Universität Wien
Dietrich Burde

Algebra I
— Aufgaben —

Aufgaben WS 2023/24

Aufgabe 1. Sei G eine Gruppe und $g, h \in G$. Man zeige, dass $(gh)^{-1} = h^{-1}g^{-1}$ gilt, und folgere $(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}$ für alle $g_1, \ldots, g_n \in G$, mit $n \geq 2$.

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

Aufgabe 3. Für eine Gruppe G ist die Ordnung eines Elements $g \in G$ definiert als die kleinste positive Zahl $k \geq 1$ mit $g^k = e$. Man liste alle Elemente der Gruppe $GL_2(\mathbb{Z}/2\mathbb{Z})$ auf und bestimme die Ordnungen aller Elemente.

Aufgabe 4. Man bestimme die Ordnung aller Elemente von S_3, und von $\mathbb{Z}/6\mathbb{Z}$.

Aufgabe 5. 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 vom Grad 9 in p.

Aufgabe 6. Man stelle die Gruppentafel für die Diedergruppe $D_3 = \{e, r, r^2, s, rs, r^2s\}$ auf, indem man das Produkt von je zwei Elementen berechnet.

$\square$

Aufgabe 7. Welche der folgenden Gruppen sind zyklisch?

$$C_2 \times C_2, C_2 \times C_3, GL_2(\mathbb{R}), D_{17}, S_5, (\mathbb{Q}, +).$$

Begründen Sie Ihre Antwort.

Aufgabe 8. 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 9. Man gebe eine endliche nicht-abelsche Gruppe G an, mit $g^3 = e$ für alle $g \in G$.

Aufgabe 10. Man bestimme das Zentrum der symmetrischen Gruppe S_3 anhand der Gruppentafel aus der Vorlesung.

Aufgabe 11. Man zeige, dass der Schnitt beliebig vieler Untergruppen einer Gruppe G wieder eine Untergruppe von G ist.

Aufgabe 12. Seien A und B Untergruppen einer Gruppe G. Man zeige, dass $A \cup B$ eine Untergruppe von G ist, genau dann, wenn $A \subseteq B$ oder $B \subseteq A$ gilt.

$\square$

Aufgabe 13. Man zeige, dass die Gruppe S_n für $n \geq 2$ von den Transpositionen erzeugt wird.

Aufgabe 14. Man bestimme eine normale Untergruppe von S_3 der Ordnung 3 und eine nicht-normale Untergruppe von S_3 der Ordnung 2.

Aufgabe 15. Man bestimme für jeden Teiler d von 24 eine Untergruppe H_d von S_4 der Ordnung d.

Aufgabe 16. 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 17. Bestimme alle Gruppenhomomorphismen $f\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$.

Aufgabe 18. 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 $\ker(f)$.

$\square$

Aufgabe 19. 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 20. 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 21. Man zeige, dass die Gruppe $(\mathbb{Q}, +)$ keine Untergruppe H besitzt mit $H \cong \mathbb{Z} \times \mathbb{Z}$.

Aufgabe 22. Man entscheide, ob die Gruppe $(\mathbb{R}, +)$ eine Untergruppe H besitzt mit $H \cong \mathbb{Z} \times \mathbb{Z}$, und begründe die Entscheidung.

Aufgabe 23. Sei $\mathbb{C}^\times$ die multiplikative Gruppe der von Null verschiedenen komplexen Zahlen, und μ_n die Untergruppe der n-ten Einheitswurzeln. Man zeige, dass

$$\mathbb{C}^\times / \mu_n \cong \mathbb{C}^\times.$$

Aufgabe 24. Man zeige, dass alle Untergruppen der Quaternionengruppe Q_8 normal sind und bestimme die möglichen Quotientengruppen bis auf Isomorphie.

$\square$

Aufgabe 25. Sei G eine endliche Gruppe, so dass jede Untergruppe von G normal ist. Man zeige, dass je zwei Elemente teilerfremder Ordnung kommutieren.

Aufgabe 26 - 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 27. 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 28. Man bestimme die Klassengleichung für die Gruppen D_4 und Q_8.

Aufgabe 29. Eine Gruppe G der Ordnung 55 operiere auf einer Menge X mit 18 Elementen. Man zeige, dass die Operation mindestens zwei Fixpunkte hat.

Aufgabe 30. Man zeige, dass es keine Gruppe G gibt mit $\mathrm{Aut}(G) \cong C_{2n+1}$ für ein $n \geq 1$.

