Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1

(a) Sei $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ ein normiertes Polynom. Sei $\overline{P}(X) \in \mathbb{F}_3[X]$ das Polynom, das aus $P(X)$ durch Reduktion der Koeffizienten modulo 3 entsteht.

(i) Sei $\overline{P}(X)$ irreduzibel in $\mathbb{F}_3[X]$. Zeigen Sie, dass $P(X)$ irreduzibel in $\mathbb{Z}[X]$ ist.

(ii) Zeigen Sie anhand eines Beispiels, dass die Umkehrung der Aussage in i) falsch ist.

(b) Zeigen Sie, dass das Polynom $X^3 + (3m-1)X + (3n+1)$ für alle $m, n \in \mathbb{Z}$ irreduzibel in $\mathbb{Z}[X]$ ist.

(12 Punkte)

Aufgabe 2

Sei R der Ring $\mathbb{F}_2[X]/\langle X^3+1\rangle$.

(a) Bestimmen Sie die Anzahl der Elemente in R und geben Sie diese an.

(b) Finden Sie alle Einheiten in R.

(c) Finden Sie alle idempotenten Elemente in R (also alle $f \in R$ mit $f^2 = f$).

(12 Punkte)

Aufgabe 3

(a) Zeichnen Sie alle 5-ten und alle 10-ten komplexen Einheitswurzeln in der komplexen Zahlenebene und markieren Sie jeweils die primitiven Einheitswurzeln.

(b) Sei $p \geq 3$ prim und $\zeta \in \mathbb{C}$. Zeigen Sie:

(i) Ist ζ eine p-te Einheitswurzel, so ist $-\zeta$ eine $2p$-te Einheitswurzel.

(ii) Genau dann ist ζ eine primitive p-te Einheitswurzel, wenn $-\zeta$ eine primitive $2p$-te Einheitswurzel ist.

(iii) Es ist $\Phi_{2p}(X) = \Phi_p(-X)$. (Mit $\Phi_n \in \mathbb{Z}[X]$ bezeichnen wir das n-te Kreisteilungspolynom.)

(12 Punkte)

Fortsetzung nächste Seite!

Aufgabe 4

Gegeben sei das Polynom $P(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$. Weiter sei $Z \subseteq \mathbb{C}$ ein Zerfällungskörper von P über $\mathbb{Q}$. Zeigen Sie:

(a) P ist irreduzibel in $\mathbb{Q}[X]$.

(b) P hat genau drei reelle Nullstellen.

(c) Die Galois-Gruppe $\mathrm{Gal}(Z/\mathbb{Q})$ enthält ein Element der Ordnung 5 und ein Element der Ordnung 2.

(12 Punkte)

Aufgabe 5

Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z}$. Zeigen Sie, dass folgende Aussagen äquivalent sind:

(a) Es gibt genau eine ganze Zahl $b \geq 0$ mit $a^2 + b^2 = (b + p)^2$.

(b) Es ist $a \equiv p \pmod{2p}$.

(12 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1

(a) Definieren Sie den Begriff *Integritätsbereich*.

(b) Formulieren Sie den *Kleinen Satz von Fermat*.

(c) Sei $a \in \mathbb{Z}$ und $f(X) = X^3 + aX^2 - (3+a)X + 1 \in \mathbb{Q}[X]$.
Zeigen Sie, dass f keine Nullstelle in $\mathbb{Q}$ hat.

(d) Seien $P_1, P_2, \dots, P_5 \in \mathbb{R}^2$ mit $P_j = (x_j, y_j)$ für $j = 1, \dots, 5$.
Zeigen Sie, dass $P_1, \dots, P_5$ auf einem (möglicherweise entarteten) Kegelschnitt liegen, d.h., es gibt $a, b, c, d, e, f \in \mathbb{R}$, nicht alle null, mit

$$ax_j^2 + bx_jy_j + cy_j^2 + dx_j + ey_j + f = 0 \qquad \text{für alle } j \in \{1, 2, 3, 4, 5\}.$$

Hinweis: Betrachten Sie ein geeignetes lineares Gleichungssystem für a, b, c, d, e, f.

(12 Punkte)

Aufgabe 2
Sei $a \in \mathbb{Z}$ und $f(X) = X^3 + aX^2 - (3+a)X + 1 \in \mathbb{Q}[X]$.

(a) Zeigen Sie: f ist irreduzibel.

(b) Sei $\alpha \in \mathbb{C}$ mit $f(\alpha) = 0$. Zeigen Sie, dass $f(1/(1-\alpha)) = 0$ ist.

(c) Zeigen Sie: $\mathbb{Q}(\alpha)$ ist eine galoissche Erweiterung von $\mathbb{Q}$.

(12 Punkte)

Aufgabe 3
Bestimmen Sie alle $a \in \mathbb{R}$, für die der Faktorring $R = \mathbb{R}[X]/\langle X^2 - a\rangle$

(a) ein Integritätsbereich ist;

(b) ein Körper ist;

(c) isomorph zum Produktring $\mathbb{R} \times \mathbb{R}$ ist.

(12 Punkte)

Fortsetzung nächste Seite!

Aufgabe 4

(a) Bestimmen Sie alle ganzen Zahlen $n \geq 0$, für die $2^n + 3$ bzw. $2^n + 5$ durch 3, 5, 7 bzw. 13 teilbar ist.

(b) Bestimmen Sie alle ganzen Zahlen $n \geq 0$ mit der Eigenschaft, dass sowohl $2^n + 3$ als auch $2^n + 5$ Primzahlen sind.

(12 Punkte)

Aufgabe 5

Das *Zentrum* einer (multiplikativ geschriebenen) Gruppe G ist die Untergruppe

$$Z(G) = \{z \in G \mid \forall g \in G\colon gz = zg\}.$$

(a) Zeigen Sie, dass $Z(G)$ ein Normalteiler von G ist.

(b) Sei D die Diedergruppe der Ordnung 12. Bestimmen Sie $Z(D)$.

