Übungen zu Algebra 2, WS 2020/21

Christoph Baxa

Definition: Es sei $(M, \cdot)$ ein Monoid mit neutralem Element e und $a \in M$. Ein $x \in M$ heißt linksinverses (bzw. rechtsinverses) Element zu a wenn $x \cdot a = e$ (bzw. $a \cdot x = e$).

Das folgende Lemma wurde in der Vorlesung Algebra 1 (wenn man genau hinsieht) eigentlich schon in Satz 3 bewiesen, dort aber nicht so formuliert:

Lemma: Es sei $(M, \cdot)$ ein Monoid mit neutralem Element e und $x, y \in M$ ein links- bzw. rechtsinverses Element zu $a \in M$ (d.h. $x \cdot a = a \cdot y = e$). Dann gilt $x = y$.

Beweis: $x = x \cdot e = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$

66) Es sei V der (reelle) Vektorraum der reellen Folgen $(a_n)_{n\geq 1}$ (mit den Verknüpfungen $(a_n)_{n\geq 1} + (b_n)_{n\geq 1} := (a_n + b_n)_{n\geq 1}$ und $\alpha \cdot (a_n)_{n\geq 1} := (\alpha a_n)_{n\geq 1}$) und R der Endomorphismenring von V. Es bezeichnen $\varphi : V \to V$ und $\psi : V \to V$ die Abbildungen

$$\varphi(a_1, a_2, a_3, \dots) = (0, a_1, a_2, \dots) \quad \text{und} \quad \psi(a_1, a_2, a_3, \dots) = (a_2, a_3, a_4, \dots).$$

Beweisen Sie die folgenden Aussagen:

a) φ und ψ sind Elemente von R (d.h. $\mathbb{R}$-lineare Abbildungen),
b) φ besitzt in R ein linksinverses, aber kein rechtsinverses Element,
c) ψ besitzt in R ein rechtsinverses, aber kein linksinverses Element.

67) Beweisen Sie (mit den Bezeichnungen des vorangegangenen Beispiels):

a) φ ist ein Rechtsnullteiler aber kein Linksnullteiler in R,
b) ψ ist ein Linksnullteiler aber kein Rechtsnullteiler in R.

Sind die links- bzw. rechtsinversen Elemente (in R) eindeutig bestimmt?

68) a) Es sei p eine Primzahl. Beweisen Sie, ohne die Resultate von Kapitel 11 zu verwenden, dass $\{a/p^n \mid a, n \in \mathbb{Z}, n \geq 0\}$ ein Unterring von $(\mathbb{Q}, +, \cdot)$ ist. Ist es auch ein Ideal?
b) Es sei p eine Primzahl. Beweisen Sie, ohne die Resultate von Kapitel 11 zu verwenden, dass $\{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$ ein Unterring von $(\mathbb{Q}, +, \cdot)$ ist. Ist es auch ein Ideal?

69) Es seien $R_1, \dots, R_n$ Ringe. Die Addition und Multiplikation auf $R_1 \times \cdots \times R_n$ seien wie in Bsp. 65 definiert. Beweisen Sie:

a) Ist S_i ein Unterring von R_i für $1 \leq i \leq n$, so ist $S_1 \times \cdots \times S_n$ ein Unterring von $R_1 \times \cdots \times R_n$.
b) Ist I_i ein Ideal von R_i für $1 \leq i \leq n$, so ist $I_1 \times \cdots \times I_n$ ein Ideal von $R_1 \times \cdots \times R_n$.

Definition: Das Zentrum $Z(R)$ eines Rings R ist definiert als

$$Z(R) := \{a \in R \mid ax = xa \text{ für alle } x \in R\}.$$

70) a) Es sei R ein Ring. Beweisen Sie, dass $Z(R)$ ein Unterring von R ist.
b) Es seien $R_1, \dots, R_n$ Ringe. Beweisen Sie, dass $Z(R_1 \times \cdots \times R_n) = Z(R_1) \times \cdots \times Z(R_n)$.

71) Es sei K ein Körper. Beweisen Sie:

a) $Z\big(M_2(K)\big) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, a \in K \right\}$,

b) $Z\big(M_2(K)\big)$ ist weder Linksideal noch Rechtsideal von $M_2(K)$.

