Aufgaben aus den Algebra-Klausuren des Bayerischen Staatsexamens 1972–2003

Inhalt

Die folgende Aufstellung (ohne Gewähr!) enthält die meisten Aufgaben, die in der Algebra-Klausur des Staatsexamens in Bayern seit 1972 gestellt wurden. Weggelassen habe ich die Aufgaben aus der Geometrie (Differentialgeometrie, Differentialtopologie, Projektive Geometrie, Grundlagen der Geometrie), die nicht mehr zum Kanon der Algebra-Klausuren gehören.

Um die Fülle etwas zu ordnen, habe ich einige Themen-Kästchen gemacht und die Aufgaben nach ihrem Schwerpunkt in die Kästchen gestellt. Die Aufstellung der Kästchen ist in keiner Weise kanonisch, die Einweisung der Aufgaben nach ihrem Schwerpunkt noch willkürlicher. Dennoch scheint mir eine subjektive und anfechtbare Einteilung besser als gar keine zu sein.

Erlangen, Januar 2004 W.-D. Geyer

Inhalt

Staatsexamensaufgaben zur Gruppentheorie

Inhalt

1. Elementare Gruppentheorie

Verknüpfungen

G1.1 [Frühjahr 1972] Sei M eine Halbgruppe, d.h. in M ist eine Multiplikation so erklärt, daß für beliebige $x, y, z \in M$ gilt: $(xy)z = x(yz)$. Auf M sei eine Äquivalenzrelation $\sim$ definiert, und es gelte:

Aus $x \sim x'$ und $y \sim y'$ folgt $xy \sim x'y'$ $(x, x', y, y' \in M)$.

Ferner sei $\widetilde{M}$ die Menge der Äquivalenzklassen $[x] := \{x' \in M\,;\ x' \sim x\}$ und $p:\ M \to \widetilde{M}$ die durch $x \mapsto [x]$ definierte Abbildung. Man zeige:

a) Erklärt man die Multiplikation beliebiger Teilmengen A und B von M vermöge

$$AB := \{xy\,;\ x \in A\,,\ y \in B\} \quad ,$$

so gilt: Zu $[x]$ und $[y]$ aus $\widetilde{M}$ gibt es genau ein $[z]$ aus $\widetilde{M}$ mit $[x][y] \subset [z]$.

b) Es gibt genau eine Multiplikation in $\widetilde{M}$ so, daß $\widetilde{M}$ eine Halbgruppe und p Homomorphismus unter dieser Multiplikation ist.

G1.2 [Frühjahr 1995] Auf der reellen Zahlengeraden $\mathbb{R}$ definiere man die Verknüpfung

$$\circ:\ \mathbb{R} \times \mathbb{R} \to \mathbb{R} \quad , \quad x \circ y := x + y + x^2 y \quad .$$

Man zeige:

a) Es gibt genau ein Einselement $e \in \mathbb{R}$ bezüglich $\circ$.

b) Zu jedem $x \in \mathbb{R}$ gibt es genau ein Rechtsinverses (d.h. es gibt ein $y \in \mathbb{R}$ mit $x \circ y = e$).

c) Für welche $x \in \mathbb{R}$ gibt es ein Linksinverses?

G1.3 [Herbst 1992] Es sei G eine endliche Gruppe mit $|G| = k$, und es sei P die Menge aller Produkte $g_1 g_2 \cdots g_k$ aller Elemente von G. Zeigen Sie:

a) P ist eine Vereinigung von Konjugiertenklassen von G.

b) Ist G kommutativ und k ungerade, so ist $P = \{1\}$.

c) Ist G die symmetrische Gruppe S_3, so ist P die Menge der Transpositionen.

Untergruppen und Normalteiler

G1.4 [Herbst 1974] Man beweise:

a) Ist $(G, \cdot)$ eine Gruppe und sind H, I, J Untergruppen von $(G, \cdot)$ mit $H \subseteq I \cup J$, dann ist $H \subseteq I$ oder $H \subseteq J$.

b) Es gibt eine Gruppe $(G, \cdot)$ mit Untergruppen H, I, J, K, so daß $H \subseteq I \cup J \cup K$, aber weder $H \subseteq I$ noch $H \subseteq J$ noch $H \subseteq K$ gilt.

HINWEIS: Man betrachte $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

G1.5 [Herbst 1981] Die Gruppe G besitze eine Untergruppe vom Index 2. Zeigen Sie: Die Elemente ungerader Ordnung von G erzeugen eine echte Untergruppe von G.

G1.6 [Frühjahr 1973] G sei eine Gruppe, $Q(G)$ das Erzeugnis der Quadrate:

$$Q(G) := \langle g^2 \,;\; g \in G \rangle \quad .$$

a) Man bestimme die Elemente von $Q(\mathfrak{S}_4)$, wobei $\mathfrak{S}_4$ die symmetrische Gruppe vierten Grades ist.

b) Man beweise, daß $Q(G)$ bei jedem Automorphismus von G im ganzen festbleibt.

c) Man bestätige, daß $Q(\mathfrak{A}_n) = \mathfrak{A}_n$ ist, wobei $\mathfrak{A}_n$ die alternierende Gruppe n-ten Grades ist.

d) Man zeige: Hat G eine Untergruppe vom Index 2, so ist $Q(G) \neq G$.

G1.7 [Frühjahr 1980] Es seien U und V Untergruppen der endlichen Gruppe G, und $UV := \{uv \,;\; u \in U\,,\; v \in V\}$.

a) Man beweise die Formel $|UV| = \frac{|U|\cdot|V|}{|U\cap V|}$. ($|X|$ bezeichnet die Kardinalzahl der Menge X).

HINWEIS: Man betrachte etwa ein Repräsentantensystem R der Linksnebenklassen von $U \cap V$ in U und weise nach:

i) $UV = \bigcup\limits_{r\in R} rV$,

ii) $r_1, r_2 \in R \quad , \quad r_1 \neq r_2 \quad \Longrightarrow \quad r_1V \neq r_2V$.

b) V sei Normalteiler von G, und die Zahlen $|U|$ und $[G:V]$ seien teilerfremd. Man zeige:

i) UV ist Untergruppe von G,

ii) $[UV:V]$ ist Teiler von $|U|$ und $[G:V]$,

und folgere $U \subset V$.

c) V sei Normalteiler von G, und $|V|$, $[G:V]$ seien teilerfremd. Man zeige: Wenn G Normalteiler einer Gruppe H ist, ist auch V Normalteiler von H.

G1.8 [Herbst 1994] Seien S und T Untergruppen einer endlichen Gruppe G. Man zeige:

a) $|S|\cdot|T| \leq |S\cap T|\cdot|\langle S\cup T\rangle|$.

b) In a) gilt Gleichheit, wenn S Normalteiler in G ist.

G1.9 [Frühjahr 1999] Seien U und V Untergruppen einer endlichen Gruppe G mit $U \cap V = \{1\}$. Es bezeichne $\langle U \cup V\rangle$ die von $U \cup V$ erzeugte Untergruppe von G. Man zeige:

a) $|U|\cdot|V| \leq |\langle U\cup V\rangle|$.

b) In a) gilt Gleichheit, wenn U Normalteiler in G ist.

c) Man gebe eine Gruppe G mit zwei Untergruppen U und V mit $U \cap V = \{1\}$ an, so dass in a) nicht Gleichheit besteht.

G1.10 [Frühjahr 1996] Sei G eine Gruppe und U eine Untergruppe. Zeigen Sie, daß folgende Aussagen äquivalent sind:

i) Für alle $g \in G$ gilt: $gU = Ug$.

ii) Die Menge der Rechtsnebenklassen und die Menge der Linksnebenklassen von G nach U stimmen überein: $G/U = U\backslash G$.

iii) Die „Definition“ $gU \circ hU := ghU$ definiert eine Verknüpfung auf den Linksnebenklassen, das heißt, eine Abbildung $G/U \times G/U \to G/U$.

G1.11 [Herbst 1978] Man beweise, daß eine Gruppe genau dann endlich ist, wenn sie nur endlich viele Untergruppen hat.

Homomorphismen

G1.12 [Frühjahr 1977] Sei G eine Gruppe. Zeigen Sie:

a) Für $G = (\mathbb{Z}/2\mathbb{Z}, +)$ zeige man, daß $\operatorname{Aut} G = \{\mathrm{id}\}$. ($\operatorname{Aut} G$ sei die Gruppe aller Gruppenautomorphismen von G.)

b) G ist genau dann abelsch, wenn die Abbildung $\varphi: G \to G$ mit $\varphi(x) := x^{-1}$ ein Gruppenautomorphismus ist.

c) Für $a \in G$ ist $\psi: G \to G$ mit $\psi(x) = axa^{-1}$ ein Gruppenautomorphismus.

d) Ist $\operatorname{Aut} G = \{\mathrm{id}\}$, so ist G abelsch.

e) Ist $\operatorname{Aut} G = \{\mathrm{id}\}$, so gilt $x^2 = e$ für alle $x \in G$. (e ist das neutrale Element von G.)

f) Ist $\operatorname{Aut} G = \{\mathrm{id}\}$, so ist G ein Vektorraum über dem Körper $\mathbb{Z}/2\mathbb{Z}$.

g) Ist $\operatorname{Aut} G = \{\mathrm{id}\}$, so ist $G = 0$ oder $G \simeq (\mathbb{Z}/2\mathbb{Z}, +)$.

G1.13 [Frühjahr 1989] G sei eine Gruppe und S^1 die multiplikative Gruppe der komplexen Zahlen vom Betrag 1. Ferner bezeichne $\operatorname{Hom}(G, S^1)$ die Menge aller Gruppenhomomorphismen $G \to S^1$.
Bestimmen Sie die Elementezahl von $\operatorname{Hom}(G, S^1)$, wenn

a) $G = S_n$, die symmetrische Gruppe n-ten Grades,

b) G zyklisch von der Ordnung n,

c) $G = D_n$, die Diedergruppe n-ten Grades

ist.

G1.14 [Frühjahr 1991] Sei $\alpha: G \to H$ ein Gruppenhomomorphismus, wobei H abelsch sei. Man zeige: α ist genau dann surjektiv, wenn für je zwei Gruppenhomomorphismen $\beta, \gamma: H \to K$ mit $\beta \circ \alpha = \gamma \circ \alpha$ gilt: $\beta = \gamma$.

G1.15 [Frühjahr 1994] Es sei p eine ungerade Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen und $\mathbb{F}_p^\times$ seine multiplikative Gruppe. Es sei φ der Endomorphismus

$$\varphi: \mathbb{F}_p^\times \to \mathbb{F}_p^\times \quad , \quad x \mapsto x^2 \quad .$$

Man bestimme die Ordnungen von Kern φ und Bild φ.
Man beweise mittels dieser Ergebnisse, daß es in $\mathbb{F}_p$ genau $\frac{p+1}{2}$ Quadrate gibt.

G1.16 [Herbst 1996] Seien G eine Gruppe, N ein Normalteiler in G und $\nu: G \to G/N$ der natürliche Epimorphismus auf die Faktorgruppe G/N. Man zeige:

a) ν induziert eine Bijektion von der Menge aller Normalteiler H von G mit $N \subseteq H$ auf die Menge aller Normalteiler von G/N.

b) Gibt es einen Normalteiler vom Index 4 in G, dann auch einen vom Index 2.

G1.17 [Herbst 1974] G sei eine endliche Gruppe und φ ein Automorphismus von G, für den $\varphi(x) = x$ nur für $x = e$ (e neutrales Element von G) gilt. Man zeige:

a) Die Abbildung $y \mapsto y^{-1}\varphi(y)$ von G in sich ist injektiv.

b) Zu jedem $x \in G$ gibt es ein $y \in G$ mit $x = y^{-1}\varphi(y)$.

c) Wenn zusätzlich $\varphi^2 = \mathrm{id}$ (id ist die Bezeichnung für die identische Abbildung) gilt, dann folgt

i. $\varphi(x) = x^{-1}$ für alle $x \in G$,

ii. G ist abelsch.

G1.18 [Frühjahr 1975] In einer Gruppe G sei die Abbildung $x \mapsto x^3$ ein Automorphismus. Man beweise: G ist abelsch.

Kommutatorgruppen und Zentrum

G1.19 [Herbst 1976] Es sei G eine Gruppe, ferner G' die Kommutatorgruppe von G, erzeugt von der Menge $\{[a,b] = aba^{-1}b^{-1}\,;\ a,b \in G\}$ der Kommutatoren. Ferner sei

$$U := \{cg^2\,;\ c \in G'\,,\ g \in G\} \quad .$$

Man zeige:

a) $g,h \in G \implies g^2h^2 \in U$.

b) U ist Untergruppe von G.

c) U ist Normalteiler von G.

d) Für alle $\bar{g} \in G/U$ gilt $\bar{g}^2 = \bar{e}$ ($\bar{e}$ neutrales Element).

e) Ist die Ordnung $|G|$ ungerade, dann gilt $G = U$.

G1.20 [Frühjahr 1992] Ist G eine Gruppe, so bezeichnet

$$[G,G] = \langle aba^{-1}b^{-1}\,;\ a,b \in G\rangle$$

die *Kommutatoruntergruppe* von G; diese ist offenbar normal in G. Es bezeichne $\langle a\rangle$ die von einem Element $a \in G$ erzeugte zyklische Untergruppe.

a) Zeigen Sie: Die Faktorgruppe G/H einer Gruppe G nach einer normalen Untergruppe H von G ist genau dann abelsch, wenn $H \supseteq [G,G]$ gilt.

b) Sei G eine endliche Gruppe, die eine zyklische normale Untergruppe $A = \langle a\rangle$ der Ordnung m enthalte, so daß $G/A = \langle bA\rangle$ zyklisch der Ordnung s ist. Es gelte $b^{-1}ab = a^r$ für irgendein r. Zeigen Sie:
Die Kommutatoruntergruppe von G ist die Untergruppe $\langle a^{r-1}\rangle$ und hat die Ordnung $\frac{m}{(r-1,m)}$, wobei $(r-1,m)$ der größte gemeinsame Teiler von $r-1$ und m ist.

G1.21 [Herbst 1981] G sei eine Gruppe und Z ihr Zentrum. Man zeige: G ist abelsch, falls G/Z zyklisch ist.

G1.22 [Herbst 1982] Beweisen Sie, daß die Gruppe der inneren Automorphismen einer nichtabelschen Gruppe nicht zyklisch ist.

G1.23 [Frühjahr 1994] Sei G eine endliche Gruppe. Sei Z ihr Zentrum, K ihre Kommutatorgruppe. Beweisen oder widerlegen Sie:

a) G/K zyklisch $\Longrightarrow$ G abelsch.

b) G/Z zyklisch $\Longrightarrow$ G abelsch.

Gruppen kleiner Ordnung

G1.24 [Frühjahr 1972] Die Gruppe G mit neutralem Element e sei gegeben durch das Erzeugendensystem $\{a, b\}$ $(e \neq a \neq b \neq e)$ und die Relationen $a^2 = b^2 = e,\ ab = ba$.

a) Welche Ordnung hat G?

b) Es gibt eine symmetrische Gruppe $\mathfrak{S}_n$ kleinster Ordnung so, daß G isomorph zu einer Untergruppe H von $\mathfrak{S}_n$ ist. Man gebe die natürliche Zahl n, einen Isomorphismus $f: G \to H$ und die Zyklenzerlegung der Elemente von H an.

c) Wieviele innere Automorphismen gestattet G?

d) Man bestimme die Automorphismengruppe von G.

G1.25 [Frühjahr 1982] Man beweise, daß es bis auf Isomorphie genau zwei Gruppen der Ordnung 6 gibt, nämlich die zyklische Gruppe $\mathbb{Z}/6\mathbb{Z}$ und die symmetrische Gruppe S_3.

G1.26 [Herbst 1991] Man beweise, daß es bis auf Isomorphie genau zwei Gruppen der Ordnung 6 gibt. (Die Sylowsätze dürfen für die Lösung benutzt werden, nicht aber allgemeine Sätze für Gruppen von der Ordnung pq, wobei p und q Primzahlen sind.)

G1.27 [Herbst 1993] Es bezeichne $\mathrm{M}(2 \times 2, S)$ den Ring aller 2-reihigen Matrizen mit Koeffizienten aus einem Ring S. Sei

$$\mathrm{O}(2) := \{A \in \mathrm{M}(2 \times 2, \mathbb{R}) : {}^tAA = 1\}$$

die Gruppe der reellen orthogonalen 2-reihigen Matrizen.

a) Man zeige:

$$G := \mathrm{O}(2) \cap \mathrm{M}(2 \times 2, \mathbb{Z})$$

ist eine Gruppe der Ordnung 8.

b) G besitzt genau eine zyklische Untergruppe G_0 der Ordnung 4.

c) Für alle $d \in G_0$ und $s \in G \backslash G_0$ gilt

$$sd = d^{-1}s \quad .$$

G1.28 [Herbst 1993]

a) Man zeige, daß die Gruppe $\mathrm{GL}(2, \mathbb{F}_2)$ der invertierbaren 2×2-Matrizen mit Koeffizienten aus dem Körper $\mathbb{F}_2$ isomorph zur symmetrischen Gruppe S_3 ist.

HINWEIS: Man betrachte die Wirkung auf den von 0 verschiedenen Vektoren des $\mathbb{F}_2^2$.

b) Sei G die Gruppe der Ordnung 8 aus der vorigen Aufgabe und

$$\varphi: G \to \mathrm{GL}(2, \mathbb{F}_2)$$

die natürliche Abbildung. Man zeige: Der Kern von φ ist eine Untergruppe der Ordnung 4, die nicht zu G_0 isomorph ist.

G1.29 [Herbst 1997] Sei $G = S_4$ die Gruppe der Permutationen von $\{1,2,3,4\}$.

a) Geben Sie eine nicht zyklische Untergruppe H der Ordnung 4 von G an, die auf $\{1,2,3,4\}$ transitiv ist.

b) Zeigen Sie, daß H normal ist.

c) Zeigen Sie, daß durch $f(g)(h) := ghg^{-1}$ für $g \in G$ und $h \in H$ ein Homomorphismus $f : G \to \mathrm{Aut}(H)$ definiert wird, der surjektiv ist und der den Kern H hat.

G1.30 [Frühjahr 1999]

a) Sei C_8 die zyklische Gruppe der Ordnung 8. Man zeige, daß die Automorphismengruppe $\mathrm{Aut}(C_8)$ isomorph zur Kleinschen Vierergruppe V ist.

b) Man zeige, daß die Automorphismengruppe $\mathrm{Aut}(V)$ der Kleinschen Vierergruppe V isomorph zur symmetrischen Gruppe S_3 ist.

G1.31 [Frühjahr 2000] Man entscheide, für welche $n = 2,3,4$ die symmetrische Gruppe S_n eine nichttriviale normale Sylowuntergruppe besitzt.

G1.32 [Herbst 1991] Man gebe eine nichtabelsche Gruppe G der Ordnung 24 an, die nicht zur symmetrischen Gruppe S_4 isomorph ist.

G1.33 [Herbst 1986] Geben Sie eine Gruppe der Ordnung 36 an, deren Zentrum die Ordnung 6 besitzt.

G1.34 [Herbst 2001] Für $3 \leq n$ sei D_n die Diedergruppe der Ordnung $2n$, es sei H die Quaternionengruppe der Ordnung 8, es sei Z_2 die zyklische Gruppe der Ordnung 2 und S_3 sei die symmetrische Gruppe auf 3 Elementen.

a) Zeigen Sie: Die drei Gruppen $D_8, D_4 \times Z_2$ und $H \times Z_2$ sind paarweise nicht isomorph.

b) Bestimmen Sie für jede der drei Gruppen aus a) die Anzahl der zyklischen Untergruppen der Ordnung 4 und geben Sie jeweils die Menge dieser Untergruppen an.

c) Zeigen Sie: Die Gruppen D_6 und $S_3 \times Z_2$ sind isomorph.

Zyklische Gruppen

G1.35 [Herbst 1976] Sei $p \geq 2$ eine Primzahl. Zeige: Die Einheitengruppe von $\mathbb{Z}/p\mathbb{Z}$ ist zyklisch.

HINWEIS: Sei $p-1 = q_1^{\alpha_1} \cdot \ldots \cdot q_r^{\alpha_r}$ die kanonische Primzahlpotenzzerlegung von $p-1$. Man beweise, daß es Elemente $a_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit der Ordnung $q_i^{\alpha_i}$ gibt, indem man $(\mathbb{Z}/p\mathbb{Z})^\times$ in den Körper $\mathbb{Z}/p\mathbb{Z}$ einbettet und dann die Elemente von $(\mathbb{Z}/p\mathbb{Z})^\times$ als Einheitswurzeln auffaßt.

G1.36 [Herbst 1977] Sei G eine zyklische Gruppe der Ordnung n, sei $x \in G$ ein erzeugendes Element von G, seien $r, s \in \mathbb{N}$ mit $rs = n$. Man zeige:

a) $\langle x^s \rangle = \{y \in G\,;\; y^r = e\}$, wobei $\langle x^s \rangle$ die von x^s erzeugte Untergruppe von G bezeichnet.

b) Die Ordnung von $\langle x^s \rangle$ ist r.

G1.37 [Herbst 1977] Die Anzahl der Elemente der Ordnung r einer zyklischen Gruppe der Ordnung r wird mit $\phi(r)$ bezeichnet ($\phi : \mathbb{N} \to \mathbb{N}$ heißt die *Eulersche Funktion*). Man zeige:

Für $n \in \mathbb{N}$ gilt

$$n = \sum_{\substack{r \in \mathbb{N} \\ r \mid n}} \phi(r) \quad .$$

G1.38 [Herbst 1977] Sei G eine Gruppe der Ordnung n mit neutralem Element e, für $r \in \mathbb{N}$ sei G_r die Menge der Elemente der Ordnung r von G.

a) Man zeige, daß G disjunkte Vereinigung der Teilmengen G_r mit $r \in \mathbb{N}$ und $r \mid n$ ist.

b) Für alle $r \in \mathbb{N}$, $r \mid n$, besitze die Menge $\{y \in G;\ y^r = e\}$ höchstens r Elemente. Man zeige, daß G zyklisch ist.

ANLEITUNG: Man zeige zuerst, daß $G_r = \{g \in G;\ \mathrm{ord}(g) = r\}$ für alle $r \in \mathbb{N}$, $r \mid n$, höchstens $\phi(r)$ Elemente besitzt, indem man im Fall $G_r \neq \varnothing$ die von einem Element $z \in G_r$ erzeugte Untergruppe betrachtet. Dann zeige man mit den vorstehenden Aufgaben, daß G_r für alle $r \in \mathbb{N}$, $r \mid n$, genau $\phi(r)$ Elemente besitzt und beachte den Spezialfall $r = n$.

G1.39 [Herbst 1977] Sei K ein Körper, G eine Untergruppe der Ordnung n der multiplikativen Gruppe $K \setminus \{0\}$. Man zeige mit der vorigen Aufgabe, daß G zyklisch ist.

G1.40 [Herbst 1983] Für eine endliche Gruppe G mit mindestens zwei Elementen sind die folgenden drei Eigenschaften äquivalent:

a) Für beliebige Untergruppen U, V von G gilt entweder $U \subseteq V$ oder $V \subseteq U$.

b) G hat genau eine maximale Untergruppe.

c) G ist zyklisch von Primzahlpotenz.

G1.41 [Frühjahr 1990] Sei G eine Gruppe der Ordnung n. Zeigen Sie:

a) Gibt es in G für jeden Teiler d von n höchstens eine Untergruppe der Ordnung d, so ist G zyklisch.

b) Ist das System der Untergruppen von G linear geordnet, so ist G eine zyklische p-Gruppe.

Direkte Produkte

G1.42 [Herbst 1982] Die Gruppe G besitze zwei Normalteiler M und N, so daß

$$G/M \simeq S_5 \quad , \quad G/N \simeq S_6 \quad \text{und} \quad M \cap N = \{1\} \quad ,$$

wobei S_n die symmetrische Gruppe n-ten Grades bezeichnet. Geben Sie (bis auf Isomorphie) alle Gruppen G an, in denen diese Bedingungen erfüllt sind.

G1.43 [Frühjahr 1984] Sei G eine Gruppe mit der Einsuntergruppe 1 und $P = G \times G$ das direkte Produkt von G mit sich selbst. Es sei $G_1 = G \times 1$ und $G_2 = 1 \times G$. Zeigen Sie:

a) Die Diagonale $D = \{(g, g);\ g \in G\}$ ist eine Untergruppe von P.

b) Für jede Untergruppe U zwischen D und P gilt:
$U \cap G_i$ ist normal in G_i für $i = 1, 2$.

c) Genau dann ist D eine maximale Untergruppe von P, wenn G einfach ist.

Semidirekte Produkte

G1.44 [Herbst 1980] Es sei K ein kommutativer Körper. Die Menge aller Matrizen der Form

$$\begin{pmatrix} a & 0 & 0 \\ b & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \qquad \text{mit} \quad a, b \in K\,,\ a \neq 0$$

werde mit M bezeichnet. Zeigen Sie:

a) Mit der Matrizenmultiplikation als Verknüpfung ist M eine Gruppe.

b) Sei T die Menge der Matrizen aus M mit $a = 1$. Je zwei von der Einheitsmatrix verschiedene Elemente aus T sind konjugiert (in M).

c) Folgern Sie, daß T minimaler Normalteiler von M ist.

G1.45 [Frühjahr 1983] Sei $\mathbb{Q}$ der Körper der rationalen Zahlen. Sei A die Automorphismengruppe des Polynomrings $\mathbb{Q}[x]$. Zeigen Sie die Existenz von Untergruppen H und K der Gruppe A, so daß folgende Aussagen gelten:

a) H ist isomorph zu additiven Gruppe von $\mathbb{Q}$.

b) K ist isomorph zur multiplikativen Gruppe von $\mathbb{Q}$.

c) $A = HK$ (Komplexprodukt)

d) H ist ein Normalteiler von A.

G1.46 [Frühjahr 1986]

a) Es seien $\mathbb{F}_q$ ein endlicher Körper mit $q \geq 3$ Elementen und U eine Untergruppe der Ordnung $r \geq 2$ der multiplikativen Gruppe $\mathbb{F}_q^\times$. Man verifiziere, daß

$$G := \left\{ \begin{pmatrix} \lambda & 0 \\ \alpha & 1 \end{pmatrix};\ \alpha \in \mathbb{F}_q\,,\ \lambda \in U \right\}$$

eine nicht-kommutative Untergruppe von $\mathrm{GL}(2, \mathbb{F}_q)$ ist.

b) Es gebe — bis auf Isomorphie — nur **eine** Gruppe der Ordnung $n \in \mathbb{N}$. Man weise nach, daß n quadratfrei ist und daß für je zwei Primteiler p, q von n stets $p \nmid q - 1$ gilt.
(*quadratfrei* bedeutet, daß eine Darstellung in der Form $n = d^2 k$ mit $d, k \in \mathbb{N}$, $d \geq 2$ nicht möglich ist.)

G1.47 [Herbst 1986] Sei $\mathbb{F}_q$ der Körper mit q Elementen und $\mathbb{F}_q^\times$ seine multiplikative Gruppe. Auf $G := \mathbb{F}_q^\times \times \mathbb{F}_q$ ist durch

$$(a, b) \cdot (a', b') = (aa', ab' + b)$$

eine Verknüpfung erklärt. Zeigen Sie:

a) G ist mit dieser Verknüpfung eine Gruppe.

b) Für $q > 2$ ist G nicht abelsch.

c) $H := 1 \times \mathbb{F}_q$ ist ein Normalteiler in G mit $G/H \simeq \mathbb{F}_q^\times$.

d) H ist die einzige Untergruppe der Ordnung q in G.

G1.48 [Herbst 1993] Es sei $\mathbb{F}_q$ der endliche Körper mit q Elementen, $\mathbb{F}_q^\times$ seine multiplikative Gruppe. Auf der Menge $G = \mathbb{F}_q^\times \times \mathbb{F}_q$ ist durch $(s,u)\cdot(t,v) := (st, sv+u)$ eine assoziative Verknüpfung erklärt. Man zeige:

a) Falls $q > 2$, so bildet G versehen mit dieser Verknüpfung eine nicht abelsche Gruppe.

b) Die Menge $U = \{(1,u)\,;\ u \in \mathbb{F}_q\}$ ist eine normale Untergruppe von G, und es gilt

$$G/U \simeq \mathbb{F}_q^\times \quad .$$

c) Die einzige Untergruppe der Ordnung q in G ist U.

G1.49 [Frühjahr 1995] Seien E, G Gruppen und $\pi: E \to G$ ein Epimorphismus. π heißt *zerfallend*, falls ein Homomorphismus $\rho: G \to E$ mit $\pi\rho = \mathrm{id}_G$ existiert.
Zeigen Sie: Ist π ein zerfallender Epimorphismus mit Kern K, so ist

$$K \times G \to E\,, \qquad (k,g) \mapsto k\rho(g) \ \text{ für alle } \ k \in K \ \text{ und } \ g \in G \quad ,$$

ein Isomorphismus, falls $K \times G$ mit der Gruppenstruktur des semidirekten Produkts bezüglich einer passenden Operation von G auf K versehen wird.

G1.50 [Frühjahr 1997]

a) Es sei p eine Primzahl. Beweisen Sie, daß es genau zwei Isomorphieklassen von Gruppen der Ordnung $2p$ gibt. Beachten Sie dabei die Fallunterscheidung $p = 2$ und $p \neq 2$.

b) Sei $p \neq 2$ und G die nichtzyklische Gruppe der Ordnung $2p$. Bestimmen Sie in G die Anzahl der Elemente der Ordnung 2 und die der Ordnung p.

G1.51 [Herbst 1997] Gegeben seien eine Primzahl p, eine natürliche Zahl n mit $q = p^n > 2$ und ein Primteiler r von $q-1$. Wie üblich bezeichne $\mathbb{F}_q$ den Körper mit q Elementen.

a) Zeigen Sie, daß die multiplikative Gruppe $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ ein Element γ der Ordnung r enthält und daß die Menge

$$G = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_q)\,;\ \alpha \in \mathbb{F}_q\,,\ \beta \in \langle\gamma\rangle \right\}$$

eine Untergruppe der Ordnung qr von $\mathrm{GL}(2,\mathbb{F}_q)$ ist. Dabei ist $\langle\gamma\rangle$ die von γ erzeugte Untergruppe von $\mathbb{F}_q^\times$.

b) Bestimmen Sie die Ordnungen der Elemente von G.

c) Geben Sie die Anzahl der p- und der r-Sylowgruppen von G an.

2. Abelsche Gruppen

Elemente der Ordnung 2

G2.1 [Frühjahr 1986] Sei G eine endliche abelsche Gruppe und $G_2 := \{g \in G\,;\ g = -g\}$. Zeigen Sie:

a) G_2 ist eine Untergruppe von G, isomorph zu $(\mathbb{Z}/2\mathbb{Z})^r$, $r \geq 0$.

b) $\sum_{x\in G} x = \sum_{y\in G_2} y \quad$ und $\quad 2 \cdot \sum_{x\in G} x = 0$.

c) Genau dann ist $\sum_{x\in G} x \neq 0$, wenn $G_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

G2.2 [Herbst 1993] Sei $(G, +)$ eine endliche abelsche Gruppe mit neutralem Element 0 und

$$G_2 := \{x \in G\,;\ 2x = 0\} \quad .$$

Man setzt

$$\sigma(G) := \sum_{x\in G} x \quad .$$

Zeigen Sie:

a) G_2 ist eine Untergruppe von G, und es ist $\sigma(G) = \sigma(G_2)$.

HINWEIS: Betrachten Sie auf G die Äquivalenzrelation

$$x \sim y \iff x = y \ \text{ oder } \ x = -y \qquad (x, y \in G) \quad .$$

b) Ist $\#G_2 \neq 2$, so ist $\sigma(G) = 0$; ist $\#G_2 = 2$, so ist $\sigma(G)$ das von 0 verschiedene Element aus G_2.

c) Genau dann ist $\#G_2 = 2$, wenn die 2-Sylowgruppe von G zyklisch und $\neq 0$ ist.

d) Sei $p \in \mathbb{N}$ eine Primzahl. Folgern Sie durch Anwendung von a), b) und c) auf die multiplikative Gruppe $G := (\mathbb{Z}/p\mathbb{Z})^\times$ die Aussage

$$(p-1)! \equiv -1 \mod p \quad .$$

G2.3 [Herbst 2001]

a) G sei eine endliche abelsche Gruppe, p das Produkt aller Elemente von G. Zeigen Sie:

$$p = \begin{cases} 1 & \text{falls } G \text{ kein oder mehr als ein Element der Ordnung 2 hat} \\ a & \text{sonst, wobei } a \text{ dann das einzige Element der Ordnung 2 von } G \text{ ist.} \end{cases}$$

b) Zeigen Sie: Jede natürliche Zahl $n \neq 4$ teilt die Zahl $((n-1)!)^2 + (n-1)!$.

G2.4 [Frühjahr 1993] Es seien N eine natürliche Zahl, G eine abelsche Gruppe der Ordnung 2^N und A die Anzahl der Elemente der Ordnung 2 in G.

a) Ist die Anzahl s der Faktoren in der Zerlegung von G in ein direktes Produkt von zyklischen Gruppen eindeutig durch A bestimmt? (Beweis oder Gegenbeispiel!)

b) Ist der Isomorphietyp von G eindeutig durch A bestimmt? (Beweis oder Gegenbeispiel!)

Exponent einer abelschen Gruppe

G2.5 [Frühjahr 1976] G sei eine Gruppe mit Einselement e. Die Exponenten $k \in \mathbb{Z}$ mit $x^k = e$ für alle $x \in G$ bilden ein Ideal (m) im Ring $\mathbb{Z}$ der ganzen Zahlen; die durch $m \geq 0$ eindeutig fixierte Erzeugende m heißt der *Exponent* der Gruppe G. Man zeige:

a) Der Exponent m von G ist das kleinste gemeinsame Vielfache der Elementordnungen in G; bei endlichem G ist m überdies ein Teiler der Gruppenordnung, der durch jeden Primteiler der Gruppenordnung teilbar ist.

b) Bei abelschem G und $m > 0$ tritt jeder Teiler des Exponenten als Elementordnung auf.

c) In einer abelschen Gruppe G mit Primzahlexponent p (elementar-abelsche p-Gruppe) ist jede Untergruppe U Bestandteil einer direkten Zerlegung $G = U \times V$.

HINWEIS: Man verschaffe sich eine maximale zu U fremde Untergruppe.

G2.6 [Frühjahr 1973] Sei G eine multiplikative, endliche, abelsche Gruppe mit dem neutralen Element e. Für $g \in G$ sei $\operatorname{ord}(g)$ definiert als die Ordnung der durch g erzeugten Untergruppe von G.
Es bezeichne $\operatorname{ggT}(m,n)$ den größten gemeinsamen Teiler und $\operatorname{kgV}(m,n)$ das kleinste gemeinsame Vielfache der natürlichen Zahlen m und n. Zeige:

a) $\operatorname{ord}(g)$ ist die kleinste natürliche Zahl m mit $g^m = e$ und aus $g^m = e$ folgt, daß $\operatorname{ord}(g)$ Teiler von m ist.

b) Sind $g, h \in G$ mit $\operatorname{ggT}(\operatorname{ord}(g), \operatorname{ord}(h)) = 1$, dann gilt $\operatorname{ord}(gh) = \operatorname{ord}(g)\operatorname{ord}(h)$.

c) Seien $g, h \in G$ und $s := \operatorname{ord}(g)$, $t := \operatorname{ord}(h)$ und sei $d := \operatorname{ggT}(s,t)$. Zerlege d in einer Form $d = d_1 d_2$, so daß

$$\operatorname{ggT}\left(\frac{s}{d_1}, \frac{t}{d_2}\right) = 1$$

gilt und gib ein Element $k \in G$ mit $\operatorname{ord}(k) = \frac{st}{d}$ $(= \operatorname{kgV}(s,t))$ an.

d) Ist g ein Element maximaler Ordnung in G, dann gilt für jedes Element $h \in G$, daß $\operatorname{ord}(h)$ Teiler von $\operatorname{ord}(g)$ ist.

e) Sei jetzt K ein Körper und sei K^* die multiplikative Gruppe der Elemente $\neq 0$ aus K.
Zeige: Jede endliche Untergruppe G von K^* ist zyklisch.

HINWEIS: Man verwende ein geeignetes Polynom aus $K[X]$

G2.7 [Frühjahr 1978] Sei G eine multiplikative, endliche, abelsche Gruppe mit dem neutralen Element e. Für $g \in G$ bezeichne $\operatorname{ord}(g)$ die Ordnung der durch g erzeugten Untergruppe von G.
Es bezeichne $\operatorname{ggT}(m,n)$ den größten gemeinsamen Teiler und $\operatorname{kgV}(m,n)$ das kleinste gemeinsame Vielfache der natürlichen Zahlen m und n. Zeige:

a) $\operatorname{ord}(g)$ ist die kleinste natürliche Zahl m mit $g^m = e$, und aus $g^m = e$ folgt, daß $\operatorname{ord}(g)$ Teiler von m ist.

b) Sind $g, h \in G$ mit $\operatorname{ggT}(\operatorname{ord}(g), \operatorname{ord}(h)) = 1$, dann gilt: $\operatorname{ord}(gh) = \operatorname{ord}(g)\operatorname{ord}(h)$.

c) Seien $g, h \in G$ und $s := \operatorname{ord}(g), t := \operatorname{ord}(h)$ und sei $d := \operatorname{ggT}(s,t)$. Zerlege d in der Form $d = d_1 d_2$, so daß gilt

$$\operatorname{ggT}\left(\frac{s}{d_1}, \frac{t}{d_2}\right) = 1 \quad ,$$

und gib ein Element $k \in G$ mit $\operatorname{ord}(k) = \frac{st}{d} = \operatorname{kgV}(s,t)$ an.

d) Ist g ein Element maximaler Ordnung in G, dann gilt für jedes Element $h \in G$, daß $\mathrm{ord}(h)$ Teiler von $\mathrm{ord}(g)$ ist.

e) Sei jetzt K ein Körper und sei $K^\times$ die multiplikative Gruppe der Elemente $\neq 0$ aus K. Zeige: Jede endliche Untergruppe G von $K^\times$ ist zyklisch.

HINWEIS: Man verwende ein geeignetes Polynom aus $K[X]$.

G2.8 [Frühjahr 1999] Unter dem Exponenten einer endlichen Gruppe G versteht man die kleinste natürliche Zahl $m \geq 1$, für die $g^m = 1$ für alle $g \in G$ gilt.

a) Man bestimme den Exponenten der symmetrischen Gruppe S_7.

b) Sei G eine endliche abelsche Gruppe mit dem Exponenten m. Man zeige, dass eine Untergruppe $G_1 \leq G$ existiert, so dass G isomorph zu $\mathbb{Z}/m\mathbb{Z} \times G_1$ ist.

Direkte Zerlegung

G2.9 [Herbst 1992] Es seien $m_1, m_2, \ldots, m_r$ durch 3 teilbare natürliche Zahlen, und sei G die abelsche Gruppe

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \quad .$$

a) Man bestimme die Anzahl der Elemente von G der Ordnung 3.

b) Man bestimme die Anzahl der Untergruppen von G der Ordnung 3.

G2.10 [Herbst 1998] Sei p eine Primzahl und G die additive Gruppe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

a) Wieviele Untergruppen der Ordnung p besitzt G?

b) Seien $x, y \in G$ mit $x \neq y$ gegeben. Man zeige, dass es genau eine Untergruppe $H < G$ der Ordnung p gibt, für die $x + H = y + H$ gilt.

c) Zu einer sechstägigen Konferenz treffen sich 25 Teilnehmer. Die sechs gemeinsamen Mittagessen nehmen sie an 5 Tischen mit je 5 Plätzen ein. Ist es möglich, täglich wechselnde Sitzordungen derart festzulegen, dass jeder Teilnehmer mit jedem anderen genau einmal am gleichen Tisch sitzt?

G2.11 [Frühjahr 1975] Zeige: Ist $Q = \mathbb{Q}^+$ Untergruppe einer abelschen Gruppe A, dann gibt es eine Untergruppe B von A mit

$$A = Q + B \quad , \quad Q \cap B = 0 \quad .$$

HINWEIS: Sei B ein maximales Element (Existenz?!) in

$$\{X\,;\ X \text{ Untergruppe von } A \text{ mit } Q \cap X = 0\} \quad .$$

Ist dann $a \in A$, so gibt es eine kleinste natürliche Zahl m mit $am \in Q + B$. Folgere $am = qm + u$, $q \in Q$, $u \in B$ und daraus $a - q \in B$.

G2.12 [Herbst 1982] G sei eine (additiv geschriebene) abelsche Gruppe und $T(G)$ die Menge aller Elemente endlicher Ordnung von G. Die Gruppe G heißt *torsionsfrei*, wenn $T(G) = \{0\}$ gilt.

a) Zeigen Sie, daß $T(G)$ eine Untergruppe von G ist und daß $G/T(G)$ torsionsfrei ist.

b) Was wissen Sie über die Struktur einer endlich erzeugten torsionsfreien abelschen Gruppe?

c) $\mathbb{R}$ und $\mathbb{Z}$ werden als Gruppen bzgl. der Addition betrachtet. Zeigen Sie, daß $T(\mathbb{R}/\mathbb{Z})$ ein direkter Summand von $\mathbb{R}/\mathbb{Z}$ ist.

G2.13 [Frühjahr 1980] G sei eine (additiv geschriebene) abelsche Gruppe der Ordnung $p_1^{n_1}p_2^{n_2}$, wobei p_1, p_2 Primzahlen sind $(p_1 \neq p_2)$ und n_1, n_2 natürliche Zahlen > 0. Sei $G(p_i)$ die Menge aller Elemente von G, deren Ordnung eine Potenz von p_i ist $(i = 1, 2)$. Man zeige:

a) $G(p_i)$ ist eine Untergruppe von G $(i = 1, 2)$.

b) $G(p_1) \cap G(p_2) = \{0\}$.

c) $G = G(p_1) \oplus G(p_2)$ (direkte Summe).

G2.14 [Frühjahr 1987] Eine Gruppe heiße *zerlegbar*, wenn sie das direkte Produkt zweier echter Untergruppen ist; andernfalls heiße sie *unzerlegbar*.

a) Bestimmen Sie bis auf Isomorphie alle endlichen zyklischen Gruppen, die unzerlegbar sind.

Zeigen Sie:

b) Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen ist unzerlegbar.

c) Die additive Gruppe $\mathbb{Q}$ der rationalen Zahlen ist unzerlegbar.

d) $\mathbb{Q}/\mathbb{Z}$ ist zerlegbar

HINWEIS: Für eine Primzahl p betrachte man die Untergruppe $A \subset \mathbb{Q}$ aller rationalen Zahlen, deren Nenner eine Potenz von p ist, und die Untergruppe $A/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$.

G2.15 [Herbst 1987] Zerlegen Sie die abelsche Gruppe $\mathbb{Z}/360\mathbb{Z}$ in eine direkte Summe zyklischer Untergruppen von Primzahlpotenzordnung.

Hauptsatz über endlich erzeugte abelsche Gruppen

G2.16 [Herbst 2001] Sei G eine freie abelsche Gruppe mit der Basis $(X_1, \ldots, X_n)$.

a) Zeigen Sie, dass jede Basis von G aus genau n Elementen besteht.

b) Seien $Y_i = \sum_{k=1}^{n} z_{ik} X_k$ (mit $z_{ik} \in \mathbb{Z}$ für $i, k = 1, \ldots, n$) Elemente aus G und $A = (z_{ik})_{i,k=1,\ldots,n}$ die zugehörige Koeffizientenmatrix. Ferner sei H die von $Y_1, \ldots, Y_n$ erzeugte Untergruppe von G. Zeigen Sie: Ist $\det A \neq 0$, so besitzt G/H die Ordnung $|\det A|$.

G2.17 [Herbst 1985] Sei $U \leq \mathbb{Z}^3$ die von den Elementen $u_1 = (4, 3, 1)$, $u_2 = (8, 3, -1)$, $u_3 = (2, 2, 2)$ erzeugte Untergruppe (= $\mathbb{Z}$-Modul). Man finde eine Basis e_1, e_2, e_3 des $\mathbb{Z}$-Moduls $\mathbb{Z}^3$ und $a_i \in \mathbb{N}$, $a_1 \mid a_2 \mid a_3$ so, daß a_1e_1, a_2e_2, a_3e_3 eine Basis von U ist und schreibe $\mathbb{Z}^3/U$ als Produkt von zyklischen Gruppen.

G2.18 [Frühjahr 1979] Die abelsche Gruppe $(A, +)$ werde von den Elementen a, b und c erzeugt, für welche die Relationen $2a = 3b$ und $4c = 0$ gelten. Zerlegen Sie A in eine direkte Summe von zyklischen Untergruppen.

G2.19 [Frühjahr 1985] Die abelsche Gruppe A werde von den Elementen a, b, c erzeugt, $A = \langle a, b, c \rangle$. Die Erzeugenden erfüllen die Relationen

$$\begin{array}{lll} a + b + 3c = 0, & & 2a + 3b + c = 0 \\ 5a + b - 4c = 0 & \text{und} & 5b + 2c = 0 \end{array}$$

aber keine weiteren von diesen Relationen unabhängige Relationen. Man bestimme die Struktur von A.

G2.20 [Frühjahr 1985] Sei p eine Primzahl. Die abelsche Gruppe G habe die Ordnung p^s und sei direkte Summe von m zyklischen Gruppen. H sei die Untergruppe von G, die aus 0 und den Elementen der Ordnung p besteht. Zeigen Sie $|H| = p^m$. Wie sieht für H eine Zerlegung als direkte Summe von zyklischen Gruppen aus?

G2.21 [Frühjahr 1987] Seien p und q verschiedene Primzahlen. Zeigen Sie:

a) Jede abelsche Gruppe der Ordnung $p^2 \cdot q^2$ wird von 2 Elementen erzeugt.

b) Jede nicht abelsche Gruppe der Ordnung p^3 wird von 2 Elementen erzeugt.

G2.22 [Frühjahr 1988]

a) Beweise: Besitzt eine endliche abelsche Gruppe G genau zwei maximale Untergruppen, so ist G zyklisch von der Ordnung $p^a q^b$, wobei p und q zwei verschiedene Primzahlen sowie a und b zwei natürliche Zahlen sind.

b) Gib ein Beispiel für eine nichtzyklische endliche Gruppe, die genau vier maximale Untergruppen besitzt.

G2.23 [Herbst 1983] Sei G eine abelsche Gruppe, in der jede absteigende und jede aufsteigende Kette von Untergruppen endlich ist. Man zeige, daß G endlich sein muß.

Homomorphismen

G2.24 [Frühjahr 1998] Sei G eine multiplikativ geschriebene endliche abelsche Gruppe der Ordnung m mit Einselement e. Für eine natürliche Zahl s bezeichne ϕ_s den Gruppen-Homomorphismus

$$\phi_s : \; G \to G \quad , \quad x \mapsto \phi_s(x) := x^s \quad .$$

a) Man zeige: Genau dann ist ϕ_s ein Automorphismus von G, falls m und s teilerfremd sind. In diesem Fall hat die Umkehrabbildung von ϕ_s ebenfalls die Gestalt ϕ_r mit einer natürlichen Zahl r.

Seien k, ℓ teilerfremde natürliche Zahlen mit $m = k\ell$. Man beweise:

b) $\quad \mathrm{Im}(\phi_k) = \mathrm{Ker}(\phi_\ell) \quad , \quad \mathrm{Im}(\phi_\ell) = \mathrm{Ker}(\phi_k)$

c) $\quad \mathrm{Im}(\phi_k) \cap \mathrm{Im}(\phi_\ell) = \{e\}$

d) Jedes Element $x \in G$ besitzt eine eindeutige Darstellung

$$x = x_1 x_2 \quad \text{mit} \quad x_1 \in \mathrm{Im}(\phi_k)\,,\; x_2 \in \mathrm{Im}(\phi_\ell)$$

e) Man bestimme die Anzahl der Elemente von $\mathrm{Im}(\phi_k)$ und $\mathrm{Im}(\phi_\ell)$.

G2.25 [Herbst 1976] Ist G eine endliche abelsche Gruppe, so nennt man einen Homomorphismus von G in die multiplikative Gruppe $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ der komplexen Zahlen einen *Charakter* von G. Das Produkt zweier Charaktere $\chi, \chi' : \; G \to \mathbb{C}^\times$ erklärt man durch

$$(\chi \cdot \chi')(x) := \chi(x)\chi'(x) \qquad (x \in G).$$

Die Menge der Charaktere von G ist zusammen mit der so definierten Verknüpfung eine Gruppe, die Charaktergruppe von G. Man beweise:

a) Hat $x \in G$ die Ordnung m und ist χ ein Charakter von G, so ist $\chi(x)$ eine m-te Einheitswurzel.

b) Ist G zyklisch, so ist auch die Charaktergruppe von G zyklisch.

c) Die Ordnung der Charaktergruppe von G ist gleich der Ordnung von G.
(Dabei kann ohne Beweis verwendet werden, daß G das direkte Produkt von endlich vielen zyklischen Untergruppen von G ist.)

d) Ist H eine Untergruppe von G und m ihr Index in G, so kann jeder Charakter von H auf genau m verschiedene Weisen zu einem Charakter von G fortgesetzt werden.

e) Ist $x \in G$ vom neutralen Element verschieden, so gibt es einen Charakter χ von G mit $\chi(x) \neq 1$.

G2.26 [Herbst 1984]

a) Es sei p eine Primzahl, G eine zyklische Gruppe der Ordnung p und H eine zyklische Gruppe der Ordnung p^2. Man bestimme die Anzahl der Endomorphismen und die Anzahl der Automorphismen von $G \times H$.

b) Es seien $n_1, n_2, \ldots, n_t$ natürliche Zahlen mit $n_i \mid n_{i+1}$ für $1 \leq i \leq t-1$. Es sei H_i eine zyklische Gruppe der Ordnung n_i. Man bestimme die Anzahl der Endomorphismen von $H_1 \times H_2 \times \ldots \times H_t$.

G2.27 [Frühjahr 1987] G sei eine endliche abelsche Gruppe vom *Exponenten* m (d.h. m ist die kleinste positive ganze Zahl mit $g^m = 1$ für alle $g \in G$). Zeigen Sie:

a) Es gibt eine Zerlegung $G = G_1 \times G_2$ in Untergruppen G_i von G $(i = 1, 2)$, wobei G_2 zyklisch von der Ordnung m ist.

b) Ist φ ein Endomorphismus von G mit $\varphi(U) \subseteq U$ für jede Untergruppe U von G, so gibt es eine modulo m eindeutig bestimmte ganze Zahl n mit $\varphi(g) = g^n$ für alle $g \in G$.

G2.28 [Herbst 1994] Sei G eine endliche abelsche Gruppe. Zeigen Sie: Der Endomorphismenring $\operatorname{End} G$ ist genau dann ein Körper, wenn G eine zyklische Gruppe von Primzahlordnung ist.

G2.29 [Herbst 1974]

a) Zeigen Sie, daß die multiplikative Gruppe M der positiven reellen Zahlen isomorph zur additiven Gruppe $\mathbb{R}^+$ der reellen Zahlen ist.

b) Beweisen Sie, daß die multiplikative Gruppe G der positiven rationalen Zahlen nicht isomorph zur additiven Gruppe der rationalen Zahlen sein kann.

Abelsche Gruppen gegebener Ordnung

G2.30 [Frühjahr 1974] Es sei G eine Gruppe der Ordnung 25. Man beweise:

a) G ist abelsch.

b) G ist zyklisch oder direktes Produkt zweier zyklischer Gruppen von Primzahlordnung.

G2.31 [Herbst 1980] Bestimmen Sie, wie viele nichtisomorphe abelsche Gruppen der Ordnung 1980 existieren, und geben Sie aus jeder Isomorphieklasse ein Beispiel.

G2.32 [Herbst 1983] $n > 1$ sei eine natürliche Zahl und $p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ ihre Primzerlegung. Zeigen Sie:

a) Für die Anzahl $a(n)$ der Isomorphietypen der abelschen Gruppen der Ordnung n gilt

$$a(n) \geq \prod_{i=1}^{r} \alpha_i \quad .$$

b) In a) herrscht Gleichheit genau dann, wenn $\alpha_i \leq 3$ für jedes $i = 1, \ldots, r$ gilt.

G2.33 [Herbst 1988]

a) Bestimme die Anzahl der nichtisomorphen abelschen Gruppen der Ordnung 1988.

b) Beweise: Die Einheiten von $\mathbb{Z}/45\mathbb{Z}$ bilden eine nichtzyklische Gruppe der Ordnung 24.
Man stelle diese (bis auf Isomorphie) als direkte Summe von primären zyklischen Gruppen dar.

G2.34 [Frühjahr 1993] Geben Sie alle Isomorphieklassen von abelschen Gruppen der Ordnung 240 an.

G2.35 [Frühjahr 1996]

a) Wie viele Isomorphieklassen von abelschen Gruppen der Ordnung 64 gibt es?

b) Bestimmen Sie die kleinste natürliche Zahl n, so daß es genau sechs Isomorphieklassen von abelschen Gruppen der Ordnung n gibt.

G2.36 [Herbst 1979] Bestimme die kleinste Zahl n, so daß die abelschen Gruppen der Ordnung n in genau 6 Isomorphieklassen zerfallen.

Lokalzyklische und dividierbare Gruppen

G2.37 [Frühjahr 1975] Im folgenden ist $\mathbb{Q} = \mathbb{Q}^+$ als abelsche Gruppe zu betrachten.

a) Zeige: Ist A eine zyklische abelsche Gruppe, dann existiert ein $m \in \{0, 1, 2, \ldots\}$ mit $A \simeq \mathbb{Z}/m\mathbb{Z}$.

b) Zeige: Für jedes $n \in \mathbb{N}$ gilt:

$$\mathbb{Q}\, n = \mathbb{Q} \quad .$$

c) Zeige: $\mathbb{Q}$ besitzt keine zyklische Faktorgruppe $\neq 0$.

HINWEIS: Benutze a) und b).

d) Zeige: Läßt man aus einer beliebigen Erzeugendenmenge von $\mathbb{Q}$ endlich viele beliebige Elemente weg, dann ist auch die Restmenge eine Erzeugendenmenge.

e) Zeige: Jede endlich erzeugte Untergruppe von $\mathbb{Q}$ ist zyklisch.

HINWEIS: Zeige zuerst, daß jede Untergruppe einer zyklischen Gruppe zyklisch ist und benutze dieses Resultat.

G2.38 [Herbst 1978] Man beweise, daß jede endlich erzeugte Untergruppe der additiven Gruppe der rationalen Zahlen zyklisch ist.

G2.39 [Herbst 1990] Beweisen Sie: Alle endlich erzeugten von $\{0\}$ verschiedenen Untergruppen der additiven Gruppe der rationalen Zahlen sind isomorph.

G2.40 [Herbst 1995] Eine Gruppe G heißt *lokal-zyklisch*, falls jede endlich erzeugte Untergruppe von G zyklisch ist. Man zeige:

a) Jede lokal-zyklische Gruppe ist abelsch.

b) Unter- und Faktorgruppen einer lokal-zyklischen Gruppe sind lokal-zyklisch.

c) Die additiven Gruppen $\mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$ sind lokal-zyklisch.

G2.41 [Frühjahr 1981] Es sei $\mathbb{Q}^+$ die additive Gruppe der rationalen Zahlen. Beweisen Sie:

a) Für jede echte Untergruppe U von $\mathbb{Q}^+$ (d.h. $U \subsetneqq \mathbb{Q}^+$) ist die Faktorgruppe $\mathbb{Q}^+/U$ nicht endlich.

b) Für je zwei von $\{0\}$ verschiedene Untergruppen U, V von $\mathbb{Q}^+$ gilt $U \cap V \neq \{0\}$.

c) Ist $U \leq \mathbb{Q}^+$ eine Untergruppe, so daß $\mathbb{Q}^+/U$ zyklisch ist, dann gilt $U = \mathbb{Q}^+$.

d) $\mathbb{Q}^+$ hat keine maximale Untergruppe. (D.h. es gibt **keine** Untergruppe U mit folgenden Eigenschaften:

i. $U \neq \mathbb{Q}^+$

ii. Für jede Untergruppe V mit $U \subseteq V \subseteq \mathbb{Q}^+$ folgt $U = V$ oder $V = \mathbb{Q}^+$.)

G2.42 [Herbst 1989] $\mathbb{Q}^+$ bezeichne die additive Gruppe des Körpers $\mathbb{Q}$ der rationalen Zahlen. Beweisen Sie die folgenden Aussagen:

a) Endlich erzeugte Untergruppen von $\mathbb{Q}^+$ sind zyklisch (man sagt $\mathbb{Q}^+$ ist *lokalzyklisch*).

b) Untergruppen und homomorphe Bilder lokalzyklischer Gruppen sind wieder lokalzyklisch.

c) Jeder Homomorphismus zwischen zwei Untergruppen von $\mathbb{Q}^+$ wird durch Multiplikation mit einer rationalen Zahl vermittelt.

d) Zwei Untergruppen $U, V \subset \mathbb{Q}^+$ sind genau dann isomorph, wenn $U \cap V$ sowohl in U als auch in V endlichen Index hat.

G2.43 [Herbst 1974] Eine (additiv geschriebene) abelsche Gruppe G heißt *torsionsfrei*, wenn jedes Element $0 \neq x \in G$ unendliche Ordnung hat, d.h. $nx \neq 0$ für alle natürlichen Zahlen n gilt. Eine (additiv geschriebene) abelsche Gruppe G heißt *teilbar*, wenn für alle natürlichen Zahlen n und alle $g \in G$ die Gleichung $nx = g$ stets lösbar ist; G heißt *eindeutig teilbar*, wenn darüber hinaus die Lösung x der Gleichung $nx = g$ eindeutig ist.

a) Beweisen Sie, daß jede torsionsfreie teilbare abelsche Gruppe eindeutig teilbar ist.

b) Zeigen Sie, daß jede torsionsfreie teilbare abelsche Gruppe G ein Vektorraum über dem Körper der rationalen Zahlen $\mathbb{Q}$ ist.

G2.44 [Herbst 1974] Eine Gruppe G heißt *lokal zyklisch*, wenn jede endlich (d.h. von endlich vielen Elementen) erzeugte Untergruppe von G zyklisch ist.

a) Sei K ein (kommutativer) Körper der Charakteristik $\neq 2$. Zeigen Sie, daß dann die additive Gruppe K^+ von K nie isomorph zur multiplikativen Gruppe $K^\times$ sein kann.

b) Sei K ein (kommutativer) Körper der Charakteristik 2. Beweisen Sie, daß die additive Gruppe K^+ von K nie isomorph zur multiplikativen Gruppe $K^\times$ von K sein kann.

c) Beweisen Sie, daß jede torsionsfreie, teilbare [Definition in voriger Aufgabe] und lokal zyklische abelsche Gruppe isomorph zur additiven Gruppe $\mathbb{Q}^+$ der rationalen Zahlen sein muß.

