Universität des Saarlandes
FR 6.1, Mathematik
Prof. Dr. E.-U. Gekeler

Aufgabensammelung zur Algebra 1

Aufgabe 1: Sei S die Menge aller rationalen Zahlen mit quadratfreiem Nenner. Zeigen Sie, daß S eine additive Untergruppe von $\mathbb{Q}$ ist, die nicht zyklisch ist.

Aufgabe 2: Sei G eine (multiplikative) Gruppe mit 8 Elementen und neutralem Element e. Seien $a \neq b$ zwei von e verschiedene Elemente von G mit

$$a^k \neq e \text{ und } b^k \neq e \quad \text{für alle} \quad 1 \leq k < 4, \quad a^4 = b^4 = e, \quad \text{und} \quad a^3 b = ba.$$

Zeigen Sie, daß $\{a, b\}$ die Gruppe G erzeugt und stellen Sie die Gruppentafel auf.

Aufgabe 3:

a) Geben Sie ein Beispiel für eine Menge M mit einer Verknüpfung $\circ$, so daß $\circ$ nicht assoziativ ist, aber M ein neutrales Element besitzt und jedes $m \in M$ eine Inverses besitzt.

b) Geben Sie ein Beispiel für eine Menge M mit einer Verknüpfung $\circ$, die den vier Bedingungen
   (i) $\circ$ ist assoziativ.
   (ii) M besitzt ein linksneutrales Element, d. h. es existiert ein $e \in M$ mit $e \circ a = a$ für alle $a \in M$.
   (iii) Jedes Element $m \in M$ besitzt ein Rechtsinverses m^{-1} mit $m \circ m^{-1} = e$.
   (iv) M ist keine Gruppe.

Aufgabe 4: Sei $G = \langle x \rangle$ die von x erzeugte Gruppe mit $|G| = n \in \mathbb{N}$. Weiter seien $D_{2n} := \{(g, e) \mid g \in G, \; e \in \{\pm 1\}\}$ und

$$\cdot : D_{2n} \times D_{2n} :\longrightarrow D_{2n}, \quad ((g, e), (h, f)) \mapsto (gh^e, ef) \; .$$

a) Zeigen Sie, daß D_{2n} eine Gruppe ist.

b) Zeigen Sie, daß für jedes $n \geq 3$ die Gruppe D_{2n} isomorph zur Gruppe der orthogonalen Abbildungen der Ebene auf sich, die ein regelmäßiges n-Eck um den Ursprung deckungsgleich in sich überführen.

c) Jede solche Drehung und Spiegelung permutiert die Ecken eines regelmäßigen n-Ecks. Zeigen Sie, daß diese Permutationen eine zu D_{2n} isomorphe Untergruppe der Permutationsgruppe S_n bilden. Welche Permutation entspricht dabei welcher Bewegung?

Hinweis zu Teil b): Ordnen Sie $(x, 1) \in D_{2n}$ die Drehung (im mathematisch positiven Sinn) um $\frac{2\pi}{n}$ und $(1, -1)$ die Spiegelung an einer geeigneten Nullpunktsgeraden zu. Die Verknüpfung sollte dann der Hintereinanderausführung zweier Bewegungen entsprechen.

Bemerkung zur Aufgabe: D_{2n} heißt Diedergruppe. Diese Aufgabe enthält genaugenommen vier verschiedene Darstellungen der Diedergruppe. Teil a) eine formal abstrakte, Teil b) sowohl eine geometrisch anschauliche als auch eine Interpretation dieser Gruppe als Untergruppe der orthogonalen (2×2)-Matrizen und Teil c) die Darstellung als Untergruppe der Permutationsgruppe.

Aufgabe 5: Es sei $T := \{z \in \mathbb{C} \mid |z| = 1\}$ der Einheitskreis in der komplexen Zahlenebene.

a) Zeigen Sie, daß T versehen mit der üblichen Multiplikation in $\mathbb{C}$ eine Gruppe ist.
b) Ein Element $\zeta \in \mathbb{C}$ heißt Einheitswurzel, falls es ein $k \in \mathbb{N}$ gibt mit $\zeta^k = 1$. Beweisen Sie, daß die Menge der Einheitswurzeln eine echte Untergruppe unendlicher Ordnung von T ist, in der jedes einzelne Element endliche Ordnung hat. Ist diese Gruppe endlich erzeugt?

