T2A4

Im Folgenden sei $R = \mathbb{Z} + i\mathbb{Z}$ der Ring der Gauß'schen Zahlen. Ohne Beweis darf benutzt werden, dass dies ein euklidischer Ring bezüglich der Normabbildung

$$N : R \setminus \{0\} \to \mathbb{N}, \quad x + iy \mapsto x^2 + y^2$$

und somit insbesondere ein Hauptidealring und ein faktorieller Ring ist.

(a) Bestimmen Sie alle $a \in R$ mit $N(a) \leq 5$.

(b) Schreiben Sie mit Hilfe der Teilaufgabe (a) jede der ganzen Zahlen aus $\{2, 3, 4, 5, 6\}$ als Produkt irreduzibler Elemente in R.

(c) Bestimmen Sie ein $d \in R$ mit $(d) = (5 + 10i, 1 + 3i)$. Zeigen Sie, dass $R/(d)$ ein Körper ist.

Lösung:
zu (a) Jedes $a \in R$ hat die Form $a = u + iv$ mit $u, v \in \mathbb{Z}$, und es ist jeweils $N(a) = u^2 + v^2$. Offenbar ist $N(a) = 0$ äquivalent zu $u^2 + v^2 = 0$ und $u = v = 0$, also ist 0 das einzige Element mit Norm 0. Ebenso erhält man

$$N(a) = 1 \quad \Leftrightarrow \quad u^2 + v^2 = 1 \quad \Leftrightarrow \quad (u, v) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$$
$$\Leftrightarrow \quad a \in \{\pm 1, \pm i\}$$

$$N(a) = 2 \quad \Leftrightarrow \quad u^2 + v^2 = 2 \quad \Leftrightarrow \quad u^2 = v^2 = 1 \quad \Leftrightarrow \quad (u, v) \in \{(1, 1), (-1, 1), (1, 1), (1, -1)\}$$
$$\Leftrightarrow \quad a \in \{1 + i, 1 - i, -1 + i, -1 - i\}$$

$$N(a) = 4 \quad \Leftrightarrow \quad u^2 + v^2 = 4 \quad \Leftrightarrow \quad \{u^2, v^2\} = \{0, 4\} \quad \Leftrightarrow \quad (u, v) \in \{(2, 0), (-2, 0), (0, 2), (0, -2)\}$$
$$\Leftrightarrow \quad a \in \{\pm 2, \pm 2i\}$$

$$N(a) = 5 \quad \Leftrightarrow \quad u^2 + v^2 = 5 \quad \Leftrightarrow \quad \{u^2, v^2\} = \{1, 4\} \quad \Leftrightarrow$$
$$(u, v) \in \{(2, 1), (-2, 1), (2, -1), (-2, -1), (1, 2), (-1, 2), (1, -2), (-1, -2)\} \quad \Leftrightarrow$$
$$a \in \{2 + i, -2 + i, 2 - i, -2 - i, 1 + 2i, -1 + 2i, 1 - 2i, -1 - 2i\}.$$

Die Gleichung $u^2 + v^2 = 3$ besitzt keine Lösung mit $u, v \in Z$. Insgesamt besteht die gesuchte Menge also aus $1 + 4 + 4 + 4 + 8 = 21$ Elementen und ist gegeben durch

$$\{0, 1, i, -1, -i, 1 + i, 1 - i, -1 + i, -1 - i, 2, -2, 2i, -2i,$$
$$2 + i, -2 + i, 2 - i, -2 - i, 1 + 2i, -1 + 2i, 1 - 2i, -1 - 2i\}.$$

zu (b) Es ist $2 = (1+i)(1-i)$. Dabei ist $N(1+i) = N(1-i) = 2$ eine Primzahl, und laut Vorlesung folgt daraus, dass die Faktoren $1 \pm i$ in R irreduzibel sind. Die Zahl 3 ist bereits selbst irreduzibel in R. Dies folgt laut Vorlesung aus der Tatsache, dass $N(3) = 3^2$ ein Primzahlquadrat ist, und dass nach Teil (a) kein Element der Norm 3 in R existiert. Für die Zahl 4 existiert die Zerlegung $4 = 2 \cdot 2 = (1+i)(1-i)(1+i)(1-i)$, und wie wir bereits oben festgestellt haben, sind alle Faktoren dieser Zerlegung irreduzibel.

Die Zahl 5 besitzt in R die Zerlegung $5 = (2+i)(2-i)$, und da $N(2+i) = N(2-i) = 5$ eine Primzahl ist, sind die Faktoren in dieser Zerlegung irreduzibel. Die Zahl 6 kann schließlich zerlegt werden in $6 = 2 \cdot 3 = (1+i) \cdot (1-i) \cdot 3$. Auch hier haben wir bereits festgestellt, dass alle Faktoren irreduzibel sind.

zu (c) Die Zahl $5+10i$ kann in der Form $5+10i = 5 \cdot (1+2i) = (2+i)(2-i)(1+2i) = i(2+i)(2-i)^2$ zerlegt werden, und wie wir in Teil (b) festgestellt haben, sind die Faktoren $2 \pm i$ in R irreduzibel, während i wegen $N(i) = 1$ eine Einheit ist. Die Rechnung

$$\frac{1+3i}{2+i} \quad = \quad \frac{(1+3i)(2-i)}{(2+i)(2-i)} \quad = \quad \tfrac{1}{5} \cdot (5+5i) \quad = \quad 1+i$$

liefert für das Element $1+3i$ die Zerlegung $1+3i = (2+i)(1+i)$ in irreduzible Faktoren. Da R laut Angabe faktoriell ist, ist jeder größte gemeinsame Teiler von $5+10i$ und $1+3i$ somit assoziiert zu 1, $2+i$, $(1+i)$ oder $(2+i)(1-i)$, denn dies sind bis auf Assoziierte die Teiler von $1+3i$.

Der Fall 1 ist ausgeschlossen, denn dann wären $5+10i$ und $1+3i$ teilerfremd, aber offenbar ist $2+i$ ein gemeinsamer Teiler der beiden Zahlen, der wegen $N(2+i) = 5 > 1$ keine Einheit ist. Andererseits kann kein Vielfaches von $1+i$ ein größter gemeinsamer Teiler der Elemente sein, denn dann müsste $1+i$ assoziiert zu einem irreduziblen Faktor von $5+10i$ sein. Insbesondere müsste ein solcher Faktor die Norm $N(1+i) = 2$ besitzen. Aber die Faktoren $2+i$, $2-i$ und $1+2i$ sind alle von Norm 5.

Somit kommen wir zu dem Ergebnis, dass $2+i$ ein größter gemeinsamer Teiler der beiden Elemente ist. Weil R ein Hauptidealring ist, folgt daraus die Idealgleichung $(5+10i, 1+3i) = (2+i)$, also ist $d = 2+i$ ein Element mit der gesuchten Eigenschaft. Weil d irreduzibel und R ein Hauptidealring ist, handelt es sich bei dem Hauptideal (d) um ein maximales Ideal, und daraus wiederum folgt, dass $R/(d)$ ein Körper ist.

Anmerkung: Man hätte auch den Euklidischen Algorithmus verwenden können, um einen ggT der Elemente $5+10i$ und $1+3i$ im Ring R zu berechnen. Aber auf Grund der Aufgabenteil (a) und (b) war es leicht, die Faktorisierung der beiden Elemente zu bestimmen, und dadurch kommt man an den ggT schneller heran.