Definition. Es sei R ein Ring. Ein Element $a \in R$ heißt nilpotent, wenn es ein $n \in \mathbb{N} \setminus \{0\}$ mit der Eigenschaft $a^n = 0$ gibt. Die Menge aller nilpotenter Elemente des Rings R bezeichnen wir mit $\mathrm{Nil}(R)$.

72) Es sei $R \neq \{0\}$ ein kommutativer Ring mit 1. Beweisen Sie:

a) Ist $a \in \mathrm{Nil}(R)$, so ist a ein Nullteiler,

b) Wenn $a, b \in \mathrm{Nil}(R)$, so ist $a + b \in \mathrm{Nil}(R)$,

c) $\mathrm{Nil}(R)$ ist ein Ideal von R,

d) Ist $u \in R^*$ und $a \in \mathrm{Nil}(R)$, so ist $u + a \in R^*$ (*Hinweis.* Geometrische Reihe).

73) Es sei K ein Körper und $1 \leq k \leq n$.

a) Es sei $I_k := \{(a_{ij})_{1 \leq i,j \leq n} \in M_n(K) \mid a_{ij} = 0 \text{ für } j \neq k\}$, d.h. die Menge aller $n \times n$-Matrizen mit Eintragungen aus K, bei denen höchstens in der k-ten Spalte Eintragungen $\neq 0$ stehen. Beweisen Sie, dass I_k ein Linksideal (aber für $n \geq 2$ kein Rechtsideal) von $M_n(K)$ ist.

b) Es sei $J_k := \{(a_{ij})_{1 \leq i,j \leq n} \in M_n(K) \mid a_{ij} = 0 \text{ für } i \neq k\}$, d.h. die Menge aller $n \times n$-Matrizen mit Eintragungen aus K, bei denen höchstens in der k-ten Zeile Eintragungen $\neq 0$ stehen. Beweisen Sie, dass J_k ein Rechtsideal (aber für $n \geq 2$ kein Linksideal) von $M_n(K)$ ist.

74) Es sei K ein Körper. Beweisen Sie, dass $M_n(K)$ nur die Ideale $\{0\}$ und $M_n(K)$ besitzt. (*Hinweis.* Es bezeichne E_{ij} jene Matrix in $M_n(K)$, die in der i-ten Zeile und j-ten Spalte die Eintragung 1 besitzt und sonst immer nur 0 als Eintragung. Ist $I \neq \{0\}$ ein Ideal von $M_n(K)$, so gibt es $A = (a_{ij})_{1 \leq i,j \leq n} \in I \setminus \{0\}$. Daher gibt es $k, \ell \in \{1, \dots, n\}$ mit der Eigenschaft $a_{k\ell} \neq 0$. Zeigen Sie für $1 \leq t \leq n$, dass $E_{tk} \cdot A \cdot E_{\ell t} = a_{k\ell} E_{tt}$. Folgern Sie daraus $a_{k\ell} E_{tt} \in I$, $a_{k\ell} E_{tt} \cdot a_{k\ell}^{-1} E_{tt} = E_{tt} \in I$ und $I_n = E_{11} + \cdots + E_{nn} \in I$.) Warum folgt aus diesem Beispiel und Satz 60 (ii) für $n \geq 2$ nicht, dass $M_n(K)$ ein Schiefkörper ist?

75) Es sei R ein Ring und $X \subseteq R$. Beweisen Sie

$$(X) = \left\{ \sum_{i=1}^{I} \alpha_i x_i \beta_i + \sum_{j=1}^{J} \gamma_j y_j + \sum_{k=1}^{K} u_k \delta_k + \sum_{\ell=1}^{L} n_\ell v_\ell \;\middle|\; \begin{array}{l} \alpha_i, \beta_i \in R \text{ und } x_i \in X \text{ für } 1 \leq i \leq I, \\ \gamma_j \in R \text{ und } y_j \in X \text{ für } 1 \leq j \leq J, \\ \delta_k \in R \text{ und } u_k \in X \text{ für } 1 \leq k \leq K, \\ n_\ell \in \mathbb{Z} \text{ und } v_\ell \in X \text{ für } 1 \leq \ell \leq L \end{array} \right\}.$$