G2.45 [Frühjahr 2001] Eine Gruppe heißt *torsionsfrei*, wenn nur das neutrale Element endliche Ordnung besitzt. Eine torsionsfreie abelsche Gruppe $\neq 0$ heißt *vom Rang* 1, wenn es für je zwei Elemente x, y dieser Gruppe ganze Zahlen a, b, nicht beide gleich 0, gibt derart, dass $ax + by = 0$ ist; z.B. ist die additive Gruppe $\mathbb{Q}$ der rationalen Zahlen torsionsfrei vom Rang 1. Beweisen Sie die folgenden Aussagen:

a) Torsionsfreie abelsche Gruppen vom Rang 1 lassen sich in $\mathbb{Q}$ einbetten.

b) Torsionsfreie *lokal zyklische Gruppen*, d.h. alle endlich erzeugten Untergruppen sind zyklisch, lassen sich in $\mathbb{Q}$ einbetten.

c) Jede Untergruppe von $\mathbb{Q}$ ist lokal zyklisch.

3. Operation von Gruppen

Rechnen in $\mathbf{S}_n$

G3.1 [Frühjahr 2003] Sei S_7 die symmetrische Gruppe aller Permutationen von $\{1,\dots,7\}$.

a) Gibt es einem injektiven Homomorphismus $\mathbb{Z}/10\mathbb{Z} \to S_7$?

b) Gibt es einen injektiven Homomorphismus $\mathbb{Z}/8\mathbb{Z} \to S_7$?

G3.2 [Herbst 1980] In S_{10}, der symmetrischen Gruppe auf 10 Elementen, werde die Permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 7 & 8 & 4 & 5 & 1 & 6 & 9 & 2 \end{pmatrix}$$

betrachtet.

a) Zerlegen Sie τ in disjunkte Zykel und bestimmen Sie das Vorzeichen von τ.

b) Wieviele zu τ konjugierte Elemente gibt es in S_{10}?

G3.3 [Frühjahr 1989] In der symmetrischen Gruppe S_n $(n \geq 3)$ betrachte man die Elemente

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & k & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & k+1 & \dots & n & 1 \end{pmatrix}$$

und

$$b = \begin{pmatrix} 1 & 2 & 3 & \dots & k & \dots & n-1 & n \\ 1 & n & n-1 & \dots & n-k+2 & \dots & 3 & 2 \end{pmatrix} .$$

a) Man zeige, daß $\operatorname{ord}(a) = n$, $\operatorname{ord}(b) = 2$ und $a^i b = b a^{-i}$ ist für alle $i \in \mathbb{Z}$.

b) Sei G die von den Elementen a und b erzeugte Untergruppe der S_n. Man zeige, daß $G = \{e, a, a^2, \dots, a^{n-1}, b, ba, ba^2, \dots, ba^{n-1}\}$ ist und daß die angegebenen Elemente paarweise verschieden sind.

c) Sei $N = \langle a \rangle$ die von a erzeugte Untergruppe von G. Man zeige, daß jede Untergruppe von N ein Normalteiler in G ist und folgere daraus, daß $\langle a^2 \rangle$ die Kommutatoruntergruppe von G ist.

d) Sei p eine Primzahl ≥ 3 und $n = p^k m$ mit $k \geq 0$, $m \geq 1$, $p \nmid m$. Man zeige, daß $P = \langle a^m \rangle$ die einzige p-Sylow-Untergruppe von G ist.

G3.4 [Herbst 1986] Sei p eine Primzahl und N der Normalisator einer p-Sylowgruppe der symmetrischen Gruppe S_p. Zeigen Sie: $|N| = p(p-1)$.

HINWEIS: Zählen Sie die Elemente der Ordnung p von S_p.

G3.5 [Herbst 1975] Sei p eine Primzahl und $G = \mathfrak{S}_p$ die symmetrische Gruppe in p Ziffern.

a) Man bestimme die Anzahl der Elemente der Ordnung p in G.

b) Man bestimme die Anzahl der p-Sylowgruppen von G und zeige ohne Verwendung der Sylowschen Sätze, daß sie alle zueinander konjugiert sind.

c) Sei S eine p-Sylowgruppe von G und C der Zentralisator von S in G. Man zeige: $C = S$.

d) Sei N der Normalisator von S in G. Man bestimme die Ordnung von N.

e) Man zeige, daß kein vom Einselement verschiedenes Element von N mehr als einen Fixpunkt hat.

f) Man zeige, daß N/S zyklisch ist.

G3.6 [Frühjahr 2002] Sei p eine Primzahl und sei S_p die Gruppe der Permutationen von $\{1, 2, \ldots, p\}$.

a) Man gebe die Anzahl der Elemente der Ordnung p in S_p an.

b) Sei P eine p-Sylowuntergruppe von S_p. Man gebe die Anzahl der Elemente des Normalisators $N(P)$ von P in S_p an.

G3.7 [Frühjahr 2003] Zeigen Sie (z.B. mit Hilfe der Zykeldarstellung von Permutationen):

a) Die alternierende Gruppe A_4 hat keine Untergruppe der Ordnung 6.

b) Die symmetrische Gruppe S_5 hat ein triviales Zentrum.

G3.8 [Herbst 1998]

a) Geben Sie eine Untergruppe der Ordnung 20 in der symmetrischen Gruppe S_5 an.

b) Gibt es Untergruppen der Ordnung 20 in A_5? Die Antwort ist zu begründen.

G3.9 [Frühjahr 1998] Zeigen Sie, daß die zwei Gruppen S_5 und $A_5 \times (\mathbb{Z}/2\mathbb{Z})$ der Ordnung 120 nicht isomorph sind; dabei ist S_5 die symmetrische und A_5 die alternierende Gruppe vom Grad 5.

G3.10 [Herbst 2003]

a) Definieren Sie die alternierende Gruppe A_n.

b) Warum ist A_n für $n \geq 2$ eine Untergruppe vom Index 2 in S_n?

c) Zeigen Sie, dass die Gruppe S_4 auflösbar ist.

G3.11 [Frühjahr 1994]

a) Es sei $\xi \in S_n$ ein Zykel der Länge n. Bestimmen Sie alle Permutationen $\pi \in S_n$, die mit ξ vertauschbar sind.

b) Es sei n ungerade und $n > 1$. Zeigen Sie: Die Menge der Zyklen der Länge n in der alternierenden Gruppe A_n zerfällt in genau zwei Konjugiertenklassen, von denen jede $\frac{1}{2}(n-1)!$ Elemente enthält.

G3.12 [Frühjahr 1985] Bestimmen Sie in der alternierenden Gruppe A_5 die Anzahl der Konjugiertenklassen von Elementen der Ordnung 5.

G3.13 [Frühjahr 1980]

a) Sei S_n die symmetrische Gruppe auf n Elementen und G eine Untergruppe von S_n, die nicht in der alternierenden Gruppe A_n enthalten ist. Zeigen Sie: Genau die Hälfte der Elemente von G liegt in $G \cap A_n$.

b) Sei G eine endliche Gruppe der Ordnung $n = 2 \cdot (2m + 1)$.
Zeigen Sie, daß G nicht einfach ist.

G3.14 [Frühjahr 1979] Es bezeichne S_n die symmetrische Gruppe aller Permutationen einer n-elementigen Menge M, und es sei $j \in M$.

a) Man beweise: Ist G eine transitive Untergruppe von S_n und $H = \{g \in G;\ g(j) = j\}$, so gilt $[G : H] = n$.

b) Man zeige: Es gibt nur eine Untergruppe der Ordnung 12 in S_4, nämlich die alternierende Gruppe.

c) Man bestimme bis auf Isomorphie alle transitiven Untergruppen von S_4.

G3.15 [Herbst 1985] Die Automorphismengruppe $\operatorname{Aut} A_4$ der alternierenden Gruppe A_4 ist isomorph zur symmetrischen Gruppe S_4. Beweisen Sie dieses Resultat auf folgendem Weg:

a) S_4 ist isomorph zu einer Untergruppe von $\operatorname{Aut} A_4$. Beachten Sie, daß A_4 Normalteiler von S_4 ist!

b) A_4 hat vier 3-Sylowuntergruppen.

c) $\operatorname{Aut} A_4$ ist isomorph zu einer Untergruppe der S_4, wobei $\operatorname{Aut} A_4$ als Permutationsgruppe auf der Menge der 3-Sylowuntergruppen betrachtet wird.

G3.16 [Herbst 1986] Zeigen Sie:

a) Die symmetrische Gruppe S_n wird von $\{(1,2),\ (1,2,\ldots,n)\}$ erzeugt.

b) Ist n eine Primzahl und i eine ganze Zahl mit $1 < i \leq n$, so wird S_n von $(1,i)$ und $(1,2,\ldots,n)$ erzeugt.

c) S_4 wird nicht von $\{(1,3),\ (1,2,3,4)\}$ erzeugt.

Transitive Gruppenoperationen

G3.17 [Frühjahr 1979] Eine Gruppe G operiere auf einer Menge M.

a) Erläutern Sie, was das heißt, und geben Sie ferner an, was man unter einer *Bahn* (auch Orbit genannt) von G in M und unter der *Fixgruppe* (auch Standgruppe, Isotropiegruppe) eines $x \in M$ versteht.

b) Zeigen Sie: Die Fixgruppen zweier Elemente aus derselben Bahn sind konjugierte Untergruppen von G.

c) Beweisen Sie die Formel

$$\operatorname{Ord}(G) = \operatorname{Ord}(G_x) \cdot b_x \quad ,$$

wobei G eine endliche Gruppe der Mächtigkeit $\operatorname{Ord}(G)$ ist, G_x die Fixgruppe eines $x \in M$ und b_x die Elementezahl der Bahn, zu der x gehört.

G3.18 [Frühjahr 1977] Es sei G eine endliche Gruppe, H eine Untergruppe von G vom Index m und $M := \{g_1H, g_2H, \ldots, g_mH\}$ die Menge aller Linksnebenklassen von H in G. Weiter sei S_M die Gruppe aller Permutationen von M. Zeigen Sie:

a) Die Abbildung $\varphi : G \to S_M$, die jedem $g \in G$ die Permutation

$$\varphi(g) : \begin{cases} M \to M \\ g_iH \mapsto gg_iH \end{cases}$$

zuordnet, ist ein Homomorphismus.

b) Der Kern K von φ ist der Durchschnitt aller zu H konjugierten Untergruppen von G.

c) Die Untergruppe $\varphi(G)$ von S_M operiert transitiv auf M, d.h. zu je zwei Elementen $g_iH, g_jH \in M$ gibt es ein $\varphi(g) \in \varphi(G)$ mit $\varphi(g)(g_iH) = g_jH$.

d) $m!$ ist ein Vielfaches der Ordnung von $\varphi(G)$.

e) m ist ein Teiler der Ordnung von $\varphi(G)$.

HINWEIS: Zeigen Sie zuerst, daß die Anzahl der Elemente aus $\varphi(G)$, die g_1H nach g_iH überführen, für alle $i \in \{1,2,\ldots,m\}$ gleich ist.

f) Für $n > 4$ besitzt die symmetrische Gruppe S_n keine Untergruppe vom Index m mit $2 < m < n$. (Man verwende dabei, daß die alternierende Gruppe A_n für $n > 4$ einfach ist.)

G3.19 [Herbst 1981] Es sei U eine Untergruppe der Gruppe G. Für jedes $g \in G$ wird durch

$$\pi(g)(hU) := ghU \quad , \quad h \in G$$

eine Selbstabbildung der Menge $\mathfrak{M} = \{xU\,;\ x \in G\}$ erklärt. Man zeige:

a) π ist ein Homomorphismus von G in die Permutationsgruppe von $\mathfrak{M}$.

b) Ist $\mathfrak{M}$ endlich, dann enthält U einen Normalteiler N von G, für den G/N ebenfalls endlich ist.

G3.20 [Frühjahr 1996] Ist $H \leq G$ Untergruppe einer Gruppe G, so definiert die Operation von G auf der Menge $C = \{Hx\,;\ x \in G\}$ der Rechtsnebenklassen von rechts via $Hx \mapsto Hxg$ für $g \in G$ einen Homomorphismus $\rho\colon\ G \to Sym(C)$ von G in die Permutationsgruppe von C. Zeigen Sie:

a) Der Kern K von ρ ist die größte normale Untergruppe von G, die in H enthalten ist, und es gilt $K = \bigcap\limits_{x \in G} x^{-1}Hx$.

b) Ist G einfach und besitzt G eine Untergruppe H vom Index k, wobei $k > 2$, dann teilt die Gruppenordnung $|G|$ den Wert $\frac{k!}{2}$.

G3.21 [Frühjahr 2002] Sei G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe vom Index n. Durch die Wirkung von G auf G/U wird ein Gruppenhomomorphismus $\varphi\colon\ G \to S_n$ definiert (dies muss nicht gezeigt werden).

a) Zeigen Sie: $\ker(\varphi) \subseteq U$.

b) Sei p der kleinste Primteiler von $|G|$ und $[G : U] = p$. Zeigen Sie: U ist normal in G.

G3.22 [Frühjahr 1994] Eine Operation einer Gruppe G auf einer Menge X heißt *treu*, falls zu jedem vom Einselement verschiedenen Element g aus G ein x in X existiert mit $gx \neq x$.
Sei G eine Gruppe der Ordnung 15, die auf einer Menge X treu und transitiv operiert. Man beweise, daß X aus genau 15 Elementen besteht. Gilt die entsprechende Aussage auch, wenn man 15 durch 12 ersetzt?

G3.23 [Herbst 2003] Sei G eine Gruppe der Ordnung n. Zeigen Sie:

a) G ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

b) Ist $n = 2u$ mit ungeradem u, so hat G einen Normalteiler vom Index 2.

G3.24 [Herbst 1992] Es sei S_n die Gruppe aller Permutationen der Menge $X = \{1, 2, \ldots, n\}$ a Es sei $x \in S_n$ ein n-Zykel. Ferner sei G eine transitive Untergruppe von S_n und N ein von 1 verschiedener Normalteiler von G. Zeigen Sie:

a) Der Zentralisator $Z := \{g \in S_n\,;\ gz = zg\}$ von z in S_n ist die von z erzeugte zyklische Untergruppe.

b) Alle Standuntergruppen von N sind in G konjugiert.

c) Alle Bahnen von N haben die gleiche Anzahl von Elementen.

Ist $n = p$ eine Primzahl, so gilt ferner:

d) N ist transitiv.

e) Ist N abelsch, so ist N zyklisch von der Ordnung p.

Bahnzerlegung

G3.25 [Herbst 1981] Sei G eine Gruppe der Ordnung 55, M eine Menge von 39 Elementen. Man zeige, daß jede Operation von G auf M mindestens einen Fixpunkt hat.

G3.26 [Frühjahr 1992] Eine Gruppe der Ordnung 55 operiere auf einer Menge M mit 18 Elementen. Zeigen Sie, daß die Gruppe auf M mindestens 2 Fixpunkte hat.

G3.27 [Frühjahr 1988] Eine endliche Gruppe G operiere als Permutationsgruppe auf einer Menge M. Zeigen Sie:

a) M ist die disjunkte Vereinigung seiner G-Bahnen $Gm, m \in M$.

b) Die Anzahl $|Gm|$ der Elemente von Gm ist ein Teiler von $|G|$.

G operiere nun mittels Konjugation auf G.

c) Folgern Sie aus a) und b): Das Zentrum einer endlichen p-Gruppe hat mindestens p Elemente.

G3.28 [Herbst 2002] Seien p eine Primzahl, $1 \leq r \in \mathbb{N}$ und $b = p^r$. Seien weiter A der Faktorring $A = \mathbb{Z}/b\mathbb{Z}$ und $A^\times$ die Gruppe der Einheiten von A. Die Gruppe $A^\times$ operiert auf A mittels der Multiplikation $A^\times \times A \to A\ ,\ (a, x) \mapsto a \cdot x$.

Bestimmen Sie die Bahnen dieser Operation, die Anzahl dieser Bahnen und ihre jeweilige Ordnung.

Operation durch Konjugation, Klassengleichung

G3.29 [Frühjahr 1974] Es sei p eine Primzahl, $n \in \mathbb{N}$ und G eine Gruppe der Ordnung p^n. Man beweise, daß das Zentrum

$$Z = \{z \in G\,;\ \bigwedge_{g \in G} zg = gz\}$$

von G nicht nur aus dem neutralen Element besteht.
Hierfür weise man im einzelnen nach:

a) Durch $gRg' :\iff \bigvee_{a \in G} g = ag'a^{-1}$ ist eine Äquivalenzrelation R über G definiert.

b) Für $g \in G$ ist $N_g = \{a \in G\,;\ aga^{-1} = g\}$ eine Untergruppe von G.

c) $G = \bigcup_{i=1}^{m} C_i$ sei die Zerlegung von G in Klassen bezüglich der Äquivalenzrelation R und $g \in C_i$. Dann gilt:

i. $C_i = \{g\} \iff g \in Z$.

ii. $[G : N_g]$ ist die Anzahl $|C_i|$ der Elemente von C_i.

d) Die Annahme $Z = \{e\}$ führt wegen $|G| = \sum_{i=1}^{m} |C_i|$ zu einem Widerspruch.

G3.30 [Herbst 1980] Sei G eine Gruppe. Elemente $g, g' \in G$ heißen zueinander *konjugiert*, falls es ein $h \in G$ mit $g' = hgh^{-1}$ gibt. G zerfällt in Klassen konjugierter Elemente.

a) Man beweise: Ist G endlich, so ist die Elementanzahl in einer jeden Klasse konjugierter Elemente ein Teiler der Ordnung von G.

b) Sei G eine endliche p-Gruppe, d.h. eine Gruppe der Ordnung p^n (p Primzahl, $n \in \mathbb{N}$). Für $i = 0, 1, 2, \ldots$ sei a_i die Anzahl derjenigen Klassen konjugierter Elemente, die genau p^i Elemente enthalten. Man zeige:

$$p^n = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1} \quad .$$

Man interpretiere a_0 und folgere, daß das Zentrum von G nicht nur aus dem neutralen Element besteht.

G3.31 [Frühjahr 1975] In dieser Aufgabe werden elementare Eigenschaften endlicher Gruppen G behandelt. G heißt *p-Gruppe*, wenn die Ordnung $|G|$ von G Potenz der Primzahl p ist. Der Index einer Untergruppe U von G wird mit $[G : U]$ bezeichnet. Eine von G verschiedene Untergruppe M heißt *maximal*, wenn für Untergruppen U von G aus $M \subset U \subset G$ entweder $U = M$ oder $U = G$ folgt. Normalteiler werden kurz *normale* Untergruppen genannt.

a) Es sei U Untergruppe von G und N die Menge aller $x \in G$, für die $xUx^{-1} = U$ ist (N heißt *Normalisator* von U). Man begründe: N ist Untergruppe von G und U ist normal in N.

b) U und V seien Untergruppen von G. Man beweise: Je zwei verschiedene der (*Doppelnebenklassen* genannten) Mengen

$$UyV := \{uyv \in G\,;\ u \in U\,,\ v \in V\}$$

in G sind disjunkt und UyV hat die Elementezahl $[U : yVy^{-1} \cap U] \cdot |V|$.

HINWEIS: Man zähle die Nebenklassen xV in UyV.

c) Es sei N Normalisator der Untergruppe U von G und S sei ein Vertretersystem der zu N punktfremden Doppelnebenklassen UyU. Man begründe die Formel

$$|G| = |N| + \sum_{y \in S} [U : yUy^{-1} \cap U] \cdot |U|$$

und folgere für p-Gruppen U, deren Index $[G : U]$ in G teilbar ist durch p, daß auch der Index $[N : U]$ durch p teilbar ist.

d) Man begründe:

i. Jede Untergruppe $U \neq G$ von G ist in mindestens einer maximalen Untergruppe enthalten.

ii. Die vom Einselement gebildete Untergruppe ist maximal in G nur dann, wenn $|G| = p$ eine Primzahl ist.

iii. Jede zugleich maximale und normale Untergruppe M von G hat einen Primzahlindex $[G : M]$.

e) Es sei G eine p-Gruppe und F der Durchschnitt aller maximalen Untergruppen von G. Man beweise:

i. Jede maximale Untergruppe M von G ist normal und F ist ebenfalls normal.

ii. In der Faktorgruppe $A := G/F$ hat jedes vom Einselement verschiedene Element die Ordnung p. Ferner ist A kommutativ.

HINWEIS: Für alle Paare $x, y \in G$ und für jede maximale Untergruppe M von G ist $xyx^{-1}y^{-1} \in M$.

G3.32 [Herbst 1996] Zeigen Sie, daß jeder Normalteiler $\neq 1$ einer endlichen p-Gruppe G ein zentrales Element $x \neq 1$ enthält, d.h. x liegt im Zentrum der Gruppe G.

G3.33 [Frühjahr 1983] Sei p eine Primzahl, G eine endliche p-Gruppe, $Z(G)$ das Zentrum von G.

a) Zeigen Sie:
Ist $N \neq \{e\}$ ein Normalteiler von G, so gilt $|N \cap Z(G)| \neq 1$.
HINWEIS: Betrachte $N^* := N \setminus \{e\}$.

b) Sei G nichtabelsch von der Ordnung $|G| = p^3$. Man bestimme die Ordnung von $Z(G)$.

G3.34 [Herbst 1999]

a) Sei $p \in \mathbb{N}$ eine Primzahl und G eine nichttriviale endliche p-Gruppe. Man beweise, dass das Zentrum von G nichttrivial ist.

b) Man konstruiere eine nichtabelsche Gruppe G der Ordnung 27, in der jedes Element $x \in G \setminus \{1\}$ die Ordnung 3 hat.

G3.35 [Frühjahr 1990] Geben Sie eine Gruppe M von 3×3-Matrizen über einem geeigneten Grundkörper an, welche die folgenden Eigenschaften hat:

a) M hat die Ordnung 27.

b) M ist nicht abelsch.

c) $x^3 = e$ für alle $x \in M$ (e = Einheitsmatrix).

G3.36 [Herbst 1988] Es sei p eine Primzahl und G eine Gruppe der Ordnung p^n mit $n \geq 2$. Sei $C(g)$ der Zentralisator eines Elements $g \in G$. Zeigen Sie:

$$|C(g)| > p \quad .$$

G3.37 [Herbst 2002] Es sei p eine Primzahl und G eine Gruppe der Ordnung p^n mit $n \geq 2$. Ferner sei $C(g)$ der Zentralisator eines Elements $g \in G$. Zeigen Sie:

$$|C(g)| > p \quad .$$

G3.38 [Frühjahr 2000] Zeigen Sie, dass eine endliche Gruppe mit einem Normalteiler, dessen Ordnung gleich dem kleinsten Primteiler der Gruppenordnung ist, ein nichttriviales Zentrum hat.

HINWEIS: Man betrachte die Operation der Gruppe auf dem Normalteiler durch Konjugation.

G3.39 [Herbst 2003] Sei G eine endliche Gruppe der Ordnung $n > 1$, sei p der kleinste Primteiler von n und P eine zyklische, normale p-Sylowgruppe von G.

a) Zeigen Sie: Ist p^m die Ordnung von P, so ist $p^{m-1}(p-1)$ die Ordnung der Automorphismengruppe $\mathrm{Aut}(P)$ von P.

b) Die Konjugation von G auf P liefert einen Homomorphismus

$$\alpha : \ G \to \mathrm{Aut}(P) \quad , \quad \alpha(g) : \ x \mapsto gxg^{-1}$$

für $g \in G$ und $x \in P$. Zeigen Sie: Der Index $[G : \mathrm{Kern}\,\alpha]$ ist ein Teiler von $p^{m-1}(p-1)$ und nicht durch p teilbar.

c) Zeigen Sie, dass P im Zentrum von G enthalten ist.

G3.40 [Frühjahr 1985] Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Bezeichne G/H die Menge der Restklassen $\bar{x} = xH$, $x \in G$, und $S(G/H)$ die Permutationsgruppe von G/H. Beweise:

a) Durch $\phi(g)(\bar{x}) := \overline{gx}$ für $g, x \in G$ ist ein Gruppenhomomorphismus $\phi : G \to S(G/H)$ definiert.

b) Kern $(\phi) =: N$ ist Normalteiler von G mit $N \leq H$. Sei $[G : H] =: t$ endlich. Dann ist $[G : N]$ endlich, t teilt $[G : N]$ und $[G : N]$ teilt $t!$

c) Jede Gruppe der Ordnung 392 besitzt eine normale 7-Untergruppe $\neq \{1\}$.

Lineare Darstellungen

G3.41 [Frühjahr 1976] Es sei $\mathrm{GF}(p)$ ein Primkörper der Charakteristik $p > 2$, $\mathfrak{G}$ die Gruppe aller Abbildungen $x \mapsto ux + v$ von $\mathrm{GF}(p)$ auf sich mit $u, v \in \mathrm{GF}(p)$ und $u \neq 0$. Weiter sei r eine primitive $(p-1)$-te Einheitswurzel in $\mathrm{GF}(p)$ und α ein Automorphismus von $\mathfrak{G}$. Die Abbildungen $\mathfrak{n}$ und $\mathfrak{r}$ aus $\mathfrak{G}$ seien definiert durch

$$\mathfrak{n} : \begin{cases} \mathrm{GF}(p) \to \mathrm{GF}(p) \\ x \mapsto x + 1 \end{cases} \quad \text{bzw.} \quad \mathfrak{r} : \begin{cases} \mathrm{GF}(p) \to \mathrm{GF}(p) \\ x \mapsto rx \end{cases} .$$

Die Elemente aus $\mathrm{GF}(p)$ seien durch die Zahlen $0, 1, 2, \ldots, p-1$ repräsentiert. Zeigen Sie:

a) Für die von $\mathfrak{n}$ erzeugte Untergruppe $\mathfrak{N}$ von $\mathfrak{G}$ gilt $\alpha(\mathfrak{N}) = \mathfrak{N}$.

b) $\{\mathfrak{n}, \mathfrak{r}\}$ ist ein Erzeugendensystem von $\mathfrak{G}$.

c) Es gibt ein $s \in \{0, 1, 2, \ldots, p-1\}$ mit $\alpha(\mathfrak{n}) = \mathfrak{r}^{-s} \cdot \mathfrak{n} \cdot \mathfrak{r}^{s}$.

d) Ist s wie unter c) bestimmt, β der durch $\beta(\mathfrak{g}) = \mathfrak{r}^{-s} \cdot \mathfrak{g} \cdot \mathfrak{r}^{s}$ für $\mathfrak{g} \in \mathfrak{G}$ bestimmte innere Automorphismus von $\mathfrak{G}$ und $\varphi := \beta^{-1}\alpha$, sowie $\varphi(\mathfrak{r})(x) := bx + c$ für alle $x \in \mathrm{GF}(p)$, dann gilt:

i) $\varphi(\mathfrak{n}) = \mathfrak{n}$

ii) $\mathfrak{n}^r = \varphi(r) \cdot \mathfrak{n} \cdot (\varphi(r))^{-1}$

iii) $b = r$ (Hinweis: Berechnen Sie $x + r$!)

e) Es gibt ein $t \in \{0, 1, 2, \ldots, p-1\}$ mit $\varphi(\mathfrak{g}) = \mathfrak{n}^{-t} \cdot \mathfrak{g} \cdot \mathfrak{n}^{t}$ für alle $\mathfrak{g} \in \mathfrak{G}$.

f) Alle Automorphismen von $\mathfrak{G}$ sind innere Automorphismen.

g) Die Automorphismengruppe von $\mathfrak{G}$ ist isomorph zu $\mathfrak{G}$.

G3.42 [Herbst 1977] Sei $\mathbb{F}_4$ ein Körper mit 4 Elementen, V ein 2-dimensionaler Vektorraum über $\mathbb{F}_4$, G die Gruppe der invertierbaren 2×2 Matrizen über $\mathbb{F}_4$ und S die Untergruppe der Matrizen von G mit Determinante 1.

a) Bestimme die Anzahl der Vektoren von V und die der 1-dimensionalen Unterräume von V.

b) Bestimme die Ordnungen der Gruppen G und S (nämlich zu 180 und 60).

c) Zeige, daß G das direkte Produkt von S mit einer Untergruppe der Ordnung 3 ist.

G3.43 [Herbst 1977] Sei $V = \mathbb{F}_4^2$ und $S = \mathrm{SL}_2(\mathbb{F}_4)$. Bezüglich einer festen Basis von V erklärt jedes $g \in S$ eine lineare Abbildung, die ebenfalls mit g bezeichnet sei.

a) Zeige, daß das Eins-Element von S das einzige Element von S ist, das jeden Unterraum von V in sich überführt.

b) Zeige, daß die Gruppe S isomorph zur alternierenden Gruppe A_5 vom Grade 5 ist (benütze die vorige Aufgabe).

G3.44 [Herbst 1977] Sei $V = \mathbb{F}_4^2$ und $S = \mathrm{SL}_2(\mathbb{F}_4)$.

a) Zeige, daß $\mathbb{F}_4$ einen Automorphismus α der Ordnung 2 besitzt.

b) Sei v_1, v_2 eine Basis von V und a die Abbildung von V, die jedem Vektor $\lambda_1 v_1 + \lambda_2 v_2$ mit $\lambda_i \in \mathbb{F}_4$ den Vektor $\lambda_1^\alpha v_1 + \lambda_2^\alpha v_2$ zuordnet. Fasse die Elemente von S als Abbildungen von V auf und sei $s \circ a$ für $s \in S$, die aus s und a zusammengesetzte Abbildung. Zeige, daß die Menge $\Gamma = \{s, s \circ a\,;\ s \in S\} = S \cup (S \circ a)$ bezüglich *Hintereinanderausführung* eine Gruppe bildet.

c) Zeige, daß die Gruppe Γ isomorph zur symmetrischen Gruppe S_5 vom Grade 5 ist. (Benütze die vorige Aufgabe)

G3.45 [Frühjahr 1979] Es seien p eine Primzahl und $d, m \geq 1$ zwei natürliche Zahlen. Sei V der d-dimensionale Vektorraum über dem Körper $K = \mathrm{GF}(n)$, der aus genau $n = p^m$ Elementen besteht.

a) Zeigen Sie: Die Ordnung der Gruppe aller Automorphismen von V ist $(n^d - 1)(n^d - n) \ldots (n^d - n^{d-1})$.

HINWEIS: Wieviele geordnete Basen von V gibt es?

b) Bestimmen Sie die Ordnung der Gruppe der semilinearen Bijektionen von V auf sich.

HINWEIS: Die Automorphismengruppe von K ist zyklisch.

c) Es sei $d \geq 3$. Bestimmen Sie die Ordnung der Gruppe aller Kollineationen des $(d-1)$-dimensionalen projektiven Koordinatenraumes über K.

G3.46 [Herbst 1979] Seien K ein Körper der Charakteristik 0 und G eine endliche Gruppe der Ordnung n. Ein endlichdimensionaler K-Vektorraum V heißt *G-Raum*, wenn es eine Abbildung $G \times V \to V$, $(g, v) \mapsto g \cdot v$, mit folgenden Eigenschaften gibt:

(i) Für alle $g \in G$ ist die Abbildung $V \to V$, $v \mapsto g \cdot v$, K-linear.

(ii) Für alle $g_1, g_2 \in G$ und $v \in V$ gilt $g_1 \cdot (g_2 \cdot v) = (g_1 g_2) \cdot v$, für das Einselement e von G gilt $e \cdot v = v$.

Ein Unterraum U von V heißt *G-Unterraum*, wenn für alle $g \in G$, $u \in U$ gilt $g \cdot u \in U$. Ein G-Raum V heißt *einfach*, wenn er von Null verschieden ist und außer 0 und V keine G-Unterräume besitzt. Sind V, V' G-Räume, so heißt eine K-lineare Abbildung $f : V \to V'$ ein *G-Homomorphismus*, wenn für alle $g \in G$, $v \in V$ gilt $f(g \cdot v) = g \cdot f(v)$; V heißt *G-isomorph* zu V', wenn es einen bijektiven G-Homomorphismus $f : V \to V'$ gibt.

Man zeige:

a) Ist $f : V \to V'$ ein G-Homomorphismus zwischen G-Räumen, so sind Kern und Bild von f G-Unterräume. Sind V und V' einfach und $f \neq 0$, dann ist f bijektiv.

b) Seien V ein G-Raum, U ein G-Unterraum von V, sei V' ein K-Unterraum von V mit $V = U \oplus V'$ und $p : V \to U$ die Projektion auf U. Dann ist die Abbildung

$$q : V \to V \quad , \quad v \mapsto \frac{1}{n} \sum_{g \in G} g^{-1} \cdot p(g \cdot v)$$

ein G-Homomorphismus (man betrachte $h^{-1} \cdot q(h \cdot v)$ für $h \in G$ und $v \in V$), es gilt $q(u) = u$ für alle $u \in U$, $q(V) = U$ und $V = U \oplus (1 - q)(V)$.

c) Jeder G-Raum ist direkte Summe endlich vieler einfacher G-Unterräume.

d) Die K-Dimension jedes einfachen G-Raumes ist höchstens n.
(Für ein $0 \neq v_0 \in V$ betrachte man den von allen $g \cdot v_0$, $g \in G$, erzeugten Untervektorraum von V.)

e) Zu jedem eindimensionalen G-Raum V gibt es genau einen Gruppenhomomorphismus $\chi_V : G \to K^\times = K - \{0\}$ mit $g \cdot v = \chi_V(g)v$ für alle $g \in G$, $v \in V$.
Für alle $g \in G$ ist $\chi_V(g)$ eine n-te Einheitswurzel von K. Ferner sind zwei eindimensionale G-Räume V, V' genau dann G-isomorph, wenn $\chi_V = \chi_{V'}$ ist.

Von nun ab sei G eine zyklische Gruppe mit erzeugendem Element t, wie bisher sei n ihre Ordnung. Man zeige weiter:

f) Gibt es n paarweise nicht G-isomorphe eindimensionale G-Räume $V_1, \ldots, V_n$, so enthält K eine primitive n-te Einheitswurzel.
(Man betrachte die Elemente $\chi_{V_i}(t)$, $1 \le i \le n$, und beachte e).)

g) Wenn K eine primitive n-te Einheitswurzel enthält, dann gibt es n paarweise nicht G-isomorphe, eindimensionale G-Räume.

h) Enthält K eine primitive n-te Einheitswurzel, so ist jeder einfache G-Raum V eindimensional.

(Die Abbildung $f : V \to V$ mit $v \mapsto t \cdot v$ ist ein G-Homomorphismus mit $f^n = \mathrm{id}_V$, wobei id_V die identische Abbildung von V ist. Man zeige durch Zerlegung von $f^n - \mathrm{id}_V$ in Faktoren der Form $f - \alpha\,\mathrm{id}_V$, $\alpha \in K$, und mit Hilfe von a), daß es eine n-te Einheitswurzel $\varepsilon \in K$ gibt mit $f - \varepsilon\,\mathrm{id}_V = 0$.)

G3.47 [Frühjahr 2003] Sei C_p eine zyklische Gruppe der Primzahlordnung p. Bestimmen Sie die Anzahl der Automorphismen der Gruppe $C_p \times C_p \times C_p$.

G3.48 [Frühjahr 1988] Es sei K ein endlicher Körper mit q Elementen. Bestimmen Sie die Ordnungen der folgenden Gruppen:

a) der Gruppe $\mathrm{GL}(2, K)$ aller invertierbaren 2×2-Matrizen mit Koeffizienten aus K;

b) der Gruppe $\mathrm{SL}(2, K)$ aller $A \in \mathrm{GL}(2, K)$ mit $\det A = 1$;

c) des Zentrums Z von $\mathrm{SL}(2, K)$.

Symmetriegruppen

G3.49 [Frühjahr 1974] Die komplexe Ebene $\mathbb{C}$ wird in üblicher Weise auch als reelle euklidische Ebene $\mathbb{R}^2$ angesehen. Sei $\rho = e^{\pi i/3}$ eine sechste Einheitswurzel in $\mathbb{C}$, sei $W = \{m + n\rho;\ m, n \in \mathbb{Z}\}$ das von 1 und ρ aufgespannte Gitter in $\mathbb{C}$.

a) Zeige: $\rho^2 - \rho + 1 = 0$. Folgere daraus: $\rho \cdot W = W$.

b) Zeige: $0, 1, \rho$ bilden ein gleichseitiges Dreieck.

c) Bestimme alle Gitterpunkte (= Zahlen aus W) mit minimalem positiven Abstand von 0. Was ist die zweitkleinste Entfernung eines Gitterpunktes von 0?

d) Sei G die Symmetriegruppe des Gitters W, bestehend aus allen eigentlichen und uneigentlichen Bewegungen der Ebene, die W in sich abbilden. Zeige:

G enthält eine zu W isomorphe Translationsgruppe T. Die 0 festlassenden Symmetrien bilden eine Diedergruppe G_0, es ist $G = G_0 \cdot T$.

e) Beschreibe die Elemente in G geometrisch: Wo sind die Fixpunkte der Drehungen, wo die Achsen der Spiegelungen bzw. Gleitspiegelungen?

G3.50 [Herbst 1982] Zeigen Sie: Die Gruppe aller Drehungen, die ein reguläres Tetraeder in sich überführen, ist zur alternierenden Gruppe A_4 isomorph.

G3.51 [Frühjahr 1989] Wie viele Isometrien hat ein n-dimensionaler Würfel in $\mathbb{R}^n$?

G3.52 [Frühjahr 1997]

a) Zeigen Sie, daß die Symmetriegruppe (= Gruppe der Isometrien) eines regulären Oktaeders im euklidischen $\mathbb{R}^3$ isomorph zur Symmetriegruppe eines Würfels ist.

b) Welche Ordnung hat diese Gruppe?

c) Wie viele Elemente der Ordnung 3 besitzt sie?

4. Sylowsätze

Gruppen mit lauter normalen Sylowgruppen

G4.1 [Frühjahr 2003] Zeigen Sie, daß jede Gruppe der Ordnung 255 zyklisch ist.

G4.2 [Frühjahr 1976] Zeige, daß jede Gruppe der Ordnung 1001 zyklisch ist.

G4.3 [Herbst 2000] Sei G eine Gruppe mit 2001 Elementen. Zeigen Sie:

a) Die p-Sylowgruppen von G sind für $p = 23$ und $p = 29$ normal.

b) Auch die 3-Sylowgruppe von G ist normal.

c) Die Gruppe G ist zyklisch.

G4.4 [Frühjahr 1984] G sei eine Gruppe der Ordnung 45.

a) Bestimmen Sie für jede Primteiler p von 45 die Anzahl der p-Sylowuntergruppen von G.

b) Folgern Sie, daß G isomorph zum direkten Produkt seiner Sylowuntergruppen ist!

c) Folgern Sie, daß G abelsch ist!

d) Wieviele Isomorphieklassen von Gruppen der Ordnung 45 gibt es?

G4.5 [Herbst 1987] Zeigen Sie, daß jede Gruppe der Ordnung 45 höchstens 12 verschiedene Untergruppen besitzt.

G4.6 [Herbst 1992] Man bestimme die Isomorphieklassen von Gruppen der Ordnung 1225.

G4.7 [Frühjahr 1993] Gruppen der Ordnung p^2q^2 mit $p \nmid q^2 - 1$:

a) Es sei p eine Primzahl. Bekanntlich ist jede Gruppe der Ordnung p^2 abelsch. Man gebe die Isomorphietypen aller Gruppen der Ordnung p^2 an.

b) Für jede Gruppe der Ordnung p^2 bestimme man die Automorphismengruppe und ihre Ordnung.

c) Es seien p und q Primzahlen mit $2 < p < q$ und $p \nmid q^2 - 1$. Es sei G eine Gruppe der Ordnung p^2q^2. Man beweise, daß G genau eine p-Sylowgruppe besitzt.

d) Man beweise, daß die Gruppe G in Teil (c) der Aufgabe abelsch ist.

G4.8 [Herbst 2002] Es sei $p \in \mathbb{N}$ eine Primzahl ≥ 5 derart, dass auch $q := p + 2$ eine Primzahl ist, wie z.B. $p = 17$ und $q = 19$.

a) Es sei G eine Gruppe der Ordnung $p^2 \cdot q^2$. Bestimmen Sie die Anzahlen und Ordnungen der Sylow-Untergruppen von G.

b) Bestimmen Sie alle Isomorphietypen von Gruppen der Ordnung $104329 = 323^2$.

G4.9 [Frühjahr 1990] G sei eine endliche Gruppe, in der Elemente teilerfremder Ordnung stets miteinander vertauschbar sind. Zeigen Sie: G ist das direkte Produkt von Sylow-Gruppen.

G4.10 [Herbst 1988] Für alle Paare x, y von Elementen der endlichen Gruppe G soll die Gleichung

$$x^3y^3 = (xy)^3$$

gelten. Beweisen Sie die folgenden Aussagen:

a) Für alle Paare x, y von Elementen aus G gilt

$$x^3y^2 = y^2x^3 \quad .$$

HINWEIS: Betrachten Sie $(xy)^3y^{-1}$.

b) Elemente teilerfremder Ordnung von G sind miteinander vertauschbar.

c) Alle p-Sylowgruppen von G sind Normalteiler.

d) Die sechste Potenz eines jeden Elements aus G liegt in $Z(G)$, dem Zentrum von G.

Gruppen mit einer normalen Sylowgruppe

G4.11 [Frühjahr 1992] Es seien p und q Primzahlen mit $p < q$.

a) Folgern Sie aus den Sylowschen Sätzen, daß im Falle $q \not\equiv 1 \mod p$ jede Gruppe der Ordnung pq zyklisch ist.

b) Geben Sie im Falle $q \equiv 1 \mod p$ eine nicht-abelsche Gruppe der Ordnung pq an, indem Sie für einen geeigneten Körper K und eine geeignete Untergruppe U von $K^\times$ die Matrizen

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

mit $a \in U$ und $b \in K$ betrachten.

G4.12 [Frühjahr 2000] Untersuchen Sie, für welche Primzahlen q mit $q \equiv 2 \mod 3$ jede Gruppe der Ordnung $3q$ zyklisch ist.

G4.13 [Frühjahr 1987] Seien p und q verschiedene Primzahlen. Beweisen Sie, daß jede Gruppe der Ordnung $p^2 \cdot q$ eine normale Sylowuntergruppe besitzt.

G4.14 [Frühjahr 2001] Sei G eine Gruppe der Ordnung 63.

a) Man zeige, dass G einen nichttrivialen Normalteiler hat.

b) Man konstruiere zwei nicht isomorphe nicht abelsche Gruppen der Ordnung 63 (als semidirektes Produkt).

G4.15 [Herbst 1989] Beweisen Sie:

a) Es gibt keine einfache Gruppe der Ordnung 333.

b) Es gibt eine kommutative, nicht zyklische Gruppe der Ordnung 333.

c) Es gibt eine nicht kommutative Gruppe der Ordnung 333.

G4.16 [Frühjahr 1983] Beweisen Sie die folgenden Aussagen:

a) Die alternierende Gruppe A_4 hat keine Untergruppe der Ordnung 6.

b) Eine Gruppe G der Ordnung 12 ohne Untergruppe der Ordnung 6 hat vier 3-Sylowuntergruppen.

c) Der Homomorphismus der Gruppe G aus b) in die symmetrische Gruppe S_4, der einem Element $g \in G$ die durch Konjugation mit g bewirkte Permutation der vier 3-Sylowuntergruppen zuordnet, ist eine Einbettung.

d) Alle Gruppen der Ordnung 12 ohne Untergruppen der Ordnung 6 sind isomorph.

G4.17 [Frühjahr 1986]

a) Zeigen Sie: Ist G eine Gruppe mit $1 < |G| < 24$, so besitzt G eine normale Sylowgruppe.

b) Geben Sie ein Beispiel für eine Gruppe der Ordnung 24 an, die keine normale Sylowgruppe besitzt (mit Begründung).

G4.18 [Herbst 1987] Wieviele Untergruppen der Ordnung 8 besitzt die symmetrische Gruppe S_4? Sind diese Untergruppen paarweise isomorph?

G4.19 [Frühjahr 1995] Zeigen Sie:

(a) Der kanonische Epimorphismus $\pi : \mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ ist nicht zerfallend, d.h. es gibt keinen Homomorphismus $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ mit $\pi \circ \varphi = \mathrm{id}$.

(b) Sei G eine Gruppe der Ordnung 196. Dann besitzt G eine normale 7-Sylowuntergruppe P, und der kanonische Epimorphismus $G \to G/P$ ist zerfallend.

G4.20 [Frühjahr 1978] G sei eine Gruppe der Ordnung $p^n q$, wobei p und q verschiedene Primzahlen sind. Von G wird vorausgesetzt, daß der Durchschnitt von je zwei verschiedenen p-Sylow-Untergruppen nur das Einselement von G enthält. Beweisen Sie: G ist nicht einfach.

G4.21 [Herbst 1984] Zeigen Sie: Jede Gruppe der Ordnung 200 enthält einen nichttrivialen abelschen Normalteiler. (Man zitiere die verwendeten Sätze!)

G4.22 [Frühjahr 1995] Sei G eine Gruppe der Ordnung 300. Zeigen Sie, daß G nicht einfach ist.

HINWEIS: Lassen Sie die Gruppe G auf der Menge ihrer 5-Sylowgruppen operieren.

G4.23 [Frühjahr 1978] Zeigen Sie: Es gibt keine einfache Gruppe der Ordnung 700.

G4.24 [Frühjahr 1998] Sei G eine Gruppe der Ordnung 750. Zeigen Sie, daß G einen echten Normalteiler besitzt.

HINWEIS: Lassen Sie G durch Konjugation auf der Menge $\mathrm{Syl}_5(G)$ aller 5-Sylowgruppen von G operieren.

G4.25 [Herbst 1978] Es sei G eine Gruppe der Ordnung $1722 = 41 \cdot 42$; mit S sei eine 41-Sylowgruppe von G bezeichnet, eine 7-Sylowgruppe von G sei T.

a) Zeigen Sie: S ist entweder Normalteiler oder normalisatorgleich.

b) Zeigen Sie: T ist entweder Normalteiler oder normalisatorgleich.

c) Beweisen Sie (etwa durch Abzählen der Elemente), daß höchstens eine der beiden Gruppen S und T normalisatorgleich sein können.

d) Begründen Sie, warum der Komplex ST eine kommutative Gruppe ist.

e) Zeigen Sie: Sowohl S als auch T ist Normalteiler von G.

f) Geben Sie ein Beispiel einer Gruppe der Ordnung 1722 an, deren maximaler abelscher Normalteiler die Ordnung $287 = 41 \cdot 7$ hat (es gibt mehrere paarweise nichtisomorphe).

G4.26 [Herbst 2002]

a) Zeigen Sie: Gruppen der Ordnung 2002 haben einen Normalteiler vom Index 2.

b) Zeigen Sie: Eine Gruppe der Ordnung 1001 ist zyklisch.

c) Zeigen Sie: Es gibt genau 8 Isomorphietypen von Gruppen der Ordnung 2002.

G4.27 [Herbst 1984] Bestimmen Sie bis auf Isomorphie alle Gruppen G, die genau vier verschiedene Untergruppen besitzen!

G4.28 [Frühjahr 1994] Es sei n eine ungerade natürliche Zahl. Zeigen Sie: Wenn es bis auf Isomorphie nur eine einzige Gruppe der Ordnung n gibt, dann gilt $(\phi(n), n) = 1$. (Dabei ist ϕ die Eulersche Phi-Funktion.)

Allgemeine Sylowtheorie

G4.29 [Frühjahr 1979] Es sei G eine endliche Gruppe, N ein Normalteiler von G und K eine p-Sylow-Untergruppe von G. Zeigen Sie: $K \cap N$ ist eine p-Sylow-Untergruppe von N.

HINWEIS: Untersuchen Sie KN.

G4.30 [Herbst 1998] Sei G eine endliche Gruppe, seien P eine p-Sylowuntergruppe und U eine weitere Untergruppe von G. Zeigen Sie:

a) Ist U oder P normal, so ist $P \cap U$ eine p-Sylowuntergruppe von U.

b) Ist P nicht normal, so gibt es eine Untergruppe U, so dass $P \cap U$ keine p-Sylowuntergruppe von U ist.

G4.31 [Herbst 1976] G sei eine einfache Gruppe der Ordnung 60. Zeigen Sie:

a) G besitzt genau sechs 5-Sylowgruppen.

b) G besitzt genau zehn 3-Sylowgruppen.

HINWEIS: Verwenden Sie a).

c) G besitzt keine Elemente der (genauen) Ordnung 6 und keine Elemente der (genauen) Ordnung 10.

HINWEIS: Wieviele solche Elemente müßte G sonst mindestens haben?

d) Der Durchschnitt je zweier verschiedener 2-Sylowgruppen von G ist trivial.

HINWEIS: Verwenden sie c).

e) G besitzt genau fünf 2-Sylowgruppen.

G4.32 [Frühjahr 1995]

a) Sei G eine einfache Gruppe der Ordnung 60. Man zeige, daß G genau sechs 5-Sylowuntergruppen und 24 Elemente der Ordnung 5 hat.

b) Man zeige, daß es in jeder Gruppe der Ordnung 56 nichttriviale Normalteiler gibt.

G4.33 [Herbst 1990] Untersuchung der symmetrischen Gruppe S_5:

a) Man bestimme die Struktur und die Anzahl der 2-Sylowgruppen der symmetrischen Gruppe S_5.

b) Man bestimme die Anzahl der 5-Sylowgruppen von S_5.

c) Besitzt S_5 eine Untergruppe der Ordnung 15?

d) Besitzt S_5 zwei zueinander nicht isomorphe Untergruppen der Ordnung 6?

G4.34 [Frühjahr 1984] Sei G eine endliche Gruppe und H eine Untergruppe von G vom Index n. Zeigen Sie:

a) $K := \bigcap_{g \in G} gHg^{-1}$ ist ein in H enthaltener Normalteiler von G, dessen Index in G ein Vielfaches von n und ein Teiler von $n!$ ist.

HINWEIS: Definieren Sie einen Homomorphismus von G in die Permutationsgruppe der Menge aller Linksnebenklassen gH, $g \in G$, von G nach H, dessen Kern K ist!

b) Jeder in H enthaltene Normalteiler von G liegt in K.

c) Ist p der kleinste Primteiler der Ordnung von G, so ist jede Untergruppe von G vom Index p ein Normalteiler.

d) Sei p eine Primzahl. Der Durchschnitt aller p-Sylowuntergruppen von G ist ein Normalteiler. Er enthält jede p-Untergruppe von G, die Normalteiler in G ist.

G4.35 [Herbst 1996] Sei $\mathbb{F}_p$ der Körper mit p Elementen (p eine Primzahl) und $\mathrm{GL}(n, \mathbb{F}_p)$ die allgemeine lineare Gruppe n-ten Grades über $\mathbb{F}_p$.

a) Gestützt auf die Formel

$$\mathrm{Ord}\,(\mathrm{GL}(n, \mathbb{F}_p)) = (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})$$

für die Ordnung der $\mathrm{GL}(n, \mathbb{F}_p)$ beweise man, daß die Untergruppe $U(n, \mathbb{F}_p) < \mathrm{GL}(n, \mathbb{F}_p)$ aller Matrizen der Form

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

eine p-Sylow-Untergruppe der $\mathrm{GL}(n, \mathbb{F}_p)$ bildet.

b) Als Anwendung zeige man: Ist G eine p-Gruppe von Automorphismen des endlich dimensionalen $\mathbb{F}_p$-Vektorraums V, so sind alle $g \in G$ simultan auf Dreiecksgestalt transformierbar.

G4.36 [Herbst 1999] Sei p eine Primzahl. Wie viele p-Sylow-Untergruppen besitzt die symmetrische Gruppe S_p?

G4.37 [Frühjahr 2001] Zeigen Sie $N_G(N_G(P)) = N_G(P)$ für eine p-Sylowuntergruppe P der endlichen Gruppe G. ($N_G(U)$ ist der Normalisator der Untergruppe U von G.)

5. Auflösbare Gruppen

G5.1 [Herbst 1994]

a) Sei N eine normale Untergruppe einer Gruppe G. Zeigen Sie: Sind die Faktorgruppen G/N und N auflösbar, so ist auch G auflösbar.

b) Sei G eine nicht-triviale endliche p-Gruppe. Zeigen Sie: G besitzt ein nichttriviales Zentrum, und G ist auflösbar.

G5.2 [Herbst 1999] Seien p und q verschiedene Primzahlen. Man beweise, dass jede Gruppe der Ordnung pq^2 auflösbar ist.

G5.3 [Herbst 1994] Beweisen Sie: Jede Gruppe der Ordnung 297 ist auflösbar.

G5.4 [Herbst 1989] Es sei S_4 die Gruppe aller Permutationen von $\{1,2,3,4\}$.

a) Man zeige, daß
$$U := \{\sigma \in S_4\,;\ \sigma(1) = 1\}$$
eine Untergruppe, aber kein Normalteiler in S_4 ist.

b) Gibt es in S_4 eine Untergruppe der Ordnung 8?

c) Man gebe eine 3-Sylow-Untergruppe von S_4 an.

d) Man zeige, daß S_4 auflösbar ist (man gebe eine Auflösung ohne Begründung an).

G5.5 [Herbst 2000]

a) Geben Sie die Definitionen der Begriffe *Normalteiler* und *auflösbare Gruppe* an.

b) Sei G eine Gruppe der Ordnung 100. Zeigen Sie:

(i) G ist auflösbar.

(ii) Hat G einen Normalteiler der Ordnung 4, so ist G abelsch.

HINWEIS: Es darf verwendet werden, dass Gruppen der Ordnung p^2 abelsch sind, wenn p eine Primzahl ist.)

G5.6 [Herbst 1973]

a) K sei ein Körper. Eine Abbildung $\ell : K \to K$ heiße *linear*, wenn es Elemente $a, b \in K$ gibt, $a \neq 0$, so daß $\ell(x) = ax + b$ für alle $x \in K$ gilt. Zeige, daß die Menge $L(K)$ aller linearen Abbildungen $\ell : K \to K$ bzgl. der Komposition von Abbildungen eine Gruppe ist.

b) Im folgenden sei K ein endlicher Körper. Sei $\ell \in L(K)$ durch $\ell(x) = ax + b$ gegeben. Zeige: Ist $a \neq 1$, dann ist die Ordnung von ℓ gleich der Ordnung von a in der multiplikativen Gruppe $K^\times$ von K. Ist $a = 1$, dann ist die Ordnung von ℓ gleich der Ordnung von b in der additiven Gruppe K^+ von K.

c) K sei ein Körper mit q Elementen. Zeige, daß es in $L(K)$ genau eine Untergruppe U der Ordnung q gibt.

d) Unter welchen Voraussetzungen über q ist U zyklisch?

e) Zeige, daß U ein Normalteiler von $L(K)$ ist und $L(K)/U$ eine zyklische Gruppe.

f) Diskutiere, unter welchen Voraussetzungen über die Elementezahl von K die Gruppe $L(K)$ zyklisch, abelsch, auflösbar ist.

G5.7 [Frühjahr 1997] Sei p eine Primzahl und $\mathbb{F}_p$ der Körper mit p Elementen. Eine Permutation σ von $\mathbb{F}_p$ heißt *affin*, falls es Elemente $a, b \in \mathbb{F}_p$ mit $a \neq 0$ gibt, so daß $\sigma(x) = ax + b$ für $x \in \mathbb{F}_p$ gilt. Es bezeichne G die Menge aller affinen Permutationen von $\mathbb{F}_p$.

a) Zeigen Sie, daß G eine Gruppe und isomorph zur Gruppe aller Matrizen $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ mit $a, b \in \mathbb{F}_p$ und $a \neq 0$ ist.

b) Geben Sie einen surjektiven Homomorphismus ϕ von G auf die multiplikative Gruppe $\mathbb{F}_p^\times$ an, dessen Kern N zyklisch von der Ordnung p ist.

c) Begründen Sie, warum G auflösbar ist.

G5.8 [Frühjahr 2002] Sei a ein Element der Ordnung $d > 1$ in der multiplikativen Gruppe des Körpers $\mathbb{Z}/p\mathbb{Z}$ und G die von den Abbildungen

$$\mu : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \quad (x \mapsto ax) \qquad \text{und} \qquad \alpha : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \quad (x \mapsto x+1)$$

erzeugte Untergruppe der Permutationsgruppe von $\mathbb{Z}/p\mathbb{Z}$. Zeigen Sie:

a) G ist nicht abelsch.

b) Jedes $g \in G$ besitzt eine eindeutige Darstellung

$$g = \mu^r \alpha^s \ (0 \leq r < d,\ 0 \leq s < p) \quad .$$

c) G ist auflösbar.

d) Es gibt eine nicht abelsche Gruppe der Ordnung 555.

G5.9 [Herbst 1985]

a) Man berechne für die Dreierzyklen $\varphi = (1,2,4),\ \psi = (3,5,1)$ das Produkt $\varphi\psi\varphi^{-1}\psi^{-1}$ (Berechnung von rechts nach links).

b) Man folgere hieraus, daß die alternierende Gruppe A_5 vom Grad 5 nicht auflösbar ist.

Staatsexamensaufgaben zur Ringtheorie

Inhalt

1. Elementare Ringtheorie

Rechnen in kommutativen Ringen

R1.1 [Herbst 1981] Sei R ein nullteilerfreier kommutativer Ring (nicht notwendig mit 1). Man beweise: Gibt es $a, c \in R$ mit $a \neq 0$ und $ac = a$, dann hat R ein Einselement, nämlich c.

R1.2 [Herbst 1999] Seien a und b Elemente eines assoziativen kommutativen Integritätsrings R. Es bezeichne α die Restklasse von a in $R/(b)$ und β die von b in $R/(a)$. Zeigen Sie: Ist α kein Nullteiler von $R/(b)$, so ist β keiner von $R/(a)$.

R1.3 [Herbst 1987] R sei ein kommutativer Ring mit Eins und d eine Derivation von R, d.h. eine Abbildung $d: R \to R$ mit

$$d(x+y) = dx + dy \quad , \quad d(x \cdot y) = x \cdot dy + y \cdot dx \qquad \text{für alle } x, y \in R.$$

a) Zeigen Sie, daß Kern $d := \{x \in R;\ dx = 0\}$ ein Unterring von R ist, der die Eins enthält.

b) Beweisen Sie die Formel $d(x^n) = n \cdot x^{n-1} dx$ für $x \in R$, $n \in \mathbb{Z}$, $n > 0$.

c) Zeigen Sie, daß jede Derivation eines endlichen Körpers die Nullabbildung ist.

d) Zeigen Sie, daß der Ring $\mathbb{Z}[X]/(X^2)$ eine nichttriviale Derivation besitzt.

