Übungen zu Algebra, WS 2015/16

Christoph Baxa

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

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

2) Beweisen Sie: Sind $G_1, \dots, G_n$ und $H_1, \dots, H_n$ Gruppen mit der Eigenschaft $H_i \cong G_i$ (für $1 \leq i \leq n$), so ist $G_1 \times \cdots \times G_n \cong H_1 \times \cdots \times H_n$.

3) Es seien $G_1, \dots, G_k$ Gruppen und $N_i \trianglelefteq G_i$ für $1 \leq i \leq k$. Beweisen Sie, dass

$$N_1 \times \cdots \times N_k \trianglelefteq G_1 \times \cdots \times G_k$$

und dass

$$(G_1 \times \cdots \times G_k)/(N_1 \times \cdots \times N_k) \cong (G_1/N_1) \times \cdots \times (G_k/N_k).$$

Hinweis. Betrachten Sie die Abbildung $G_1 \times \cdots \times G_k \to (G_1/N_1) \times \cdots \times (G_k/N_k)$, $(a_1, \dots, a_k) \mapsto (a_1 N_1, \dots, a_k N_k)$.

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

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

Beweisen Sie

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

5) Es sei G eine Gruppe und $N_i \trianglelefteq G$ (für $1 \leq i \leq k$). Beweisen Sie, dass $N_1 \cdot \ldots \cdot N_k \trianglelefteq G$.

6) Es seien $G_1, \dots, G_k$ Gruppen. Beweisen Sie: Das äußere direkte Produkt $G_1 \times \cdots \times G_k$ ist das innere direkte Produkt von $N_1, \dots, N_k$, wobei

$$N_i := \big\{ (a_j)_{1 \leq j \leq k} \in G_1 \times \cdots \times G_k \,\big|\, a_j = e_j \text{ für } 1 \leq j \leq k,\, j \neq i \big\} \quad \text{für } 1 \leq i \leq k.$$

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

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

9) 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 $i, j \in \{1, 2\}$.

10) Es seien N und H Gruppen und $\theta : H \to \mathrm{Aut}(N)$, $h \mapsto \theta_h$ ein Homomorphismus (d.h. $\theta_{h_1 h_2} = \theta_{h_1} \circ \theta_{h_2}$ für alle $h_1, h_2 \in H$). Beweisen Sie (mit neutralen Elementen e_N und e_H): Versieht man $N \times H$ mit der Verknüpfung $(n_1, h_1) \bullet (n_2, h_2) := (n_1 \cdot \theta_{h_1}(n_2), h_1 h_2)$, so wird dadurch eine Gruppe definiert, die man mit $N \rtimes_\theta H$ bezeichnet.

Bemerkung. Die Gruppe $N \rtimes_\theta H$ wird als (äußeres) semidirektes Produkt von N und H bezeichnet. Ist $\theta_h = \mathrm{id}_N$ für alle $h \in H$, so erhält man als Spezialfall das (äußere) direkte Produkt der Gruppen N und H.

11) Die Bezeichnungen N, H und θ mögen dieselbe Bedeutung haben wie im vorangegangenen Beispiel. Beweisen Sie: Bezeichnen

$$N^* = \{(n, e_H) \mid n \in N\} \text{ und } H^* = \{(e_N, h) \mid h \in H\},$$

so gelten $H^* \leq N \rtimes_\theta H$, $N^* \trianglelefteq N \rtimes_\theta H$, $H^* \cong H$, $N^* \cong N$, $N^* \cap H^* = \{(e_N, e_H)\}$ und $N^* \bullet H^* = N \rtimes_\theta H$.

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 $G = N \rtimes H$.

12) 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.

13) Beweisen Sie: a) Für $n \geq 3$ ist S_n semidirektes Produkt von $A_n (\trianglelefteq S_n)$ und $\{\varepsilon, (12)\} (\leq S_n)$. (Da $\{\varepsilon, (12)\} \cong \mathbb{Z}_2$ schreibt man auch $S_n = A_n \rtimes \mathbb{Z}_2$.)

b) Für $n \geq 3$ ist D_n semidirektes Produkt von $\langle \alpha \rangle (\trianglelefteq D_n)$ und $\{\varepsilon, \beta\} (\leq D_n)$. Dabei haben α und β dieselbe Bedeutung wie in Satz 45, vergleiche auch Übungsbeispiel 42 zur Vorlesung *Algebraische Strukturen* im WS 2014/15. (Da $\langle \alpha \rangle \cong \mathbb{Z}_n$ und $\{\varepsilon, \beta\} \cong \mathbb{Z}_2$ schreibt man auch $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$.)

14) 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 $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes K^*$.)