76) a) Es sei R ein kommutativer Ring und $X \subseteq R$. Beweisen Sie

$$(X) = \left\{ \sum_{i=1}^{I} \alpha_i x_i + \sum_{j=1}^{J} n_j y_j \;\middle|\; \begin{array}{l} \alpha_i \in R \text{ und } x_i \in X \text{ für } 1 \leq i \leq I, \\ n_j \in \mathbb{Z} \text{ und } y_j \in X \text{ für } 1 \leq j \leq J \end{array} \right\}.$$

b) Es sei R ein Ring mit Eins und $X \subseteq R$. Beweisen Sie

$$(X) = \left\{ \sum_{i=1}^{n} \alpha_i x_i \beta_i \;\middle|\; \alpha_i, \beta_i \in R \text{ und } x_i \in X \text{ für } 1 \leq i \leq n \right\}.$$

c) Es sei R ein kommutativer Ring mit Eins und $X \subseteq R$. Beweisen Sie

$$(X) = \left\{ \sum_{i=1}^{n} \alpha_i x_i \;\middle|\; \alpha_i \in R \text{ und } x_i \in X \text{ für } 1 \leq i \leq n \right\}.$$

Definition: Es sei R ein Ring und I und J Ideale von R. Das Produkt $I \cdot J$ der Ideale I und J ist definiert als

$$I \cdot J := \{x_1 y_1 + \cdots + x_n y_n \mid n \geq 0, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}.$$

77) Es sei R ein Ring und I und J Ideale von R. Beweisen Sie:

a) $I \cdot J$ ist ein Ideal von R,

b) $I \cdot J$ ist das von der Menge $\{xy \mid x \in I, y \in J\}$ erzeugte Ideal von R,

c) Ist R ein kommutativer Ring mit Eins und sind $a, b \in R$, so gilt $(a) \cdot (b) = (ab)$.

78) Beweisen Sie, dass die folgenden Abbildungen Ringisomorphismen sind:

a) $\varphi : \mathbb{C} \to \mathbb{C}$, $\varphi(z) = \overline{z}$,

b) $\varphi : \mathbb{C} \to \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$, $\varphi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ (mit $a, b \in \mathbb{R}$),

c) Es sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei und $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ sowie $\varphi : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$, $\varphi(a + b\sqrt{d}) = a - b\sqrt{d}$ (wobei $a, b \in \mathbb{Z}$).

79) Beweisen Sie, dass $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ und $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ als abelsche Gruppen aber nicht als Ringe isomorph sind. D.h. die beiden abelschen Gruppen $\big(\mathbb{Z}[i], +\big)$ und $\big(\mathbb{Z}[\sqrt{2}], +\big)$ sind isomorph, nicht aber die beiden Ringe $\big(\mathbb{Z}[i], +, \cdot\big)$ und $\big(\mathbb{Z}[\sqrt{2}], +, \cdot\big)$

80) Es sei p eine Primzahl. Beweisen Sie, ausgehend von der Definition des Primideals, dass

$$P = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \mid a, p \nmid b \right\}$$

ein Primideal des Rings

$$R = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \nmid b \right\}$$

(aus Bsp. 68b) ist.

81) Es sei $R\big(\neq \{0\}\big)$ ein kommutativer Ring mit Eins und $P(\neq R)$ ein Ideal von R. Beweisen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(i) P ist ein Primideal,
(ii) Sind I, J Ideale und $I \cdot J \subseteq P$, so ist $I \subseteq P$ oder $J \subseteq P$.

Bemerkungen: 1) Eigenschaft (ii) aus Bsp. 81 wird benützt, um den Begriff des Primideals in beliebigen Ringen (die nicht kommutativ zu sein brauchen) zu definieren.
2) Ist $R\big(\neq \{0\}\big)$ ein kommutativer Ring mit Eins und P ein Ideal von R, so haben wir in den Sätzen 75 und 76 und Bsp. 81 die Äquivalenz der folgenden vier Eigenschaften gezeigt, die alle vier Primideale charakterisieren:

(i) $P \neq R$ und aus $ab \in P$ folgt $a \in P$ oder $b \in R$ (wobei $a, b \in R$),
(ii) $R \setminus P$ ist eine multiplikative Teilmenge von R,
(iii) $P \neq R$ und aus $I \cdot J \subseteq P$ folgt $I \subseteq P$ oder $J \subseteq P$ (wobei I, J Ideale von R sind),
(iv) R/P ist ein Integritätsbereich.

