Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 11. November 2008

Algebra

5. Übung

Aufgabe 23 Es sei R ein euklidischer Integritätsbereich. Zeige, daß folgende Aussagen für ein Element $u \in R$ äquivalent sind.

(1) Das Element u ist eine Einheit.

(2) Es gilt $\varphi(u) = \varphi(1)$, wobei φ die euklidische Bewertungsfunktion bezeichne.

Aufgabe 24 Es sei R ein Integritätsbereich mit Eins.

(a) Sei R zusätzlich ein Hauptidealring. Setze für $u \in R^\times$ bzw. $x \in R - \{0\}$ irreduzibel

$$\beta_0(u) = 1, \quad \text{bzw.} \quad \beta_0(x) = 2.$$

Zeige, daß diese Abbildung β eine eindeutige und wohldefinierte Fortsetzung zu einer multiplikativen Abbildung

$$\beta : R - \{0\} \to \mathbb{N}$$

besitzt. Welche Eigenschaft eines Hauptidealrings brauchst Du hierfür?

(b) Es sei wieder R ein Hauptidealring und es sei β die in (a) definierte Abbildung auf $R - \{0\}$. Zeige, daß β folgende Eigenschaft hat: Für Ringelemente $x, y \in R - \{0\}$ gilt:

$$\text{Teilt } y \text{ nicht } x, \text{ dann existieren Elemente } a, b \in R \text{ mit } \beta(a \cdot x + b \cdot y) < \beta(y).$$

(c) Zeige, daß für einen Ring R folgende Aussagen äquivalent sind:

(1) Der Ring R ist ein Hauptidealring.

(2) Es existiert eine Funktion β, welche multiplikativ ist und die Eigenschaft aus (b) besitzt.

(3) Es existiert eine Funktion β, welche die Eigenschaft aus (b) besitzt.

Hinweis: *Für die Implikation* $(3) \Rightarrow (1)$ *nutze aus, daß* β *auf einer Menge* $I \subseteq R - \{0\}$ *sein Minimum annehmen muß.*

(d) Folgere direkt aus der Definition eines euklidischen Integritätsbereiches, daß jeder euklidische Integritätsbereich ein Hauptidealring ist, indem Du die Existenz einer Abbildung β nachweist.

Aufgabe 25 Es sei $R = \mathcal{O}_{10} = \{a + \sqrt{10} \cdot b : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ und es sei $N : R \to \mathbb{Z}$, $N(a + \sqrt{10} \cdot b) := a^2 - 10 \cdot b^2$ die multiplikative Normabbildung.

(a) Zeige, daß für ein Element $u \in R$ folgende Aussagen äquivalent sind.

(1) Die Zahl u ist eine Einheit.

(2) Es gilt $N(u) = \pm 1$.

(b) Mache Dir klar, welche Zahlen in $\mathbb{Z}_{10}$ Quadratwurzeln haben.

(c) Zeige, daß die Zahlen $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ irreduzibel in R sind.

(d) Zeige, daß die Zahlen $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ keine Primelemente von R sein können.

(e) Zeige, daß jedes Element $x \in R$ zwar eine Zerlegung in irreduzible Faktoren besitzt, diese aber nicht eindeutig sein braucht. Somit ist R ein nicht faktorieller Ring, obwohl jede Zahl in Irreduzible faktorisiert werden kann.

Aufgabe 26 Modifiziere den Beweis, daß die Ringe $\mathcal{O}_d$ für $d \in \{-2, -1, 2, 3\}$ euklidisch sind derart, daß Du zeigen kannst, daß auch die Ringe $\mathcal{O}_d$ für $d \in \{-11, -7, -3, 5\}$ euklidische Integritätsringe sind[1].
Hinweis: *Mit den gleichen Bezeichnungen wie im Beweis obigen Resultats, wähle* $n \in \mathbb{Z}$ *mit* $\beta := v - \frac{1}{2} \cdot n$ *und* $|\beta| < \frac{1}{4}$, *sowie* $m \in \mathbb{Z}$ *um* $u - \frac{1}{2} \cdot n$ *zu approximieren, d.h.* $|\alpha| \leq \frac{1}{2}$ *und* $\alpha = u - m - \frac{1}{2} \cdot n$. *Weiter betrachte* $q := m + \frac{1}{2} \cdot n(1 + \sqrt{d})$.

Hausübungen

Aufgabe H9 In dieser Aufgabe bereiten wir eine Hilfsaussage für Aufgabe H10 vor.

(a) Sei $\mathbb{K}$ ein endlicher Körper mit ungerader Charakteristik. Zeige, daß es in der Einheitengruppe $\mathbb{K}^\times$ von $\mathbb{K}$ genau ein Element der Ordnung 1 und ein Element der Ordnung 2 gibt. Was geht für gerade Charakteristik schief?

(b) Zeige, daß die folgenden Aussagen für eine ganze Zahl p äquivalent sind.

(1) Die Zahl p ist eine Primzahl.

(2) Der Ring $\mathbb{Z}_p$ ist ein Körper.

(3) Die Zahl p teilt die Zahl $\big((p-1)! + 1\big)$.

Hinweis: *Interpretiere bei* (3) $\Rightarrow$ (1) *die Bedingung als Kongruenz modulo* p *und verwende Teil (a).*

Die Äquivalenz von (1) und (3) ist die Aussage des *Satzes von Wilson.*

Aufgabe H10 In dieser Aufgabe beweisen wir einen Satz aus der Zahlentheorie. Du kannst die Resultate aus Aufgabe 9 zur Bearbeitung dieser Aufgabe als bewiesen annehmen.

(a) Zeige, daß für eine Primzahl $p \in \mathbb{Z}$ mit $p = 4 \cdot k + 1$ für ein $k \in \mathbb{Z}$ folgende Aussage gilt.

$$p \mid (1 + x^2) \quad \text{mit } x = \left(\frac{p-1}{2}\right)!.$$

Hinweis: *Teilt* p *ein Produkt* $x \cdot (2k+r)$, *so auch* $x \cdot (2k + r - 4k - 1) = (-1) \cdot x \cdot (2k + 1 - r))$ *für* $0 < r < 2k + 1$.

(b) Zeige, daß für eine Primzahl $p \in \mathbb{Z}$ folgende Aussagen äquivalent sind.

(1) Es gilt $p = 4 \cdot k + 1$ für ein $k \in \mathbb{Z}$.

(2) Es gilt $2 \neq p = a^2 + b^2$ für geeignete Zahlen $a, b \in \mathbb{Z}$

Freiwilliger Zusatz: Sind die äquivalenten Bedingungen für eine Primzahl p erfüllt, so ist die Darstellung als Summe von Quadratzahlen bis auf Vorzeichen und Reihenfolge von a, b eindeutig.

Hinweis: *Für* (1) $\Rightarrow$ (2) *rechne in* $\mathcal{O}_{-1}$, *für* (2) $\Rightarrow$ (1) *rechne in* $\mathbb{Z}_4$.

[1] Mit gleichen Bezeichnungen kannst Du den Beweis in [Jan], p.88f nachvollziehen.