$\square$

Aufgabe 31. 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 32. Man zeige mit Hilfe der Sylow-Sätze, dass es keine einfache Gruppe der Ordnung 250000 gibt.

Aufgabe 33 - 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 34. Man zeige mit Hilfe der Sylow-Sätze, dass es keine einfache Gruppe der Ordnung 56 gibt.

Aufgabe 35. Sei p eine Primzahl und G eine nicht-abelsche Gruppe der Ordnung p^3. Man zeige, dass $|Z(G)| = p$ gilt.

Aufgabe 36. Man bestimme bis auf Isomorphie alle Gruppen, die ein semidirektes Produkt von C_p und C_p sind, für eine Primzahl p.

$\square$

Aufgabe 37. Man zeige, dass die Quaternionengruppe Q_8 nicht als semidirektes Produkt zweier nicht-trivialer Untergruppen geschrieben werden kann.

Aufgabe 38. 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 39. 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 ist.

Aufgabe 40. Man zeige, dass jede Gruppe der Ordnung 20159 auflösbar ist und finde eine Gruppe der Ordnung 20160, die nicht auflösbar ist.

$\square$

Aufgabe 41. Man zeige, dass die Gruppe $SL_2(\mathbb{R})$ von Matrizen der Form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$$

mit $x, y \in \mathbb{R}$ erzeugt wird.

Aufgabe 42. Man zeige mit Aufgabe 41, dass die Kommutatoruntergruppe von $SL_2(\mathbb{R})$ gleich $SL_2(\mathbb{R})$ ist und folgere, dass $SL_2(\mathbb{R})$ nicht auflösbar ist.

Aufgabe 43. Sei G eine endliche Gruppe und N ein Normalteiler von G, so dass N und G/N nilpotent sind. Man entscheide, ob dann auch G nilpotent sein muss und begründe dies.

Aufgabe 44. Man zeige, dass die Menge $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ein Unterring von $\mathbb{C}$ ist.

Aufgabe 45. Man zeige, dass die Unterringe $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{2}]$ von $\mathbb{C}$ nicht isomorph sind.

Aufgabe 46. 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 47. Sei R ein kommutativer Ring, und I, J zwei Ideale in R mit $I + J = R$. Man zeige, dass $IJ = I \cap J$ gilt. Ohne die Voraussetzung $I + J = R$ muss die Gleichheit nicht gelten. Man gebe einen kommutativen Ring R und zwei Ideale I, J an, mit $IJ \neq I \cap J$.

Aufgabe 48. Sei R ein Ring und I ein Ideal in R. Man zeige, dass der Quotientenring R/I genau dann kommutativ ist, wenn $xy - yx \in I$ gilt für alle $x, y \in R$.

$\square$

Aufgabe 49. Sei R der Ring der Matrizen

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{C} \right\}.$$

Man bestimme ein Ideal I in R, so dass der Quotientenring R/I kommutativ ist.

Aufgabe 50. 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 51. 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 52. Sei R ein Integritätsring mit Einselement 1 und Nullelement 0. Angenommen, die Einheitengruppe $U(R)$ ist endlich. Man zeige, dass

$$\prod_{u \in U(R)} u = -1$$

gilt. Welchen Wert hat das Produkt für den Ring $R = \mathbb{Z}/12\mathbb{Z}$, der kein Integritätsring ist?

Aufgabe 53. Man folgere aus Aufgabe 52 das Theorem von Wilson, nämlich das gilt

$$(p-1)! \equiv -1 \bmod p$$

für alle Primzahlen p. Umgekehrt zeige man, dass für $n \geq 1$ aus der Kongruenz $(n-1)! \equiv -1 \bmod n$ folgt, dass n eine Primzahl ist.

Aufgabe 54. Sei R ein endlicher Ring mit 1. Man zeige, dass jedes Element ungleich Null in R entweder eine Einheit oder ein Nullteiler ist.

Lösung: Sei a ein Element in R ungleich Null. Da R endlich ist, sind die Potenzen von a nicht alle verschieden. Es gibt also $0 \leq m < n$ mit $a^m = a^n$. Wir dürfen annehmen, dass n minimal mit dieser Eigenschaft ist. Offenbar ist $n - 1 \geq 0$.

$\square$

Aufgabe 55. Man zeige, dass jeder endliche Integritätsring ein Körper ist.