Aufgabe 6:(*10 Punkte*) Welche der H_i sind normale Untergruppen in G_i?

i)	$H_1 = \langle(1,3,2)\rangle$,	$G_1 = S_3$
ii)	$H_2 = \langle(1,3,2)\rangle$,	$G_2 = S_{17}$
iii)	$H_3 = A_n$,	$G_3 = S_n$
iv)	$H_4 = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a,b,c \in \mathbb{Q},\ ac \neq 0\}$,	$G_4 = \mathrm{GL}(2,\ \mathbb{Q})$
v)	$H_5 = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathbb{Q}\}$,	$G_5 = H_4$
vi)	$H_6 = H_5$,	$G_6 = G_4$
vii)	$H_7 = Z(G_7)$,	G_7 beliebige Gruppe
viii)	$H_8 = \{\zeta \in \mathbb{C} \mid \zeta$ ist Einheitswurzel $\}$,	$G_8 = \{z \in \mathbb{C} \mid \lvert z\rvert = 1\}$

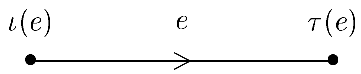
Aufgabe 7: Sei G eine Gruppe mit Zentrum $Z(G)$. Zeigen Sie:
a) $\mathrm{Aut}(G)$ ist eine Gruppe bezüglich der Komposition.
b) Sei $g \in G$. Dann ist

$$\begin{aligned} \kappa_g : G &\longrightarrow G \\ x &\mapsto gxg^{-1} \end{aligned}$$

ein Automorphismus.
c) $\kappa : g \mapsto \kappa_g$ definiert einen Homomorphismus von G nach $\mathrm{Aut}(G)$.
d) $\mathrm{Ker}\ (\kappa) = Z(G)$.
e) Die Menge der inneren Automorphismen $\mathrm{Inn}(G) := \mathrm{Im}\ (\kappa)$ ist eine normale Untergruppe in $\mathrm{Aut}(G)$.

Aufgabe 8: Sei G eine Gruppe. Zeigen Sie die Äquivalenz der folgenden drei Aussagen:
a) G ist abelsch.
b) Für alle $a, b \in G$ ist $(ab)^2 = a^2b^2$.
c) Für alle $a, b \in G$ ist $(ab)^{-1} = a^{-1}b^{-1}$.

Aufgabe 9:(*15 Punkte*) Ein *Graph* Γ ist die disjunkte Vereinigung zweier Mengen $V = V(\Gamma) \neq \emptyset$ und $E = E(\Gamma)$ zusammen mit zwei Abbildungen $\iota,\ \tau : E \longrightarrow V$.
Die Elemente von V heißen *Knoten* von Γ und die Elemente von E *(orientierte) Kanten* von Γ. Für ein Element $e \in E$ heißen die Knoten $\iota(e)$ und $\tau(e)$ *Aufknoten* und *Endknoten* einer Kante. Eine Kante wird üblicherweise beschrieben durch:



Seien $n \in \mathbb{N}$ und G eine Gruppe mit endlichem Erzeugendensystem $X = \{x_1, \dots, x_n\}$. Der *Cayley–Graph* $\Gamma = \Gamma(G, X)$ ist wie folgt definiert:
Die Knotenmenge ist die Menge aller Elemente von G, die Kantenmenge ist $E(\Gamma) = G \times X$ und die beiden Abbildungen sind gegeben durch $\iota(g, x) = g$ und $\tau(g, x) = gx$ für alle $(g, x) \in E(\Gamma)$.

Zeichnen Sie (möglichst überschneidungsfrei) Cayley-Graphen von C_3, C_∞, S_3, V_4 und D_8. Dabei sind C_n mit $n \in \mathbb{N}$ bzw. C_∞ zyklische Gruppen mit n bzw. unendlich vielen Elementen und $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ die Kleinsche Vierergruppe.

Aufgabe 10: Zeigen Sie, daß der Index des Zentrums einer Gruppe niemals Primzahl sein kann.

Aufgabe 11: Sei G eine Gruppe und $n \in \mathbb{N}$. Ist dann $U = \{x \in G \mid x^n = 1_G\}$ eine Untergruppe von G?

Aufgabe 12: Bestimmen Sie mit Hilfe von Gruppenoperationen die Anzahl verschiedener Perlenketten, die man bilden kann aus drei weißen und sechs schwarzen Perlen.

Aufgabe 13: Eine Gruppe G der Ordnung 55 operiere auf einer Menge X mit 18 Elementen. Zeigen Sie, daß G auf X mindestens zwei Fixpunkte hat.

Aufgabe 14: Sei p eine Primzahl. Weiter sei G eine Gruppe der Ordnung n. Zeigen Sie: Ist $n = p$ oder $n = p^2$, so ist G abelsch. Ist $n = p^3$ so ist G nicht unbedingt abelsch. (Konstruieren/Finden Sie eine nichtabelsche Guppe der Ordnung p^3 für ein $p \in \mathbb{P}$.)

Aufgabe 15: Sei G eine einfache endliche Gruppe und $|G| \neq 2$. Weiter sei $\varphi : G \longrightarrow H$ ein Homomorphismus. Zeigen Sie:
Besitzt H eine normale Untergruppe A vom Index 2, so liegt $\varphi(G)$ in A.
Hinweis: Eine Gruppe $G \neq \{1\}$ heißt *einfach*, wenn sie außer den trivialen keine weiteren normalen Untergruppen besitzt.

Aufgabe 16: Sei G eine endliche abelsche Gruppe. Zeigen Sie
a) $U = \{x \in G \mid x^2 = 1\}$ ist eine Untergruppe von G.
b) $\prod\limits_{g \in G} g = \prod\limits_{g \in U} g = \begin{cases} 1 & \text{falls } |U| \neq 2 \\ x & \text{falls } U = \{1, x\} \text{ mit } x \neq 1 \end{cases}$
c) den *Satz von Wilson:*
Für eine Primzahl $p \neq 2$ gilt $(p-1)! \equiv -1 \pmod{p}$.

