Übungen zu Algebra, WS 2013/14

Wiederholungsbeispiele zum Thema Ringe

Christoph Baxa

1) Es sei R ein Ring und $a_1, \dots, a_n, b_1, \dots, b_n \in R$. Beweisen Sie die *Abelsche Umformung*

$$\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n-1} (a_i - a_{i+1}) \sum_{j=1}^{i} b_j + a_n \sum_{j=1}^{n} b_j.$$

2) 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.

3) Es sei

$$\mathbb{H} := \left\{ \begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix} \,\middle|\, z, w \in \mathbb{C} \right\}.$$

Beweisen Sie, dass $\mathbb{H}$, versehen mit der üblichen Addition und Multiplikation von Matrizen, einen Schiefkörper, aber keinen Körper bildet.

4) Beweisen Sie, dass die Gleichung $x^2 + 1 = 0$ überabzählbar unendlich viele Lösungen $x \in \mathbb{H}$ besitzt.

5) a) Es sei p eine Primzahl. Beweisen Sie, 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, dass $\{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$ ein Unterring von $(\mathbb{Q}, +, \cdot)$ ist. Ist es auch ein Ideal?

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

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

6) 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 $Z(R_1 \times \cdots \times R_n) = Z(R_1) \times \cdots \times Z(R_n)$.

7) 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 $n \in \mathbb{Z}$, $n \geq 1$ mit der Eigenschaft $a^n = 0$ gibt. Die Menge aller nilpotenter Elemente des Rings R bezeichnen wir mit $\mathrm{Nil}(R)$.

8) 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).

9) 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.

10) 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 70 (iii) für $n \geq 2$ nicht, dass $M_n(K)$ ein Schiefkörper ist?

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

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

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

13) 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 $(a) \cdot (b) = (ab)$.

14) 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 $R \cdot I = I \cdot R = I$.

15) 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

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

16) 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 $a, b \in \mathbb{Z}$),

d) Es sei p eine Primzahl und $\varphi : \mathbb{Z}_p \to \mathbb{Z}_p$, $\varphi(x) = x^p$.

17) 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.

18) Es sei $R(\neq \{0\})$ ein kommutativer Ring mit 1. Beweisen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(i) R ist ein Körper,

(ii) Ist S ein Ring und $\varphi : R \to S$ ein Ringhomomorphismus, so ist φ die Nullabbildung oder injektiv.

19) Es sei K ein Körper, $A \in M_n(K)$ und $\det A = 0$. Beweisen Sie, dass A in $M_n(K)$ ein Nullteiler ist. *Hinweis.* Bezeichnen $A^1, \dots, A^n$ die Spaltenvektoren von A, so gibt es $x_1, \dots, x_n \in K$ (nicht alle $= 0$), die $x_1 A^1 + \cdots + x_n A^n = 0$ erfüllen. Bezeichnen $A_1, \dots, A_n$ die Zeilenvektoren von A, so gibt es $y_1, \dots, y_n \in K$ (nicht alle $= 0$), sodass $y_1 A_1 + \cdots + y_n A_n = 0$. Betrachten Sie die Matrix $B := (x_i y_j)_{1 \leq i,j \leq n}$.

20) Beweisen Sie mit den Bezeichnungen von Beispiel 2:

a) φ ein Rechtsnullteiler aber kein Linksnullteiler in R,

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

21) a) Es sei R ein Ring und $a \in R$. Beweisen Sie: Ist a kein Linksnullteiler (bzw. kein Rechtsnullteiler), so folgt aus $ax = ay$ (bzw. $xa = ya$), dass $x = y$ (für $x, y \in R$).
b) Es seien R und S Integritätsbereiche und R ein Unterring von S. Beweisen Sie $1_R = 1_S$.

22) Es sei p eine Primzahl. Beweisen Sie, dass $\left\{a/b \;\middle|\; a, b \in \mathbb{Z}, p \mid a, p \nmid b\right\}$ ein Primideal des Rings $\{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$ (aus Bsp. 5b) ist.