Aufgabe H24T2A5

Gegeben sei das Polynom $f = x^6 - 6 \in \mathbb{Q}[x]$.

(a) Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von f über $\mathbb{Q}$. Bestimmen Sie den Grad $[L : \mathbb{Q}]$.

(b) Zeigen Sie, dass $L|\mathbb{Q}$ eine Galois-Erweiterung ist. Zeigen Sie weiter, dass die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ einen Normalteiler der Ordnung 6 enthält.

(c) Entscheiden Sie begründet, ob die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ abelsch ist.

Lösung:
zu (a) Sei $\alpha = \sqrt[6]{6} \in \mathbb{R}^+$ und $\zeta = e^{\pi i/3}$, eine primitive 6-te Einheitswurzel. Dann ist $N = \{\zeta^k\alpha \mid 0 \leq k \leq 5\}$ die Menge der komplexen Nullstellen von f. Dass es sich bei allen Elementen von N tatsächlich um Nullstellen handelt, folgt aus der für $0 \leq k \leq 5$ gültigen Rechnung $f(\zeta^k\alpha) = (\zeta^k\alpha)^6 - 6 = (\zeta^6)^k \cdot \alpha^6 - 6 = 1 \cdot 6 - 6 = 0$. Weil ζ in der Gruppe $\mathbb{C}^\times$ ein Element der Ordnung 6 ist, sind die Elemente ζ^k mit $0 \leq k \leq 5$ alle verschieden, und wegen $\alpha \neq 0$ gilt dies auch für die Elemente $\zeta^k\alpha$ mit $0 \leq k \leq 5$. Weil f als Polynom vom Grad 6 nicht mehr als sechs verschiedene komplexe Nullstellen besitzt, muss N also die genaue Nullstellenmenge von f in $\mathbb{C}$ sein. Daraus folgt, dass der Zerfällungskörper L durch $L = \mathbb{Q}(N)$ gegeben ist.

Darüber hinaus gilt $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \zeta)$. Für den Nachweis genügt es zu überprüfen, dass $N \subseteq \mathbb{Q}(\alpha, \zeta)$ und $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$ gilt. Die erste Inklusion ist erfüllt, denn mit α und ζ ist auch jedes Element der Form $\zeta^k\alpha$ mit $0 \leq k \leq 5$ in $\mathbb{Q}(\alpha, \zeta)$ enthalten. Für die zweite Inklusion genügt es festzustellen, dass α wegen $\alpha \in N$ auch in $\mathbb{Q}(N)$ liegt, und dass wegen $\alpha, \zeta\alpha \in N$ die beiden Elemente auch im Teilkörper $\mathbb{Q}(N)$ von $\mathbb{C}$ liegen somit somit dasselbe auch für den Quotienten $\zeta = \frac{\zeta\alpha}{\alpha}$ gilt.

Nun bestimmen wir noch den Erweiterungsgrad $[L : \mathbb{Q}]$. Auf Grund der Gradformel gilt

$$[L : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha)(\zeta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Das Polynom f ist normiert, besitzt α als Nullstelle, und ist auf Grund des Eisenstein-Kriteriums (angewendet zum Beispiel auf die Primzahl 2) irreduzibel in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$. Es handelt sich also um das Minimalpolynom von α über $\mathbb{Q}$, und daraus folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 6$. Nun überprüfen wir noch, dass das sechste Kreisteilungspolynom $\Phi_6 \in \mathbb{Z}[x]$ das Minimalpolynom von ζ nicht nur über $\mathbb{Q}$, sondern auch über $\mathbb{Q}(\alpha)$ ist. Bekanntlich ist Φ_6 normiert, und weil ζ eine primitive 6-te Einheitswurzel ist, gilt $\Phi_6(\zeta) = 0$. Wäre Φ_6 über $\mathbb{Q}(\alpha)$ reduzibel, dann müsste wegen $\mathrm{grad}(\Phi_6) = \varphi(6) = 2$ die Nullstelle ζ bereits in $\mathbb{Q}(\alpha)$ liegen. Aber dies ist ausgeschlossen, denn wegen $\alpha \in \mathbb{R}$ gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, aber $\zeta = \cos(\frac{1}{3}\pi) + i\sin(\frac{1}{3}\pi)$ ist wegen $\sin(\frac{1}{3}\pi) \neq 0$ keine reelle Zahl.

Also ist Φ_6 tatsächlich das Minimalpolynom von ζ über $\mathbb{Q}(\alpha)$, und wir erhalten $[\mathbb{Q}(\alpha)(\zeta) : \mathbb{Q}(\alpha)] = \mathrm{grad}(\Phi_6) = 2$. Ingesamt erhalten wir $[L : \mathbb{Q}] = 2 \cdot 6 = 12$.

Hinweis: Das sechste Kreisteilungspolynom ist gegeben durch $\Phi_6 = x^2 - x + 1$. Durch Einsetzen sieht man leicht, dass $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$ eine primitive sechste Einheitswurzel ist. Wegen $\cos(\frac{1}{3}\pi) = \frac{1}{2}$ und $\sin(\frac{1}{3}\pi) = \frac{1}{2}\sqrt{3}$ stimmt diese mit der komplexen Zahl ζ überein.

zu (b) Aus der Tatsache, dass L Zerfällungskörper eines Polynoms $f \in \mathbb{Q}[x]$ ist, folgt direkt, dass es sich bei $L|\mathbb{Q}$ um eine normale Erweiterung handelt. Als normale Erweiterung ist $L|\mathbb{Q}$ insbesondere algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ folgt daraus wiederum, dass $L|\mathbb{Q}$ auch separabel ist. Insgesamt ist $L|\mathbb{Q}$ also eine Galois-Erweiterung.

Sei $G = \mathrm{Gal}(L|\mathbb{Q})$. Um zu zeigen, dass G einen Normalteiler der Ordnung 6 besitzt, betrachten wir den Zwischenkörper $K = \mathbb{Q}(\zeta)$. Weil ζ eine primitive sechste Einheitswurzel ist, ist das sechste Kreisteilungspolynom Φ_6 das Minimalpolynom von ζ über $\mathbb{Q}$. Daraus folgt $[K : \mathbb{Q}] = \mathrm{grad}(\Phi_6) = 2$. Sei $N = \mathrm{Gal}(L|K)$ die zu K korrespondierende Untergruppe von G. Laut Galoistheorie gilt $(G : N) = [K : \mathbb{Q}] = 2$. Weil $L|\mathbb{Q}$ eine Galois-Erweiterung ist, gilt außerdem $|G| = [L : \mathbb{Q}] = 12$. Wegen $|G| = (G : N) \cdot |N|$ ist die Ordnung von N gleich $|N| = \frac{|G|}{(G:N)} = \frac{12}{2} = 6$. Wegen $(G : N) = 2$ ist N darüber hinaus ein Normalteiler von G.

zu (c) Wäre G abelsch, dann müsste jede Untergruppe von G ein Normalteiler sein. Sei $K_1 = \mathbb{Q}(\alpha)$ und $U = \mathrm{Gal}(L|K_1)$ die korrespondierende Untergruppe. Ist U ein Normalteiler von G, dann muss $K_1|\mathbb{Q}$ laut Galoistheorie eine normale Erweiterung sein. Demnach müsste jedes über $\mathbb{Q}$ irreduzible Polynom, das in K_1 eine Nullstelle besitzt, über K_1 bereits in Linearfaktoren zerfallen. Das Polynom f besitzt in K_1 die Nullstelle α, und wir haben in Teil (a) festgestellt, dass es über $\mathbb{Q}$ irreduzibel ist. Würde f über K_1 in Linearfaktoren zerfallen, dann müssten alle komplexen Nullstellen bereits in K_1 liegen. Wegen $\alpha \in \mathbb{R}$ gilt $K_1 \subseteq \mathbb{R}$; somit wären alle komplexen Nullstellen von f reell. Aber wie wir oben gesehen haben, ist ζ nicht-reell, und wegen $\alpha \in \mathbb{R}^+$ gilt dasselbe für die Nullstelle $\zeta\alpha$ von f. Die Annahme, dass G abelsch ist, führt also zu einem Widerspruch.