Aufgabe 17: Sei G eine Gruppe und N eine normale Untergruppe von G. Weiter sei $\varphi : G/N \longrightarrow \mathbb{Z}$ ein Gruppenepimorphismus (d. h. ein surjektiver Gruppenhomomorphismus). Zeigen Sie, daß es zu jedem $n \in \mathbb{N}$ einen Normalteiler U von G gibt mit $|G : U| = n$.

Aufgabe 18: Sei G eine endliche Gruppe und $H \neq G$ eine Untergruppe von G. Weiter sei $X := \{gH \mid g \in G\}$. Zeigen Sie:
a) G operiert auf X durch Linksmultiplikation.
b) Ist $|G|$ kein Teiler von $|G : H|!$, dann enthält H einen echten Normalteiler von G.

c) Gilt zusätzlich $|G : H| = p$ und p der kleinste Primteiler von $|G|$, dann ist H Normalteiler von G.

d) In einer Gruppe der Ordnung 99 ist jede Untergruppe der Ordnung 11 Normalteiler.

Hinweis: Teil b) ist ein eleganter und häufig anwendbarer Existenzsatz für Normalteiler.

Aufgabe 19: Bestimmen Sie die die abgeleitete Reihe $D^i(D_{2n})$ und die (obere) Zentralreihe $C^i(D_{2n})$ der Diedergruppe D_{2n}.

Aufgabe 20: Zeigen Sie, daß jede Gruppe der Ordnung 15 zyklisch ist.
Hinweis: Betrachten Sie eine geeignete Operation der Gruppe auf einer ihrer p-Gruppen.

Aufgabe 21: Seien p, q verschiedene Primzahlen mit $q < p$ und G eine Gruppe mit $|G| = pq$. Wieviele Elemente der Ordnung p, q und pq enthält G, und wieviele Sylowgruppen der Ordnung p bzw. q gibt es, falls

a) G abelsch ist?

b) G nicht abelsch ist?
Welche Bedingung ergibt sich hier für p?

Aufgabe 22: Seien G eine Gruppe, $H \leq G$ eine echte Untergruppe und $K \trianglelefteq G$ ein Normalteiler von G sowie $P \leq G$ eine p-Sylowgruppe. Zeigen Sie:

a) Aus $N_G(P) \leq H$ folgt $H = N_G(H)$.

b) $P \cap K$ ist eine p-Sylowgruppe von K.

c) $(PK)/K$ ist eine p-Sylowgruppe von G/K.

Aufgabe 23: Sei G eine Gruppe mit 45 Elementen. Zeigen Sie:

a) Alle Sylowgruppen von G sind normal in G.

b) G ist das direkte Produkt seiner Sylowgruppen.

c) G ist abelsch.

Bestimmen Sie

d) bis auf Isomorphie alle Gruppen der Ordnung 45.

Aufgabe 24: Sei G eine Gruppe mit 12 Elementen. Bestimmen Sie die Anzahl s_2 bzw. s_3 der 2- bzw. 3-Sylowgruppen.
Zeigen Sie, daß $s_2 = 3$ und $s_3 = 4$ nicht vorkommen kann und daß im Falle $s_2 = s_3 = 1$ dir Gruppe G sogar abelsch ist.

Aufgabe 25: Zeigen Sie: Gruppen der Ordnung 75 und 100 sind auflösbar.

Aufgabe 26: Zeigen Sie: Gruppen der Ordnung 24 sind auflösbar.

Aufgabe 27: Zeigen Sie, daß es bis auf Isomorphie vier vierelementige Ringe gibt.
Welche davon sind kommutativ, nullteilerfrei oder Körper?
Hinweis: Bestimmen Sie zunächst die möglichen additiven Gruppen $(R, +)$ und dann mit Hilfe von Gruppentafeln und den Distributivregeln die möglichen Verknüpfungstafeln der Multiplikation.

Aufgabe 28: Zeigen Sie, daß es bis auf Isomorphie vier Ringe mit p^2 Elementen für eine Primzahl $p \in \mathbb{P}$ gibt.

Aufgabe 29: Zeigen Sie, daß die Unterringe $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ und $\mathbb{Z}[\sqrt{3}] \subset \mathbb{R}$ nicht isomorph sind.

Aufgabe 30:
a) Geben Sie einen Ringhomomorphismus an, der nicht jeden Nullteiler auf einen Nullteiler abbildet. Zeigen Sie, daß ein solcher Homomorphismus nicht injektiv sein kann.
b) Für einen Ringhomorphismus $f : R \longrightarrow S$ gilt: $f(R^*) \subset S^*$.