82) Es seien R und S zwei kommutative Ringe und $\varphi : R \to S$ ein Ringepimorphismus. Beweisen Sie:

a) Ist P ein Primideal von R mit $\ker\varphi \subseteq P$, so ist $\varphi(P)$ ein Primideal von S.
b) Ist Q ein Primideal von S, so ist $\varphi^{-1}(Q)$ ein Primideal von R und $\ker\varphi \subseteq \varphi^{-1}(Q)$.
c) Es gibt eine ordnungserhaltende Bijektion zwischen den Primidealen von R, die $\ker\varphi$ enthalten und den Primidealen von S.
d) Ist I ein Ideal von R, so ist jedes Primideal des Faktorrings R/I von der Gestalt P/I, wobei P ein Primideal von R mit der Eigenschaft $I \subseteq P$ ist.

83) Es sei R ein kommutativer Ring mit Eins und $M \neq R$ ein Ideal von R. Beweisen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(i) M ist ein maximales Ideal von R,
(ii) $\forall\, x \in R \setminus M \;\; \exists\, y \in R : 1_R - xy \in M$.

84) Es sei p eine Primzahl. Beweisen Sie, ausgehend von der Definition eines maximalen Ideals, dass

$$M = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, p \mid a, p \nmid b \right\}$$

ein maximales Ideal des Rings

$$R = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, p \nmid b \right\}$$

(aus Bsp. 68b) ist.

85) Es sei $R = 2\mathbb{Z}$ (d.h. R bezeichnet den Ring der geraden Zahlen mit der üblichen Addition und Multiplikation) und $M = 4\mathbb{Z}$. Beweisen Sie:

a) M ist ein maximales Ideal aber kein Primideal von R,
b) R/M ist kein Körper.

86) Es sei R ein Integritätsbereich und S eine multiplikative Teilmenge von R mit der Eigenschaft $0 \notin S$. Beweisen Sie:

a) Ist I ein Ideal von R, so ist $S^{-1}I := \{a/s \mid a \in I, s \in S\}$ ein Ideal von $S^{-1}R$.
b) Ist I ein Ideal von R und $S \cap I \neq \varnothing$, so ist $S^{-1}I = S^{-1}R$.

87) Es seien $G_1, \ldots, G_n$ Gruppen. Beweisen Sie: Ist $\sigma \in S_n$, so ist

$$G_{\sigma(1)} \times \cdots \times G_{\sigma(n)} \cong G_1 \times \cdots \times G_n.$$

88) Es sei $I \neq \varnothing$ eine (Index)Menge und G_i eine Gruppe für alle $i \in I$. Es bezeichne e_i das neutrale Element der Gruppe G_i und

$$\prod_{i\in I}^{w} G_i := \left\{ (x_i)_{i\in I} \,\middle|\, x_i \in G_i \text{ für alle } i \in I \text{ und } x_i = e_i \text{ für alle bis auf endlich viele } i \right\}.$$

Beweisen Sie (mit komponentenweiser Verknüpfung wie in Satz 93)

$$\prod_{i\in I}^{w} G_i \trianglelefteq \prod_{i\in I} G_i.$$

89) Beweisen Sie: Ist die Gruppe G inneres direktes Produkt ihrer beiden Normalteiler N_1 und N_2, so ist $G/N_1 \cong N_2$ und $G/N_2 \cong N_1$.

90) Ist die Gruppe S_3 inneres direktes Produkt von zwei ihrer Untergruppen N_1, N_2 (mit $N_1, N_2 \neq \{\varepsilon\}$ und $N_1, N_2 \neq S_3$)?

91) Finden Sie Gruppen G_1, G_2, H_1 und H_2 mit der Eigenschaft, dass $G_1 \times G_2 \cong H_1 \times H_2$ aber $G_i \ncong H_j$ für $i, j \in \{1, 2\}$.

Definition: Es sei G eine Gruppe, $N \trianglelefteq G$ und $H \leq G$. Man sagt, G sei das (innere) semidirekte Produkt von N und H, wenn $G = NH$ und $N \cap H = \{e\}$. Man schreibt dafür $G = N \rtimes H$.