Beispiele kommutativer Ringe

R1.4 [Herbst 1978] Sei M eine Menge und $P(M)$ die Menge aller Teilmengen von M. Für $a, b \in P(M)$ definiere man eine Summe und ein Produkt durch

$$a + b = \{m \in M:\ m \in a \cup b,\ m \notin a \cap b\}$$
$$ab = a \cap b \quad .$$

a) Man zeige, daß $P(M)$ ein kommutativer, assoziativer Ring mit 1 ist.

b) Sei T eine Teilmenge von M. Man zeige, daß

$$P(M) \to P(T):\ a \to a \cap T$$

ein Epimorphismus ist. Welches ist sein Kern?

c) Sei M nicht leer. Für $m \in M$ sei $I_m = \{a \in P(M):\ m \notin a\}$. Man zeige, daß I_m ein maximales Ideal von $P(M)$ ist. Welches ist der Körper $P(M)/I_m$? Für endliches M ist jedes maximale Ideal von $P(M)$ ein I_m.

d) Sei K der Körper mit zwei Elementen. Man zeige, daß die Menge aller Abbildungen $f: M \to K$ (bezüglich welcher Operationen?) einen zu $P(M)$ isomorphen Ring bildet.

R1.5 [Frühjahr 1973] Sei M die Menge aller Polynome in der Variablen x mit Koeffizienten aus dem Körper der reellen Zahlen. Wir definieren folgende Verknüpfungen für zwei beliebige Polynome P, Q:

$P + Q$ als die (übliche) Addition, und die Multiplikation $*$ als

$$(P * Q)(x) = \int_0^x P'(t)Q'(t)\, dt + P(0)Q(0) \quad .$$

a) Zeigen Sie, daß M unter den Verknüpfungen $+$ und $*$ ein Ring ist. Im folgenden kürzen wir $(M, +, *)$ durch M ab.

b) Untersuchen Sie, ob M eine Eins besitzt.

c) Zeigen Sie, daß die Menge der Konstanten ein Ideal I_1 in M ist.

d) Zeigen Sie, daß die Menge der Polynome $R(x)$ mit $R(0) = 0$ ein Ideal I_2 in M ist.

e) Geben Sie die idempotenten Elemente von M an.

f) Zeigen Sie, daß M Nullteiler besitzt.

g) Geben Sie alle Ideale von I_2 an.

HINWEIS: Betrachten Sie die Abbildung $P \mapsto P'$ von $(M, +, *)$ in $(M, +, \cdot)$

h) Geben Sie alle Ideale von $M = I_1 + I_2$ an. Welche Ideale von M sind keine Hauptideale?

R1.6 [Herbst 1977] Sei M die Menge aller reellwertigen auf den nichtnegativen reellen Zahlen definierten und dort stetig differenzierbaren Funktionen. Mit der üblichen Addition und der neuen Multiplikation $*$ definiert durch

$$(f * g)(x) = f(0)g(0) + \int_0^x f'(t)g'(t)\, dt$$

(so daß also insbesondere $(f * g)'(x) = f'(x)g'(x)$ gilt) ist $M(+, *)$ ein kommutativer Ring (dies ist nicht zu zeigen).

a) Bestimmen Sie alle idempotenten Elemente von $M(+, *)$.

b) Geben Sie notwendige und hinreichende Bedingungen dafür an, daß zu einer Funktion f das multiplikative Inverse in $M(+, *)$ existiert.

c) Zu reellem nichtnegativen a definiert man eine Funktion $t_a \in M$ durch die Vorschrift

$$t_a(x) = \begin{cases} 0 & \text{für } x \le a \\ (x-a)^2 & \text{für } x \ge a \ . \end{cases}$$

Zeigen Sie, daß für jede Funktion g aus dem von t_a erzeugten Hauptideal der Grenzwert

$$\lim_{x \to a+0} \frac{g(x) - g(a)}{(x-a)^2}$$

existiert und beschreiben Sie den Werteverlauf von g für $x \le a$.

d) Manche Ideale von M lassen sich dadurch beschreiben, daß man Bedingungen über den Werteverlauf der darin enthaltenen Funktionen angibt, die notwendig und hinreichend sind.
Geben Sie solche Bedingungen an

i. für jedes von einem idempotenten Element erzeugte Hauptideal von M,

ii. für das Ideal J, das erzeugt ist von allen Funktionen f mit $f(x) = 0$ für $1 \le x \le 2$.

HINWEIS: Betrachten Sie zunächst $(cf) * f$ mit f aus J und c aus R.

R1.7 [Herbst 2001] Auf der Menge $\mathbf{D}$ aller Polynome in x mit rationalen Koeffizienten seien die Operation „Addition“ $\oplus$ und „Multiplikation“ $\odot$ wie folgt definiert:

$$f(x) \oplus g(x) = f(x) + g(x) \quad ,$$

$$f(x) \odot g(x) = \int_0^x f'(t)g'(t)dt + f(0)g(0) \quad .$$

a) Zeigen Sie: Auch mit diesen Operationen ist $\mathbf{D}$ ein assoziativer Ring mit Einselement.

b) Bestimmen Sie die idempotenten Elemente von $\mathbf{D}$, d.h. die Elemente mit $f \odot f = f$.

c) Geben Sie $\mathbf{D}$ als direkte Summe von Teilringen an und beschreiben Sie einen der beiden Summanden.

Endliche Ringe

R1.8 [Herbst 1975] In allen Teilaufgaben dieser Aufgabe ist R ein kommutativer endlicher Ring (nicht notwendig mit 1). Zur Lösung sollen keine Struktursätze aus der Theorie der Ringe mit Minimalbedingung als bekannt vorausgesetzt werden.

a) R besitze ein (von 0 und 1 verschiedenes) idempotentes Element. Beweisen Sie, daß R dann die direkte Summe von zwei nichttrivialen Ringen ist.

b) Beweisen Sie, daß jedes Element x aus R eine der drei folgenden Aussagen erfüllt:

i. x ist 0 oder nilpotent,

ii. x ist eine Einheit in R,

iii. eine Potenz von x ist idempotent.

c) Zeigen Sie, daß R genau dann die direkte Summe von Körpern ist, wenn R keine (von 0 verschiedene) nilpotenten Elemente besitzt.

d) Beweisen Sie die Äquivalenz der folgenden zwei Aussagen:

i. R ist direkte Summe eines Rings mit trivialer Multiplikation und eines Rings ohne (von 0 verschiedene) nilpotente Elemente,

ii. Jedes nilpotente Element von R liegt im Annullator von R.

e) Für jedes Element x aus R gelte die Gleichung

$$x^5 - x = 0 \quad . \qquad (*)$$

Sei R als direkte Summe möglichst vieler nichttrivialer Summanden geschrieben. Bestimmen Sie die Isomorphieklassen dieser Summanden.

Hinweis: Untersuchen Sie zunächst die nilpotenten Elemente von R.

f) Geben Sie einen unendlichen kommutativen Ring ohne 1 an, dessen Elemente die Gleichung $(*)$ erfüllen.

R1.9 [Herbst 1983] Ist R ein Ring, so bezeichne $R[x]$ den Polynomring über R in der Unbestimmten x. Ist f ein Polynom aus $R[x]$, so sei $R[x]/(f)$ der Restklassenring von $R[x]$ nach dem von f erzeugten Ideal. Für natürliche Zahlen n sei ferner $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ der Restklassenring der ganzen Zahlen modulo n.

Man zeige, daß es genau vier nicht-isomorphe Ringe mit Eins mit vier Elementen gibt, nämlich $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2[x]/(x^2+x+1)$ und $\mathbb{Z}_2[x]/(x^2)$. Welche davon sind Körper?

R1.10 [Herbst 1990] Es sei p eine Primzahl und R ein kommutativer Ring mit Einselement und p^2 Elementen.

a) Man beweise, daß genau einer der folgenden vier Fälle vorliegt:
Fall 1: $R \simeq \mathbb{Z}/p^2\mathbb{Z}$
Fall 2: R ist ein Körper
Fall 3: $R \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
Fall 4: $R \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2)$.

b) In jedem dieser vier Fälle bestimme man die Ordnung und die Struktur der Einheitengruppe von R.

R1.11 [Frühjahr 1993] Es seien p und q zwei verschiedene Primzahlen und R ein Ring mit Einselement mit pq Elementen. Man beweise, daß

$$R \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

ist.

R1.12 [Frühjahr 1979] Beweisen Sie: Wenn in einem Integritätsbereich R jeder echte Unterring nur endlich viele Elemente enthält, dann ist R ein Körper.
(Aussagen über endliche nullteilerfreie Ringe können ohne Beweis verwendet werden.)

R1.13 [Frühjahr 1991] Sei R ein Integritätsring. Man beweise:
R ist ein Körper, wenn jeder von einem Element erzeugte Unterring von R nur endlich viele Elemente enthält.

R1.14 [Frühjahr 1986] Zeigen Sie, daß der Ring $\mathbb{Z}[X]/(X^5+2,\ X^4+X^3+X^2+X+1)$ ein Körper ist.

R1.15 [Herbst 1986] Im Polynomring $\mathbb{Z}[X]$ sei I das von

$$X^4 - 2X^3 + X^2 \quad \text{und} \quad X^6 - 2X^4 + X^2 - 2$$

erzeugte Ideal, und es sei $R := \mathbb{Z}[X]/I$.

a) Zeigen Sie, daß R endlich ist, und bestimmen Sie die Anzahl der Elemente von R.

b) Zeigen Sie, daß R genau zwei Primideale besitzt.

c) Bestimmen Sie die Struktur der Einheitengruppe von R.

d) Bestimmen Sie die nilpotenten Elemente von R.

R1.16 [Frühjahr 2002] Sei $I \subset \mathbb{Z}[X]$ das von den Polynomen X^4+3X^3+X und $X^5-9X^3+X^2-3X+3$ erzeugte Ideal.

a) Zeigen Sie, dass $3 \in I$ ist.

b) Bestimmen Sie die Anzahl der Elemente von $R := \mathbb{Z}[X]/I$.

c) Zeigen Sie, dass R eine zu $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2$ isomorphe Einheitengruppe hat.

R1.17 [Herbst 1980] Sei K ein endlicher Körper mit q Elementen. Gegeben seien paarweise verschiedene normierte irreduzible Polynome $p_1, \ldots, p_r \in K[X]$ (Grad $p_i =: n_i$). Man berechne die Ordnung der Einheitengruppe des Restklassenrings

$$K[X]/(f) \quad \text{mit} \quad f = p_1 p_2 \ldots p_r \quad .$$

Ringhomomorphismen

R1.18 [Frühjahr 1979] In dem Ring R sei U ein Unterring und V ein Ideal. Beweisen Sie:

$$(U+V)/V \simeq U/(U \cap V) \quad .$$

(Der Homomorphiesatz für Ringe kann ohne Beweise verwendet werden.)

R1.19 [Herbst 1979] Bestimme alle Homomorphismen des Ringes $\mathbb{Z}[X]/(X^4-1)$ in die Ringe $\mathbb{Z}/16$, $\mathbb{F}_{16}$, $\mathbb{Z}/60$, sowie in den Ring $\mathrm{M}_2(\mathbb{R})$ der zweireihigen Matrizen über $\mathbb{R}$.

R1.20 [Herbst 1995] Man bestimme alle unitären Ringhomomorphismen des Ringes $\mathbb{Z}[X]/(X^4-1)$ in die Ringe $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/60\mathbb{Z}$ sowie in den Körper $\mathbb{F}_{64}$ mit 64 Elementen.

R1.21 [Frühjahr 1980]

a) Es seien R, S, T Ringe und $\sigma : R \to S$, $\tau : R \to T$ Ringhomomorphismen. Man beweise: Wenn τ surjektiv ist und der Kern K_τ von τ im Kern K_σ von σ enthalten ist, gibt es einen Homomorphismus $\varphi : T \to S$ mit $\sigma = \varphi \circ \tau$; und $\tau(K_\sigma)$ ist der Kern von φ.

b) Bleibt die Aussage a) gültig, wenn in der Voraussetzung auf die Surjektivität von τ verzichtet wird?

R1.22 [Herbst 1983] Seien R und S kommutative Ringe mit $1 \neq 0$. Sei $\varphi : R \to S$ ein surjektiver Ringhomomorphismus. X sei eine Unbestimmte. Man zeige:

a) Für jedes Primideal $\mathfrak{p}$ von S ist $\varphi^{-1}(\mathfrak{p})$ ein Primideal von R. Zu jedem Primideal $\mathfrak{P}$ von R, welches den Kern von φ umfaßt, gibt es genau ein Primideal $\mathfrak{p}$ von S mit $\varphi^{-1}(\mathfrak{p}) = \mathfrak{P}$. (Man verwende den Homomorphiesatz).

b) In $R[X]$ gibt es unendlich viele Primideale. (Beweisen Sie dies zunächst für den Fall, daß R ein Körper ist, und führen Sie den allgemeinen Fall darauf zurück).

R1.23 [Frühjahr 1990] Sei $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ die Menge aller Primzahlen. Für eine natürliche Zahl $n > 2$ sei

$$\mathbb{P}_n = \{p \in \mathbb{P} : p < n\} \quad .$$

Man betrachte die Ringe

$$R_n := \prod_{p \in \mathbb{P}_n} \mathbb{F}_p \quad \text{und} \quad R := \prod_{p \in \mathbb{P}} \mathbb{F}_p \quad .$$

Dabei ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Primkörper der Charakteristik p. Die kanonische Abbildung $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induziert Abbildungen

$$\varphi_n : \mathbb{Z} \to R_n, \quad x \mapsto (x \bmod p)_{p \in \mathbb{P}_n} \quad ,$$
$$\varphi : \mathbb{Z} \to R, \quad x \mapsto (x \bmod p)_{p \in \mathbb{P}} \quad .$$

Man zeige: φ_n ist surjektiv, aber nicht injektiv; und φ ist injektiv, aber nicht surjektiv.

R1.24 [Frühjahr 1990] Mit den Bezeichnungen der vorigen Aufgabe sei $I \subseteq R$ die Menge aller Folgen $(a_p)_{p \in \mathbb{P}} \in R$ mit folgender Eigenschaft:

$$\text{Es gibt ein } n \in \mathbb{N}, \text{ so daß } a_p = 0 \text{ für alle } p > n.$$

a) Man zeige, daß I ein Ideal von R ist.

b) Sei $\overline{R} = R/I$ der Restklassenring und $\bar{\varphi} : \mathbb{Z} \to \overline{R}$ die Komposition der Abbildung $\varphi : \mathbb{Z} \to R$ und der kanonischen Abbildung $R \to \overline{R}$. Man zeige, daß $\bar{\varphi}$ injektiv, aber nicht surjektiv ist.

R1.25 [Frühjahr 2001] Sei $K|\mathbb{Q}$ eine quadratische Erweiterung. Sei $\mathrm{End}_{\mathbb{Q}}(K)$ der Ring der $\mathbb{Q}$-linearen Abbildungen von K nach K. Man definiere $T: K \to \mathrm{End}_{\mathbb{Q}}(K)$ durch $T(a)(b) = ab$, $a, b \in K$.

a) Man zeige, dass T ein injektiver Ringhomomorphismus ist.

b) Sei $Z(T(K))$ der Zentralisator von $T(K)$ in $\mathrm{End}_{\mathbb{Q}}(K)$. Man zeige, dass $Z(T(K)) = T(K)$ gilt.

Faktorringe

R1.26 [Frühjahr 1980] Sei K ein Körper und sei R die Menge derjenigen $(2,2)$-Matrizen mit Koeffizienten in K, die mit der Matrix $\begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}$ kommutieren.

a) Bestimmen Sie R und zeigen Sie, daß R bzgl. der Matrizenaddition und -multiplikation ein kommutativer Ring ist.

b) Geben Sie ein $f \in K[X]$ an, so daß R isomorph zum Restklassenring $K[X]/(f)$ ist, wobei (f) das von f in $K[X]$ erzeugte Hauptideal ist.

c) Zeigen Sie: Für $K = \mathbb{Q}$ und für $K = \mathbb{F}_3$ ist R ein Körper, für $K = \mathbb{F}_{11}$ jedoch nicht. ($\mathbb{F}_p$ ist ein Körper mit p Elementen).

R1.27 [Herbst 1995] Es sei K ein Körper und R die Menge aller 2×2-Matrizen über K, die mit $\begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}$ vertauschbar sind. Zeigen Sie:

a) R ist ein Unterring von $M_2(K)$ und R ist kommutativ.

b) Es existiert ein $f \in K[X]$ mit $R \simeq K[X]/(f)$.

c) Für $K = \mathbb{Q}$ und $K = \mathbb{Z}/3\mathbb{Z}$ ist R ein Körper. Für $K = \mathbb{Z}/11\mathbb{Z}$ ist R kein Körper.

R1.28 [Frühjahr 1981] Sei K ein Körper, X eine Unbestimmte über K und $f \in K[X]$ vom Grad $n > 0$. Sei $K[X]/(f) = L$.
Zeige: L besitzt genau dann nilpotente Elemente $\neq 0$, wenn in $K[X]$ eine Zerlegung $f = g^2 \cdot h$ gilt mit Grad $(g) > 0$.

R1.29 [Frühjahr 1984] p sei eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen. Zeigen Sie:

a) Es gibt einen Ringisomorphismus $\mathbb{Z}[X]/p\mathbb{Z}[X] \simeq \mathbb{F}_p[X]$.

b) Jedes Ideal von $\mathbb{Z}[X]$, welches p enthält, wird von zwei (oder weniger) Elementen erzeugt.

R1.30 [Frühjahr 2000] Sei k ein Körper, X eine Unbestimmte über k und $f \in k[X]$ vom Grad $n > 0$. Sei $u := X + (f)$ in $k[X]/(f)$.

a) Man zeige: Jedes Element von $k[u] = k[X]/(f)$ lässt sich eindeutig in der Form

$$a_0 + a_1 u + \ldots + a_{n-1} u^{n-1}$$

mit $a_i \in k$ schreiben.

b) Man zeige: $k[u]$ besitzt genau dann nilpotente Elemente $\neq 0$, wenn $f = g^2 h$ in $k[X]$ mit $\deg g > 0$ gilt.

c) Sei speziell $k = \mathbb{Q}$ und $f = X^3 + 3X - 2$. Man zeige, dass $k[u]$ ein Körper ist und stelle das Element

$$(u^2 + 1)^{-1}$$

als Polynom vom Grad ≤ 2 in u über $\mathbb{Q}$ dar.

R1.31 [Herbst 2001] Im Polynomring $K[X,Y]$ in den Unbestimmten X,Y über einem Körper K sei I das von X^4, Y^4, X^3Y, XY^3 erzeugte Ideal und $R := K[X,Y]/I$. Ferner seien $\zeta := X+I$, $\eta := Y+I$ die Restklassen von X bzw. Y in R.

a) Welche Dimension besitzt R als K-Vektorraum? Begründen Sie Ihre Aussage.

b) Welche Dimension besitzt der Sockel $S := \{f \in R;\ \zeta f = \eta f = 0\}$ von R als K-Vektorraum? Begründen Sie Ihre Aussage.

c) Bestimmen Sie alle Primideale von R.

R1.32 [Frühjahr 1991] Sei $R = \mathbb{R}[x,y]/(x^2+y^2-1)$.

a) Zeigen Sie, daß jedes Element von R durch genau ein $f \in \mathbb{R}[x,y]$ der Form

$$f = a + by\,, \quad a,b \in \mathbb{R}[x] \quad ,$$

repräsentiert wird.

b) Zeigen Sie, daß R ein Integritätsbereich ist.

c) Bestimmen Sie die Einheiten von R.

Bruchrechnung

R1.33 [Frühjahr 1985] Seien R ein kommutativer Integritätsring und $a,b \in R$ mit $b \neq 0$. Beweise die Äquivalenz folgender Aussagen:

(i) Es gibt $c,d \in R$ mit $d \neq 0$, $\frac{a}{b} = \frac{c}{d}$ (im Quotientenkörper von R) und $Rc + Rd = R$.

(ii) $Ra + Rb$ ist Hauptideal.

Primelemente

R1.34 [Frühjahr 1981] Definieren Sie die Begriffe „irreduzibles Element“ und „Primelement“ in einem kommutativen Integritätsring mit 1. Zeigen Sie, daß jedes Primelement irreduzibel ist und geben Sie (ohne Beweis) einen Integritätsring an, in dem es irreduzible Elemente gibt, welche keine Primelemente sind.

R1.35 [Herbst 1996] Man definiere für einen kommutativen Ring die Begriffe „irreduzibles Element“, „Primelement“ und „Primideal“ und zeige, daß in einem Integritätsring A mit 1 für ein Element $p \in A$ gilt:

a) p Primelement $\implies$ p irreduzibel

b) p Primelement $\iff$ (p) Primideal $\neq 0$

c) p irreduzibel $\iff$ Es gilt $0 \neq (p) \subsetneqq A$, und es existiert kein $a \in A$ mit $(p) \subsetneqq (a) \subsetneqq A$.

R1.36 [Frühjahr 1979] Euklid hat gezeigt, daß die Menge der Primzahlen unendlich ist.

a) Verwenden Sie seine Schlußweise, um zu beweisen, daß es für jeden Körper K im Polynomring $K[X]$ unendlich viele, paarweise nichtassoziierte irreduzible Polynome gibt.

b) Folgern Sie, daß jeder algebraisch abgeschlossene Körper unendlich viele Elemente besitzt.

R1.37 [Frühjahr 1982] Modifizieren Sie den Euklidischen Beweis für die Existenz unendlich vieler Primzahlen zu einem Beweis für die folgende Aussage: Für jeden Körper K enthält der Polynomring $K[X]$ unendlich viele normierte irreduzible Polynome.

R1.38 [Frühjahr 1988] Zeigen Sie:

a) Im Polynomring $K[X]$ über einem beliebigen Körper K gibt es unendlich viele paarweise nicht assoziierte irreduzible Polynome.

b) Endliche Körper sind nicht algebraisch abgeschlossen.

Ringe mit Polynomidentität

R1.39 [Frühjahr 1978] R sei ein kommutativer Ring mit 1, in dem $x^2 = x$ für alle x aus R gilt. Beweisen Sie: Jedes Primideal von R ist ein maximales Ideal.

R1.40 [Frühjahr 1980] Sei R ein kommutativer Ring mit 1, der folgende Eigenschaft besitzt: Für alle $a \in R$ gibt es eine natürliche Zahl $n \geq 2$ mit $a^n = a$. Zeigen Sie:
Jedes Primideal $(\neq R)$ in R ist maximales Ideal.

R1.41 [Frühjahr 1977] Sei R ein kommutativer Ring mit Einselement. Seien p, q positive Primzahlen in $\mathbb{Z}$. Für alle $r \in R$ gelte $r^p = r$. Zeigen Sie:

a) Sei $I \subsetneq R$ ein Ideal. Dann gilt $s^p = s$ für alle $s \in R/I$.

b) R hat keine nilpotenten Elemente ($r \in R$ heißt *nilpotent*, wenn $r \neq 0$ und wenn ein $n \in \mathbb{N}$ mit $r^n = 0$ existiert.)

c) Ist R nullteilerfrei, so ist jedes $r \in R \setminus \{0\}$ invertierbar.

d) Jedes Primideal von R ist ein maximales Ideal.

e) Für jedes $m \in \mathbb{Z}$ und jedes $r \in R$ gilt $(m^p - m) \cdot r = 0$.

f) Sei n_p das positive Erzeugende des Hauptideals $(m^p - m\,;\ m \in \mathbb{Z})$.

i) Es gilt $n_p \cdot r = 0$ für alle $r \in R$.

ii) Für alle $r \in \mathbb{Z}/(n_p)$ gilt $r^p = r$.

g) Für alle $r \in \mathbb{Z}/(p) \setminus \{\bar{0}\}$ gilt $r^{p-1} = 1$.

h) Es ist $r^p = r$ für alle $r \in \mathbb{Z}/(q)$ dann und nur dann, wenn $q - 1 \mid p - 1$.
HINWEIS: Die multiplikative Gruppe der invertierbaren Elemente von $\mathbb{Z}/(q)$ ist zyklisch.

i) Es ist $r^p = r$ für alle $r \in \mathbb{Z}/(q)$ dann und nur dann, wenn $q \mid n_p$ gilt.
HINWEIS: Man benutze Teil a) und f).

j) n_p ist quadratfrei. ($n \in \mathbb{Z}$ heißt *quadratfrei*, wenn gilt: Aus $n \mid c^2$ folgt $n \mid c$.)
HINWEIS: Man verwende b) und f).

k) Ist J = Menge der positiven Primzahlen q aus $\mathbb{Z}$ mit $q - 1 \mid p - 1$, so gilt

$$n_p = \prod_{q \in J} q \quad .$$

Nichtkommutative Ringe

R1.42 [Herbst 1974] Es sei $\mathfrak{R} = (R, +, \cdot)$ ein Ring mit mehr als einem Element und mit der Eigenschaft, daß es zu jedem von 0 verschiedenen Element $x \in R$ ein eindeutig bestimmtes $a \in R$ mit $x \cdot a \cdot x = x$ gibt. Man beweise:

a) $\mathfrak{R}$ besitzt keine von 0 verschiedenen Nullteiler.

b) Ist $x \cdot a \cdot x = x$ mit $x \neq 0$, so ist $a \cdot x \cdot a = a$.

c) $\mathfrak{R}$ hat ein Einselement.

d) $\mathfrak{R}$ ist ein Schiefkörper.

R1.43 [Herbst 1976] Alle vorkommenden Ringe seien assoziativ. Ein Ring R heißt *regulär*, wenn es zu jedem $a \in R$ ein $b = b(a) \in R$ gibt mit $a = a^2 b$. Man zeige:

a) Ist $f: R \to S$ ein Ringepimorphismus und ist R regulär, so ist auch S regulär.

b) Sind $R_1, R_2, \ldots, R_n$ reguläre Ringe, dann ist auch das direkte Produkt $R = R_1 \times R_2 \times \ldots \times R_n$ ein regulärer Ring.

c) Ist R ein regulärer Ring und ist $x \in R$ nilpotent (d.h. es gibt ein $n \in \mathbb{N}$ mit $x^n = 0$), dann folgt $x = 0$.

d) Für eine ganze Zahl $m > 1$ ist der Ring $\mathbb{Z}/m\mathbb{Z}$ genau dann regulär, wenn m quadratfrei ist. (m heißt *quadratfrei*, wenn m sich schreiben läßt in der Form $m = p_1 p_2 \ldots p_r$ mit paarweise verschiedenen Primzahlen $p_i (1 \leq i \leq r)$.)

HINWEIS: Verwende b) und c).

R1.44 [Herbst 1993]

a) Zeigen Sie: Jeder Ring R mit Einselement ist vermöge der Zuordnung

$$R \to \operatorname{End} R^+$$
$$a \mapsto (L_a : \; x \mapsto ax)$$

isomorph zu einem Unterring des Endomorphismenrings seiner additiven Gruppe R^+.

(b) Zu einem beliebigen (d.h. nicht notwendig ein Einselement enthaltenden) Ring Q seien auf der Menge $S_Q = \{(m, a);\ m \in \mathbb{Z},\ a \in Q\}$ die Verknüpfungen

$$(m, a) + (n, b) := (m + n, a + b) \quad , \quad (m, a) \cdot (n, b) := (mn, ab + mb + na)$$

definiert.

Zeigen Sie: Dadurch erhält S_Q die Struktur eines Ringes mit Einselement. Der Ring S_Q ist kein Integritätsbereich, falls Q ein Einselement besitzt.

(c) Kann ein beliebiger Ring Q als Unterring eines Endomorphismenringes aufgefaßt werden? (Antwort mit Begründung)

R1.45 [Frühjahr 1999] Seien $\mathrm{M}_2(\mathbb{R})$ der Ring aller reellen 2×2-Matrizen, $A \in \mathrm{M}_2(\mathbb{R})$ eine Matrix und $\mathbb{R}[A]$ der von A und $\mathbb{R} \cdot \mathbf{1}_2$ in $\mathrm{M}_2(\mathbb{R})$ erzeugte Teilring. Man zeige, dass dann (in Abhängigkeit von A) genau einer der folgenden $\mathbb{R}$-linearen Ringisomorphismen existiert:

i) $\mathbb{R}[A] \xrightarrow{\simeq} \mathbb{R}$,

ii) $\mathbb{R}[A] \xrightarrow{\simeq} \mathbb{R} \times \mathbb{R}$,

iii) $\mathbb{R}[A] \xrightarrow{\simeq} \mathbb{R}[X]/(X^2)$,

iv) $\mathbb{R}[A] \xrightarrow{\simeq} \mathbb{C}$.

R1.46 [Frühjahr 1990] Sei K ein Körper und $m \in K$. Man betrachte die folgende Teilmenge des Matrizenringes $\mathrm{M}_2(K)$:

$$L_m := \left\{ \begin{pmatrix} a & b \\ mb & a \end{pmatrix} : \; a, b \in K \right\} \quad .$$

a) Man zeige: L_m ist bezüglich der Matrizen-Addition und -Multiplikation ein kommutativer Ring.

b) Man beweise: Genau dann ist L_m ein Körper, wenn m kein Quadrat in K ist.

c) Sei speziell $K = \mathbb{F}_p$ mit einer ungeraden Primzahl p. Man zeige, daß es stets ein $m \in \mathbb{F}_p$ gibt, das der Bedingung in b) genügt. Welcher Körper entsteht dabei?

R1.47 [Frühjahr 2000] Es sei V ein Vektorraum mit der Basis $\{e_1, e_2\}$ über einem Körper K und R die Menge der K-linearen Abbildungen $f : \; V \to V$ mit $f(e_1) = \alpha e_1$ und $f(e_2) = \beta e_1 + \gamma e_2$ mit $\alpha, \beta, \gamma \in K$. Man zeige:

a) R ist ein Teilring des Endomorphismenringes $\mathrm{End}_K V$, und V besitzt als R-Modul einen von 0 und V verschiedenen Untermodul.

b) Die Menge $\mathrm{End}_R(V)$ der R-linearen Abbildungen des R-Moduls V in sich ist ein Körper.

R1.48 [Herbst 1999] Es bezeichne $\mathrm{M}_4(\mathbb{Q})$ den Ring aller rationalen 4×4-Matrizen und R die Menge aller $A \in \mathrm{M}_4(\mathbb{Q})$ der Form

$$A = \begin{pmatrix} a & d & c & b \\ b & a & d & c \\ c & b & a & d \\ d & c & b & a \end{pmatrix} \quad .$$

Es sei $E \in \mathrm{M}_4(\mathbb{Q})$ die Einheitsmatrix und

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

a) Zeigen Sie, dass $P^4 = E$ ist und dass jedes $A \in R$ in der Form

$$A = a_0 E + a_1 P + a_2 P^2 + a_3 P^3$$

mit rationalen a_k dargestellt werden kann $(k = 0, \ldots, 3)$.

b) Zeigen Sie, dass R ein kommutativer Teilring von $\mathrm{M}_4(\mathbb{Q})$ ist.

c) Zeigen Sie, dass R isomorph ist zu einem Produkt von drei Körpern und bestimmen Sie diese Körper.

R1.49 [Frühjahr 2001] Für ein Element r eines assoziativen Ringes R mit 1, das ein Rechtsinverses s in R besitzt, sind äquivalent:

(i) r hat mindestens zwei verschiedene Rechtsinverse in R;

(ii) r ist ein Linksnullteiler in R;

(iii) r hat kein Linksinverses in R.

2. Polynome

Werte von Polynomen

R2.1 [Frühjahr 1972] Sei $P(x) \in \mathbb{Z}[x]$ ein Polynom mit der Eigenschaft, daß es ganze Zahlen a, b gibt mit $P(a) - P(b) = q$, wobei q eine Primzahl ist. Zeigen Sie, daß $a - b$ nur einen der Werte $-q, -1, 1, q$ annehmen kann.

R2.2 [Frühjahr 1972] Sei $R(x) \in \mathbb{Z}[x]$ ein Polynom zweiten Grades, so daß vier ganze Zahlen $u_1 = 0 < u_2 < u_3 < u_4$ existieren mit $(R(u_i))^2 = 1$ für $i = 1, 2, 3, 4$.

a) Geben Sie die Zahlen u_i an und bestimmen Sie alle $R(u_i)$ für den Fall, daß $R(x)$ existiert.

b) Geben Sie $R(x)$ an.

HINWEIS: Vgl. vorige Aufgabe.

R2.3 [Frühjahr 1972] Sei $P(x) \in \mathbb{Z}[x]$ ein Polynom beliebigen Grades, für das fünf verschiedene ganze Zahlen u_i existieren, so daß $|P(u_i)| = 1$ gilt. Zeigen Sie: Entweder gilt: $P(u_i) = 1$ für alle u_i, oder es gilt: $P(u_i) = -1$ für alle u_i.

HINWEIS: Vgl. vorige Aufgaben.

R2.4 [Herbst 1978] K sei ein Körper mit unendlich vielen Elementen, F ein Element des Polynomrings $K[X_1, \ldots, X_n]$ in den Variablen $X_1, \ldots, X_n$ über K mit $n \geq 1$. Man zeige durch Induktion nach n:
Ist $F \neq 0$, so gibt es unendlich viele verschiedene $(x_1, \ldots, x_n) \in K^n$ mit $F(x_1, \ldots, x_n) \neq 0$.

R2.5 [Frühjahr 1986] K sei ein Körper und $f \in K[X]$ ein Polynom. Für ein $a \in K$ gelte $f(n \cdot 1) = a^n$ für alle ganzen Zahlen $n \geq 1$. Welche Werte kann a annehmen?

R2.6 [Frühjahr 1983] Es sei $f \in \mathbb{Q}[X]$ das Polynom

$$f = 4x^8 - 12x^7 - 5x^6 + 6x^5 - 9x^3 + 8x^2 - 15x + 4 \quad .$$

Man zeige: f hat keine Nullstelle in $\mathbb{Q}$.

R2.7 [Herbst 1972] $\mathbb{C}[X]$ sei der Ring aller Polynome in einer Unbestimmten über dem Körper $\mathbb{C}$ der komplexen Zahlen. A bezeichne die Menge der $f \in \mathbb{C}[X]$, deren Wert an allen ganzen Stellen ganzzahlig ist, also

$$A := \{f \in \mathbb{C}[X];\ f(\mathbb{Z}) \subset \mathbb{Z}\} \quad .$$

a) Man begründe, daß A ein Unterring von $\mathbb{C}[X]$ ist.

b) Man zeige, daß für jedes $m \in \mathbb{Z}$ die Menge

$$\mathfrak{p}_m := \{f \in A;\ f(m) = 0\}$$

ein Primideal in A, aber kein maximales Ideal ist; und man gebe ein „über“ $\mathfrak{p}_m$ liegendes maximales Ideal $\mathfrak{m}$ von A an (also mit $\mathfrak{p}_m \subset \mathfrak{m} \subset A$).

c) Durch die Einsetzung $X \mapsto X + 1$ in $\mathbb{C}[X]$ wird ein Automorphismus T von A definiert, und die Abbildung

$$\Delta := T - \mathrm{id}_A \quad , \qquad \text{also} \quad \Delta(f)(X) = f(X + 1) - f(X)$$

bildet einen Homomorphismus der abelschen Gruppe A in sich.

d) Man beweise für alle $f, g \in A$ die Identitäten

$$\Delta(fg) = \Delta(f)g + T(f)\Delta(g) = \Delta(f)T(g) + f\Delta(g)$$

und beschreibe den Kern von Δ.

e) Durch

$$\binom{X}{0} := 1 \quad , \qquad \binom{X}{n+1} := \binom{X}{n} \cdot \frac{X-n}{n+1} \qquad (n \geq 0)$$

werden rekursiv Polynome $\binom{X}{n} \in \mathbb{C}[X]$ definiert. Man beweise die Formel des „Pascal'schen Dreiecks"

$$\Delta\binom{X}{n+1} = \binom{X}{n} \quad , \quad n \geq 0 \quad .$$

ANLEITUNG: Die Nullstellenzahl der Differenz beider Seiten ist größer als ihr Grad.

f) Man beweise, daß stets $\binom{X}{n} \in A$ ist und folgere, daß jedes $f \in A$ eine eindeutige Darstellung der Form

$$f = \sum_{n=0}^{\infty} a_n \binom{X}{n}$$

besitzt, wo alle $a_n \in \mathbb{Z}$ und fast alle $a_n = 0$ sind.

R2.8 [Herbst 1988] Es sei M der Teilring aller derjenigen Polynome aus $\mathbb{R}[x]$, die ganzzahlige Werte für alle ganzzahligen x haben. Zeigen Sie:

a) Die additive Gruppe M^+ von M wird erzeugt von den Polynomen $1, \binom{x}{1}, \ldots, \binom{x}{n}, \ldots$ mit

$$\binom{x}{n} = \frac{1}{n!} x(x-1)\ldots(x-n+1) \quad .$$

b) Die Menge der Elemente

$$3a_0 + \sum_{n=1}^{k} a_n \binom{x}{n} \quad a_0, a_n \in \mathbb{Z}\,,\ k \in \mathbb{N}$$

ist ein Primideal von M.

R2.9 [Frühjahr 2003] Die Elemente des Restklassenkörpers $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ seien mit 0, 1, 2, 3, 4 bezeichnet. Bestimmen Sie zu dem Polynom

$$f(X) = X^7 + 2X^5 + 3X^4 + X + 4 \quad \in \mathbb{F}_5[X]$$

ein Polynom $g \in \mathbb{F}_5[X]$ vom Grad ≤ 3 mit

$$g(i) = f(i) \quad \text{für} \quad i = 1, 2, 3, 4 \quad .$$

Einheiten, Nullteiler, nilpotente Elemente im Polynomring

R2.10 [Frühjahr 1982] Begründen Sie Ihre Antwort: Wieviele Einheiten besitzt der Polynomring $R[X]$, wenn $R = \mathbb{Z}/(3)$ ist, wieviele, wenn $R = \mathbb{Z}/(4)$ ist?

R2.11 [Frühjahr 1983] Sei R ein kommutativer Ring mit Eins, $R^\times$ die Einheitengruppe von R, J der Durchschnitt aller maximalen Ideale von R und R^0 die Menge aller nilpotenten Elemente von R. Dabei heißt $x \in R$ *nilpotent*, wenn es eine natürliche Zahl $e \geq 1$ gibt mit $x^e = 0$. Zeigen Sie:

a) R^0 ist ein Ideal von R und eine Teilmenge von J.

b) $u \in R^\times$ und $x \in R^0 \implies u - x \in R^\times$.

Für die weiteren Teile ist A ein kommutativer Ring mit Eins, $R = A[x]$ und

$$f = \sum_{i=0}^{n} a_i x^i \quad .$$

Zeigen Sie:

c) $f \in R^0 \iff a_i \in A^0$ für alle $0 \leq i \leq n$.

d) $f \in R^\times \implies a_0 \in A^\times$, $a_n \in A^0$.

HINWEIS: Sei $fg = 1$ mit $g = \sum_{i=0}^{k} b_i x^i$. Zeigen Sie $a_n^{i+1} b_{k-i} = 0$.

e) $f \in R^\times \iff a_0 \in A^\times$ und $a_i \in A^0$ für alle $1 \leq i \leq n$.

f) $R^0 = J$.

HINWEIS: Zeigen Sie für $f \in J$ zuerst, daß $1 + xf \in R^\times$ ist.

Kreisteilungspolynome

R2.12 [Herbst 1997] Sei R ein Ring und $f = X^{27} - X \in R[X]$. Bestimmen Sie die Anzahl der irreduziblen Faktoren von f und ihre Grade für $R = \mathbb{C}$, $R = \mathbb{R}$, $R = \mathbb{Z}$ und $R = \mathbb{Z}/3\mathbb{Z}$.

R2.13 [Herbst 1985] Man berechne $\Phi_{45}(X) \in \mathbb{Q}[X]$, das irreduzible 45-te Kreisteilungspolynom, explizit als Polynom (Hier darf die Faktorisierung von $X^{45} - 1$ in irreduzible Polynome benutzt werden).

R2.14 [Frühjahr 1981] $\mathbb{Q}[X]$ sei der Polynomring in einer Unbestimmten X über dem Körper $\mathbb{Q}$ der rationalen Zahlen. Wieviele maximale Ideale besitzt der Restklassenring $\mathbb{Q}[X]/(X^{1981} - 1)$? (Mit Begründung).

R2.15 [Frühjahr 1991] Sei $m > 1$ eine ungerade natürliche Zahl. Man zeige:

a) $a \in \mathbb{C}$ ist genau dann eine primitive m-te Einheitswurzel, wenn $-a$ eine primitive $2m$-te Einheitswurzel ist.

b) Kreisteilungspolynome erfüllen die Identität:

$$\Phi_{2m}(X) = \Phi_m(-X) \quad .$$

R2.16 [Frühjahr 1985] Es sei p eine Primzahl und $\nu \geq 1$.
Sei $\Phi_{p^\nu}(X) = \prod (X - \zeta)$, wobei ζ alle primitiven p^ν-ten Einheitswurzeln durchläuft.

a) Man zeige:

$$\Phi_{p^\nu}(X) = \sum_{\alpha=0}^{p-1} X^{\alpha p^{\nu-1}} \quad .$$

b) Man zeige:

i) Die Summe über alle primitiven p-ten Einheitswurzeln in $\mathbb{C}$ ist -1.

ii) Die Summe über alle p^ν-ten Einheitswurzeln in $\mathbb{C}$ für $1 < \nu$ ist gleich 0.

c) Man zeige, daß $\Phi_{p^\nu}(X)$ über $\mathbb{Q}$ irreduzibel ist.

HINWEIS: Beachten Sie $\Phi_{p^\nu}(1) = p$ für alle $\nu \geq 1$.

Automorphismen von Polynomringen

R2.17 [Frühjahr 1987] $K[X]$ sei der Polynomring in einer Variablen X über einem Körper K. Bestimmen Sie alle Automorphismen von $K[X]$, die K identisch abbilden.

R2.18 [Frühjahr 1995] Sei A ein kommutativer nullteilerfreier Ring mit Eins, und sei $A[X]$ der Polynomring in einer Variablen über A.

a) Seien $a, b \in A$, und a sei eine Einheit. Zeigen Sie, daß der A-Algebra-Endomorphismus ϕ von $A[X]$ mit $\phi(X) = aX + b$ ein Automorphismus von $A[X]$ ist.

b) Zeigen Sie, daß jeder A-Algebra-Automorphismus von $A[X]$ von der in a) beschriebenen Form ist.

Restklassenringe

R2.19 [Frühjahr 1974] R sei ein kommutativer Ring mit 1 und $R[X]$ der Polynomring in einer Unbestimmten X über R. Sei $F \in R[X]$ ein Polynom der Form

$$F = X^n + r_1 X^{n-1} + \ldots + r_n \qquad (r_1, \ldots, r_n \in R)$$

mit $n > 0$ und $S := R[X]/(F)$ sei der Restklassenring von $R[X]$ nach dem von F erzeugten Hauptideal (F).

a) Zeige: Für jedes $G \in R[X]$ gibt es Polynome $Q, P \in R[X]$, wobei Grad $(P) < n$ ist, so daß $G = Q \cdot F + P$ gilt.

b) Zeige: Der kanonische Homomorphismus $\varphi: R \to S$ (der $r \in R$ auf die Restklasse von r in S abbildet) ist injektiv.

Im folgenden wird R mit seinem Bild bei φ in S identifiziert, also als Unterring von S aufgefaßt.

c) Zeige: Ist x die Restklasse von X in S, dann besitzt jedes Element $s \in S$ eine Darstellung

$$s = \rho_0 + \rho_1 x + \ldots + \rho_{n-1} x^{n-1}$$

mit eindeutig bestimmten Koeffizienten $\rho_0, \ldots, \rho_{n-1} \in R$.

d) Für ein Ideal I aus R sei IS die Menge aller $y \in S$, für die es eine natürliche Zahl $k > 0$, Elemente $i_1, \ldots, i_k \in I$ und $s_1, \ldots, s_k \in S$ gibt, so daß $y = \sum_{\nu=1}^{k} i_\nu s_\nu$ gilt.
Zeige, daß IS ein Ideal von S ist.

e) Zeige: Ist $1 \in IS$, dann hat man in S eine Gleichung

$$1 = i_0 + i_1 x + \ldots + i_{n-1} x^{n-1} \quad \text{mit} \quad i_0, \ldots, i_{n-1} \in I \quad .$$

Folgere, daß für $I \neq R$ auch $IS \neq S$ ist.

f) Zeige: Ist S ein Körper, dann ist auch R ein Körper.

g) Zeige: Ist I ein maximales Ideal von R, dann ist $IS \cap R = I$.

h) Zeige: Zu jedem maximalem Ideal I von R gibt es mindestens ein und höchstens endlich viele maximale Ideale J von S mit $J \cap R = I$.

R2.20 [Herbst 1990] Sei $\mathbb{F}_4$ der Körper mit 4 Elementen und sei

$$R := \mathbb{F}_4[X]/(X^5 - X^2) \quad .$$

a) Wie viele Elemente besitzt R?

b) Wie viele Primideale gibt es in R?

c) Wie viele Einheiten besitzt R?

d) Wie viele Nullteiler besitzt R?

R2.21 [Herbst 1997] Sei $f = X^3 - 9X + 3 \in \mathbb{Q}[X]$.

a) Zeigen Sie, daß $K = \mathbb{Q}[X]/(f)$ ein Körper ist.

b) Bestimmen Sie die Anzahl der Körperhomomorphismen $K \to \mathbb{R}$ von K in die reellen Zahlen.

R2.22 [Herbst 1986] Es soll die Struktur des Rings $R := \mathbb{Q}[X]/((X^2+1)^2)$ untersucht werden. Zeigen Sie:

a) Es gibt ein Polynom $g \in \mathbb{Q}(i)[X]$ mit $g(i) = i$, $g'(i) = 0$ und $g(-i) = g'(-i) = 0$, wobei g' die Ableitung von g bezeichnet.

b) Mit einem g wie in a) sei $h := g + \bar{g}$, wobei $\bar{g}$ das Polynom ist, das aus g durch Konjugation der Koeffizienten entsteht. Dann ist $h \in \mathbb{Q}[X]$ und $h - i$ wird in $\mathbb{Q}(i)[X]$ von $(X-i)^2$ geteilt.

c) $h^2 + 1$ ist in $\mathbb{Q}[X]$ ein Vielfaches von $(X^2+1)^2$.

d) Sei ξ die Restklasse von X in R und $k := \mathbb{Q}[h(\xi)] \subset R$. Dann ist k ein zu $\mathbb{Q}(i)$ isomorpher Körper.

HINWEIS: Betrachten Sie den Kern des Homomorphismus $\mathbb{Q}[Y] \to \mathbb{Q}[h(\xi)]$ mit $Y \mapsto h(\xi)$.

e) $\{1, \xi^2 + 1\}$ ist eine Basis von R als k-Vektorraum.

R2.23 [Frühjahr 1992] Sei K ein Körper, und es bezeichne $\mathfrak{a}_b$ für $b \in K$ den Kern des Homomorphismus

$$\varphi_b : \ K[X] \to K \quad ,$$

der durch $f(X) \mapsto f(b)$ gegeben ist. Man zeige:

a) Für $b_1, b_2 \in K$, $b_1 \neq b_2$, sind $\mathfrak{a}_{b_1}, \mathfrak{a}_{b_2}$ teilerfremde Ideale in $K[X]$.

b) Zu $a_1, \ldots, a_n \in K$ und paarweise verschiedenen $b_1, \ldots, b_n \in K$ gibt es ein $g(X) \in K[X]$ mit $g(b_i) = a_i$, $i = 1, \ldots, n$.

R2.24 [Herbst 1997] Sei $f = X^4 + aX + 2 \in \mathbb{Z}[X]$. 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. Für welche a treten die jeweiligen Fälle ein?

R2.25 [Herbst 1998] Im Ring $\mathrm{M}_3(\mathbb{Q})$ der dreireihigen Matrizen über $\mathbb{Q}$ sei R der von der Einheitsmatrix E und von der Matrix

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 3 & -6 & 18 \\ 1 & -2 & 6 \end{pmatrix}$$

erzeugte Unterring.

a) Ist R isomorph zu einem direkten Produkt von Körpern? Die Antwort ist zu begründen.

HINWEIS: Fassen Sie R als Faktorring eines Polynomringes auf.

b) Geben Sie alle $X \in R$ mit $X^2 = X$ und alle $Y \in R$ mit $Y^2 = 0$ an.

Euklidischer Algorithmus

R2.26 [Herbst 1978] K sei algebraisch abgeschlossener Körper und $F \in K[X_1, \ldots, X_n]$ ein Polynom mit $n \geq 1$. Man zeige:

a) Es sei $n \geq 2$. Ist F in X_n von positivem Grad und $D \in K[X_1, \ldots, X_{n-1}]$ ein nicht verschwindendes Polynom, so gibt es unendlich viele verschiedene $(x_1, \ldots, x_n) \in K^n$ mit $D(x_1, \ldots, x_{n-1}) \neq 0$, $F(x_1, \ldots, x_n) = 0$.

b) F sei irreduzibel und in X_n von positivem Grad, $G \in K[X_1, \ldots, X_n]$ ein weiteres Polynom. Ist F kein Teiler von G, dann gibt es Polynome $A, B \in K[X_1, \ldots, X_n]$ und $D \in K[X_1, \ldots, X_{n-1}]$, $D \neq 0$, so daß

$$D = AF + BG \quad .$$

(Für den Beweis dieser Aussage darf verwendet werden, daß die Polynome F und G als Elemente von $K(X_1, \ldots, X_{n-1})[X_n]$ teilerfremd sind, wobei $K(X_1, \ldots, X_{n-1})$ der Quotientenkörper von $K[X_1, \ldots, X_{n-1}]$ ist).

c) F sei irreduzibel, $G \in K[X_1, \ldots, X_n]$ ein weiteres Polynom. Für alle $(x_1, \ldots, x_n) \in K^n$ mit $F(x_1, \ldots, x_n) = 0$ gelte auch $G(x_1, \ldots, x_n) = 0$. Dann ist F ein Teiler von G.
(Zum Beweis verwende man b) und a)).

R2.27 [Herbst 1978] K sei ein beliebiger Körper, $F, G \in K[X_1, X_2]$ seien zwei teilerfremde Polynome. Man beweise, daß es nur endlich viele $(x_1, x_2) \in K^2$ geben kann mit

$$F(x_1, x_2) = G(x_1, x_2) = 0 \quad .$$

Zum Beweis dieser Aussage zeige man zuerst, daß es genügt, die Behauptung nachzuweisen, wenn

i) K algebraisch abgeschlossen und

ii) F irreduzibel

ist. Man verwende sodann die Aussage von Teil b) der vorigen Aufgabe.

R2.28 [Herbst 1989] Sei K ein Körper der Charakteristik Null. Sei $f(X) \in K[X]$ vom Grad ≥ 1. Sei L eine Erweiterung von K, in der $f(X)$ zerfällt:

$$f(X) = c(X - a_1)^{k_1} \ldots (X - a_n)^{k_n}$$

mit $a_j \in L$, $k_j \in \mathbb{N}$ und $a_i \neq a_j$ für $i \neq j$.
Man beweise: $(X - a_1) \ldots (X - a_n) \in K[X]$.

R2.29 [Herbst 1989] Seien

$$f := X^3 + 2X^2 - X - 1$$
$$g := X^2 + X - 3$$

Polynome in $\mathbb{Q}[X]$.

a) Man zeige, daß f, g in keinem Erweiterungskörper von $\mathbb{Q}$ eine gemeinsame Nullstelle besitzen.

b) Man zeige, daß es Polynome $a, b \in \mathbb{Q}[X]$ gibt mit

$$af + bg = 1 \quad ;$$

man gebe a, b explizit an.

Polynome in mehreren Variablen

R2.30 [Herbst 1972] Es sei $\mathbb{Q}$ der Körper der rationalen Zahlen, $f(x,y)$ ein gegebenes über $\mathbb{Q}$ unzerlegbares Polynom dritten Grades, $P(x_0,y_0)$ ein *rationaler*, nicht singulärer Punkt der Kurve $f(x,y)=0$ der reellen affinen Ebene. Man zeige durch Taylorentwicklung von $f(x,y)$, daß die Tangente der Kurve in P diese entweder nicht mehr, oder noch in einem weiteren rationalen Punkte trifft!

R2.31 [Herbst 1972] Gegeben sei das Polynom

$$g(x,y) := x^3 + xy^2 - 2y^3 \quad .$$

a) Man ermittle seine Zerlegung in über $\mathbb{Q}$ unzerlegbare Faktoren. Mit Hilfe derselben beweise man, daß die Kurve $f(x,y) :\equiv g(x,y) - 8 = 0$ genau zwei *ganzzahlige* Punkte besitzt; diese haben gemeinsame Abszisse x_0 und einer von ihnen liegt auf der Tangente des anderen.

b) Wie ist die Riemannsche Fläche der durch $f(x,y)=0$ über der komplexen Zahlenebene definierten algebraischen Funktion $y=y(x)$ über einer Umgebung von x_0 gestaltet? Skizze hierfür und für den Gesamtverlauf der Kurve $f(x,y)=0$ im reellen!

R2.32 [Frühjahr 1975] Sei k ein Körper und $K = k(x_{ij}\,;\ i,j = 1,\ldots,n)$ die n^2-fache transzendente Erweiterung von k. Man zeige, daß die Determinante der Matrix (x_{ij}) in K nicht verschwindet.

R2.33 [Frühjahr 1982]

a) Man gebe den größten gemeinsamen Teiler von

$$f := X^3 + 2X^2 - 2X - 1 \quad \text{und} \quad g := X^2 + X - 2$$

in $\mathbb{Q}[X]$ an. Außerdem untersuche man, ob das von f und g in $\mathbb{Q}[X]$ erzeugte Ideal Hauptideal, prim, maximal ist.

b) Man zeige, daß der Ringhomomorphismus

$$\mathbb{Q}[X,Y] \to \mathbb{Q}[X] \qquad (h(X,Y) \mapsto h(X,0))$$

surjektiv ist und gebe ein Primideal $\neq (0)$ in $\mathbb{Q}[X,Y]$ an, das nicht maximal ist. Warum ist $\mathbb{Q}[X,Y]$ kein Hauptidealring?

R2.34 [Frühjahr 1982] a,b und c seien die drei komplexen Nullstellen des Polynoms $X^3+10X^2-20X+30$. Ohne Berechnung von a,b,c bestimme man die Zahl $a^2b^2c + ab^2c^2 + a^2bc^2$.

R2.35 [Frühjahr 1990] Seien p und q aus $\mathbb{N}$ teilerfremd, und U,V und W Unbestimmte. Wir wollen einsehen, daß die Ringe

$$R = \mathbb{Z}[U,V]/(U^p-1,\ V^q-1) = \mathbb{Z}[u,v] \quad \text{und} \quad S = \mathbb{Z}[W]/(W^{pq}-1) = \mathbb{Z}[w]$$

isomorph sind. Hierbei bezeichnen u,v und w die Restklassen von U,V und W. Dazu betrachten wir den Einsetzungshomomorphismus

$$\phi :\ \mathbb{Z}[U,V] \to \mathbb{Z}[W] \quad (U \mapsto W^q\,,\ V \mapsto W^p) \quad .$$

Zeigen Sie:

a) ϕ induziert einen Homomorphismus $\varphi :\ R \to S$ mit $\varphi(u) = w^q$ und $\varphi(v) = w^p$.

b) Die additive Gruppe $(S,+)$ von S ist frei vom Rang pq und $(R,+)$ wird von pq Elementen erzeugt.

c) $w \in \operatorname{Bild}\varphi$.

d) φ ist ein Isomorphismus.

R2.36 [Herbst 1993] Sei K ein algebraisch abgeschlossener Körper und $p(X,Y) \in K[X,Y]$ ein homogenes, nicht-konstantes Polynom. Zeigen Sie: Es gibt $a_1, \ldots, a_n, b_1, \ldots, b_n \in K$, so daß

$$p(X,Y) = (a_1X + b_1Y) \cdot \ldots \cdot (a_nX + b_nY) \quad .$$

3. Irreduzibilität von Polynomen

Polynome über verschiedenen Körpern

R3.1 [Frühjahr 1991] Man formuliere drei wesentlich verschiedene Kriterien für die Irreduzibilität von Polynomen.

R3.2 [Frühjahr 1982] Bestimmen Sie alle über $\mathbb{R}$ irreduziblen Polynome in einer Variablen.

R3.3 [Herbst 1989]

a) Man untersuche

$$f := X^3 - 5X^2 + 25X + 10$$

auf Irreduzibilität in den Ringen $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ und $\mathbb{C}[X]$.

b) Man entscheide (mit Begründung), ob folgende Polynome separabel sind:

1) $X^9 + X^7 + 8X^4 + 5X^3 + 1 \in \mathbb{Q}[X]$,

2) $X^9 + X^6 + X^3 + 1 \in \mathbb{F}_3[X]$.

R3.4 [Herbst 1980] Sei $K = \mathbb{Q}(\sqrt{2})$. Zeigen Sie, daß $X^3 - 3$ irreduzibel ist im Polynomring $K[X]$.

R3.5 [Herbst 1982] Beweisen Sie, daß es keine Polynome $P(X)$ und $Q(X)$ in $\mathbb{Z}[X]$ gibt, welche der folgenden Gleichung genügen:

$$P(X)^3 - P(X) + 2 = (X^4 - 7) \cdot Q(X) \quad .$$

R3.6 [Herbst 1980] Sei K ein Körper der Charakteristik $\neq 2$ und a ein Element von K, das kein Quadrat in K ist.

a) Sei c ein Element eines Erweiterungskörpers von K mit $c^2 = a$. Man zeige: c ist genau dann Quadrat in $K(c)$, wenn $-4a$ eine vierte Potenz in K ist.

b) Zeige: $X^4 - a$ ist genau dann irreduzibel über K, wenn $-4a$ keine vierte Potenz in K ist.

HINWEIS: Sei b eine Nullstelle von $X^4 - a$ in einem Erweiterungskörper von K. Man betrachte $K \subset K(b^2) \subset K(b)$ und wende a) mit $x = b^2$ an.

c) Sei K ein Körper mit 5 Elementen. Man zeige: Jeder Zerfällungskörper von $X^4 - 3$ über K hat 625 Elemente.

R3.7 [Herbst 1990] Sei K ein Körper und $a \in K$ kein Quadrat in K. Sei β eine Wurzel von $X^4 - a$ und $\alpha := \beta^2$.