Aufgabe H24T3A1

Für einen Körper K sei

$$G(K) \quad = \quad \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b \in K \right\}.$$

(a) Zeigen Sie, dass $G(K)$ eine abelsche Untergruppe von $\mathrm{GL}_3(K)$ ist.

(b) Für eine Primzahl p sei $\mathbb{F}_p$ der Körper mit $|\mathbb{F}_p| = p$. Entscheiden Sie begründet, zu welchem direkten Produkt zyklischer Gruppen $G(\mathbb{F}_p)$ isomorph ist.
Hinweis: Hauptsatz für endliche abelsche Gruppen

(c) Für eine Primzahl p sei $\mathbb{F}_{p^2}$ der endliche Körper mit $\mathbb{F}_{p^2} = p^2$. Entscheiden Sie begründet, zu welchem direkten Produkt zyklischer Gruppen $G(\mathbb{F}_{p^2})$ isomorph ist.

Lösung:
zu (a) Um zu zeigen, dass $G(K)$ eine Untergruppe ist, stellen wir zunächst fest, dass die Einheitsmatrix E, das Neutralelement von $\mathrm{GL}_3(K)$, in $G(K)$ enthalten ist, denn diese erhält man, indem man $a = b = 0$ setzt. Seien nun $A, B \in G(K)$ vorgegeben,

$$A = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad B = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix}$$

mit $a, b, c, d \in K$. Die Rechnung

$$AB \quad = \quad \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 & a+c \\ 0 & 1 & b+d \\ 0 & 0 & 1 \end{pmatrix}$$

zeigt, dass auch AB in $G(K)$ enthalten ist. Aus

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -a \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E \quad \text{folgt} \quad A^{-1} = \begin{pmatrix} 1 & 0 & -a \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \quad ,$$

also ist auch A^{-1} in $G(K)$ enthalten. Damit ist die Untergruppen-Eigenschaft nachgewiesen. Die Rechnung

$$BA \quad = \quad \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 & c+a \\ 0 & 1 & d+b \\ 0 & 0 & 1 \end{pmatrix} \quad = \quad AB$$

zeigt, dass zwei beliebige Elemente aus $G(K)$ vertauschbar sind, es sich bei $G(K)$ also um eine abelsche Gruppe handelt.

zu (b) Sei $A \in G(\mathbb{F}_p)$ wie oben vorgegeben, mit $a, b \in \mathbb{F}_p$. Wir überprüfen durch vollständige Induktion, dass für alle $m \in \mathbb{N}_0$ die Gleichung

$$A^m \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} & ma \\ \bar{0} & \bar{1} & mb \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

gilt. Für $m = 0$ ist dies offenbar der Fall, denn A^0 ist nach Definition die Einheitsmatrix, und wegen $ma = mb = \bar{0}$ stimmte auch die Matrix auf der rechten Seite mit der Einheitsmatrix überein. Sei nun $m \in \mathbb{N}_0$ vorgegeben, und setzen wir die Gleichung für m voraus. Dann erhalten wir

$$A^{m+1} \quad = \quad A^m \cdot A \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} & ma \\ \bar{0} & \bar{1} & mb \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} & ma+a \\ \bar{0} & \bar{1} & mb+b \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} & (m+1)a \\ \bar{0} & \bar{1} & (m+1)b \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}.$$

Wegen $pa = pb = \bar{0}$ in $\mathbb{F}_p$ ist A^p wiederum die Einheitsmatrix. Dies zeigt, dass die Orndung jedes Elements in $G(K)$ ein Teiler von p ist.

Da es für die Einträge in a und b jeweils p Wahlmöglichkeiten gibt, ist $G(K)$ eine Gruppe der Ordnung p^2, und nach Teil (a) ist diese außerdem abelsch. Aus dem Hauptsatz über endliche abelsche Gruppen folgt, dass $G(K)$ isomorph zu einem Produkt zyklischer Gruppen mit Primzahlpotenzordnungen > 1 ist. Damit erhalten wir $G(K) \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G(K) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Im ersten Fall hätte $G(K)$ ein Element der Ordnung p^2, weil $\bar{1}$ in $\mathbb{Z}/p^2\mathbb{Z}$ ein solches Element ist. Aber p^2 ist kein Teiler von p, somit widerspricht dies unserer Feststellung von oben. Damit bleibt $G(K) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ als einzige Möglichkeit.

zu (c) Die Gruppe $G(\mathbb{F}_{p^2})$ ist diesmal eine abelsche Gruppe Ordnung p^4, weil es diesmal für die Einträge a und b jeweils p^2 Wahlmöglichkeiten gibt. Die einzigen Möglichkeiten, die Zahl p^4 als Produkt von Primzahlpotenzen größer als 1 darzustellen, sind $p \cdot p \cdot p \cdot p$, $p^2 \cdot p \cdot p$, $p^3 \cdot p$, $p^2 \cdot p^2$ und p^4. Aus dem Hauptsatz über endliche abelsche Gruppen folgt somit diesmal, dass G isomorph zu einer der fünf Gruppen

$$G_1 = (\mathbb{Z}/p\mathbb{Z})^4 \quad , \quad G_2 = \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^2 \quad , \quad G_3 = \mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad ,$$
$$G_4 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \quad , \quad G_5 = \mathbb{Z}/p^4\mathbb{Z}$$

ist. Mit Ausnahme der ersten enthält jede dieser Gruppen ein Element mit Ordnung größer als p: die Gruppe G_2 das Element $(\bar{1}, \bar{0}, \bar{0})$ der Ordnung p^2, die Gruppe G_3 das Element $(\bar{1}, \bar{0})$ der Ordnung p^3, die Gruppe G_4 das Element $(\bar{1}, \bar{0})$ der Ordnung p^2 und die Gruppe G_5 das Element $\bar{1}$ der Ordnung p^4. Dieselbe Rechnung wie in Teil (b) zeigt aber, dass auch für alle $A \in G(\mathbb{F}_{p^2})$ jeweils $A^p = E$ gilt, es also nur Elemente gibt, deren Ordnung p teilt. Also muss G isomorph zu G_1 sein.

Aufgabe H24T3A2

Sei R der Restklassenring $\mathbb{Z}[x]/(x^3+x)$.

(a) Zeigen Sie, dass R zum Produktring $\mathbb{Z}\times\mathbb{Z}[i]$ isomorph ist.

(b) Geben Sie sämtliche Einheiten des Rings $\mathbb{Z}\times\mathbb{Z}[i]$ an.

