Universität Wien
Prof. Dr. D. Burde

Algebra I
— Aufgaben —

Aufgaben SS 2019

Aufgabe 1. Sei G eine Gruppe und $g, h \in G$. Man zeige, dass $(gh)^{-1} = h^{-1}g^{-1}$ gilt.

Aufgabe 2. Sei G eine Gruppe mit $g^2 = e$ für alle $g \in G$. Man zeige, dass G abelsch ist.

Aufgabe 3. Es sei p eine Primzahl. Man bestimme die Anzahl der Elemente der endlichen Gruppe $GL_n(\mathbb{Z}/p\mathbb{Z})$, indem man die Matrizen abzählt, deren Zeilen linear unabhängig über dem Körper $\mathbb{Z}/p\mathbb{Z}$ sind. Für $n = 3$ schreibe man die Anzahl explizit als Polynom in p.

Aufgabe 4. Sei p eine Primzahl. Man zeige, dass die Menge

$$\mathrm{Heis}(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

unter Matrizenmultiplikation eine nicht-abelsche Gruppe der Ordnung p^3 bildet. Sie heißt die *Heisenberggruppe* über $\mathbb{Z}/p\mathbb{Z}$.

Aufgabe 5. Man gebe eine endliche nicht-abelsche Gruppe G an, mit $g^3 = e$ für alle $g \in G$.

Aufgabe 6. Man bestimme das Zentrum der symmetrischen Gruppe S_3 anhand der Gruppentafel aus der Vorlesung.

Aufgabe 7 - extra. Sei G eine Gruppe und a, b Elemente in G, die $a^{-1}ba = b^{-1}$ und $b^{-1}ab = a^{-1}$ erfüllen. Man zeige, dass sie auch die Relationen $a^4 = b^4 = e$ erfüllen.

Aufgabe 8. Welche der folgenden Gruppen sind zyklisch?

$$C_2 \times C_2, C_2 \times C_3, GL_2(\mathbb{R}), D_{17}, F_2, (\mathbb{Q}, +).$$

Begründen Sie Ihre Antwort.

Aufgabe 9. Man zeige, dass die Abbildung $f\colon (\mathbb{R}^\times, \cdot) \to GL_2(\mathbb{R})$ mit

$$x \mapsto \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

ein Gruppenhomomorphismus ist, und bestimme $\ker(f)$.

Aufgabe 10. Sei G eine endliche Gruppe, in der jedes Element $g \neq e$ Ordnung 2 hat. Man zeige, dass

$$G \cong C_2 \times \cdots \times C_2$$

gilt.

Aufgabe 11. Es sei $G = GL_2(\mathbb{R})$ und

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Elemente aus G. Man bestime die Ordnung von A, B und AB.

Aufgabe 12. Man zeige, dass die Gruppe $(\mathbb{Q}, +)$ keine Untergruppe H besitzt mit $H \cong \mathbb{Z} \times \mathbb{Z}$.

Aufgabe 13. Man entscheide, ob die Gruppe $(\mathbb{R}, +)$ eine Untergruppe H besitzt mit $H \cong \mathbb{Z} \times \mathbb{Z}$, und begründe die Entscheidung.

Aufgabe 14 - extra. Sei G eine endliche nicht-triviale Gruppe. Beweisen oder widerlegen Sie folgende Aussage. Es gibt immer eine Untergruppe H in G vom Index $(G : H) = p$ mit einer Primzahl p.

Aufgabe 15. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ und $g \in G$ zeige man, dass

$$gG_xg^{-1} = G_{gx}$$

für die Stabilisatoren gilt.

Aufgabe 16. Man bestimme die Klassengleichung für die Gruppen D_4 und Q_8.

Aufgabe 17. Eine Gruppe G der Ordnung 55 operiere auf einer Menge X mit 18 Elementen. Man zeige, dass die Operation mindestens zwei Fixpunkte hat.

Aufgabe 18. Man zeige, dass es keine Gruppe G gibt mit $\mathrm{Aut}(G) \cong C_{2n+1}$ für ein $n \geq 1$.

