Übungen zu Algebra, WS 2013/14

Christoph Baxa

1) Es sei G eine endliche Gruppe und $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$ eine Normalreihe. Beweisen Sie

$$|G| = \prod_{i=0}^{n-1} |G_i/G_{i+1}|.$$

2) Finden Sie eine Kompositionsreihe und ihre Faktoren für die folgenden Gruppen:

a) Die symmetrische Gruppe S_n (mit $n \in \{1, 2, 3, 4\}$),

b) Die Quaternionengruppe Q_8.

3) Finden Sie eine Kompositionsreihe und ihre Faktoren für die Diedergruppe D_n (mit $n \geq 3$). Beachten Sie die Konvention $|D_n| = 2n$.

4) a) Beweisen Sie, dass die Gruppe $(\mathbb{Z}, +)$ keine Kompositionsreihe besitzt.

b) Beweisen Sie, dass die Gruppen $(\mathbb{Z}_4, +)$ und $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ in ihren Kompositionsreihen Faktoren besitzen, die nach Art (d.h. bis auf Isomorphie) und Anzahl übereinstimmen.

5) a) Es seien $I : \mathbb{R}^2 \to \mathbb{R}^2$, $I(x, y) = (x, y)$ und $S : \mathbb{R}^2 \to \mathbb{R}^2$, $S(x, y) = (x, -y)$. Weiters bezeichne $G = (\{I, S\}, \circ)$ und $M = \mathbb{R}^2$. Bestimmen Sie für die Operation von G auf M die Bahnen und Isotropiegruppen für alle $(x, y) \in \mathbb{R}^2$ sowie die Fixpunkte dieser Operation.

b) Die Gruppe $\mathrm{SO}(2)$ operiere auf dem $\mathbb{R}^2$ mittels $(A, \mathbf{x}) \mapsto A\mathbf{x}$. Bestimmen Sie die Bahnen und Isotropiegruppen für alle $\mathbf{x} \in \mathbb{R}^2$ sowie die Fixpunkte dieser Operation.

6) Es bezeichne $\mathbb{F}_2 = \{0, 1\}$ den Körper mit zwei Elementen. Die Gruppe $\mathrm{GL}_2(\mathbb{F}_2)$ operiere auf $\mathbb{F}_2^2$ mittels $(A, \mathbf{x}) \mapsto A\mathbf{x}$.

a) Bestimmen Sie die Bahnen und Isotropiegruppen für alle $\mathbf{x} \in \mathbb{F}_2^2$ sowie die Fixpunkte dieser Operation.

b) Betrachten Sie die Operation von $\mathrm{GL}_2(\mathbb{F}_2)$ auf $\mathbb{F}_2^2 \setminus \{\mathbf{0}\}$. Leiten Sie $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ ab.

7) Beweisen Sie die folgenden Aussagen:

a) Die Gruppe $\mathrm{SL}_2(\mathbb{R})$ operiert auf der oberen Halbebene $H = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$ mittels

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}.$$

b) Die Isotropiegruppe von i für diese Operation ist die Gruppe $\mathrm{SO}(2)$.

Definition. Man sagt, die Gruppe G operiert transitiv auf der Menge M, wenn es für alle $x, y \in M$ ein $a \in G$ mit der Eigenschaft $a \cdot x = y$ gibt.

8) Entscheiden Sie, ob die folgenden Operationen von Gruppen auf Mengen transitiv sind:

a) S_n operiert auf $\{1, \dots, n\}$ mittels $(\sigma, i) \mapsto \sigma(i)$,
b) D_n operiert auf $\{1, \dots, n\}$ mittels $(\sigma, i) \mapsto \sigma(i)$,
c) Die Operation aus Beispiel 5a),
d) Die Operation aus Beispiel 5b),
e) Die Operation aus Beispiel 6a),
f) Die Operation aus Beispiel 6b).