Aufgabe 31: Sei $i \in \mathbb{C}$ mit $i^2 = -1$.
a) Bestimmen Sie alle Einheiten in $\mathbb{Z}[i]$.
b) Zeigen Sie, daß jede Primzahl $p \in \mathbb{P}$ genau dann in $\mathbb{Z}[i]$ reduzibel ist, wenn p Summe zweier Quadrate ist, d. h. $p = a^2 + b^2$ für $a, b \in \mathbb{Z} - \{0\}$.
(*Hinweis:* Zur „Hin"-Richtung läßt sich zeigen: aus $(a + bi) \mid p$ folgt $(a - bi) \mid p$.)
c) Zerlegen Sie 210 in irreduzible Elemente von $\mathbb{Z}[i]$.

Aufgabe 32: Sei R ein Integritätsring.
Ein Element $p \in R$ heißt *Primelement*, wenn
(i) p eine von Null verschiedene Nichteinheit ist und
(ii) für alle $a, b \in R$ aus $p \mid ab$ stets $p \mid a$ oder $p \mid b$ folgt.
Ein Element $q \in R$ heißt *irreduzibel*, wenn
(i) q eine von Null verschiedene Nichteinheit ist und
(ii) $q = ab$ mit $a, b \in R$ nur für $a \in R^*$ oder $b \in R^*$ möglich ist.
Zeigen Sie,
a) daß jedes Primelement irreduzibel ist.
b) daß die Umkehrung nicht gilt, indem Sie in $\mathbb{Z}[\sqrt{-5}]$ ein geeignetes Element auf zwei verschiedene Weisen in irreduzible Faktoren zerlegen.

Aufgabe 33: (*Zusatzaufgabe*)
Definition: *Sei K ein Körper und V ein n-dimensionaler K-Vektorraum, $n \in \mathbb{N}$. Eine Familie von Unterverktorräumen $\mathcal{F} := \{F_1, \dots, F_n\}$ heißt eine* Fahne, *wenn gilt:*

$$(i)\ F_1 \lneqq F_2 \lneqq \dots \lneqq F_n = V, \quad (ii)\ dim_K(F_i) = i \text{ für alle } i = 1, \dots, n\ .$$

Seien nun p eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen, $V := \mathbb{F}_p^n$ und $G := \mathrm{GL}(n, \mathbb{F}_p)$.

a) Jede p-Sylowgruppe H von G läßt eine Fahne $\mathcal{F}$ fest, d.h. für alle $h \in H$ und alle $i = 1, \dots, n$ ist $hF_i = F_i$.
b) Die Menge aller Fahnen von V steht in Bijektion mit der Menge aller p-Sylowgruppen von G.
c) Berechnen Sie die Anzahl der p-Sylowgruppen von G.
d) Sei nun $H \leq \mathrm{GL}(4, \mathbb{F}_p)$ eine p-Sylowgruppe und $\mathcal{F} = \{F_i\}_{1 \leq i \leq 4}$ eine Fahne, die von H festgelassen wird. Dann gilt für die obere Zentralreihe $\{C^i(H)\}_{0 \leq i \leq 3}$von H, daß für alle $i = 0, \dots, 3$ die $C^i(H)$ die F_j für $j \leq i + 1$ elementweise festlassen.
Machen Sie sich klar, daß diese Aussage auch für beliebiges n und nicht nur für 4 gilt.

Hinweise: Fahnensatz (Lamprecht, Lineare Algebra 1; Fischer, Lineare Algebra, Bemerkung zu 4.4.2); $H = \left\{\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\right\}$ ist p-Sylowgruppe in G; Zahl der (verschiedenen) Fahnen.

Aufgabe 34: Sei R ein kommutativer Ring mit 1. Zeigen Sie:

a) Für ein Ideal $I \neq R$ von R sind äquivalent:
   (i) Für Elemente $a, b \in R$ gilt: $ab \in I \Rightarrow a \in I$ oder $b \in I$.
   (ii) Der Ring R/I ist nullteilerfrei.
   Solche Ideale heißen *Primideale*.

b) Ist jedes von R verschiedene Hauptideal in R ein Primideal, so ist R Körper.

c) Sei I ein Ideal in R und $I[X] = IR[X]$ das von I im Ring $R[X]$ erzeugte Ideal. Dann ist $I[X]$ Primideal in $R[X]$ genau dann, wenn I Primideal von R ist.

d) $I := \{f \in \mathbb{Z}[X] \mid f(0) = 0\} \subset \mathbb{Z}[X]$ ist ein Hauptideal in $\mathbb{Z}[X]$. Ist I Primideal? Ist I maximales Ideal? Ist $\mathbb{Z}[X]$ ein Hauptidealring?