Aufgabe 19. Sei G die Gruppe $GL_n(\mathbb{Z}/p\mathbb{Z})$ für eine Primzahl p. Eine Matrix heißt *unitriangulär*, wenn sie Dreiecksgestalt hat mit Diagonaleinträgen 1. Man zeige, dass die Untergruppe der oberen unitriangulären Matrizen in G eine p-Sylowgruppe von G ist.

Aufgabe 20. Man zeige mit Hilfe der Sylow-Sätze, dass es keine einfache Gruppe der Ordnung 250000 gibt.

Aufgabe 21 - extra. Man bestimme die Anzahl n_p der p-Sylowgruppen in der Gruppe $GL_2(\mathbb{Z}/p\mathbb{Z})$, für eine Primzahl p.

Aufgabe 22. Man zeige mit Hilfe der Sylow-Sätze, dass es keine einfache Gruppe der Ordnung 56 gibt.

Aufgabe 23. Sei p eine Primzahl und G eine nicht-abelsche Gruppe der Ordnung p^3. Man zeige, dass $|Z(G)| = p$ gilt.

Aufgabe 24. Man bestimme bis auf Isomorphie alle Gruppen, die ein semidirektes Produkt von C_p und C_p sind, für eine Primzahl p.

Aufgabe 25. Man zeige, dass die Diedergruppe D_n für $n \geq 3$ genau dann nilpotent ist, wenn $n = 2^m$ ist, mit $m \geq 2$.

Aufgabe 26. Man zeige, dass die Menge $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ein Unterring von $\mathbb{C}$ ist.

Aufgabe 27. Es seien I, und J zwei Ideal in einem Ring R. Man zeige, dass $I + J$, IJ und $I \cap J$ wieder Ideale in R sind, mit $IJ \subseteq I \cap J$.

Aufgabe 28 - extra. Sei $B_n(K)$ die Untergruppe von $GL_n(K)$, die aus allen invertierbaren oberen Dreiecksmatrizen in $GL_n(K)$ besteht. Man zeige, dass $B_n(K)$ für alle $n \geq 2$ auflösbar, aber nicht nilpotent ist.

Aufgabe 29. Man entscheide, ob für den Ring $\mathbb{Z}/18\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{17}\}$ die Teilmenge $S = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$ ein Unterring von $\mathbb{Z}/18\mathbb{Z}$ ist.

Aufgabe 30. Man zeige, dass die Einheitsgruppe des Ringes $\mathbb{Z}[i]$ durch

$$\mathbb{Z}[i]^{\times} = \{1, -1, i, -i\}$$

gegeben ist. Zu welcher Gruppe (aus unserer Liste der Gruppen der Ordnung $n \leq 8$) ist diese Gruppe isomorph?

Aufgabe 31. Sei R ein endlicher Ring mit 1. Man zeige, dass jedes Element ungleich Null in R entweder eine Einheit oder ein Nullteiler ist.

Aufgabe 32. Man zeige, dass jeder endliche Integritätsring ein Körper ist.

Aufgabe 33. Seien $f = X^7 - X^6 + 3X^5 + 4X^4 - 22X^3 - 10X^2 + 38X - 13$ und $g = X^2 - 1$ Polynome in $\mathbb{Z}[X]$. Man finde eindeutig bestimmte Polynome $g, r \in \mathbb{Z}[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$. Wie kann man den Rest r auch ohne Polynomdivision finden?

Aufgabe 34. Sei $m \in \mathbb{N}$. Man zeige direkt aus den Definitionen, dass ein Ideal $m\mathbb{Z}$ in $\mathbb{Z}$ genau dann prim ist, wenn $m = 0$ oder m prim ist. Man zeige, dass es genau dann maximal ist, wenn m eine Primzahl ist.

Aufgabe 35 - extra. Man zeige, dass der Ring $\mathbb{Z}[i]$ Norm-Euklidisch ist.

Aufgabe 36. Man bestimme alle Ideale des Ringes $\mathbb{Z}/15\mathbb{Z}$. Welche davon sind maximale Ideale?