9) Die Gruppe G operiere transitiv auf der Menge M. Beweisen Sie:

a) Für alle $x \in M$ ist die Bahn von x ganz M,
b) Die Isotropiegruppen G_x (mit $x \in M$) sind zueinander konjugiert,
c) $|M| = [G : G_x]$ für alle $x \in M$,
d) $|M| \mid |G|$.
e) Was bedeuten Teile a) bis d) für die Beispiele aus Bsp. 8 (für die sie sinnvoll sind)?

Definition. Es sei G eine Gruppe und $H \leq G$. Die Menge

$$C_G(H) := \{a \in G \mid ha = ah \text{ für alle } h \in H\}$$

wird als Zentralisator von H bezeichnet.

10) Es sei G eine Gruppe und $H \leq G$. Beweisen Sie $C_G(H) \trianglelefteq N_G(H)$.

11) Es sei G eine Gruppe, $\varphi \in \mathrm{Aut}(G)$ und C eine Konjugationsklasse von G. Zeigen Sie:

a) $\varphi(C)$ ist ebenfalls eine Konjugationsklasse von G,
b) Ist $\varphi \in \mathrm{Inn}(G)$, so gilt $\varphi(C) = C$.

12) Für eine Permutation $\sigma \in S_n$ und $r \geq 1$ bezeichne $z_r(\sigma)$ die Anzahl der r-Zyklen in der Zerlegung von σ in paarweise elementfremde Zyklen. Beweisen Sie, dass $\sigma, \tau \in S_n$ genau dann konjugiert sind, wenn $z_r(\sigma) = z_r(\tau)$ für alle $r \geq 1$.

13) Es sei $n \geq 3$. Finden Sie alle Konjugationsklassen der Gruppe D_n und beweisen Sie, dass D_n genau $\frac{n+6}{2}$ (bzw. $\frac{n+3}{2}$) Konjugationsklassen besitzt, wenn n gerade (bzw. ungerade) ist.

14) Eine Gruppe G der Ordnung $|G| = 55$ operiere auf einer Menge M der Kardinalität $|M| = 39$. Beweisen Sie, dass diese Operation einen Fixpunkt besitzt.

15) Es sei G eine Gruppe. Beweisen Sie: Ist $G/Z(G)$ zyklisch, so ist G abelsch.

16) Es sei p eine Primzahl und G eine Gruppe der Ordnung $|G| = p^2$. Beweisen Sie, dass G abelsch ist. Folgern Sie, dass entweder $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ gilt.

17) Bestimmen Sie Anzahl und Gestalt der 5-Sylowgruppen der Gruppe S_5.

18) Es sei G eine endliche, einfache Gruppe mit Ordnung $|G| = 168$. Bestimmen Sie die Anzahl der $a \in G$ mit Ordnung $\operatorname{ord}(a) = 7$.

19) Bestimmen Sie Anzahl und Gestalt der 2-Sylowgruppen der Gruppe S_4.

20) Beweisen Sie, dass die Gruppen a) S_4 und b) $\mathrm{GL}_2(\mathbb{Z}_2)$ auflösbar sind.

21) Es sei K ein Körper. Beweisen Sie, dass die Gruppe

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in K, ac \neq 0 \right\}$$

(versehen mit der Matrixmultiplikation) auflösbar ist. *Hinweis.* Betrachten Sie den Homomorphismus

$$\varphi : G \to K^* \times K^*, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c).$$

Definition. Es sei G eine Gruppe. Eine Untergruppe H von G heißt charakteristisch, wenn $\varphi(H) = H$ für alle $\varphi \in \operatorname{Aut}(G)$.

22) Es sei G eine Gruppe und $H \leq G$. Beweisen Sie:

a) Wenn H charakteristische Untergruppe von G ist, dann ist $H \trianglelefteq G$,

b) H ist genau dann charakteristische Untergruppe von G wenn $\varphi(H) \leq H \ \forall \varphi \in \operatorname{Aut}(G)$.

23) Es sei G eine Gruppe. Beweisen Sie:

a) $Z(G)$ ist charakteristische Untergruppe von G,

b) G' ist charakteristische Untergruppe von G.

24) Beweisen Sie $D_n' = \langle \alpha^2 \rangle$. Leiten Sie die Struktur von D_n' ab. Ist D_n auflösbar?