92) Die Gruppe G sei das semidirekte Produkt von $N \trianglelefteq G$ und $H \leq G$. Beweisen Sie:

a) Für jedes $a \in G$ sind die Elemente $n \in N$ und $h \in H$ mit der Eigenschaft $a = nh$ eindeutig bestimmt (d.h. die Abbildung $N \times H \to G$, $(n, h) \mapsto nh$ ist bijektiv).

b) Die Abbildung $\theta : H \to \mathrm{Aut}(N)$, $h \mapsto \theta_h$ ist ein Homomorphismus. Dabei sei $\theta_h : N \to N$ durch $\theta_h(n) = hnh^{-1}$ gegeben.

93) Beweisen Sie: Für $n \geq 3$ ist S_n semidirektes Produkt von

$$A_n (\trianglelefteq S_n) \text{ und } \{\varepsilon, (12)\} (\leq S_n).$$

(Da $\{\varepsilon, (12)\} \cong \mathbb{Z}_2$ schreibt man auch $S_n = A_n \rtimes \mathbb{Z}_2$.)

94) Beweisen Sie: Für $n \geq 3$ ist D_n semidirektes Produkt von

$$\langle\alpha\rangle (\trianglelefteq D_n) \text{ und } \{\varepsilon, \beta\} (\leq D_n).$$

Dabei haben α und β die selbe Bedeutung wie in Satz 47, siehe auch Übungsbeispiel 56 zur Vorlesung Algebra 1 im SS 2020. (Da $\langle\alpha\rangle \cong \mathbb{Z}_n$ und $\{\varepsilon, \beta\} \cong \mathbb{Z}_2$ schreibt man auch $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$.)

95) Es sei K ein Körper. Beweisen Sie: Die General Linear Group $\mathrm{GL}_n(K)$ ist semidirektes Produkt der Special Linear Group $\mathrm{SL}_n(K)(\trianglelefteq \mathrm{GL}_n(K))$ und der Gruppe

$$H := \{\mathrm{diag}(a, 1, \dots, 1) \mid a \in K^*\}(\leq \mathrm{GL}_n(K)),$$

wobei $\mathrm{diag}(a_1, \dots, a_n)$ die Diagonalmatrix mit Eintragungen $a_1, \dots, a_n \in K$ bezeichnet. (Da $H \cong K^*$ schreibt man auch $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes K^*$.)

Bemerkungen: 1) Das (innere) direkte Produkt ist (wegen Korollar 98) ein Spezialfall des (inneren) semidirekten Produkts. (D.h. ist die Gruppe G das innere direkte Produkt ihrer Normalteiler N_1 und N_2, so ist G auch semidirektes Produkt von N_1 und N_2.)

2) Es kann passieren, dass zwei Gruppen G und H semidirekte Produkte isomorpher Normalerteiler und isomorpher Untergruppen sind, aber selbst nicht isomorph sind.
D.h. es ist möglich, dass $G_1 = N_1 \rtimes H_1$, $G_2 = N_2 \rtimes H_2$, $N_1 \cong N_2$ und $H_1 \cong H_2$, aber $G_1 \ncong G_2$. Z.B. ist $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$ (nach Satz 101) und $\mathbb{Z}_6$ ist daher (nach Bemerkung 1) auch semidirektes Produkt von $\mathbb{Z}_3$ und $\mathbb{Z}_2$. Andererseits ist nach Übungsbeispiel 94 auch $D_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$. Da $\mathbb{Z}_6$ abelsch ist, D_3 aber nicht, sind sie aber nicht isomorph. Der Unterschied wird verständlich, wenn man die (in den beiden Fällen verschiedenen) Abbildungen θ wie in Übungsbeispiel 92 betrachtet.

96) 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.

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

98) Beweisen Sie: Die Gruppe $\mathrm{SL}_2(\mathbb{R})$ operiert auf der oberen Halbebene der komplexen Zahlenebene (d.h. auf $H = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$) mittels

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

99) Beweisen Sie: Die Isotropiegruppe von i für die Operation der Gruppe $\mathrm{SL}_2(\mathbb{R})$ auf der oberen Halbebene H aus dem vorangegangenen Beispiel ist die Gruppe $\mathrm{SO}(2)$.