Aufgabe 35: Sei $f(X,Y) = XY^2 + X^3 \in \mathbb{Q}[X,Y]$ Untersuchen Sie, welche der folgenden Faktorringe Körper sind.

$$(i) \quad \mathbb{Q}[X,Y]/(f(X,Y)), \qquad (ii) \quad \mathbb{Q}(X)[Y]/(f(X,Y)), \quad (iii) \quad \mathbb{Q}(Y)[X]/(f(X,Y)).$$

Aufgabe 36: Welche der folgenden Körpererweiterungen sind endlich, algebraisch, transzendent? Versuchen Sie jeweils, den Grad der Erweiterung zu bestimmen.

a) $\mathbb{R}/\mathbb{Q}$,
b) $\mathbb{R}/\mathbb{Q}(\sqrt{2})$,
c) $\mathbb{Q}(\zeta)/\mathbb{Q}$, wobei $\zeta \in \mathbb{C}$ eine n-te Einheitswurzel ist,
d) $\mathbb{Q}(\{a \in \mathbb{C} \mid a \text{ algebraisch}/\mathbb{Q}\})/\mathbb{Q}$,
e) $\mathbb{R}(\{a \in \mathbb{C} \mid a \text{ algebraisch}/\mathbb{R}\})/\mathbb{R}$,
f) $\mathbb{R}(\{a \in \mathbb{C} \mid a \text{ algebraisch}/\mathbb{Q}\})/\mathbb{Q}$,
g) $\mathbb{Q}(\{\sqrt[n]{2} \mid n \in \mathbb{N}\})/\mathbb{Q}$,
h) $\mathbb{Q}(\{\sqrt{2^n} \mid n \in \mathbb{N}\})/\mathbb{Q}$.

Aufgabe 37: Sei $a = \sqrt{3} + \sqrt{5}$.

a) Berechnen Sie den Körpergrad von $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{15})/\mathbb{Q}$.

b) Zeigen Sie, daß a algebraisch über $\mathbb{Q}$ ist, und berechnen Sie das Minimalpolynom von a über $\mathbb{Q}(\sqrt{15})$ und über $\mathbb{Q}$.

c) Zeigen Sie, daß $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(a)$ ist, also (warum?) jedes Element aus $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ von der Form $b_o + b_1 a + b_2 a^2 + b_3 a^3$ mit $b_i \in \mathbb{Q}$ ist. Berechnen Sie diese b_i explizit für a^4 und $\frac{1}{a}$.

Aufgabe 38: Sei $\frac{m}{n} \in \mathbb{Q}$ mit $\mathrm{ggT}(m,n) = 1$ Nullstelle des Polynoms $a_0 + a_1 X + \ldots + a_k X^k \in \mathbb{Z}[X]$. Dann gilt $m \mid a_0$ und $n \mid a_k$.

Aufgabe 39: Zeigen Sie die Irreduzibilität der folgenden Polynome über $\mathbb{Q}$:

$$\begin{aligned} f_1 &= X^2 + n_1 X + n_0 \in \mathbb{Z}[X] \,\mathrm{mit}\, n_1, n_0 \in (\mathbb{Z} - 2\mathbb{Z}) \;, \\ f_2 &= X^4 + m_3 X^3 + m_2 X^2 + m_1 X + m_0 \,\mathrm{mit}\, m_1, m_2 \in 2\mathbb{Z} \,\mathrm{und}\, m_0, m_3 \in (\mathbb{Z} - 2\mathbb{Z}) \;. \end{aligned}$$

Aufgabe 40: Sei $f(X) = a_0 + a_1 X + \ldots + a_s X^s \in \mathbb{Z}[X]$ mit $a_s \neq 0$ und $p \in \mathbb{P}$ eine Primzahl. $f(X)$ ist irreduzibel über $\mathbb{Q}$, falls eine der Bedingungen erfüllt ist:

a) Das reduzierte Polynom $\overline{f}(X) \in \mathbb{F}_p[X]$ hat denselben Grad wie $f(X)$, d. h. $a_s \not\equiv 0 (\mathrm{mod} p)$, und ist irreduzibel über $\mathbb{F}_p$.

b) $a_s \not\equiv 0 (\mathrm{mod} p)$, $a_i \equiv 0 \pmod p$ für $0 \leq i \leq s-1$ und $a_0 \not\equiv 0 (\mathrm{mod} p^2)$.

Aufgabe 41: Für einen beliebigen Körper K sei $g(X) \in K[X]$ irreduzibel über K. Dann ist für alle $c \in K$ auch $g(X+c)$ irreduzibel.

Aufgabe 42: Sei $p \in \mathbb{P}$. Das Polynom $h(X) = X^p - X + a \in \mathbb{F}_p[X]$ ist für $a \in \mathbb{F}_p - \{0\}$ irreduzibel.

Aufgabe 43: Verwenden Sie obige Kriterien, um die folgenden Polynome auf Irreduzibilität über $\mathbb{Q}$ zu prüfen.

a) $X^3 - 7X^2 + 3X + 3$

b) $X^8 + 1$

c) $X^3 + 3X - 2$

d) $X^4 + 15X^3 + 7$

e) $X^7 + 21X^5 + 35X^2 + 34X - 8$

f) $2X^{15} + 6X^{10} + 9X^5 + 3$

Aufgabe 44: Sei L/K eine Körpererweiterung und $\alpha \in L$ transzendent über K. Zeigen Sie:

a) α^2 ist transzendent über K.

b) $K(\alpha^2) \neq K(\alpha)$.

c) Ist $\beta \in K(\alpha) - K$, dann ist β transzendent über K.

d) Ist $\beta = f(\alpha)$ für $f \in K[X]$ mit $\deg(f) = n \geq 1$, dann ist $K(\alpha)$ algebraisch über $K(\beta)$ vom Grad n.

e) $K(\alpha)/K$ besitzt unendlich viele Zwischenkörper.