(c) Bestimmen Sie die Struktur der Faktorgruppe $D/Z(D)$.

(12 Punkte)

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1

(a) Bestimmen Sie alle Nullteiler und alle Einheiten im Ring $\mathbb{Z}/(12)$.

(b) Bestimmen Sie die Mächtigkeit des Kerns einer surjektiven linearen Abbildung

$$\psi : \mathbb{F}_5^3 \to \mathbb{F}_5^2,$$

wobei $\mathbb{F}_5$ ein Körper mit 5 Elementen ist.

(c) Gegeben sei die Permutation $\varphi \in S_9$ mit folgender Wertetabelle:

k	1	2	3	4	5	6	7	8	9
$\varphi(k)$	5	9	6	8	4	2	1	7	3

Schreiben Sie φ als Produkt von elementfremden Zykeln, und bestimmen Sie die kleinste natürliche Zahl $k \geq 1$ mit $\varphi^k = \text{id}$.

(d) Es sei U der Untervektorraum

$$U = \text{span}(x - 1, \quad x^2 - x, \quad x^2 - 1, \quad x^{10} + x^8, \quad x^{10} - x^6)$$

von $V = \mathbb{R}[x]$ (der Vektorraum der Polynome über $\mathbb{R}$). Bestimmen Sie die Dimension von U.

(12 Punkte)

Fortsetzung nächste Seite!

Aufgabe 2

In der Gruppe $\mathrm{GL}_2(\mathbb{Q})$ der invertierbaren Matrizen über $\mathbb{Q}$ wähle $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

und $b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.

(a) Zeigen Sie, dass a und b endliche Ordnungen haben, und bestimme diese Ordnungen.

(b) Zeigen Sie, dass $c = ab$ keine endliche Ordnung hat.

(12 Punkte)

Aufgabe 3

Für eine endliche Gruppe G und eine Primzahl p, die die Ordnung von G teilt, bezeichnen wir mit n_p die Anzahl der p-Sylowgruppen in G.

(a) Es seien G eine endliche Gruppe und $p, q \in \mathbb{N}$ zwei verschiedene Primzahlen, die die Ordnung von G teilen. Angenommen, $n_p = n_q = 1$. Es seien H_1 die einzige p-Sylowgruppe und H_2 die einzige q-Sylowgruppe in G.

Zeigen Sie, dass die Elemente von H_1 und H_2 miteinander kommutieren, d. h. für alle $x \in H_1$ und für alle $y \in H_2$ gilt $xy = yx$.

(b) Es sei G eine Gruppe der Ordnung 12.

(i) Zeigen Sie, dass nicht gleichzeitig $n_2 = 3$ und $n_3 = 4$ gelten kann.

(ii) Zeigen Sie, dass im Fall $n_2 = n_3 = 1$ die Gruppe G abelsch ist und es bis auf Isomorphie genau zwei verschiedene Möglichkeiten für G gibt.

(12 Punkte)

Aufgabe 4

(a) Zeigen Sie, dass $R_1 := \mathbb{Q}[X]/(X^4 + 12X - 2)$ ein Integritätsbereich ist.

(b) Zeigen Sie, dass $R_2 := \mathbb{Z}[X]/(2, X^2 + X + 1)$ ein Körper ist. Wie viele Elemente besitzt dieser Körper?

(12 Punkte)

Fortsetzung nächste Seite!

Aufgabe 5

Es sei $K = \mathbb{Q}(i) \subset \mathbb{C}$ und $\alpha := \sqrt[4]{7} \in \mathbb{R}$. Sei $L \subset \mathbb{C}$ der Zerfällungskörper des Polynoms $f := X^4 - 7 \in K[X]$ über dem Grundkörper K.

(a) Zeigen Sie, dass $L = K(\alpha)$ gilt.

(b) Bestimmen Sie die Grade der Körpererweiterungen $[L : \mathbb{Q}]$ und $[L : K]$ und begründen Sie Ihre Antworten.

(c) Zeigen Sie, dass die Körpererweiterung L/K galoissch ist.

(d) Es sei $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(\alpha) = i\alpha$. Bestimmen Sie damit $\sigma^2(\alpha)$ und folgern Sie, dass $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ gilt.

(12 Punkte)

Prüfungsteilnehmer	Prüfungstermin	Einzelprüfungsnummer
Kennzahl: ______	**Herbst 2018**	**63912**
Kennwort: ______		
Arbeitsplatz-Nr.: ______		

Erste Staatsprüfung für ein Lehramt an öffentlichen Schulen

— Prüfungsaufgaben —

Fach: **Mathematik (vertieft studiert)**

Einzelprüfung: **Algebra**

Anzahl der gestellten Themen (Aufgaben): 3

Anzahl der Druckseiten dieser Vorlage: 7

Bitte wenden!

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

(a) Zeigen Sie, dass das Polynom $x^7 + 3x + 3 \in \mathbb{Q}[x]$ irreduzibel ist.

(b) Bestimmen Sie die Ordnung der Permutation $(12)(34)(567) \in S_7$.

(c) Sei G eine abelsche Gruppe und seien $a, b, c \in G$. Angenommen a hat Ordnung 2, b hat Ordnung 4 und c hat Ordnung 6. Bestimmen Sie die Ordnung von $abc \in G$.

(d) Bestimmen Sie alle Einheitswurzeln in dem Körper $\mathbb{Q}(\sqrt{3})$.

Aufgabe 2 (12 Punkte)

Sei G eine Gruppe.

(a) Sei $H \subseteq G$ eine Untergruppe von endlichem Index. Zeigen Sie, dass die Menge $\{gHg^{-1} \mid g \in G\}$ endlich ist.

(b) Es seien $n_1, n_2 \in \mathbb{N}$ und es seien $H_1, H_2 \subseteq G$ Untergruppen von G mit $[G : H_1] = n_1$ und $[G : H_2] = n_2$. (Für eine Untergruppe K von G bezeichnet $[G : K]$ den Index von G nach K.) Zeigen Sie, dass $[G : (H_1 \cap H_2)] \leq n_1 n_2$ ist.