(c) Bestimmen Sie alle Elemente $a,b\in\mathbb{Z}$, so dass die Restklasse von x^2+ax+b in R eine Einheit ist.

Lösung:
zu (a) Wir beweisen die Isomorphie $R\cong\mathbb{Z}\times\mathbb{Z}[i]$ mit Hilfe des Homomorphiesatzes und definieren dafür einen geeigneten Ringhomomorphismus. Die Abbildung $\varphi_0:\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}[i]$, $c\mapsto(c,c)$ ist ein Ringhomomorphismus, denn es gilt $\varphi_0(1)=(1,1)=1_{\mathbb{Z}\times\mathbb{Z}[i]}$, $\varphi_0(c+d)=(c+d,c+d)=(c,c)+(d,d)=\varphi_0(c)+\varphi_0(d)$ und $\varphi_0(cd)=(cd,cd)=(c,c)\cdot(d,d)=\varphi_0(c)\varphi_0(d)$ für alle $c,d\in\mathbb{Z}$. Auf Grund der universellen Eigenschaft des Polynomrings existiert ein Ringhomomorphismus $\varphi:\mathbb{Z}[x]\to\mathbb{Z}\times\mathbb{Z}[i]$ mit $\varphi|_{\mathbb{Z}}=\varphi_0$ und $\varphi(x)=(0,i)$.

Nun überprüfen wir die Voraussetzungen des Homomorphiesatzes. Für den Nachweis der Surjektivität sei $(u,v+iw)\in\mathbb{Z}\times\mathbb{Z}[i]$ vorgegeben, mit $u,v,w\in\mathbb{Z}$. Es gilt $\varphi(1)=(1,1)$, $\varphi(x)=(0,i)$ und $\varphi(x^2)=(0,i^2)=(0,-1)$. Für alle $a,b,c\in\mathbb{Z}$ erhalten wir damit

$$\varphi(a+bx+cx^2) \quad=\quad a\varphi(1)+b\varphi(x)+c\varphi(x^2) \quad=\quad (a,a)+(0,ib)+(0,-c) \quad=\quad (a,a-c+ib).$$

Weiter gilt die Äquivalenz $(a,a-c+ib)=(u,v+iw)\Leftrightarrow a=u\wedge a-c=v\wedge b=w$, was zu $a=u$, $b=w$, $c=u-v$ umgeformt werden kann. Setzen wir $g=u+wx+(u-v)x^2$, dann erhalten wir somit $\varphi(g)=(u,u-(u-v)+iw)=(u,v+iw)$, wodurch die Surjektivität nachgewiesen ist.

Nun überprüfen wir noch, dass der Kern von φ mit dem Hauptideal (x^3+x) übereinstimmt. Mit $\varphi_1:\mathbb{Z}[x]\to\mathbb{Z}$ und $\varphi_2:\mathbb{Z}[x]\to\mathbb{Z}[i]$ bezeichnen wir die beiden Komponenten von φ. Nach Definition gilt $\varphi_1(c)=\varphi_2(c)=c$ für alle $c\in\mathbb{Z}$, außerdem $\varphi_1(x)=0$ und $\varphi_2(x)=i$. Also ist φ_1 der Auswertungshomomorphismus auf $\mathbb{Z}[x]$ an der Stelle 0 und φ_2 der Auswertungshomomorphismus an der Stelle i. Für jedes $f\in\mathbb{Z}[x]$ gilt somit die Äquivalenz

$$f\in\ker(\varphi) \quad\Leftrightarrow\quad \varphi(f)=0_{\mathbb{Z}\times\mathbb{Z}[i]} \quad\Leftrightarrow\quad (f(0),f(i))=(0,0) \quad\Leftrightarrow\quad f(0)=0\wedge f(i)=0.$$

Nun ist x das Minimalpolynom von 0 über $\mathbb{Q}$, und x^2+1 ist das Minimalpolynom von i über $\mathbb{Q}$ (denn dieses Polynom ist normiert, hat i als Nullstelle und ist als viertes Kreisteilungspolynom irreduzibel in $\mathbb{Q}[x]$). Die Gleichung $f(0)=0$ ist somit äquivalent zu $x\mid f$, und $f(i)=0$ ist äquivalent zu $(x^2+1)\mid f$ in $\mathbb{Q}[x]$. Weil x^2+1 und x in $\mathbb{Q}[x]$ teilerfremd sind, gilt darüber hinaus die Äquivalenz

$$x\mid f\wedge(x^2+1)\mid f \quad\Leftrightarrow\quad x(x^2+1)\mid f \quad\Leftrightarrow\quad (x^3+x)\mid f \quad ,$$

wobei auch hier die Teilbarkeit in $\mathbb{Q}[x]$ gemeint ist. Nun ist x^3+x als normiertes Polynom in $\mathbb{Z}[x]$ aber primitiv, und somit ist die Teilbarkeit $(x^3+x)\mid f$ in $\mathbb{Q}[x]$ äquivalent zur Teilbarkeit in $\mathbb{Z}[x]$. Dies wiederum ist gleichbedeutend mit $f\in(x^3+x)$, wobei (x^3+x) das Hauptideal in $\mathbb{Z}[x]$ bezeichnet. Insgesamt haben wir damit die Äquivalenz $f\in\ker(\varphi)\Leftrightarrow f\in(x^3+x)$ und damit $\ker(\varphi)=(x^3+x)$ nachgewiesen. Damit sind alle Voraussetzungen des Homomorphiesatzes überprüft, und wir erhalten den gewünschten Isomorphismus $R\cong\mathbb{Z}[x]/\ker(\varphi)\cong\mathbb{Z}\times\mathbb{Z}[i]$.

zu (b) Aus der Vorlesung ist bekannt: Sind R und S beliebige Ringe, dann ist die Einheitengruppe von $R \times S$ gegeben durch $(R \times S)^\times = R^\times \times S^\times$. Außerdem ist bekannt, dass $\mathbb{Z}^\times = \{\pm 1\}$ und $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ gilt. Es folgt

$$\begin{gathered}(\mathbb{Z} \times \mathbb{Z}[i])^\times \quad = \quad \mathbb{Z}^\times \times \mathbb{Z}[i]^\times \quad = \quad \{\pm 1\} \times \{\pm 1, \pm i\} \quad = \\ \{(1,1), (1,i), (1,-1)(1,-i), (-1,1), (-1,i), (-1,-1), (-1,-i)\} \quad = \\ \{(a,b) \mid a,b \in \{\pm 1\}\} \cup \{(a,ib) \mid a,b \in \{\pm 1\}\}.\end{gathered}$$

zu (c) Sei $I = (x^3 + x)$. Der Isomormphismus $\bar{\varphi} : R \to \mathbb{Z} \times \mathbb{Z}[i]$, den uns die Anwendung des Homomorphiesatzes aus Teil (a) liefert, ist gegeben durch $\bar{\varphi}(f+I) = \varphi(f) = (f(0), f(i))$ für alle $f \in \mathbb{Z}[x]$. Außerdem haben wir in Teil (a) gesehen, dass für alle $u, v, w \in \mathbb{Z}$ das Polynom $u + wx + (u - v)x^2$ durch φ auf $(u, v + iw)$ abgebildet wird. Da die Einheiten in R genau die Urbilder der Einheiten in $\mathbb{Z} \times \mathbb{Z}[i]$ unter $\bar{\varphi}$ sind, müssen wir also lediglich die Urbilder der acht in Teil (b) gefundenen Elemente bestimmen.