Man zeige:

a) Das Polynom $X^4 - a \in K[X]$ ist genau dann irreduzibel, wenn α kein Quadrat in $K(\alpha)$ ist.

b) Es ist α genau dann ein Quadrat in $K(\alpha)$, wenn $\operatorname{char} K \neq 2$ ist und $x^4 + 4a$ eine Nullstelle in K hat.

R3.8 [Herbst 1978] Es sei das Polynom $P(x) = x^4 - 40x^2 + 36$ gegeben.

a) Zeigen Sie: Ist $z \neq 0$ eine Nullstelle von $P(x)$, so sind die anderen Nullstellen $-z$, $6z^{-1}$ und $-6z^{-1}$ (unabhängig von dem Körper K, über dem $P(x)$ betrachtet wird).

b) Zeigen Sie: Ist $P(x)$ über einem Körper K reduzibel, so hat $P(x) \in K[x]$ einen Teiler der Form $x^2 - u$, $x^2 + kx + 6$ oder $x^2 + rx - 6$ aus $K[x]$.

c) Bestimmen Sie für jede der in b) angegebenen Formen eines Teilers $R(x)$ von $P(x)$ dasjenige Polynom $S(x)$ aus $K[x]$ für das $R(x)S(x) = P(x)$ gilt, und geben Sie Bedingungen dafür an, daß eine Zerlegung der angegebenen Art möglich ist.

d) Zeigen Sie, daß $P(x)$ über jedem endlichen Primkörper zerlegbar ist.

HINWEIS: Dies ist gleichwertig mit der Aussage, daß wenigstens eine der drei in c) entwickelten Bedingungen erfüllt wird.

e) Zeigen Sie, daß $P(x)$ irreduzibel über $\mathbb{Q}$ ist.

R3.9 [Frühjahr 1992]

a) Sei K ein Körper, a ein Element von K, und seien m und n zwei natürliche Zahlen $\neq 0$, die relativ prim zueinander sind. Zeigen Sie, daß das Polynom $X^{mn} - a$ genau dann irreduzibel über K ist, wenn die Polynome $g_m(X) = X^m - a$ und $g_n(X) = X^n - a$ irreduzibel über K sind.

b) Sei p eine Primzahl, und sei a ein Element in K, das in K keine p-te Wurzel besitzt. Zeigen Sie, daß $X^p - a = g_p(X)$ irreduzibel über K ist.

R3.10 [Herbst 1998] Sei p eine Primzahl.

a) Zeigen Sie, dass das Polynom $f = X^p - X - 1$ irreduzibel über dem endlichen Körper $\mathbb{F}_p$ ist.

b) Ist f auch irreduzibel über $\mathbb{Z}$? Die Antwort ist zu begründen.

R3.11 [Frühjahr 1998] Es sei $f(X) \in \mathbb{Q}[X]$ irreduzibel und von ungeradem Grad m. Sei w eine primitive 17te Einheitswurzel. Zeigen Sie, daß $f(X)$ über $\mathbb{Q}(w)$ irreduzibel ist.

Polynome über Q

R3.12 [Frühjahr 1972] Sei ein Polynom $P(x) \in \mathbb{Z}[x]$ vom Grad $2k+1$ gegeben mit der Eigenschaft, daß es $2k+1$ verschiedene ganze Zahlen u_i gibt mit $P(u_i) = 1$ für alle diese u_i. Zeigen Sie, daß $P(x)$ irreduzibel ist.

HINWEIS: Benutze Aufgabe R2.1.

R3.13 [Frühjahr 1972] Sei $P(x) \in \mathbb{Z}[x]$ ein Polynom vom Grad $2k$ mit $2k$ verschiedenen ganzen Zahlen u_i, so daß $P(u_i) = 1$ für alle diese u_i gilt. Zeigen Sie:

a) Ist $P(x)$ reduzibel, so ist $P(x)$ ein Quadrat.

b) $P(x)$ ist irreduzibel für $k \geq 3$.

HINWEIS: Vgl. vorige Aufgabe.

R3.14 [Frühjahr 1972] Sei $P(x) \in \mathbb{Z}[x]$ ein Polynom vom Grade $n > 7$, und seien $k > \frac{n}{2}$ verschiedene ganze Zahlen u_i gegeben, sodaß $|P(u_i)| = 1$ für alle u_i. Zeigen Sie, daß $P(x)$ irreduzibel ist.

HINWEIS: Vgl. vorige Aufgabe.

R3.15 [Frühjahr 1997] Bestimmen Sie alle ganzen Zahlen a, für die das Polynom $f_a(X) = 4X^2 + 4X + a$ in $\mathbb{Z}[X]$ bzw. in $\mathbb{Q}[X]$ irreduzibel ist.

R3.16 [Herbst 1998] Ist das Polynom

$$3X^3 - 6X^2 + \frac{3}{2}X - \frac{3}{5}$$

in $\mathbb{Q}[X]$ irreduzibel?

R3.17 [Frühjahr 1976] Für welche ganzen Zahlen n ist das Polynom $f = X^3 + X^2 + nX + 2$ irreduzibel über $\mathbb{Q}$?

R3.18 [Frühjahr 1972] Sei n eine natürliche Zahl > 1 und $j : \mathbb{Z} \to \mathbb{Z}/(n)$ der kanonische Epimorphismus, sowie $\mathbb{Z}[X]$ (bzw. $(\mathbb{Z}/(n))[X]$) der Ring der Polynome mit Koeffizienten aus $\mathbb{Z}$ (bzw. $\mathbb{Z}/(n)$) in der Unbestimmten X. Ferner sei $j_* : \mathbb{Z}[X] \to (\mathbb{Z}/(n))[X]$ die durch $j_*|\mathbb{Z} = j$ eindeutig bestimmte Fortsetzung von j mit $j_*X = X$ (hierbei bezeichnet $j_*|\mathbb{Z}$ die Beschränkung von j_* auf den zu $\mathbb{Z}$ isomorphen Unterring der Polynome nullten Grades aus $\mathbb{Z}[X]$).

a) Für $f := \sum_k a_k X^k \in \mathbb{Z}[X]$ schreibe man $j_*(f)$ als Element von $(\mathbb{Z}/(n))[X]$.

b) Es habe $f \in \mathbb{Z}[X]$ den höchsten Koeffizienten 1, und es sei $j_*(f)$ irreduzibel in $(\mathbb{Z}/(n))[X]$, sowie Grad $j_*(f) > 1$. Man zeige: f ist irreduzibel in $\mathbb{Z}[X]$.

c) Man belege durch ein Beispiel (etwa eines Polynoms vom Grade 2), daß die Umkehrung der Aussage unter b) nicht gilt.

R3.19 [Herbst 1984]

a) Zeigen Sie, daß $f := X^3 + 2X^2 + 3X + 3$ in $\mathbb{Q}[X]$ irreduzibel ist!

b) Schreiben Sie 1 als Linearkombination von f und $g := X^2 + X + 1$ mit Koeffizienten aus $\mathbb{Q}[X]$.

R3.20 [Frühjahr 1973]

a) Zeigen Sie: Das Polynom $x^4 - 10x^2 + 1$ hat die Nullstelle $\sqrt{2} + \sqrt{3}$ und ist irreduzibel über den rationalen Zahlen.

b) Zeigen Sie, daß $x^4 - 10x^2 + 1$ über jedem endlichen Primkörper in zwei (nicht unbedingt irreduzible) Faktoren des Grades 2 zerfällt.

HINWEIS: Man bemerke, daß das Produkt zweier Nichtquadrate in einem endlichen Körper ein Quadrat ist.

R3.21 [Herbst 1990] Beweisen Sie, daß folgende Polynome über $\mathbb{Q}$ irreduzibel sind:

$$f = X^4 - 4X^3 + 2$$
$$g = X^2 + 4X + 7$$
$$h = X^3 - 38X^2 - 5X + 719 \quad .$$

R3.22 [Herbst 1994] Sind folgende Polynome reduzibel oder irreduzibel in $\mathbb{Q}[X]$?

a) $x^3 - 5x^2 + 2x + 1$

b) $x^4 - 4x^3 + 6x^2 - 4x + 4$

R3.23 [Frühjahr 1975] Ist das Polynom

$$6x^4 - 25x^3 + 15x^2 + 10x - 2$$

irreduzibel im Polynomring $\mathbb{Q}[x]$ über den rationalen Zahlen?

R3.24 [Herbst 1979] Für welche ganze Zahlen n ist das Polynom $f = X^4 + nX + 1$ irreduzibel über $\mathbb{Q}$?

R3.25 [Frühjahr 1998] Man beweise, daß die Polynome

a) $X^4 + 1$

b) $X^4 + X + 1$

c) $X^4 + X^3 + X^2 + 1$

über $\mathbb{Q}$ irreduzibel sind.

R3.26 [Herbst 1981] Zeigen Sie die Irreduzibilität des Polynoms $g = x^4 - 3$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen.

R3.27 [Herbst 1981] Für welche $n \in \mathbb{Z}$ ist das Polynom $X^4 + nX^3 + X^2 + X + 1$ über $\mathbb{Q}$ reduzibel?

R3.28 [Frühjahr 2002] Sei $f(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ ein Polynom mit ganzzahligen Koeffizienten. Seien alle a_i ungerade. Man zeige, dass $f(X)$ irreduzibel über $\mathbb{Q}$ ist.

R3.29 [Herbst 1980] Es sei $P(a, X) = X^4 + aX^2 + X + 1$, wobei a ein ganzzahliger Parameter ist.

a) Für welche Werte des Parameters a hat $P(a, X)$ lineare Faktoren in $\mathbb{Q}[X]$ und welche linearen Faktoren treten auf?

b) Zeigen Sie: $P(a, X)$ zerfällt in $\mathbb{Q}[X]$ niemals in zwei Faktoren des Grades 2.

R3.30 [Frühjahr 1987] Gegeben sei das Polynom $f := X^4 - aX - 1 \in \mathbb{Z}[X]$, wobei $a \neq 0$ ist. Sei $\alpha \in \mathbb{C}$ eine Nullstelle von f und $K := \mathbb{Q}(\alpha)$.

a) Zeigen Sie, daß f das Minimalpolynom von α über $\mathbb{Q}$ ist.

b) Sei L ein Körper mit $\mathbb{Q} \subsetneq L \subsetneq K$. Bekanntlich ist L von der Form $\mathbb{Q}(\sqrt{d})$ mit einer quadratfreien ganzen Zahl $d \neq 0, 1$, und für den einzigen nichttrivialen Automorphismus σ von L gilt $\sigma(\sqrt{d}) = -\sqrt{d}$. Sei $g := X^2 + uX + v \in L[X]$ das Minimalpolynom von α über L. Beweisen Sie: Es gilt

$$f = (X^2 + uX + v)(X^2 + \sigma(u)X + \sigma(v)) \quad , \quad u = r\sqrt{d} \quad \text{mit} \quad r \in \mathbb{Q}$$

und $a^2 = (r^4d^2 + 4)r^2d$.

c) Zeigen Sie, daß r eine ganze Zahl ist.

d) Folgern Sie aus b) und c): Ist a eine Primzahl, so gibt es keinen Zwischenkörper L mit $\mathbb{Q} \subsetneq L \subsetneq K$.

R3.31 [Herbst 2001]

a) Zeigen Sie: Es gibt kein Polynom $P(x) \in \mathbb{Z}[x]$ so dass $P(7) = 5$ und $P(9) = 4$ gilt.

b) Zeigen Sie für $a, b \geq 3$, $a, b \in \mathbb{Z}$:
$x(x-3)(x-a)(x-b) + 1$ ist irreduzibel in $\mathbb{Z}[x]$.

R3.32 [Herbst 1973] Man untersuche, ob das Polynom

$$f(x) = x^5 - 5x^4 - 6x - 1$$

über dem Körper $\mathbb{Q}$ der rationalen Zahlen irreduzibel ist.

ANLEITUNG: Betrachte $f(x)$ mod p für eine geeignete Primzahl p.

R3.33 [Frühjahr 1984] Geben Sie je ein irreduzibles Polynom 5. Grades aus $\mathbb{Q}[X]$ an, welches

a) genau eine reelle Nullstelle besitzt,

b) genau drei verschiedene reelle Nullstellen besitzt!

(Mit Begründung!)

R3.34 [Herbst 2003] Zeigen Sie die Irreduzibilität der folgenden Polynome f über $\mathbb{Z}$:

a) $f = X^p + pX - 1$ für jede Primzahl p

b) $f = X^4 - 42X^2 + 1$

Polynome in mehreren Variablen

R3.35 [Herbst 1999]

a) Seien R ein Integritätsring und $a \in R$. Man zeige: Das Polynom $X^2 + a$ ist genau dann reduzibel in $R[X]$, wenn $-a$ ein Quadrat in R ist.

b) Sei K ein Körper, der nicht die Charakteristik 2 besitzt. Man zeige: Für alle $n \in \mathbb{N}$, $n \geq 3$, ist das Polynom $X_1^2 + X_2^2 + \ldots + X_n^2$ im Polynomring $K[X_1, \ldots, X_n]$ irreduzibel.

R3.36 [Frühjahr 1982] Es sei K ein Körper der Charakteristik $\neq 2$ und X, Y, Z seien unabhängige Unbestimmte über K. Zeigen Sie mit Hilfe des Eisensteinkriteriums:

a) $X^2 + Y^2 - 1$ ist über dem Körper $K(X)$ irreduzibel.

b) $X^2 + Y^2 + Z^2 - 1$ ist über dem Körper $K(X, Y)$ irreduzibel.

Zitieren Sie sorgfältig die in Ihren Beweisen benützten Sätze.

R3.37 [Frühjahr 1977] Gegeben sei das Polynom $f(X, Y) = X^2 + Y^2 - 3 \in \mathbb{Q}[X, Y]$. Man beweise:

a) f besitzt keine Nullstelle in $\mathbb{Q} \times \mathbb{Q}$ (man nehme das Gegenteil an und rechne modulo 3).

b) f ist ein irreduzibles Element von $\mathbb{Q}[X, Y]$.

R3.38 [Herbst 1987] Gegeben sind das Polynom $f(X, Y) := Y^3 + X^2Y + 3Y^2 + X^2 + 3Y + X + 1 \in \mathbb{Z}[X, Y]$ und eine Primzahl p. Zeigen Sie:

a) $f(X, Y)$ ist irreduzibel in $\mathbb{Z}[X, Y]$.

b) $f(p, Y)$ ist irreduzibel in $\mathbb{Q}[Y]$.

c) Faßt man $f(p, Y)$ als Polynom in $\mathbb{F}_3[Y]$ auf, dann ist $f(p, Y)$ reduzibel.

R3.39 [Herbst 1980] Sei f eines der folgenden Polynome aus $\mathbb{Q}[X, Y]$:

a) $X - Y$,

b) $Y^3 + X^2 + 2$,

c) $X^3 - Y^3$,

d) $Y^4 + (X + 1)^2Y^2 + X^2 - 1$.

In welchen Fällen ist f irreduzibel in $\mathbb{Q}[X, Y]$? (Eisenstein!).

R3.40 [Frühjahr 2003] Sei $K = \mathbb{Q}(X)$ der Körper der rationalen Funktionen in einer Unbestimmten über $\mathbb{Q}$, und sei f das Polynom

$$f(Y) = 1 + XY + (XY)^2 + (XY)^3 + (XY)^4 + (XY)^5 + (XY)^6$$

in $K[Y]$. Ist f irreduzibel in dem Ring $K[Y]$?

R3.41 [Frühjahr 1996] Man betrachte das Polynom $f = X^7 + X - Y$ im Polynomring $\mathbb{Q}[X, Y]$.

a) Zeigen Sie: Der Ring $R := \mathbb{Q}[X, Y]/(f)$ ist ein Integritätsring, wobei (f) das von f erzeugte Ideal ist.

b) Zeigen Sie: Durch $\varphi(X) = X + (f)$ ist ein injektiver $\mathbb{Q}$-Homomorphismus $\varphi : \mathbb{Q}[X] \to R$ gegeben.

c) Ist der Quotientenkörper $\mathrm{Quot}(R)$ von R eine algebraische Erweiterung von $\mathbb{Q}$? (Begründen Sie Ihre Antwort).

R3.42 [Frühjahr 1978] Sei K ein Körper.

a) Man zeige, daß für jedes Polynom $f(X) \in K[X]$ von ungeradem Grad das Polynom $Y^2 + f(X)$ in $K[X, Y]$ irreduzibel ist.

b) Seien f und g teilerfremde homogene Polynome aus $K[X_1, X_2, \ldots, X_n]$ und sei $\operatorname{grad} g = 1 + \operatorname{grad} f$. Man zeige, daß $f + g$ irreduzibel ist.

R3.43 [Frühjahr 1984] Zeigen Sie, daß das Polynom $Z^n + Y^3 + X^2$ für alle ganzen Zahlen $n \geq 1$ irreduzibel in $\mathbb{C}[X, Y, Z]$ ist!

R3.44 [Herbst 2000] Seien a, b, c positive natürliche Zahlen. Man zeige:

a) Das Polynom $X^a + Y^b$ ist im Polynomring $\mathbb{C}[X, Y]$ durch kein Quadrat eines Primpolynoms teilbar.

b) Das Polynom $X^a + Y^b + Z^c$ ist irreduzibel in $\mathbb{C}[X, Y, Z]$.

R3.45 [Herbst 2000] Sei P der Polynomring über $\mathbb{Q}$ in den Unbestimmten X, Y und Z, und sei

$$f = X^a + Y^b \cdot Z^c \in P$$

mit positiven, teilerfremden, ganzen Zahlen a, b, c.
Zeigen Sie:

a) Es gibt ganze Zahlen α, β und γ, so dass

$$2^{\alpha a} \cdot f\big(2^{-\alpha} \cdot X,\ 2^{\beta} \cdot Y,\ 2^{\gamma} \cdot Z\big) = X^a + 2Y^b \cdot Z^c \quad .$$

b) f ist in P irreduzibel.

4. Idealtheorie

Rechnen mit Idealen

R4.1 [Herbst 1974] R sei ein kommutativer Ring. Für ein Ideal $\mathfrak{a}$ von R sei

$$\mathfrak{r}(\mathfrak{a}) := \{x \in R;\ \text{Zu } x \text{ gibt es } n \in \mathbb{N} \text{ mit } x^n \in \mathfrak{a}\} \quad .$$

Ferner sei

$$\mathfrak{N}(R) := \mathfrak{r}((0)) = \{x \in R;\ \text{zu } x \text{ gibt es } n \in \mathbb{N} \text{ mit } x^n = 0\} \quad .$$

Man zeige:

a) $\mathfrak{r}(\mathfrak{a})$ ist ein Ideal von R mit $\mathfrak{a} \subseteq \mathfrak{r}(\mathfrak{a})$.

b) $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$.

c) Ist $\mathfrak{p}$ ein Primideal, so gilt $\mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$.

d) Für den Faktorring $R/\mathfrak{a}$ von R nach einem Ideal $\mathfrak{a}$ von R gilt

$$\mathfrak{N}(R/\mathfrak{a}) = \mathfrak{r}(\mathfrak{a})/\mathfrak{a} \quad .$$

e) Nun sei $R = \mathbb{Z}$ der Ring der ganzen Zahlen, $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ ein Element aus $\mathbb{N}$ in seiner kanonischen Primfaktorisierung, (n) das von n erzeugte Ideal in $\mathbb{Z}$. Man gebe ein erzeugendes Element von $\mathfrak{r}((n))$ an.

f) Man zeige $\mathfrak{N}(\mathbb{Z}/(96)) \simeq \mathbb{Z}/(16)$ (Isomorphie von $\mathbb{Z}$-Moduln).

R4.2 [Frühjahr 1996] Es sei I die Menge aller Polynome $f \in \mathbb{Q}[X]$ mit $f(0) = f'(0) = 0$.

a) Zeigen Sie, daß I ein Ideal von $\mathbb{Q}[X]$ ist.

b) Geben Sie ein erzeugendes Element für das Ideal I an.

c) Ist I ein Primideal?

R4.3 [Frühjahr 1992] Sei R ein kommutativer Ring.

a) Wie ist das Produkt zweier Ideale in R definiert?

b) Es sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5};\ a, b \in \mathbb{Z}\}$. Es sei P das von 3 und $1 + \sqrt{-5}$ erzeugte Ideal und Q das von 3 und $1 - \sqrt{-5}$ erzeugte Ideal in R.
Berechnen Sie PQ, und bestimmen Sie die Anzahl der Elemente sowie die Anzahl der Einheiten des Restklassenringes R/PQ.

Idealtheorie in $\mathbb{Z}[X]$

R4.4 [Herbst 1975] Sei p eine Primzahl. $\mathbb{F}_p$ sei der endliche Körper $\mathbb{F}_p = \mathbb{Z}/(p)$. Für ein Polynom $f \in \mathbb{Z}[X]$ bezeichnen (p, f) das von p und f in $\mathbb{Z}[X]$ erzeugte Ideal und $\bar{f}$ das kanonische Bild von f in $\mathbb{F}_p[X]$.

a) i. Zeige: Die kanonische Abbildung $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ induziert einen Ringisomorphismus

$$\mathbb{Z}[X]/p\mathbb{Z}[X] \simeq \mathbb{F}_p[X] \quad .$$

ii. Für $f \in \mathbb{Z}[X]$ sei $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]/(\bar{f})$ der durch $\varphi(X) = X + (\bar{f})$ definierte Ringhomomorphismus. Zeige: $\mathrm{Kern}(\varphi) = (p, f)$.

iii. Sei $f \in \mathbb{Z}[X]$. Zeige: (p, f) ist genau dann maximales Ideal in $\mathbb{Z}[X]$, wenn $\bar{f}$ irreduzibles Polynom in $\mathbb{F}_p[X]$ ist.

b) Sei M ein Ideal in $\mathbb{Z}[X]$ mit $p \in M$.
Zeige: Es gibt $f \in \mathbb{Z}[X]$ mit $M = (p, f)$.

HINWEIS: Es gibt einen Ringhomomorphismus

$$\psi : \mathbb{F}_p[X] \to \mathbb{Z}[X]/M \quad \text{mit} \quad \psi(X) = X + M \quad .$$

Verwende a)ii.

c) Zeige: In $\mathbb{F}_p[X]$ gibt es unendlich viele irreduzible Polynome.

d) Seien K ein Körper der Charakteristik 0 und $\alpha \in K$.
Zeige: $K \neq \mathbb{Z}[\alpha]$, wobei $\mathbb{Z}[\alpha]$ den von α in K erzeugten Unterring bezeichnet.

HINWEIS: Aus der Annahme $K = \mathbb{Z}[\alpha]$ folgt:

i. α ist algebraisch über $\mathbb{Q}$ (identifiziere $\mathbb{Q}$ mit einem Unterkörper von K).

ii. Sei

$$F = X^n + \frac{1}{r}\sum_{i=0}^{n-1} r_i X^i \quad , \quad 0 \neq r \in \mathbb{Z} \quad , \quad r_i \in \mathbb{Z} \quad , \quad 0 \leq i \leq n-1$$

das Minimalpolynom von α über $\mathbb{Q}$ (nach i. existiert F). Für $m \geq n$ gibt es $s_i \in \mathbb{Z}$ für $0 \leq i \leq n-1$ mit

$$\alpha^m = \frac{1}{r^{m+1-n}} \sum_{i=0}^{n-1} s_i \alpha^i \quad .$$

iii. Für alle Primzahlen q gilt $\frac{1}{q} \in \mathbb{Z}[\alpha]$, und mit ii. folgt: q ist ein Teiler von r.

e) Folgere aus a)iii, b) und d): Zu jedem maximalen Ideal M in $\mathbb{Z}[X]$ gibt es eine Primzahl q und ein $f \in \mathbb{Z}[X]$, so daß $\bar{f}$ irreduzibel in $\mathbb{F}_q[X]$ ist, mit $M = (q, f)$.

R4.5 [Frühjahr 1979] Für $R = \mathbb{Z}$ und $R = \mathbb{Z}[x]$ (Polynomring über $\mathbb{Z}$) untersuche man das durch die Primzahl $2 \in \mathbb{Z}$ erzeugte Hauptideal (2) in R und beweise oder widerlege die folgenden Aussagen:

a) (2) ist ein Primideal in R.

b) (2) ist ein maximales Ideal in R.

R4.6 [Herbst 1980] Geben Sie ein maximales Ideal von $\mathbb{Z}[X]$ an, das $X^2 + X + 1$ enthält.

R4.7 [Frühjahr 1985] Seien $f := X^3 - X^2 + X - 1$, $g := 3X^4 + 6X^2 + 3 \in \mathbb{Z}[X]$.

a) Bestimme ein erzeugendes Element des von f, g erzeugten Ideals in $\mathbb{Q}[X]$.

b) Beweise: Das von f, g in $\mathbb{Z}[X]$ erzeugte Ideal ist kein Hauptideal.

Funktionenringe

R4.8 [Frühjahr 1975] Es seien $\alpha := (a_n)$, $\beta := (b_n)$ mit $n \geq 0$ reelle beschränkte Zahlenfolgen und B der Ring dieser Zahlenfolgen mit den Verknüpfungen

$$\alpha + \beta := (a_n + b_n) \quad , \quad \alpha\beta := (a_n b_n) \quad ;$$

ferner seien folgende Teilmengen von B gegeben:

C, die Menge aller konvergenten Zahlenfolgen,

N, die Menge aller Nullfolgen,

N_0, die Menge aller trivialen Nullfolgen (d.h. derjenigen, deren Glieder fast alle 0 sind),

J_k, die Menge aller Zahlenfolgen $\alpha = (a_n)$ mit $a_n = 0$ für alle $n \geq k$ $(k = 0, 1, 2, \ldots)$.

Man zeige:

a) Diese Teilmengen sind Teilringe von B (gegebenenfalls ohne Einselement), die außer in den Fällen J_0 und J_1 echte Nullteiler besitzen; J_k ist ein Ideal in B; $\bigcup_{k=0}^{\infty} J_k = N_0$ ist ein Ideal in B, C und N.

b) J_k und N_0 sind nicht Primideale in N, C und B; N ist ein maximales Ideal und ein Primideal in C; N ist nicht Primideal in B.

R4.9 [Herbst 1981] $R := \mathcal{C}[0,1]$ sei der Ring der auf dem Intervall $[0,1]$ stetigen, reellwertigen Funktionen. Für $x \in [0,1]$ sei das Ideal $\mathfrak{m}_x$ durch $\mathfrak{m}_x = \{f \in R\,;\ f(x) = 0\}$ definiert. Zeigen Sie:

a) Das Ideal $\mathfrak{m}_x$ ist maximal in R.

b) Jedes maximale Ideal in R ist von der Form $\mathfrak{m}_y$ mit einem $y \in [0,1]$.

HINWEIS: Das Intervall $[0,1]$ ist kompakt. Sind $f_1, \ldots, f_n$ Funktionen aus dem Ideal J, so ist $f_1^2 + \ldots + f_n^2$ eine nicht-negative Funktion in J.

R4.10 [Frühjahr 1986] Sei $A = \mathcal{C}[0,1]$ der Ring der reellwertigen stetigen Funktionen auf dem Intervall $[0,1]$. Zeigen Sie:

a) Sei $I \subset A$ ein Ideal. Für jedes $r \in [0,1]$ enthalte I eine Funktion f mit $f(r) \neq 0$. Dann ist $I = A$.

b) Zu jedem maximalen Ideal $\mathfrak{m}$ von A gibt es ein $r \in [0,1]$, so daß

$$\mathfrak{m} = \{f \in A\,;\ f(r) = 0\} \quad .$$

R4.11 [Frühjahr 1990] $R = \mathcal{C}[a,b]$ ist der Ring der auf dem Intervall $[a,b]$ stetigen reellwertigen Funktionen. Beweisen Sie: Eine Funktion f ist genau dann Nullteiler von R, wenn

$$N_f = \{x \in [a,b]\,;\ f(x) = 0\}$$

ein offenes Intervall enthält.

Maximale Ideale

R4.12 [Herbst 1984] Sei R ein kommutativer Ring mit Eins, $R^\times$ die Einheitengruppe von R und $J(R)$ der Durchschnitt der maximalen Ideale von R. Zeigen Sie: Für $x \in R$ gilt genau dann $x \in J(R)$, wenn $1 - xy \in R^\times$ für alle $y \in R$.

R4.13 [Frühjahr 1989] Seien K ein Körper und R der Ring der fastkonstanten Folgen in K, d.h.

$$R = \{(x_i)_{i\geq 1}\,, \quad \text{alle } x_i \in K \quad \text{und} \quad x_n = x_{n+1} = \ldots \text{ für ein } n\}$$

mit komponentenweiser Addition und Multiplikation. Man zeige:

a) Zu jedem $x \in R$ gibt es eine Einheit $u \in R^\times$ mit $x = x^2 u$.

b) Zu jedem endlich erzeugten Ideal I von R gibt es ein Idempotent $e \in R$ mit $I = Re$.

HINWEIS: Sind e und f Idempotente von R, so zeige man, daß auch $g = e(1-f)+f$ ein Idempotent ist und damit $Re + Rf = Rg$ ist.

c) Die Menge $M = \{(x_i)_{i\geq 1}$ alle $x_i \in K$ und $x_n = x_{n+1} = \ldots = 0$ für ein $n\}$ bildet ein maximales Ideal in R, das nicht endlich erzeugt ist.

d) Für jedes $n \geq 1$ sei $e^{(n)} = (1, \ldots, 1, 0, 1, 1, \ldots)$ mit 0 an der Stelle n und 1 an allen anderen Stellen.
Dann ist $\{Re^{(n)}\,;\ n \geq 1\}$ die Menge aller von M verschiedenen maximalen Ideale von R.

R4.14 [Frühjahr 2002] Sei $R = \mathbb{Z}[[T]]$ der Ring der formalen Potenzreihen mit Koeffizienten in $\mathbb{Z}$.

a) Sei $m \subseteq R$ ein maximales Ideal in R. Zeigen Sie: $m \cap \mathbb{Z}$ ist ein maximales Ideal in $\mathbb{Z}$.

b) Bestimmen Sie die Gruppe der Einheiten $R^\times$.

c) Bestimmen Sie alle maximalen Ideale in R.

Primideale in allgemeinen kommutativen Ringen

R4.15 [Herbst 1978] Sei R ein kommutativer, assoziativer Ring mit 1 und $1 \neq 0$. Ein Ideal P von R heißt *Primideal*, wenn $P \neq R$ und wenn aus $ab \in P$ stets $a \in P$ oder $b \in P$ folgt. Man zeige:

a) R besitzt ein maximales Ideal.

b) Jedes maximale Ideal von R ist ein Primideal.

c) Ist P Primideal von R und R/P endlich, so ist P maximales Ideal von R.

d) Sei $R = \mathbb{Z}[x]$ der Ring der Polynome in einer Variablen x mit ganzzahligen Koeffizienten. Sei M die Menge der Polynome mit geradem konstanten Glied und P die Menge der Polynome mit konstantem Glied 0. Dann ist M ein maximales Ideal von R, während P ein Primideal ist, aber kein maximales Ideal.

R4.16 [Herbst 1991] Es sei R ein kommutativer Ring mit 1. Die folgenden Behauptungen sind zu beweisen oder durch ein Gegenbeispiel zu widerlegen:

a) Ist M ein maximales Ideal von R, so ist M auch ein Primideal von R.

b) Ist P ein Primideal von R, so ist P auch ein maximales Ideal von R.

c) R hat stets ein maximales Ideal.

d) R hat höchstens ein maximales Ideal.

e) Es seien P, Q Primideale von R. Dann gilt:

i) $P \cap Q$ ist ein Primideal von R.

ii) $P \cap Q$ ist ein Ideal von R.

iii) $P \cup Q$ ist ein Ideal von R.

iv) $P \cup Q$ ist ein Primideal von R.

R4.17 [Frühjahr 1999] Sei R ein kommutativer Ring mit Einselement und $S \supset R$ ein kommutativer Oberring von R; das Einselement von R sei auch das Einselement von S.

a) Man zeige: Ist $I \subset S$ ein Ideal von S, so ist $I \cap R$ ein Ideal von R.

b) Sei $I \subset S$ ein Ideal. Man untersuche, welche der folgenden Implikationen wahr sind:

i) I Primideal in $S \implies I \cap R$ Primideal in R.

ii) $I \cap R$ Primideal in $R \implies I$ Primideal in S.

(Beweis oder Gegenbeispiel!)

R4.18 [Herbst 1982] R sei ein kommutativer Ring, I_1 und I_2 seien Ideale und P ein Primideal in R. Beweisen Sie: Aus $I_1 \cap I_2 \subseteq P$ folgt, daß I_1 oder I_2 in P enthalten ist.

R4.19 [Frühjahr 1986] Gegeben seien ein Integritätsbereich R mit Quotientenkörper K und verschiedene Primideale $P_1, \ldots, P_n$ $(\neq R)$ von R.

a) Beweisen Sie etwa mit vollständiger Induktion nach n:
Ist S ein in $P_1 \cup \ldots \cup P_n$ enthaltenes Ideal von R, so gilt $S \subset P_k$ für mindestens ein $k \in \{1, \ldots, n\}$.
(Wo liegt $y := x_1 + \prod_{i=2}^{n} x_i$, wenn $x_i \in S \setminus \bigcup\limits_{j \neq i} P_j$ für jedes $i = 1, \ldots, n$?).

b) Es gelte $R = R_{P_1} \cap \ldots \cap R_{P_n}$, wobei $R_{P_i} := \left\{ \frac{a}{b};\ a \in R,\ b \in R \setminus P_i \right\} \subset K$. Man zeige:

i) $P_1 \cup \ldots \cup P_n$ ist die Menge der Nichteinheiten von R.

ii) Ist $P_i \not\subset P_j$ für $i \neq j$, $i, j = 1, \ldots, n$, so sind $P_1, \ldots, P_n$ die maximalen Ideale von R.

R4.20 [Frühjahr 1979] Es sei R ein kommutativer Ring mit 1. Für jede nichtleere Teilmenge S von R sei $\mathrm{Ann}(S)$ durch

$$\mathrm{Ann}(S) = \{y \in R;\ ys = 0 \text{ für alle } s \in S\}$$

definiert. Das Ideal A in R habe die Eigenschaft, daß für jedes Ideal $\overline{U} \neq (0)$ in $\overline{R} = R/A$ die Aussage $\mathrm{Ann}(\overline{U}) = \mathrm{Ann}(\overline{R})$ gilt. Zeigen Sie, daß A ein Primideal ist.

R4.21 [Frühjahr 1994] Es sei R ein kommutativer Ring, $R \neq 0$. Zeigen Sie: In der Menge der Primideale von R gibt es ein minimales Element (bezüglich der Inklusion).

R4.22 [Herbst 1982] R sei ein kommutativer Ring mit Eins, $\mathfrak{p}$ ein Primideal von R. Zeigen Sie mit Hilfe des Zornschen Lemmas, daß in $\mathfrak{p}$ ein minimales Primideal von R enthalten ist (d.h. ein solches, in dem kein weiteres Primideal echt enthalten ist).

R4.23 [Frühjahr 1992] Seien R ein kommutativer Ring, S eine multiplikative Teilmenge (d.h. $S \neq \varnothing$ und $S \cdot S \subset S$) und I ein Ideal mit $I \cap S = \varnothing$. Zeigen Sie mit Hilfe des Zornschen Lemmas, daß es ein Primideal P von R gibt mit $I \subset P$ und $P \cap S = \varnothing$.

R4.24 [Herbst 1979] Sei A ein kommutativer Ring mit Einselement 1.

a) Sei $S \subset A$ eine multiplikativ abgeschlossene Teilmenge von A mit $0 \notin S$. Man beweise mit Hilfe des Zorn'schen Lemmas: Es gibt ein Primideal $\mathfrak{p}$ von A mit $\mathfrak{p} \cap S = \varnothing$.

b) Als eine Anwendung folgere man: Der Durchschnitt $\mathfrak{N}$ aller Primideale $\mathfrak{p}$ von A besteht genau aus den nilpotenten Elementen von A. Dabei heißt ein Element $x \in A$ *nilpotent*, falls $x^n = 0$ für ein $n \in \mathbb{N}$ gilt.

Primärideale

R4.25 [Frühjahr 1973] Ist R ein kommutativer Ring, so sei $(x_1, \ldots, x_m)$ das von den $x_i \in R$ $(1 \leq i \leq m)$ in R erzeugte Ideal. Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in R, so sei $\mathfrak{a} \cdot \mathfrak{b}$ die Menge aller endlichen Summen

$$\sum_j a_j b_j \qquad (a_j \in \mathfrak{a};\ b_j \in \mathfrak{b}).$$

Dann ist $\mathfrak{a} \cdot \mathfrak{b}$, versehen mit den in R definierten Ringoperationen $(+, \cdot)$, ein Ideal in R. (Diese Aussage soll nicht bewiesen werden.)

a) Im Ring $\mathbb{Z}[\tau]$ der Polynome in einer Unbestimmten τ und mit ganzzahligen Koeffizienten betrachte man das Ideal $(4, \tau)$.

i. Man prüfe, ob $(4, \tau)$ Hauptideal in $\mathbb{Z}[\tau]$ ist.

ii. Man zeige: Es gibt genau zwei Ideale in $\mathbb{Z}[\tau]$, die $(4, \tau)$ echt umfassen. Ist $(4, \tau)$ Primideal in $\mathbb{Z}[\tau]$?

iii. Man prüfe, ob $(4, \tau)$ gleich dem Produktideal $(2, \tau) \cdot (2, \tau)$ ist.

b) Sei $\mathfrak{q}$ ein Ideal des kommutativen Ringes R.

i. Man zeige die Gleichwertigkeit der folgenden Aussagen (A_1) und (A_2):

(A_1): Gilt für die Elemente a und b aus R:

$$ab \in \mathfrak{q} \quad , \quad b \notin \mathfrak{q} \quad ,$$

so gibt es eine natürliche Zahl n mit $a^n \in \mathfrak{q}$.

(A_2): Zu jedem Nullteiler $\alpha \in R/\mathfrak{q}$ gibt es eine natürliche Zahl n mit $\alpha^n = 0$.

ii. Man prüfe, ob (A_i) ($i = 1$ oder 2) im Falle $R = \mathbb{Z}[\tau]$ und $\mathfrak{q} = (4, \tau)$ erfüllt ist.

c) Der Ring $S := \mathbb{Z}[2\tau, \tau^2, \tau^3]$ ist definiert als der Durchschnitt aller Unterringe von $\mathbb{Z}[\tau]$, die die Menge $\{2\tau, \tau^2, \tau^3\}$ enthalten.

i. Man beschreibe die Elemente von S durch eine Eigenschaft ihrer Koeffizienten.

ANLEITUNG: Man bestimme zunächst alle Polynome aus $\mathbb{Z}[\tau^2, \tau^3]$.

ii. Man zeige: $\mathfrak{p} := (2\tau, \tau^2, \tau^3)$ ist Primideal in S.

iii. Man prüfe, ob (A_i) ($i = 1$ oder 2) im Falle $R = S$ und $\mathfrak{q} = \mathfrak{p} \cdot \mathfrak{p}$ mit $\mathfrak{p}$ wie ii. erfüllt ist.

R4.26 [Herbst 1976] Es bezeichne R den Ring $\mathbb{R}[X,Y]$ der reellen Polynome in zwei Veränderlichen, $\mathfrak{a}$ bezeichne das von X und Y erzeugte Ideal (X,Y) von R.

a) Man zeige, daß $\mathfrak{a}$ kein Hauptideal, jedoch maximales Ideal ist.

b) Es sei $\mathfrak{b}$ ein Ideal von R mit $\mathfrak{a}^5 \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Man beweise, daß die Nullteiler von $R/\mathfrak{b}$ nilpotent sind.

Weiter sei $\mathfrak{c}$ das Ideal (X^2,Y) von R.

c) Man beweise, daß die Nullteiler von $R/\mathfrak{c}$ nilpotent sind, und daß es kein Primideal $\mathfrak{p}$ von R und keine natürliche Zahl n mit $\mathfrak{p}^n = \mathfrak{c}$ gibt.

Weiter sei $\mathfrak{d}$ das Ideal (X^2,XY) von R.

d) Man beweise $\mathfrak{d} = \mathfrak{c} \cap (X)$, und man bestimme den Durchschnitt aller Primideale $\mathfrak{p}$ von R mit $\mathfrak{d} \subseteq \mathfrak{p}$.

R4.27 [Frühjahr 1997] Sei R ein kommutativer Ring mit Einselement. Ein Ideal I in R heißt ein *Primideal*, falls der Restklassenring R/I nullteilerfrei ist. Es heißt ein *Primärideal*, falls für jeden Nullteiler $\bar{a}$ in R/I eine Potenz $\bar{a}^m = 0$ in R/I ist. Das Radikal $\sqrt{I}$ des Ideals I besteht aus allen $a \in R$, für die es eine natürliche Zahl k mit $a^k \in I$ gibt.

Sei $R = \mathbb{Z}$ und $I = (n)$ das von der natürlichen Zahl $n \geq 0$ erzeugte Hauptideal in $\mathbb{Z}$. Geben Sie notwendige und hinreichende Bedingungen dafür an, daß

a) I ein Primideal ist;

b) I ein Primärideal ist;

c) $\sqrt{I} = I$ gilt.

Primideale in bestimmten Ringen

R4.28 [Frühjahr 1984] Sei $\mathbb{Z}$ der Ring der ganzen Zahlen. Die Menge $R := \mathbb{Z} \times \mathbb{Z}$ ist bzgl. der Addition

$$(\alpha,\beta) + (\gamma,\delta) := (\alpha+\gamma,\ \beta+\delta)$$

und Multiplikation

$$(\alpha,\beta) \cdot (\gamma,\delta) := (\alpha\gamma, \alpha\delta + \beta\gamma)$$

ein kommutativer Ring mit Nullelement $(0,0)$ und Einselement $(1,0)$ (nicht nachzuweisen). Zeigen Sie:

a) $I := \{0\} \times \mathbb{Z}$ ist ein Ideal von R, das genau aus den nilpotenten Elementen von R besteht. Jedes Primideal von R enthält I.

b) Der Faktorring R/I ist isomorph zu $\mathbb{Z}$.

c) Die Primideale von R sind: I und die Ideale $p\mathbb{Z} \times \mathbb{Z}$, wobei p alle Primzahlen durchläuft.

R4.29 [Herbst 1988] Für $R = \mathbb{Q}[x]$ (Polynomring über $\mathbb{Q}$) und für $R = \mathbb{Z}[x]$ (Polynomring über $\mathbb{Z}$) untersuche man das durch $f = x^2 + 2$ in R erzeugte Hauptideal (f) und beweise oder widerlege die folgenden Aussagen:

a) (f) ist ein Primideal in R.

b) (f) ist ein maximales Ideal in R.

R4.30 [Herbst 2003] Sei R der Unterring des Matrizenringes $\mathbb{Q}^{2\times 2}$, der aus den Matrizen $\begin{pmatrix} z & a \\ 0 & z \end{pmatrix}$ mit $z \in \mathbb{Z}$, $a \in \mathbb{Q}$ besteht.

a) Zeigen Sie, dass jedes Primideal von R die Elemente

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \qquad \text{für} \quad a \in \mathbb{Q}$$

enthält, und dass diese Elemente ein Ideal N von R bilden, für das $R/N \simeq \mathbb{Z}$ gilt.

b) Bestimmen Sie alle Primideale von R.

Lokale Ringe

R4.31 [Herbst 1980] Zeigen Sie, daß für einen kommutativen Ring R mit 1 folgende Aussagen äquivalent sind:

(i) Die nicht invertierbaren Elemente von R bilden ein Ideal.

(ii) R besitzt genau ein maximales Ideal.

HINWEIS: Sie können die Tatsache benutzen, daß jedes Ideal $\neq R$ in einem maximalen Ideal enthalten ist.

R4.32 [Herbst 1985] R sei ein kommutativer Ring mit 1. R heißt *lokal*, wenn R genau ein maximales Ideal besitzt. Zeigen Sie:

a) Ist p eine Primzahl, so ist die Menge $\mathbb{Z}_{(p)}$ aller rationalen Zahlen $\frac{a}{b}$ mit ganzen Zahlen a, b und $\mathrm{ggT}(a, b) = 1$, deren Nenner nicht durch p teilbar ist, ein lokaler Ring.

b) Ist R ein lokaler Ring und $I \subset R$ ein Ideal mit $I \neq R$, so ist auch R/I ein lokaler Ring.

c) Ist $R \neq \{0\}$ und ist jede Nichteinheit von R nilpotent, so ist R ein lokaler Ring.

R4.33 [Herbst 1984] Für eine Primzahl p sei $\mathbb{Z}_{(p)}$ die Menge der rationalen Zahlen, deren Nenner prim zu p ist. Zeigen Sie:

a) $\mathbb{Z}_{(p)}$ ist Hauptidealring.

b) Für verschiedene Primzahlen p und q ist jeder Ringhomomorphismus $\mathbb{Z}_{(p)} \to \mathbb{Z}_{(q)}$ trivial.

c) Für verschiedene Primzahlen p und q ist $\mathbb{Z}_{(p)} \cap \mathbb{Z}_{(q)}$ ein Hauptidealring mit genau zwei maximalen Idealen.

R4.34 [Herbst 1999] Sei $R = \mathbb{R}[[X]]$ der Ring der formalen Potenzreihen mit reellen Koeffizienten. Man zeige:

a) Jede Potenzreihe $a = a_0 + a_1 X + a_2 X^2 + \ldots$ mit $a_0 \neq 0$ ist eine Einheit in R.

b) R ist Hauptidealring.

c) Es gibt genau ein maximales Ideal in R.

d) Es gibt genau zwei Primideale in R.

e) Der Quotientenkörper Q von R besitzt als R-Modul ein abzählbares Erzeugendensystem.

Direkte Produkte und Chinesischer Restsatz

R4.35 [Herbst 1972] Es sei S der Restklassenring des Polynombereichs $\mathbb{Q}[x]$ nach

$$f(x) := x^3 + x - 2 \quad .$$

e_k bedeute die Restklasse von x^k $(k = 0, 1, 2)$.

a) Wie drücken sich die Produkte $e_j e_k$ je zweier dieser Basiselemente wieder linear durch diese aus (Multiplikationstafel)?

b) Man bestimme alle Elemente q von S mit der Eigenschaft $q^2 = q$. In welcher Weise läßt sich mit ihrer Hilfe der Ring S als direkte Summe von zwei Körpern darstellen, von denen einer zu $\mathbb{Q}$, der andere zu $\mathbb{Q}\left(\sqrt{-7}\right)$ isomorph ist?

R4.36 [Herbst 1976] D sei die direkte Summe zweier kommutativer Ringe R und S, also die Menge aller Paare (r, s) mit r aus R und s aus S, für die Addition und Multiplikation komponentenweise definiert ist. U sei ein Unterring von D.
Sei U_R die Menge aller r aus R, für die ein s aus S so existiert, daß (r, s) zu U gehört. Genau dann gehört r zu N_R, wenn $(r, 0)$ zu U gehört. U_S und N_S seien analog definiert. Zeigen Sie:

a) U_R ist ein Unterring von R.

b) N_R ist ein Ideal von U_R.

c) Die folgenden drei Aussagen sind äquivalent:

i) $N_R = U_R$

ii) $N_S = U_S$

iii) U ist direkte Summe von U_R und U_S und kanonisch in D eingebettet.

Sei nun R ein Körper der Ordnung 2 und S ein Körper der Ordnung 8.

d) Bestimmen Sie alle Unterringe von D.

R4.37 [Herbst 1985] Der Polynomring $R = \mathbb{Z}_6[x]$ in einer Variablen über dem Ring $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$ mit 6 Elementen soll untersucht werden.

a) Zeigen Sie, daß R die direkte Summe der Hauptideale $(\bar{2})$ und $(\bar{3})$ ist, wobei $\bar{2}$ und $\bar{3}$ die Restklassen von 2 und 3 in $\mathbb{Z}_6$ sind!

b) Bestimmen Sie die Einheiten, Nullteiler und nilpotenten Elemente von R, indem Sie Elemente von R gemäß a) als Summen darstellen!

c) Bestimmen Sie alle maximalen und alle primen Ideale von R! Beachten Sie für letzteres $\bar{2} \cdot \bar{3} = \bar{0}$ in R!

R4.38 [Frühjahr 1980] R sei ein kommutativer Ring mit Eins, I_1, I_2 seien Ideale von R und

$$\alpha_j : \; R/I_j \to R/(I_1 + I_2) \qquad (j = 1, 2)$$

die kanonischen Epimorphismen. F sei der Unterring von $R/I_1 \times R/I_2$, der aus allen Paaren $(r_1 + I_1, r_2 + I_2)$ mit $\alpha_1(r_1 + I_1) = \alpha_2(r_2 + I_2)$ besteht. Man zeige, daß

$$\gamma : \; R \to F \qquad , \qquad r \mapsto (r + I_1, r + I_2)$$

ein surjektiver Ringhomomorphismus mit dem Kern $I_1 \cap I_2$ ist.

R4.39 [Herbst 1982] R sei ein kommutativer Ring, der einen Körper k enthält. Es sei $\dim_k R < \infty$. Beweisen Sie:

a) Alle Primideale von R sind maximal.

b) R hat höchstens $\dim_k R$ maximale Ideale.

R4.40 [Herbst 1989]

a) Sei K ein Körper und $\mathrm{char}(K) = p > 0$. Beweisen Sie:
$K[X]/(X^n - 1)$ ist als Ring genau dann isomorph zu einem endlichen direkten Produkt von Körpern, wenn p kein Teiler von n ist.

b) Seien $K_1, \ldots, K_s$ endlich viele Körper und $R := K_1 \times \ldots \times K_s$ der Produktring. Wie viele Ideale hat R?

c) Wie viele Ideale hat $\mathbb{Q}[X]/(X^{15} - 1)$?

R4.41 [Herbst 1995] R sei ein kommutativer Ring, der einen Körper k enthält und somit auf natürliche Weise ein k-Vektorraum ist. Es sei $\dim_k R < \infty$. Man beweise:

a) Alle Primideale von R sind maximal.

b) R hat höchstens $\dim_k R$ maximale Ideale.

R4.42 [Herbst 2001] Betrachtet sei folgendes System von zwei Kongruenzen in $\mathbb{Q}[X]$:

$$f \equiv X - 1 \mod (X^2 - 1)$$
$$f \equiv X + 1 \mod (X^2 + X + 1) \quad .$$

Bestimmen Sie eine konkrete Lösung und die Menge aller Lösungen des Systems.

Polynomringe in mehreren Variablen

R4.43 [Frühjahr 1973] Es sei $R = K[x, y, z]$ der Polynomring in den unabhängigen Unbestimmten x, y, z über dem Körper K und

$$\mathfrak{m} := \{f(x, y, z) \in R;\ f(0, 0, 0) = 0\} \quad .$$

Man zeige:

a) $\mathfrak{m}$ ist ein maximales Ideal in R.

b) $\mathfrak{m} = (x, y, z)$.

c) (x) und (x, y) sind Primideale in R, aber keine maximalen Ideale in R.

R4.44 [Herbst 1981] Es sei $K[x, y, z]$ der Polynomring in drei Unbestimmten über dem Körper K und

$$R := K[x, y, z]/(xy - z^2) \quad .$$

Zu $f \in K[x, y, z]$ definiert man $\bar{f} = f + (xy - z^2)$. Zeigen Sie: $(\bar{x}, \bar{z})$ ist ein Primideal in R.

R4.45 [Frühjahr 1975] Sei k ein Körper, $k[x_1, x_2]$ der Polynomring in zwei Unbestimmten, und das Ideal $\mathfrak{a} \subset k[x_2, x_2]$ sei erzeugt von den beiden Elementen

$$a_{11}x_1 + a_{12}x_2 \quad , \quad a_{21}x_1 + a_{22}x_2$$

mit $a_{ij} \in k$. Man zeige, daß $\mathfrak{a}$ ein Primideal ist, und daß $k[x_1, x_2]/\mathfrak{a}$ isomorph zu einem der Ringe $k, k[x]$ oder $k[x_1, x_2]$ ist.

R4.46 [Frühjahr 1987] Es seien K ein Körper, $P := K[X_1, X_2, X_3, \ldots]$ der Polynomring über K in den Unbestimmten $X_n (n \geq 1)$ und I das von X_1^2 und allen $X_n - X_{n+1}^2 (n \geq 1)$ erzeugte Ideal von P. Ferner sei $R := P/I$, x_n die Restklasse von X_n in R $(n \geq 1)$ und $\mathfrak{a}$ das von $\{x_n\,,\ n \geq 1\}$ erzeugte Ideal von R. Zeigen Sie:

a) Jedes Element $r \in \mathfrak{a}$ ist nilpotent.

b) $R/\mathfrak{a} \simeq K$ und $\mathfrak{a}$ ist das einzige Primideal von R.

c) Die Einheiten von R sind genau die Elemente der Form $\alpha \cdot 1 + r$, wobei $\alpha \in K \setminus \{0\}$ und $r \in \mathfrak{a}$.

d) Jedes $r \in R$, $r \neq 0$, läßt sich in der Form $r = u \cdot x_n^e$ schreiben mit einer Einheit $u \in R$, einem $n \geq 1$ und einer nicht negativen ganzen Zahl e.

e) Für alle $r, s \in R$ gilt $Rr \subseteq Rs$ oder $Rs \subseteq Rr$.

R4.47 [Frühjahr 1988] K sei ein Körper, $K[T]$ der Polynomring in einer Variablen T und $K[X,Y]$ der Polynomring in den Variablen X, Y über K. Für zwei fest gewählte $f, g \in K[T]$ sei

$$I := \{F \in K[X,Y]\,,\ F(f,g) = 0\} \quad .$$

a) Zeigen Sie, daß I ein Primideal von $K[X,Y]$ ist.

b) Unter welcher Bedingung für f und g ist I ein maximales Ideal von $K[X,Y]$?

R4.48 [Herbst 2002] K sei ein Körper, $K[T]$ der Polynomring in einer Variablen T und $K[X,Y]$ der Polynomring in den Variablen X, Y über K. Für zwei fest gewählte $f, g \in K[T]$ sei

$$I := \{F \in K[X,Y] \mid F(f,g) = 0\} \quad .$$

a) Zeigen Sie, dass I ein Primideal von $K[X,Y]$ ist.

b) Unter welcher Bedingung für f und g ist I ein maximales Ideal von $K[X,Y]$? Begründen Sie Ihre Antwort!

R4.49 [Frühjahr 1989] K sei ein Körper und R der Restklassenring des Polynomrings $K[X,Y]$ nach dem von X^3, Y^3, X^2Y^2 erzeugten Ideal: $R = K[X,Y]/(X^3, Y^3, X^2Y^2)$.

a) Bestimmen Sie die Dimension von R als K-Vektorraum.

b) Zeigen Sie, daß R genau ein Primideal $(\neq R)$ besitzt.

R4.50 [Frühjahr 1993] Es sei R der Polynomring in zwei Unbestimmten X und Y über einem Körper K. Es sei P das von $X - Y$ erzeugte Ideal in R, und es sei M das von $X - Y$ und X erzeugte Ideal in R. Zeigen Sie:

a) P ist ein Primideal.

b) M ist ein maximales Ideal.

(Sie dürfen verwenden, daß R faktoriell ist.)

R4.51 [Herbst 2002] Welche der folgenden drei Ideale in $\mathbb{C}[X,Y]$

$$I_1 = (X \cdot Y) \quad , \quad I_2 = (X + Y) \quad , \quad I_3 = (X, Y)$$

sind Primideale bzw. sogar maximale Ideale?

Nichtkommutative Idealtheorie

R4.52 [Frühjahr 1985] Es sei R der Unterring $\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} ;\ a,b,c \in \mathbb{Z} \right\}$ des Ringes aller 2×2-Matrizen über $\mathbb{Z}$. Man ermittle

a) alle (zweiseitigen) Ideale von R,

b) alle maximalen Ideale von R,

c) die Struktur aller Faktorringe R/A (A ein Ideal), die kommutativ sind.

R4.53 [Frühjahr 2003] Sei K ein Körper und R die Menge aller 2×2-Matrizen der Form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ mit $a,b,c \in K$. Bestimmen Sie alle nichttrivialen zweiseitigen Ideale I des Ringes R.

R4.54 [Frühjahr 2001] Sei k eine positive Zahl und sei $R := \mathrm{M}_k(\mathbb{Z})$ der Ring der ganzzahligen $k \times k$-Matrizen. Zeigen Sie:

a) Für jede natürliche Zahl $n \geq 0$ ist nR ein zweiseitiges Ideal in R.

b) Jedes zweiseitige Ideal von R ist von der in a) genannten Art.

R4.55 [Herbst 2001] Sei R ein (nicht notwendigerweise kommutativer) Ring mit 1.

a) Sei $a \in R$. Man beschreibe — mit Beweis — das Hauptideal (a), d.h. das kleinste beidseitige Ideal von R, das a enthält.

b) Sei nun $\mathcal{I} \subsetneq R$ ein beidseitiges Ideal. Zeigen Sie die Äquivalenz folgender Aussagen:

aa) Für alle beidseitigen Ideale $\mathcal{A}, \mathcal{B}$ aus R gilt: $\mathcal{A} \cdot \mathcal{B} \subseteq \mathcal{I} \implies \mathcal{A} \subseteq \mathcal{I}$ oder $\mathcal{B} \subseteq \mathcal{I}$.

bb) Für alle $a,b \in R$ gilt: $aRb \subseteq \mathcal{I} \implies a \in \mathcal{I}$ oder $b \in \mathcal{I}$.

cc) Für alle Linksideale $\mathcal{A}, \mathcal{B}$ aus R gilt: $\mathcal{A} \cdot \mathcal{B} \subseteq \mathcal{I} \implies \mathcal{A} \subseteq \mathcal{I}$ oder $\mathcal{B} \subseteq \mathcal{I}$.

R4.56 [Frühjahr 2002] Es sei p eine Primzahl.

a) Zeigen Sie, dass die folgende Menge ganzzahliger 3×3-Matrizen

$$M = \{(a_{ij}) \in \mathrm{M}_3(\mathbb{Z}) ;\ a_{ij} \in p\mathbb{Z} \ \text{ falls } \ i < j\}$$

ein Ring (mit Einselement) ist.

b) Geben Sie drei Ideale I von M an mit $M/I \simeq \mathbb{Z}/p\mathbb{Z}$.