Aufgabe 45: Finden Sie für

$$\sqrt{7}, \quad \frac{\sqrt{11}+3}{2}, \quad \frac{i\sqrt{3}-1}{2} \quad \text{und} \quad \sqrt[3]{2}$$

die Minimalpolynome über $\mathbb{Q}$.

Aufgabe 46: 1873 zeigte *Charles Hermite*, daß e transzendent ist, und 1882 wurde die Transzendenz von π durch *Ferdinand Lindemann* nachgewiesen. Inzwischen weiß man auch, daß e^π transzendent ist (*Aleksandr Gelfond* 1934). Bis heute ist aber ungeklärt, ob die Zahl $e + \pi$ rational oder irrational, algebraisch oder transzendent ist, ebenso für $e \cdot \pi$. Zeigen Sie:

a) π ist transzendent. Nutzen Sie dazu den
Satz von Lindemann: *Ist $0 \neq a \in \mathbb{C}$ algebraisch über $\mathbb{Q}$, dann ist e^a transzendent.*
(Diesen Satz müssen Sie nicht zeigen!)

b) Sei $0 \neq b \in \mathbb{Q}$. Für jedes $a \in \mathbb{R}$ gilt:

$$a \text{ ist transzendent } \Leftrightarrow a^b \text{ ist transzendent }.$$

c) Wenigstens eine der Zahlen $e + \pi$ und $e \cdot \pi$ ist transzendent. Nutzen Sie dazu die Transzendenz von e und π.

Charles Hermite

Ferdinand Lindemann

Aleksandr Gelfond

Aufgabe 47: Sei $\zeta_7 \in \mathbb{C}$ eine primitive 7-te Einheitswurzel.

a) Zeigen Sie, daß die Erweiterung $\mathbb{Q}(\sqrt[7]{7})/\mathbb{Q}$ nicht normal ist, indem Sie eine Einbettung von $\mathbb{Q}(\sqrt[7]{7})$ in den (fixierten) algebraischen Abschluß von $\mathbb{Q}$ angeben, die kein Automorphismus von $\mathbb{Q}(\sqrt[7]{7})$ ist.

b) Ist die Erweiterung $\mathbb{Q}(\zeta_7, \sqrt[7]{7})/\mathbb{Q}(\zeta_7)$ normal?

c) Zeigen Sie, daß jede Erweiterung vom Grad 2 normal ist.

d) Geben Sie eine normale Körpererweiterung vom Grad 3 an.

Aufgabe 48: Sei k ein Körper und $L = k(X)$ der Körper der rationalen Funktionen in X über k. Weiter sei $u = \frac{f}{g}$ eine nichtkonstante rationale Funktion und $\mathrm{ggT}(f, g) = 1$.

a) u ist transzendent über k.

b) $f(T) - ug(T) \in k(u)[T]$ ist ein irreduzibles Polynom mit Nullstelle X in L.

c) Genau dann ist $k(u) = L$, wenn $\max\{\deg(f), \deg(g)\} = 1$ gilt.

d) Ist σ ein k-Automorphismus von L, so ist $\sigma(X) = \frac{aX+b}{cX+d}$ mit $a, b, c, d \in k$ und $ad - bc \neq 0$.
Umgekehrt bestimmt jede derartige rationale Funktion $\frac{aX+b}{cX+d}$ einen k-Automorphismus von L.

e) Beschreiben Sie die Gruppe $\mathrm{Aut}(L|k)$ aller k-Automorphismen von L.
Wieviele Elemente besitzt sie für $k = \mathbb{F}_7$ bzw. $k = \mathbb{F}_{31}$?

Aufgabe 49:

a) Seien $n, m \in \mathbb{N}$ und K ein Körper der Charakteristik 0 und $\sqrt{m} \notin K$. Zeigen Sie:
Ist $K(\sqrt{n}, \sqrt{m}) = K(\sqrt{n})$, so gilt $\sqrt{mn} \in K$.

b) Seien $s \in \mathbb{N}$ und $n_1, \dots, n_s \in \mathbb{N}$ paarweise teilerfremde natürliche Zahlen mit $\sqrt{n_i} \notin \mathbb{Q}$. Weiter sei $S := \{\sqrt{n_i} \mid 1 \leq i \leq s\}$. Zeigen Sie, daß $\mathbb{Q}(S)|\mathbb{Q}$ galoissch ist vom Grade 2^s und die Galoisgruppe von $\mathbb{Q}(S)|\mathbb{Q}$ isomorph zu $(\mathbb{Z}/2\mathbb{Z})^s$ ist.

Hinweis: Beachten Sie, daß aus $a\sqrt{n} + b\sqrt{m} \in K$ durch Quadrieren $ab\sqrt{nm} \in K$ folgt. Die Gradbehauptung in Teil b) läßt sich beispielsweise mittels vollständiger Induktion nach s zeigen, wobei beim Induktionsschritt Teil a) benutzt werden kann.