Aufgabe 37. Man zeige, dass die Faktorringe $\mathbb{Z}[X]/(X^2 - 2)$ und $\mathbb{Z}[X]/(X^2 - 3)$ nicht isomorph sind.

Aufgabe 38. Sei f ein Polynom in $\mathbb{Q}[X]$ vom Grad 3 und $\alpha, \beta, \gamma \in \mathbb{C}$ die Nullstellen von f in $\mathbb{C}$. Man zeige, dass gilt

$$\begin{aligned} \alpha + \beta + \gamma &\in \mathbb{Q}, \\ \alpha^2 + \beta^2 + \gamma^2 &\in \mathbb{Q}. \end{aligned}$$

Aufgabe 39. Man zeige, dass der Ring $\mathbb{Z}[i]$ faktoriell ist und bestimme die Primfaktorzerlegung der Elemente $2, 3, 5$ in $\mathbb{Z}[i]$.

Aufgabe 40. Man bestimme die Einheiten des Ringes $\mathbb{Z}[\sqrt{-n}]$ für quadratfreies $n \geq 2$. Man zeige, dass $\mathbb{Z}[\sqrt{3}]$ unendlich viele Einheiten besitzt.

Aufgabe 41. Sei $I \neq 0$ ein Ideal in $\mathbb{Z}[i]$. Man zeige, dass der Quotientenring $\mathbb{Z}[i]/I$ endlich ist.

Aufgabe 42 - extra. Sei R ein Hauptidealring und S eine multiplikativ abgeschlossene Teilmenge von R mit $0 \notin S$. Man zeige, dass der Ring der Brüche $S^{-1}R$ ein Hauptidealring ist.

Aufgabe 43. Man entscheide (mit Beweis) für jeden der Polynomringe $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ und $\mathbb{R}[X]$, ob das Polynom $X^4 + 1$ irreduzibel ist, oder nicht.

Aufgabe 44. Man verwende das Reduktionskriterium um zu zeigen, dass $X^5 + 5X^2 + 1 \in \mathbb{Z}[X]$ irreduzibel ist.

Aufgabe 45. Man zeige, dass das Polynom $X^4 - 2$ irreduzibel ist in $(\mathbb{Z}[i])[X]$.

Aufgabe 46. Man bestimme alle irreduziblen Polynome $f \in \mathbb{F}_2[X]$ vom Grad $n = 1, 2, 3, 4$.

Aufgabe 47. Man zerlege das Polynom $X^4 + 1$ in irreduzible Faktoren über $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ und $\mathbb{F}_7$.

Aufgabe 48. Man bestimme alle natürlichen Zahlen $n \in \mathbb{N}$, für die das Polynom $X^4 + nX^3 + X^2 + X + 1$ in $\mathbb{Q}[X]$ reduzibel ist.

Aufgabe 49 - extra. Man bestimme das Minimalpolynom von

$$\alpha = \sqrt[3]{2} + \sqrt[3]{3} + \sqrt[3]{5}$$

über $\mathbb{Q}$.

Aufgabe 50. Sei $\mathbb{F}$ ein endlicher Körper und $z \in \mathbb{F}$ ein beliebiges Element. Man zeige, dass es $x, y \in \mathbb{F}$ gibt mit $z = x^2 + y^2$.

Aufgabe 51. Es sei $L \mid K$ eine Körpererweiterung und $f = \sum_{i=0}^{n} a_i X^i \in L[X]$ ein Polynom, deren Koeffizienten algebraisch über K sind. Man zeige, dass die Nullstellen von f in L ebenfalls algebraisch über K sind.

Aufgabe 52. Man zeige, dass mindestens eine der Zahlen $e + \pi$, $e\pi$ transzendent ist. Es darf verwendet werden, dass e und π transzendent sind.

Aufgabe 53. Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n \geq 1$. Man zeige, dass es eine Körpererweiterung $L \mid K$ gibt mit $[L : K] \leq n!$, so dass f über L in Linearfaktoren zerfällt.

Aufgabe 54. Man bestimme einen Zerfällungskörper L des Polynoms $X^6 - 8$ über $\mathbb{Q}$ und berechne den Körpergrad $[L : \mathbb{Q}]$.