5. Faktorielle Ringe

R5.1 [Frühjahr 1977] Die Menge R aller Potenzreihen $\sum a_n z^n$ in einer komplexen Variablen z mit komplexen Koeffizienten und positivem Konvergenzradius ist zusammen mit den wie folgt erklärten Verknüpfungen ein Integritätsring:

$$\Big(\sum a_n z^n\Big) + \Big(\sum b_n z^n\Big) = \sum (a_n + b_n) z^n$$

$$\Big(\sum a_n z^n\Big) \cdot \Big(\sum b_n z^n\Big) = \sum c_n z^n \quad \text{mit} \quad c_n = \sum_{l+m=n} a_l b_m \ \text{ für } \ n \in \mathbb{N}$$

Man zeige:

a) $\sum a_n z^n \in R$ ist genau dann eine Einheit von R, wenn $a_0 \neq 0$ ist.

b) Zu jedem Ideal $\mathfrak{a}$ von R mit $\mathfrak{a} \neq \{0\}$ und $\mathfrak{a} \neq R$ gibt es ein $m \in \mathbb{N}$, so daß $\mathfrak{a}$ von z^m erzeugt wird.

c) R besitzt genau ein maximales Ideal.

d) z ist ein Primelement von R und jedes Primelement von R ist zu z assoziiert.

R5.2 [Herbst 1987]

a) Sei R ein Integritätsring (kommutativer, nullteilerfreier Ring mit 1-Element). Zeigen Sie:

i) Jedes Primelement aus r ist auch ein irreduzibles Element.

ii) Sind p und q Primelemente aus R und ist p ein Teiler von q, so ist p assoziiert zu q.

b) Sei R ein ZPE-Ring (= faktorieller Ring) und K sein Quotientenkörper. Zeigen Sie, daß für zwei nicht assoziierte Primelemente $p, q \in R$ gilt: $[K(\sqrt{p}, \sqrt{q}) : K] = 4$.

c) Verwenden Sie, daß $\mathbb{Z}[i]$ ein ZPE-Ring ist. Zeigen Sie, daß $1 + 2i$ und $1 - 2i$ nichtassoziierte Primelemente in $\mathbb{Z}[i]$ sind.

R5.3 [Frühjahr 1988] R sei ein faktorieller Ring mit dem Quotientenkörper K, und es sei 2 in R Einheit. Ferner sei $S := R[X]/(X^2 - \rho^2\sigma)$, wobei ρ, σ Nichteinheiten $\neq 0$ in R sind und σ nicht durch das Quadrat eines Primelements von R teilbar ist. ξ bezeichne die Restklasse von X in S. Zeigen Sie:

a) S ist ein Integritätsring und jedes Element z aus dem Quotientenkörper L von S besitzt eine eindeutige Darstellung $z = x + y\xi$ mit $x, y \in K$.

b) Für $z = x + y\xi$ $(x, y \in K)$ sei $\mathrm{Sp}(z) := 2x$, $\mathrm{N}(z) := x^2 - y^2\xi^2$ (Spur und Norm von z). Dann ist

$$T := \{z \in L;\ \mathrm{Sp}(z) \in R,\ \mathrm{N}(z) \in R\}$$

ein Unterring von L mit $S \subset T$.

c) Die Menge $F := \{z \in T;\ z \cdot u \in S \ \text{ für alle } \ u \in T\}$ ist ein Ideal sowohl in S wie auch in T, und es gilt

$$F = \{a\rho + b\xi;\ a, b \in R\} \quad .$$

d) Genau dann ist F ein Primideal von S, wenn ρ ein Primelement von R ist.

R5.4 [Frühjahr 1988]

a) Sei R ein faktorieller Ring mit dem Quotientenkörper Q, sei weiter $f = f_0 + f_1X + \ldots + f_nX^n \in R[X]$ ein Polynom mit Koeffizienten in R. Eine Nullstelle von f sei $\frac{r}{s}$, wobei r und s teilerfremde Elemente aus R sind mit $s \neq 0$. Zeigen Sie, daß r Teiler von f_0 und s Teiler von f_n ist.

b) Berechnen Sie alle rationalen Nullstellen von

$$f = 3X^4 + 4X^3 - 12X^2 + 4X - 15 \in \mathbb{Z}[X] \quad .$$

c) Zeigen Sie: $qX^3 - p$ ist in $\mathbb{Z}[X]$ irreduzibel, wenn p und q verschiedene Primzahlen sind.

R5.5 [Herbst 1992] Es sei p ein Primelement eines faktoriellen Ringes R. Für $q \in R$ mit $q \neq 0$ sei $S := R[X]/(X^2 - pq^2)$, und es bezeichne ξ die Restklasse von X in S. Zeigen Sie:

a) S ist ein Integritätsring.

b) $S = R \oplus R\xi$.

c) $I := \{aq + b\xi\,;\ a, b \in R\}$ ist ein Ideal von S.

d) Es ist $S/I \simeq R/(q)$, und I ist genau dann ein Primideal von S, wenn q ein Primelement von R ist.

6. Kettenbedingungen

Artinsche Ringe

R6.1 [Herbst 1981] R sei ein Integritätsring derart, daß jede absteigende Kette von Hauptidealen von R nach unten stationär wird. Man beweise, daß R ein Körper ist.

R6.2 [Frühjahr 1997] Sei R ein assoziativer, kommutativer Ring mit Eins, in dem jede Kette

$$I_0 \supseteq I_1 \supseteq \ldots \supseteq I_n \supseteq \ldots$$

von Idealen stationär wird. Ein solcher Ring heißt *artinsch*. Zeigen Sie:

a) Jedes homomorphe Bild von R ist artinsch.

b) Ein artinscher Integritätsring ist sogar ein Körper.

HINWEIS: Betrachten Sie für $a \in R \setminus \{0\}$ die Ideale (a^n).

c) Jedes Primideal eines artinschen Rings ist maximal.

Noethersche Ringe

R6.3 [Herbst 1978] k bezeichnet stets einen kommutativen Körper, $k[T_1, \ldots, T_n]$ sei der Polynomring in n Unbestimmten darüber. Für eine beliebige Teilmenge $S \subset k[T_1, \ldots, T_n]$ sei

$$V(S) = \{(x_1, \ldots, x_n) \in k^n \,;\; f(x_1, \ldots, x_n) = 0 \text{ für alle } f \in S\}$$

die Menge der gemeinsamen Nullstellen und $I(S) \subset k[T_1, \ldots, T_n]$ das von S erzeugte Ideal. Eine Teilmenge $X \subset k^n$ heißt *algebraisch*, wenn es ein $S \subset k[T_1, \ldots, T_n]$ gibt, mit $X = V(S)$.

Man beweise:

1) a) Ist $S' \subset S \subset k[T_1, \ldots, T_n]$, so ist $V(S) \subset V(S')$.

b) $V(S) = V(I(S))$ für jede Teilmenge $S \subset k[T_1, \ldots, T_n]$.

2) a) Für jede algebraische Teilmenge $X \subset k^1$ gibt es ein $f \in k[T]$ mit $X = V(f)$.

b) Eine Teilmenge $X \subset k^1$ ist algebraisch genau dann, wenn $X = k^1$ oder wenn X endlich ist.

c) Zu jeder algebraischen Teilmenge $X \subset k^n$ gibt es endlich viele Polynome $f_1, \ldots, f_r$ aus $k[T_1, \ldots, T_n]$ mit $X = V(f_1, \ldots, f_r)$.

3) a) Für Ideale $\mathfrak{a}, \mathfrak{b} \subset k[T_1, \ldots, T_n]$ gilt in k^n

$$V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b}) \quad \text{und} \quad V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cdot \mathfrak{b}) \quad .$$

b) Man beweise oder widerlege: Sind für eine beliebige Indexmenge J die Teilmengen $X_j \subset k^n$ für $j \in J$ algebraisch, so sind auch

$$\bigcap_{j \in J} X_j \quad \text{bzw.} \quad \bigcup_{j \in J} X_j$$

in k^n algebraisch.

4) a) Ist $X \subset \mathbb{R}^n$ algebraisch, so gibt es ein $f \in \mathbb{R}[T_1, \ldots, T_n]$ mit $X = V(f)$.

b) Zu je zwei verschiedenen Punkten $p, q \in k^n$ gibt es ein Polynom $g \in k[T_1, \ldots, T_n]$ mit $g(p) = 1$ und $g(q) = 0$.

c) Ist k endlich und $X \subset k^n$ algebraisch, so gibt es ein $f \in k[T_1, \ldots, T_n]$ mit $X = V(f)$.

R6.4 [Herbst 1989] Es sei $\mathbb{Z}[X]$ der Polynomring über $\mathbb{Z}$ und

$$\mathfrak{a} := \{f \in \mathbb{Z}[X] : f(0) = 0\} \quad .$$

a) Zeigen Sie: $\mathfrak{a}$ ist Hauptideal.

b) Ist $\mathfrak{a}$ Primideal?

c) Ist $\mathbb{Z}[X]$ ein Hauptidealring?

d) Ist $\mathbb{Z}[X]$ ein noetherscher Ring?

Begründen Sie Ihre Antwort.

R6.5 [Herbst 1974] Ist $\mathfrak{R} = (R, +, \cdot)$ ein Ring und wird jedes Ideal in $\mathfrak{R}$ von einem Element erzeugt, so gibt es zu jeder abzählbaren Folge $I_1, \ldots, I_n, \ldots$ von Idealen in $\mathfrak{R}$ mit $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ eine natürliche Zahl n_0, so daß $I_{n_0} = I_n$ für alle $n \geq n_0$ gilt.

R6.6 [Frühjahr 1991] Zeigen Sie:

a) In einem Hauptidealring werden alle aufsteigenden Ketten von Idealen stationär.

b) Sei P eine beliebige Menge von Primzahlen. Ganze Zahlen $\neq 0$, deren Primteiler sämtlich aus P sind, heißen *P-Zahlen*. Dann ist die Menge der rationalen Zahlen

$$\mathbb{Q}(P) := \left\{ \frac{a}{b} \in \mathbb{Q} \,;\; a \in \mathbb{Z}\,,\; b \;\; P\text{-Zahl} \right\}$$

ein Hauptidealring.

R6.7 [Herbst 1975] Man zeige: Jeder surjektive Homomorphismus $f : \mathbb{Z} \to \mathbb{Z}$ ist Isomorphismus.

R6.8 [Frühjahr 1994] Sei R ein noetherscher kommutativer Ring mit Eins, und sei $f : R \to R$ ein Ringendomorphismus. Zeigen Sie:

$$f \text{ surjektiv} \quad \Longrightarrow \quad f \text{ injektiv} \quad .$$

HINWEIS: Betrachten Sie die Folge $f, f^2, f^3, \ldots$

Nichtnoethersche Ringe

R6.9 [Herbst 1997] Sei $R = \{f \in \mathbb{R}[X] \,;\; f(0) \in \mathbb{Q}\}$ der Ring aller Polynome mit reellen Koeffizienten, deren konstantes Glied rational ist. Zeigen Sie:

a) Das Element X ist im Ring R unzerlegbar, aber kein Primelement.

b) Jede aufsteigende Folge $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ von Hauptidealen wird stationär.

c) Das Ideal $I = \{f \in R \,;\; f(0) = 0\}$ von R ist nicht endlich erzeugt.

Staatsexamensaufgaben zur Körpertheorie

Inhalt

0. Vermischtes

K0.1 [Herbst 1982] Geben Sie in den folgenden Fällen ein Beispiel an oder begründen Sie kurz, weshalb es kein solches Beispiel gibt:

a) eine endliche separabel algebraische Körpererweiterung, die unendlich viele verschiedene Zwischenkörper besitzt;

b) für jede natürliche Zahl $n > 0$ eine galoissche Körpererweiterung vom Grad n, deren Galoisgruppe die symmetrische Gruppe n-ten Grades ist;

c) eine inseparable Körpererweiterung von $\mathbb{Q}$;

d) ein erzeugendes Element der Automorphismengruppe des Körpers $\mathbb{F}_q$ mit q Elementen;

e) einen endlichen algebraisch abgeschlossenen Körper.

K0.2 [Herbst 2003] Begründen oder widerlegen Sie folgende Aussagen:

a) Ist p eine Primzahl, sind $1 \leq i \leq j$ natürliche Zahlen, sind K bzw. L Körper mit p^i bzw. p^j Elementen, so ist K zu einem Teilkörper von L isomorph.

b) Für jede Primzahl p und jede natürliche Zahl a gilt: Ist $X^2 \equiv a \bmod p$ lösbar in $\mathbb{Z}$, so auch $X^4 \equiv a \bmod p$.

c) Die Zahl $\zeta_{13} = e^{2\pi i/13}$ ist mit Zirkel und Lineal konstruierbar.

d) Seien $\alpha_1, \alpha_2 \in \mathbb{C}$ algebraische Zahlen, sei $K_i = \mathbb{Q}(\alpha_i)$ für $i = 1, 2$, sei $L = \mathbb{Q}(\alpha_1, \alpha_2)$ und es gelte $K_1 \cap K_2 = \mathbb{Q}$. Dann gilt

$$[L : \mathbb{Q}] \quad \text{teilt} \quad [K_1 : \mathbb{Q}] \cdot [K_2 : \mathbb{Q}] \quad .$$

1. Elementare Körpertheorie

K1.1 [Herbst 2001] Sei $L|K$ eine Körpererweiterung. Eine K-lineare Abbildung $d: L \to L$ heißt *Derivation* von $L|K$, wenn für alle $a, b \in L$ die Produktregel $d(ab) = ad(b) + bd(a)$ erfüllt ist. Zeigen Sie, dass für ein solches d die folgenden Aussagen richtig sind:

a) $d(a) = 0$ für alle $a \in K$.

b) Ist $f \in K[X]$ ein Polynom und $a \in L$, so gilt $d(f(a)) = f'(a)da$ mit der Ableitung f' von f.

c) $Z := \ker d := \{a \in L;\ d(a) = 0\}$ ist ein Zwischenkörper von $L|K$.

d) Ist $a \in L$ separabel algebraisch über Z, so ist $a \in Z$.

e) Ist L ein endlicher Körper und K sein Primkörper, so ist d die Nullabbildung.

K1.2 [Frühjahr 1987] Man entscheide, ob die folgenden Aussagen richtig oder falsch sind und begründe die Antwort.

a) Der Körper $\mathbb{Q}$ der rationalen Zahlen besitzt echte Teilkörper.

b) Jedes nicht konstante irreduzible Polynom über $\mathbb{Q}$ hat nur einfache Nullstellen in $\mathbb{C}$.

c) Ist $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit den Nullstellen $\alpha, \beta \in \mathbb{C}$, so gilt $\beta \in \mathbb{Q}(\alpha)$.

d) Das direkte Produkt $\mathbb{R} \times \mathbb{R}$ des Körpers $\mathbb{R}$ mit sich selbst ist ein zu $\mathbb{C}$ isomorpher Körper.

Endliche Körpererweiterungen

K1.3 [Herbst 1982] Zeigen Sie: Jede quadratische Erweiterung von $\mathbb{Q}$ hat die Form $\mathbb{Q}(\sqrt{d})$ mit einer eindeutig bestimmten quadratfreien ganzen Zahl d.

K1.4 [Herbst 1994] Gegeben seien $a, b \in \mathbb{Q}^\times$. Zeigen Sie: Wenn es einen Körperisomorphismus

$$\varphi: \ \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$$

gibt, dann gilt $\frac{a}{b} \in (\mathbb{Q}^\times)^2$.

K1.5 [Herbst 1988] $L|K$ sei eine Körpererweiterung. Es gebe ein $x \in L$ mit $L = K[x]$. Zeigen Sie, daß $L|K$ algebraisch ist.

K1.6 [Herbst 1997] Sei $K \subset L$ eine endliche Körpererweiterung und $f \in K[X]$ ein irreduzibles nichtlineares Polynom mit

$$\mathrm{ggT}(\mathrm{grad}\, f,\ [L:K]) = 1 \quad .$$

Zeigen Sie, daß f keine Nullstelle in L hat.

K1.7 [Herbst 1989] Sei $z \in \mathbb{C}$ eine algebraische Zahl, also eine solche, die Nullstelle eines von 0 verschiedenen Polynoms aus $\mathbb{Q}[X]$ ist.
Man beweise: Auch $\mathrm{Re}(z)$ und $|z|$ sind algebraische Zahlen.

K1.8 [Frühjahr 1979] Es sei $L|K$ eine endliche Körpererweiterung. Die Charakteristik von K sei kein Teiler des Grades $[L:K]$. Beweisen Sie, daß $L|K$ separabel ist.

K1.9 [Frühjahr 1985] Berechne die Grade der folgenden Körpererweiterungen in $\mathbb{R}$ bzw. $\mathbb{C}$:

a) $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[7]{40}\right)$.

b) $\mathbb{Q}(i) \subset \mathbb{Q}\left(e^{\pi i/8}\right)$.

K1.10 [Herbst 1980] L sei ein algebraischer Erweiterungskörper eines Körpers K. Zeigen Sie: Ist R ein Ring mit $K \subset R \subset L$, so ist R ein Körper.

K1.11 [Herbst 1998] Sei $K|k$ eine algebraische Körpererweiterung. Seien $\alpha_1, \ldots, \alpha_n$ Elemente aus K und seien $f_1(X), \ldots, f_n(X)$ die zugehörigen Minimalpolynome über k. Beweisen Sie

$$\left[k(\alpha_1, \ldots, \alpha_n) : k\right] \leq \prod_{i=1}^{n} \operatorname{grad} f_i \quad .$$

K1.12 [Frühjahr 2003] Sei K eine algebraische Erweiterung des Körpers k und R ein Ring mit $k \subset R \subset K$. Folgt dann, dass R ein Körper ist?

K1.13 [Frühjahr 1996] Sei L Erweiterungskörper eines unendlichen Körpers K mit $[L : K] < \infty$. Man beweise: Besitzt die Erweiterung $L|K$ nur eine endliche Zahl von Zwischenkörpern, so ist $L|K$ einfach.

K1.14 [Frühjahr 1997] Zeigen Sie: Ist $L|K$ eine (nicht notwendig endliche) separabel algebraische Körpererweiterung, für die es ein $n \in \mathbb{N}$ gibt mit $[K(x) : K] \leq n$ für alle $x \in L$, dann ist $[L : K] \leq n$.

Primzahlcharakteristik

K1.15 [Herbst 1974] Sei K ein Körper der Charakteristik $p \neq 0$ und L ein beliebiger Körper. Es bezeichne K^+ die additive Gruppe von K und $L^\times$ die multiplikative Gruppe von L.

Beweisen Sie, daß K^+ und $L^\times$ genau dann isomorph sind, wenn die folgende Bedingung gilt: Der Körper K ist der Primkörper mit p, und L der Körper mit $p+1$ Elementen; dabei ist p entweder gleich 2 oder eine Mersennesche Primzahl.

K1.16 [Herbst 1976] Es sei p eine Primzahl, K ein Körper der Charakteristik p und α aus einem Erweiterungskörper von K. Man zeige:

a) $K(\alpha^p) \subseteq K(\alpha)$.

b) Falls $\alpha^k \in K(\alpha^p)$ für ein k mit $1 \leq k < p$, dann gilt bereits $\alpha \in K(\alpha^p)$.

c) Ist das Polynom $x^p - \alpha^p \in K(\alpha^p)[x]$ reduzibel, so folgt $\alpha \in K(\alpha^p)$ (x bezeichnet die Unbestimmte).

HINWEIS: Man betrachte die Zerlegung über $K(\alpha^p)$ auch als Zerlegung über $K(\alpha)$.

d) $\alpha \notin K(\alpha^p) \implies [K(\alpha) : K(\alpha^p)] = p$.

K1.17 [Herbst 1986] K sei ein Körper der Charakteristik $p \neq 0$ und M ein Erweiterungskörper von K. Für zwei Elemente $u, w \in M$ gelte $u^p, w^p \in K$ und $[K(u, w) : K] = p^2$. Zeigen Sie, daß die Körpererweiterung $K(u, w)|K$ kein primitives Element besitzt.

K1.18 [Herbst 1986] K sei ein Körper und $f \in K[X]$ ein normiertes irreduzibles Polynom. Sei α eine Nullstelle von f in einem Erweiterungskörper von K, und es sei auch $f(\alpha+1)=0$. Zeigen Sie:

a) K hat positive Charakteristik.

b) Ist p die Charakteristik von K und zudem $\alpha^p-\alpha \in K$, so ist $f = X^p - X - \alpha^p + \alpha$, und $K(\alpha)|K$ ist galoissch mit zyklischer Galoisgruppe.

K1.19 [Herbst 1995] Sei K ein Körper der Charakteristik $p>0$ und $f \in K[X]$ ein nichtkonstantes irreduzibles Polynom. Man beweise:

a) f ist genau dann separabel, wenn die Ableitung $Df \neq 0$ ist.

b) Ist f nicht separabel, so gibt es ein Polynom $g \in K[X]$ mit $f(X) = g(X^p)$.

c) Jede endliche Körpererweiterung von K ist separabel $\iff$ Der Frobenius-Homomorphismus von K ist ein Automorphismus.

Minimalpolynome

K1.20 [Herbst 1979] Sei $K|k$ eine endliche Körpererweiterung vom Grad n. Für jedes Element $\alpha \in K$ ist

$$\begin{aligned} \ell(\alpha): \ K &\to K \\ x &\mapsto \alpha x \end{aligned}$$

ein Endomorphismus des k-Vektorraums K. Vermöge $\alpha \mapsto \ell(\alpha)$ erhält man einen injektiven Homomorphismus $\ell: K \to \mathrm{End}_k(K)$ von k-Algebren.
Für $\alpha \in K$ sei $\chi(X)$ das charakteristische Polynom des Endomorphismus $\ell(\alpha): K \to K$, also $\chi(X) = \det(X \cdot \mathrm{id}_K - \ell(\alpha))$. Dann ist $\chi(X)$ ein normiertes Polynom n-ten Grades mit Koeffizienten aus k. Man nennt $\chi(X)$ auch das *charakteristische Polynom* von α für $K|k$. Man beweise:

a) $\chi(\alpha)=0$.

b) Ist $q(X) \in k[X]$ das (normierte) Minimalpolynom von α über k, so gilt

$$\chi(X) = q(X)^{[K:k(\alpha)]} \quad .$$

c) Schreibt man $\chi(X) = X^n - \mathrm{tr}_{K|k}(\alpha)X^{n-1} + \ldots$, so heißt das Element $\mathrm{tr}_{K|k}(\alpha) \in k$ die *Spur von* α für $K|k$. Man zeige:

$$\begin{aligned} \mathrm{tr}_{K|k}(\alpha+\beta) &= \mathrm{tr}_{K|k}(\alpha) + \mathrm{tr}_{K|k}(\beta) \\ \mathrm{tr}_{K|k}(a\cdot\alpha) &= a \cdot \mathrm{tr}_{K|k}(\alpha) \\ \mathrm{tr}_{K|k}(a) &= [K:k]\cdot a \end{aligned}$$

für $\alpha, \beta \in K$ und $a \in k$.

K1.21 [Herbst 1994] Sei $L|K$ eine endliche Körpererweiterung und $\alpha \in L$. Multiplikation mit α auf L definiert eine K-lineare Abbildung $\varphi_\alpha: L \to L$. Sei χ_α das charakteristische Polynom dieses K-Vektorraumhomomorphismus. Zeigen Sie: χ_α ist eine Potenz des Minimalpolynoms P_α von α.

K1.22 [Herbst 1994]

a) Sei $k(a)|k$ eine endliche Körpererweiterung. Für einen Teilkörper L, $k(a) \supset L \supset k$, sei $m_{a,L}(X)$ das Minimalpolynom von a über L. Man zeige:

$$m_{a,L}(X) \mid m_{a,k}(X) \quad .$$

b) Man bestimme den Grad und alle Zwischenkörper von $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$.

K1.23 [Herbst 1989] Sei L eine algebraische Erweiterung des Körpers K. Sei $f(X) \in L[X]$ vom Grad ≥ 1. Man beweise:
Es gibt ein $g(X) \in K[X]$ vom Grad ≥ 1 mit $f(X) \mid g(X)$. Ist $f(X)$ irreduzibel, dann gibt es genau ein normiertes irreduzibles $g(X) \in K[X]$ mit $f(X) \mid g(X)$.

K1.24 [Herbst 1981] Sei $f : \mathbb{C}^n \to \mathbb{C}^n$ eine $\mathbb{C}$-lineare Abbildung mit n verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_n$. Wie sehen die $2n$ Eigenwerte von f aus, wenn man f als $\mathbb{R}$-lineare Abbildung eines $\mathbb{R}$-Vektorraums der Dimension $2n$ interpretiert?

K1.25 [Herbst 1979] Es seien $f := X^3 - 2 \in \mathbb{Q}[X]$ und $g := X^2 - 7 \in \mathbb{Q}[X]$.

a) Man zeige: f und g sind in $\mathbb{Q}[X]$ irreduzibel.

b) Welche der folgenden Ideale in $\mathbb{Q}[X]$ sind maximal: (f), $(f \cdot g)$, (f, g) ?
Dabei bezeichnet $(f) := \{hf \in \mathbb{Q}[X];\ h \in \mathbb{Q}[X]\}$ das von f in $\mathbb{Q}[X]$ erzeugte Ideal und $(f, g) := \{h_1 f + h_2 g \in \mathbb{Q}[X];\ h_1, h_2 \in \mathbb{Q}[X]\}$ das von f, g in $\mathbb{Q}[X]$ erzeugte Ideal.

c) Man bestimme die Grade

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \quad \text{und} \quad [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] \quad .$$

d) Sei $\beta := \sqrt[3]{2} \cdot \sqrt{7}$. Man zeige, daß gilt:

$$\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{7}) \quad .$$

Man bestimme den Grad $[\mathbb{Q}(\beta) : \mathbb{Q}]$ und gebe das Minimalpolynom von β über $\mathbb{Q}$ an.

K1.26 [Herbst 1992] Zeigen Sie durch Gradbetrachtung einer geeigneten Erweiterung von $\mathbb{Q}$, daß der Grad des Minimalpolynoms der komplexen Zahl

$$z := \frac{\sqrt{2} + \sqrt{3} + i\sqrt{3}}{\sqrt{5} + \sqrt{7} + i\sqrt{7}}$$

über $\mathbb{Q}$ ein Teiler von 32 ist.

K1.27 [Herbst 2001] Si $\alpha = \sqrt{2 + \sqrt[3]{2}} \in \mathbb{R}$ die positive Quadratwurzel von $2 + \sqrt[3]{2} \in \mathbb{R}$.

a) Bestimmen Sie das Minimalpolynom $f(x)$ von α über $\mathbb{Q}$ und den Grad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

b) Geben Sie alle Nullstellen von $f(x)$ in $\mathbb{C}$ an. Ist $\mathbb{Q}(\alpha)$ ein Zerfällungskörper von $f(x)$?

Rechnen im Wurzelkörper

K1.28 [Herbst 1995] Sei K ein Körper und $f \in K[X]$ ein nicht-konstantes irreduzibles Polynom. Man beweise (ohne Benutzung des Satzes über den Zerfällungskörper oder des Satzes über den algebraischen Abschluß), daß f in einer geeigneten Körpererweiterung eine Nullstelle besitzt.

K1.29 [Frühjahr 1980] Sei f das Polynom $X^3 - X + 1$ aus $\mathbb{Q}[X]$.

a) Zeigen Sie, daß f irreduzibel in $\mathbb{Q}[X]$ ist.

b) Sei $\mathbb{Q}(\alpha)$ eine einfache algebraische Erweiterung von $\mathbb{Q}$, wobei f das Minimalpolynom von α über $\mathbb{Q}$ ist. Ferner sei $a := 2 - 3\alpha + 2\alpha^2$. Stellen Sie a^{-1} als Linearkombination der Potenzen von α mit Koeffizienten aus $\mathbb{Q}$ dar.

K1.30 [Frühjahr 1996]

a) Zeigen Sie, daß $f := X^3 - X + 1 \in \mathbb{Q}[X]$ keine Nullstelle in $\mathbb{Q}$ hat.

b) Sei $z \in \mathbb{C}$ eine Nullstelle von f. Stellen Sie z^{-1} als Linearkombination von $1, z, z^2$ mit rationalen Koeffizienten dar.

c) Bestimmen Sie das Minimalpolynom von z^2 über $\mathbb{Q}$.

K1.31 [Frühjahr 1995] Sei $f(X) = X^3 + 2X + 2 \in \mathbb{Q}[X]$, und sei α eine komplexe Nullstelle von f.

a) Zeigen Sie, daß $1, \alpha, \alpha^2$ eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\alpha)$ ist.

b) Schreiben Sie $(1+\alpha)^{-1}$ als Linearkombination mit rationalen Koeffizienten bezüglich dieser Basis.

K1.32 [Frühjahr 1984]

a) Zeigen Sie: $f(X) = X^4 - X - 1$ ist irreduzibel über $\mathbb{Q}$.

b) Für $a \in \mathbb{C}$ sei $f(a) = 0$. Stellen Sie $b = (1 + a^2)^{-1}$ als Polynom in a dar!

c) Bestimmen Sie das Minimalpolynom von b über $\mathbb{Q}$!

K1.33 [Herbst 1985] Sei K ein Körper und $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein irreduzibles normiertes Polynom vom Grade $n > 1$. Sei L ein Erweiterungskörper von K.

a) Sei $\mathrm{char}(K) \neq 2$ und $\alpha \in L$ mit $f(\alpha) = f(-\alpha) = 0$. Man zeige:

$$f(X) = g(X^2) \quad \text{mit} \quad g \in K[X] \quad .$$

b) Sei $a_{n-i} = a_i$ für alle $i = 0, 1, \ldots, n$. Man zeige: Ist $\alpha \in L$ und $f(\alpha) = 0$, so gibt es ein $\beta \in L$, $\alpha \neq \beta$, mit $f(\beta) = 0$.

Zerfällungskörper

K1.34 [Frühjahr 1980] Sei K ein Körper. Zeigen Sie: Jede Erweiterung von K vom Grade 2 ist normal über K.

K1.35 [Herbst 1980] Sei K ein Körper, $f \in K[X]$ ein Polynom vom Grad $n \geq 1$ über K und L sei ein Zerfällungskörper von f über K. Zeigen Sie, daß für den Grad $[L : K]$ von L über K die folgende Abschätzung gilt:

$$[L : K] \leq n! \qquad (= n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1)$$

K1.36 [Frühjahr 1981] Bestimme den Zerfällungskörper K von $X^3 - 7$ über $\mathbb{Q}$, sowie $[K : \mathbb{Q}]$.

K1.37 [Herbst 2002]

a) Zerlegen Sie das Polynom $f := X^6 + 4X^4 + 4X^2 + 3 \in \mathbb{Q}[X]$ in irreduzible Faktoren.

b) Bestimmen Sie den Zerfällungskörper Z von f über $\mathbb{Q}$ und $[Z : \mathbb{Q}]$.

K1.38 [Frühjahr 1984] Es seien K ein Körper der Charakteristik 0, $f \in K[X]$ ein normiertes irreduzibles Polynom und α, β Nullstellen von f in einem geeigneten Erweiterungskörper von K. Es sei $\gamma := \alpha - \beta \in K$. Zeigen Sie:

a) $f(X + \gamma)$ ist normiert und irreduzibel in $K[X]$.

b) Für jede natürliche Zahl n gilt $f(X + n\gamma) = f$.

c) $\alpha = \beta$.

Satz vom primitiven Element

K1.39 [Herbst 1997] Sei $L|K$ eine endliche galoissche Erweiterung mit Galoisgruppe G. Sei H eine Untergruppe von G. Zeigen Sie, daß es ein $\ell \in L$ gibt mit $H = \{g \in G\,;\; g(\ell) = \ell\}$.

K1.40 [Frühjahr 2001] Bestimmen Sie alle Teilkörper eines Zerfällungskörpers E des Polynoms

$$(x^3 - 3x + 1)(x^2 + 2)$$

über $\mathbb{Q}$ und ein primitives Element von $E|\mathbb{Q}$.

K1.41 [Frühjahr 2000]

a) Man bestimme ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$.

b) Seien x und y Unbestimmte über dem Körper $\mathbb{F}_p$ von p Elementen. Man zeige: Die Körpererweiterung $\mathbb{F}_p(x, y)|\mathbb{F}_p(x^p, y^p)$ besitzt kein primitives Element.

Angeordnete Körper

K1.42 [Frühjahr 1977] Das Paar (R, P) heißt *angeordneter Ring*, falls R ein Ring und P eine Teilmenge von R mit folgenden Eigenschaften ist:

(i) Für alle $a \in R$ mit $a \neq 0$ gilt entweder $a \in P$ oder $-a \in P$. Es gilt $0 \notin P$.

(ii) Für alle $a, b \in P$ gilt $a + b \in P$ und $ab \in P$.

Zeigen Sie:

a) Ist (R, P) ein angeordneter Integritätsbereich (d.h. ein angeordneter kommutativer nullteilerfreier Ring) mit mindestens zwei Elementen, so gibt es genau eine Teilmenge P' des Quotientenkörpers K von R derart, daß (K, P') ein angeordneter Körper ist und $P' \cap R = P$ gilt. (Man beachte, daß R auf natürliche Weise in K eingebettet ist.)

b) Es gibt genau eine Teilmenge P des Körpers $\mathbb{Q}$ der rationalen Zahlen derart, daß $(\mathbb{Q}, P)$ ein angeordneter Körper ist.

c) Es gibt keine Teilmenge P des Körpers $\mathbb{C}$ der komplexen Zahlen derart, daß $(\mathbb{C}, P)$ ein angeordneter Körper ist.

d) Jeder Automorphismus φ des Körpers $\mathbb{R}$ der reellen Zahlen führt positive Zahlen in positive über.

e) Ist φ ein Automorphismus des Körpers $\mathbb{R}$, so ist φ die Identität.

K1.43 [Frühjahr 1983] Ein Körper K heißt *angeordnet*, wenn für Elemente aus K eine Relation > 0 erklärt ist, so daß folgende Axiome erfüllt sind:

i) Für alle $a \in K$ gilt genau eine der drei Aussagen

$$a > 0 \quad , \quad a = 0 \quad , \quad -a > 0 \quad .$$

ii) Aus $a > 0,\ b > 0$ folgt $a + b > 0$ und $a \cdot b > 0$ $(a, b \in K)$.

Zeigen Sie:

a) In einem angeordneten Körper ist $a^2 > 0$ für jedes $a \neq 0$.

b) Ein angeordneter Körper besitzt die Charakteristik 0.

c) Ein algebraisch abgeschlossener Körper läßt sich auf keine Weise zu einem angeordneten Körper machen.

d) Der Körper $\mathbb{R}(X)$ der rationalen Funktionen in einer Variablen X über $\mathbb{R}$ wird zu einem angeordneten Körper, wenn für $f \in \mathbb{R}(X)$ die Relation $f > 0$ durch folgende Bedingung erklärt wird:

Es gibt ein $M \in \mathbb{R}$, so daß $f(a) > 0$ für alle $a \in \mathbb{R}$ mit $a > M$.

e) Ist in $\mathbb{R}(X)$ mit der in d) erklärten Anordnung das Archimedische Axiom erfüllt, d.h. gibt es für alle $f, g \in \mathbb{R}(X)$ mit $f > 0$, $g > 0$ stets ein $n \in \mathbb{N}$ mit $nf - g > 0$?

K1.44 [Frühjahr 1979]

a) Zeigen Sie, daß genau eine Ordnungsrelation $<$ auf dem Körper $\mathbb{Q}(t)$ der rationalen Funktionen über dem Körper $\mathbb{Q}$ der rationalen Zahlen existiert, so daß $(\mathbb{Q}(t), <)$ ein angeordneter Körper ist, in dem ein jedes Polynom $a_0 + a_1 t + \ldots + a_n t^n \in \mathbb{Q}[t]$ mit $a_n \neq 0$ genau dann positiv ist, wenn a_n in $\mathbb{Q}$ positiv ist. (Vergessen Sie nicht zu zeigen, daß die Relation $<$ wohldefiniert ist.)

b) Zeigen Sie: Die in a) bestimmte Anordnung von $\mathbb{Q}(t)$ ist nicht archimedisch.

2. Endliche Körper

Allgemeine Theorie

K2.1 [Frühjahr 1973] Sei K ein Körper mit endlich vielen Elementen. Zeige:

a) Die Elementezahl von K ist p^n, wobei p die Charakteristik von K und n eine natürliche Zahl ist.

b) Sei P der Primkörper von K, dann ist K galoissch über P.

c) Die Galoisgruppe von K über P ist zyklisch.

HINWEIS: Benutze den Automorphismus $K \ni k \mapsto k^p \in K$.

d) K ist vollkommen, d.h. K besitzt keine inseparablen Erweiterungen.

K2.2 [Frühjahr 1978] Sei K ein Körper mit endlich vielen Elementen. Zeige:

a) Es gibt eine Primzahl p, so daß K einen zu $\mathbb{Z}/p\mathbb{Z}$ isomorphen Unterkörper hat (= Primkörper P).

b) Die Elementezahl von K ist p^n, wobei p die Charakteristik von K und n eine natürliche Zahl ist.

c) Sei P der Primkörper von K, dann ist K galoissch über P.

d) Die Galoisgruppe von K über P ist zyklisch.

HINWEIS: Benutze den Automorphismus $K \ni k \mapsto k^p \in K$.

e) K ist vollkommen, d.h. K besitzt keine inseparablen Oberkörper endlicher Dimension über K.

K2.3 [Herbst 1973] Es sei K ein endlicher Körper. Die Anzahl der Elemente einer Menge A wird mit $|A|$ bezeichnet. Man beweise die folgenden Aussagen:

a) Die Charakteristik von K ist eine Primzahl p.

b) Der Primkörper P von K ist isomorph $\mathbb{Z}/p\mathbb{Z}$.

c) $|K| = p^n$ mit $n = [K : P]$.
(Mit $[K : P]$ ist der Grad von K über P bezeichnet.)

d) Für jedes Element $a \in K$ gilt:

$$a^q - a = 0 \quad \text{mit} \quad q = p^n \quad .$$

e) K ist ein Zerfällungskörper von $x^q - x \in P[x]$ über P.

f) Zwei endliche Körper von gleicher Elementeanzahl sind isomorph.

g) Zu jeder Primzahlpotenz p^n, $n \in \mathbb{N}$, gibt es einen Körper mit p^n Elementen.

h) Der algebraische Abschluß von K hat unendlichen Grad über K.

i. Die additive Gruppe von K ist isomorph einer direkten Summe von n zyklischen Gruppen, von denen jede die Ordnung p hat.

j) Die multiplikative Gruppe $K^\times$ von K ist zyklisch.

HINWEIS: Es gilt die Aussage $(*)$ „In einer endlichen abelschen Gruppe gibt es zu zwei Elementen a, b stets ein Element c mit $\operatorname{ord} c = \operatorname{kgV}(\operatorname{ord} a, \operatorname{ord} b)$.“

Diese Aussage soll nicht bewiesen werden. Man zeige mit $(*)$, daß für $j = \mathrm{Max}\{\,\mathrm{ord}\,a\,;\ a \in K^*\}$ gilt: $a^j = e$ für jedes $a \in K^*$, also $a^{j+1} = a$ für jedes $a \in K$.

k) K ist eine einfache Körpererweiterung von P.

l) i. Für jedes $i \in \mathbb{N}$ ist $\sigma_i = (a \mapsto a^{p^i})$ ein Automorphismus von K.

ii. $\Sigma = \{\sigma_i\,;\ i \in \mathbb{N}\}$ ist eine zyklische Untergruppe der Automorphismengruppe Γ von K mit $|\Sigma| = n$.

iii. Γ ist die Galoisgruppe von K über P, und Γ ist zyklisch von der Ordnung n.

m) Für einen Unterkörper U von K gilt:

i. $|U| = p^m$ mit m ist ein Teiler von n.

ii. Die Galoisgruppe von K über U ist zyklisch.

n) Zu jedem Teiler m von n gibt es genau einen Unterkörper U von K mit $|U| = p^m$.

K2.4 [Frühjahr 1979] Skizzieren Sie den Beweis des folgenden Satzes: Die Elementezahl eines endlichen Körpers ist eine Primzahlpotenz, ferner gibt es zu jeder Zahl p^n (p Primzahl, $n \in \mathbb{Z}$, $n > 0$) einen (und bis auf Isomorphie nur einen) Körper mit p^n Elementen.

K2.5 [Herbst 1999] Der Körper K enthalte einen endlichen Teilkörper, der aus den n Elementen $a_1, \ldots, a_n$ bestehe. Man beweise: Für jedes Element $a \in K$ gilt

$$a^n - a = \prod_{i=1}^{n} (a - a_i) \quad .$$

K2.6 [Frühjahr 1982]

a) Man gebe unendlich viele nichtisomorphe kommutative Ringe mit Eins an, die genau 2 bzw. 3 bzw. 4 Einheiten besitzen.

b) Man zeige, daß kein kommutativer Ring mit Eins genau 5 Einheiten besitzt.

K2.7 [Frühjahr 2001] Sei $\mathbb{F}_q$ ein Körper mit q Elementen und sei $n \in \mathbb{N}$ teilerfremd zu q. Sei K ein Zerfällungskörper von $X^n - 1$ über $\mathbb{F}_q$. Man zeige

$$[K : \mathbb{F}_q\,] = \min\{k \in \mathbb{N}\,;\ n \text{ teilt } q^k - 1\} \quad .$$

K2.8 [Frühjahr 1979] Es sei K ein endlicher Körper mit q Elementen, L sei der Zerfällungskörper von $x^n - 1$ über K und es sei $m = [L : K]$.
Zeigen Sie, daß m die kleinste natürliche Zahl ist, für die $n \mid q^m - 1$ gilt.

K2.9 [Herbst 1995] Es sei F ein endlicher Körper und $\overline{F}$ sein algebraischer Abschluß. Bekanntlich gibt es für jede natürliche Zahl n genau einen Zwischenkörper von $\overline{F}|F$, der über F den Grad n hat. Es sei n eine natürliche Zahl und $f \in F[X]$ irreduzibel vom Grad n.
Zeigen Sie, daß der Zerfällungskörper von f über F den Grad n über F hat.

Quadratische Gleichungen

K2.10 [Frühjahr 2003] Sei K ein Körper mit vier Elementen.
Bestimmen Sie eine Additions- und eine Multiplikationstafel von K.

K2.11 [Frühjahr 1974] Es sei p eine Primzahl und $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Man zeige:

a) Ein Zerfällungskörper K von $x^{p^2} - x \in \mathbb{Z}_p[x]$ hat p^2 Elemente.

b) Die additive Gruppe K^+ von K ist einer direkten Summe von zwei zyklischen Gruppen der Ordnung p isomorph.

K2.12 [Herbst 1977] Sei $K = \mathbb{Z}/2\mathbb{Z}$ der Körper mit 2 Elementen und $f = x^2 + x + 1 \in K[x]$.

a) Zeige, daß f irreduzibel in $K[x]$ ist.

b) Sei (f) das von f in $K[x]$ erzeugte Ideal. Bestimme die Elemente von $K[x]/(f)$, ihre Addition und ihre Multiplikation.

K2.13 [Herbst 1977] Sei $K = \mathbb{F}_q$. Man zeige: Ist q gerade oder $q \equiv 1 \mod 4$, so gibt es ein $x \in K$ mit $x^2 = -1$.

K2.14 [Herbst 1985] Sei p eine von 2 verschiedene Primzahl, $q = p^n$ mit $1 \leq n \in \mathbb{N}$ und sei $\mathbb{F}_q$ ein Körper mit q Elementen.

a) Sei $-1 \in \mathbb{F}_q^2$ ein Quadrat. Man zeige: $\sum_{x \in \mathbb{F}_q^2} x = 0$.

b) Man charakterisiere durch Kongruenzen für p und n die Potenzen q mit der Eigenschaft, daß $-1 \in \mathbb{F}_q^2$ gilt.

K2.15 [Frühjahr 1999] Bekanntlich kann man den Körper der komplexen Zahlen aus dem Körper $K := \mathbb{R}$ der reellen Zahlen wie folgt gewinnen: Man führe auf der Menge $C(K) := K \times K$ aller Paare von Elementen von K folgende Addition und Multiplikation ein:

$$(x, y) + (x', y') := (x + x', y + y') \quad ,$$
$$(x, y) \cdot (x', y') := (xx' - yy', xy' + yx') \quad .$$

Für einen beliebigen Körper K ist $C(K)$ mit den obigen Verknüpfungen nicht notwendig ein Körper, jedoch stets ein kommutativer Ring mit Einselement (dies braucht nicht bewiesen zu werden).

a) Für welche Primzahlen p ist $C(\mathbb{F}_p)$ ein Körper? (Dabei ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen.) (Begründung!)

b) Man zeige: Ist p eine ungerade Primzahl und $C(\mathbb{F}_q)$ kein Körper, so gibt es einen Ring-Isomorphismus

$$C(\mathbb{F}_p) \simeq \mathbb{F}_p \times \mathbb{F}_p \quad ,$$

wobei die Ringstruktur auf $\mathbb{F}_p \times \mathbb{F}_p$ durch komponentenweise Addition und Multiplikation gegeben sei.

c) Ist folgende Aussage richtig: Für eine ungerade Primzahl p ist $C(\mathbb{F}_p)$ genau dann ein Körper, wenn die multiplikative Gruppe $C(\mathbb{F}_p)^\times$ der Einheiten von $C(\mathbb{F}_p)$ zyklisch ist? (Begründung!)

K2.16 [Frühjahr 2002] Sei $\mathrm{M}_2(\mathbb{F}_3)$ der Ring der 2×2-Matrizen mit Koeffizienten im Körper $\mathbb{F}_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

a) Man zeige, dass es ein $\alpha \in \mathrm{M}_2(\mathbb{F}_3)$ gibt mit Ordnung 8 bezüglich der Multiplikation.

b) Man zeige, dass $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^7\}$ ein Körper ist mit den von $\mathrm{M}_2(\mathbb{F}_3)$ induzierten Operationen.

K2.17 [Herbst 1977] Sei K ein endlicher Körper mit q Elementen. Man zeige:

a) Ist q gerade, so gibt es zu jedem $y \in K$ genau ein $x \in K$ mit $y = x^2$ (Man betrachte die Abbildung $K \to K\,,\ x \mapsto x^2$).

b) Ist q ungerade, so ist die Abbildung

$$\varphi:\ K \setminus \{0\} \to K \setminus \{0\} \qquad , \qquad x \mapsto x^{\frac{q-1}{2}}$$

ein Gruppenhomomorphismus mit

$$\mathrm{Bild}(\varphi) = \{1, -1\} \quad , \quad \mathrm{Kern}(\varphi) = \{x \in K \setminus \{0\};\ \text{es gibt } y \in K \setminus \{0\} \ \text{ mit } \ y^2 = x\} \quad .$$

(Es darf benutzt werden, daß die multiplikativen Gruppen endlicher Körper zyklisch sind.)

K2.18 [Herbst 1996] Gegeben sei das Polynom

$$f(X) = (X^2 - 2)(X^2 - 3)(X^2 - 6)$$

in $\mathbb{Z}[X]$. Man zeige: Für jede Primzahl p hat die Reduktion $f(X)$ mod p eine Nullstelle in $\mathbb{F}_p$. Hingegen hat $f(X)$ keine Nullstelle in $\mathbb{Q}$.

K2.19 [Herbst 1987] Sei p eine Primzahl und $n \geq 1$ eine ganze Zahl.

a) Begründen Sie, warum alle Körper mit p^n Elementen isomorph sind.

b) Geben Sie explizit einen Körper K und ein Polynom f an, so daß der Faktorring $K[X]/(f)$ ein Körper mit 8 Elementen ist.

c) Zeigen Sie, daß eine der Gleichungen $x^2 = 2$ oder $x^2 = -2$ im Körper $\mathbb{Z}/p\mathbb{Z}$ lösbar ist, falls $p \notin \{4k + 1\,;\ k \in \mathbb{N}\}$.

Kubische Gleichungen

K2.20 [Frühjahr 1979] Es sei L ein Zerfällungskörper von $x^3 - 2$ über $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.

a) Welchen Grad hat L über $\mathbb{F}_5$?

b) Man begründe, weshalb L über $\mathbb{F}_5$ galoissch ist.

c) Man bestimme die Galoisgruppe $\mathrm{Gal}(L|\mathbb{F}_5)$ von L über $\mathbb{F}_5$ bis auf Isomorphie.

K2.21 [Herbst 2002] Über dem Körper $\mathbb{F}_2$ mit zwei Elementen seien die Polynome

$$p(X) = X^3 + X + 1 \quad \text{und} \quad q(X) = X^3 + X^2 + 1$$

gegeben. Zeigen Sie:

a) p und q sind die einzigen irreduziblen Polynome in $\mathbb{F}_2[X]$ vom Grad 3.

b) Ist Z der Zerfällungskörper von p über $\mathbb{F}_2$ und $a \in Z$ eine Nullstelle von p, so sind a^2 und a^4 die beiden anderen Nullstellen von p.

c) Z besteht genau aus den Elementen $0, 1$, den drei Nullstellen a, a^2, a^4 von p und den drei Nullstellen a^3, a^5, a^6 von q in Z.

K2.22 [Herbst 1979]

a) Man zerlege $X^3 - 1 \in \mathbb{F}_2[X]$ in irreduzible Faktoren ($\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ bezeichnet einen Körper mit 2 Elementen).

b) Es sei $L \supset \mathbb{F}_2$ ein Zerfällungskörper von $X^3 - 1 \in \mathbb{F}_2[X]$. Man zeige: Es gibt ein $\zeta \in L$ mit $\mathbb{F}_2(\zeta) = L$ und L besteht aus 4 Elementen (nämlich $0, 1, \zeta, 1 + \zeta$).
Außerdem gebe man die Verknüpfungstafeln für Addition und Multiplikation in L an.

c) Es sei $M \supset L$ ein Zerfällungskörper von $X^3 - \zeta \in L[X]$. Man zeige: Ist $\eta \in M$ eine Nullstelle von $X^3 - \zeta$, so ist $L(\eta) = M$. Man gebe den Grad $[M : L]$ an. Ist die Galoisgruppe von $X^3 - \zeta \in L[X]$ abelsch?

Gleichungen höheren Grades

K2.23 [Herbst 2002] Bestimmen Sie

a) alle Lösungen der Gleichung $X^4 = 81$ im Körper $\mathbb{F}_{167}$;

b) alle natürlichen Zahlen n mit $1 \leq n \leq 2003$ und

$$n^4 \equiv 81 \mod 2004 \qquad [\text{es ist } 2004 = 167 \cdot 12]$$

K2.24 [Herbst 1980] Bestimmen Sie die Ordnung der Galoisgruppe von $X^4 + 6X^2 + X + 1$

a) über $\mathbb{Z}/(2)$,

b) über $\mathbb{Z}/(3)$.

K2.25 [Frühjahr 1994] Das Polynom $f(X) = X^6 + 3$ werde über dem Körper $\mathbb{F}$ mit 7 Elementen betrachtet. Sei L der Zerfällungskörper von $f(X)$ über $\mathbb{F}$. Man berechne $[L : \mathbb{F}]$.

K2.26 [Frühjahr 1976]

a) Man bestimme den Zerfällungskörper des Polynoms $f := x^6 + x^3 + 1$ über dem Körper GF(5) mit 5 Elementen, sowie die Teilkörper des Zerfällungskörpers. Zweckmäßig überlegt man sich zunächst, daß die Nullstellen neunte Einheitswurzeln sind.

b) Man betrachte das Polynom f nun über dem Körper GF(p) mit beliebiger Primzahl $p \neq 3$ und bestimme den Grad des Zerfällungskörpers in Abhängigkeit von p. Insbesondere gebe man für jeden der möglichen Grade das kleinste p an, das ihn realisiert.

K2.27 [Herbst 1975] Das Polynom $f(x) = x^7 - 2$ ist reduzibel über dem Körper $\mathbb{F}_p$ von p Elementen, wenn $p \not\equiv 1 \mod 7$ ist.

K2.28 [Herbst 2003] Sei F der Körper mit zwei Elementen. Zeigen Sie:

a) Ist $n > 1$ eine natürliche Zahl, ist $2^n - 1$ eine Primzahl und ist $f \in F[X]$ ein irreduzibles Polynom vom Grad n, dann erzeugt die Restklasse $X + (f)$ die multiplikative Gruppe des Körpers $F[X]/(f)$.

b) Für $g = X^4 + X^3 + X^2 + X + 1 \in F[X]$ ist $K = F[X]/(g)$ ein Körper, und die Restklasse $X + (g)$ in $K^\times$ hat die Ordnung 5.

Irreduzible Polynome

K2.29 [Frühjahr 1978] Es sei K ein endlicher Körper. Beweisen Sie: Zu jeder natürlichen Zahl n gibt es ein irreduzibles Polynom aus $K[x]$ vom Grad n.

K2.30 [Herbst 1975] Sei p Primzahl, m und n natürliche Zahlen, K ein Körper mit genau $q = p^m$ Elementen und f irreduzibel in $K[X]$. Man zeige:

f ist Teiler von $X^{q^n} - X$ genau dann, wenn der Grad von f Teiler von n ist.

K2.31 [Frühjahr 1978] Sei K ein endlicher Körper mit q Elementen, sei $f(X) \in K[X]$ irreduzibel und sei n eine natürliche Zahl. Man zeige, daß $f(X)$ genau dann ein Teiler von $X^{q^n} - X$ ist, wenn der Grad von $f(X)$ ein Teiler von n ist.

K2.32 [Herbst 2003] Es seien p und q Primzahlen. Warum zerfällt das Polynom

$$f(X) = X^{p^q} - X$$

über dem Körper $\mathbb{F}_p$ mit p Elementen in p verschiedene Faktoren vom Grad 1 und in $\frac{p^q - p}{q}$ verschiedene irreduzible Faktoren von Grad q?

HINWEIS: Die Faktoren müssen nicht angegeben werden! Zum Einstieg in die Aufgabe überlege man, dass die Nullstellen von f einen Körper bilden.

K2.33 [Frühjahr 1987] Sei p eine Primzahl und K ein Körper mit p Elementen. Für eine ganze Zahl $n \geq 1$ bezeichne I_n die Menge der normierten, irreduziblen Polynome vom Grad n aus $K[X]$ und u_n ihre Anzahl. Sei $g := X^{p^n} - X \in K[X]$. Zeigen Sie:

a) Jeder Erweiterungskörper von K mit p^n Elementen ist ein Zerfällungskörper von g über K.

b) $g = \prod_{\substack{f \in I_d \\ d \mid n}} f \qquad (\text{in } K[X])$

c) $p^n = \sum_{d \mid n} d \cdot u_d$

d) Berechnen Sie u_4 im Fall $p = 2$.

K2.34 [Frühjahr 1978] Es sei p eine Primzahl. Wieviel kubische Polynome gibt es in $\mathbb{F}_p[x]$, die normiert und irreduzibel sind?

K2.35 [Frühjahr 1998] Sei $\mathbb{F}_q$ der endliche Körper mit q Elementen.

a) Wieviele normierte irreduzible Polynome dritten Grades gibt es in $\mathbb{F}_q[X]$?
Geben Sie ein irreduzibles Polynom dritten Grades aus $\mathbb{F}_3[X]$ an.
Die Antworten sind zu begründen.

b) Geben Sie einen Unterkörper im Ring $\mathbb{F}_3^{3\times 3} = \mathrm{M}_3(\mathbb{F}_3)$ der dreireihigen Matrizen über $\mathbb{F}_3$ an, der isomorph zum Körper $\mathbb{F}_{27}$ ist.

K2.36 [Frühjahr 1989] Bestimmen Sie die Zahl der normierten irreduziblen Polynome vom Grad 9 über $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

K2.37 [Herbst 1975] Man berechne die Anzahl der irreduziblen Polynome vom Grade 10 über dem Körper K mit 2 Elementen.

ANLEITUNG: Man beachte, daß jedes irreduzible Polynom vom Grade n über K ein Teiler von $x^{2^n} - x$ ist, und man verwende die Möbiussche Umkehrformel.

K2.38 [Herbst 1988]

a) Sei p eine ungerade Primzahl. Zeige: $aX^2 + bX + c \in \mathbb{F}_p[X]$, $a \neq 0$, ist genau dann irreduzibel über dem Körper $\mathbb{F}_p$ $(= \mathbb{Z}/p\mathbb{Z})$, wenn $b^2 - 4ac$ kein Quadrat in $\mathbb{F}_p$ ist.

b) Bestimme alle irreduziblen quadratischen Polynome über $\mathbb{F}_3$.

c) Bestimme alle irreduziblen quadratischen und kubischen Polynome über $\mathbb{F}_2$ und zeige damit, daß $X^5 - X^2 + 1$ irreduzibel über $\mathbb{Q}$ ist.

K2.39 [Herbst 1985] $\mathbb{F}_3$ bezeichne den Körper mit 3 Elementen.

a) Zerlegen Sie das Polynom $f := X^5 + X^2 - X + 1 \in \mathbb{F}_3[X]$ in irreduzible Faktoren!

b) Ist die Einheitengruppe des Rings $R := \mathbb{F}_3[X]/(f)$ zyklisch?
Begründen Sie die Antwort!

K2.40 [Frühjahr 2000] Weisen Sie für eine Primzahl p die Äquivalenz folgender Aussagen nach:

i) $f(X) = X^2 + 2X + 2$ ist irreduzibel über dem Körper mit p^3 Elementen.

ii) $p \equiv 3 \mod 4$.

K2.41 [Herbst 2000] Sei k ein endlicher Körper und $K|k$ eine algebraische Körpererweiterung. f und g seien irreduzible Polynome in $K[X]$ vom gleichen Grad. Zeigen Sie, dass die Körper $K[X]/(f)$ und $K[X]/(g)$ isomorph sind.

ANLEITUNG: Nehmen Sie zunächst an, dass K ebenfalls endlich ist, und führen Sie den allgemeinen Fall darauf zurück.

Automorphismen

K2.42 [Frühjahr 1981] Es seien $K = \{-1, 0, 1\} = \mathrm{GF}(3)$ der Primkörper mit 3 Elementen, $K[x]$ (bzw. $K[x, y]$) der Polynomring in der Unbestimmten x (bzw. den Unbestimmten x, y) über K. Mit $\mathrm{GF}(3^m)$ wird das Galois-Feld mit 3^m Elementen bezeichnet.

a) Geben Sie alle normierten, irreduziblen Polynome vom Grad 2 aus $K[x]$ an.

b) Zeigen Sie: Ist $f \in K[x]$ ein irreduzibler Faktor von $x^9 - x \in K[x]$, so gilt Grad $f \leq 2$.

c) Geben Sie die maximalen Ideale des Faktorringes $K[x]/(x^9 - x)$ an.

d) Geben Sie ein Primideal in $K[x, y]/(x^9 - x)$ an, das nicht maximal ist.

e) Es sei L der Zerfällungskörper von $x^9 - x + 1$ über K.
Zeigen Sie $L \subseteq \mathrm{GF}(3^6)$.

HINWEIS: Bestimmen Sie a^{3^6} für eine Wurzel a von $x^9 - x + 1$.

f) Bestimmen Sie die Galois-Gruppe von $x^9 - x + 1 \in K[x]$.