Aufgabe 50: Sei $L = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$. Bestimmen Sie die 14 echten Zwischenerweiterungen $M = \mathbb{Q}(?)$ sowie die Galoisgruppen $\mathrm{Gal}(L|M) \leq \mathrm{Gal}(L|\mathbb{Q})$ explizit, also in der Form $\mathrm{Gal}(L|M) \ni \sigma : L \to L$ ist M-Automorphismus.

Aufgabe 51: Sei $p(X) = X^4 - 5$.

a) Zeigen Sie, daß $L := \mathbb{Q}(i, \sqrt[4]{5})$ der Zerfällungskörper von $p(X)$ ist.

b) Bestimmen Sie eine Basis von $L|\mathbb{Q}$.

c) Zeigen Sie: $\mathrm{Gal}(L|\mathbb{Q}) \cong D_8$, die Diedergruppe mit 8 Elementen.

d) Ordnen Sie in einem entsprechenden Diagramm jeder Untergruppe H von D_8 ihren Fixkörper L^H zu. Welche der Erweiterungen $L|L^H$ und $L^H|\mathbb{Q}$ sind galoissch?
e) Bestimmen Sie $L^H = \mathbb{Q}(?)$ für wenigstens zwei nichttriviale Untergruppen $H \leq D_8$.

Hinweis: D_8 hat acht nichttriviale Untergruppen.

Aufgabe 52: Betrachten Sie die Körper $K_1 := \mathbb{Q}(\sqrt[6]{5})$, $K_2 := \mathbb{Q}(\sqrt{3}+\sqrt{5})$ und K_3 der Zerfällungskörper von $X^3 - 5 \in \mathbb{Q}[X]$.
Untersuchen Sie, welche der Körpererweiterungen $K_i/\mathbb{Q}$, K_iK_j/K_i und $K_i \cap K_j/\mathbb{Q}$ für $i, j \in \{1, 2, 3\}$ galoissch sind.

Aufgabe 53:
a) Sei $n \in \mathbb{N}$. Zeigen Sie, daß $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ genau dann galoissch ist, wenn $n \leq 2$ ist.
b) Es sei $K \subset \mathbb{C}$ ein Körper, der alle Einheitswurzeln enthält. Zeigen Sie, daß $K(\sqrt[n]{2})/K$ galoissch ist.

Aufgabe 54: Sei $\zeta_7 \in \mathbb{C}$ eine primitive 7-Einheitswurzel, d. h. $\zeta_7^7 = 1$ und $\zeta_7^j \neq 1$ für $1 \leq j \leq 6$.
a) Zeigen Sie, daß das Minimalpolynom $M(\zeta_7, \mathbb{Q}) = 1 + X + X^2 + \ldots + X^6$ ist.
b) Zeigen Sie, daß $\mathrm{Gal}(\mathbb{Q}(\zeta_7)|\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ ist.
c) Zeigen Sie, daß $\mathbb{Q}(\sqrt{-7})$ und $\mathbb{Q}(\zeta_7) \cap \mathbb{R}$ die einzigen Körper sind, die zwischen $\mathbb{Q}$ und $\mathbb{Q}(\zeta_7)$ liegen.
d) Berechnen Sie $\mathrm{Aut}_k(K)$ für $k, K \in \{\mathbb{Q},\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\zeta_7) \cap \mathbb{R}, \mathbb{Q}(\zeta_7)\}$.

Hinweis: Ist $n \in \mathbb{N}$ ungerade, so gelten die folgenden Relationen, die Sie eventuell nützlich finden werden:

$$\prod_{j=1}^{n-1}(1-\zeta_n^j) = n \text{ und } (1-\zeta_n^j)(1-\zeta_n^{-j}) = -(\zeta_n^{\frac{-j}{2}} - \zeta_n^{\frac{j}{2}})^2 \in \mathbb{R},$$

wobei $\pm\frac{a}{2}$ modulo n zu verstehen ist. Versuchen Sie, diese Relationen zu beweisen.

Aufgabe 55: Sei $k = \mathbb{F}_3(t)$ Bestimmen Sie den Separabilitäts– und den Inseparabilitätsgrad von $k(\alpha)/k$, wobei α eine Nullstelle von
a) $X^3 + t$,
b) $X^6 + t$,
c) $X^6 + t^2X + t$,
d) $X^2 - t^2$ ist.

Aufgabe 56: Sei $p \in \mathbb{P}$ und $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad p. Zeigen Sie:
a) Enthält die Galoisgruppe von f ein Element der Ordnung p und eine Transposition, so ist sie S_p.
b) Hat f nur zwei nicht reelle Nullstellen in $\mathbb{C}$, dann ist die Galoisgruppe von f die Gruppe S_p.

Aufgabe 57: Bestimmen Sie die Galoisgruppen der Zerfällungskörper folgender Polynome über $\mathbb{Q}$.
a) $X^4 + X^2 - 6$
b) $X^3 - 3X + 1$

c) $4X^5 - 15X^4 + 20X^3 - 30X^2 + 40X - 10$

Hinweis zu b) und c): Wieviele reelle und wieviele komplexe Nullstellen haben diese Polynome?