Für alle $a, b \in \{\pm 1\}$ gilt jeweils $\bar{\varphi}(a + (a - b)x^2 + I) = \varphi(a + (a - b)x^2) = (a, b)$; dies zeigt, dass die Restklassen der vier Polynome 1, $1 + 2x$, $-1 - 2x$ und -1 Einheiten in R sind. Außerdem gilt für alle $a, b \in \{\pm 1\}$ auch $\bar{\varphi}(a + bx + ax^2 + I) = \varphi(a + bx + ax^2) = (a, ib)$. Damit sind die Restklassen der vier Polynome $1 + x + x^2$, $1 - x + x^2$, $-1 + x - x^2$ und $-1 - x - x^2$ ebenfalls Einheiten in R, und auf Grund der Vorüberlegung gibt es keine weiteren Polynome mit dieser Eigenschaft. Es gibt also genau zwei Paare $(a, b) \in \mathbb{Z}^2$ mit der Eigenschaft, dass $x^2 + ax + b + I$ in R eine Einheit ist, nämlich $(1, 1)$ und $(-1, 1)$.

Aufgabe H24T3A3

Sei $f = x^{2024}+2024 \in \mathbb{Z}[x]$. Wir definieren die Iterierten von f als $f_0 = x$ und $f_{n+1} = f(f_n) = f_n^{2024}+2024$ für $n \geq 0$. Zeigen Sie:

(a) f ist irreduzibel.

(b) Für alle $n \geq 1$ gilt $f_n(0) \equiv 2024 \bmod 2024^2$.

(c) f_n ist irreduzibel für alle $n \geq 0$.

Lösung:
zu (a) Die Zahl 2024 hat die Primfaktorzerlegung $2024 = 2^3 \cdot 11 \cdot 23$. Weil die Primzahl 11 den konstanten Term von f nur einfach teilt, der Leitkoeffizient 1 von 11 nicht geteilt wird und alle anderen Koeffizienten gleich null sind, liefert das Eisenstein-Kriterium die Irreduzibilität von f in $\mathbb{Z}[x]$. (Genauso gut hätte man natürlich auch die Primzahl 23 nehmen können.)

zu (b) Wir beweisen die Aussage durch vollständige Induktion über n. $f_1 = f(f_1) = f = x^{2024} + 2024$, also $f_1(0) = 2024$ und damit auch $f_1(0) \equiv 2024 \bmod 2024^2$. Sei nun $n \in \mathbb{N}$ beliebig, und setzen wir die Aussage für n voraus. Dann erhalten wir

$$f_{n+1}(0) \equiv f_n(0)^{2024} + 2024 \equiv 2024^{2024} + 2024 \equiv 0 + 2024 \equiv 2024 \bmod 2024^2 \quad ,$$

wobei wir im vorletzten Schritt verwendet haben, dass 2024^m für alle $m \geq 2$ durch 2024^2 teilbar ist und somit $2024^m \equiv 0 \bmod 2024^2$ gilt.

zu (c) Unser Ziel ist der Nachweis, dass das Eisenstein-Kriterium auf alle Polynome f_n mit $n \geq 1$ und die Primzahl 11 angewendet werden kann. Wir bemerken vorweg, dass f_n für alle $n \geq N$ nicht-konstant und normiert ist: Für $f_1 = f$ ist dies unmittelbar klar. Ist nun $n \in \mathbb{N}$, und setzen wir die Aussage für f_n voraus, dann ist mit f_n auch f_n^{2024} nicht konstant, und damit ist auch $f_{n+1} = f_n^{2024} + 2024$ kein konstantes Poylnom. Mit f_n ist auch f_n^{2024} nicht normiert, und weil f_n^{2024} nicht konstant ist, ist mit f_n^{2024} auch das Polynom $f_{n+1} = f_n^{2024} + 2024$ normiert.

Für jedes $n \in \mathbb{N}$ sei nun $\bar{f}_n$ jeweils das Bild von f_n in $\mathbb{F}_{11}[x]$. Wir zeigen durch vollständige Induktion, dass $\bar{f}_n$ für alle $n \geq 1$ ein Monom ist. Weil f_n normiert ist, folgt daraus, dass alle Koeffizienten von f_n mit Ausnahme des Leitkoeffizienten durch 11 teibar sind. Offenbar ist $\bar{f}_1 = x^{2024} + \overline{2024} = x^{2024} + \bar{0} = x^{2024} \in \mathbb{F}_{11}[x]$ ein Monom. Sei nun $n \in \mathbb{N}$ vorgegeben, und setzen wir $\bar{f}_n = x^d$ für ein $d \in \mathbb{N}$ voraus. Dann folgt $\bar{f}_{n+1} = \bar{f}_n^{2024} + \overline{2024} = (x^d)^{2024} + \bar{0} = x^{2024d}$.

Sei nun $n \in \mathbb{N}$ beliebig vorgegeben. Das Polynom f_n ist normiert, und alle Koeffizienten von f_n mit Ausnahme des Leitkoeffizienten sind durch 11 teilbar. Weil 11^2 ein Teiler von 2024^2 ist, erfüllt der konstante Term a_0 von f_n nach Teil (b) die Kongruenz $a_0 \equiv f_n(0) \equiv 2024 \equiv 88 \bmod 11^2$. Weil 88 durch 11, aber nicht durch 11^2 teilbar ist, gilt auch $11 \mid a_0$ und $11^2 \mid a_0$. Damit sind alle Voraussetzungen des Eisenstein-Kriteriums erfüllt, und f_n ist in $\mathbb{Z}[x]$ irreduzibel.

Aufgabe H24T3A4

Sei $f = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ und $a \in \mathbb{C}$ eine beliebige Nullstelle von f.

(a) Zeigen Sie durch Polynomdivision, dass $f(x^2 - 2)$ durch f teilbar ist.

(b) Zeigen Sie, dass a und $a^2 - 2$ verschiedene Nullstellen von f sind.

(c) Zeigen Sie, dass $\mathbb{Q}(a)|\mathbb{Q}$ eine Galois-Erweiterung ist, deren Galois-Gruppe zu $\mathbb{Z}/3\mathbb{Z}$ isomorph ist.

Lösung:
zu (a) Auf Grund des binomischen Lehrsatzes ist $(x^2 - 2)^3 = x^6 - 6x^4 + 12x^2 - 8$, und $(x^2 - 2)^2 = x^4 - 4x^2 + 4$. Auf diese Weise erhält man $f(x^2 - 2) = x^6 - 5x^4 + 6x^2 - 1$. Die Polynomdivision ergibt $f(x^2 - 2) = fg$ mit $g = x^3 - x^2 - 2x + 1$. (Aus Zeitgründen verzichten wir hier auf die Ausführung.)

zu (b) Wegen $f(x^2 - 2) = fg$ gilt $f(a^2 - 2) = f(a) \cdot g(a) = 0 \cdot g(a) = 0$. Dies zeigt, dass mit a auch $a^2 - 2$ eine komplexe Nullstelle von f ist. Nehmen wir nun an, es gilt $a = a^2 - 2$, was zu $a^2 - a - 2 = 0$ äquivalent ist. Die Elemente $1, a, a^2$ wären also im $\mathbb{Q}$-Vektorraum $\mathbb{Q}(a)$ linear abhängig. Dies führen wir zu einem Widerspruch.