Aufgabe 55. Seien d_1, d_2 zwei ganze Zahlen. Man zeige, dass die Körper $\mathbb{Q}(\sqrt{d_1})$ und $\mathbb{Q}(\sqrt{d_2})$ isomorphe algebraische Abschlüsse haben.

Aufgabe 56 - extra. Man bestimme einen Zerfällungskörper L des Polynoms X^3+X+1 über dem Körper $\mathbb{F}_2$ und berechne den Körpergrad $[L : \mathbb{F}_2]$.

Aufgabe 57. Man zeige, dass $\mathbb{F}_2[X]/(X^2 + X + 1)$ ein Körper mit 4 Elementen ist und gebe explizite Tabellen für die Addition und Multiplikation an.

Aufgabe 58. Es seien K und L Unterkörper von $\mathbb{F}_{p^n}$ mit $|K| = p^a$ und $|L| = p^b$. Man bestimme $|K \cap L|$ für den Unterkörper $K \cap L$ in $\mathbb{F}_{p^n}$.

Aufgabe 59. Man entscheide, ob die Erweiterung $\mathbb{Q}\left(\sqrt{1-\sqrt{2}}\right) \mid \mathbb{Q}$ normal ist oder nicht und begründe dies.

Aufgabe 60. Man entscheide, ob die Gleichheit

$$\mathbb{Q}\left(\sqrt{1-\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{-1}, \sqrt{2}\right)$$

gilt und begründe dies.

Aufgabe 61. Man zeige, dass die Körpererweiterung

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \dots, \sqrt{p}, \dots) \mid \mathbb{Q},$$

wobei die Wurzeln aller Primzahlen p adjungiert werden, algebraisch ist. Ist sie auch normal?

Aufgabe 62. Sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$ und ζ_n eine primitive n-te Einheitswurzel. Sei $L = \mathbb{Q}(\zeta_n, \sqrt[n]{a})$. Man zeige, dass die Körpererweiterung $L \mid \mathbb{Q}$ normal ist. Für $n = 6$ und $a = 2$ berechne man den Grad $[L : \mathbb{Q}]$.

Aufgabe 63 - extra. Sei $n \in \mathbb{N}$ und L der Zerfällungskörper des Polynoms $X^n - 2$ über $\mathbb{Q}$. Man zeige, dass gilt

$$[L : \mathbb{Q}] = \begin{cases} n\varphi(n) & \text{falls } 8 \nmid n, \\ \frac{n\varphi(n)}{2} & \text{falls } 8 \mid n \end{cases}$$

Aufgabe 64. Sei K ein Körper der Charakteristik $p > 0$, $a \in K$ und α eine Nullstelle des Polynoms $X^p - a \in K[X]$. Man bestimme die Automorphismengruppe $\mathrm{Aut}(K(\alpha) \mid K)$.

Aufgabe 65. Sei K ein Körper der Charakteristik $p > 0$. Man zeige, dass das Polynom $X^5 - X^2 + 1$ separabel ist für $p = 5$, aber inseparabel für $p = 7$.

Aufgabe 66. Sei $L \mid K$ eine Körpererweiterung vom Grad 2 und $\mathrm{char}(K) \neq 2$. Man zeige, dass es ein $\alpha \in L \setminus K$ gibt mit $\alpha^2 \in K$ und $L = K(\alpha)$. Man gebe ein Gegenbeispiel für diese Aussage mit $K = \mathbb{F}_2$.

Aufgabe 67. Es seien $K = \mathbb{Q}$ und

$$L = K\left(\sqrt{2}, e^{\frac{2\pi i}{2019}}, \sqrt{3 + \sqrt[4]{12}}\right).$$

Man zeige, dass es ein primitives Element $\alpha \in L$ gibt mit $L = K(\alpha)$.

Aufgabe 68. Man bestimme ein primitives Element für die Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \mid \mathbb{Q}$, d.h., ein $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$ mit $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha)$.

Aufgabe 69. Sei $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Man bestimme die Galoisgrupe der Erweiterung $L \mid \mathbb{Q}$.