(c) Sei $H \subseteq G$ eine Untergruppe von endlichem Index. Zeigen Sie, dass ein Normalteiler $N \subseteq G$ von endlichem Index existiert, für den $N \subseteq H$ gilt.

Aufgabe 3 (12 Punkte)

Seien p eine Primzahl, $q = p^n$ $(n \geq 1)$ eine Primzahlpotenz und $\mathbb{F}_q$ der endliche Körper mit q Elementen.

(a) Zeigen Sie im Falle $p \neq 2$: $|\{x^2 \mid x \in \mathbb{F}_q\}| = \frac{q+1}{2}$.

(b) Sei $\alpha \in \mathbb{F}_q$ gegeben. Zeigen Sie, dass $x, y \in \mathbb{F}_q$ so existieren, dass $\alpha = x^2 + y^2$ gilt.
Hinweis: Betrachten Sie den Schnitt der Mengen $\{\alpha - x^2 \in \mathbb{F}_q \mid x \in \mathbb{F}_q\}$ und $\{y^2 \in \mathbb{F}_q \mid y \in \mathbb{F}_q\}$.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Seien $p > 0$ eine Primzahl, $\mathbb{Q} \subseteq K$ eine Körpererweiterung vom Grad p, $\alpha \in K$ ein Element mit $K = \mathbb{Q}(\alpha)$, $\alpha_1 := \alpha, \ldots, \alpha_p \in \mathbb{C}$ die Konjugierten von α über $\mathbb{Q}$ und letztlich $E := \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ die normale Hülle von $K/\mathbb{Q}$.

(a) Zeigen Sie, z.B. durch Betrachten der Operation der Galoisgruppe auf den Nullstellen, dass die Galoisgruppe $\mathrm{Gal}(E/\mathbb{Q})$ eine zyklische Untergruppe der Ordnung p enthält.

(b) Zeigen Sie: Gilt $\alpha_2 \in K$, so folgt $K = E$.

Aufgabe 5 (12 Punkte)

Sei $K = \{0, 1, a, b\}$ ein Körper mit vier Elementen (0 sei das Nullelement, 1 das Einselement).

(a) Stellen Sie die Additions- und die Multiplikationstabelle von K auf.

(b) Sei $f(X) = X^4 + X + 1 \in K[X]$. Zeigen Sie, dass f reduzibel ist.

(c) Bestimmen Sie den Grad des Zerfällungskörpers von f über K.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

(a) Man zeige, dass die beiden Zahlen $12n+1$ und $30n+2$ für alle $n \in \mathbb{Z}$ teilerfremd sind.

(b) Sei K ein Körper. Man zeige, dass der Polynomring $K[X]$ unendlich viele irreduzible Polynome enthält.
(Hinweis: Man verwende z.B. die Idee in Euklids Beweis der Unendlichkeit der Primzahlmenge.)

Aufgabe 2 (12 Punkte)

Sei L/K eine Körpererweiterung. Seien $m, n \in \mathbb{N}$, sei A eine $m \times n$-Matrix mit Koeffizienten in K und sei $b \in K^m$. Zeigen Sie, dass das lineare Gleichungssystem $Ax = b$ genau dann eine Lösung $x \in K^n$ hat, wenn es eine Lösung $x \in L^n$ hat.

Aufgabe 3 (12 Punkte)

Sei $(G, +)$ eine abelsche Gruppe. Die *Torsion* $T(G)$ von G ist die Menge aller Elemente endlicher Ordnung von G. Die Gruppe G heißt *torsionsfrei*, falls $T(G) = \{0_G\}$, wobei 0_G das neutrale Element von G bezeichnet.

(a) Sei $(G, +)$ eine abelsche Gruppe. Zeigen Sie:

 (i) $T(G)$ ist eine Untergruppe von G.

 (ii) $G/T(G)$ ist torsionsfrei.

(b) Geben Sie eine unendliche abelsche Gruppe mit nichttrivialer Torsion an.

Aufgabe 4 (12 Punkte)

Es seien p eine Primzahl und $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Es sei $\mathbb{Z}[\zeta]$ der Durchschnitt aller Teilringe von $\mathbb{C}$, die $\mathbb{Z}$ und ζ enthalten. Weiter seien $z_0, z_1, \ldots, z_{p-1} \in \mathbb{Z}$ und
$x := z_0 + z_1\zeta + \cdots + z_{p-1}\zeta^{p-1} \in \mathbb{Q}(\zeta)$. Zeigen Sie:

(a) $\mathbb{Z}[\zeta] = \{y_0 + y_1\zeta + \cdots + y_{p-2}\zeta^{p-2} \mid y_0, \ldots, y_{p-2} \in \mathbb{Z}\} \subseteq \mathbb{Q}(\zeta)$.

(b) Ist $\frac{x}{p} \in \mathbb{Z}[\zeta]$, so gilt $z_0 \equiv \cdots \equiv z_{p-1} \pmod{p}$.

Fortsetzung nächste Seite!

Aufgabe 5 (12 Punkte)

Sei p eine ungerade Primzahl und sei ζ eine primitive p-te Einheitswurzel. Zeigen Sie:

(a) Die Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ hat genau einen Zwischenkörper Z vom Grad 2 über $\mathbb{Q}$.

(b) Komplexe Konjugation induziert ein Element der Ordnung 2 in der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

(c) Der Körper Z aus (a) ist genau dann ein Unterkörper von $\mathbb{R}$, wenn $p \equiv 1 \mod 4$.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

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

(b) Sei $d \geq 1$ eine natürliche Zahl. Geben Sie eine Definition für das d-te *Kreisteilungspolynom* $\Phi_d(X)$ über den rationalen Zahlen an.

(c) Geben Sie eine Formulierung des *Satzes vom primitiven Element* an.