25) Es sei G eine Gruppe und $H \leq G$. Beweisen Sie:

a) $H^{(i)} \leq G^{(i)}$ für alle $i \geq 0$,

b) Wenn G auflösbar ist, ist H ebenfalls auflösbar.

26) a) Es seien G und H Gruppen und $\varphi : G \to H$ ein Gruppenepimorphismus. Beweisen Sie $\varphi(G^{(i)}) = \varphi(G)^{(i)}$ für alle $i \geq 0$.
b) Es seien G und H Gruppen und $\varphi : G \to H$ ein Gruppenepimorphismus. Beweisen Sie: Wenn G auflösbar ist, ist H ebenfalls auflösbar.
c) Es sei G eine auflösbare Gruppe und $N \trianglelefteq G$. Beweisen Sie, dass G/N auflösbar ist.

27) Es seien R, S kommutative Ringe mit 1, $\varphi : R \to S$ ein Ringhomomorphismus mit der Eigenschaft $\varphi(1_R) = 1_S$ und M ein S-Modul. Beweisen Sie, dass M durch $R \times M \to M$, $(a, m) \mapsto \varphi(a) \cdot m$ zu einem R-Modul wird.

28) Es sei M ein R-Modul und I ein Ideal von R mit der Eigenschaft, dass $am = 0$ für alle $a \in I$ und alle $m \in M$. Beweisen Sie:

a) $bm = cm$ wenn $b - c \in I$,
b) M wird durch $(a + I) \cdot m := a \cdot m$ ein R/I-Modul.

29) Es sei M ein R-Modul. Beweisen Sie:

a) $a \cdot 0 = 0$ für alle $a \in R$,
b) $0 \cdot m = 0$ für alle $m \in M$,
c) $(-a)m = -(am) = a(-m)$ für alle $a \in R$ und alle $m \in M$,
d) $k(am) = a(km)$ für alle $k \in \mathbb{Z}$, alle $a \in R$ und alle $m \in M$.

30) Es seien M und N zwei R-Moduln. Beweisen Sie: Setzt man

$$(\varphi + \psi)(m) := \varphi(m) + \psi(m) \quad (\text{für } \varphi, \psi \in \mathrm{Hom}_R(M, N),\ m \in M)$$

und

$$(a\varphi)(m) := a\varphi(m) \quad (\text{für } a \in R,\ \varphi \in \mathrm{Hom}_R(M, N),\ m \in M),$$

so wird $\mathrm{Hom}_R(M, N)$ dadurch ein R-Modul.

31) a) Es seien M, N und L drei R-Moduln. Zeigen Sie: Ist $\varphi \in \mathrm{Hom}_R(M, N)$ und $\psi \in \mathrm{Hom}_R(N, L)$, dann ist $\psi \circ \varphi \in \mathrm{Hom}_R(M, L)$.

b) Beweisen Sie: Versieht man $\mathrm{End}_R M$ mit der Addition aus dem vorangegangenen Beispiel und der Verknüpfung von Abbildungen (d.h. $(\varphi \circ \psi)(m) = \varphi(\psi(m))$ für $\varphi, \psi \in \mathrm{End}_R M$ und $m \in M$), so wird $\mathrm{End}_R M$ dadurch zu einem Ring mit 1.

32) Es sei M ein R-Modul. Beweisen Sie:
a) Ist $X \subseteq M$, so ist

$$\langle X \rangle_R = \left\{ \sum_{i=1}^{n} a_i m_i \;\middle|\; n \geq 0, a_1, \dots, a_n \in R, m_1, \dots, m_n \in X \right\}.$$

b) Ist $m \in M$, so ist $\langle m \rangle_R = Rm = \{am \mid a \in R\}$.