15) Beweisen Sie: Die Gruppe $(\mathbb{Z}_6, +)$ ist (inneres) direktes Produkt von Normalteilern, die zu den Gruppen $\mathbb{Z}_3$ und $\mathbb{Z}_2$ isomorph sind (und daher auch semidirektes Produkt dieser Gruppen). Ebenso ist S_3 semidirektes Produkt eines Normalteilers und einer Untergruppe, die zu $\mathbb{Z}_3$ bzw. $\mathbb{Z}_2$ isomorph sind. Es gilt also $\mathbb{Z}_6 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ und $S_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ obwohl $\mathbb{Z}_6 \ncong S_3$. Worin besteht der Unterschied zwischen den beiden semidirekten Produkten?

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

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

17) Finden Sie eine Kompositionsreihe und ihre Faktoren für die symmetrische Gruppe S_n (mit $n \in \{1, 2, 3, 4\}$).

18) Finden Sie ein Beispiel einer Normalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$, bei der nicht jeder Term G_i Normalteiler der Gruppe G ist.

19) Finden Sie eine Kompositionsreihe und ihre Faktoren für die Quaternionengruppe Q_8. (Vergleiche auch die Übungsbeispiele 17 und 38 zur Vorlesung *Algebraische Strukturen* im WS 2014/15.)

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

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

22) Es seien $k, \ell \in \mathbb{Z}$, $k, \ell \geq 1$. Finden Sie äquivalente Verfeinerungen der Normalreihen $\mathbb{Z} \trianglerighteq k\mathbb{Z} \trianglerighteq \{0\}$ und $\mathbb{Z} \trianglerighteq \ell\mathbb{Z} \trianglerighteq \{0\}$ der Gruppe $(\mathbb{Z}, +)$.

23) 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.

24) Es sei p eine Primzahl, $n \in \mathbb{Z}$, $n \geq 0$ und G eine zyklische Gruppe der Ordnung $|G| = p^n$. Beweisen Sie, dass G genau eine Kompositionsreihe besitzt, in der keine Terme wiederholt werden.

25) 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.

26) Die Gruppe 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.

27) 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.

28) 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 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.

29) 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 25),
d) Die Operation aus Beispiel 26),
e) Die Operation aus Beispiel 27a),
f) Die Operation aus Beispiel 27b).

30) 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) Für alle $x \in M$ und alle $a \in G$ gilt $G_{a \cdot x} = a \cdot G_x \cdot a^{-1}$, d.h. die Isotropiegruppen sind alle zueinander konjugiert.
c) $|M| = [G : G_x]$ für alle $x \in M$.
d) Ist G endlich, so gilt $|M| \mid |G|$.
e) Was bedeuten Teile a) bis d) für die Operationen von Gruppen auf Mengen aus Bsp. 29 (für die das sinnvoll ist)?

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.

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

32) 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 $\varphi(C) = C$.

33) 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 $r \geq 1$.

34) 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.

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

36) Es sei p eine Primzahl. Finden Sie eine unendliche p-Gruppe. (Falls Sie sich ein wenig mit Kardinalzahlen auskennen, wollen Sie vielleicht gleich unendlich viele paarweise nicht isomorphe unendliche p-Gruppen konstruieren.)

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

38) 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.

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

40) 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.

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

Bemerkung. Es sei p eine Primzahl. Für das nachfolgende Beispiel wird die Definition der p-Sylowgruppe einer (nicht notwendig endlichen) Gruppe G folgendermaßen abgeändert: Eine Untergruppe P von G heißt p-Sylowgruppe, wenn P eine (bezüglich der Mengeninklusion) maximale p-Untergruppe von G ist. Diese Definition ist für endliche Gruppen mit der in der Vorlesung gegebenen Definition äquivalent.

42) Es sei p eine Primzahl und G eine Gruppe. Beweisen Sie:

a) Ist H eine p-Untergruppe von G, so gibt es eine p-Sylowgruppe P von G, in der H enthalten ist. *Hinweis.* Verwenden Sie das Lemma von Zorn.

b) G enthält eine p-Sylowgruppe.

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

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

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

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

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

b) Es sei R ein Ring mit 1 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 1 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 $I \cdot J := \{x_1y_1 + \cdots + x_ny_n \mid n \geq 0, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}$.

46) 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 1 und sind $a, b \in R$, so gilt $(a) \cdot (b) = (ab)$.

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

a) $I \cdot J \subseteq I \cap J$,
b) Ist R kommutativ, so gilt $I \cdot J = J \cdot I$,
c) Ist R ein Ring mit 1, so gilt $R \cdot I = I \cdot R = I$.