Aufgabe 2 (12 Punkte)

(a) Geben Sie ein normiertes Polynom mit rationalen Koeffizienten an, welches $\sqrt{2} + \sqrt{7}$ als Nullstelle hat.

(b) Mit S_n wollen wir die symmetrischen, mit A_n die alternierenden Gruppen bezeichnen. Begründen Sie, warum $A_3 \times A_3$ die einzige 3-Sylowgruppe von $S_3 \times S_3$ ist.

(c) Sei $f(X) = X^2 + pX + q$ ein Polynom mit rationalen Koeffizienten. Was können Sie über die Galoissche Gruppe von $f(X)$ sagen, wenn die Diskriminante $\Delta := p^2 - 4q$ ein Quadrat in den rationalen Zahlen ist?

Aufgabe 3 (12 Punkte)

Mit $\mathbb{Q}$ bezeichnen wir den Körper der rationalen Zahlen.

Sei $f(X)$ ein irreduzibles Polynom fünften Grades über den rationalen Zahlen, dessen galoissche Gruppe isomorph zur symmetrischen Gruppe S_5 ist. Mit L bezeichnen wir einen Zerfällungskörper von $f(X)$ über den rationalen Zahlen.

(a) Welchen Grad hat L über $\mathbb{Q}$? (Geben Sie eine kurze Begründung an.)

(b) Seien $x_1, \ldots, x_5$ die Nullstellen von $f(X)$ in L. Kann der Fall $x_i = x_j$ mit $i \neq j$ auftreten? (Geben Sie eine kurze Begründung an.)

(c) Für jedes $i = 0, \ldots, 5$ betrachten wir die Zwischenerweiterung $K_i = \mathbb{Q}(x_1, \ldots, x_i)$ (d. h. insb. $K_0 = \mathbb{Q}$) von L über $\mathbb{Q}$. Bestimmen Sie den Grad von K_{i+1} über K_i für $i = 0, \ldots, 4$.

(d) Geben Sie Begründungen dafür an, warum $f(X)$ über $\mathbb{Q}$ nicht, dafür aber über K_1 auflösbar ist.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Zur Erinnerung: Eine komplexe Zahl heißt *algebraisch*, wenn sie Nullstelle eines Polynoms mit rationalen Koeffizienten ist.

(a) Sei $n \geq 1$ eine natürliche Zahl und sei $c \in \mathbb{C}^n$ ein nicht verschwindender Vektor aus komplexen Zahlen. Zeigen Sie, dass eine komplexe Zahl z algebraisch ist, wenn eine rationale $n \times n$-Matrix A mit

$$z \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

existiert.

(Hinweis: Betrachten Sie das charakteristische Polynom von A.)

(b) Seien x und y zwei algebraische Zahlen. Benutzen Sie die Aussage aus dem ersten Aufgabenteil, um zu zeigen, dass $z = x + y$ ebenfalls algebraisch ist. (Hinweis: Betrachten Sie einen Vektor c, dessen Einträge von der Form $x^i y^j$ sind.)

Aufgabe 5 (12 Punkte)

(a) Sei $\mathbb{Z}$ der Ring der ganzen Zahlen. Zeigen Sie, dass der Ring $\mathbb{Z}[i]/(2)$ (wobei $i^2 = -1$) genau vier Elemente hat.

(b) Sei R ein kommutativer Ring mit 1. Sei weiter $t \in R$. Zeigen Sie, dass jedes Element im Quotientenring $R[X]/(tX - 1)$ kongruent zu einem Element der Form aX^n modulo $tX - 1$ ist, wobei $a \in R$ und $n \geq 1$ eine natürliche Zahl ist.

(c) Für einen kommutativen Ring R mit 1 wollen wir mit $\operatorname{Spec}(R)$ die Menge der Primideale von R bezeichnen. Sei $\phi\colon R \to S$ ein Ringhomomorphismus in einen weiteren kommutativen Ring mit 1. Geben Sie einen Beweis dafür an, dass

$$\phi^{-1}\colon \operatorname{Spec}(S) \to \operatorname{Spec}(R), \mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$$

eine wohldefinierte Abbildung ist.

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

(a) Bestimmen Sie das (multiplikative) Inverse von $\overline{47}$ im Restklassenring $\mathbb{Z}/112\mathbb{Z}$.

(b) Bestimmen Sie eine Zerlegung des Polynoms $2X^4 + 4X^3 + 4X^2 + 2X \in \mathbb{Z}[X]$ in irreduzible Faktoren aus $\mathbb{Z}[X]$.

(c) Geben Sie drei nichtisomorphe Gruppen der Ordnung 12 an (mit Begründung).

(d) Zeigen Sie, dass jede Gruppe der Ordnung 95 zyklisch ist.

Aufgabe 2 (12 Punkte)

Es seien X die Menge der diagonalisierbaren 2×2-Matrizen über $\mathbb{R}$ und $G := \mathrm{GL}_2(\mathbb{R})$ die Gruppe der invertierbaren 2×2-Matrizen über $\mathbb{R}$.

(a) Zeigen Sie, dass

$$\cdot : G \times X \to X \ , \ (B, M) \mapsto B\,M\,B^{-1}$$

eine Operation ist.

(b) Ist die Operation aus (a) transitiv? Begründen Sie Ihre Antwort.

(c) Geben Sie ein Repräsentantensystem für die Bahnen der Operation aus (a) an.

Aufgabe 3 (12 Punkte)

Gegeben sind der Ring $R := \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ und die multiplikative Funktion $N : R \to \mathbb{N}_0$, $N(a + b\sqrt{-3}) = a^2 + 3b^2$. (Die Multiplikativität von N muss nicht gezeigt werden.)

(a) Bestimmen Sie die Einheitengruppe $R^\times$ von R.

(b) Zeigen Sie, dass jedes Element $a + b\sqrt{-3}$ mit $N(a + b\sqrt{-3}) = 4$ irreduzibel ist.

(c) Ist R ein faktorieller Ring? Begründen Sie Ihre Antwort.

