Fakultät für Mathematik
Universität Bielefeld
Joa Weber

WS 2010/11

Elementare Zahlentheorie

Übungsblatt 8

Abgabe: In den Übungsgruppen am 9.12. und 10.12.

Vermerken Sie bitte auf jeder Abgabe: **Name, Matrikelnummer, Übungsgruppe**
Präsenzübungsblätter können zur Lösung verwendet werden

Aufgabe 1. (Kleiner Fermat nicht umkehrbar) Zeigen Sie: Für $m := 561$ $(= 3 \cdot 11 \cdot 17 \notin \mathbb{P})$ gilt

$$a^{560} \equiv 1 \ (561)$$

für alle $a \in \mathbb{N}$ teilerfremd zu 561.

Integritätsringe

Definition I. Ein Tripel $(R, +, \cdot)$ heißt **kommutativer Ring mit Einselement 1** (kurz: R heißt **K1-Ring**), wenn folgende Axiome gelten. 1) Das Paar $(R, +)$ ist eine **abelsche Gruppe**:

(Abbildung) Das Symbol + bezeichnet eine Abbildung $+ : R \times R \to R$.

(Assoziativgesetz) Für alle Elemente $a, b, c \in R$ gilt

$$(a + b) + c = a + (b + c).$$

(neutrales Element) Es gibt ein Element $n \in R$ (Schreibweise 0) mit der Eigenschaft

$$a + 0 = a, \quad \forall a \in R.$$

(Inverse) Zu jedem Element $a \in R$ gibt es ein Element $b \in R$ (Schreibweise $-a$) mit

$$a + (-a) = 0.$$

(Kommutativgesetz) Für alle Elemente $a, b \in R$ gilt

$$a + b = b + a.$$

2) Für das Paar $(R, \cdot)$ gilt:

(Abbildung) Das Symbol $\cdot$ bezeichnet eine Abbildung $\cdot : R \times R \to R$.

(Assoziativgesetz) Für alle Elemente $a, b, c \in R$ gilt

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(neutrales Element) Es gibt ein Element $e \in R$ (Schreibweise 1) mit der Eigenschaft

$$a \cdot 1 = a, \quad \forall a \in R.$$

(KOMMUTATIVGESETZ) Für alle Elemente $a, b \in R$ gilt

$$a \cdot b = b \cdot a.$$

3) Es gilt $n \neq e$ und es gilt:

(DISTRIBUTIVGESETZ) Für alle Elemente $a, b, c \in R$ gilt

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Definition II. Ein **Integritätsring** ist ein K1-Ring R in dem zusätzlich gilt:

(NULLTEILERFREIHEIT) Aus $a \cdot b = 0$ mit $a, b \in R$ folgt $a = 0$ oder $b = 0$.

Definition und Bemerkung III. Ein Element a eines K1-Ringes R heißt **Nullteiler**, wenn es ein Element $b \neq 0$ in R gibt mit $a \cdot b = 0$. Das Element $a = 0$ ist stets ein Nullteiler und heißt der **triviale Nullteiler**. Ein K1-Ring R ist genau dann ein Integritätsring, wenn 0 der einzige Nullteiler ist.

Aufgabe 2. Es sei R ein K1-Ring und es seien $a, b, c \in R$. Beweisen Sie:
1) Es gibt genau ein Element $x \in R$ mit $x + b = a$, nämlich $x := a + (-b)$.
2) Beide neutrale Elemente 0 und 1 sind eindeutig bestimmt.
3) $a \cdot 0 = 0$, $-(-a) = a$, $(-a) \cdot b = -(a \cdot b)$.
4) Ist R ein Integritätsring, so gilt die **Kürzungsregel**:

$$a \cdot b = a \cdot c \quad \wedge \quad a \neq 0 \qquad \Rightarrow \qquad b = c.$$

Definition IV. Ein **Körper** ist ein K1-Ring R in dem zusätzlich gilt:

(INVERSE) Zu jedem Element $a \in R$, $a \neq 0$, gibt es ein Element $b \in R$ (Schreibweise a^{-1}) mit

$$a \cdot a^{-1} = 1.$$

Aufgabe 3. Beweisen Sie:
1) Es sei R ein Körper und es sei $b \in R$ mit $b \neq 0$. Dann gibt es zu jedem $a \in R$ genau ein Element $x \in R$ mit $x \cdot b = a$, nämlich $x := b^{-1} \cdot a$.
2) Jeder Körper ist ein Integritätsring.

Die K1-Ringe $\mathbb{Z}[\sqrt{m}]$

Definition V. a) Es sei m eine fest vorgegebene ganze Zahl ungleich 0. Auf der Menge

$$R := \mathbb{Z} \times \mathbb{Z} := \{(a, b) \mid a, b \in \mathbb{Z}\}$$

definieren wir zwei Abbildungen $R \times R \to R$ durch

$$(a_0, a_1) + (b_0, b_1) := (a_0 + b_0, a_1 + b_1), \qquad (a_0, a_1) \cdot (b_0, b_1) := (a_0 b_0 + a_1 b_1 m, a_0 b_1 + a_1 b_0).$$

Das Tripel $(R, +, \cdot)$ bezeichnet man mit $\mathbb{Z}[\sqrt{m}]$.
b) Eine ganze Zahl m $(\neq 0)$ heißt **Quadratzahl** falls gilt $m = r^2$ für ein $r \in \mathbb{N}$.
c) Ist $m \in \mathbb{Z}$ keine Quadratzahl, so heißt $\mathbb{Z}[\sqrt{m}]$ der **quadratische Zahlbereich**.
d) Für $m := -1$ schreibt man i anstatt $\sqrt{-1}$ und nennt $\mathbb{Z}[i]$ den **Ring der Gaußschen Zahlen**.

Bemerkung VI. Es ist nützlich die Notation der Elemente von $\mathbb{Z}[\sqrt{m}]$ zu vereinfachen. Da gilt

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1), \qquad (0, 1) \cdot (0, 1) = (m, 0),$$

ist es naheliegend $a \in \mathbb{Z}$ mit $(a, 0) \in R$ zu identifizieren und für das Element $(0, 1) \in R$ das Symbol $\sqrt{m}$ einzuführen. Damit schreibt sich ein Element $(a, b) \in R$ in der Form $a + b\sqrt{m}$ und die komplizierte Formel der Multiplikation $(a, b) \cdot (c, d)$ wird zu einfachem Ausmultiplizieren und somit *unvergesslich*:

$$(a + b\sqrt{m})(c + d\sqrt{m}) = (ac + bdm) + (ad + bc)\sqrt{m}.$$

Aufgabe 4. Es sei $m \in \mathbb{Z}$. Zeigen Sie, daß $\mathbb{Z}[\sqrt{m}]$ ein K1-Ring ist.

Bemerkung VII. Für $m \in \mathbb{Z}$ gilt (siehe Vorlesung):

$$m \text{ ist keine Quadratzahl} \qquad \Leftrightarrow \qquad \mathbb{Z}[\sqrt{m}] \text{ ist ein Integritätsring.}$$

Die Trivialität, daß Quadratzahlen nicht negativ sind wird hier zu einer interessanten Aussage.