K2.43 [Frühjahr 1986] Sei $f := X^5 + aX^4 - b \in \mathbb{F}_5[X]$ mit $b \neq 0$. Sei L ein algebraischer Abschluß von $\mathbb{F}_5$ und

$$\varphi : \; L \to L \qquad \text{mit} \qquad \varphi(y) = y^5$$

der Frobenius-Automorphismus. Sei $\alpha \in L$ eine Nullstelle von f und $K := \mathbb{F}_5(\alpha)$.

a) Zeigen Sie, daß φ einen Automorphismus von K induziert.

b) Schreiben Sie $\varphi(\alpha)$ in der Form $\dfrac{b_0 + b_1\alpha}{a_0 + a_1\alpha}$ mit $a_i, b_i \in \mathbb{F}_5$.

c) Bestimmen Sie die Nullstellen von f in $\mathbb{F}_5$.

d) Für welche $a, b \in \mathbb{F}_5$ ist f irreduzibel?

e) Berechnen Sie für irreduzibles f alle Nullstellen von f in K.

(Verwenden Sie a) und b) zur Lösung von d) und e).)

K2.44 [Herbst 1991] Es sei K ein endlicher Körper mit p^n Elementen ($n, p \in \mathbb{N}$, p eine Primzahl). Man beweise:

a) $\sigma : \; K \to K$, $a \mapsto a^p$ ist ein Automorphismus von K.

b) Die Automorphismengruppe G von K ist zyklisch von der Ordnung n.

HINWEIS: G wird von σ erzeugt.

K2.45 [Frühjahr 1975] Sei p eine Primzahl und K der Körper mit p^n Elementen. Sei $\varphi : \; K \to K$ der Frobenius-Homomorphismus $\varphi(\alpha) = \alpha^p$; sei $f = \sum_{i=0}^{m} a_i x^i \in K[x]$ ein Polynom. Dann ist

$$f(\varphi) : \; K \to K \quad , \quad \alpha \mapsto \sum_{i=0}^{m} a_i \varphi^i(\alpha) \quad , \quad \varphi^i := \varphi \circ \varphi^{i-1} \quad , \quad \varphi^\circ := \mathrm{id} \quad ,$$

ein Endomorphismus der additiven Gruppe von K.

Man zeige: Ist $f(\varphi) = 0$, so ist $f = (x^n - 1) \cdot g$ für ein Polynom $g \in K[x]$.

K2.46 [Herbst 1991] Sei k ein Körper der Primzahlcharakteristik p. Sei n eine natürliche Zahl und k_n der n-te Kreisteilungskörper über k, d.h. der Zerfällungskörper von $X^n - 1$ über k. Man beweise, daß $k_n | k$ zyklisch ist.

K2.47 [Herbst 1999] Sei K ein Körper von Primzahlcharakteristik. Sei n eine natürliche Zahl und K_n der n-te Kreisteilungskörper über K (d.h. der Zerfällungskörper von $X^n - 1$ über K). Beweisen Sie, dass die Erweiterung $K_n | K$ zyklisch ist.

K2.48 [Frühjahr 1989] Seien k ein endlicher Körper mit $q = p^e$ Elementen (p eine Primzahl, $e \geq 1$), n eine natürliche Zahl mit $p \nmid n$ und $R = \mathbb{Z}/n\mathbb{Z}$. Man zeige:

a) Ist K der Zerfällungskörper von $X^n - 1$ über k und $G = \mathrm{Aut}(K|k)$, so ist die Ordnung von G gleich der Ordnung von $\bar{q} = q + n\mathbb{Z}$ in der Einheitengruppe $R^\times$ von R.

b) Das n-te Kreisteilungspolynom $\Phi_n \in k[X]$ ist genau dann irreduzibel, wenn $\bar{q}$ ein erzeugendes Element der Gruppe $R^\times$ ist.

c) Für alle Primzahlen $p \geq 5$ ist $\Phi_{12} \in (\mathbb{Z}/p\mathbb{Z})[X]$ reduzibel.

d) Das Polynom $X^4 - X^2 + 1$ ist über $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ reduzibel.

K2.49 [Frühjahr 1990] Sei p eine Primzahl und $f_p = X^p - X - 1$ ein Polynom. K sei ein algebraischer Abschluß des Körpers $\mathbb{F}_p$ mit p Elementen und $a \in K$ eine Nullstelle von f_p. Zeigen Sie:

a) Es ist $a \notin \mathbb{F}_p$ und $f_p(a+1) = 0$.

b) $\mathbb{Z}/p\mathbb{Z}$ ist die Galoisgruppe von f_p über $\mathbb{F}_p$.

c) Als Polynom in $\mathbb{Q}[X]$ ist f_p irreduzibel.

K2.50 [Herbst 2000] Seien K ein Körper mit 15625 Elementen und G seine Automorphismengruppe. Wie viele und wie große Bahnen hat G in K?

K2.51 [Herbst 2003] Sei K ein Körper mit 81 Elementen, sei G die Gruppe aller Automorphismen von K. Bestimmen Sie:

a) die Längen der Bahnen der Operation von G auf K, sowie

b) die Anzahl der Bahnen gegebener Länge.

K2.52 [Herbst 1986] Es seien $K \subset L$ endliche Körper, wobei $|K| = q$ und $[L : K] = n$. Bekanntlich ist $L|K$ galoissch, und die Galoisgruppe von $L|K$ wird vom Frobeniusautomorphismus $a \mapsto a^q$ erzeugt (Diese Aussagen dürfen ohne Beweis benutzt werden). Zeigen Sie:

a) Die Norm jedes Elements $a \in L$ bezüglich $L|K$ ist gegeben durch

$$\mathrm{N}_{L|K}(a) = a^{(q^n-1)/(q-1)} \quad .$$

b) Die Norm $\mathrm{N}_{L|K}$ induziert einen Epimorphismus der multiplikativen Gruppe $L^\times$ von L auf die multiplikative Gruppe $K^\times$ von K.

Teilkörper

K2.53 [Herbst 2001]

a) Bestimmen Sie alle irreduziblen Polynome 2. und 3. Grades über $\mathbb{F}_2$.

b) Zeigen Sie: $f = X^6 + X + 1$ ist irreduzibel in $\mathbb{F}_2[X]$.

c) Sei $K = \mathbb{F}_2(\alpha)$, wo α eine Nullstelle des Polynoms f aus b) ist. Geben Sie alle Körper L mit $\mathbb{F}_2 \subsetneq L \subsetneq K$ an, indem Sie explizit jeweils ein $z \in K$ mit $L = \mathbb{F}_2(z)$ bestimmen.

K2.54 [Herbst 1997] Sei $K = \mathbb{F}_q$ der Körper mit $q = 2^{10}$ Elementen und $k = \mathbb{F}_2$ der Primkörper von K. Bestimmen Sie

a) die Anzahl der erzeugenden Elemente der multiplikativen Gruppe $K^\times = K \setminus \{0\}$,

b) alle Unterkörper von K,

c) die Anzahl der primitiven Elemente von $K|k$.

K2.55 [Herbst 2000] Sei $K = \mathbb{F}_{2^{2000}}$ der Körper mit 2^{2000} Elementen.

a) Wie viele Teilkörper besitzt K?

b) Wie viele erzeugende Elemente hat die Erweiterung $K|\mathbb{F}_2$?

HINWEIS: Die bei der Berechnung auftretenden Potenzen von 2 müssen nicht „ausgerechnet“ werden.

K2.56 [Herbst 1996] Sei $p \in \mathbb{N}$ eine Primzahl, seien $n, m \geq 1$ natürliche Zahlen und K ein Körper mit p^n Elementen. Man zeige:

a) $p^m - 1$ teilt genau dann $p^n - 1$, wenn m Teiler von n ist.

b) K enthält genau dann einen Unterkörper mit p^m Elementen, wenn m Teiler von n ist.

c) In wie viele irreduzible Faktoren zerfällt das Kreisteilungspolynom Φ_{31} über $\mathbb{Z}/2\mathbb{Z}$?

K2.57 [Frühjahr 2002] Sei Ω der algebraische Abschluss des Körpers $\mathbb{Z}/p\mathbb{Z}$, und seien K und L endliche Teilkörper von Ω mit p^r beziehungsweise p^s Elementen. Sei α ein primitives Element von K über $\mathbb{Z}/p\mathbb{Z}$. Zeigen Sie die Äquivalenz der folgenden Aussagen:

(i) r und s sind teilerfremd.

(ii) Das Minimalpolynom von α über $\mathbb{Z}/p\mathbb{Z}$ ist in $L[X]$ irreduzibel.

(iii) $K \cap L = \mathbb{Z}/p\mathbb{Z}$.

K2.58 [Herbst 1983] K sei ein algebraisch abgeschlossener Körper der Charakteristik 2 mit der Eigenschaft, daß jedes Element $a \in K$ algebraisch über dem Primkörper ist. Man zeige:

a) K hat für jedes $k \in \mathbb{N}$ genau einen Teilkörper mit 2^k Elementen. Im weiteren wird dieser Teilkörper mit $\mathrm{GF}(2^k)$ bezeichnet.

b) $K_p := \bigcup_{\ell \in \mathbb{N}_0} \mathrm{GF}(2^{p^\ell})$ ($p \in \mathbb{N}$ Primzahl) ist ein Teilkörper von K.
Ferner bestimme man alle Teilkörper von K_p.

c) Das System $\{K_p\,;\ p \in \mathbb{N}$ Primzahl$\}$ erzeugt K.

d) Jeder von der Identität verschiedene Automorphismus von K hat unendliche Ordnung.

3. Kreisteilungskörper

Allgemeine Theorie

K3.1 [Frühjahr 1983]

a) Es sei E eine endliche Erweiterung von $\mathbb{Q}$. Kann E unendlich viele Einheitswurzeln enthalten?

b) Es sei K ein endlicher Körper oder gleich dem Körper der rationalen Zahlen $\mathbb{Q}$. Gibt es irreduzible Polynome jeden Grades über K?

Man begründe in a) und in b) die jeweilige Antwort.

K3.2 [Frühjahr 1996] Sei n eine natürliche Zahl und ζ_n eine primitive n-te Einheitswurzel. Bestimmen Sie alle Einheitswurzeln im Körper $\mathbb{Q}(\zeta_n)$.

K3.3 [Frühjahr 1990] Es sei α eine primitive $(2n+1)$-te Einheitswurzel über $\mathbb{Q}$. Zeigen Sie:

$$\beta = -\alpha^2$$

ist eine primitive $(4n+2)$-te Einheitswurzel. Folgern Sie daraus, daß $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ ist.

K3.4 [Herbst 1991] Für jede natürliche Zahl n sei $\mathbb{Q}_n$ der Körper, der aus $\mathbb{Q}$ durch Adjunktion aller n-ten Einheitswurzeln entsteht.

a) Man beweise: Für ungerade natürliche Zahlen n gilt $\mathbb{Q}_n = \mathbb{Q}_{2n}$.

b) Man bestimme alle natürlichen Zahlen n, für welche die Erweiterung $\mathbb{Q}_n|\mathbb{Q}$ den Grad 6 hat.

c) Für jede Erweiterung $\mathbb{Q}_n|\mathbb{Q}$ vom Grad 6 bestimme man den Zwischenkörper, der über $\mathbb{Q}$ den Grad 2 hat.

K3.5 [Herbst 1994] Sei $k \in \mathbb{N}$, $k \geq 1$, $n = 3 \cdot 2^k$ und $\xi = e^{2\pi i/n} \in \mathbb{C}$. Bestimmen Sie das Minimalpolynom von ξ über $\mathbb{Q}$ explizit.

K3.6 [Herbst 1998] Sei n eine natürliche Zahl und w eine primitive n-te Einheitswurzel.

a) Zeigen Sie, dass für jeden Teilkörper $K \subseteq \mathbb{C}$ der Körpergrad $[K(w) : K]$ ein Teiler von $\phi(n)$ ist.

b) Sei d ein positiver Teiler von $\phi(n)$. Zeigen Sie, dass es einen Körper $K \subseteq \mathbb{C}$ gibt, für den $[K(w) : K] = d$ ist.

c) Sei speziell $n = 5$. Geben Sie für jeden positiven Teiler d von $\phi(5)$ einen Körper $K \subseteq \mathbb{C}$ an, für den $[K(w) : K] = d$ ist.

K3.7 [Frühjahr 1985] Sei $n \in \mathbb{N}$, $z = e^{\frac{2\pi i}{n}} \in \mathbb{C}$, und $\mathbb{Q}_n = \mathbb{Q}(z)$. Zeigen Sie:

a) Ist $n = p = 2^i + 1$ eine Primzahl, so enthält $\mathbb{Q}_n$ genau einen minimalen Zwischenkörper Z mit $\mathbb{Q} \subsetneq Z \subseteq \mathbb{Q}_n$.

b) Für $n = 5$ ist $Z = \mathbb{Q}(\sqrt{5})$ der einzige Zwischenkörper Z mit $\mathbb{Q} \subsetneq Z \subsetneq \mathbb{Q}_n$.

c) Bestimmen Sie explizit für $n = 20$ die minimalen Zwischenkörper Z mit $\mathbb{Q} \subsetneq Z \subsetneq \mathbb{Q}_n$.

K3.8 [Herbst 1986] Es sei n eine ganze Zahl > 2 und ξ eine primitive n-te Einheitswurzel über $\mathbb{Q}$. Geben Sie das Minimalpolynom von ξ über $\mathbb{Q}(\xi + \xi^{-1})$ an und bestimmen Sie

$$[\,\mathbb{Q}(\xi + \xi^{-1}) : \mathbb{Q}\,] \quad .$$

K3.9 [Frühjahr 1990] Sei $\zeta \in \mathbb{C}$ eine primitive d-te Einheitswurzel mit $d > 1$. Die Norm der Körpererweiterung $\mathbb{Q}(\zeta)|\,\mathbb{Q}$ werde mit $\mathrm{N} : \mathbb{Q}(\zeta) \to \mathbb{Q}$ bezeichnet. Sei p eine Primzahl, die d nicht teilt und $\mathbb{Z}_{(p)} = \left\{\frac{a}{b}\,;\ a, b \in \mathbb{Z}\,,\ p \nmid b\right\}$. Zeigen Sie:

a) Das Minimalpolynom von $1 - \zeta$ über $\mathbb{Q}$ ist ein Teiler von $(1 - X)^d - 1$ in $\mathbb{Z}[X]$.

b) $\mathrm{N}(1 - \zeta)$ ist ganzzahlig und teilt d.

c) $1 - \zeta$ ist eine Einheit in $\mathbb{Z}_{(p)}[\zeta]$.

Quadratische Einheitswurzeln

K3.10 [Frühjahr 1976] Für welche natürlichen Zahlen $n > 2$ gibt es n ein regelmäßiges n-Eck bildende Punkte eines quadratischen Gitters in der euklidischen Ebene?

K3.11 [Herbst 1982] Welche Einheitswurzeln enthält der Körper $\mathbb{Q}\left(\sqrt{-3}\right)$?

K3.12 [Herbst 1986] Sei $K := \mathbb{Q}\left(\sqrt{d}\right)$ mit einer quadratfreien ganzen Zahl d. Bestimmen Sie alle d, für die K mehr als 2 Einheitswurzeln enthält.

K3.13 [Frühjahr 1994] Bestimmen Sie alle Einheitswurzeln in $\mathbb{Q}\left(\sqrt{d}\right)$ für quadratfreies $d \in \mathbb{Z}$.

K3.14 [Frühjahr 1978] Für jede natürliche Zahl n sei $\mathbb{Q}_n$ der Körper, der durch Adjunktion aller n-ten Einheitswurzeln zum Körper $\mathbb{Q}$ der rationalen Zahlen entsteht.

a) Für welche n ist $[\,\mathbb{Q}_n : \mathbb{Q}\,] = 2$?

b) Sei G eine endliche Gruppe. Man zeige, daß G genau dann eine elementar-abelsche 2-Gruppe ist, wenn der Durchschnitt aller Untergruppen vom Index 2 nur aus dem Einselement besteht.

c) Für welche n ist $\mathbb{Q}_n$ Kompositum von Teilkörpern, die über $\mathbb{Q}$ quadratisch sind?

Fünfte Einheitswurzeln

K3.15 [Frühjahr 1980] Es sei $\xi := e^{\frac{2\pi i}{5}}$ und $y := \xi + \xi^4$. Man zeige:

a) $y = \dfrac{-1 + \sqrt{5}}{2}$.

b) $\mathbb{Q}\left[\sqrt{5}\right]$ ist der einzige echte Zwischenkörper zwischen $\mathbb{Q}$ und $\mathbb{Q}[\xi]$.

c) $X^2 + \frac{1-\sqrt{5}}{2}X + 1$ ist das Minimalpolynom von ξ über $\mathbb{Q}\left[\sqrt{5}\right]$.

K3.16 [Frühjahr 1980] Man schildere kurz, wie man Ergebnisse der vorigen Aufgabe dazu benutzen kann, um zu einer Konstruktion des regelmäßigen 5-Ecks mit Zirkel und Lineal zu gelangen (nicht notwendig der elegantesten).

K3.17 [Herbst 1995] Sei $K = \mathbb{Q}(\omega)$ mit $\omega := e^{2\pi i/5}$ und F ein Zwischenkörper mit $\mathbb{Q} \subsetneqq F \subsetneqq K$.

a) Man ermittle das Minimalpolynom von ω über $\mathbb{Q}$ und gebe eine Vektorraum-Basis von K über $\mathbb{Q}$ an.

b) Warum ist $K \subset \mathbb{Q}$ galoissch? Man berechne $\mathrm{Gal}(K|\mathbb{Q})$.

c) Man berechne das Minimalpolynom von ω über F.

K3.18 [Herbst 1996] Man bestimme (bis auf Isomorphie) die Galoisgruppe des Polynoms

$$X^4 + X^3 + X^2 + X + 1$$

über $\mathbb{Q}$.

K3.19 [Frühjahr 1997]

a) Es sei ζ eine primitive fünfte Einheitswurzel und $\eta = \zeta + \zeta^{-1}$. Leiten Sie aus der Minimalgleichung von ζ über $\mathbb{Q}$ eine quadratische Gleichung von η über $\mathbb{Q}$ her. Beweisen Sie, daß $\sqrt{5}$ in $\mathbb{Q}(\zeta)$ enthalten ist.

b) Zeigen Sie, daß $X^5 - 2$ über $\mathbb{Q}(\sqrt{5})$ irreduzibel ist.

c) Es sei E der Zerfällungskörper von $X^5 - 2$ über $\mathbb{Q}(\sqrt{5})$. Bestimmen Sie den Grad $[E : \mathbb{Q}(\sqrt{5})]$.

d) Bestimmen Sie die Galoisgruppe G von E über $\mathbb{Q}(\sqrt{5})$ und alle Zwischenkörper.

e) Ist E über $\mathbb{Q}$ normal?

K3.20 [Frühjahr 2000] Sei $\xi = e^{\frac{2\pi i}{5}}$.

a) Zeigen Sie, dass $\alpha = \xi + \xi^{-1}$ einer normierten quadratischen Gleichung mit Koeffizienten aus $\mathbb{Z}$ genügt.

b) Stellen Sie α^{-1} als Polynom in α dar und zeigen Sie $0 < \alpha < 1$.

K3.21 [Herbst 2003] Beweisen Sie

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4} \quad .$$

Siebte Einheitswurzeln

K3.22 [Frühjahr 1976] Sei ξ eine primitive 7-te Einheitswurzel über $\mathbb{Q}$.

a) Man gebe die Gruppe $\mathrm{Aut}(\mathbb{Q}(\xi)|\mathbb{Q})$ und ihre Operation auf $\mathbb{Q}(\xi)$ explizit an (es genügen dabei kurze Begründungen).

b) Man zeige, daß es genau eine Galoiserweiterung $K \supset \mathbb{Q}$ mit folgenden Eigenschaften gibt:

i) $K \subseteq \mathbb{Q}(\xi) \cap \mathbb{R}$.

ii) $\mathrm{Aut}(K|\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$.

c) Man zeige, daß $a := \xi + \xi^6$ ein primitives Element von K über $\mathbb{Q}$ ist.

d) Man bestimme das Minimalpolynom von a über $\mathbb{Q}$.

K3.23 [Herbst 1998] Man gebe eine komplexe Zahl α an, für die $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine Galoiserweiterung von Grad 3 ist.

K3.24 [Frühjahr 1991] Sei $\zeta \in \mathbb{C}$ eine primitive siebente Einheitswurzel.

a) Zeigen Sie, daß $\sqrt{-7}$ in $\mathbb{Q}(\zeta)$ liegt.

b) Berechnen Sie das Minimalpolynom von ζ über $K = \mathbb{Q}\left(\sqrt{-7}\right)$.

c) Bestimmen Sie ein Polynom $f \in K[x]$ mit $f(\zeta) = \zeta^{-1}$.

K3.25 [Herbst 1992] Es sei a eine primitive siebente Einheitswurzel. Dann ist ihr Minimalpolynom über $\mathbb{Q}$ bekanntlich gleich dem siebenten Kreisteilungspolynom

$$f(X) = \sum_{j=0}^{6} X^j \quad .$$

Ferner ist $\mathbb{Q}(a)|\,\mathbb{Q}$ eine galoissche Erweiterung. Mit G sei die zugehörige Galoisgruppe bezeichnet.

a) Man beweise, daß ein $\sigma \in G$ existiert mit $\sigma(a) = a^3$. Man berechne die Ordnung von σ.

b) Man beweise, daß G von σ erzeugt wird.

c) Man beweise, daß $\sigma^3(z) = \bar{z}$ ist für alle $z \in \mathbb{Q}(a)$.

d) Man bestimme die Minimalpolynome von $b := a + a^6$ und von $c := a + a^2 + a^4$ über $\mathbb{Q}$.

e) Man beweise, daß $\mathbb{Q}(b)$ und $\mathbb{Q}(c)$ die einzigen echten Zwischenkörper der Erweiterung $\mathbb{Q}(a)|\,\mathbb{Q}$ sind.

K3.26 [Frühjahr 1996] Sei ζ_7 eine primitive siebte Einheitswurzel und $E := \mathbb{Q}(\zeta_7)$. Zeigen Sie:

a) Es gibt genau eine über $\mathbb{Q}$ quadratische Teilerweiterung L in E.

b) Zeigen Sie: $L = \mathbb{Q}\left(\sqrt{-7}\right)$.

K3.27 [Frühjahr 1999] Sei $\zeta \in \mathbb{C}$ eine primitive 7-te Einheitswurzel. Man bestimme das Minimalpolynom von $\zeta + \zeta^2 + \zeta^4$ über $\mathbb{Q}$.

K3.28 [Frühjahr 2002] Sei $\xi \in \mathbb{C}$ eine primitive 7-te Einheitswurzel.

a) Man bestimme α bzw. β in $\mathbb{Q}(\xi)$ so, dass $[\,\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ und $[\,\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ ist.

b) Man bestimme jeweils das Minimalpolynom von α und von β.

Achte Einheitswurzeln

K3.29 [Herbst 1973] Man beweise, daß das achte Kreisteilungspolynom

$$x^4 + 1$$

über $\mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p reduzibel ist.
Für $p = 2, 3, 5$ und 7 gebe man die Zerlegung in irreduzible Faktoren an.

K3.30 [Frühjahr 1987] Bestimmen Sie den Grad des Zerfällungskörpers des Polynoms $X^4 + 4$ über $\mathbb{Q}$.

K3.31 [Herbst 1988]

a) Bestimmen Sie den Zerfällungskörper K des Polynoms $X^4 - 4$ über $\mathbb{Q}$.

b) Bestimmen Sie die Galoisgruppe von $K|\,\mathbb{Q}$.

c) Bestimmen Sie die verschiedenen Zwischenkörper von $K|\,\mathbb{Q}$.

K3.32 [Frühjahr 1991] Sei $f = x^6 + x^4 + x^2 + 1$ ein Polynom.

(a) Bestimmen Sie einen Zerfällungskörper von f über den rationalen Zahlen $\mathbb{Q}$.

(b) Bestimmen Sie die Galoisgruppe von f über $\mathbb{Q}$.

(c) Bestimmen Sie die Galoisgruppe von f über dem Primkörper $\mathbb{F}_5$ mit fünf Elementen.

K3.33 [Herbst 2000]

a) Sei $p \neq 2$ eine Primzahl. Zeigen Sie, dass der Körper $\mathbb{F}_{p^2}$ mit p^2 Elementen eine primitive 8-te Einheitswurzel enthält.

b) Zeigen Sie, dass das Polynom $X^4 + 1$ über $\mathbb{Q}$ irreduzibel und über jedem endlichen Körper reduzibel ist.

Neunte Einheitswurzeln

K3.34 [Herbst 1987] Beweisen Sie, daß man einen Winkel von 120 Grad nicht mit Zirkel und Lineal dreiteilen kann.

K3.35 [Herbst 2000] Sei $n > 2$ eine ganze Zahl und ϕ die Eulersche phi-Funktion.

a) Zeigen Sie, dass $\mathbb{Q}(\cos\frac{2\pi}{n}) | \mathbb{Q}$ eine Galoiserweiterung vom Grad $\frac{\phi(n)}{2}$ ist.

b) Bestimmen Sie das neunte Kreisteilungspolynom über $\mathbb{Q}$.

c) Bestimmen Sie das Minimalpolynom von $\cos\frac{2\pi}{9}$ über $\mathbb{Q}$.

Zwölfte Einheitswurzeln

K3.36 [Frühjahr 1972]

a) Man zerlege das Polynom

$$f(X) = X^6 + 2X^5 + 2X^4 + X^2 + 2X + 2 \in \mathbb{Q}[X]$$

in irreduzible Faktoren.

b) Bestimme den Zerfällungskörper Z von $f(X)$ über $\mathbb{Q}$ und den Grad von Z über $\mathbb{Q}$.

c) Ist die Galoisgruppe von Z über $\mathbb{Q}$ zyklisch? (Begründung!)

d) Man fasse jetzt $f(X)$ als ein Polynom über $\mathbb{F}_3 = \mathbb{Z}/(3)$ auf und bestimme seine Zerlegung in irreduzible Faktoren über $\mathbb{F}_3$.

e) Welchen Grad hat der Zerfällungskörper Z' des Polynoms über $\mathbb{F}_3$ und wieviele Elemente besitzt Z'?

f) Wieviele verschiedene Nullstellen hat das Polynom in Z'?

K3.37 [Frühjahr 1982] Sei $f := X^6 + 1$.

a) Welchen Grad hat der Zerfällungskörper K von f über $\mathbb{Q}$?

b) Man bestimme die Galoisgruppe der Erweiterung $K/\mathbb{Q}$ und alle Zwischenkörper.

c) Man finde ein $\zeta \in K$ mit $K = \mathbb{Q}(\zeta)$.

K3.38 [Herbst 1993] Sei $\zeta = e^{2\pi i/12}$ eine primitive 12-te Einheitswurzel. Die Automorphismen des Kreisteilungskörpers $\mathbb{Q}(\zeta)$ sind durch die Zuordnungen

$$\delta_k : \zeta \mapsto \zeta^k \quad , \quad \text{wo } [k] \text{ prime Restklasse modulo 12, i.e. } [k] \in (\mathbb{Z}/12\mathbb{Z})^\times$$

vollständig beschrieben, und die Zuordnung $j : \delta_k \mapsto k \bmod 12$ liefert einen Isomorphismus der Galoisgruppe G der Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ auf $(\mathbb{Z}/12\mathbb{Z})^\times$.

a) Zeigen Sie: Die Galoisgruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$ wird durch die Automorphismen δ_1, δ_5, δ_7 und δ_{11} gebildet und ist isomorph zur Kleinschen Vierergruppe.

b) Man bestimme sämtliche Unterkörper der Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ und schreibe sie als einfache Erweiterungen von $\mathbb{Q}$.

K3.39 [Frühjahr 1998]

a) Drücken Sie die komplexen Nullstellen des Polynoms $f = X^4 - X^2 + 1$ durch Werte der Exponentialfunktion aus.

b) Zeigen Sie, daß f über dem Körper $\mathbb{Q}$ der rationalen Zahlen irreduzibel ist.

c) Bestimmen Sie den Isomorphietyp der Galoisgruppe von f über $\mathbb{Q}$.

Einzelne höhere Einheitswurzeln

K3.40 [Herbst 1981] $\mathbb{Q}_{17}$ sei der 17te Kreisteilungskörper über $\mathbb{Q}$. Geben Sie für zwei echte Zwischenkörper von $\mathbb{Q}_{17}|\mathbb{Q}$ je ein primitives Element an.

K3.41 [Frühjahr 1977] Eine Gruppe (mit neutralem Element e) heißt *unzerlegbar*, wenn sie nicht direktes Produkt zweier Untergruppen H_1 und H_2 mit $H_1 \neq \{e\}$ und $H_2 \neq \{e\}$ ist. Man beweise:

a) Ist $n \in \mathbb{N}$, $n \geq 2$, Potenz einer Primzahl, so ist die Gruppe $\mathbb{Z}/n\mathbb{Z}$ unzerlegbar.

b) Der Zerfällungskörper K des Polynoms

$$f(X) = \sum_{i=0}^{16} X^i \ \in \mathbb{Q}[X]$$

über $\mathbb{Q}$ besitzt keine echten Unterkörper L und M, so daß $L \cap M = \mathbb{Q}$ gilt und K der kleinste Unterkörper von K ist, der L und M enthält.

K3.42 [Frühjahr 1995] Sei ζ_{23} primitive 23-te Einheitswurzel in $\mathbb{C}$. Bestimmen Sie die Anzahl aller Zwischenkörper K mit $\mathbb{Q} \subsetneqq K \subsetneqq \mathbb{Q}(\zeta_{23})$.

K3.43 [Herbst 1979] Diese Aufgabe dreht sich um die 24^{sten} Einheitswurzeln. Die Irreduzibilität des Kreisteilungspolynoms Φ_{24} über $\mathbb{Q}$ soll nicht vorausgesetzt werden. Es sollen aber Behauptungen von Teilaufgaben zur Bearbeitung späterer Teile verwendet werden.

a) Man begründe, daß $a^2 \equiv 1 \pmod{24}$ gilt für jede zu 6 teilerfremde ganze Zahl a. Dann folgere man, daß die Einheitengruppe des Restklassenringes $\mathbb{Z}/24\mathbb{Z}$ isomorph zu $Z_2 \times Z_2 \times Z_2$ ist. (Hier bezeichnet Z_2 eine Gruppe der Ordnung 2.)

b) Es sei k ein Körper mit von 2 und 3 verschiedener Charakteristik. Man beweise, daß das Polynom $F = X^8 - X^4 + 1$ in einem Zerfällungskörper über k als Nullstellenmenge die Gesamtheit der primitiven 24^{sten} Einheitswurzeln hat. ($X^2 - X + 1$ hat die primitiven sechsten Einheitswurzeln als Nullstellen.)

c) Das Polynom $F = X^8 - X^4 + 1$ ist über jedem endlichen Primkörper $\mathbb{F}_p$ Produkt von irreduziblen Faktoren vom Grad ≤ 2. (Man beachte beim Beweis die beiden Sonderfälle $p = 2$ und $p = 3$.)

d) ζ_n sei eine primitive n-te Einheitswurzel über dem Körper $\mathbb{Q}$ der rationalen Zahlen. Man zeige, daß $\mathbb{Q}(\zeta_{24})$ mindestens vier Teilkörper vom Grad 2 hat und folgere die Irreduzibilität von $X^8 - X^4 + 1$ über $\mathbb{Q}$ sowie die Struktur der Galoisgruppe von $\mathbb{Q}(\zeta_{24})$.

e) Man beweise $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ und man gebe alle Teilkörper K von $\mathbb{Q}(\zeta_{24})$ mit dem Grad $[K : \mathbb{Q}] = 2$ an.

K3.44 [Frühjahr 1989]

a) Zeigen Sie, daß der Körper $\mathbb{Q}(e^{\frac{\pi i}{3}}, e^{\frac{\pi i}{5}}, e^{\frac{2\pi i}{15}})$ galoissch über $\mathbb{Q}$ ist.

b) Ist seine Galoisgruppe abelsch?

K3.45 [Herbst 1981] ζ sei eine primitive 42-te Einheitswurzel. Wieviele Zwischenkörper gibt es zwischen $\mathbb{Q}$ und $\mathbb{Q}(\zeta)$? (mit Begründung)

Einheitswurzeln von Primzahlordnung

K3.46 [Frühjahr 1976] Sei p eine Primzahl und $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Man beweise:

Ist $a \in \mathbb{Q}$ p-te Potenz eines Elementes von $\mathbb{Q}(\zeta)$, so ist a schon p-te Potenz eines Elementes von $\mathbb{Q}$.

K3.47 [Frühjahr 1978] $\mathbb{Q}_n$ sei der n-te Kreisteilungskörper über $\mathbb{Q}$ (Körper der rationalen Zahlen). Zeigen Sie, daß die primitiven n-ten Einheitswurzeln eine Basis von $\mathbb{Q}_n | \mathbb{Q}$ bilden, wenn n eine Primzahl ist.

K3.48 [Frühjahr 1982]

a) Sei p eine Primzahl und ζ eine primitive p-te Einheitswurzel. Was wissen Sie über die Struktur der Galoisgruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$?

b) Zeigen Sie: Es gibt eine Galois-Erweiterung von $\mathbb{Q}$ vom Grad 3.

K3.49 [Herbst 1984] Es sei p eine ungerade Primzahl und ζ eine primitive p-te Einheitswurzel. Man beweise, daß $\mathbb{Q}(\zeta)$ genau einen quadratischen Teilkörper K (d.h. K hat über $\mathbb{Q}$ den Grad 2) besitzt! Man beweise, daß K genau dann reell ist, wenn $p \equiv 1 \pmod 4$ ist.

K3.50 [Frühjahr 1996] Sei p eine Primzahl, sei $\zeta = \zeta_0$ eine primitive p-te Einheitswurzel über $\mathbb{Q}$. Ist $s \in \{1, \ldots, p-1\}$ so, daß $\bar{s}$ ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ ist, so ist $\varphi : \zeta \mapsto \zeta^s$ ein erzeugendes Element der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ des p-ten Kreisteilungskörpers $\mathbb{Q}(\zeta)$.

Zeigen Sie: Zu jedem Teiler d von $p-1$ gibt es genau einen Zwischenkörper M von $\mathbb{Q}(\zeta)|\mathbb{Q}$ mit $[M : \mathbb{Q}] = m$, wobei $p - 1 = d \cdot m$, und es gilt $M = \mathbb{Q}(\eta_i)$ mit

$$\eta_i := \sum_{k=0}^{d-1} \zeta_{i+km} \qquad (0 \leq i \leq m-1),$$

wobei $\zeta_j := \varphi^j(\zeta) = \zeta^{s^j}$ für $j \geq 0$ (i.e. jedes der Elemente η_i hat die Eigenschaft, den Zwischenkörper M zu erzeugen).

K3.51 [Frühjahr 1997] Sei $G = C_q$ eine zyklische Gruppe, deren Ordnung q eine Primzahlpotenz sei. Es sei p eine Primzahl mit $p \equiv 1 \mod q$, und $K_p = \mathbb{Q}(e^{2\pi i/p})$ sei der p-te Kreisteilungskörper.

a) Konstruieren Sie einen surjektiven Gruppenhomomorphismus $\phi : H \to G$, wobei $H = C_{p-1}$ die zyklische Gruppe der Ordnung $p-1$ sei.

b) Begründen Sie kurz, warum H zur Galoisgruppe von K_p über $\mathbb{Q}$ isomorph ist.

c) Warum gibt es einen Teilkörper von K_p, dessen Galoisgruppe über $\mathbb{Q}$ isomorph zu G ist?

d) Nennen Sie eine normale Erweiterung von $\mathbb{Q}$ mit der Galoisgruppe C_3 über $\mathbb{Q}$.

Erweiterungen von Q mit gegebener abelscher Gruppe

K3.52 [Frühjahr 1976] Man konstruiere eine Galoiserweiterung $K \supset \mathbb{Q}$ mit $\mathrm{Aut}(K|\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$.

K3.53 [Frühjahr 1990]

a) Man gebe eine komplexe Zahl z an, so daß $\mathbb{Q}(z)|\mathbb{Q}$ eine galoissche Körpererweiterung mit einer zyklischen Galoisgruppe der Ordnung 22 ist.

b) Man löse die gleiche Aufgabe für die zyklische Gruppe der Ordnung 11.
(Insbesondere soll wie in a) ein primitives Element angegeben werden.)

K3.54 [Herbst 2001]

a) Sei p eine Primzahl. Man gebe — mit entsprechendem Beweis — eine komplexe Zahl z an, so dass $\mathbb{Q}(z)$ eine Galoiserweiterung über $\mathbb{Q}$ vom Grade $p-1$ ist.

b) Man gebe — mit entsprechendem Beweis — eine komplexe Zahl z an, so dass $\mathbb{Q}(z)$ eine Galoiserweiterung vom Grade 500 über $\mathbb{Q}$ ist.

K3.55 [Frühjahr 1978]

a) Jede endliche abelsche Gruppe ist isomorph zu einer Faktorgruppe der Gruppe

$$\prod_p \mathbb{Z}/(p-1)\mathbb{Z} \quad ,$$

wobei p alle Primzahlen durchläuft.

HINWEIS: Man benutze den Dirichletschen Primzahlsatz: Zu jeder natürlichen Zahl n gibt es unendliche viele Primzahlen p mit $p \equiv 1 \mod n$.

b) Jede endliche abelsche Gruppe ist isomorph zu einer Faktorgruppe der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ der teilerfremden Reste $\mod n$, wenn n passend gewählt wird.

c) Zu jeder endlichen abelschen Gruppe A gibt es eine galoissche Erweiterung $K|\mathbb{Q}$, deren Galoisgruppe $G(K|\mathbb{Q})$ zu A isomorph ist.

4. Galoistheorie

Vermischtes

K4.1 [Herbst 1994] Welche der folgenden Körpererweiterungen sind galoissch? Man begründe das Ergebnis.

a) $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$,

b) $\mathbb{Q}(\sqrt[6]{2}, \sqrt{-3})|\mathbb{Q}$,

c) $\mathbb{Q}(t)|\mathbb{Q}(t^2)$, t über $\mathbb{Q}$ transzendent,

d) $\mathbb{F}_p(t)|\mathbb{F}_p(t^p)$, p eine Primzahl, t über $\mathbb{F}_p$ transzendent, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

K4.2 [Frühjahr 1999] Welche der folgenden Körpererweiterungen sind galoissch? Man begründe das Ergebnis.

a) $\mathbb{Q}(\sqrt[6]{-3})|\mathbb{Q}$,

b) $\mathbb{Q}(X)|\mathbb{Q}(X^3), X$ über $\mathbb{Q}$ transzendent,

c) $\mathbb{F}_2(X)|\mathbb{F}_2(X^2), X$ über $\mathbb{F}_2$ transzendent.

K4.3 [Frühjahr 1992]

a) Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom ungeraden Grades $n > 1$, das höchstens $n-1$ reelle Nullstellen besitzt. Zeigen Sie, daß die Ordnung der Galoisgruppe von f über $\mathbb{Q}$ durch $2n$ teilbar ist.

b) Zeigen Sie, daß X^5+2X+2 über $\mathbb{Q}$ irreduzibel ist und daß $\mathbb{Q}[X]/(X^5+2X+2)$ keine galoissche Erweiterung von $\mathbb{Q}$ ist.

K4.4 [Herbst 1992] Es sei $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in K[X]$ ein nichtkonstantes, separables Polynom mit $a_0a_n \neq 0$. Sei $g = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$ das sogenannte „reziproke“ Polynom zu f. Zeigen Sie:

f und g haben dieselbe Galoisgruppe über K.

Theoretische Grundlagen

K4.5 [Herbst 1975] Sei $K|k$ eine galoissche Körpererweiterung mit der Galoisgruppe G. Sei $f(x) \in k[x]$ ein über k irreduzibles, separables, normiertes Polynom und

$$f(x) = \prod_{i=1}^{s} f_i(x)$$

die Zerlegung von $f(x)$ in irreduzible normierte Faktoren über K. Zeige:

a) Die Gruppe G operiert auf der Menge $\{f_1(x), \ldots, f_s(x)\}$.

b) Die Operation ist transitiv.

c) Die Gruppen $G_i = \{\sigma \in G;\ f_i^\sigma(x) = f_i(x)\}$ sind paarweise konjugiert in G.

d) Die Faktoren $f_i(x) \in K[x]$ haben gleichen Grad.

e) Die Anzahl s ist ein Teiler des Grades $[K : k]$.

K4.6 [Herbst 1975] Sei N normale Erweiterung des kommutativen Körpers K und $f \in K[X]$ irreduzibel. Man zeige:

Je zwei in $N[X]$ irreduzible Teiler von f haben gleichen Grad.

K4.7 [Frühjahr 1976] Sei G eine beliebige endliche Gruppe.

a) Man zeige, daß es Körpererweiterungen $\mathbb{C} \supset K \supset k \supset \mathbb{Q}$ gibt, so daß gilt:

i) $K \supset k$ ist Galoiserweiterung.

ii) $\mathrm{Aut}(K|k) \simeq G$.

HINWEIS: Benutzt werden darf die Tatsache, daß es für jedes $n \in \mathbb{N}$ eine galoissche Erweiterung $K|\mathbb{Q}$ gibt mit $\mathrm{Aut}(K|\mathbb{Q}) = S_n$.

b) Man untersuche, ob die dabei entstehende Körpererweiterung $k \supset \mathbb{Q}$ im allgemeinen eine Galoiserweiterung ist.

K4.8 [Herbst 1999] Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad n mit den Wurzeln $\xi_1, \ldots, \xi_n$. Sei $\delta := \prod_{1 \le i < j \le n} (\xi_i - \xi_j) \notin K$. Zeigen Sie, dass die Ordnung der Galoisgruppe von f über K eine gerade Zahl ist.

K4.9 [Frühjahr 2001] Der Körper k habe Charakteristik $p \neq 0$; K sei der Zerfällungskörper eines Polynoms aus $k[x]$. Zeigen Sie, dass der separable Abschluss K_{sep} von k in K der Zerfällungskörper eines separablen Polynoms aus $k[x]$ ist.

Kubische Gleichungen

K4.10 [Herbst 1979] Bestimme die Galoissche Gruppe des Polynoms $f = X^3 - X + 1$ über den Körpern $\mathbb{F}_3$, $\mathbb{F}_7$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-23})$.

K4.11 [Frühjahr 1984] Geben Sie eine normale und eine nichtnormale Erweiterung dritten Grades von $\mathbb{Q}$ an.

K4.12 [Frühjahr 2001] Welches sind die Galoisgruppen der Polynome $x^3 - 3x + 3$, $x^3 - 1$, $x^3 - 3x + 1$ über $\mathbb{Q}$?

K4.13 [Frühjahr 1991] Sei $K(\alpha)|K$ eine separable Körpererweiterung, und das Minimalpolynom g von α über K habe den Grad $n > 1$. Zeigen Sie:

a) Die Gleichung $x^3 = \alpha$ besitzt genau dann eine Lösung in $K(\alpha)$, wenn das Polynom $f(x) = g(x^3) \in K[x]$ vom Grad $3n$ reduzibel ist.

b) Die Grade der irreduziblen Faktoren von f sind Vielfache von n.

c) f besitzt genau dann eine mehrfache Nullstelle in einem Erweiterungskörper von K, wenn K die Charakteristik 3 hat.

Biquadratische Gleichungen

K4.14 [Frühjahr 1979] Es sei K ein (kommutativer) Körper mit Charakteristik $\neq 2$ und $f = x^4 + ax^2 + b \in K[x]$ irreduzibel. Man bestimme den Isomorphietyp der Galoisgruppe von f über K.

HINWEIS: Man kann (muß aber nicht) die vier Fälle, welche sich ergeben, je nachdem ob b oder $b(a^2 - 4b)$ Quadrat in K ist oder nicht, von vorneherein getrennt behandeln.

K4.15 [Frühjahr 1998] Betrachten Sie die Polynome

$$f_n = X^4 + 4nX^2 + 2$$

mit dem Parameter $n \in \mathbb{Z}$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen.

a) Für welche $n \in \mathbb{Z}$ ist f_n irreduzibel?

b) Man zeige, daß für den Isomorphietyp der Galoisgruppe von f_n über $\mathbb{Q}$ nur zwei Gruppen möglich sind.

c) Man zeige: Genau dann ist $\mathrm{Gal}(f_n|\,\mathbb{Q})$ zyklisch, wenn $2n^2 - 1$ eine Quadratzahl ist.

K4.16 [Frühjahr 1984] Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, dessen Grad > 1 ist und das eine Nullstelle $z \in \mathbb{C}$ vom Betrag 1 besitzt. Zeigen Sie:

a) $\frac{1}{z}$ ist Nullstelle von f.

b) Für jede Nullstelle $z' \in \mathbb{C}$ von f gilt $z' \neq 0$, und $\frac{1}{z'}$ ist eine von z' verschiedene Nullstelle von f.

HINWEIS: Verwenden Sie einen geeigneten $\mathbb{Q}$-Isomorphismus von $\mathbb{Q}(z)$ nach $\mathbb{Q}(z')$!

c) f hat geradzahligen Grad.

d) Besitzt f den Grad 4, so hat der Zerfällungskörper von f über $\mathbb{Q}$ höchstens den Grad 8.

Körperisomorphismen

K4.17 [Herbst 1979] Sei $K|k$ eine separable endliche Körpererweiterung vom Grad n. Man beweise:

a) Sind $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \bar{k}$ die n verschiedenen k-Homomorphismen von K in einen algebraischen Abschluß $\bar{k}$ von k, so gilt

$$\mathrm{tr}_{K|k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{für alle } \alpha \in K \quad .$$

b) Es gibt ein $\alpha \in K$ mit $\mathrm{tr}_{K|k}(\alpha) \neq 0$, anders ausgedrückt: Jedes Element aus k ist Spur eines Elements aus K.

K4.18 [Herbst 1996] Sei K ein Körper, sei G eine Gruppe von Automorphismen von K und $k = K^G$ ihr Fixkörper. Man beweise: Ein Element $\alpha \in K$ ist algebraisch über k genau dann, wenn die Menge $\{\sigma(\alpha)\,;\ \sigma \in G\}$ endlich ist.

K4.19 [Frühjahr 1990] K sei ein Körper der Charakteristik 2, die Polynome $f_1 = x^2 - a_1$ und $f_2 = x^2 - x - a_2$, mit $a_1, a_2 \in K$, seien über K irreduzibel, L_1 bzw. L_2 seien Zerfällungskörper von f_1 bzw. f_2. Kann es einen K-Isomorphismus von L_2 auf L_1 geben?
Begründen Sie Ihre Antwort.

K4.20 [Frühjahr 2001] $K|\,\mathbb{Q}$ sei eine endliche Körpererweiterung vom Grad n. Zeigen Sie, dass es genau n verschiedene Körpermonomorphismen von K nach $\mathbb{C}$ gibt und dass die Anzahl s derjenigen mit nicht-reellem Bild gerade ist. Mit $n = r + s$ weisen Sie $r = 0$ oder $s = 0$ für den Fall nach, dass $K|\,\mathbb{Q}$ galoissch ist, und geben Sie Beispiele für beide Fälle.

K4.21 [Herbst 2003] Sei K ein Teilkörper von $\mathbb{C}$, der über $\mathbb{Q}$ von endlichem Grad n ist. Zeigen Sie: Ist n ungerade und K normal über $\mathbb{Q}$, so gilt $K \subseteq \mathbb{R}$.

Elementar-abelsche 2-Gruppen

K4.22 [Frühjahr 1981]

a) Zeige: $\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2},\ \sqrt{5})$. Bestimme den Grad von $\sqrt{2}+\sqrt{5}$ über $\mathbb{Q}$.

b) Zeige: $\mathbb{Q}(\sqrt{2},\sqrt{5})$ ist galoissch über $\mathbb{Q}$ und bestimme die Galoisgruppe.

K4.23 [Herbst 1983] Sei $\mathbb{Q}$ der Körper der rationalen Zahlen und i die komplexe Zahl $\sqrt{-1}$.

a) Zeige, daß $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}+i)$ und $\mathbb{Q}(i) \subseteq \mathbb{Q}(\sqrt{2}+i)$.

b) Beweise $\mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\sqrt{2}+i)$.

c) Finde eine Basis von $\mathbb{Q}(\sqrt{2}+i)$ über $\mathbb{Q}(\sqrt{2})$, über $\mathbb{Q}(i)$ und über $\mathbb{Q}$.

d) Bestimme das Minimalpolynom von $\sqrt{2}+i$ über $\mathbb{Q}(\sqrt{2})$, über $\mathbb{Q}(i)$ und über $\mathbb{Q}$.

e) Bestimme die Galois-Gruppe von $\mathbb{Q}(\sqrt{2}+i)$ über $\mathbb{Q}$.

K4.24 [Herbst 1984] Es sei $K := \mathbb{Q}\left(\sqrt{2},\sqrt{3},\sqrt{5}\right)$.

a) Bestimmen Sie $[K:\mathbb{Q}]$!

b) Zeigen Sie, daß $K|\mathbb{Q}$ eine Galoiserweiterung ist!

c) Wieviele verschiedene Zwischenkörper besitzt $K|\mathbb{Q}$ und wieviele davon sind über $\mathbb{Q}$ galoissch?

K4.25 [Herbst 1985] K sei der Erweiterungskörper von $\mathbb{Q}$, der aus $\mathbb{Q}$ durch Adjunktion aller Nullstellen in $\mathbb{C}$ aller Polynome X^2+aX+b $(a,b \in \mathbb{Q})$ hervorgeht. Ferner sei M die Menge aller Quadratwurzeln $\sqrt{p}$, wobei $p=-1$ oder p eine Primzahl ist. Zeigen Sie:

a) $K = \mathbb{Q}(M)$.

b) Für jeden Automorphismus σ von $K|\mathbb{Q}$ gilt $\sigma^2 = \mathrm{id}$.

c) Ist Z ein Zwischenkörper von $K|\mathbb{Q}$ mit $[Z:\mathbb{Q}] < \infty$, so gibt es Elemente $\sqrt{p_1},\ldots,\sqrt{p_n}$ in M mit $Z \subset \mathbb{Q}\left[\sqrt{p_1},\ldots,\sqrt{p_n}\right]$.

d) Jedes solche Z ist über $\mathbb{Q}$ galoissch und $[Z:\mathbb{Q}]$ ist eine Potenz von 2.

K4.26 [Frühjahr 1989] Zeigen Sie, daß für das Polynom $f(X) = X^4 - 16X^2 + 4$ gilt:

a) Es ist über $\mathbb{Q}$ irreduzibel.

b) Es ist über $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(\sqrt{15})$ reduzibel, aber über keiner anderen quadratischen Erweiterung von $\mathbb{Q}$.

c) Es ist über jedem endlichen Körper reduzibel.

d) Es hat die Wurzeln $\pm\sqrt{3} \pm \sqrt{5}$.

K4.27 [Frühjahr 1991]

a) Man zeige, daß $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$ die einzigen echten Unterkörper von $\mathbb{Q}(\sqrt{2},\sqrt{3})$ sind.

b) Man berechne das Minimalpolynom von $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$ und über $\mathbb{Q}(\sqrt{2})$.

K4.28 [Frühjahr 1993] Sei $K|\mathbb{Q}$ die Körpererweiterung, die aus $\mathbb{Q}$ durch Adjunktion aller komplexen Nullstellen aller Polynome X^2+aX+b mit $a,b\in\mathbb{Q}$ hervorgeht. Ferner sei M die Menge der Quadratwurzeln $\sqrt{p}$, wobei $p=-1$ oder p eine Primzahl ist. Zeigen Sie:

a) $K=\mathbb{Q}(M)$.

b) Für jeden Zwischenkörper Z von $K|\mathbb{Q}$ mit $[Z:\mathbb{Q}]<\infty$ gibt es Elemente $\sqrt{p_1},\ldots,\sqrt{p_n}\in M$ mit $Z\subseteq\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n})$.

c) Jede solche Erweiterung $Z|\mathbb{Q}$ ist galoissch und ihre Galoisgruppe $\mathrm{Gal}(Z|\mathbb{Q})$ ist isomorph zu einem Produkt $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\ldots\times\mathbb{Z}/2\mathbb{Z}$.

K4.29 [Herbst 1993] Bestimmen Sie alle Unterkörper von $L:=\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7})$, und geben Sie deren Körpergrad über $\mathbb{Q}$ an.

K4.30 [Frühjahr 1995] Sei $M:=\mathbb{Q}(\sqrt{2},\sqrt{6},i)$ (wobei $i^2=-1$).

a) Berechnen Sie den Körpergrad $[M:\mathbb{Q}]$.

b) Zeigen Sie, daß $\mathbb{Q}\subset M$ Galoiserweiterung ist und berechnen Sie $\mathrm{Aut}(M|\mathbb{Q})$.

K4.31 [Herbst 1999]

a) Sei K ein Erweiterungskörper von $\mathbb{Q}$ mit $[K:\mathbb{Q}]=2$. Zeigen Sie, dass es genau eine quadratfreie Zahl $m\in\mathbb{Z}$ gibt, so dass $K\simeq\mathbb{Q}[\sqrt{m}]$ ist. ($m\in\mathbb{Z}$ heißt *quadratfrei*, wenn $m\notin\{0,1\}$ und wenn m nicht durch das Quadrat einer Primzahl teilbar ist.)

b) Sei $\alpha:=\sqrt{7}+\sqrt{6}$. Man berechne das Minimalpolynom von α über $\mathbb{Q}$, den zugehörigen Zerfällungskörper und seine Galoisgruppe.

K4.32 [Frühjahr 2000] Beweisen Sie folgende Aussagen:

a) Die Körper $\mathbb{Q}(\sqrt{d})$, wobei d die quadratfreien ganzen Zahlen ungleich 1 durchlaufe, sind genau alle quadratischen Erweiterungskörper von $\mathbb{Q}$.

b) Sind $d_1,\ldots,d_n$ paarweise teilerfremde, quadratfreie ganze Zahlen ungleich 1, so ist $\mathbb{Q}(\sqrt{d_1},\ldots,\sqrt{d_n})$ eine über $\mathbb{Q}$ galoissche Erweiterung mit Galoisgruppe $(\mathbb{Z}/2\mathbb{Z})^n$.

c) Die Quadratwurzeln von endlich vielen paarweise verschiedenen Primzahlen sind linear unabhängig über $\mathbb{Q}$.

Zyklische Galoisgruppen

K4.33 [Frühjahr 1984]

a) Zeigen Sie, daß die Abbildung $f:\ x\mapsto\frac{-1}{1+x}$ auf $\mathbb{R}\setminus\{0,-1\}$ eine fixpunktfreie Permutation der Ordnung 3 ist!

b) Zeigen Sie: Genau dann ist mit y auch $f(y)$ eine Nullstelle von $X^3+aX^2+bX+c\in\mathbb{Z}[X]$, wenn $c=-1$ und $b=a-3$ ist.

c) Zeigen Sie, daß $P:=X^3+aX^2+(a-3)X-1$ für jedes $a\in\mathbb{Z}$ irreduzibel über $\mathbb{Q}$ ist und bestimmen Sie die Galoisgruppe von P über $\mathbb{Q}$!

K4.34 [Herbst 1988]

a) Zeigen Sie: Die Substitution

$$\varphi : \; x \mapsto \frac{1+x}{1-x}$$

ist eine Permutation der Ordnung 4 auf $\mathbb{R} \setminus \{-1, 0, 1\}$, deren Quadrat keine Fixpunkte hat.

b) Bestimmen Sie $k(x) = x + \varphi(x) + \varphi^2(x) + \varphi^3(x)$.

c) Beweisen Sie: Ist a eine Nullstelle von $x^4 - kx^3 - 6x^2 + kx + 1$, so auch $\varphi(a)$.

d) Sei k eine ganze Zahl.
Zeigen Sie: $x^4 - kx^3 - 6x^2 + kx + 1$ hat keine rationalen Nullstellen und ist für $k \notin \{-3, 0, 3\}$ irreduzibel über $\mathbb{Q}$.

e) Sei k eine ganze Zahl und $R_k = \mathbb{Q}[x]/(x^4 - kx^3 - 6x^2 + kx + 1)\,\mathbb{Q}[x]$.
Beweisen Sie: Für $k \notin \{-3, 0, 3\}$ ist R_k eine normale Erweiterung von $\mathbb{Q}$.

K4.35 [Herbst 1994] Sei L der Zerfällungskörper des Polynoms $f(X) = X^4 - 2$ über dem Körper $K = \mathbb{Q}(i)$, $i^2 = -1$. Man bestimme die Galoisgruppe $\mathrm{Gal}(L|K)$ der Erweiterung $L|K$ und die Zwischenkörper von $L|K$.

K4.36 [Herbst 1995] Sei $f := X^4 - 2 \in \mathbb{Q}[X]$ und L der Zerfällungskörper von f. Man zeige:

a) $L = \mathbb{Q}[i, \sqrt[4]{2}]$.

b) $[L : \mathbb{Q}] = 8$.

c) $L = \mathbb{Q}[i + \sqrt[4]{2}]$.

d) $\mathrm{Aut}(L|\,\mathbb{Q}[i])$ ist zyklisch; das erzeugende Element σ ist bestimmt durch $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$.

e) Man bestimme die Automorphismengruppe $\mathrm{Aut}(L|\,\mathbb{Q}[\sqrt[4]{2}])$.

K4.37 [Herbst 1990] In dieser Aufgabe ist der Grundkörper $K = \mathbb{Q}(i)$. Es sei $f(X) = X^8 - 2$, α eine Nullstelle von $f(X)$ und $L := K(\alpha)$.
Man beweise die folgenden Aussagen a) bis e).

a) $f(X)$ ist über K irreduzibel.

b) L enthält die achten Einheitswurzeln.

c) L ist Zerfällungskörper von $f(X)$ über K.

d) Es gibt genau einen Automorphismus σ von $L|K$ mit $\sigma(\alpha) = (1+i)\alpha^{-3}$.

e) Die Galoisgruppe von $L|K$ ist zyklisch und wird von dem Automorphismus σ in Teil d) der Aufgabe erzeugt.

f) Man bestimme alle Zwischenkörper von $L|K$.

K4.38 [Herbst 1995]

a) Zeigen Sie, daß $f = X^8 - 2$ über $\mathbb{Q}(i)$ irreduzibel ist.

b) Bestimmen Sie den Zerfällungskörper L von f über $\mathbb{Q}(i)$ und berechnen Sie den Grad $[L : \mathbb{Q}(i)]$.

c) Beweisen Sie, daß die Galoisgruppe von $L|\,\mathbb{Q}(i)$ zyklisch ist.

d) Bestimmen Sie alle Zwischenkörper von $L|\,\mathbb{Q}(i)$.

e) Bestimmen Sie den Grad des Zerfällungskörpers von f über dem Grundkörper $\mathbb{Z}/17\mathbb{Z}$.