Aufgabe 4 (12 Punkte)

Für ein Polynom $f(X) \in \mathbb{C}[X]$ bezeichne $f'(X)$ die Ableitung und $\deg(f)$ den Grad von $f(X)$. Ferner sei $n_0(f) \in \mathbb{N}_0$ die Anzahl der verschiedenen Nullstellen von $f(X)$ in $\mathbb{C}$ (also ohne Vielfachheiten gezählt). Zeigen Sie, dass für jedes Polynom $f(X) \in \mathbb{C}[X]$ mit $f(X) \neq 0$ die Gleichung

$$\deg(f) = \deg(\,\mathrm{ggT}(f, f')) + n_0(f)$$

gilt.

Fortsetzung nächste Seite!

Aufgabe 5 (12 Punkte) = H 17 III .4 identisch!

Es sei α die reelle Zahl $\alpha := \sqrt[3]{2+\sqrt{2}} \in \mathbb{R}$, und es sei ζ die dritte Einheitswurzel $\zeta := e^{\frac{2\pi i}{3}} \in \mathbb{C}$.

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

(b) Es sei $\beta = \sqrt[3]{2-\sqrt{2}} \in \mathbb{R}$ und $L \subseteq \mathbb{C}$ der Zerfällungskörper von f über $\mathbb{Q}$. Zeigen Sie, dass $L = \mathbb{Q}(\alpha, \beta, \zeta)$ gilt.

(c) Zeigen Sie, dass die reelle Zahl $\sqrt[3]{2}$ in L liegt, und folgern Sie, dass die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ einen Normalteiler vom Index 6 besitzt.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

Eine *Kruppe* ist ein Paar $(K, \cdot)$, bestehend aus einer Menge K und einer Abbildung $\cdot : K \times K \longrightarrow K$, die die folgenden Eigenschaften besitzt:

(K1) Es gibt ein $e \in K$ mit
$$x \cdot e = x \text{ für alle } x \in K.$$

(K2) Die Verknüpfung „ $\cdot$ " ist assoziativ.

(K3) Für jedes $x \in K$ sind die folgenden Abbildungen injektiv:

$$\begin{aligned} K &\longrightarrow K \\ y &\longmapsto x \cdot y \end{aligned} \qquad\qquad \begin{aligned} K &\longrightarrow K \\ y &\longmapsto y \cdot x \end{aligned}$$

Sei nun $(K, \cdot)$ eine Kruppe.

(a) Zeigen Sie: $e \cdot x = x$ für alle $x \in K$.

(b) Zeigen Sie: Sind $x, y \in K$ mit $y \cdot x = x$, so folgt $y = e$.

(c) Zeigen Sie: Ist K endlich, so ist $(K, \cdot)$ eine Gruppe.

(d) Ist $(\mathbb{N}_0, +)$ eine Kruppe? Begründen Sie Ihre Antwort.

Aufgabe 2 (12 Punkte)

Es sei $G \neq \{1_G\}$ eine endliche Gruppe, für welche die Automorphismengruppe $A = \mathrm{Aut}(G)$ transitiv auf $G \setminus \{1_G\}$ operiert. Das heißt für alle $g, h \in G \setminus \{1_G\}$ gibt es ein $\alpha \in A$ mit $\alpha(g) = h$. Zeigen Sie:

(a) Es gibt eine Primzahl p, so dass $g^p = 1_G$ für alle $g \in G$ ist.

(b) $Z(G) \neq \{1_G\}$. (Hier ist $Z(G) = \{\, g \in G \mid xg = gx \text{ für alle } x \in G \,\}$ das Zentrum von G.)

(c) Die Gruppe G ist abelsch.

Fortsetzung nächste Seite!

Aufgabe 3 (12 Punkte)

(a) Sei $m \geq 1$ eine ungerade ganze Zahl. Zeigen Sie, dass

$$1^m + 2^m + \ldots + (m-1)^m \equiv 0 \pmod{m}.$$

(b) Sei $m \in \mathbb{N}$ und seien $x_1, x_2, \ldots, x_m$ ganze Zahlen. Zeigen Sie, dass es eine nichtleere Teilmenge $I \subseteq \{1, 2, \ldots, m\}$ gibt, so dass

$$\sum_{i \in I} x_i \equiv 0 \pmod{m}.$$

(Hinweise: (a) Betrachten Sie geeignete Paare von Summanden.
(b) Betrachten Sie $x_1, x_1 + x_2, \ldots, x_1 + \ldots + x_m$.)

Aufgabe 4 (12 Punkte)

Begründen Sie jeweils Ihre Antwort.

(a) Ist $\mathbb{Q}[X]/(X^5 - 2,\ X^6 + X^5 - 2X - 2)$ ein Körper?

(b) Ist $\mathbb{Z}[X]/(5,\ X^3 - 2X^2 + 4)$ ein Körper?

(Hinweis zur Notation: $(X^5 - 2,\ X^6 + X^5 - 2X - 2)$ bezeichnet in (a) das von $X^5 - 2$ und $X^6 + X^5 - 2X - 2$ erzeugte Ideal von $\mathbb{Q}[X]$, analog in (b).)

Aufgabe 5 (12 Punkte)

Sei $L/\mathbb{Q}$ eine endliche Galoiserweiterung mit $L \subseteq \mathbb{C}$ und $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3 \times H$ mit $|H| = 88$, wobei S_3 die symmetrische Gruppe auf 3 Punkten bezeichnet.

(a) Zeigen Sie: Es gilt $L \cap \mathbb{Q}(\sqrt[5]{5}) = \mathbb{Q}$.

(b) Zeigen Sie: Es gibt einen Zwischenkörper K von $L/\mathbb{Q}$ mit $[K : \mathbb{Q}] = 8$, der ein Zerfällungskörper eines Polynoms in $\mathbb{Q}[X]$ vom Grad 8 ist.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

Im Folgenden sei p eine Primzahl. Betrachten Sie den folgenden Teilring von $\mathbb{Q}$:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b \right\} .$$

(Sie müssen nicht nachprüfen, dass dies ein Teilring von $\mathbb{Q}$ ist.)