48) Es sei R ein Ring. Beweisen Sie:

a) $I \cdot (J_1 + J_2) = I \cdot J_1 + I \cdot J_2$ für alle Ideale I, J_1, J_2 von R,
b) $(I_1 + I_2) \cdot J = I_1 \cdot J + I_2 \cdot J$ für alle Ideale I_1, I_2, J von R,
c) Für alle Ideale I_1, I_2, I_3 von R gilt

$$\begin{aligned}(I_1 \cdot I_2) \cdot I_3 &= I_1 \cdot (I_2 \cdot I_3) \\ &= \left\{ \sum_{i=1}^{n} x_i y_i z_i \;\middle|\; n \geq 0, x_1, \ldots, x_n \in I_1, y_1, \ldots, y_n \in I_2, z_1, \ldots, z_n \in I_3 \right\}.\end{aligned}$$

Definition. Es sei R ein kommutativer Ring mit 1. Eine Menge $S \subseteq R$ wird multiplikativ genannt, wenn $1 \in S$ und $ab \in S$ $\forall a, b \in S$.

49) Es sei R ein kommutativer Ring mit 1 und P ein Ideal von R. Beweisen Sie, dass P genau dann ein Primideal ist, wenn $R \setminus P$ multiplikativ ist.

50) Es sei R ein kommutativer Ring 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 $J \subseteq P$.

Bemerkung. Eigenschaft (ii) aus Bsp. 50 wird benützt, um den Begriff des Primideals in beliebigen Ringen (die nicht kommutativ zu sein brauchen) zu definieren.

Bemerkung. Ist R ein kommutativer Ring mit 1 und P ein Ideal von R, so haben wir in Satz 72 und den Übungsbeispielen 49 und 50 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 multiplikativ,
(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.

51) 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.

52) Es sei R ein kommutativer Ring mit 1 und $M \neq R$ ein Ideal von R. Beweisen Sie, dass die folgenden beiden Aussagen äquivalent sind:

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

53) Es sei R ein Integritätsbereich mit Quotientenkörper K und $S \subseteq R$ multiplikativ, $0 \notin S$. Beweisen Sie:

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

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, dasss 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 $N(x + iy) = x^2 + y^2$).

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

a) $N(a \cdot b) = N(a) \cdot N(b)$,
b) Wenn $a \mid b$ (in $\mathbb{Z}[i]$) dann $N(a) \mid N(b)$ (in $\mathbb{Z}$),
c) $a \in \mathbb{Z}[i]^* \Leftrightarrow N(a) = 1 \Leftrightarrow a \in \{1, -1, i, -i\}$,
d) Ist $N(a)$ eine Primzahl, so ist a in $\mathbb{Z}[i]$ irreduzibel (und daher auch prim).

55) 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 assoziert 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).

Definition. Für $a \in \mathbb{Z}[i\sqrt{5}] = \{x + i\sqrt{5}y \mid x, y \in \mathbb{Z}\}$ definiert man die Norm $N(a)$ durch $N(a) := a \cdot \overline{a} = |a|^2$ (d.h. ist $a = x + i\sqrt{5}y$ mit $x, y \in \mathbb{Z}$, so ist $N(x + i\sqrt{5}y) = x^2 + 5y^2$).

56) Beweisen Sie:

a) $N(a \cdot b) = N(a) \cdot N(b)$ für alle $a, b \in \mathbb{Z}[i\sqrt{5}]$,
b) Wenn $a \mid b$ (in $\mathbb{Z}[i\sqrt{5}]$) dann $N(a) \mid N(b)$ (in $\mathbb{Z}$),
c) $\mathbb{Z}[i\sqrt{5}]^* = \{a \in \mathbb{Z}[i\sqrt{5}] \mid N(a) = 1\} = \{1, -1\}$.

57) Beweisen Sie, dass 2 in $\mathbb{Z}[i\sqrt{5}]$ irreduzibel aber nicht prim ist. *Hinweis.* Verwenden Sie $2 \mid \big((1 + i\sqrt{5})(1 - i\sqrt{5})\big)$, um zu zeigen, dass 2 nicht prim ist.

58) Beweisen Sie, dass $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ durch die Abbildung

$$\varphi : \mathbb{Z}[\sqrt{2}] \to \{0, 1, 2, 3, \dots\}, \quad \varphi\big(a + b\sqrt{2}\big) = |a^2 - 2b^2| \text{ (mit } a, b \in \mathbb{Z})$$

ein euklidischer Ring wird. *Hinweis.* Bezeichnet σ den Automorphismus

$$\sigma : \mathbb{Q}\big(\sqrt{2}\big) \to \mathbb{Q}\big(\sqrt{2}\big), \quad \sigma\big(x + y\sqrt{2}\big) = x - y\sqrt{2} \text{ (mit } x, y \in \mathbb{Q}),$$

so ist $\varphi(\alpha) = |\alpha \cdot \sigma(\alpha)| = |\operatorname{id}_{\mathbb{Q}(\sqrt{2})}(\alpha) \cdot \sigma(\alpha)|$.