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

23) 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.

24) Es sei R ein kommutativer Ring mit 1 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 $J \subseteq P$.

25) 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 P 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.

26) Beweisen Sie, dass der Ring $R = 2\mathbb{Z}$ ein maximales Ideal M enthält, derart dass R/M kein Körper ist.

27) 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) $\forall\, x \in R \setminus M \;\; \exists\, y \in R : 1_R - xy \in M$.

28) Es sei p eine Primzahl. Beweisen Sie, dass $\left\{a/b \;\middle|\; a, b \in \mathbb{Z}, p \mid a, p \nmid b\right\}$ ein maximales Ideal des Rings $\{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$ (aus Bsp. 5b) ist.

29) Beweisen Sie, dass der Ring $R = 2\mathbb{Z}$ ein maximales Ideal M enthält, das kein Primideal ist.

30) 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 $S^{-1}I = S^{-1}R$.

31) Es sei R ein faktorieller Ring und $a, b \in R$. Die Menge $\{\pi_i \mid i \in I\}$ enthalte aus jeder Äquivalenzklasse zueinander assozierter irreduzibler Elemente genau einen Repräsentanten. Es seien

$$a = u \prod_{i \in I} \pi_i^{\alpha_i} \quad \text{und} \quad b = v \prod_{i \in I} \pi_i^{\beta_i}$$

die in Lemma 179 beschriebenen Darstellungen, d.h. $u, v \in R^*$, $\alpha_i, \beta_i \in \mathbb{Z}$ und $\alpha_i, \beta_i \geq 0$ für alle $i \in I$, $\alpha_i = 0$ für fast alle $i \in I$ und $\beta_i = 0$ für fast alle $i \in I$. Beweisen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(i) $a \mid b$,
(ii) $\alpha_i \leq \beta_i$ für alle $i \in I$.

Definition. Es sei R ein faktorieller Ring und $a_1, \ldots, a_n \in R$.

Es seien $a_1, \ldots, a_n$ nicht alle $= 0$. Ein $g \in R$ wird größter gemeinsamer Teiler von $a_1, \ldots, a_n$ genannt, wenn die folgenden beiden Bedingungen erfüllt sind:

1) $g \mid a_i$ für $1 \leq i \leq n$,
2) Wenn $d \mid a_i$ für $1 \leq i \leq n$ dann $d \mid g$.

Es seien $a_1, \ldots, a_n \neq 0$. Ein $k \in R$ wird kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$ 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 $k \mid \ell$.

Bemerkung. Beachten Sie, dass diese Definitionen nicht mit den in der Zahlentheorie für $\mathbb{Z}$ üblichen übereinstimmt. Sind z.B. $a_1 = 8$ und $a_2 = 12$, so sind (nach der obigen Definition) sowohl 4 als auch -4 größter gemeinsamer Teiler von a_1 und a_2 und sowohl 24 als auch -24 kleinstes gemeinsames Vielfaches von a_1 und a_2. Insbesondere sind größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches nicht eindeutig bestimmt.

32) Es sei R ein faktorieller Ring und $a_1, \dots, a_n \in R \setminus \{0\}$. Die Menge $\{\pi_i \mid i \in I\}$ enthalte aus jeder Äquivalenzklasse zueinander assoziierter irreduzibler Elemente genau einen Repräsentanten. Für $1 \leq j \leq n$ sei $a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$ die in Lemma 179 beschriebene Darstellung, d.h. für $1 \leq j \leq n$ und $i \in I$ ist $u_j \in R^*$, $\alpha_{ij} \in \mathbb{Z}$, $\alpha_{ij} \geq 0$ und für festes $j \in \{1, \dots, n\}$ ist $\alpha_{ij} = 0$ für fast alle $i \in I$. Beweisen Sie:

a) Es sei $g \in R$ ein größter gemeinsame Teiler von $a_1, \dots, a_n$. Ein $g' \in R$ ist genau dann ein größter gemeinsame Teiler von $a_1, \dots, a_n$ wenn g und g' zueinander assoziert sind (d.h. der größte gemeinsame Teiler ist bis auf Einheiten eindeutig bestimmt).