(a) Zeigen Sie, dass die folgende Abbildung ein Ringisomorphismus ist:

$$\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}, \ a + p\mathbb{Z} \mapsto a + p\mathbb{Z}_{(p)} .$$

(b) Betrachten Sie den Fall $p = 5$. Für $x \in \mathbb{Z}_{(5)}$ schreiben wir zur Abkürzung $\bar{x} := x + 5\mathbb{Z}_{(5)}$. Bestimmen Sie die (eindeutig bestimmte) ganze Zahl $y \in \{0, \dots, 4\}$ mit

$$\bar{y} = \overline{\frac{2}{3}} + \overline{\frac{1}{7}} .$$

Aufgabe 2 (12 Punkte)

Es sei G eine Gruppe. Für $g, x, y \in G$ sei

$$^{(x,y)}g := xgy^{-1} . \tag{1}$$

(a) Zeigen Sie, dass (1) eine transitive Operation von $G \times G$ auf G definiert. Bestimmen Sie die Elemente des Stabilisators von 1_G in $G \times G$.

(b) Bestimmen Sie den Kern der obigen Operation von $G \times G$ auf G. Wann ist die Operation treu?
(Der Kern der Operation einer Gruppe H auf einer Menge X ist die Menge aller $h \in H$ mit $^h x = x$ für alle $x \in X$. Die Operation heißt treu, falls der Kern nur aus dem neutralen Element besteht.)

Aufgabe 3 (12 Punkte)

Sei $\zeta = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$ (mit $i^2 = -1$) und seien $K = \mathbb{Q}(\zeta)$, $L = \mathbb{Q}(\zeta, \sqrt[4]{2})$. Zeigen Sie:

(a) $\zeta^4 = -1$, und K ist der Zerfällungskörper von $X^4 + 1$ über $\mathbb{Q}$.

(b) $f(X) = X^4 + 2$ ist irreduzibel über $\mathbb{Q}$.

(c) L ist der Zerfällungskörper von f über $\mathbb{Q}$.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Sei $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ der Körper mit elf Elementen.

(a) Zeigen Sie, dass die Restklassenringe $\mathbb{F}_{11}[X]/(X^2+1)$ und $\mathbb{F}_{11}[X]/(X^2+X+4)$ jeweils einen Körper (mit 121 Elementen) definieren.

(b) Bestimmen Sie konkret einen Isomorphismus

$$\mathbb{F}_{11}[X]/(X^2+1) \to \mathbb{F}_{11}[X]/(X^2+X+4)$$

durch Angabe des Bilds von $[X] \in \mathbb{F}_{11}[X]/(X^2+1)$.

Aufgabe 5 (12 Punkte)

Zeigen Sie, dass die Gruppen S_5 und $A_5 \times \mathbb{Z}/2\mathbb{Z}$ nicht isomorph sind.
(Hier bezeichnet S_5 die symmetrische und A_5 die alternierende Gruppe auf 5 Elementen.)

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

(a) Finden Sie alle rationalen Nullstellen des Polynoms $X^3 - 2X + 1 \in \mathbb{Q}[X]$.

(b) Zeigen Sie, dass das Polynom $X^5 + 18X^2 - 15 \in \mathbb{Q}[X]$ irreduzibel ist.

(c) Man zeige $1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(d) Finden Sie i und k, so dass die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 7 & 4 & i & 5 & 6 & k & 9 \end{pmatrix}$ gerade ist.

Aufgabe 2 (12 Punkte)

Es sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, das sowohl reelle als auch nicht reelle Nullstellen hat. Man zeige, dass die Galoisgruppe von f über $\mathbb{Q}$ nicht abelsch ist.

Aufgabe 3 (12 Punkte)

Sei $L|K$ ein Körpererweiterung. Sei $\alpha \in L$ algebraisch über K und sei $F_\alpha \in K[X]$ das Minimalpolynom von α.
Zeigen Sie: Ist $\deg F_\alpha$ ungerade, so gilt $K(\alpha) = K(\alpha^2)$.

Aufgabe 4 (12 Punkte)

Sei G eine nicht abelsche Gruppe der Ordnung $715 = 5 \cdot 11 \cdot 13$. Zeigen Sie:

(a) 5 ist die einzige Primzahl, für die die Anzahl der p-Sylowgruppen von G echt größer als 1 ist.

(b) Sei p die Primzahl aus Aufgabenteil (a) und sei P eine p-Sylowgruppe von G. Bestimmen Sie den Isomorphietyp des Normalisators von P:
$$N_G(P) := \{g \in G \mid ghg^{-1} \in P \text{ für alle } h \in P\}.$$

Aufgabe 5 (12 Punkte)

Es sei die Gleichung $X^2 + uX + v = 0$ mit $u, v \in \mathbb{F}_q$ betrachtet, wobei $\mathbb{F}_q$ der endliche Körper mit q Elementen ist.

(a) Zeigen Sie für ungerades q: Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$, wenn $u^2 - 4v$ ein Quadrat in $\mathbb{F}_q$ ist.

(b) Zeigen Sie für gerades q und $u \neq 0$: Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$, wenn v/u^2 von der Form $z^2 + z$ für ein $z \in \mathbb{F}_q$ ist.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

(a) Seien $k, \ell \in \mathbb{N}_0$ mit $k < \ell$. Betrachte die Polynome $X^{2^k} + 1$ und $X^{2^\ell} - 1$ aus $\mathbb{Q}[X]$. Man zeige, dass $X^{2^k} + 1$ ein Teiler von $X^{2^\ell} - 1$ ist.

(b) Für $m \in \mathbb{N}$ setze $n = 2^{2^m} + 1$. Man beweise, dass $2^{n-1} \equiv 1 \pmod{n}$.