K4.39 [Frühjahr 1976] Man beweise:

a) Sind K, L, k Unterkörper eines Körpers, gilt $L \cap K = k$, und ist die Körpererweiterung K von k normal, so ist das Minimalpolynom über k eines Elementes von K irreduzibel über L.

b) Eine Galoiserweiterung K von $\mathbb{Q}$ mit zyklischer Galoisgruppe der Ordnung 4 enthält nicht $\sqrt{-1}$.

HINWEIS: Man fasse K als Unterkörper von $\mathbb{C}$ auf und beachte $\mathbb{R} \subset \mathbb{C}$.

K4.40 [Frühjahr 1978] Eine galoissche Erweiterung $K|\mathbb{Q}$ mit zyklischer Galoisgruppe der Ordnung 4 kann nicht $\sqrt{-1}$ enthalten.

HINWEIS: Man ziehe den Körper $\mathbb{R}$ der reellen Zahlen heran.

K4.41 [Frühjahr 1993] Es gibt keine galoissche Erweiterung $K|\mathbb{Q}$ mit zyklischer Galoisgruppe der Ordnung 4, welche $i = \sqrt{-1}$ enthält.

HINWEIS: Fassen Sie K als Teilkörper von $\mathbb{C}$ auf!

K4.42 [Frühjahr 1977] Zeigen Sie:

a) Sei G eine endliche Gruppe, die genau eine größte echte Untergruppe U besitzt (d.h. U enthält alle echten Untergruppen von G). Dann ist G abelsch.

b) Sei $K|k$ eine endliche galoissche Körpererweiterung. Es besitze die Menge $\{L;\ k \subsetneq L \subseteq K\}$ der Zwischenkörper $\neq k$ ein kleinstes Element. Dann ist jeder Zwischenkörper L galoissch über k.

Artin-Schreier-Gleichungen

K4.43 [Herbst 1991] Für eine endliche Körpererweiterung $K|k$ bezeichne $\mathrm{tr}_{K|k} : K \to k$ die Spurabbildung. Man beweise mit den Mitteln der linearen Algebra:

Ist $K|k$ eine endliche zyklische Erweiterung und σ ein erzeugendes Element der Galoisgruppe G von $K|k$, so sind für ein Element $\alpha \in K$ die folgenden Bedingungen äquivalent:

i) $\mathrm{tr}_{K|k}(\alpha) = 0$

ii) $\alpha = \sigma(\beta) - \beta$ mit einem $\beta \in K$.

K4.44 [Herbst 1991] Es sei k ein Körper der Primzahlcharakteristik p und $K|k$ eine galoissche Erweiterung vom Grad p. Man beweise, daß K Zerfällungskörper eines irreduziblen Polynoms der Form $X^p - X - a$ über k ist.

HINWEIS: Benutze vorige Aufgabe und $\mathrm{tr}_{K/k}(1) = 0$.

K4.45 [Frühjahr 1972] Sei K ein Körper der Charakteristik $p > 0$ und $f := X^p - X - a$ ein irreduzibles Element des Polynomringes über K in der Unbestimmten X. Ferner sei x eine Wurzel von f in einer algebraischen Abschließung von K.

a) Man zeige: Der durch Adjunktion von x an K entstehende Körper $K(x)$ ist normal.

b) Man zerlege f in $(K(x))[X]$ in Faktoren ersten Grades.

K4.46 [Frühjahr 1976] Sei k ein Körper der Charakteristik $p \neq 0$ und K der Zerfällungskörper des Polynoms $f = X^p - X - a \in k[X]$ über k. Man beweise:

a) Ist $x \in K$ eine Nullstelle von f, so auch $x + 1$.

b) K ist eine Galoiserweiterung von k.

c) Wenn f in $k[X]$ nicht in Linearfaktoren zerfällt, ist die Galoisgruppe von f über k eine zyklische Gruppe der Ordnung p.

K4.47 [Frühjahr 1976] Es sei p eine Primzahl, K ein kommutativer Körper der Charakteristik p und $f := x^p - x - a$ ein Polynom aus dem Polynomring $K[x]$.

a) Zeigen Sie: Die Differenz verschiedener Lösungen von f in einem geeigneten Erweiterungskörper von K liegt im Primkörper von K.

b) Zeigen Sie: Ist f irreduzibel in $K[x]$, so ist der Restklassenring $L := K[x]/(f)$ von $K[x]$ nach dem von f erzeugten Ideal (f) der Zerfällungskörper von f.

c) Geben Sie die Galois-Gruppe der Körpererweiterung L über K an, wenn f irreduzibel ist.

d) Zeigen Sie: f ist genau dann irreduzibel in $K[x]$, wenn in K keine Nullstelle von f liegt. (Beachte Teil a)!)

K4.48 [Herbst 1993] Sei $f \in K[X]$ ein normiertes irreduzibles Polynom über einem Körper K, sei α eine Nullstelle von f in einem Erweiterungskörper von K und es gelte $f(\alpha + 1) = 0$. Man zeige:

a) Der Körper K hat positive Charakteristik.

Ist $\mathrm{char}(K) = p$ eine Primzahl und gilt zudem $\alpha^p - \alpha \in K$, so zeige man:

b) f stimmt mit dem Polynom $X^p - X - \alpha^p + \alpha$ überein.

c) Die Erweiterung $K(\alpha)|K$ hat eine zyklische Galoisgruppe der Ordnung p.

Kummertheorie

K4.49 [Herbst 1976] Sei k ein beliebiger Körper und K eine Galois-Erweiterung von k mit Galois-Gruppe G. Man beweise:

a) Zu jedem Charakter (= Homomorphismus) $\chi : G \to K^\times$ gibt es ein $x \in K$ mit

$$a := \sum_{\phi \in G} \chi(\phi)\phi(x) \neq 0 \quad .$$

ANLEITUNG: Man zeige, daß endlich viele paarweise verschiedene Automorphismen von K linear unabhängig über K sind.

b) Eine Abbildung $\chi : G \to k^\times$ ist genau dann ein Charakter, wenn es ein $a \in K^\times$ gibt mit

$$\chi(\psi) = \frac{a}{\psi(a)} \text{ für jedes } \psi \in G \quad .$$

c) Zu $a, b \in K^\times$ mit

$$\frac{a}{\phi(a)} = \frac{b}{\phi(b)} \text{ für alle } \phi \in G$$

gibt es ein $c \in k$ mit $b = ca$.

K4.50 [Herbst 1982] K sei ein Körper der Charakteristik $p \geq 0$, der eine primitive n-te Einheitswurzel enthält. Sei p kein Teiler von n und L der Zerfällungskörper des Polynoms

$$(X^n - a_1)(X^n - a_2) \cdot \ldots \cdot (X^n - a_r) \text{ mit } a_i \in K \quad (i = 1, \ldots, r) \quad .$$

Beweisen Sie:

a) $L|K$ ist Galoiserweiterung.

b) Die Galoisgruppe G von $L|K$ ist abelsch.

c) Die Ordnung jedes Elements von G ist ein Teiler von n.

K4.51 [Frühjahr 1995] Sei $L|K$ eine endliche Galoiserweiterung und p eine Primzahl. Es gebe ein $\alpha \in L$ mit $\alpha^p \in K$ und $\alpha^n \notin K$ für $1 \leq n < p$. Zeigen Sie: L enthält eine primitive p-te Einheitswurzel.

K4.52 [Frühjahr 1985] Seien K ein Körper der Charakteristik 0, $n \in \mathbb{N}$ und $\varepsilon \in K$ eine primitive n-te Einheitswurzel und $a \in K$, so daß $X^n - a$ irreduzibel über K ist. Sei M ein Zerfällungskörper von $X^n - a$ und $\alpha \in M$ mit $\alpha^n = a$. Beweise:

a) Es ist $M = K(\alpha)$ und M ist Galoiserweiterung von K vom Grad n.

b) Seien $k, h \in \mathbb{N}$ mit $n = k \cdot h$. Dann gibt es genau einen Zwischenkörper L, also $K \subseteq L \subseteq M$, mit $[L : K] = k$, nämlich $L = K(\alpha^h)$.

K4.53 [Frühjahr 1994] Es sei K ein Körper, der eine primitive n-te Einheitswurzel enthält. Außerdem sei $\operatorname{char} K = p$, $p \neq 0$, also ist p kein Teiler von n. Es sei L ein Zerfällungskörper des Polynoms $f = (x^n - a_1)(x^n - a_2) \in K[x]$. Zeigen Sie:

a) $L|K$ ist eine Galois-Erweiterung.

b) Die Galois-Gruppe $G = \operatorname{Gal}(L|K)$ ist abelsch.

c) Die Ordnung jedes Elements von G teilt n.

K4.54 [Herbst 1994] Sei K ein Körper. Zeigen Sie: Ist n eine positive ganze Zahl, die kein Vielfaches der Charakteristik von K ist, und enthält K die n-ten Einheitswurzeln, so ist jede Körpererweiterung L der Form $K(\sqrt[n]{a}), a \in K$, von K eine Galoiserweiterung mit zyklischer Galoisgruppe $\operatorname{Gal}(L|K)$. Die Ordnung von $\operatorname{Gal}(L|K)$ ist ein Teiler von n.

K4.55 [Frühjahr 1996] Seien k, ℓ, n natürliche Zahlen mit $n = k\ell$. Sei K ein Körper der Charakteristik 0, der eine primitive n-te Einheitswurzel enthält. Sei $f = X^n - a$ ein irreduzibles Polynom aus $K[X]$ und L sein Zerfällungskörper über K. Sei $z \in L$ eine Nullstelle von f. Man zeige:

a) Es ist $L = K(z)$.

b) Es gibt genau einen Zwischenkörper Z von $L|K$ mit $[Z : K] = k$.

c) Es ist $Z = K(z^\ell)$.

Abelsche Galoisgruppen

K4.56 [Frühjahr 1980] Man bestimme den Zerfällungskörper $K \subset \mathbb{C}$ des Polynoms $f(x) = x^4 - 3x^2 + 4 \in \mathbb{Q}[x]$. Man zeige, daß die Galoisgruppe von $K|\mathbb{Q}$ die Kleinsche Vierergruppe ist und ermittle alle Teilkörper von K.

K4.57 [Herbst 1994] Bestimmen Sie den Zerfällungskörper K und die Galoisgruppe G von

$$x^4 - 4x^2 + 1$$

über $\mathbb{Q}$. Welche Unterkörper hat K?

K4.58 [Herbst 1996] Bestimmen Sie den Isomorphietyp der Galoisgruppe des Polynoms $x^4 - 13x^2 + 1$ über dem Körper der rationalen Zahlen.

K4.59 [Herbst 1995] Man beweise: Ist das Polynom $f := X^4 + aX^2 + 1$ mit $a \in \mathbb{Z}$ irreduzibel über $\mathbb{Q}$, dann hat der Zerfällungskörper von f über $\mathbb{Q}$ den Grad 4 und seine Galoisgruppe ist die nichtzyklische Gruppe der Ordnung 4.

K4.60 [Herbst 1979] Beweisen Sie die folgenden Aussagen.

a) Ist das Polynom $f := x^4 + ax^2 + 1$ mit $a \in \mathbb{Z}$ irreduzibel über $\mathbb{Q}$, dann hat der Zerfällungskörper von f über $\mathbb{Q}$ den Grad 4.

b) Das Polynom f ist genau dann über $\mathbb{Q}$ irreduzibel, wenn $\sqrt{2-a} \notin \mathbb{Z}$ und $\sqrt{-2-a} \notin \mathbb{Z}$.

c) Ist das Polynom f irreduzibel über $\mathbb{Q}$, dann ist seine Galoisgruppe über $\mathbb{Q}$ die nichtzyklische Gruppe der Ordnung 4.

Seien weiterhin K stets ein endlicher Körper und

$$K^2 := \{\mu \in K\,;\ \exists \lambda \in K:\ \lambda^2 = \mu\} \quad .$$

d) Hat der Körper K die Charakteristik 2, dann ist $K = K^2$. Hat der Körper K nicht die Charakteristik 2, dann gilt:

$$2|K^2| = |K| + 1 \quad .$$

(Ohne Beweis sind Kenntnisse über die multiplikative Gruppe endlicher Körper und über Potenzendomorphismen abelscher Gruppen verwendbar.)

e) Für $\lambda, \mu \in K \setminus K^2$ gilt: $\lambda\mu \in K^2$.

f) Das Polynom $g := x^4 + ax^2 + 1$ mit $a \in K$ ist stets reduzibel über K. (Verwenden Sie d), e) und den Beweis von b).)

g) Hat das Polynom g keine Nullstelle in K, so ist seine Galoisgruppe über K die zyklische Gruppe der Ordnung 2.

K4.61 [Frühjahr 1995] Sei $\alpha = \sqrt{5 + 2\sqrt{5}}$.

a) Man bestimme das Minimalpolynom von α über $\mathbb{Q}$.

b) Zeigen Sie: $\mathbb{Q}(\alpha)|\,\mathbb{Q}$ ist galoissch.

c) Bestimmen Sie die Galoisgruppe von $\mathbb{Q}(\alpha)|\,\mathbb{Q}$.

K4.62 [Herbst 2000] Sei $\alpha \in \mathbb{C}$ eine Lösung der Gleichung

$$\alpha^4 + 2\alpha^3 + 5\alpha^2 + 4\alpha + 1 = 0 \quad .$$

a) Seien $\beta := 2\alpha^3 + 3\alpha^2 + 9\alpha + 4$ und $\gamma := \alpha - \beta$. Zeigen Sie, dass β das Minimalpolynom $X^2 + 1$ und γ das Minimalpolynom $X^2 + X + 1$ über $\mathbb{Q}$ hat.

b) Zeigen Sie, daß $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ galoissch ist, und bestimmen Sie die Galoisgruppe.

K4.63 [Frühjahr 1985] Es sei K ein Körper, $\operatorname{char} K = 0$, $f \in K[X]$ ein irreduzibles Polynom und L ein Zerfällungskörper von f über K.

a) Man zeige: Ist die Galois-Gruppe $\operatorname{Gal}(L|K)$ abelsch und ist $\eta \in L$ eine beliebige Nullstelle von f, dann gilt $L = K(\eta)$.

HINWEIS: Man beachte, daß alle Untergruppen von $\operatorname{Gal}(L|K)$ Normalteiler sind.

b) Ist die unter a) gemachte Aussage für $K = \mathbb{Q}$ auch ohne die Voraussetzung über die Galois-Gruppe richtig? Ist dies nicht der Fall, dann belege man dies durch ein Beispiel. Begründen Sie Ihre Antworten!

c) Es sei $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ die gewöhnliche Quaternionengruppe ($i \cdot j = k = -j \cdot i$, $j \cdot k = i = -k \cdot j$, $k \cdot i = k = -i \cdot k$ und $i^2 = j^2 = k^2 = -1$).
Ist $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, L der Zerfällungskörper von f und $\operatorname{Gal}(L|\,\mathbb{Q}) = Q$, gilt dann auch $L = K(\eta)$ für jede Nullstelle $\eta \in L$ von f?
Begründen Sie Ihre Antwort!

K4.64 [Frühjahr 1994] Sei k ein Körper und $f(t) \in k[t]$ ein irreduzibles, separables Polynom über k mit abelscher Galoisgruppe G. Zeigen Sie, daß die Ordnung von G gleich dem Grad von f ist.

K4.65 [Frühjahr 1977] Betrachte das folgende Polynom

$$f(X) = X^5 + 9X^3 + X^2 - 10X + 10 \quad .$$

a) Man zerlege f über dem Körper $\mathbb{Q}$ der rationalen Zahlen in irreduzible Faktoren.

b) Man bestimme die Galoisgruppe von f über $\mathbb{Q}$.

c) Man zerlege f über dem Körper $\mathbb{F}_7$ mit 7 Elementen in irreduzible Faktoren.

d) Man bestimme die Galoisgruppe von f über $\mathbb{F}_7$.

S_3 als Galoisgruppe

K4.66 [Frühjahr 1998] Sei k ein Körper und $L = k(X_1, X_2)$ der Körper der rationalen Funktionen in den Variablen X_1, X_2. Für

$$X_3 := -(X_1 + X_2) \quad , \quad Q := X_1X_2X_3 \quad , \quad P := X_1X_2 + X_2X_3 + X_3X_1$$

in L setze man $K = k(P, Q) \subseteq L$. Zeigen Sie: Die Körpererweiterung $L|K$ ist eine Galoiserweiterung mit Galoisgruppe S_3.

K4.67 [Herbst 1979]

a) Man gebe alle Untergruppen der symmetrischen Gruppe $\mathfrak{S}_3$ an.

b) Man zeige, daß das Polynom

$$f(X) := X^3 + 7X + 7$$

in $\mathbb{Q}[X]$ irreduzibel ist ($\mathbb{Q}$ bezeichnet der Körper der rationalen Zahlen).

c) Man zeige, daß $f(X) = X^3 + 7X + 7$ genau eine reelle Nullstelle besitzt; diese reelle Nullstelle sei mit α bezeichnet. Man gebe den Grad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ an. Zerfällt $X^3 + 7X + 7$ über $\mathbb{Q}(\alpha)$ in Linearfaktoren? Ist die Körpererweiterung $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ galoissch?

d) Es sei $L \supset \mathbb{Q}$ ein Zerfällungskörper von X^3+7X+7. Man gebe $[L : \mathbb{Q}]$ an. Ist die Galoisgruppe von $X^3 + 7X + 7 \in \mathbb{Q}[X]$ abelsch?

K4.68 [Herbst 1978] Sei M der Zerfällungskörper von $x^3 - 5$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen.

a) Man bestimme $[M : \mathbb{Q}]$, die Dimension von M über $\mathbb{Q}$.

b) Man bestimme die Ordnung der Galoisgruppe G von M über $\mathbb{Q}$.

c) Man bestimme alle Körper F mit $\mathbb{Q} \subseteq F \subseteq M$.

d) Man bestimme alle Untergruppen von G.

e) Man beschreibe die Beziehung zwischen c) und d).

K4.69 [Frühjahr 1979] Es sei S ein Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$.

a) Man beweise, daß S über $\mathbb{Q}$ den Grad 6 hat.

b) Man begründe, weshalb S über $\mathbb{Q}$ galoissch ist.

c) Man bestimme die Galoisgruppe $\mathrm{Gal}(S|\mathbb{Q})$ von S über $\mathbb{Q}$ bis auf Isomorphie.

K4.70 [Frühjahr 1982] Sei $f := X^3 + 2X + 2 \in \mathbb{Q}[X]$.

a) Man zeige, daß f irreduzibel ist.

b) Man zeige, daß f genau eine reelle Nullstelle a besitzt und gebe den Grad $[\mathbb{Q}(a) : \mathbb{Q}]$ an. Ist $\mathbb{Q}(a)|\mathbb{Q}$ eine Galois-Erweiterung?

c) Man stelle a^{-1} als Linearkombination von $1, a, a^2$ dar.

d) Man bestimme die Galoisgruppe von f.

K4.71 [Frühjahr 1986] Sei $f := 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} \in \mathbb{Q}[X]$. Zeigen Sie:

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

b) f hat genau eine reelle Nullstelle.

c) Ist K ein Zerfällungskörper von f, so gilt

$$\mathrm{Gal}(K|\mathbb{Q}) \simeq S_3 \quad .$$

K4.72 [Frühjahr 1988]

a) Zerlege das über $\mathbb{Q}$ irreduzible Polynom $f(t) = t^3 - 7$ aus $\mathbb{Q}[t]$ über dem Körper $K = \mathbb{Q}[t]/(f)$ in irreduzible Faktoren.

b) Bestimme den Zerfällungskörper L von f über $\mathbb{Q}$. Welchen Grad hat die Körpererweiterung $L|\mathbb{Q}$?

c) Finde ein $\alpha \in L$ mit der Eigenschaft $L = \mathbb{Q}(\alpha)$.

d) Zeige, daß die Galoisgruppe von L über $\mathbb{Q}$ isomorph zur symmetrischen Gruppe S_3 ist.

e) Bestimme alle Zwischenkörper der Erweiterung L über $\mathbb{Q}$.

K4.73 [Frühjahr 1992]

a) Sei a eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $f(t) = t^3 - 2$. Zerlegen Sie $f(t)$ über dem Körper $\mathbb{Q}(a)$ in irreduzible Faktoren.

b) Geben Sie den Zerfällungskörper L von f über $\mathbb{Q}$ an. Welchen Grad hat die Körpererweiterung $L|\mathbb{Q}$? Bestimmen Sie die Galoisgruppe.

K4.74 [Frühjahr 1993] Es seien p eine Primzahl, α eine Nullstelle von $f(X) = X^3 + p^2$ und E der Zerfällungskörper von f in $\mathbb{C}$.

a) Begründen Sie, warum $E \neq \mathbb{Q}(\alpha)$ ist.

b) Welchen Grad und welche Galoisgruppe hat E über $\mathbb{Q}$?

c) Geben Sie für jeden Körper $L \neq E$ mit $L \subset E$ ein primitives Element an!

K4.75 [Herbst 1990] Sei $\mathbb{Q}[X,Y]$ der Polynomring in Unbestimmten X, Y, sei I das von $X^3 - 2$ und $X^2 + XY + Y^2$ in $\mathbb{Q}[X,Y]$ erzeugte Ideal I.

a) Zeigen Sie, daß $\mathbb{Q}[X,Y]/I =: K$ ein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ ist, und geben Sie die Galoisgruppe von K über $\mathbb{Q}$ an.

b) Zeigen Sie, daß man einen Isomorphismus

$$\mathbb{Q}[Z]/(Z^6 + 108) \xrightarrow{\sim} K$$

durch $Z \mapsto X + 2Y$ hat.

K4.76 [Frühjahr 2003] Sei x eine komplexe Zahl mit $x^6 + 675 = 0$. Zeigen Sie:

a) Es ist $\sqrt{-3} \in \mathbb{Q}(x)$.

b) Der Körper $\mathbb{Q}(x)$ ist eine normale Erweiterung von $\mathbb{Q}$.

c) Das Polynom $X^6 + 675$ hat eine zu S_3 isomorphe Galoisgruppe über $\mathbb{Q}$.

K4.77 [Herbst 1984] Zeigen Sie: Die Galoisgruppe des Polynoms $x^6 + 3$ über $\mathbb{Q}$ ist isomorph zur symmetrischen Gruppe S_3.

D_4 als Galoisgruppe

K4.78 [Herbst 1985] Das Polynom $f = x^4 + 2$ soll über dem Körper $\mathbb{Q}$ der rationalen Zahlen und über $\mathbb{F}_5$, dem Körper mit 5 Elementen, untersucht werden.

a) Zeigen Sie, daß die Diedergruppe D_4 der Ordnung 8 isomorph zur 2-Sylowgruppe der symmetrischen Gruppe S_4 ist!

b) Zeigen Sie, daß die Galoisgruppe von f über $\mathbb{Q}$ isomorph zu D_4 ist!

c) Bestimmen Sie die Galoisgruppe von f über $\mathbb{F}_5$!

K4.79 [Herbst 1974] Es sei N der Zerfällungskörper von $x^4 - 3$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen und es sei $r = \sqrt[4]{3}$, $r \in \mathbb{R}$, $r > 0$.

a) Man berechne die Ordnung der Galoisgruppe von N über $\mathbb{Q}$ und gebe eine Vektorraumbasis des Vektorraumes N über $\mathbb{Q}$ an.

b) Man zeige, daß die $\mathbb{Q}$-Automorphismen δ, σ von N mit

$$\delta(r) = ir \quad , \quad \delta(i) = i \qquad \text{und} \qquad \sigma(r) = r \quad , \quad \sigma(i) = -1$$

die Galoisgruppe von N über $\mathbb{Q}$ erzeugen.

c) Man gebe die Elemente der Galoisgruppe von N über $\mathbb{Q}$ an, die die Galoisgruppe von N über $\mathbb{Q}(r(1+i))$ bzw. die Galoisgruppe von N über $\mathbb{Q}(r(1-i))$ erzeugen.

d) Man wähle fünf beliebige aber verschiedene Untergruppen $U_1, \ldots, U_5$ der Galoisgruppe von N über $\mathbb{Q}$ und gebe die Zwischenkörper $L_1, \ldots, L_5$ zwischen N und $\mathbb{Q}$ an, so daß U_i die Galoisgruppe von N über L_i ist für alle $i = 1, \ldots, 5$.

K4.80 [Herbst 1981] Bestimmen Sie die Galoisgruppen des Polynoms $g = x^4 - 3$ über $\mathbb{Q}$ und über $\mathrm{GF}(5)$, dem Körper mit 5 Elementen.

K4.81 [Herbst 1989] Sei das Polynom $f = x^4 - 3$ gegeben.

a) Geben Sie eine Zerlegung von f über dem Körper $K = \mathbb{Q}[x]/(f)$ in irreduzible Polynome an.

b) Bestimmen Sie den Zerfällungskörper von f über $\mathbb{Q}$ und seinen Grad über $\mathbb{Q}$.

c) Bestimmen Sie die Galoisgruppe von f über $\mathbb{Q}$ und über $\mathbb{F}_5$.

K4.82 [Frühjahr 1992] Es sei E der Zerfällungskörper des Polynoms $X^4 - 3$ über $\mathbb{Q}$. Zeigen Sie:

a) Der Grad von E über $\mathbb{Q}$ ist 8.

b) Die Galoisgruppe von E über $\mathbb{Q}$ ist nicht abelsch.

K4.83 [Herbst 1988]

a) Bestimme die Galoisgruppe von $X^4 - 3 \in \mathbb{Q}[X]$ über $\mathbb{Q}$.

b) Bestimme die Galoisgruppe von $X^4 + 4 \in \mathbb{Q}[X]$ über $\mathbb{Q}(i)$.

K4.84 [Herbst 1993] Im Polynomring $\mathbb{Q}[X]$ sei f das Polynom

$$f(X) := X^4 + 3 \quad .$$

a) Man zeige: f ist irreduzibel.

b) Man bestimme den Zerfällungskörper K von f als Unterkörper des Körpers der komplexen Zahlen $\mathbb{C}$, bestimme seinen Grad und gebe eine Basis von K über $\mathbb{Q}$ an.

c) Man skizziere die Wurzeln $\zeta_1, \zeta_2, \zeta_3, \zeta_4 \in \mathbb{C}$ des Polynoms f in der komplexen Ebene und zeige: Die Galois-Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ induziert genau diejenigen Permutationen σ von $\{\zeta_1, \ldots, \zeta_4\}$, für die

$$|\sigma(\zeta_\nu) - \sigma(\zeta_\mu)| = |\zeta_\nu - \zeta_\mu|$$

für alle $\nu, \mu \in \{1, 2, 3, 4\}$ gilt.

d) Man bestimme eine Kompositionsreihe von $\mathrm{Gal}(K|\mathbb{Q})$ und die zugehörige Folge von Unterkörpern von K.

K4.85 [Herbst 1990] Bestimmen Sie die Galois-Gruppen des Polynoms $X^4 - 5$ über den Körpern $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(i)$.

K4.86 [Frühjahr 1986]

a) Bestimmen Sie den Zerfällungskörper K von $p(X) = X^4 + 2X^2 - 6$ über $\mathbb{Q}$.

b) Zeigen Sie, daß die Galoisgruppe G von $K|\mathbb{Q}$ eine Diedergruppe ist. (G kann als Permutationsgruppe auf den Wurzeln von $p(X)$ aufgefaßt werden.)

c) Ermitteln Sie alle Zwischenkörper Z von $K|\mathbb{Q}$ mit $[Z : \mathbb{Q}] = 2$.

K4.87 [Herbst 1987] Sei L ein Zerfällungskörper des Polynoms $X^4 - 2X^2 + 5$ über $\mathbb{Q}$. Ferner sei G die Galoisgruppe von $L|\mathbb{Q}$.

a) Bestimmen Sie $[L : \mathbb{Q}]$.

b) Schreiben Sie L in der Form $L = \mathbb{Q}(i, a, b)$, und beschreiben Sie die Elemente von G durch ihre Wirkung auf i, a, b.

c) Ist G abelsch? Geben Sie ein Element maximaler Ordnung von G an.

d) Geben Sie ein primitives Element von $L|\mathbb{Q}$ an.

K4.88 [Frühjahr 2002] Bestimmen Sie die Galoisgruppe über $\mathbb{Q}$ des Zerfällungskörpers von $\varphi(X) = X^4 + 6X^2 + 2 \in \mathbb{Z}[X]$.

K4.89 [Frühjahr 1999] Sei $f(X) = 1 - \frac{X^2}{2!} + \frac{X^4}{4!} \in \mathbb{Q}[X]$. Sei K der Zerfällungskörper von f über $\mathbb{Q}$.

a) Man beweise, dass der Erweiterungsgrad $[K : \mathbb{Q}] = 8$ ist.

b) Man bestimme die Struktur der Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$.

K4.90 [Frühjahr 1975] Gegeben sei das Polynom

$$f(x) = x^4 - 8x^3 + 22x^2 - 24x + 10 \in \mathbb{Q}[x]$$

und es sei $\alpha \in \mathbb{C}$ eine Nullstelle von $f(x)$.

a) Man weise nach, daß $f(x)$ über $\mathbb{Q}$ irreduzibel ist, und bestätige: $f(x) = f(4-x)$.

b) Man zeige: Es existiert genau ein Automorphismus

$$\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha) \quad \text{mit} \quad \varphi(\alpha) = 4 - \alpha \quad .$$

c) Man gebe den Fixpunktkörper von φ

$$L := \{\zeta \in \mathbb{Q}(\alpha);\ \varphi(\zeta) = \zeta\}$$

an; ferner bestimme man ein erzeugendes Element β der Körpererweiterung L über $\mathbb{Q}$ und das Minimalpolynom von β über $\mathbb{Q}$ und zeige: $L = \mathbb{Q}(i)$.

d) Man bestimme die Nullstellen von $f(x)$, den Zerfällungskörper W von $f(x) \in \mathbb{Q}[x]$ und den Grad $[W : \mathbb{Q}]$.

Weitere Diedergruppen

K4.91 [Frühjahr 2002] Bestimmen Sie die Primfaktorzerlegung von

$$f(x) = x^5 + x^4 + 14x^3 + 14x^2 + 28x + 28$$

über den Polynomringen $\mathbb{F}_2[x], \mathbb{F}_3[x]$ und $\mathbb{Q}[x]$. Bestimmen Sie in diesen drei Fällen jeweils die Ordnung der Galoisgruppe von f.

K4.92 [Frühjahr 1994] Man bestimme den Zerfällungskörper L des Polynoms $f(X) = X^6 + 3$ über $\mathbb{Q}$. Man bestimme den Grad $[L : \mathbb{Q}]$ und die Struktur der Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$.

K4.93 [Herbst 1977]

a) Zeigen Sie, daß das Polynom $x^6 + 35k + 3$ für jedes ganzzahlige k irreduzibel über $\mathbb{Z}$ ist.

b) Beweisen Sie, daß $\mathbb{Q}[x]/(x^6 + 108)\,\mathbb{Q}[x]$ eine normale Erweiterung von $\mathbb{Q}$ ist.

c) Begründen Sie, warum $\mathbb{Q}[x]/(x^3 + 108)\,\mathbb{Q}[x]$ keine normale Erweiterung von $\mathbb{Q}$ ist.

d) Geben Sie anhand von b) und c) die Galoisgruppe von $x^6 + 108$ über $\mathbb{Q}$ an, und geben Sie alle normalen Erweiterungen von $\mathbb{Q}$ an, die in $\mathbb{Q}[x]/(x^6 + 108)\,\mathbb{Q}[x]$ enthalten sind.

K4.94 [Herbst 1983] Sei f das Polynom $f(X) = X^6 - 2$.

a) Man zeige, daß f über $\mathbb{Q}$ irreduzibel ist.

b) Man bestimme den Zerfällungskörper K von f über $\mathbb{Q}$ durch Angabe von Erzeugenden.

c) Man berechne den Körpergrad $[K : \mathbb{Q}]$.

d) Man bestimme die Struktur der Galoisgruppe $G = \mathrm{Gal}(K|\mathbb{Q})$.

e) Man beweise, daß K genau drei über $\mathbb{Q}$ quadratische Teilkörper enthält und bestimme diese.

f) Ist f über $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ irreduzibel?

g) Es sei L der Zerfällungskörper von f über $\mathbb{F}_7$. Man berechne den Körpergrad $[L : \mathbb{F}_7]$.

h) Enthält L einen über $\mathbb{F}_7$ quadratischen Teilkörper?

i) Was ist die Struktur der Galoisgruppe $H = \mathrm{Gal}(L|\mathbb{F}_7)$?

K4.95 [Frühjahr 2001] Seien S_2 respektive S_3 die Gruppen der Permutationen von $\{1,2\}$ resp. $\{1,2,3\}$. Man zeige, dass es eine Galoissche Erweiterung $K|\mathbb{Q}$ gibt mit Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q}) \simeq S_2 \times S_3$.

K4.96 [Herbst 1997] Sei $n > 1$ eine natürliche Zahl, sei K ein Körper der Charakteristik Null, der eine primitive n-te Einheitswurzel ζ enthält, und sei $K(X)$ der Körper der rationalen Funktionen in der Unbestimmten X über K. Ferner seien α bzw. β die K-Automorphismen von $K(X)$, die durch

$$\alpha(X) = \zeta X \qquad \text{bzw.} \qquad \beta(X) = \frac{1}{X}$$

bestimmt sind, sei G die von α, β erzeugte Gruppe und $F \subseteq K(X)$ der Fixkörper von G. Zeigen Sie:

a) G ist die Diedergruppe der Ordnung $2n$.

b) $K(X)$ ist eine Galoiserweiterung vom Grad $2n$ über F.

c) Das Minimalpolynom von X über F ist $T^{2n} - (X^n + X^{-n})T^n + 1$.

d) Es ist $F = K(X^n + X^{-n})$.

Affine lineare Galoisgruppen

K4.97 [Herbst 1989] Gegeben seien in $\mathbb{Q}[X]$ die Polynome

$$f := X^5 - 7 \quad ,$$
$$g := X^4 + X^3 + X^2 + X + 1 \quad .$$

Es sei $\alpha := \sqrt[5]{7} \in \mathbb{R}$, außerdem sei $\xi \in \mathbb{C}$ eine Nullstelle von g.

a) Man zeige, daß die Körpererweiterung $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ nicht galoissch ist.

b) Man zeige, daß $\mathbb{Q}(\xi) \supset \mathbb{Q}$ eine galoissche Erweiterung mit abelscher Galoisgruppe ist.

c) Man zeige, daß $\mathbb{Q}(\alpha, \xi)$ ein Zerfällungskörper von $f \in \mathbb{Q}[X]$ ist; außerdem bestimme man den Grad $[\mathbb{Q}(\alpha, \xi) : \mathbb{Q}]$.

d) Man bestimme die Struktur der Galoisgruppe von $\mathbb{Q}(\xi, \alpha)$ über $\mathbb{Q}(\xi)$.

K4.98 [Frühjahr 1991] Sei L der Zerfällungskörper des Polynoms $X^5 - 2$ über $\mathbb{Q}$. Man berechne $[L : \mathbb{Q}]$.

K4.99 [Herbst 1975] Das Polynom $f(x) = x^7 - 2$ ist über jeder abelschen Erweiterung K des Körpers $\mathbb{Q}$ der rationalen Zahlen irreduzibel.

K4.100 [Herbst 1992]

a) In einer Erweiterung des Körpers K sei a eine primitive fünfte Einheitswurzel und b eine Nullstelle des Polynoms $t^2 - 5$. Man beweise die Inklusion $K(b) \subseteq K(a)$.

b) Beweisen Sie: $X^{10} - 5$ ist irreduzibel über $\mathbb{Q}$ und reduzibel über jedem endlichen Körper.

K4.101 [Herbst 1993] Sei K ein Körper, $n \in \mathbb{N}$ mit $\mathrm{char}\, K \nmid n$ und L ein Zerfällungskörper des Polynoms $X^n - a \in K[X]$. Zeigen Sie: Die Galoisgruppe von $L|K$ ist isomorph zu einer Untergruppe der Gruppe der Matrizen $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ mit $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $y \in \mathbb{Z}/n\mathbb{Z}$.

K4.102 [Frühjahr 1993]

(a) Man beweise, daß $\zeta = \frac{1+i}{\sqrt{2}}$ eine primitive achte Einheitswurzel ist.

(b) Man beweise, daß $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{2}, i)$ ist, und man bestimme den Grad des Körpers über $\mathbb{Q}$.

(c) Man bestimme die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ und alle quadratischen Teilkörper von $\mathbb{Q}(\zeta)$.

(d) Es sei $\alpha = \sqrt[8]{2}$. Man berechne den Grad von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$.

(e) Man beweise, daß $\mathbb{Q}(\alpha, i)$ der Zerfällungskörper des Polynoms $X^8 - 2$ über $\mathbb{Q}$ ist, und man berechne seinen Grad über $\mathbb{Q}$.

(f) Man bestimme die Struktur der Galoisgruppe von $\mathbb{Q}(\alpha, i)$ über $\mathbb{Q}$ durch Angabe von Erzeugenden und definierenden Relationen.

K4.103 [Frühjahr 1997] Sei p eine ungerade Primzahl und q eine weitere Primzahl. Setze $f := X^p - q$.

a) Zeigen Sie: Ist $z \in \mathbb{C}$ eine Nullstelle von f, so enthält der Körper $\mathbb{Q}(z)$ keine weitere Nullstelle von f.

b) Welche Ordnung besitzt die Galoisgruppe von f über $\mathbb{Q}$?

K4.104 [Frühjahr 1999] Sei $K|\mathbb{Q}$ eine galoissche Erweiterung vom Grade 55 mit einer Galoisgruppe G, die nicht abelsch ist.
Man zeige, dass es genau einen echten Zwischenkörper L von $K|\mathbb{Q}$ gibt, der über $\mathbb{Q}$ galoissch ist und bestimme seinen Grad über $\mathbb{Q}$.

K4.105 [Frühjahr 2000] Sei p prim und $f(x) = x^p - a \in \mathbb{Q}[x]$ irreduzibel. Zeigen Sie, dass die Galoisgruppe von $f(x)$ über $\mathbb{Q}$ isomorph ist zu der Gruppe der Transformationen des Primkörpers $\mathbb{F}_p$ von der Form $y \mapsto ky + \ell$ mit $k, \ell \in \mathbb{F}_p$, $k \neq 0$.

K4.106 [Herbst 2000]

a) Man zeige, dass das Polynom $f = X^{1999} - 2000$ irreduzibel über $\mathbb{Q}$ ist.

b) Man bestimme die Ordnung der Galoisgruppe von f über $\mathbb{Q}$.

Auflösbare Galoisgruppen

K4.107 [Herbst 1988]

a) Ist $K(\sqrt[3]{5})$ normal über K, wobei $K := \mathbb{Q}\left(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right)$ ist?

b) Sei $L := \mathbb{Q}(\sqrt[4]{2})$ und $K := \mathbb{Q}(\sqrt[2]{2})$. Zeige: $L|K$ und $K|\mathbb{Q}$ sind normale Körpererweiterungen, aber $L|\mathbb{Q}$ ist es nicht.

c) Seien K_1 und K_2 normale Körpererweiterungen eines Körpers k, und sei L eine gemeinsame Körpererweiterung von K_1 und K_2. Zeige:

i) $K_1 \cdot K_2$ ist normal über k; ($K_1 \cdot K_2$ ist dabei der von K_1 und K_2 in L erzeugte Körper).

ii) $K_1 \cap K_2$ ist normal über k.

K4.108 [Herbst 1972] Nach L. Euler gewinnt man den Zerfällungskörper eines biquadratischen Polynoms

$$f(z) = z^4 + az^2 + bz + c$$

mit Koeffizienten aus einem Körper K dadurch, daß man die Quadratwurzeln $\delta_i = \sqrt{t_i}$ der Nullstellen t_i der sogenannten kubischen Resolventen

$$R(t) = t^3 + 2at^2 + (4c - a^2)t - b^2$$

zum Grundkörper K adjungiert.
Man untersuche die Folge der biquadratischen Polynome

$$f_n(z) = z^4 - z - n \qquad \text{für } n = 1, 2, 3, \ldots$$

aus dem Polynomring $\mathbb{Q}[z]$ über dem rationalen Zahlkörper $\mathbb{Q}$. Es bezeichne G_n die Galoisgruppe des zugehörigen Zerfällungskörpers K_n von f_n über $\mathbb{Q}$.

a) Für welche Werte n ist $f_n(z)$ in $\mathbb{Q}$ irreduzibel?

b) Für welche Werte n ist die Resolvente $R_n(t)$ irreduzibel?

c) Man bestimme Ordnung und Struktur der Galoisgruppe G_n

   i. im Falle eines irreduziblen Polynoms $f_n(z)$,

   ii. im Falle eines reduziblen Polynoms $f_n(z)$.

K4.109 [Frühjahr 1983] Zeigen Sie für das Polynom $f = X^4 + X + 1 \in \mathbb{Z}[X]$:

a) f hat keine reelle Nullstelle.

b) f ist irreduzibel über $\mathbb{Q}$.

   Hinweis: Reduktion modulo 2

c) Ist $u+iv$ (mit $u, v \in \mathbb{R}$) eine Nullstelle von f in $\mathbb{C}$, so ist $g = X^3 - 4X - 1$ das Minimalpolynom von $4u^2$ über $\mathbb{Q}$.

d) Die Galoisgruppe von f über $\mathbb{Q}$ besitzt ein Element der Ordnung 3.

e) Sei a eine Nullstelle von f in $\mathbb{C}$. Ist a, als Punkt der Zahlenebene, aus den Punkten 0 und 1 mit Zirkel und Lineal konstruierbar (Begründung)?

K4.110 [Herbst 1996] Man zeige für das Polynom $f = X^4 - X + 1 \in \mathbb{Z}[X]$:

a) f hat keine reelle Nullstelle.

b) f ist irreduzibel über $\mathbb{Q}$.

   Hinweis: Reduktion modulo 2

c) Ist $u+iv$ (mit $u, v \in \mathbb{R}$) eine Nullstelle von f in $\mathbb{C}$, so ist $g = X^3 - 4X - 1$ das Minimalpolynom von $4u^2$ über $\mathbb{Q}$.

d) Die Galoisgruppe von f über $\mathbb{Q}$ besitzt ein Element der Ordnung 3.

e) Keine Nullstelle $a \in \mathbb{C}$ von f ist, als Punkt der Zahlenebene, aus den Punkten 0 und 1 mit Zirkel und Lineal konstruierbar.

K4.111 [Frühjahr 1995] Sei $F|K$ eine nichttriviale endliche Galoiserweiterung mit auflösbarer Galoisgruppe. Zeigen Sie, daß es einen Zwischenkörper $K \subset E \subseteq F$ gibt, so daß $E|K$ galoissch mit abelscher Galoisgruppe ist.

K4.112 [Herbst 1982] Zeigen Sie: Eine galoissche Erweiterung $N|K$ mit $N \neq K$, deren Galoisgruppe auflösbar ist, besitzt stets eine galoissche Teilerweiterung $L|K$ mit einer Galoisgruppe vom Primzahlgrad.

K4.113 [Herbst 1997] Sei $L|K$ eine galoissche Körpererweiterung vom Grad 40. Beweisen Sie, daß es Zwischenkörper vom Grad 2, 4 und 8 über K gibt, die galoissch über K sind.

K4.114 [Herbst 2001] Sei $L|K$ eine galoissche Körpererweiterung mit einer zur alternierenden Gruppe A_4 isomorphen Galoisgruppe.

a) Bestimmen Sie für jedes $n \in \mathbb{N}$ die Zahl z_n der Zwischenkörper Z von $L|K$ mit dem Grad $[Z : K] = n$.

b) Wie viele Zwischenkörper Z von $L|K$ gibt es, für die $Z|K$ eine Galoiserweiterung ist?

Begründen Sie Ihre Aussagen.

K4.115 [Herbst 2002] Das Polynom

$$f(X) = X^6 + 3X^3 + 3$$

habe die Nullstelle $a \in \mathbb{C}$.

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

b) Zeigen Sie, dass $\mathbb{Q}(a)$ die dritte Einheitswurzel

$$\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

enthält.

c) Zeigen Sie, dass $\mathbb{Q}(a)$ nicht normal über $\mathbb{Q}$ ist.

d) Bestimmen Sie den Grad des Zerfällungskörpers von f über $\mathbb{Q}$.

K4.116 [Frühjahr 1975]

a) Für das Polynom $f = \sum_{i=0}^{n} a_i X^i$ von geradem Grad $n = 2m$ (d.h. $a_n \neq 0$) gelte $a_i = a_{n-i}$ für alle $i = 0, \ldots, m$. Zeige: Die rationale Funktion $X^{-m} f(X)$ ist ein Polynom in $Y = X + X^{-1}$ vom Grade m.

b) Stelle das in a) gesuchte Polynom in Y für

$$f = X^6 + 3X^5 + 5X^3 + 3X + 1 \qquad \in \mathbb{Q}[X]$$

explizit auf, berechne dessen Wurzeln und die Wurzeln von f als Quadratwurzelausdrücke.

c) Bestimme die Grade der von den Wurzeln von f über $\mathbb{Q}$ erzeugten Körper.

d) Zerlege f in $\mathbb{Q}[X]$ und in $\mathbb{R}[X]$ in irreduzible Faktoren.

e) Bestimme die Galoissche Gruppe von f über $\mathbb{Q}$.

Nichtauflösbare Galoisgruppen

K4.117 [Herbst 1997] Es sei $f(X) = X^5 - 5X - 1 \in \mathbb{Q}[X]$.

a) Beweisen Sie, daß f über $\mathbb{Q}$ irreduzibel ist.

b) Bestimmen Sie die Anzahl der reellen Nullstellen von f.

c) Bestimmen Sie die Galoisgruppe von f über $\mathbb{Q}$.

K4.118 [Herbst 1999] Die Antworten auf die folgenden Fragen sind mit einer kurzen Begründung zu versehen:

a) Gibt es ein irreduzibles Polynom aus $\mathbb{Q}[X]$, das in $\mathbb{C}$ eine doppelte Nullstelle besitzt?

b) Gibt es ein irreduzibles Polynom aus $K[X]$, das in einem Erweiterungskörper von K eine doppelte Nullstelle besitzt, wenn K ein endlicher Körper ist?

c) Geben Sie einen Körper K an und ein irreduzibles Polynom aus $K[X]$, das im algebraischen Abschluss von K eine doppelte Nullstelle besitzt.

d) Geben Sie einen Körper K und ein Polynom 5. Grades aus $K[X]$ an, das nicht durch Radikale auflösbar ist.

K4.119 [Herbst 2002] Zu $f \in \mathbb{Q}[x]$ sei G_f die Galoisgruppe von f über $\mathbb{Q}$. Geben Sie — mit Begründung — jeweils ein Beispiel für ein f mit folgender Eigenschaft an:

a) $G_f \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$

b) $G_f \simeq S_5$ (symmetrische Gruppe auf fünf Elementen)

K4.120 [Herbst 1991] Es sei $K|k$ eine endliche galoissche Körpererweiterung, deren Galoisgruppe isomorph zur symmetrischen Gruppe S_n $(n \geq 2)$ ist. Man beweise, daß K einen und nur einen über k quadratischen Teilkörper enthält.

K4.121 [Frühjahr 2003] Sei f ein separables Polynom vom Grad n mit Koeffizienten in einem Körper k. Der Zerfällungskörper K von f über k habe den Grad $n!$ über k. Zeigen Sie, dass f irreduzibel ist, und dass die Galoisgruppe von f über k die symmetrische Gruppe S_n ist.

K4.122 [Frühjahr 1973] Es sei

$$f_k(x) := x^5 - kx + 1 \qquad (k \in \mathbb{Z}) \quad .$$

a) Für welche Werte von k ist $f_k(x)$ über $\mathbb{Q}$ reduzibel?
Man gebe in jedem dieser Fälle die zugehörige Primzerlegung an.

b) Für welche Werte von k hat die Gleichung $f_k(x) = 0$ genau drei reelle Nullstellen?

c) Im Fall $k \geq 3$ zeige man, daß die Galoisgruppe G der Gleichung $f_k(x) = 0$ über $\mathbb{Q}$ einen Zyklus der Länge 5 und eine Transposition enthält. Welche Gruppe ist dann G?

K4.123 [Herbst 2002] Für eine rationale Zahl $q \in \mathbb{Q}$ sei G_q die Galoisgruppe des Polynoms

$$f_q(x) = x^5 - 2002x + q$$

über dem Körper $\mathbb{Q}$ der rationalen Zahlen. Zeigen Sie:

a) Für unendlich viele $q \in \mathbb{Q}$ ist $|G_q| = 120$.

b) Für unendlich viele $q \in \mathbb{Q}$ ist $|G_q|$ ein Teiler von 24.

5. Transzendente Körpererweiterungen

Transzendente Erweiterungen

K5.1 [Herbst 1982] $\mathbb{Q}[X,Y]$ sei der Polynomring in den Unbestimmten X und Y über $\mathbb{Q}$ und $f := X^3 + X^2 - Y^2$.

a) Zeigen Sie, daß $A := \mathbb{Q}[X,Y]/(f)$ ein Integritätsbereich ist.

b) Zeigen Sie, daß der $\mathbb{Q}$-Homomorphismus $\alpha : \mathbb{Q}[X] \to A$, bei dem X auf die Restklasse $X+(f)$ abgebildet wird, injektiv ist.

c) Ist der Quotientenkörper K von A algebraisch über $\mathbb{Q}$?

K5.2 [Herbst 1991] $K(z)$ sei eine einfache transzendente Erweiterung des Körpers K. Man beweise die folgenden beiden Aussagen:

a) $K(z^2)$ ist eine transzendente Erweiterung von K.

b) Es gibt unendlich viele Zwischenkörper zwischen K und $K(z)$.

K5.3 [Herbst 1987] K sei ein Körper, $f \in K[X]$ ein irreduzibles und separables Polynom vom Grad n und L ein Zerfällungskörper von f über K. Seien $a_1, \ldots, a_n$ die Nullstellen von f in L. Weiter seien $\widehat{K} = K(X_1, \ldots, X_n)$ und $\widehat{L} = L(X_1, \ldots, X_n)$ die Körper der rationalen Funktionen in n Unbestimmten $X_1, \ldots, X_n$ über K bzw. L. Beweisen Sie:

a) $\widehat{L}$ ist eine Galoiserweiterung von $\widehat{K}$.

b) Für jedes Element σ der Galoisgruppe $\mathrm{Aut}(\widehat{L}, \widehat{K})$ von $\widehat{L}$ über $\widehat{K}$ gilt: $\sigma(L) \subseteq L$.

c) $\mathrm{Aut}(\widehat{L}, \widehat{K}) \simeq \mathrm{Aut}(L, K)$.

d) Sei $g := a_1 X_1 + \ldots + a_n X_n$ und $\sigma \in \mathrm{Aut}(\widehat{L}, \widehat{K})$. Gilt $\sigma(g) = g$, so ist σ die Identität auf $\widehat{L}$.

e) $\widehat{L} = \widehat{K}(g)$.

K5.4 [Frühjahr 2002] Sei $K(t)$ der Körper der rationalen Funktionen in einer Unbestimmten über einem Körper K, und sei $f \in K(t)$ nicht konstant. Schreiben Sie $f = \frac{g}{h}$ mit $g, h \in K[t]$ und $\mathrm{ggT}(g,h) = 1$. Zeigen Sie:

a) Das Polynom $h(X) \cdot f - g(X) \in K(f)[X]$ ist irreduzibel.

b) Genau dann ist $K(f) = K(t)$, wenn f von der Form

$$f = \frac{at+b}{ct+d} \qquad (a,b,c,d \in K,\ ad - bc \neq 0)$$

ist.

c) Die Automorphismengruppe von $K(t)$ über K ist isomorph zur Faktorgruppe

$$\mathrm{GL}(2,K) \Big/ \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} ;\ \lambda \neq 0 \right\}$$

Inseparable Erweiterungen

K5.5 [Herbst 1991] Es sei K ein Körper der Charakteristik p (p eine Primzahl) und $L = K(t)$ eine einfache transzendente Erweiterung. Man beweise, daß das Polynom $X^p - t$ über L irreduzibel und inseparabel ist.

K5.6 [Frühjahr 1992] Es sei F ein endlicher Körper, z transzendent über F und $K = F(z)$.

a) Warum gibt es keine irreduziblen inseparablen Polynome in $F[X]$?

b) Geben Sie ein irreduzibles inseparables Polynom in $K[X]$ an (mit Begründung!).

K5.7 [Frühjahr 1973] Sei P ein Primkörper der Charakteristik $p > 0$ und sei $L := P(y, z)$ der Körper der rationalen Funktionen in den Unbestimmten y und z mit Koeffizienten in P. Zeige:

a) Das Polynom $X^p - y \in L[X]$ hat nur eine (und folglich p-fache) Nullstelle in einem Zerfällungskörper und ist irreduzibel.

b) Sei β Nullstelle von $X^p - y$ und sei γ Nullstelle von $X^p - z$. Gib eine Basis von $L(\beta, \gamma)$ über L an.

c) Sei $a \in L(\beta, \gamma)$, $a \notin L$. Gib eine Basis von $L(a)$ über L an.

d) Gib unendlich viele verschiedene Zwischenkörper zwischen L und $L(\beta, \gamma)$ an.

K5.8 [Frühjahr 1978] Sei P ein Primkörper der Charakteristik $p > 0$ und sei $L := P(y, z)$ der Körper der rationalen Funktionen in den Unbestimmten y und z mit Koeffizienten in P. Zeige:

a) Das Polynom $X^p - y \in L[X]$ hat nur eine (und folglich p-fache) Nullstelle in einem Zerfällungskörper und ist irreduzibel.

b) Sei β Nullstelle von $X^p - y$ und sei γ Nullstelle von $X^p - z$. Gib eine Basis von $L(\beta, \gamma)$ über L an.

c) Sei $a \in L(\beta, \gamma)$, $a \notin L$. Gib eine Basis von $L(a)$ über L an.

d) Gib unendlich viele verschiedene Zwischenkörper zwischen L und $L(\beta, \gamma)$ an.

Galoistheorie in K(t)

K5.9 [Herbst 1978] Sei k ein Körper und $K := k(x)$ der Körper der rationalen Funktionen in der Unbestimmten x über k. Jedes Element von K hat also die Form $\frac{f(x)}{g(x)}$ mit teilerfremden $f(x), g(x) \in k[x]$. Der *Grad* von $\frac{f(x)}{g(x)}$ sei das Maximum der Grade von $f(x)$ und $g(x)$. Benützen Sie im weiteren folgenden Satz:

SATZ: *Ist* $u = \frac{f(x)}{g(x)} \in K$ *vom Grad* $n > 0$, *so ist* $[K : k(u)] = n$.

a) Zeigen Sie:

i. Für $u \in K$ gilt $K = k(u)$ genau dann, wenn u von der Form

$$\frac{ax + b}{cx + d} \quad , \qquad a, d, b, c \in k \quad \text{mit} \quad ad - bc \neq 0$$

ist.

ii. Die Gruppe G derjenigen Automorphismen von K, die k elementweise festlassen, ist isomorph zur Gruppe der gebrochenen linearen Substitutionen

$$x \mapsto \frac{ax+b}{cx+d} \qquad \text{mit} \quad a,b,c,d \in k \quad \text{und} \quad ad-bc \neq 0 \quad .$$

b) Sei im weiteren k der Körper mit 2 Elementen, also gleich $\mathbb{Z}/2\mathbb{Z}$. Man identifiziere die Automorphismengruppe G aus 1b) mit der Gruppe der gebrochenen linearen Substitutionen.

i. Zeigen Sie $|G| = 6$.

ii. Seien die Elemente $\alpha, \beta, \gamma \in G$ definiert durch

$$\alpha: \; x \mapsto x+1 \quad , \quad \beta: \; x \mapsto \frac{1}{x} \quad , \quad \gamma: \; x \mapsto 1+\frac{1}{x} \quad .$$

Zeigen Sie

$$G = \langle \alpha, \beta \rangle = \langle \alpha, \gamma \rangle = \langle \beta, \gamma \rangle$$

($\langle \ldots \rangle$ = Erzeugnis).

iii. $\langle \gamma \rangle$ ist ein Normalteiler von G.

c) Sei die Situation wie in b). Für eine Untermenge U von G sei

$$\operatorname{Fix} U := \{a \in K; \; \eta(a) = a \; \forall \eta \in G\}$$

der Fixkörper von U in K.

i. Für welches $F \in \{\operatorname{Fix}\alpha, \operatorname{Fix}\beta, \operatorname{Fix}\gamma, \operatorname{Fix} G\}$ ist $K|F$ galoissch? Gibt es noch weitere Zwischenkörper $k \subset F \subset K$, so daß $K|F$ galoissch ist?

ii. Zeigen Sie $\operatorname{Fix}\gamma = k(u)$, wobei u das Element $\dfrac{x^3+x^2+1}{x^3+x+1}$ ist.

iii. Bestimmen Sie $\operatorname{Fix}\alpha$ und $\operatorname{Fix}\beta$ (vergleiche ii.).

iv. Zeigen Sie, daß $\operatorname{Fix}\gamma$ unter G invariant ist. Zeigen Sie $\alpha|_{\operatorname{Fix}\gamma} = \beta|_{\operatorname{Fix}\gamma}$.

v. Bestimmen Sie mit Hilfe von iv. den Körper $\operatorname{Fix} G$ (vergleiche ii.).

d) Beweisen Sie den anfangs formulierten Satz.

ANLEITUNG: Zeige, daß das Polynom $f(X) - ug(X)$ in $k(u)[X]$ (X Unbestimmte, $\operatorname{ggT}(f,g) = 1$) irreduzibel ist.

K5.10 [Frühjahr 1994] Es sei K ein Körper, $L = K(x)$ sei der Körper der rationalen Funktionen über K. Die Elemente σ und τ von $\operatorname{Aut}(L|K)$ seien durch $\sigma(x) = 1-x$ und $\tau(x) = \frac{1}{x}$ definiert, sie erzeugen eine Gruppe H der Ordnung 6. (Das ist nicht nachzuweisen.) Man setzt

$$y = \frac{(x^2-x+1)^3}{x^2(x-1)^2} \in L \quad .$$

Zeigen Sie: Der Fixkörper von H ist $K(y)$.