Aufgabe 70 - extra. Man zeige ohne Galoistheorie, dass folgende Gleichheit gilt,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}).$$

Aufgabe 71. Man bestimme die Galoisgruppe des Polynoms $X^4 - 2$ über $\mathbb{Q}$.

Aufgabe 72. Man zeige mit Galoistheorie, dass es keine primitive n-te Einheitswurzel ζ_n in $\mathbb{C}$ gibt mit $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\zeta_n)$.

Aufgabe 73. Sei p eine Primzahl mit $p \equiv 1 \bmod 3$ und ζ_p eine primitive p-te Einheitswurzel in $\mathbb{C}$. Man zeige, dass die Erweiterung $\mathbb{Q}(\zeta_p) \mid \mathbb{Q}$ einen eindeutigen Zwischenkörper L enthält mit $[L : \mathbb{Q}] = 3$.

Aufgabe 74. Es sei ζ_8 eine primitive 8-te Einheitswurzel und $L = \mathbb{Q}(\zeta_8)$. Man bestimme die Galoisgruppe der Erweiterung $L \mid \mathbb{Q}$ und alle ihre Untergruppen, sowie die zugehörigen Fixkörper.

Aufgabe 75. Seien $m, n \in \mathbb{N}$ teilerfremd, ζ_m eine primitive m-te Einheitswurzel und ζ_n eine primitive n-te Einheitswurzel in $\mathbb{C}$. Man zeige, dass $\mathbb{Q} = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$ und

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n), \mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m), \mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$$

gilt.

Aufgabe 76. Man bestimme die Galoisgruppe des Polynoms $X^6 + X^4 + X^2 + 1$ über $\mathbb{Q}$ und über $\mathbb{F}_5$.

Aufgabe 77 - extra. Man finde eine Galoiserweiterung $L \mid \mathbb{Q}$ vom Grad 8 mit $\mathrm{Gal}(L, \mathbb{Q}) \cong Q_8$, der Quaternionengruppe.

Aufgabe 78. Man zeige, dass die Galoisgruppe des Polynoms $X^5 - 3$ auflösbar ist.

Aufgabe 79. Man zeige, dass die Gleichung

$$X^5 - 5X^4 + 10X^3 + 50X^2 - 5 = 0$$

über $\mathbb{Q}$ nicht durch Radikale auflösbar ist.

Aufgabe 80. Sei $p \geq 5$ eine Primzahl. Man zeige, dass es eine ganze Zahl $m \geq 1$ gibt, so dass die Galoisgruppe von

$$X^p + mp^2(X-1)(X-2)\cdots(X-p+2) - p$$

über $\mathbb{Q}$ isomorph zu S_p ist.

Aufgabe 81. Sei $L \mid K$ eine Galoiserweiterung mit $G = \mathrm{Gal}(L, K)$. Für $\alpha \in L$ definieren man die *Norm* von α durch

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Man zeige, dass $N(\alpha) \in K$ gilt und $N(\alpha\beta) = N(\alpha)N(\beta)$ für alle $\alpha, \beta \in L$.

Aufgabe 82. Sei $L \mid K$ eine quadratische Körpererweiterung mit $G = \mathrm{Gal}(L, K) = \{\mathrm{id}, \sigma\}$ und $\alpha \in L$. Man zeige, dass $N(\alpha) = 1$ genau dann gilt, wenn es ein $\beta \in L$ gibt mit $\alpha = \frac{\beta}{\sigma(\beta)}$.

Aufgabe 83. Das reguläre n-Eck ist genau dann konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist. Man zeige, dass dies genau dann der Fall ist, wenn n ein Produkt einer Zweierpotenz und von verschiedenen Fermat Primzahlen (also von der Form $2^{2^m} + 1$) ist.

Aufgabe 84 - extra. Sei $p > 2$ ein Primzahl und

$$f = X^p + pX^{p-1} + p.$$

Man zeige, dass f irreduzibel über $\mathbb{Q}$ ist und genau eine reelle Nullstelle hat. Man bestimme die Galoisgruppe von f über $\mathbb{Q}$.

Ende: 31.01.2020