b) Es sei $k \in R$ ein kleinstes gemeinsames Vielfache von $a_1, \dots, a_n$. Ein $k' \in R$ ist genau dann ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$ wenn k und k' zueinander assoziert sind (d.h. das kleinste gemeinsame Vielfache ist bis auf Einheiten eindeutig bestimmt).

c) $\prod_{i \in I} \pi_i^{\min\{\alpha_{i1}, \dots, \alpha_{in}\}}$ ist ein größter gemeinsame Teiler von $a_1, \dots, a_n$.

d) $\prod_{i \in I} \pi_i^{\max\{\alpha_{i1}, \dots, \alpha_{in}\}}$ ist ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$.

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

33) 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) $a \in \mathbb{Z}[i]^* \iff N(a) = 1$,
d) Ist $N(a)$ eine Primzahl, so ist a in $\mathbb{Z}[i]$ irreduzibel (und daher auch prim).

34) 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 $N(x + iy) = x^2 + 5y^2$).

35) 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) $\mathbb{Z}[i\sqrt{5}]^* = \{a \in \mathbb{Z}[i\sqrt{5}] \mid N(a) = 1\} = \{1, -1\}$.

36) 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.

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

38) Es sei R ein kommutativer Ring mit $1 (\neq 0)$ und $p(X) = a_0 + a_1 X + \dots + a_n X^n \in R[X]$. Beweisen Sie

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

Hinweis. Es sei $p(X) \cdot q(X) = 1$ mit $q(X) = b_0 + b_1 X + \dots + b_m X^m \in R[X]$. 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 8 der Wiederholungsbeispiele zum Thema Ringe.

39) Es sei $p(X) = X^3 + X^2 + X + \overline{6} \in \mathbb{Z}_9[X]$.

a) Zeigen Sie, dass p in $\mathbb{Z}_9$ mehr als $3 = \operatorname{grad} p$ Nullstellen besitzt,
b) Finden Sie eine Zerlegung von p in drei Linearfaktoren,
c) Erklären Sie, warum a) und b) einander nicht widersprechen.

40) Es sei R ein Integritätsbereich. Beweisen Sie:

a) $(ap)' = ap'$ für alle $a \in R$ und alle $p \in R[X]$,
b) $(p + q)' = p' + q'$ für alle $p, q \in R[X]$,
c) $(p \cdot q)' = p' \cdot q + p \cdot q'$ für alle $p, q \in R[X]$,
d) $(p^n)' = np^{n-1} \cdot p'$ für alle $p \in R[X]$ und alle $n \in \mathbb{Z}$, $n \geq 1$.

41) 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.

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

43) a) Zeigen Sie mit Hilfe des Eisensteinkriteriums, dass $p(X) = X^2 + X + 2 \in \mathbb{Q}[X]$ irreduzibel ist, indem Sie $p(X + 3)$ betrachten.
b) Zeigen Sie, dass $p(X) = X^2 + X + 2 \in \mathbb{Q}[X]$ irreduzibel ist, indem Sie die Abbildung $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_3[X]$, $\varphi\big(a_n X^n + \cdots + a_1 X + a_0\big) = \overline{a_n} X^n + \cdots + \overline{a_1} X + \overline{a_0}$ betrachten.

44) 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.

45) Es sei R ein faktorieller Ring und $p(X, Y) = Y^3 + X^2Y^2 + X^3Y + X \in R[X, Y]$. Beweisen Sie mit Hilfe des Eisensteinkriteriums, dass p in $R[X, Y]$ irreduzibel ist. *Hinweis.* Fassen Sie p als Element von $R[X][Y]$ auf.