33) Es sei $I \neq \varnothing$ eine Indexmenge. Für alle $i \in I$ sei M_i ein R-Modul. Beweisen Sie:
a) Versieht man

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i \text{ für alle } i \in I\}$$

mit den Verknüpfungen $(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)_{i \in I}$ und $a \cdot (m_i)_{i \in I} := (am_i)_{i \in I}$, so wird $\prod_{i \in I} M_i$ dadurch zu einem R-Modul.
b) Versieht man

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i \text{ für alle } i \in I \text{ und } m_i = 0 \text{ für fast alle } i \in I\}$$

mit den Verknüpfungen $(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)_{i \in I}$ und $a \cdot (m_i)_{i \in I} := (am_i)_{i \in I}$, so wird $\bigoplus_{i \in I} M_i$ dadurch zu einem R-Modul, der ein Teilmodul von $\prod_{i \in I} M_i$ ist.

34) Es sei $I \neq \varnothing$ eine Indexmenge. Für alle $i \in I$ sei M_i ein R-Modul. Beweisen Sie:
a) Für alle $k \in I$ ist die Projektion

$$\pi_k : \prod_{i \in I} M_i \to M_k, \quad \pi_k\big((m_i)_{i \in I}\big) = m_k$$

ein R-Modulepimorphismus.
b) Für alle $k \in I$ ist die Einbettung

$$\iota_k : M_k \to \bigoplus_{i \in I} M_i, \quad \iota_k(m) = (m_i)_{i \in I} \quad \text{mit} \quad m_i = \begin{cases} m & \text{für } i = k, \\ 0 & \text{für } i \in I \setminus \{k\}. \end{cases}$$

ein R-Modulmonomorphismus (und daher $\iota_k(M_k)$ ein zu M_k isomorpher Untermodul von $\bigoplus_{i \in I} M_i$).

35) Es sei R ein faktorieller Ring und K sein Quotientenkörper. Beweisen Sie:
a) Ist $a \in R$, $p \in R[X]$ und gilt $a \mid C(p)$ (in R), so gilt $a \mid p(X)$ (in $R[X]$).
b) Sind $f, g \in R[X]$ mit f primitiv und gilt $f \mid g$ in $K[X]$, so gilt sogar $f \mid g$ in $R[X]$.

36) Beweisen Sie, dass $\mathbb{Z}[X]$ kein Hauptidealbereich ist. *Hinweis.* Betrachten Sie das Ideal $I := (2, X)$.

37) Es sei L/K eine Körpererweiterung. Beweisen Sie, dass $E_n := \{a \in L \mid a^n = 1\}$ für alle $n \in \mathbb{Z}$, $n \geq 1$ eine endliche zyklische Untergruppe von $(L^*, \cdot)$ ist.

38) Es sei p eine Primzahl, K ein Körper mit $\operatorname{char} K = p$ und $a, b \in K$. Beweisen Sie $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$ für alle $n \in \mathbb{Z}$, $n \geq 1$.

39) Es sei p eine Primzahl und K ein Körper mit $\operatorname{char} K = p$. Beweisen Sie:

a) Die Abbildung $\varphi : K \to K$, $\varphi(a) = a^p$ ist ein Monomorphismus.

b) Ist der Körper K endlich, so ist die Abbildung φ aus Teil a) ein Automorphismus.

Definition. Es sei p eine Primzahl und K ein endlicher Körper mit $\operatorname{char} K = p$. Die Abbildung $\varphi : K \to K$, $\varphi(a) = a^p$ wird Frobenius-Automorphismus genannt.

40) Es sei M ein Zwischenkörper der Körpererweiterung L/K.

a) Beweisen Sie: Ist $(x_i)_{i \in I}$ Basis von M als K-Vektorraum und $(y_j)_{j \in J}$ Basis von L als M-Vektorraum, so ist $(x_i y_j)_{(i,j) \in I \times J}$ Basis von L als K-Vektorraum.

b) Folgern Sie $[L : K] = [L : M] \cdot [M : K]$.

41) Es sei p eine Primzahl und L/K eine Körpererweiterung mit $[L : K] = p$. Beweisen Sie, dass $L = K(a)$ für alle $a \in L \setminus K$.

42) Beweisen Sie, dass $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine Basis von $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ als $\mathbb{Q}$-Vektorraum ist.