K5.11 [Frühjahr 1999] Der Körper $\mathbb{Q}(t)$ der rationalen Funktionen über $\mathbb{Q}$ hat zwei Automorphismen σ, τ mit $\sigma(t) = \frac{1}{t}$ und $\tau(t) = 1-t$. Es sei G die von diesen beiden Automorphismen erzeugte Untergruppe von $\operatorname{Aut}\mathbb{Q}(t)$ und F der Fixkörper von G.

a) Bestimmen Sie die Ordnung und die Struktur von G.

b) Wie viele Zwischenkörper hat die Erweiterung $\mathbb{Q}(t)|F$ und was sind deren Grade über F? (Begründung!)

K5.12 [Herbst 1984] Es seien K ein Körper, x eine Unbestimmte und n eine ganze Zahl ≥ 1.

a) Bestimmen Sie alle Automorphismen von $K(x)$, die $K(x^n)$ elementweise festlassen. Ihre Menge sei G.

b) Ermitteln Sie die Struktur der Gruppe G.

c) Beschreiben Sie den Fixkörper F_τ jedes Elements τ aus G.

d) Geben Sie den Fixkörper F von G und alle Teilkörper von $K(x)$ an, die F enthalten.

e) Geben Sie eine notwendige und hinreichende Bedingung dafür an, daß $K(x)$ über $K(x^n)$ galoissch ist.

K5.13 [Herbst 1987] Sei $H[T]$ der Polynomring in der Unbestimmten T über einem Körper H der Charakteristik $p > 2$ und sei $L := H(T)$ der Quotientenkörper von $H[T]$. Ferner seien g_1 und g_2 die Körperautomorphismen von $L|H$, die durch

$$g_1(T) = -T \quad , \quad g_2(T) = 1 - T$$

bestimmt sind.

a) Zeigen Sie: Die von g_1 und g_2 erzeugte Untergruppe G von $\mathrm{Aut}(L)$ hat die Ordnung $2p$. Ist G abelsch?

b) Sei K der Fixkörper von G in L. Zeigen Sie, daß $(X^p - X)^2 - (T^p - T)^2$ das Minimalpolynom von T in $K[X]$ ist. Geben Sie auch das Minimalpolynom von $1 - T$ an.

c) Die Körperautomorphismen g_1 und g_2 von $L|K$ sind auch Endomorphismen von L als K-Vektorraum (d.h. K-lineare Abbildungen von L nach L). Bestimmen Sie die Minimalpolynome von g_1 und g_2.

d) Geben Sie die Eigenvektorräume von g_1 und g_2 an.

K5.14 [Herbst 2003] Gegeben sei das Element $z = X^2 + X^{-2}$ des rationalen Funktionenkörpers $\mathbb{Q}(X)$.

a) Zeigen Sie, dass $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ endlich vom Grad ≤ 4 ist.

b) Bestimmen Sie die Gruppe aller Automorphismen von $\mathbb{Q}(X)$, die z festlassen.

c) Zeigen Sie, dass $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ galoissch ist und geben Sie alle Körper zwischen $\mathbb{Q}(X)$ und $\mathbb{Q}(z)$ an.

Galoistheorie über K(t)

K5.15 [Frühjahr 1987] $K = \mathbb{Q}(t)$ sei der Körper der rationalen Funktionen in der Unbestimmten t über $\mathbb{Q}$.

a) Zeigen Sie, daß das Polynom $f := X^n - t \in K[X]$ irreduzibel ist.

b) Bestimmen Sie die Einheitswurzeln in K.

c) Sei L der Zerfällungskörper von f über K. Bestimmen Sie die Galoisgruppe von $L|K$.

K5.16 [Frühjahr 1988] K sei ein endlicher Körper und $K(t)$ der Körper der rationalen Funktionen in einer Unbestimmten t über K.

a) Gibt es zu jedem $n \geq 1$ ein irreduzibles Polynom n-ten Grades über K?

b) Gibt es ein irreduzibles Polynom über $K(t)$, das im algebraischen Abschluß von $K(t)$ mehrfache Nullstellen besitzt?

c) Gibt es ein irreduzibles Polynom über $\mathbb{Q}$, das in $\mathbb{C}$ eine doppelte Nullstelle besitzt?

Begründen Sie jeweils Ihre Antwort.

K5.17 [Frühjahr 1995] Sei x transzendent über einem Körper k.

a) Man zeige: $k(x)$ ist eine algebraische Erweiterung von $k\left(\frac{x^3}{x+1}\right)$.

b) Man bestimme das Minimalpolynom von x über $k\left(\frac{x^3}{x+1}\right)$.

Staatsexamensaufgaben zur Zahlentheorie

Inhalt

1. Elementare Zahlentheorie in Z

Z1.1 [Frühjahr 1977] Es sei $n_1, n_2, n_3, \ldots$ eine additiv abgeschlossene, streng monotone Folge natürlicher Zahlen. Es gebe ein $g \in \mathbb{N}$ mit $n_g = 2g$. Man beweise die Ungleichung

$$\sum_{i=1}^{g} n_i \geq g(g+1) \quad .$$

Man zeige, daß hierin das Gleichheitszeichen genau dann steht, wenn $n_i = 2i$ für $1 \leq i \leq g$ ist.

ANLEITUNG: Man ordne die nicht in der Folge vorkommenden natürlichen Zahlen $< 2g$ nach Restklassen mod n_1 und schätze ihre Summe nach oben ab.

Teilbarkeit

Z1.2 [Frühjahr 1975] Eine Zahl $p \in \mathbb{N}$ heißt eine Primzahl, wenn $p \neq 1$ und p in $\mathbb{N}$ nur die Teiler p und 1 besitzt.

a) Zeige: Ist $a \in \mathbb{N}$, $a > 1$, dann gibt es eine Primzahl p mit $p \mid a$ (p Teiler von a).
(Beachte: Die eindeutige Primzahlpotenzzerlegung der natürlichen Zahlen steht noch nicht zur Verfügung)

b) Zeige: $p \in \mathbb{N}$ ist genau dann eine Primzahl, wenn für beliebige $a, b \in \mathbb{N}$ aus $p \mid ab$ stets folgt: $p \mid a$ oder $p \mid b$.

HINWEIS: Benutze die Wohlordnungseigenschaft von $\mathbb{N}$.

c) Beweise die eindeutige Primzahlpotenzzerlegung der ganzen Zahlen: Jede ganze Zahl $z \in \mathbb{Z}$, $z \neq 0$, $z \neq \pm 1$ läßt sich eindeutig in der Form

$$z = (\pm 1) p_1^{n_1} \ldots p_t^{n_t}$$

schreiben, wobei $p_1, \ldots, p_t$ paarweise verschiedene Primzahlen sind und alle $n_i \geq 1$ für $i = 1, \ldots, t$.

Z1.3 [Frühjahr 2001] Bestimmen Sie alle Tripel (a, b, c) paarweise verschiedener natürlicher Zahlen, derart, dass jede dieser drei Zahlen die Summe der beiden anderen teilt.

Z1.4 [Herbst 2002] Geben Sie eine natürliche Zahl n an, so daß $n!$ im Dezimalsystem mit genau 2002 Nullen endet!

Z1.5 [Frühjahr 1980] Beweisen Sie, daß $\sqrt{2}$ irrational ist.

Z1.6 [Frühjahr 1981] Seien $p_1, \ldots, p_r$ verschiedene Primzahlen und $m \in \mathbb{N}$, $m \geq 2$. Zeige: $\sqrt[m]{p_1 \ldots p_r}$ ist irrational.

Z1.7 [Herbst 1974] Zeigen Sie: Die Zahl $2^k - 1$ ist nur dann eine Primzahl, wenn k eine Primzahl ist. Eine Primzahl der Form $2^k - 1$ heißt eine Mersennesche Primzahl.

Z1.8 [Frühjahr 1983] Beweisen Sie die folgenden Aussagen:

a) Ist $2^n - 1$ eine Primzahl, dann auch n.

b) Ist $2^n + 1$ eine Primzahl, dann ist n eine Potenz von 2.

Z1.9 [Herbst 1990] Beweisen Sie: Sind m und n zwei verschiedene natürliche Zahlen, so sind $2^{2^m}+1$ und $2^{2^n}+1$ teilerfremd.

Z1.10 [Herbst 1996] Zeigen Sie, daß die Fermatzahlen $F_n = 2^{2^n}+1$ paarweise teilerfremd sind, z.B. mittels einer Zerlegung von $F_{n+k}-2$, und folgern Sie daraus den Satz von Euklid, daß es unendlich viele Primzahlen gibt.

Z1.11 [Herbst 1988] Beweisen Sie die folgende Aussage:
Es gibt unendlich viele Primzahlen p mit der Eigenschaft, daß 6 kongruent zu einem Quadrat modulo p ist.

HINWEIS: Modifizieren Sie den Beweis Euklids, daß es unendlich viele Primzahlen gibt.

Z1.12 [Frühjahr 1989]

a) K sei ein Körper der Charakteristik $\neq 2$. Es soll gezeigt werden, daß die Lösungsmenge $C \subset K^2$ der Gleichung $X^2+Y^2=1$ aus $(0,1)$ und den Punkten

$$\Big(\frac{2t}{t^2+1}\,,\ \frac{t^2-1}{t^2+1}\Big) \quad \text{mit} \quad t \in K\,,\ t^2+1 \neq 0$$

besteht. Betrachten Sie hierzu alle Geraden in K^2 durch $(0,-1)$ und ihre Schnittpunkte mit C.

b) Ein Tripel $(a,b,c) \in \mathbb{Z}^3$ heißt *pythagoräisch*, wenn $a^2+b^2=c^2$. Im folgenden sei (a,b,c) ein pythagoräisches Tripel, wobei $a,b,c \in \mathbb{Z}\setminus\{0\}$ teilerfremd sind. Zeigen Sie:

1) a und b sind nicht beide gerade und nicht beide ungerade.

2) Ist a gerade, so gibt es Zahlen $u,v \in \mathbb{Z}$ mit

$$(a,b,c) = (2uv,\ u^2-v^2,\ u^2+v^2) \quad .$$

3) Jedes Tripel $(2uv, u^2-v^2, u^2+v^2)$ mit $u,v \in \mathbb{Z}$ ist pythagoräisch.

Lineare Kongruenzen

Z1.13 [Herbst 1976] Seien $m_1,\ldots,m_r$ paarweise teilerfremde natürliche Zahlen $\neq 1$, sei $n = m_1 m_2 \cdot \ldots \cdot m_r$ und $n_i = \frac{n}{m_i}$ für $i = 1,\ldots,r$.

a) Zeige: Die Gleichung $n_1X_1 + n_2X_2 + \ldots + n_rX_r = 1$ ist in ganzen Zahlen lösbar.

b) Zeige: Es gibt genau einen Ringisomorphismus

$$\varphi:\ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \quad .$$

c) Welcher Zusammenhang besteht zwischen den Urbildern $\varphi^{-1}(0,\ldots,0,1+m_i\mathbb{Z},0,\ldots,0)$, $i = 1,\ldots,r$, und einer Lösung der Gleichung in a)?

d) Zeige: Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ von $\mathbb{Z}/n\mathbb{Z}$ ist isomorph zu dem direkten Produkt

$$(\mathbb{Z}/m_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})^\times$$

der Einheitengruppen von $\mathbb{Z}/m_1\mathbb{Z},\ldots,\mathbb{Z}/m_r\mathbb{Z}$.

e) Stelle die Einheitengruppe von $\mathbb{Z}/168\mathbb{Z}$ als direktes Produkt zyklischer Untergruppen von Primzahlpotenzordnung dar.

Z1.14 [Frühjahr 1980] Man bestimme alle Lösungen $x \in \mathbb{Z}$ des Kongruenzensystems

$$x \equiv 7 \mod 12$$
$$x \equiv 11 \mod 20 \quad .$$

Z1.15 [Frühjahr 1982] Beantworten Sie die folgenden Fragen und begründen Sie Ihre Antwort.

a) Wie lautet die letzte Ziffer in der 12-adischen Darstellung von 2^{1000}?

b) Gibt es Zahlen $x, y \in \mathbb{Z}$ mit $264x + 195y = 12$?

c) Gibt es Zahlen $a, b \in \mathbb{Z}$, so daß das Kongruenzensystem

$$x \equiv a \mod 6$$
$$x \equiv b \mod 15$$

keine Lösung in $\mathbb{Z}$ hat?

Z1.16 [Herbst 1983]

a) Man beweise: Die Kongruenz

$$ax + by \equiv c \pmod{n}$$

ist für die ganzen Zahlen a, b, c und die natürliche Zahl n genau dann lösbar, wenn

$$\mathrm{ggT}(a, b, n) \text{ ein Teiler von } c \text{ ist} \quad .$$

b) Ist die Kongruenz

$$23707x + 33673y \equiv 1831 \pmod{47867}$$

lösbar?

Z1.17 [Herbst 1986] Berechnen Sie alle $x \in \mathbb{Z}$, welche die Kongruenzen

$$x \equiv 7 \mod 8 \quad , \quad x \equiv 2 \mod 9 \quad , \quad x \equiv -1 \mod 5$$

gleichzeitig lösen.

Z1.18 [Frühjahr 1988] Berechnen Sie alle Zahlen $x \in \mathbb{Z}$, die die folgenden Kongruenzen gleichzeitig erfüllen:

$$x \equiv 5 \mod 8$$
$$x \equiv 4 \mod 9$$
$$x \equiv 3 \mod 5 \quad .$$

Höhere Kongruenzen

Z1.19 [Frühjahr 1976] Ist die Gleichung

$$1001x^2 + 1000y = 999$$

mit ganzen Zahlen $x, y \in \mathbb{Z}$ lösbar?

Z1.20 [Herbst 1979] Ist die Gleichung $2^x + x^2 = 7y^3$ in natürlichen Zahlen x, y lösbar?

Z1.21 [Frühjahr 1994] Man bestimme alle Lösungen der Kongruenz

$$3x^2 - 2x + 9 \equiv 0 \pmod{35} \quad .$$

Z1.22 [Herbst 1998] Wieviele Lösungen besitzt die Kongruenz

$$x^2 \equiv 9 \mod 1386$$

im Bereich $\{0, 1, \ldots, 1385\}$?

Z1.23 [Frühjahr 1999] Man beweise oder widerlege die Behauptung

$$x^{200} \equiv x^8 \mod 221 \text{ für alle } x \in \mathbb{Z} \quad .$$

Z1.24 [Frühjahr 1998]

a) Man zeige, daß die Gleichung $x^2 + y^2 + z^2 = 7$ unlösbar in ganzen Zahlen $x, y, z \in \mathbb{Z}$ ist.

b) Man zeige, daß eine Zahl $n \in \mathbb{Z}$ mit

$$n \equiv 7 \mod 8$$

in $\mathbb{Z}$ nicht Summe von drei Quadraten ist.

Z1.25 [Frühjahr 2003] Geben Sie drei Körper mit verschiedenen Charakteristiken an, für die die binomische Formel

$$(a+b)^5 = a^5 + b^5$$

für alle Körperelemente a, b gilt.

Lineare Gleichungen

Z1.26 [Frühjahr 1984] Finden Sie eine ganzzahlige 3×3-Matrix mit Determinante 1, deren erste Zeile 4, 10, 15 lautet.

Z1.27 [Herbst 1994] Sei x ein Geldbetrag (in Mark und Pfennig) unter 100 Mark mit folgender Eigenschaft: Vertauscht man Mark- und Pfennigbeträge miteinander und zieht 5 Pfennig ab, so erhält man das Doppelte von x. Wie groß ist x?

Struktur von $\mathbb{Z}/n\mathbb{Z}$

Z1.28 [Frühjahr 1975]

a) Zeige: $\mathbb{Z}$ ist ein Hauptidealring.

b) Zeige: Sind $a, b \in \mathbb{Z}$ und ist c ein größter gemeinsamer Teiler von a und b, dann gibt es $x, y \in \mathbb{Z}$ mit $ax + by = c$.

c) Gib alle maximalen und minimalen Ideale von $\mathbb{Z}$ an.

d) Gib alle maximalen und minimalen Ideale des Ringes $\mathbb{Z}/12\mathbb{Z}$ an.

e) Bestimme Ideale A und B von $R := \mathbb{Z}/12\mathbb{Z}$ mit

$$R = A + B \quad , \quad A \cap B = 0 \quad , \quad A \neq R \quad , \quad B \neq R \quad .$$

f) Zeige für $n \in \mathbb{N}$: Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Z1.29 [Herbst 1975] Für jede Primzahl p berechne man die Anzahl $a(p)$ der p-ten Potenzen in dem Restklassenring $\mathbb{Z}/375\mathbb{Z}$.

Z1.30 [Frühjahr 1979] R sei ein kommutativer Ring mit 1. Ein Ideal I von R mit $I \neq R$ heißt *primär*, wenn in R/I jeder Nullteiler nilpotent ist. Welches sind die Primärideale $\neq (0)$ des Rings $\mathbb{Z}$ der ganzen Zahlen? (mit Beweis!)

Z1.31 [Herbst 1981] Zu einem Ideal A in einem kommutativen Ring R definiert man das Radikal $r(A)$ durch

$$r(A) = \{r\,;\ r \in R\,,\ r^n \in A \ \text{ für ein geeignetes } \ n \in \mathbb{N}\} \quad .$$

Für welche Ideale in $\mathbb{Z}$ gilt $r(A) = A$?

Z1.32 [Frühjahr 1998]

a) Zeigen Sie, daß in dem Ring $\mathbb{Z}/81\mathbb{Z}$ jeder Nullteiler nilpotent und jeder Nichtnullteiler invertierbar ist.

b) Gelten diese Aussagen auch in dem Ring $\mathbb{Z}/100\mathbb{Z}$?

Z1.33 [Frühjahr 1983] Für den Ring $R := \mathbb{Z}/(420)$ bestimme man die Anzahl

a) aller Ideale, aller Primideale und aller maximalen Ideale,

b) aller idempotenten und aller nilpotenten Elemente,

c) aller Einheiten und aller Nullteiler.

Die Antworten sind zu begründen.

Z1.34 [Herbst 1993] Sei $R := \mathbb{Z}/100\,000\mathbb{Z}$ der Ring der ganzen Zahlen modulo $100\,000$.

a) Bestimmen Sie alle nilpotenten und alle idempotenten Elemente von R sowie die Anzahl der Nullteiler von R.

b) Geben Sie alle Primideale und alle maximalen Ideale von R an.

c) Bestimmen Sie die Struktur der Einheitengruppe von R durch Angabe ihrer invarianten Faktoren.

Z1.35 [Frühjahr 1997]

a) Beweisen Sie, daß die Abbildung

$$\phi: \quad \begin{cases} \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \longrightarrow \mathbb{Z}/45\mathbb{Z} \\ (a \bmod 9\,,\ b \bmod 5) \longmapsto 10a - 9b \bmod 45 \end{cases}$$

wohldefiniert und ein Ringisomorphismus ist.

b) Bestimmen Sie den zu ϕ inversen Isomorphismus.

c) Bestimmen Sie alle nilpotenten Elemente von $\mathbb{Z}/45\mathbb{Z}$.

Z1.36 [Frühjahr 2000] Bestimmen Sie die Anzahl der Ideale, der Primideale, der Einheiten, der Nullteiler und der nilpotenten Elemente im Ring $\mathbb{Z}/2000\mathbb{Z}$.

Struktur von $(\mathbb{Z}/n\mathbb{Z})^\times$

Z1.37 [Herbst 1981] Es ist ein kommutativer Ring R gesucht, in dem das Polynom $X^2 + 1$ mehr als vier verschiedene Nullstellen hat.

Z1.38 [Frühjahr 1985]

a) Bestimme $x \in \mathbb{N}$, $1 \leq x \leq 30$, so daß die Restklasse $\bar{x}$ im Ring $\mathbb{Z}/(30)$ eine Einheit der Ordnung 4 ist.

b) Ist die Einheitengruppe von $\mathbb{Z}/(30)$ zyklisch?

Z1.39 [Frühjahr 1996] Es sei a eine zu 10 teilerfremde natürliche Zahl. Man zeige, daß unendlich viele der Dezimalzahlen 1, 11, 111, 1111, ... durch a teilbar sind.

Z1.40 [Frühjahr 1998]

a) Sei p ein Primteiler der natürlichen Zahl n. Zeigen Sie, daß die Einheitengruppe des Ringes $\mathbb{Z}/n\mathbb{Z}$ ein Element der Ordnung $p-1$ enthält.

b) Beweisen Sie, daß in der Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ genau dann $e^2 = 1$ für jede Einheit e gilt, wenn n ein Teiler von 24 ist.

Z1.41 [Herbst 1999]

a) Sei p eine ungerade Primzahl und $\nu \in \mathbb{Z}$, $\nu > 0$. Zeigen Sie, dass die Gleichung $X^2 = 1$ im Ring $\mathbb{Z}/(p^\nu)$ genau zwei Lösungen besitzt.

b) Sei $n = p_1^{\nu_1} \cdot \ldots \cdot p_s^{\nu_s}$ mit paarweise verschiedenen ungeraden Primzahlen p_i und positiven ganzen Zahlen ν_i $(i = 1, \ldots, s)$. Ferner sei a eine Einheit des Rings $\mathbb{Z}/(n)$. Zeigen Sie, dass die Gleichung $X^2 = a$ in $\mathbb{Z}/(n)$ entweder keine oder genau 2^s verschiedene Lösungen besitzt.

Z1.42 [Frühjahr 2000] Bestimmen Sie den Isomorphietyp der primen Restklassengruppe modulo 360, und geben Sie hierin explizit ein Element $n + 360\mathbb{Z}$ maximaler Ordnung an.

Z1.43 [Herbst 2000] Wie viele Elemente x mit der Eigenschaft $x^2 = x$ hat der Ring $\mathbb{Z}/15015\mathbb{Z}$? Geben Sie vier solche Elemente explizit an.

Zahlentheoretische Funktionen

Z1.44 [Frühjahr 1977] Es sei ϕ die bekannte Eulersche Funktion. Für natürliche Zahlen a und b sei mit $\mathrm{ggT}(a,b)$ der größte gemeinsame Teiler bezeichnet. Für $n \in \mathbb{N}$ definiere

$$h(n) := \sum_{d|n} \phi\Big(\mathrm{ggT}\left(d, \frac{n}{d}\right)\Big) \quad .$$

a) Man zeige, daß h multiplikativ ist, d.h. es ist $h(mn) = h(m)h(n)$ für teilerfremde m und n.

b) Man berechne $h(p^n)$ für Primzahlen p und natürliche Zahlen n.

c) Man berechne $h(432)$.

Z1.45 [Frühjahr 1989] Für welche natürlichen Zahlen n ist $\phi(n)$ ungerade?

HINWEIS: Die Eulersche ϕ-Funktion ist definiert als $\phi(n) =$ Zahl der invertierbaren Elemente im Ring $\mathbb{Z}/n\mathbb{Z}$.

Z1.46 [Frühjahr 1985] Es sei p eine Primzahl und $1 < n \in \mathbb{N}$. Man zeige:

a) Es gibt genau dann ein $0 < m \in \mathbb{N}$, so daß $n \mid p^m - 1$, wenn $p \nmid n$.
($p \mid a$: p teilt a ; $p \nmid n$: p teilt n nicht)

b) Ist $p \nmid n$, dann gibt es sogar ein $0 < m \in \mathbb{N}$ mit $m \mid \phi(n)$ und $n \mid p^m - 1$.
(ϕ = Eulersche ϕ-Funktion)

Z1.47 [Frühjahr 1981]

a) Zeige: 30 teilt $n^5 - n$ für alle $n \in \mathbb{Z}$.

b) Es bezeichne ϕ die Eulersche Phi-Funktion.
Man finde alle $m \in \mathbb{N}$, für die $\phi(m)$ ein Teiler von m ist.

Bruchrechnung

Z1.48 [Herbst 1976] Sei $n \neq 1$ eine zu 10 teilerfremde natürliche Zahl. Zeige: Die Periode in der Dezimalbruchentwicklung von $\frac{1}{n}$ ist gleich der Ordnung des Elementes $10 + n\mathbb{Z}$ in der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Z1.49 [Frühjahr 1989] Sei $N = 1 + 10^n$. Welche Länge hat die Periode des Dezimalbruchs für $\frac{1}{N}$?

Z1.50 [Frühjahr 1982] Sei p eine Primzahl. Man zeige:

a) $\mathbb{Z}_{(p)} := \left\{ \frac{r}{s} \in \mathbb{Q} \; ; \; s \not\equiv 0 \mod p \right\}$ ist Integritätsring.

b) $p \cdot \mathbb{Z}_{(p)} := \left\{ p \cdot \frac{r}{s} \in \mathbb{Q} \; ; \; s \not\equiv 0 \mod p \right\}$ ist das einzige maximale Ideal in $\mathbb{Z}_{(p)}$.

c) $\mathbb{Z}_{(p)}/p \cdot \mathbb{Z}_{(p)} \simeq \mathbb{Z}/(p)$.

Z1.51 [Frühjahr 1991] Sei $\mathbb{Q}$ die Menge der rationalen Zahlen. Sei M eine Teilmenge der natürlichen Zahlen, die die 1 enthält. Sei

$$\mathbb{Q}_M := \left\{ \frac{a}{b} \in \mathbb{Q} \; ; \; a \in \mathbb{Z} \, , \; b \in M \, , \quad a \text{ und } b \text{ teilerfremd} \right\} \quad .$$

Zeigen Sie:

a) $\mathbb{Q}_M$ ist genau dann eine Gruppe unter der Addition, eine sogenannte rationale Gruppe, wenn M alle Teiler und alle kleinsten gemeinsamen Vielfachen seiner Elemente enthält.

b) Eine solche rationale Gruppe $\mathbb{Q}_M$ ist genau dann ein Teilring von $\mathbb{Q}$, wenn M multiplikativ abgeschlossen ist.

Z1.52 [Herbst 1992] Es sei R der folgende Teilring des Körpers der rationalen Zahlen

$$R = \left\{ \frac{a}{b} ; \; a, b \in \mathbb{Z} \, , \; \mathrm{ggT}(b, 10) = 1 \right\} \quad .$$

a) Man bestimme die Einheitengruppe von R.

b) Man bestimme alle Ideale von R und zeige, daß R ein Hauptidealring ist.

c) Man bestimme alle irreduziblen Elemente von R bis auf Assoziierte.

Z1.53 [Frühjahr 1994] Sei p eine Primzahl. Dazu werde die Menge

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} ; \; b \in \mathbb{N} \, , \; a \in \mathbb{Z} \, ; \; \mathrm{ggT}(a, b) = 1, \; \mathrm{ggT}(b, p) = 1 \right\}$$

betrachtet. Zeigen Sie:

a) $\mathbb{Z}_{(p)}$ ist ein Unterring mit Eins von $\mathbb{Q}$.

b) $\mathfrak{m}_p := \{ \frac{a}{b} \; ; \; p \text{ teilt } a \text{ und nicht } b \}$ ist das einzige maximale Ideal in $\mathbb{Z}_{(p)}$.

c) $\mathbb{Z}_{(p)}/\mathfrak{m}_p$ ist isomorph zu $\mathbb{F}_p$, dem Körper mit p Elementen. Geben Sie den Isomorphismus an.

2. Ganze algebraische Zahlen

Grundlagen

Z2.1 [Frühjahr 1981] $\overline{\mathbb{Q}}$ sei der algebraische Abschluß von $\mathbb{Q}$ im Körper $\mathbb{C}$ der komplexen Zahlen. $x \in \overline{\mathbb{Q}}$ heißt *ganze algebraische* Zahl, wenn ein Polynom $f = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$ existiert mit $n > 0$ und $f(x) = 0$. Zeigen Sie:

a) Das Minimalpolynom von x über $\mathbb{Q}$ ist in $\mathbb{Z}[X]$ enthalten.

b) Für jede ganze algebraische Zahl x sind auch die zu x über $\mathbb{Q}$ konjugierten Zahlen ganz algebraisch.

Z2.2 [Frühjahr 1992] Eine Zahl $a \in \mathbb{C}$ heißt *ganz-algebraisch*, wenn a Nullstelle eines Polynoms aus $\mathbb{Z}[X]$ ist mit höchstem Koeffizienten 1, d.h. $f(a) = 0$ mit

$$f = X^n + f_{n-1}X^{n-1} + \ldots + f_1 X + f_0 \quad , \quad f_i \in \mathbb{Z} \quad .$$

Es sei

$$A := \{a \in \mathbb{C} \; ; \; a \text{ ist ganz-algebraisch}\} \quad .$$

Zeigen Sie:

a) Ist $z \in \mathbb{C}$ algebraisch über $\mathbb{Q}$, dann gibt es ein $q \in \mathbb{Z}$ mit $q \neq 0$ und $qz \in A$.

b) Es gilt $A \cap \mathbb{Q} = \mathbb{Z}$.

c) $a \in A \iff \mathbb{Z}[a]$ liegt in einer endlich erzeugten additiven Untergruppe von $\mathbb{C}$.
(Man kann für die Implikation von rechts nach links beispielsweise verwenden, daß Untergruppen endlich erzeugter abelscher Gruppen stets endlich erzeugt sind.)

d) A ist ein Unterring von $\mathbb{C}$.

Der Ring der vierten Einheitswurzeln

Z2.3 [Frühjahr 1993] Zeigen Sie, daß der Ring der Gaußschen Zahlen

$$\mathbb{Z}[i] = \{a + bi \; ; \; a, b \in \mathbb{Z}\} \; , \quad i = \sqrt{-1} \quad ,$$

aus genau denjenigen Elementen des Körpers $\mathbb{Q}(i)$ besteht, die einer normierten Gleichung

$$X^2 + cX + d = 0$$

mit ganzen Koeffizienten $c, d \in \mathbb{Z}$ genügen.

Z2.4 [Frühjahr 2003] Sei $R := \mathbb{Z} + i\mathbb{Z}$ der Ring der ganzen Gaußschen Zahlen mit $i^2 = -1$ und $a := 1 + 2i$. Zeigen Sie, dass der Faktorring R/aR ein Körper mit fünf Elementen ist.

Z2.5 [Frühjahr 1978] Bestimmen Sie einen größten gemeinsamen Teiler von $a = 31 - 2i$ und $b = 6 + 8i$ im Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen.

Z2.6 [Herbst 1990] Zerlegen Sie 2, 3 und 5 im Ring $\mathbb{Z}[i]$ der Gaußschen ganzen Zahlen in Primfaktoren.

Z2.7 [Herbst 1984] Sei $\mathbb{Z}[i]$ der (euklidische) Ring der ganzen Gaußschen Zahlen. Zeigen Sie in elementarer Weise für die Primzahl p:

a) p ist genau dann zerlegbar in $\mathbb{Z}[i]$, wenn p die Summe zweier Quadrate ist ($p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$).

b) Ist $p \neq 2$ zerlegbar, so wird $p-1$ von 4 geteilt.

Z2.8 [Herbst 1988] Entscheiden Sie, ob es rationale Zahlen a, b gibt, die die Bedingung

$$a^2 + b^2 = 1988$$

erfüllen, und begründen Sie Ihre Entscheidung.

Z2.9 [Frühjahr 2003] Sei p eine Primzahl $\equiv 1 \mod 4$. Zeigen Sie:

a) Es gibt eine natürliche Zahl x mit $x^2 \equiv -1 \mod p$.

b) p ist kein Primelement im Hauptidealring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen.

c) Es gibt natürliche Zahlen x, y mit $p = x^2 + y^2$.

Z2.10 [Herbst 2003] Sei $R = \mathbb{Z} + \mathbb{Z}i$ der Hauptidealring der ganzen Gaußschen Zahlen mit $i^2 = -1$, sei $\mathrm{N}: R \to \mathbb{Z}$ die komplexe Norm $\mathrm{N}(a+bi) = a^2 + b^2$.

a) Zeigen Sie, dass 11 ein Primelement und 13 kein Primelement in R ist.

b) Zeigen Sie, dass $11R$ ein maximales Ideal in R ist, und zerlegen Sie $13R$ in ein Produkt von zwei maximalen Idealen.

c) Welche Ordnung und welche Struktur hat die Gruppe $(R/11R)^\times$ der teilerfremden Restklassen modulo 11 in R?

d) Welche Ordnung und welche Struktur hat die Gruppe $(R/13R)^\times$ der teilerfremden Restklassen modulo 13 in R?

HINWEIS: Der Chinesische Restsatz kann nützlich sein.

Der Ring der dritten Einheitswurzeln

Z2.11 [Frühjahr 1988] Der Unterring $\mathbb{Z}[\omega] = \{a + b\omega\,;\ a, b \in \mathbb{Z}\}$, $\omega = \frac{-1+\sqrt{-3}}{2}$ primitive dritte Einheitswurzel, von $\mathbb{Q}(\sqrt{-3})$ ist abgeschlossen unter komplexer Konjugation $a + b\omega \mapsto \overline{a + b\omega}$ und versehen mit der Normabbildung

$$\mathrm{N}(a + b\omega) = (a + b\omega)\overline{(a + b\omega)} = a^2 - ab + b^2$$

ein euklidischer Ring (Dies ist nicht zu beweisen).

a) Zeige, daß ein Element y in $\mathbb{Z}[\omega]$ genau dann eine Einheit ist, wenn $\mathrm{N}(y) = 1$ gilt. Bestimme alle Einheiten des Ringes $\mathbb{Z}[\omega]$.

b) Zeige: Ist $x \in \mathbb{Z}[\omega]$ ein Primelement, so gibt es eine Primzahl p aus $\mathbb{Q}$ mit $\mathrm{N}(x) = p$ oder $\mathrm{N}(x) = p^2$. Falls $\mathrm{N}(x) = p^2$ gilt, so ist x assoziiert zu p; falls $\mathrm{N}(x) = p$ gilt, so ist x zu keiner Primzahl q assoziiert.

c) Zeige: Gilt $\mathrm{N}(z) = p$ für ein Element z aus $\mathbb{Z}[\omega]$, wobei p eine Primzahl ist, so ist z ein Primelement in $\mathbb{Z}[\omega]$.

d) Zeige: Ist p eine Primzahl, die kongruent zu 2 modulo 3 ist, so ist p als Element in $\mathbb{Z}[\omega]$ ein Primelement.

Der Ring des goldenen Schnitts

Z2.12 [Herbst 1977] Man betrachte den Unterring $R = \mathbb{Z}[\omega]$ von $\mathbb{R}$ mit

$$\omega = \frac{1}{2}(1 + \sqrt{5}) \quad .$$

Man zeige:

a) Jedes $z \in R$ läßt sich auf genau eine Weise in der Form

$$z = a + b\omega$$

mit ganzen Zahlen a und b darstellen.

b) Sei $\bar{\omega} := \frac{1}{2}(1 - \sqrt{5})$. Dann ist für $z = a + b\omega \in R \setminus \{0\}$ mit $a, b \in \mathbb{Z}$ die Norm $\mathrm{N}(z) := |(a + b\omega)(a + b\bar{\omega})|$ von z eine von 0 verschiedene natürliche Zahl.

c) Es gilt

$$\mathrm{N}(z_1 z_2) = \mathrm{N}(z_1) \cdot \mathrm{N}(z_2) \quad \text{für} \quad z_1, z_2 \in R \quad .$$

Genau dann ist $z \in R$ Einheit, wenn $\mathrm{N}(z) = 1$ ist.

d) Man zeige: R bildet mit der Funktion $\mathrm{N} : R \setminus \{0\} \to \mathbb{N}$ einen euklidischen Ring, d.h. zu zwei Elementen $z, w \in R \setminus \{0\}$ gibt es $u, v \in R$ mit

$$z = uw + v \quad ,$$

wobei $v = 0$ oder $\mathrm{N}(v) < \mathrm{N}(w)$ ist.

HINWEIS: Das Element $\frac{z}{w}$ aus dem Quotientenkörper von R schreibe man in der Form

$$\frac{z}{w} = u + (x + y\omega)$$

mit einem $u \in R$ und rationalen Zahlen x, y, deren Betrag kleiner oder gleich $\frac{1}{2}$ ist.

e) Euklidische Ringe sind bekanntlich Hauptidealringe; insbesondere gilt der Satz von der eindeutigen Primfaktorzerlegung. Man zeige durch Normbetrachtungen:

i) Eine Primzahl $p \in \mathbb{N}$ betrachtet als Element von R, ist — bis auf Einheiten — Produkt von höchstens zwei Primelementen aus R.

ii) 2 ist auch in R Primelement.

iii) Außer $p = 5$ enthält keine Primzahl p einen quadratischen Primfaktor in R.

HINWEIS: Sei $z = a + b\omega$ quadratischer Primfaktor von p; dann teilt p sowohl z^2 als auch $\mathrm{N}(z) = \frac{1}{4}|(2a + b)^2 - 5b^2|$.

iv) Genau dann ist eine Primzahl $p \neq 2, 5$ Produkt zweier nichtassoziierter Primelemente von R, wenn 5 Quadratrest modulo p ist.

f) Die Primfaktorzerlegungen von 11 und 19 in R gebe man explizit an.

g) Man zeige: Der Unterring $S := \mathbb{Z}[\sqrt{5}]$ von R ist kein Hauptidealring.

Sonstige faktorielle quadratische Zahlringe

Z2.13 [Frühjahr 1986] Es sei R der Unterring von $\mathbb{Q}(\sqrt{-2})$ aller Zahlen der Form $a+b\sqrt{-2}$ mit $a,b\in\mathbb{Z}$. Für $x\in\mathbb{Q}(\sqrt{-2})$ sei $\mathrm{N}(x):=x\cdot\bar{x}$ gesetzt, wobei $\bar{x}$ die zu x konjugiert-komplexe Zahl bezeichnet.

a) Man beweise, daß die Funktion N folgende Eigenschaften hat:

$$\mathrm{N}(x)\in\mathbb{N} \quad \text{für alle } x\in R,\ x\neq 0 \quad .$$
$$\mathrm{N}(0)=0 \quad , \quad \mathrm{N}(1)=1 \quad , \quad \mathrm{N}(xy)=\mathrm{N}(x)\mathrm{N}(y) \quad .$$

b) Man beweise, daß ein Element $x\in R$ genau dann eine Einheit in R ist, wenn $\mathrm{N}(x)=1$ ist. Man bestimme alle Einheiten von R.

c) Man beweise, daß zu jedem $x\in\mathbb{Q}(\sqrt{-2})$ ein $y\in R$ existiert mit $\mathrm{N}(x-y)\leq\frac{3}{4}$.

d) Man beweise, daß R bezüglich der Funktion N ein euklidischer Ring ist.

e) Man beweise, daß 19 in R zerlegbar ist.

Z2.14 [Herbst 1998] Betrachten Sie das Gitter

$$R=\left\{n+m\frac{1+\sqrt{-7}}{2};\ n,m\in\mathbb{Z}\right\}$$

in der komplexen Ebene $\mathbb{C}$.

a) Zeigen Sie, dass R ein Ring ist.

b) Sei

$$d(z,R)=\min\{|z-r|;\ r\in R\}$$

der Abstand einer komplexen Zahl z vom Gitter R. Bestimmen Sie das Maximum dieser Abstände, also

$$d=\max_{z\in\mathbb{C}} d(z,R) \quad ,$$

und zeigen Sie $d<1$.

c) Folgern Sie aus b), dass R ein euklidischer Ring ist, wobei die euklidische Wertfunktion auf R der Absolutbetrag komplexer Zahlen sei.

Nichtfaktorielle quadratische Zahlringe

Z2.15 [Frühjahr 1982] Sei $R:=\mathbb{Z}[\sqrt{-3}]=\left\{a+b\sqrt{-3};\ a\in\mathbb{Z},\ b\in\mathbb{Z}\right\}$.

a) Man bestimme die Einheiten von $\mathbb{Z}$.

b) Durch Zerlegung von 4 zeige man, daß R kein faktorieller Ring (ZPE-Ring) ist.

c) Ist jedes in R unzerlegbare Element prim in R?

Z2.16 [Frühjahr 1983] Zeigen Sie: $\mathbb{Z}[\sqrt{10}]=\{a+b\sqrt{10}\in\mathbb{C},\ a,b\in\mathbb{Z}\}$ ist kein ZPE-Ring.

HINWEIS: Verwenden Sie die Multiplikativität der Norm $\mathrm{N}(a+b\sqrt{10})=a^2-10b^2$ und $3^2=(\sqrt{10}+1)(\sqrt{10}-1)$ ohne Beweis.

Z2.17 [Herbst 1988] Es sei der Integritätsbereich

$$R := \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \in \mathbb{C}\ ;\ m, n \in \mathbb{Z}\}$$

gegeben. Zeige:

a) Sind $x := x_1 + x_2\sqrt{-5}$ und $y := y_1 + y_2\sqrt{-5}$ in R, wobei x_1, x_2, y_1, y_2 aus $\mathbb{Z}$ gewählt sind und $xy \neq 0$ ist, so gilt: Genau dann ist x ein Teiler von y in R, wenn $x_1^2 + 5x_1^2$ ein gemeinsamer Teiler von $x_1y_1 + 5x_2y_2$ und $y_1x_1 - y_1x_2$ in $\mathbb{Z}$ ist.

b) Die Einheitengruppe $R^\times$ von R ist $\{-1, +1\}$.

c) Jede Nichteinheit $\neq 0$ aus R ist Produkt von irreduziblen Elemente aus R.

d) R ist nicht faktoriell.

Z2.18 [Frühjahr 1995] Sei R der Integritätsbereich

$$R := \mathbb{Z}[\sqrt{-5}] \quad .$$

Man zeige:

a) Für Elemente $x := x_1 + x_2\sqrt{-5} \neq 0$ und $y := y_1 + y_2\sqrt{-5}$ von R gilt:
$x \mid y \iff x_1^2 + 5x_2^2$ ist gemeinsamer Teiler von $x_1y_1 + 5x_2y_2$ und $y_2x_1 - y_1x_2$ in $\mathbb{Z}$.

b) Die Einheitengruppe von R ist $R^\times = \{\pm 1\}$.

c) Jede Nichteinheit $\neq 0$ aus R ist Produkt von irreduziblen Elementen.

d) R ist nicht faktoriell.

Z2.19 [Frühjahr 1996] Im Ring $R := \mathbb{Z}[\sqrt{-3}]$ sei die Norm eines Elementes $x = a + b\sqrt{-3}$ definiert durch:

$$\mathrm{N}(a + b\sqrt{-3}) := (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2 \quad .$$

Zeigen Sie:

a) $x \in R$ ist eine Einheit in R genau dann, wenn $\mathrm{N}(x) = 1$ gilt, und dies gilt genau dann, wenn $x = \pm 1$.

b) 2 ist ein irreduzibles Element in R, das heißt, es gibt keine Zerlegung $2 = xy$, wobei $x, y \in R$ beide keine Einheiten in R sind.

c) Das von 2 und $1 + \sqrt{-3}$ in R erzeugte Ideal ist kein Hauptideal.

d) 2 ist kein Primelement in R.

Z2.20 [Herbst 1996] Zeigen Sie, daß der Ring $\mathbb{Z}[\sqrt{-31}] = \{a + b\sqrt{-31}\,;\ a, b \in \mathbb{Z}\}$ nicht faktoriell ist, d.h. keine Primfaktorzerlegung hat.

HINWEIS: Verwenden Sie etwa, daß $32 = (1 + \sqrt{-31})(1 - \sqrt{-31})$ gilt.

Einheiten quadratischer Zahlringe

Z2.21 [Herbst 1989] Im Ring $R := \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\,;\ a, b \in \mathbb{Z}\}$ ist die Normabbildung $\mathrm{N} : R \to \mathbb{Z}$ definiert durch $\mathrm{N}(x) := a^2 - 2b^2$. Bekanntlich ist $\mathrm{N}(x)$ multiplikativ. Zeigen Sie:

a) Die Einheiten von R sind genau die Elemente mit Norm ± 1.

b) Elemente x von R mit $1 < x < \omega := 1 + \sqrt{2}$ sind keine Einheiten.

c) Die Einheitengruppe von R enthält genau die Elemente $\pm\omega^n$, $n \in \mathbb{Z}$, und ist isomorph zu $\mathbb{Z}_2 \oplus \mathbb{Z}$.

Z2.22 [Herbst 1994] Gegeben sei der Teilring $R = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ von $\mathbb{C}$. Mit $R^\times$ sei seine Einheitengruppe bezeichnet. Man zeige:

a) Für alle $\varepsilon = x + y\sqrt{2} \in R^\times$ gilt $x^2 - 2y^2 = \pm 1$.

b) Für alle $\varepsilon = x + y\sqrt{2} \in R^\times$ gilt: $(\varepsilon > 1 \implies x, y > 0)$,

c) $\mathrm{Min}\{\varepsilon \in R^\times \,;\, \varepsilon > 1\} = 1 + \sqrt{2}$,

d) $R^\times = \{ \pm (1 \pm \sqrt{2})^n \,;\, n \in \mathbb{N}\}$.

Z2.23 [Frühjahr 1999] Gegeben sei der Teilring $R = \mathbb{Z} + \mathbb{Z}\sqrt{5}$ von $\mathbb{C}$.

a) Man zeige, dass in R jedes von (0) verschiedene Primideal maximal ist.

b) $R^\times$ bezeichne die Einheitengruppe des Ringes R. Man zeige:
Für alle $\varepsilon = x + y\sqrt{5} \in R^\times$ gilt $x^2 - 5y^2 = \pm 1$.

Höhere Einheitswurzeln

Z2.24 [Herbst 1995] Sei K ein Körper, $n \geq 2$ eine natürliche Zahl und ζ eine n-te Einheitswurzel über K. Man beweise:

a)
$$\sum_{k=0}^{n-1} \zeta^k = \begin{cases} n & \text{falls } \zeta = 1 \\ 0 & \text{sonst} \end{cases}$$

b) ζ ist genau dann primitive n-te Einheitswurzel über K, wenn gilt:
$$\sum_{k=0}^{n-1} \zeta^{ik} = 0 \qquad \text{für} \quad 1 \leq i < n \quad .$$

c) Ist $n = 2^r$ mit einer natürlichen Zahl r, so gilt für alle $a \in K$:
$$\sum_{k=0}^{n-1} a^k = \prod_{k=0}^{r-1} (1 + a^{2^k}) \quad .$$

d) Sei nun p eine Fermatsche Primzahl und $K = \mathbb{F}_p$. Seien r, s natürliche Zahlen mit $2^{2^{r+s-1}} = p - 1$. Sei $n = 2^r$ und $\zeta = \overline{2^{2^s}} \in K$. Dann ist ζ eine primitive n-te Einheitswurzel.

e) Man bestimme eine primitive 16-te Einheitswurzel in $\mathbb{Z}_{65537}$.

Z2.25 [Herbst 2002] Zeigen Sie:

a) Ist $\zeta = e^{\pi i/1001}$ eine primitive 2002-te Einheitswurzel in $\mathbb{C}$, so ist $\varepsilon = 1 + \zeta + \zeta^2$ eine Einheit in $\mathbb{Z}[\zeta]$.

ANLEITUNG: Stellen Sie $\dfrac{1}{\varepsilon} = \dfrac{\zeta - 1}{\zeta^3 - 1}$ als Summe von Potenzen von ζ dar.

b) Es gibt keinen Integritätsring der Charakteristik Null, der genau 2002 Einheiten besitzt.

c) Ist R ein Integritätsring mit genau 2002 Einheiten, so hat R die Charakteristik 2003 (ist Primzahl!).

d) Geben Sie zwei nichtisomorphe Integritätsringe mit genau 2002 Einheiten an.

3. Quadratisches Reziprozitätsgesetz

Z3.1 [Herbst 1973] Man untersuche, ob die Gleichung

$$x^2 + 391y - 7 = 0$$

eine ganzzahlige Lösung besitzt.

Z3.2 [Frühjahr 1976] Über welchen endlichen Körpern $\mathbb{F}_q$ (q = Elementezahl des Körpers) ist der goldene Schnitt realisierbar, d.h. wann gibt es zu $a \in \mathbb{F}_q^\times$ stets ein $b \in \mathbb{F}_q$ mit $a : b = b : (a - b)$?

Z3.3 [Herbst 1998] Sei q eine ungerade Primpotenz. Man zeige: Genau dann kann man den goldenen Schnitt über dem endlichen Körper $\mathbb{F}_q$ realisieren, d.h. genau dann gibt es drei verschiedene Elemente $\alpha, \beta, \gamma \in \mathbb{F}_q$ mit

$$\frac{\gamma - \alpha}{\gamma - \beta} = \frac{\gamma - \beta}{\beta - \alpha} \quad ,$$

wenn 5 ein Quadrat in $\mathbb{F}_q$ ist.

Z3.4 [Frühjahr 1992] Für Primzahlen p bezeichne $\mathbb{F}_p$ den Körper aus p Elementen. Kennzeichnen Sie durch Kongruenzbedingungen diejenigen ungeraden Primzahlen p, für die das Polynom $X^2 - 5$ irreduzibel in $\mathbb{F}_p[X]$ ist.

Z3.5 [Frühjahr 1993] Für Primzahlen p sei $\mathbb{F}_p$ der Körper aus p Elementen. Welche der folgenden Aussagen ist für alle Primzahlen p gültig? (Beweis oder Gegenbeispiel!)

a) Das Polynom $X^2 - 17$ ist genau dann irreduzibel in $\mathbb{F}_p[X]$, wenn $X^2 - p$ irreduzibel in $\mathbb{F}_{17}[X]$ ist.

b) Das Polynom $X^2 - 3$ ist genau dann irreduzibel in $\mathbb{F}_p[X]$, wenn $X^2 - p$ irreduzibel in $\mathbb{F}_3[X]$ ist.

Z3.6 [Herbst 1997] Sei $p = 4k + 3$ eine Primzahl, so daß auch $q = 2p + 1$ eine Primzahl ist. Zeigen Sie, daß q ein Teiler von $2^p - 1$ ist.

Gemischte Staatsexamensaufgaben

Mengenlehre

M.1 [Herbst 1975] Sei M Menge. Für $i = 1, 2$ sei R_i Äquivalenzrelation auf M mit kanonischer Projektion $p_i : M \to M/R_i$. Man zeige:

Gibt es eine bijektive Abbildung $f : M/R_1 \to M/R_2$ und gilt $f \circ p_1 = p_2$, so ist $R_1 = R_2$ und f die identische Abbildung.

Gruppen und Ringe

M.2 [Herbst 1983]

a) Man zeige, daß es bis auf Isomorphie genau eine Gruppe der Ordnung 1295 gibt.

b) Es sei R ein Ring mit 1, der aus 1295 Elementen besteht. Man beweise, daß R isomorph zu einem direkten Produkt von drei Körpern ist und man bestimme diese Körper.

c) Was ist die Ordnung der Einheitengruppe von R?

d) Wieviele Nullteiler enthält R?

M.3 [Herbst 1995]

a) Zeigen Sie, daß jede abelsche Gruppe der Ordnung 1995 zyklisch ist.

b) Geben Sie eine nichtabelsche Gruppe der Ordnung 1995 an.

c) Wieviele maximale Ideale hat der Restklassenring $\mathbb{Z}/1995\mathbb{Z}$?

Gruppen, Ringe, Körper

M.4 [Herbst 1972] Alle Ringe seien kommutativ mit Eins-Element und für alle Ringhomomorphismen $f : R \to S$ gelte: $f(1_R) = 1_S$.

Ist $f : A \to B$ ein Homomorphismus zwischen Gruppen (bzw. Ringen, bzw. Körpern) A und B, dann heiße f *rechtskürzbar*, wenn für alle Gruppen (bzw. Ringe, bzw. Körper) C und für alle Homomorphismen $h, k : B \to C$ gilt: Aus $hf = kf$ folgt $h = k$.

a) Seien f, g Homomorphismen und sei gf definiert; man zeige:

   i. Ist gf rechtskürzbar, dann auch g.

   ii. Sind g und f rechtskürzbar, dann auch gf.

b) Man zeige: Ein Homomorphismus zwischen abelschen Gruppen ist genau dann rechtskürzbar, wenn er surjektiv ist.

c) Seien $\mathbb{Z}$ die additive Gruppe der ganzen Zahlen, $n \in \mathbb{Z}$, $n \neq 0$ und $g : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ der kanonische Homomorphismus.

   Man suche eine Untergruppe $A \subseteq \mathbb{Z}$, so daß für die Inklusion $i : A \to \mathbb{Z}$ gilt: gi ist surjektiv, aber i ist nicht rechtskürzbar.

d) Seien p prim, $m, n \in \mathbb{Z}$, $0 \neq m \leq n$ und $g : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ der Homomorphismus mit $g(z + p^n\mathbb{Z}) = z + p^m\mathbb{Z}$ für alle $z + p^n\mathbb{Z} \in \mathbb{Z}/p^n\mathbb{Z}$. Sei $f : A \to \mathbb{Z}/p^n\mathbb{Z}$ ein Homomorphismus von einer beliebigen abelschen Gruppe A in $\mathbb{Z}/p^n\mathbb{Z}$. Man berechne die Untergruppen von $\mathbb{Z}/p^n\mathbb{Z}$ und zeige:
Ist gf surjektiv, dann auch f.

e) Sei R ein Integritätsring und K sein Quotientenkörper. Man zeige: Die Inklusion $i : R \to K$ ist rechtskürzbarer Ringhomomorphismus.

g) Man zeige: Die Inklusion $K \to K(X)$ ist kein rechtskürzbarer Homomorphismus (wobei $K(X)$ den Körper der rationalen Funktionen über einem Körper K bezeichnet).

h) Seien $K \subseteq \Omega$ eine Körpererweiterung, Ω algebraisch abgeschlossen, $\alpha \in \Omega$ ein separables Element mit einem Minimalpolynom vom Grad n.
Man zeige: Die Anzahl der Homomorphismen von $K(\alpha)$ nach Ω, die K elementweise fest lassen, ist n.

i) Sei $K \subseteq L$ eine endlichdimensionale Körpererweiterung, $\operatorname{char} K = 0$ oder K endlich.
Man zeige: Falls die Inklusion $i : K \to L$ rechtskürzbar ist, gilt $K = L$.

j) Sei $K \subseteq L$ eine rein inseparable Körpererweiterung mit $\operatorname{char} K = p \neq 0$ (d.h. für alle $\alpha \in L$ gibt es eine natürliche Zahl e, so daß $x^{p^e} \in K$).
Man zeige: Die Inklusion $i : K \to L$ ist rechtskürzbar.

k) Sei $K \subseteq L$ eine endlichdimensionale Körpererweiterung, $\operatorname{char} K = p \neq 0$.
Man zeige: Die Inklusion $i : K \to L$ ist genau dann ein rechtskürzbarer Körperhomomorphismus, wenn L eine rein inseparable Körpererweiterung von K ist.

M.5 [Frühjahr 1981] Man gebe für die folgenden Fälle jeweils ein Beispiel an oder begründe kurz, warum es ein derartiges Beispiel nicht gibt:

a) eine auflösbare nicht-abelsche Gruppe,

b) eine einfache nicht-abelsche Gruppe,

c) eine nicht-abelsche Gruppe der Ordnung 7,

d) ein kommutativer Körper mit genau 6 Elementen,

e) ein maximales Ideal in $\mathbb{Q}[X, Y]$, das nicht Hauptideal ist,

f) ein irreduzibles separables Polynom 2. Grades in $\mathrm{GF}(2)[X]$,

g) ein irreduzibles Polynom 3. Grades in $\mathbb{R}[X]$.

M.6 [Herbst 1992] Definieren Sie folgende Begriffe, und geben Sie in allen Fällen noch mindestens eine zur Definition äquivalente Charakterisierung an:

a) auflösbare Gruppe

b) noetherscher kommutativer Ring

c) durch Radikale auflösbares Polynom (Charakterisierung im Falle der Charakteristik 0).

Zahlentheorie und Algebra

M.7 [Herbst 1991]

a) Es sei die natürliche Zahl n in ihrer Dezimaldarstellung

$$n = \sum_{k \geq 0} a_k 10^k \qquad , \qquad 0 \leq a_k \leq 9$$

gegeben. Man beweise die Kongruenz

$$n \equiv \sum_{k \geq 0} (-1)^k a_k \qquad (\mathrm{mod}\ 11)$$

und leite daraus ein Kriterium für die Teilbarkeit durch 11 her.

b) Man zerlege 1991 in Primfaktoren.

c) Man bestimme alle Gruppen (bis auf Isomorphie) der Ordnung 1991.

d) Es sei R der Restklassenring $\mathbb{Z}/1991\mathbb{Z}$ und $R^\times$ seine Einheitengruppe. Man stelle $R^\times$ als direktes Produkt von zyklischen Gruppen von Primzahlpotenz-Ordnung dar.

M.8 [Frühjahr 1997]

a) Zeigen Sie: Für jede Primzahl p ist die Menge der primitiven p-ten Einheitswurzeln aus $\mathbb{C}$ linear unabhängig über $\mathbb{Q}$.

b) Ist $1997^{1997} - 4$ durch 7 teilbar? Begründen Sie Ihre Antwort.

M.9 [Frühjahr 1997] Beantworten Sie die folgenden Fragen. Es werden keine Begründungen verlangt.

a) Zu welchem direkten Produkt zyklischer Gruppen ist die Einheitengruppe des Ringes $\mathbb{Z}/255\mathbb{Z}$ isomorph?

b) Definieren Sie das Legendre-Symbol $\left(\frac{a}{p}\right)$ für Primzahlen $p \neq 2$. Wie lautet das quadratische Reziprozitätsgesetz von Gauß?

c) Welche Teilkörper besitzt der Körper mit 128 Elementen?

d) Nennen Sie eine Definition für die Quaternionengruppe Q der Ordnung 8. Wie viele Elemente der Ordnung 2 gibt es in Q?

M.10 [Herbst 1997]

a) Wieviele Primitivwurzeln modulo 1997 gibt es? Gehen Sie davon aus, daß 1997 eine Primzahl ist.

b) Berechnen Sie die Summe der Koeffizienten des Polynoms $(X^2 - X + 1)^{1997}$.

c) Untersuchen Sie, ob die Kongruenz $X^2 \equiv 593 \mod 1997$ eine Lösung in $\mathbb{Z}/1997\mathbb{Z}$ besitzt.

M.11 [Herbst 2001]

a) Zeigen Sie: Es gibt keine ganzen Zahlen x und y mit $x^2 + 3y^2 = 2001$.

b) Bestimmen Sie die Isomorphieklassen der Gruppen der Ordnung 2001.

M.12 [Frühjahr 2002] Beantworten Sie die folgenden Fragen und geben Sie jeweils eine kurze Begründung für Ihre Antwort:

a) Kann man ein regelmäßiges 19-Eck mit Zirkel und Lineal konstruieren?

b) Ist $x^2 + x + 11 \equiv 0 \ (\mathrm{mod}\ 370368)$ lösbar?

c) Ist $\mathbb{Z}[x]$ ein Hauptidealring?

d) Sei $f(x) = x^{19} + 19x + 57 \in \mathbb{Q}[x]$. Ist die Restklasse von $x^{18} + 2$ in $\mathbb{Q}[x]/(f)$ invertierbar?