Aufgabe 56. 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 57. 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 58 - extra. Man zeige, dass der Ring $\mathbb{Z}[i]$ Norm-Euklidisch ist.

Aufgabe 59. Man bestimme alle Ideale des Ringes $\mathbb{Z}/15\mathbb{Z}$. Welche davon sind maximale Ideale?

Aufgabe 60. Man zeige, dass die Faktorringe $\mathbb{Z}[X]/(X^2 - 2)$ und $\mathbb{Z}[X]/(X^2 - 3)$ nicht isomorph sind.

$\square$

Aufgabe 61. 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

$$\alpha + \beta + \gamma \in \mathbb{Q},$$
$$\alpha^2 + \beta^2 + \gamma^2 \in \mathbb{Q}.$$

Aufgabe 62. Man zeige, dass der Ring $\mathbb{Z}[i]$ faktoriell ist und bestimme die Primfaktorzerlegung der Elemente $2, 3, 5$ in $\mathbb{Z}[i]$.

Aufgabe 63. 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 64. Sei $I \neq 0$ ein Ideal in $\mathbb{Z}[i]$. Man zeige, dass der Quotientenring $\mathbb{Z}[i]/I$ endlich ist.

Aufgabe 65. 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 66. Sei R ein Integritätsbereich und Q sein Quotientenkörper. Man zeige, dass $|R| = |Q|$ gilt.

$\square$

Aufgabe 67. Sei $R = \mathbb{Z}[X]$. Man bestimme ein Primideal in R, dass nicht maximal ist, und finde ein maximales Ideal in R.

Aufgabe 68. Es sei $R[X]$ ein faktorieller Ring. Man zeige, dass auch R faktoriell ist. Also gilt die Umkehrung des Satzes von Gauß.

Aufgabe 69. 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 70. Man verwende das Reduktionskriterium um zu zeigen, dass $X^5 + 5X^2 + 1 \in \mathbb{Z}[X]$ irreduzibel ist.

Aufgabe 71. Man zeige, dass das Polynom $X^4 - 2$ irreduzibel ist in $(\mathbb{Z}[i])[X]$.

Aufgabe 72. Man bestimme alle irreduziblen Polynome $f \in \mathbb{F}_2[X]$ vom Grad $n = 1, 2, 3, 4$.

$\square$

Aufgabe 73. Man zeige mit Eisenstein (nach Substitution $X \to X + c$ für ein geeignetes c), dass das Polynom

$$X^5 + 10X^4 + 15X^3 + 15X^2 - 10X + 1$$

irreduzibel über $\mathbb{Q}$ ist.

Aufgabe 74. 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 75. 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 76. Man bestimme alle ganzzahligen Lösungen des Systems von Kongruenzen, das durch

$$x \equiv 2 \bmod 5,\ x \equiv 3 \bmod 7,\ x \equiv 10 \bmod 11$$

gegeben ist.

Aufgabe 77. Sei $n \in \mathbb{N}$ und $\varphi(n)$ die Eulersche φ-function. Man beweise die Formel

$$\sum_{d|n} \varphi(d) = n,$$

wobei die Summe über alle positiven Teiler d von n läuft.

Aufgabe 78. Man zeige, dass es kein $n \in \mathbb{N}$ gibt mit $\varphi(n) = 14$.

$\square$

Aufgabe 79. Man bestimme alle Primitivwurzeln modulo 11.

Aufgabe 80. Sei $p > 3$ eine Primzahl. Man beweise, dass -3 genau dann ein QR modulo p ist, wenn $p \equiv 1 \bmod 6$ gilt.

Aufgabe 81. Sei $F_n = 2^{2^n} + 1$ die n-te Fermat-Zahl. Angenommen, F_n ist eine Primzahl. Man zeige, dass

$$3^{\frac{F_n - 1}{2}} \equiv -1 \bmod F_n$$

gilt.

Aufgabe 82. Sei $p > 2$ eine Primzahl. Man zeige, dass

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right) = -1$$

gilt.

Aufgabe 83. Sei p eine ungerade Primzahl. Man zeige, dass

$$\left(\frac{5}{p}\right) = 1 \Longleftrightarrow p \equiv 1, 9, 11, 19 \bmod 20$$

gilt.

Aufgabe 84. Man schreibe $1+3i \in \mathbb{Z}[i]$ als Produkt von Primelementen in $\mathbb{Z}[i]$.

$\square$

Abgabe: 30.01.2024