Aufgabe 2 (12 Punkte)

Sei $f(X) \in \mathbb{Z}[X]$ ein Polynom mit ganzzahligen Koeffizienten.

(a) Man zeige für alle $a, c \in \mathbb{Z}$ und $n \in \mathbb{N}$: Aus $a \equiv c \pmod{n}$ folgt $f(a) \equiv f(c) \pmod{n}$.

(b) Man zeige: Sind $f(0)$ und $f(2019)$ ungerade, dann hat f keine ganzzahligen Nullstellen.

(c) Seien p und q zwei verschiedene Primzahlen. Man zeige: Gibt es ein $a \in \mathbb{Z}$, so dass $f(a)$ nicht durch p teilbar ist, und ein $b \in \mathbb{Z}$, so dass $f(b)$ nicht durch q teilbar ist, dann gibt es ein $c \in \mathbb{Z}$, so dass $f(c)$ weder durch p noch durch q teilbar ist.
(Hinweis: Man verwende den chinesischen Restsatz.)

Aufgabe 3 (12 Punkte)

Seien $a \in \mathbb{Q}$, $\beta \in \mathbb{R} \setminus \{0\}$, $i = \sqrt{-1}$ und $\gamma = a + \beta i$ algebraisch über $\mathbb{Q}$. Man zeige, dass $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ gerade ist.

Aufgabe 4 (12 Punkte)

Seien S_3 die symmetrische Gruppe auf $\{1, 2, 3\}$ und $G = S_3 \times S_3$.

(a) Man zeige, dass G genau eine 3-Sylowgruppe hat.

(b) Man gebe drei verschiedene 2-Sylowgruppen P, Q und R von G an, sodass $| P \cap Q | = 1$ ist, aber $| P \cap R | > 1$ gilt.

Aufgabe 5 (12 Punkte)

Sei K ein Körper der Charakteristik $p \neq 0$, seien $a \in K$ und $f := X^p - X - a \in K[X]$.
Zeigen Sie:

(a) Sind L ein Erweiterungskörper von K und $b \in L$ eine Nullstelle von f, dann ist auch $b + 1$ eine Nullstelle von f.

(b) Entweder hat $f := X^p - X - a \in K[X]$ eine Nullstelle in K oder f ist irreduzibel.

(c) Ist f irreduzibel, dann ist die Galoisgruppe von f eine zyklische Gruppe der Ordnung p.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

Seien $a, b, c \in \mathbb{Z}$. Zeigen Sie:

(a) ggT (a, bc) teilt das Produkt ggT $(a, b) \cdot$ ggT (a, c).

(b) ggT (a, bc) kann verschieden sein von ggT $(a, b) \cdot$ ggT (a, c).

(c) ggT $(a, bc) =$ ggT $(a, b) \cdot$ ggT (a, c), falls b und c teilerfremd sind.

Aufgabe 2 (12 Punkte)

Sei H eine Untergruppe der (nicht notwendig endlichen) Gruppe G von endlichem Index $[G : H] = n \in \mathbb{N}$.

(a) Man zeige, dass es für alle $g \in G$ ein $j \in \mathbb{N}$ mit $1 \leq j \leq n$ und $g^j \in H$ gibt.
(Hinweis: Betrachte die Nebenklassen $g^i H$, $0 \leq i \leq n$.)

(b) Man zeige an einem Beispiel, dass in (a) nicht zusätzlich gefordert werden kann, dass j ein Teiler von n ist.

Aufgabe 3 (12 Punkte)

Sei G eine endliche Gruppe. Zeigen Sie:

(a) Falls eine Untergruppe $H \subseteq G$ mit Index $[G : H] = k \in \mathbb{N}$ existiert, so existiert auch ein Normalteiler $N \trianglelefteq G$ mit $N \subseteq H$, so dass die Teilbarkeitsrelationen

$$k \mid [G : N] \text{ und } [G : N] \mid k!$$

erfüllt sind.
(Hinweis: Operation der Gruppe G auf der Menge der Linksnebenklassen von H in G durch Linksmultiplikation.)

(b) Zeigen Sie, dass es keine einfache Gruppe der Ordnung 108 geben kann.

Aufgabe 4 (12 Punkte)

Es bezeichne p eine Primzahl und $\mathbb{F}_p$ einen Körper mit p Elementen. Zeigen Sie:

(a) Ist $g(X) \in \mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$ vom Grad $\deg(g) = m$, so ist die Teilbarkeitsrelation

$$g(X) \mid \left(X^{p^m} - X\right)$$

erfüllt.

(b) Genau dann ist $f(X) \in \mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$, wenn für jedes $m \in \mathbb{N}$ mit $1 \leq m \leq \frac{\deg(f)}{2}$ gilt, dass

$$\mathrm{ggT}\left(f(X), X^{p^m} - X\right) = 1\,.$$

Fortsetzung nächste Seite!

Aufgabe 5 (12 Punkte)

Es seien $p \geq 3$ eine Primzahl und $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel.

(a) Sei $a \in \mathbb{N}$. Zeigen Sie, dass das Polynom $X^{a+1} - 1$ ein Teiler des Polynoms $X^{2a} - X^{a+1} - X^{a-1} + 1$ in $\mathbb{Q}[X]$ ist und bestimmen Sie den Quotienten.

(b) Zeigen Sie, dass die Körpererweiterung $\mathbb{Q}(\zeta + \zeta^{-1}) \mid \mathbb{Q}$ galoissch ist und dass $(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q})$ zyklisch der Ordnung $\frac{p-1}{2}$ ist.

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1:
Sei K ein Körper und $V = K^{2\times 2}$ der K-Vektorraum der 2×2-Matrizen über K. Für $A, B \in K^{2\times 2}$ betrachten wir die Abbildung $\Phi\colon V \to V$, $X \mapsto AXB$.
Zeigen Sie:

(a) Φ ist ein Endomorphismus von V.

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

Aufgabe 2:
Seien $R = \mathbb{Z}/15\mathbb{Z}$ und $f\colon R \to R$, $x \mapsto 7x$.