Definition. Es sei R ein faktorieller Ring und $a_1, \dots, a_n \in R$. Ein $b \in R$ wird gemeinsames Vielfaches von $a_1, \dots, a_n$ genannt, wenn $a_i \mid b$ für $1 \leq i \leq n$.

Definition. Es sei R ein faktorieller Ring und $a_1, \dots, a_n \in R$. Ein $k \in R$ wird kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$ genannt, wenn die folgenden beiden Bedingungen erfüllt sind:

1) $a_i \mid k$ für $1 \leq i \leq n$,
2) Wenn $a_i \mid \ell$ für $1 \leq i \leq n$ dann $k \mid \ell$.

59) Es sei R ein faktorieller Ring, $a_1, \dots, a_n \in R$ und $k, \ell \in R$. Beweisen Sie:

a) Sind k, ℓ beide kleinste gemeinsame Vielfache von $a_1, \dots, a_n$, so sind k und ℓ assoziert.
b) Ist k ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$ und k und ℓ sind assoziert, so ist ℓ ebenfalls ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$.
c) Gibt es ein $j \in \{1, \dots, n\}$, derart dass $a_j = 0$, so ist 0 das einzige kleinste gemeinsame Vielfache von $a_1, \dots, a_n$.

60) Es sei R ein faktorieller Ring und $a_1, \dots, a_n \in R \setminus \{0\}$. Besitzt a_j die Darstellung $a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$ (wie in Satz 126) für $1 \leq j \leq n$, so sind genau die Elemente der Gestalt

$$u \prod_{i \in I} \pi_i^{\max\{\alpha_{i1}, \dots, \alpha_{in}\}} \quad \text{mit } u \in R^*$$

die kleinsten gemeinsamen Vielfachen von $a_1, \dots, a_n$. Insbesondere existieren stets kleinste gemeinsame Vielfache.

61) Es sei R ein Hauptidealbereich, $a_1, \dots, a_n \in R$ und $k \in R$. Beweisen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(i) k ist ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$,
(ii) $(k) = (a_1) \cap \dots \cap (a_n)$.

62) Es sei R ein euklidischer Ring (durch die Funktion $\varphi : R \setminus \{0\} \to \{0, 1, 2, \dots\}$) und $a, b \in R$ mit $b \neq 0$. Beweisen Sie, dass man den euklidischen Algorithmus verwenden kann, um einen größten gemeinsamen Teiler von a und b zu finden. D.h. man setzt $r_0 := b$ und berechnet

$$\begin{aligned}
a &= q_0 b + r_1 && \text{mit } r_1 = 0 \text{ oder } \varphi(r_1) < \varphi(b), \\
b &= q_1 r_1 + r_2 && \text{mit } r_2 = 0 \text{ oder } \varphi(r_2) < \varphi(r_1), \\
r_1 &= q_2 r_2 + r_3 && \text{mit } r_3 = 0 \text{ oder } \varphi(r_3) < \varphi(r_2), \\
&&& \dots \\
r_k &= q_{k+1} r_{k+1} + r_{k+2} && \text{mit } r_{k+2} = 0 \text{ oder } \varphi(r_{k+2}) < \varphi(r_{k+1}), \\
&&& \dots
\end{aligned}$$

Ist $n \geq 0$ der kleinste Index mit $r_{n+1} = 0$, so ist r_n ein größter gemeinsamer Teiler von a und b.

Definition. Es sei R ein Ring. Ein Element $a \in R$ heißt nilpotent, wenn es ein $n \in \mathbb{Z}$, $n \geq 1$ mit der Eigenschaft $a^n = 0$ gibt. Die Menge aller nilpotenter Elemente des Rings R bezeichnen wir mit $\mathrm{Nil}(R)$.

63) 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).

64) Es sei $R(\neq \{0\})$ ein kommutativer Ring mit 1 und

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

Beweisen Sie

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

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 das vorangegangene Beispiel.

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

66) 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.

67) Es sei K ein Körper und $f \in K[X]$ mit $\operatorname{grad} f \geq 1$. Beweisen Sie:

a) Ist $\operatorname{char} K = 0$, so ist $\operatorname{grad} f' = \operatorname{grad} f - 1$,
b) Ist $\operatorname{char} K = p > 0$, so ist $f' = 0$ genau dann, wenn es ein $g \in K[X]$ gibt, derart dass $f(X) = g(X^p)$ gilt.

68) 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) $X^{11} - 7X^6 + 21X^5 + 49X - 56$

69) 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.

70) 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) $f(X) = X^8 - 1$, $g(X) = X^2 - 1$

71) 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.

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

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

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

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

76) 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?