Aufgabe 58: Vereinfachen Sie den Ausdruck $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}$, indem Sie ein Polynom $f(X)$ mit dieser Nullstelle bestimmen und $f(X)$ faktorisieren.

Am Ende der Veranstaltung wurde eine zweistündige Klausur abgehalten. Für eine Eins genügte die vollständige und richtige Bearbeitung von sechs der acht Aufgaben.

Probeklausur zur Algebra I, WS 2000/01

Gruppentheorie

Aufgabe 59: Sei G eine Gruppe mit Zentrum $Z(G)$. Ist $G/Z(G)$ zyklisch, dann ist G abelsch.

Aufgabe 60: Operiert die Gruppe G mit $|G| = 55$ auf einer Menge M mit $|M| = 34$, so gibt es mindestens einen Fixpunkt.

Aufgabe 61: Zeigen Sie: Gruppen der Ordnung 45 sind auflösbar.

Ringtheorie, Körpererweiterungen

Aufgabe 62: Zeigen Sie, daß $X^3 + 6X^2 - 12X + 2$ irreduzibel über $\mathbb{Q}$ und über $\mathbb{Q}(\sqrt[5]{2})$ ist.

Aufgabe 63: Für alle $a \in \mathbb{Q}$ sind $\cos(a\pi)$ und $\sin(a\pi)$ algebraisch über $\mathbb{Q}$.

Galoistheorie

Aufgabe 64: Zeigen Sie, daß $\mathbb{Q}(i\sqrt{5})|\mathbb{Q}$ und $\mathbb{Q}((1+i)\sqrt[4]{5})|\mathbb{Q}(i\sqrt{5})$ galoissch sind, aber $\mathbb{Q}((1+i)\sqrt[4]{5})|\mathbb{Q}$ nicht galoissch ist.

Aufgabe 65: Bestimmen Sie die Galoisgruppen der Zerfällungskörper der folgenden Polynome über $\mathbb{Q}$:

a) $(X^2 + 5)(X^2 - 5)$

b) $X^4 + X^3 + X^2 + X + 1$

c) $(X^3 - 5)(X^2 - 7)$

Aufgabe 66: Zeigen Sie, daß $\mathbb{Q}(\sqrt[4]{-1})|\mathbb{Q}$ eine galoissche Erweiterung vom Grad 4 ist.

Klausur zur Algebra I, WS 2000/01

Gruppentheorie

Aufgabe 67: Seien G und H Gruppen sowie $\varphi : G \longrightarrow H$ ein Homomorphismus. Beweisen oder widerlegen Sie:

a) Für $x \in G$ mit $\mathrm{ord}(x) = m < \infty$ gilt $\mathrm{ord}(\varphi(x)) \mid m$.

b) Aus $x \in Z(G)$ folgt $\varphi(x) \in Z(H)$.

c) Aus $N \trianglelefteq G$ folgt $\varphi(N) \trianglelefteq \varphi(G)$.

Aufgabe 68: Seien $p, q \in \mathbb{P}$ mit $p > q$. Zeigen Sie, daß alle Gruppen der Ordnung $p^2 q$ auflösbar sind.

Aufgabe 69: Operiert die Gruppe G mit $|G| = 39$ auf einer Menge M mit $|M| = 17$, so gibt es mindestens einen Fixpunkt.

Ringtheorie, Körpererweiterungen

Aufgabe 70: Konstruieren Sie einen Körper K mit 125 Elementen und geben Sie eine Basis von K über seinem Primkörper $\mathbb{F}_5$ an. Hat $X^2 + X + 1$ in diesem Körper eine Nullstelle?

Aufgabe 71: Sei K ein Körper und α algebraisch über K. Zeigen Sie: Ist der Grad des Minimalpolynoms von α ungerade, so ist $K(\alpha^2) = K(\alpha)$.

Galoistheorie

Aufgabe 72: Sei $L = \mathbb{Q}(\sqrt{2} + \sqrt{5})$. Bestimmen Sie $\mathrm{Gal}(L|\mathbb{Q}) = \{\sigma : L \longrightarrow L \mid \sigma \text{ ist } \mathbb{Q} - \text{Automorphismus}\}$ sowie alle Untergruppen $U \leq \mathrm{Gal}(L|\mathbb{Q})$ und deren Fixkörper $L^U = \mathbb{Q}(?)$.

Aufgabe 73: Bestimmen Sie die Galoisgruppen der Zerfällungskörper der folgenden Polynome über $\mathbb{Q}$:

a) $X^2 + X + 1$

b) $(X^3 - 2)(X^2 - 5)$

c) $(X^2 + 1)(X^4 - 5)$

Aufgabe 74: Zeigen Sie, daß $\mathbb{Q}(\sqrt[4]{-4})|\mathbb{Q}$ eine galoissche Erweiterung vom Grad 2 ist. Geben Sie eine einfachere Beschreibung dieses Körpers.