Dazu stellen wir zunächst fest, dass das Polynom f in $\mathbb{Q}$ irreduzibel ist. Denn andernfalls hätte f wegen $\text{grad}(f) = 3$ eine rationalen Nullstelle c. Weil f in $\mathbb{Z}[x]$ liegt und f normiert ist, wäre c darüber hinaus ganzzahlig und ein Teiler des konstanten Terms -1 von f, also $c \in \{\pm 1\}$. Aber wegen $f(1) =$ und $f(-1) =$ sind ± 1 keine Nullstellen von f. Damit ist die Irreduzibilität nachgewiesen. Da f außerdem normiert ist und a eine Nullstelle von f ist, handelt es sich bei f um das Minimalpolynom von a über $\mathbb{Q}$. Laut Vorlesung gilt: Ist $L|K$ eine Körpererweiterung, $\alpha \in L$ ein über K algebraisches Element, $g = \mu_{\alpha,K}$ und $n = \text{grad}(g)$, dann sind bilden die Elemente $1, \alpha, ..., \alpha^{n-1}$ eine n-elementige Basis von $K(a)$ als K-Vektorraum; insbesondere sind sie über K linear unabhängig. In unserer Situation bedeutet das wegen $\text{grad}(f) = 3$, dass die Elemente $1, a, a^2$ im $\mathbb{Q}$-Vektorraum $\mathbb{Q}(a)$ linear unabhängig sind. Die Annahme $a = a^2 - 2$ hat also zu einem Widerspruch geführt, und folglich sind a und $a^2 - 2$ *verschiedene* Nullstellen von f.

zu (c) Um zu zeigen, dass $\mathbb{Q}(a)|\mathbb{Q}$ eine normale Erweiterung ist, überprüfen wir, dass $\mathbb{Q}(a)$ ein Zerfällungskörper des Polynoms f über $\mathbb{Q}$ ist. Wegen $f(a) = f(a^2 - 2) = 0$ sind $x - a$ und $x - (a^2 - 2)$ Teiler von f im Polynomring $\mathbb{Q}(a)[x]$. Wegen $a \neq a^2 - 2$ sind diese außerdem teilerfremd; daraus folgt, dass f vom Produkt $(x - a)(x - (a^2 - 2))$ geteilt wird. Es existiert also ein Polynom $h \in \mathbb{Q}(a)[x]$ mit $f = (x-a)(x-(a^2-2))h$, und wegen $\text{grad}(f) = 3$ ist $\text{grad}(h) = 3-2 = 1$. Damit ist nachgewiesen, dass f über $\mathbb{Q}(a)$ in Linearfaktoren zerfällt. Außerdem wird $\mathbb{Q}(a)$ über $\mathbb{Q}$ von den Nullstellen des Polynoms f in $\mathbb{Q}(a)$ erzeugt, da unter anderem a eine Nullstelle von f und bereits $\{a\}$ ein Erzeugendensystem von $\mathbb{Q}(a)$ über $\mathbb{Q}$ ist. Damit ist gezeigt, dass $\mathbb{Q}(a)$ tatsächlich ein Zerfällungskörper von f über $\mathbb{Q}$ ist. Als normale Erweiterung ist $\mathbb{Q}(a)|\mathbb{Q}$ insbesondere algebraisch, und wegen $\text{char}(\mathbb{Q}) = 0$ folgt daraus wiederum, dass $\mathbb{Q}(a)|\mathbb{Q}$ auch eine separable Erweiterung ist. Insgesamt ist $\mathbb{Q}(a)|\mathbb{Q}$ damit eine Galois-Erweiterung.

Bereits in Teil (b) haben wir festgestellt, dass f das Minimalpolynom von a über $\mathbb{Q}$ ist. Weil die Erweiterung $\mathbb{Q}(a)|\mathbb{Q}$ zudem galois'sch ist, erhalten wir $|\text{Gal}(\mathbb{Q}(a)|\mathbb{Q})| = [\mathbb{Q}(a) : \mathbb{Q}] = \text{grad}(f) = 3$. Als Gruppe der Primzahlordnung 3 ist $\text{Gal}(\mathbb{Q}(a)|\mathbb{Q})$ zyklisch und somit isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Â¸

Aufgabe H24T3A5

Sei $\zeta_{16} = e^{\frac{2\pi i}{16}}$.

(a) Zeigen Sie, dass $\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i)$ eine Galois-Erweiterung vom Grad 4 ist.

(b) Bestimmen Sie das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$.

(c) Entscheiden Sie begründet, ob die Galois-Gruppe von $\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i)$ zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ isomorph ist.

Lösung:

zu (a) Laut Vorlesung ist $\mathbb{Q}(\zeta_{16})|\mathbb{Q}$ als Kreisteilungserweiterung eine Galois-Erweiterung. Allgemein gilt: Ist $M|K$ eine Galois-Erweiterung, und ist L ein Zwischenkörper von $M|K$, dann ist auch $M|L$ eine Galois-Erweiterung. Nun ist $\mathbb{Q}(i)$ ein Zwischenkörper von $\mathbb{Q}(\zeta_{16})|\mathbb{Q}$, wegen $i = e^{\frac{2\pi i}{4}} = \zeta_{16}^4 \in \mathbb{Q}(\zeta_{16})$. Also ist auch $\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i)$ eine Galois-Erweiterung. Allgemein gilt: Ist $n \in \mathbb{N}$ und $\zeta_n = e^{\frac{2\pi i}{n}}$, dann ist $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ eine Erweiterung von Grad $\varphi(n)$. Daraus folgt $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] = \varphi(16) = 8$. Wegen $i = \zeta_4$ gilt auch $[\mathbb{Q}(i) : \mathbb{Q}] = \varphi(4) = 2$. Auf Grund der Gradformel gilt

$$8 \quad = \quad [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\zeta^{16}) : \mathbb{Q}(i)] \cdot 2$$

und somit $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] = \frac{8}{2} = 4$.

zu (b) Auf Grund der Gleichung $\zeta_{16}^4 - i = 0$ ist ζ_{16} eine Nullstelle des Polynoms $f = x^4 - i \in \mathbb{Q}(i)[x]$. Sei $g = \mu_{\zeta_{16},\mathbb{Q}(i)}$, das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$. Wegen $f \in \mathbb{Q}(i)[x]$ und $f(\zeta_{16}) = 0$ ist g ein Teiler von f in $\mathbb{Q}(i)[x]$. Außerdem sind f und g beide normiert, und es gilt $\text{grad}g = [\mathbb{Q}(i)(\zeta_{16}) : \mathbb{Q}(i)] = [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] = 4 = \text{grad}f$. Dies zeigt, dass f und g übereinstimmen und somit $x^4 - i$ das gesuchte Minimalpolynom ist.

zu (c) Aus der Vorlesung ist bekannt, dass die Elemente von $\text{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q})$ alle durch $\sigma_a(\zeta_{16}) = \zeta_{16}^a$ gegeben sind, wobei a die ganzen, zu 16 teilerfremden (also ungeraden) Zahlen durchläuft. Dabei ist $\sigma_a = \sigma_b$ für $a, b \in \mathbb{Z} \setminus 2\mathbb{Z}$ genau dann erfüllt, wenn die Bilder von a und b in $(\mathbb{Z}/16\mathbb{Z})^\times$ übereinstimmen. Wegen $(\mathbb{Z}/16\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{15}\}$ ist also

$$\text{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}) \quad = \quad \{\sigma_1, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}\}.$$

