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

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) Sei $u \in R$ eine Einheit. Wir zeigen durch vollständige Induktion, dass folgende Aussage für alle $n \in \mathbb{N}$ gilt: Ist $x \in R$ 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 $x^{n+1} = 0$. Zu zeigen ist, dass es sich bei $u+x$ um eine Einheit handelt. Setzen wir $y = -x^2$, dann gilt $(u + x)(u - x) = u^2 - x^2 = u + y$. Das Element y erfüllt die Bedingung $y^n = 0$. Denn wegen $n \geq 1$ ist $n - 1 \geq 0$, und es folgt $y^n = (-x^2)^n = (-1)^n x^{2n} = (-1)^n x^{n-1} x^{n+1} = (-1)^n x^{n-1} \cdot 0 = 0$. Auf Grund der Induktionsvoraussetzung ist $(u+x)(u-x) = u+y$ 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.