100) Die Gruppe G operiere auf der Menge M. Beweisen Sie, dass für alle $x \in M$ und alle $a \in G$ die Gleichung $G_{a \cdot x} = a \cdot G_x \cdot a^{-1}$ gilt, d.h. die Isotropiegruppen von $x \in M$ und $a \cdot x \in M$ sind zueinander konjugiert.

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

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

102) Für eine Permutation $\sigma \in S_n$ und $r \in \{1, \dots, n\}$ 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 $r \in \{1, \dots, n\}$.

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

104) Bestimmen Sie Anzahl und Elemente der 2-Sylowgruppen der Gruppe S_4.

105) Bestimmen Sie Anzahl und Elemente der 5-Sylowgruppen der Gruppe S_5.

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

Bemerkung: Man kann zeigen, dass die Gruppe $\mathrm{SL}_3(\mathbb{Z}_2)$ einfach ist und Ordnung 168 besitzt.

107) Beweisen Sie, dass die Gruppe A_5 keine Untergruppe der Ordnung 15 besitzt.

Satz (Fermat): Es sei p eine Primzahl (in $\mathbb{Z}$). Dann sind äquivalent:

(i) Es gibt $x, y \in \mathbb{Z}$, derart dass $p = x^2 + y^2$,
(ii) $p = 2$ oder $p \equiv 1 \pmod 4$.

Beweis: (i) $\Rightarrow$ (ii) Wenn $2 \mid x$, dann $x^2 \equiv 0 \pmod 4$. Wenn $2 \nmid x$ dann $x^2 \equiv 1 \pmod 4$. Es folgt, dass $p = x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. Es ist unmöglich, dass $p \equiv 0 \pmod 4$ und $p \equiv 2 \pmod 4$ ist nur für $p = 2$ möglich.
(ii) $\Rightarrow$ (i) (Heath-Brown) Es ist $2 = 1^2 + 1^2$. Sei darum ab jetzt $p \equiv 1 \pmod 4$. Es sei

$$S := \{(x, y, z) \in \mathbb{Z}^3 \mid x, y \geq 1, 4xy + z^2 = p\}.$$

Die Menge S ist nicht leer (da $((p-1)/4, 1, 1) \in S$) und endlich, da aus $(x, y, z) \in S$ folgt, dass $x, y \leq p/4$ und es zu gegebenen x, y höchstens zwei z geben kann. Es sei $f : S \to S$, $(x, y, z) \mapsto (y, x, -z)$. Die Abbildung f ist eine Involution (d.h. $f \circ f = \mathrm{id}_S$) und besitzt

keine Fixpunkt (denn $f(x,y,z) = (x,y,z)$ würde bedeuten, dass $(y,x,-z) = (x,y,z)$, woraus $z = 0$ und daher $p = 4xy$ folgen würde, was unmöglich ist). Offenbar bildet f die Menge $T := \{(x,y,z) \in S \mid z > 0\}$ bijektiv auf $S \setminus T$ ab. Es gibt kein $(x,y,z) \in S$ mit der Eigenschaft $x - y + z = 0$, weil daraus $p = 4xy + z^2 = 4xy + (x-y)^2 = (x+y)^2$ folgen würde. Bezeichnet $U := \{(x,y,z) \in S \mid x - y + z > 0\}$, so bildet f die Menge U bijektiv auf $S \setminus U$ ab. Es folgt, dass $|T| = |S|/2 = |U|$. Betrachte nun die Abbildung

$$g : U \to U, \quad (x,y,z) \mapsto (x - y + z, y, 2y - z).$$

Wir zeigen zunächst, dass g wohldefiniert ist. Ist $(x,y,z) \in U$, so gelten $x - y + z > 0$ und $y > 0$ und daher

$$4(x-y+z)y + (2y-z)^2 = 4xy - 4y^2 + 4yz + 4y^2 - 4yz + z^2 = 4xy + z^2 = p,$$

also ist $g(x,y,z) \in S$. Da $x - y + z - y + 2y - z = x > 0$, ist $g(x,y,z) \in U$. Weiters ist g ebenfalls eine Involution, denn