Weil $\mathbb{Q}(i)$ ein Zwischenkörper von $\mathbb{Q}(\zeta_{16})|\mathbb{Q}$ ist, handelt es sich bei $G = \text{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i))$ um eine Untergruppe von $\text{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q})$ mit Ordnung $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] = 4$, bestehend aus genau den Elementen $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q})$ mit $\sigma|_{\mathbb{Q}(i)} = \text{id}_{\mathbb{Q}(i)}$, was zu $\sigma(i) = i$ äquivalent ist. Nun ist für alle $a \in \mathbb{Z} \setminus 2\mathbb{Z}$ die Gleichung $i = \sigma_a(i)$ äquivalent zu $\zeta_{16}^4 = \sigma_a(\zeta_{16}^4) = \sigma_a(\zeta_{16})^4 = (\zeta_{16}^a)^4 = \zeta_{16}^{4a}$, was wegen $\text{ord}(\zeta_{16}) = 16$ in $\mathbb{C}^\times$ zu $16 \mid (4a - 4)$ äquivalent ist, und dies wiederum zu $4 \mid (a - 1)$ und $a \equiv 1 \bmod 4$. Das Urbild der Untergruppe G unter dem Isomorphismus $(\mathbb{Z}/16\mathbb{Z})^\times \to \text{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q})$, $a + 16\mathbb{Z} \mapsto \sigma_a$ ist somit die Untergruppe von $(\mathbb{Z}/16\mathbb{Z})^\times$ gegeben durch $\{\bar{1}, \bar{5}, \bar{9}, \overline{13}\}$. Wegen $\bar{5}^2 = \overline{25} = \bar{9} \neq \bar{1}$ und $\bar{5}^4 = (\bar{5}^2)^2 = \bar{9}^2 = \overline{81} = \bar{1}$ ist $\bar{5}$ ein Element der Ordnung 4 in der Untergruppe von $(\mathbb{Z}/16\mathbb{Z})^\times$. Dies zeigt, dass auch G ein Element der Ordnung 4 enthält, und wegen $|G| = 4$ folgt daraus $G \cong \mathbb{Z}/4\mathbb{Z}$.

Aufgabe F25T1A1

Sei p eine Primzahl, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen und $G = \mathrm{GL}_2(\mathbb{F}_p)$.

(a) Zeigen Sie, dass für die Anzahl der Elemente in G gilt: $|G| = p(p-1)^2(p+1)$.

(b) Bestimmen Sie die Ordnung des Elements $T \in G$ gegeben durch

$$T \quad = \quad \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}.$$

(c) Zeigen Sie, dass es mehr als eine p-Sylowgruppe in G gibt.

(d) Sei nun speziell $p = 3$ und $H = \langle T \rangle = \{T^k \mid k \in \mathbb{Z}\}$. Zeigen Sie, dass der Normalisator $N = \{g \in G \mid g \cdot H = H \cdot g\}$ von H in G aus den oberen Dreiecksmatrizen in G besteht. Folgern Sie, dass G genau vier 3-Sylowgruppen besitzt.

Aufgabe F25T1A2

Für $b \in \mathbb{Z} \setminus \{0\}$ betrachte man $R_b = \{\frac{a}{b^k} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ und } k \in \mathbb{N}_0\} \subseteq \mathbb{Q}$.

(a) Zeigen Sie, dass R_b ein Teilring von $\mathbb{Q}$ und damit ein kommutativer Ring mit Eins ist.

(b) Zeigen Sie, dass für die Einheitengruppe von R gilt:

$$(R_b)^\times \quad = \quad \left\{ \frac{a}{b^k} \;\middle|\; a \in \mathbb{Z}, \text{ und es existieren } c \in \mathbb{Z} \setminus \{0\} \text{ und } \ell \in \mathbb{N}_0 \text{ mit } ac = b^\ell \right\}$$

(c) Zeigen Sie, dass R_b ein Hauptidealbereich ist, und dass jedes Ideal $\mathfrak{a}$ von R_b die Form $\mathfrak{a} = R_b w$ für ein $w \in \mathbb{Z}$ hat.

Aufgabe F25T1A3

Sei $A \in \mathcal{M}_{3,\mathbb{Q}}$ eine 3×3-Matrix, deren charakteristisches Polynom $\chi_A \in \mathbb{Q}[x]$ irreduzibel über $\mathbb{Q}$ ist. Seien $\alpha \in \mathbb{C}$ eine Nullstelle von χ_A und $\mathbb{Q}(\alpha)$ der davon erzeugte Zwischenkörper $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{C}$. Betrachten Sie die Multiplikation mit α, also die Abbildung $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$, $\gamma \mapsto \alpha\gamma$.

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

(b) Bestimmen Sie die darstellende Matrix B von φ bezüglich der Basis $1, \alpha, \alpha^2$ von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum und zeigen Sie, dass deren charakteristisches Polynom identisch mit dem von A ist, also $\chi_A = \chi_B$ in $\mathbb{Q}[x]$ gilt.

(c) In der Situation von (b), zeigen Sie, dass die beiden Matrizen A und B, betrachtet in $\mathcal{M}_{3,\mathbb{C}}$, ähnlich sind.

Aufgabe F25T1A4

Sei G eine endliche Gruppe und p eine Primzahl, die die Gruppenordnung $|G|$ teilt. Seien ferner $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen und $\mathbb{F}_p^\times$ die Einheitengruppe von $\mathbb{F}_p$. Wir definieren

$$M \quad = \quad \{g \in G \mid \mathrm{ord}(g) = p\}$$

als die Menge aller Gruppenelemente, deren Ordnung gleich p ist.

(a) Zeigen Sie, dass durch $\mathbb{F}_p^\times \times M \to M$, $([a], g) \mapsto g^a$ eine Gruppenoperation definiert ist.

(b) Sei $g \in M$ ein beliebiges Element. Zeigen Sie, dass der Stabilisator $(\mathbb{F}_p)_g^\times = \{[a] \in \mathbb{F}_p^\times \mid g^a = g\}$ von g trivial ist, also mit $\{[1]\}$ übereinstimmt.

(c) Folgern Sie, dass $|M|$ ein Vielfaches von $p-1$ ist.

Aufgabe F25T1A5

Betrachten Sie das Polynom $f = x^{15} - 7 \in \mathbb{Q}[x]$.

(a) Sei $L|\mathbb{Q}$ ein Zerfällungskörper von f. Bestimmen Sie den Körpergrad $[L : \mathbb{Q}]$.

(b) Zeigen Sie, dass die Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$ einen Normalteiler der Ordnung 15 besitzt.

(c) Sei $\alpha \in L$ eine Nullstelle von f. Zeigen Sie, dass die Körpererweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}(\alpha^5)$ den Körpergrad $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^5)] = 5$ besitzt.

Aufgabe F25T2A1

(a) Sei $n \in \mathbb{N}$ und R ein Ring. Ein Element $\omega \in R$ ist eine *n-te Einheitswurzel* in R, wenn $\omega^n = 1$ gilt, und eine *primitive n-te Einheitswurzel*, wenn zusätzlich für alle $1 \leq m < n$ gilt, dass $\omega^m - 1 \in R^\times$ (also eine Einheit in R) ist. Zeigen Sie, dass (die Restklasse von) 7 in $\mathbb{Z}/100\mathbb{Z}$ eine vierte Einheitswurzel, aber keine primitive vierte Einheitswurzel ist.