43) Gegeben sei die Körpererweiterung L/K und $a \in L$. Bestimmen Sie das Minimalpolynom $m_{a,K}$ von a über K.

a) $L = \mathbb{C}$, $K = \mathbb{R}$, $a = \sqrt{7}$,

b) $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \sqrt{7}$,

c) $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \big(1 + \sqrt{5}\big)/2$.

44) Es sei $a \in \mathbb{R}$ eine reelle Nullstelle des Polynoms $p(X) = X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$. Beweisen Sie, dass $1, a, a^2$ eine Basis von $\mathbb{Q}(a)$ als $\mathbb{Q}$-Vektorraum ist und drücken Sie die Zahlen a^4, a^5 und $3a^5 - a^4 + 2$ als Linearkombination dieser Basis aus.

45) Es seien p und q zwei verschiedene Primzahlen und $L = \mathbb{Q}(\sqrt{p}, \sqrt[3]{q})$. Beweisen Sie $L = \mathbb{Q}(\sqrt{p} \cdot \sqrt[3]{q})$ und $[L : \mathbb{Q}] = 6$.

46) Beweisen Sie, dass $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorräume, aber nicht als Körper isomorph sind.

47) Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Beweisen Sie: Ist $\operatorname{grad} m_{a,K}$ ungerade, so ist $K(a^2) = K(a)$. Bleibt diese Aussage auch richtig, wenn $\operatorname{grad} m_{a,K}$ gerade ist?

48) Es sei L/K eine algebraische Körpererweiterung und R ein Integritätsbereich, derart dass K Teilring von R und R Teilring von L ist (d.h. $K \subseteq R \subseteq L$). Beweisen Sie, dass R dann ein Körper ist. Was folgt daraus, wenn $[L : K]$ eine Primzahl ist?

49) Bestimmen Sie den Zerfällungskörper L des Polynoms $f \in \mathbb{Q}[X]$ und $[L : \mathbb{Q}]$ für

a) $f(X) = X^4 + 5X^2 + 6$,
b) $f(X) = X^4 - X^2 - 2$,
c) $f(X) = X^3 - 1$,
d) $f(X) = X^4 - 2X^2 + 9$,
e) $f(X) = X^p - 1$, wobei p eine Primzahl bezeichnen soll. *Hinweis.* Verwenden Sie Beispiel 44 der Wiederholungsbeispiele zum Thema Ringe.

50) Es sei K ein endlicher Körper. Zeigen Sie, dass K nicht algebraisch abgeschlossen ist.

51) a) Beweisen Sie, dass $\overline{\mathbb{Q}} := \{a \in \mathbb{C} \mid a \text{ ist algebraisch über } \mathbb{Q}\}$ ein algebraischer Abschluss von $\mathbb{Q}$ ist.
b) Beweisen Sie, dass $\mathbb{C}$ kein algebraischer Abschluss von $\mathbb{Q}$ ist.

52) Es sei L/K eine Körpererweiterung und $[L : K] = 2$. Beweisen Sie, dass L/K eine normale Körpererweiterung ist.

53) a) Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ beide normal sind, nicht aber die Körpererweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.
b) Es bezeichne $\zeta := e^{2\pi i/3}$. Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}(\sqrt[3]{2})$ beide normal sind, nicht aber die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

54) Es sei K ein endlicher Körper und $f \in K[X] \setminus K$. Beweisen Sie, dass f separabel ist.

55) Finden Sie ein primitives Element $\alpha \in K$, derart dass $K = \mathbb{Q}(\alpha)$ für

a) $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ b) $K = \mathbb{Q}(\sqrt{2}, i)$ c) $K = \mathbb{Q}(\sqrt{2}, i\sqrt{2})$

56) Beweisen Sie, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ eine Galoiserweiterung ist und bestimmen Sie die Galoisgruppe $G\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)$. Finden Sie alle Zwischenkörper der Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ und alle Untergruppen von $G\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)$ und beschreiben Sie die zwischen ihnen nach dem Hauptsatz der Galoistheorie bestehenden Beziehungen.