$$(g \circ g)(x,y,z) = g(x-y+z, y, 2y-z) = (x - y + z - y + 2y - z, y, 2y - 2y + z) = (x,y,z)$$

und g besitzt genau einen Fixpunkt, denn $g(x,y,z) = (x,y,z)$ besagt ja gerade, dass $(x - y + z, y, 2y - z) = (x,y,z)$, woraus $y = z$ und daher $p = 4xy + y^2 = (4x + y)y$ folgt. Also muss $y = z = 1$ und $x = (p-1)/4$ gelten. Daher ist $|U| \equiv 1 \pmod 2$ und somit auch $|T| \equiv 1 \pmod 2$. Schließlich sei $h : T \to T$, $(x,y,z) \mapsto (y,x,z)$. Offenbar ist h wohldefiniert und eine Involution. Da $|T| \equiv 1 \pmod 2$, muss h einen Fixpunkt besitzen, d.h. es gibt ein $(x,y,z) \in T$ mit der Eigenschaft $x = y$ und daher $p = 4x^2 + z^2 = (2x)^2 + z^2$.

Definition: Für $a \in \mathbb{Z}[i]$ definiert man die Norm $N(a)$ durch $N(a) := a \cdot \overline{a} = |a|^2$ (d.h. ist $a = x + iy$ mit $x, y \in \mathbb{Z}$, so ist $N(x + iy) = x^2 + y^2$).

108) Es seien $a, b \in \mathbb{Z}[i]$. Beweisen Sie:

a) $N(a \cdot b) = N(a) \cdot N(b)$,

b) Wenn $a \mid b$ (Teilbarkeit in $\mathbb{Z}[i]$) dann $N(a) \mid N(b)$ (Teilbarkeit in $\mathbb{Z}$),

109) Es sei $a \in \mathbb{Z}[i]$. Beweisen Sie:

a) $a \in \mathbb{Z}[i]^* \Leftrightarrow N(a) = 1 \Leftrightarrow a \in \{1, -1, i, -i\}$,

b) Ist $N(a)$ eine Primzahl, so ist a in $\mathbb{Z}[i]$ irreduzibel (und daher auch prim).

110) Beweisen Sie die folgenden Eigenschaften des faktoriellen Rings $\mathbb{Z}[i]$:
Hinweis. Verwenden Sie den obigen Satz von Fermat und das vorangegangene Beispiel.

a) $1+i$ ist irreduzibel in $\mathbb{Z}[i]$ (und es gilt $2 = -i \cdot (1+i)^2$, d.h. 2 *verzweigt*),
b) Ist $p \equiv 1 \pmod 4$ eine Primzahl und $x, y \in \mathbb{Z}$, $x > y > 0$ derart dass $p = x^2 + y^2$, so sind $x + iy$ und $x - iy$ beide irreduzibel und nicht zueinander assoziiert in $\mathbb{Z}[i]$ (und es gilt $p = (x+iy)(x-iy)$, d.h. p *zerfällt*),
c) Ist $p \equiv 3 \pmod 4$ eine Primzahl, so ist p auch in $\mathbb{Z}[i]$ irreduzibel (d.h. p ist *träge*).

111) Es sei R ein euklidischer Ring, dessen Funktion $\varphi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ zusätzlich die Bedingung $\varphi(ab) \geq \varphi(a)$ $\forall a, b \in R \setminus \{0\}$ erfüllt.

a) Welche der euklidischen Ringe, die bisher besprochen wurden, erfüllen diese Bedingung?
b) Zeigen Sie für $a, b \in R \setminus \{0\}$: Sind a und b assoziiert, so ist $\varphi(a) = \varphi(b)$,
c) Zeigen Sie für $a, b \in R \setminus \{0\}$: Ist $\varphi(a) = \varphi(b)$ und $a \mid b$, so sind a und b assoziiert,
d) Zeigen Sie für $a \in R \setminus \{0\}$: $a \in R^* \Leftrightarrow \varphi(a) = \varphi(1_R)$.

112) Es sei R ein faktorieller Ring und $a \in R \setminus \{0\}$. Beweisen Sie, dass das Ideal (a) nur in endlich vielen Hauptidealen von R enthalten ist.

113) Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und

$$p(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X].$$

a) Beweisen Sie

$$p \in R[X]^* \quad \Longleftrightarrow \quad a_0 \in R^* \text{ und } a_1, \ldots, a_n \in \operatorname{Nil}(R).$$

Hinweis. Es sei $p(X) \cdot q(X) = 1$ mit $q(X) = b_0 + b_1 X + \cdots + b_m X^m \in R[X]$. Zeigen Sie mit Induktion nach r, dass $a_n^{r+1} b_{m-r} = 0$. Folgern Sie, dass a_n nilpotent ist und verwenden Sie Beispiel 72.

b) Finden Sie $\left(\overline{2}X + \overline{3}\right)^{-1} \in \mathbb{Z}_8[X]$.

114) Führen Sie Division mit Rest für die folgenden Polynome $f, g \in \mathbb{Q}[X]$ durch, d.h. finden Sie die Polynome $q, r \in \mathbb{Q}[X]$, die $f = qg + r$ und $\operatorname{grad} r < \operatorname{grad} g$ erfüllen:

a) $f(X) = X^6 + X^5 - X^4 - 4X^3 - 2X^2 + 2X - 4$,
   $g(X) = X^5 + 2X^4 - 2X^3 - 5X^2 - 5X + 2$
b) $f(X) = X^5 - 2X^4 + 3X^3 - 6X^2 + 2X - 4$, $g(X) = X^4 + X^3 - 5X^2 + X - 6$
c) $f(X) = X^8 - 1$, $g(X) = X^2 - 1$

115) Finden Sie die größten gemeinsamen Teiler der beiden Polynome

$$p(X) = X^3 - 2X^2 - X + 2 \quad \text{und} \quad q(X) = X^3 - 4X^2 + 3X$$

im Polynomring $\mathbb{Q}[X]$ mit Hilfe des euklidischen Algorithmus. Finden Sie Polynome $f_1, f_2 \in \mathbb{Q}[X]$, derart dass $f_1 p + f_2 q = g$ gilt, wobei $g \in \mathbb{Q}[X]$ den eindeutig bestimmten normierten größten gemeinsamen Teiler von p und q bezeichnet.

116) Beweisen Sie direkt, dass $\mathbb{Z}[X]$ kein Hauptidealbereich ist, indem Sie zeigen, dass das Ideal $I := (2, X)$ kein Hauptideal ist.

117) Es sei R ein unendlicher Integritätsbereich. Beweisen Sie, dass die Abbildung, die jedem $p \in R[X]$ die Polynomfunktion $f_p : R \to R$, $\alpha \mapsto p(\alpha)$ zuordnet, injektiv ist.

118) Es sei K ein Körper mit $\operatorname{char} K = p > 0$ und $f \in K[X]$ mit $\operatorname{grad} f \geq 1$. Beweisen Sie, dass $f' = 0$ genau dann gilt, wenn es ein $g \in K[X]$ gibt, derart dass $f(X) = g(X^p)$.

119) Beweisen Sie die Irreduzibilität der folgenden Polynome in $\mathbb{Q}[X]$ mit Hilfe des Eisensteinkriteriums:

a) $X^3 + 6X + 2$
b) $3X^4 + 15X^2 + 10$
c) $2X^5 - 6X^3 + 9X^2 - 15$
d) $X^{11} - 7X^6 + 21X^5 + 49X - 56$

120) Es sei p eine Primzahl. Das p-te Kreisteilungspolynom $\Phi_p(X)$ hat die Gestalt

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Zeigen Sie mit Hilfe des Eisensteinkriteriums, dass $\Phi_p(X)$ in $\mathbb{Q}[X]$ irreduzibel ist.
Hinweis. Verwenden Sie $\Phi_p(X) = (X^p - 1)/(X - 1)$, betrachten Sie $\Phi_p(X + 1)$ und wenden Sie den binomischen Lehrsatz an.

121) Es sei K ein Körper und $n \in \mathbb{N} \setminus \{0\}$. Beweisen Sie, dass $E_n := \{a \in K \mid a^n = 1\}$ eine endliche zyklische Untergruppe von $(K^*, \cdot)$ ist.

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

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

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

125) 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? Folgern Sie $\mathbb{Q}\big(\sqrt[3]{2}\big) = \mathbb{Q}\big(\sqrt[3]{4}\big)$.