(b) Bestimmen Sie die Ordnung der Einheitengruppe von $\mathbb{Z}/2025\mathbb{Z}$, und zeigen Sie, dass diese nicht zyklisch ist.

Aufgabe F25T2A2

Sei p eine Primzahl.

(a) Sei q ein Primteiler von $2^p - 1$. Zeigen Sie: $q \equiv 1 \bmod p$.
Hinweis: Betrachten Sie die Ordnung von $\bar{2} \in (\mathbb{Z}/q\mathbb{Z})^\times$.

(b) Zeigen Sie: Es gibt eine Galois-Erweiterung $K_p|\mathbb{Q}$ mit $\mathrm{Gal}(K_p|\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$.
Hinweis: Betrachten Sie Teilkörper von geeigneten Kreisteilungskörpern.

Aufgabe F25T2A3

Sei K ein Körper mit algebraischem Abschluss $\bar{K}$, sei $f \in K[x]$ normiert und sei $L = K(\alpha)$ mit einer Nullstelle $\alpha \in \bar{K}$ von f.

(a) Zeigen Sie: Ist $[L : K] = \text{grad}(f)$, dann ist f irreduzibel in $K[x]$.

(b) Sei jetzt $f \in K[x]$ irreduzibel, und sei weiter $g \in K[x]$. Wir nehmen an, dass das Polynom $g - \alpha$ in $L[x]$ irreduzibel ist. Zeigen Sie, dass dann $f(g(x)) \in K[x]$ in $K[x]$ irreduzibel ist.
Hinweis: Sei $\beta \in \bar{K}$ mit $g(\beta) = \alpha$. Zeigen Sie $K(\beta) = L(\beta)$.

Aufgabe F25T2A4

Sei G eine Gruppe der Ordnung $2025 = 3^4 \cdot 5^2$. Seien U_5, U_5' zwei verschiedene 5-Sylowgruppen von G.

(a) Bestimmen Sie die Anzahl der 5-Sylowgruppen von G.

(b) Sei U die von der Teilmenge $U_5 \cup U_5'$ erzeugte Untergruppe von G. Zeigen Sie: Dann gilt $U = G$.
Hinweis: Wieviele 5-Sylowgruppen kann eine echt zwischen U_5 und G liegende Untergruppe haben?

Aufgabe F25T2A5

Sei p eine Primzahl und $\mathbb{F}_p$ der endliche Körper mit p Elementen. Sei weiter

$$G \quad = \quad \left\{ \begin{pmatrix} a & \bar{0} \\ b & a \end{pmatrix} \;\middle|\; a \in \mathbb{F}_p^\times \;,\; b \in \mathbb{F}_p \right\}.$$

Zeigen Sie:

(a) Die Menge G ist eine Untergruppe von $\mathrm{GL}_2(\mathbb{F}_p)$.

(b) Die Gruppe G enthält eine zyklische Untergruppe H_{p-1} der Ordnung $p-1$ und eine zyklische Gruppe H_p der Ordnung p.

(c) Die Gruppe G ist zyklisch.

Aufgabe F25T3A1

Sei $n \in \mathbb{N}$, sei K ein Körper, sei $\mathcal{M}_{n,K}$ der Ring der $n \times n$-Matrizen über K, und sei $A \in \mathcal{M}_{n,K}$. Bekanntlich ist das *Minimalpolynom* von A das eindeutig bestimmte normierte Polynom $\mu_A \in K[x]$ minimalen Grades, das $\mu_A(A) = 0_{\mathcal{M}_{n,K}}$ erfüllt.

(a) Sei $m \in \mathbb{N}$ und $B \in \mathcal{M}_{m,K}$. Desweiteren sei $C \in \mathcal{M}_{m+n,K}$ die Blockdiagonalmatrix

$$C \quad = \quad \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Beweisen Sie, dass μ_C ein kleinstes gemeinsames Vielfaches von μ_A und μ_B ist.

(b) Entscheiden Sie begründet, ob es eine Matrix $A \in \mathcal{M}_{6,\mathbb{R}}$ mit charakteristischem Polynom $x^6 + x^4$ und Minimalpolynom μ_A vom Grad 5 gibt.

Aufgabe F25T3A2

(a) Sei $\mathbb{F}_3$ der Körper mit drei Elementen, und sei G die Menge der oberen Dreiecksmatrizen in $\mathcal{M}_{3,\mathbb{F}_3}$ mit Einsen auf der Hauptdiagonalen. Zeigen Sie, dass G eine nicht-abelsche Untergruppe von $\mathrm{GL}_3(\mathbb{F}_3)$ der Ordnung 27 ist.

(b) Bestimmen Sie 12 paarweise nicht-isomorphe Gruppen der Ordnung 2025.

Aufgabe F25T3A3

(a) Zerlegen Sie die Polynome $x^6 - y^6$ und $x^5y + x^3y^3 + xy^5$ im faktoriellen Ring $\mathbb{Q}[x, y]$ in Primfaktoren.
Hinweis: Es sind jeweils vier Primfaktoren.

(b) Finden Sie alle Paare von Polynomen $(f, g) \in \mathbb{Q}[x, y]^2$ mit

$$f \cdot (x^6 - y^6) + g \cdot (x^5y + x^3y^3 + xy^5) \quad = \quad 0.$$

Aufgabe F25T3A4

Für $a \in \mathbb{Z}$ sei $f_a = x^4 + ax^2 + 1 \in \mathbb{Q}[x]$. Mit $\mathrm{Gal}(f_a|\mathbb{Q})$ werde im Folgenden die Galoisgruppe des in $\mathbb{C}$ enthalten Zerfällungskörpers von f_a über $\mathbb{Q}$ bezeichnet.

(a) Finden Sie ein $a \in \mathbb{Z}$, so dass $\mathrm{Gal}(f_a)$ nur aus der Identität besteht.

(b) Finden Sie ein $a \in \mathbb{Z}$, so dass $\mathrm{Gal}(f_a)$ nur aus der Identität und der komplexen Konjugation besteht.

(c) Bestimmen Sie den Isomorphietyp von $\mathrm{Gal}(f_a)$ im Fall $a = -1$.

Aufgabe F25T3A5

Sei $R = \mathbb{Z}[\sqrt{3}]$, sei $K = \mathbb{Q}(\sqrt{3})$, und sei $N_K : K \to \mathbb{Q}$ die Normabbildung, die gegeben ist durch $N_K(a + b\sqrt{3}) = a^2 - 3b^2$ für alle $a, b \in \mathbb{Q}$.

(a) Beweisen Sie, dass es zu $x \in R$ und $y \in R \setminus \{0\}$ ein Element $q \in R$ gibt mit $|N_K(\frac{x}{y} - q)| < 1$.
Hinweis: Schreiben Sie $\frac{x}{y}$ in der Form $a + b\sqrt{3}$ mit $a, b \in \mathbb{Q}$.

(b) Sei $N_R : R \to \mathbb{Z}$ die Einschränkung der Abbildung N_K. Zeigen Sie, dass R bezüglich der Abbildung $|N_R|$ ein euklidischer Ring ist, d.h. zu zwei Elementen $x, y \in R$ mit $y \neq 0$ gibt es Elemente $q, r \in R$ mit $x = qy + r$ und $|N_R(r)| < |N_R(y)|$.