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

(b) Bestimmen Sie die Fixpunkte von f.

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

Aufgabe 3:

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

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

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

Fortsetzung nächste Seite!

Aufgabe 4:
Sei $\zeta \in \mathbb{C}$ eine primitive elfte Einheitswurzel und $K = \mathbb{Q}(\zeta)$.

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

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

Aufgabe 5:
Ein n-Tupel $(a_1, a_2, \ldots, a_n)$ von ganzen Zahlen heiße *hübsch*, wenn $a_i a_j + 2$ eine Quadratzahl ist für alle $1 \leq i < j \leq n$. Zeigen Sie:

(a) Es gibt hübsche Tripel.

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

(c) Es gibt keine hübschen Quadrupel.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1:
Für $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{C}$ seien a_0, a_1, a_2 die Koeffizienten des Polynoms

$$f(X) := (X - \lambda_1) \cdot (X - \lambda_2) \cdot (X - \lambda_3) = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X].$$

Ferner sei

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

die sogenannte Begleitmatrix zu den gegebenen Zahlen. Zeigen Sie:

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

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

Aufgabe 2:
Zeigen Sie:

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

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

Aufgabe 3:
Seien p eine Primzahl und $\mathbb{F}_p \subset \mathbb{F}_{p^k}$ eine Körpererweiterung vom Grad k über dem Körper $\mathbb{F}_p$. Betrachten Sie die Gruppe $G := \mathrm{GL}_2(\mathbb{F}_{p^k})$ der invertierbaren 2×2-Matrizen über $\mathbb{F}_{p^k}$. Zeigen Sie:

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

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

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

Fortsetzung nächste Seite!

Aufgabe 4:

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

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

(c) Man zeige oder widerlege folgende Aussage: Für alle $a, b, c \in \mathbb{N}$ gilt

$$\mathrm{ggT}(a, b, c)\,\mathrm{kgV}(a, b, c) = abc.$$

Aufgabe 5:

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

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

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

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

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1:
Seien G und G' Gruppen und $f\colon G \to G'$ ein Gruppenhomomorphismus.

(a) Definieren Sie den Begriff *Normalteiler.*

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

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

ist.

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

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

Aufgabe 2:
Berechnen Sie die letzten beiden Ziffern der Zahl

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

Gehen Sie dazu wie folgt vor:

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

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

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

Aufgabe 3:
Sei p eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen und $V = \mathbb{F}_p^n$ für $n \in \mathbb{N}$. Weiter sei $G \leq \mathrm{GL}_n(\mathbb{F}_p)$ eine Gruppe, deren Ordnung eine Potenz von p ist.
Man zeige, dass es einen Vektor $0 \neq v \in \mathbb{F}_p^n$ gibt mit $gv = v$ für alle $g \in G$.
(Hinweis: $|V \setminus \{0\}|$ ist nicht durch p teilbar.)

Fortsetzung nächste Seite!

Aufgabe 4:

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

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

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

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

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

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

Aufgabe 5:

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

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

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

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1:

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

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

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

Aufgabe 2:

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

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

Aufgabe 3:
Sei $V = \mathrm{Mat}_2(\mathbb{Q})$ der $\mathbb{Q}$-Vektorraum der 2×2 Matrizen über $\mathbb{Q}$ und sei $\phi : V \longrightarrow V$ die Linksmultiplikation mit der Matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

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

(b) Entscheiden Sie, ob das charakteristische Polynom von ϕ ist.

(b) Entscheiden Sie, ob das Minimalpolynom von ϕ ist.

Aufgabe 4:
Sei G eine Gruppe und sei H die Untergruppe von G, die aus allen Produkten von Elementen der Form g^2 mit $g \in G$ besteht.

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

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

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

Fortsetzung nächste Seite!

Aufgabe 5:
Sei $\omega = \frac{1}{2}(1 - \sqrt{-3})$.

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

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

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

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

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1:

(a) Bestimmen Sie das $a \in \{0, 1 \ldots, 6\}$ mit $3^{2020} \equiv a \bmod 7$.

Hinweis: Benutzen Sie den kleinen Satz von Fermat.

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

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

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

Aufgabe 2:

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

(a) Die übliche Operation von $GL_2(\mathbb{R})$ auf $\mathbb{R}^2 \setminus \{0\}$ ist transitiv. (Hinweis: Betrachte die Bahn von $v = (1, 0)$).

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

Aufgabe 3:

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

Fortsetzung nächste Seite!

Aufgabe 4:

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

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

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

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

(b) $kG \cong k[X]/(X^n - 1)$,

(c) kG ist kein Integritätsbereich.

Aufgabe 5:

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

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1:
Es sei $f = X^4 + aX + 2 \in \mathbb{Z}[X]$.

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

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

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

Aufgabe 2:
Es sei U eine Untergruppe einer endlichen einfachen Gruppe G vom Index $n := (G : U) \geq 3$.

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

(b) Zeigen Sie, dass $|G|$ ein Teiler von $n!/2$ ist.

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

Aufgabe 3:
Sei R ein Ring mit 1, und seien $a, b \in R$. Es gelte $ab = 1$ und $ba \neq 1$. Insbesondere ist R also nicht kommutativ. Ein Element x in R heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ gibt mit $x^n = 0$. Ein Element x in R heißt *idempotent*, falls $x^2 = x$ gilt.

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

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

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

Aufgabe 4:
Es sei $\mathbb{F}_3$ der Körper mit 3 Elementen. Sei I das von $X^2 + 1$ im Polynomring $R = \mathbb{F}_3[X]$ erzeugte Ideal.

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

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

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

Fortsetzung nächste Seite!

Aufgabe 5:
Gegeben ist das Polynom $f = X^3 - 3X^2 + 3X - 6 \in \mathbb{Q}[X]$. Weiter sei $\zeta = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ eine primitive dritte Einheitswurzel.

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

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

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

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