Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE
UNIVERSITÄT
DARMSTADT

WS 08/09 18. November 2008

Algebra

6. Übung

Aufgabe 27 (Pythagoreische Tripel) In dieser Aufgabe wollen wir alle Lösungen der Gleichung

$$a^2 + b^2 = c^2$$

verstehen. Eine Lösung $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ heißt *pythagoreisches Tripel.*

(a) Zeige, daß jedes pythagoreische Tripel $(\tilde{a}, \tilde{b}, \tilde{c})$ mit $\tilde{a} \neq 0, \tilde{b} \neq 0$ und $\tilde{c} \neq 0$ ein eindeutiges pythagoreisches Tripel (a, b, c) bestimmt, so daß gilt:

(PT1) Die Zahl a ist gerade.

(PT2) $a > 0, b > 0$ und $c > 0$.

(PT3) Der größte gemeinsame Teiler der Zahlen a, b, c ist 1.

– Es gibt ein $d \in \mathbb{Z}$ mit $(\tilde{a}, \tilde{b}, \tilde{c}) \in \{(\pm d \cdot a, \pm d \cdot b, \pm d \cdot c)\}$.

Ein Tripel, welches PT1 - PT3 erfüllt, heißt *primitives pythagoreisches Tripel.*

(b) Zeige, daß in einem primitiven pythagoreischen Tripel (a, b, c) die Zahlen b und c stets ungerade sein müssen.

(c) Zeige, daß für $z \in \mathbb{Q}_{-1}$ folgende Aussagen äquivalent sind:

(1) Für ein $y \in \mathbb{Q}_{-1}$ gilt $z = \frac{y}{\bar{y}}$.

(2) Es gilt $N(z) = 1$.

(d) Es seien $(A, B) \in \mathbb{N} \times \mathbb{N}$ natürliche Zahlen mit $A > B > 0$, $\mathrm{ggT}(A, B) = 1$ und $A \cdot B$ gerade, dann definiert

$$a := 2 \cdot A \cdot B,$$
$$b := A^2 - B^2,$$
$$c := A^2 + B^2$$

ein primitives pythagoreisches Tripel.

(e) Zeige, daß jedes primitive pythagoreische Tripel durch solch eine Wahl von $A > B > 0$ erzeugt wird.
Hinweis: *Berechne die Norm von* $z := \frac{b}{c} + \frac{a}{c} \cdot i$.

Aufgabe 28 Sei $p \in \mathbb{Z}$ eine Primzahl, $S := (p)^C$ das Komplement von (p) in $\mathbb{Z}$ und $Z_{(p)} := S^{-1}\mathbb{Z}$ der Ring der Brüche. Zeige, daß

$$\varphi : \mathbb{Z}_p \to \mathbb{Z}_{(p)}/\left(p \cdot \mathbb{Z}_{(p)}\right), \quad \varphi\left(n + p \cdot \mathbb{Z}\right) := n + p \cdot \mathbb{Z}_{(p)}$$

ein Isomorphismus von Ringen ist.
Hinweis: *Finde zuerst für jedes Element in* $\mathbb{Z}_{(p)}/\left(p \cdot \mathbb{Z}_{(p)}\right)$ *einen ganzzahligen Repräsentanten.*

Aufgabe 29 Wir betrachten den euklidischen Ring $\mathbb{Q}[X]$ der Polynome in X mit rationalen Koeffizienten mit euklidischer Bewertung deg, dem Grad eines Polynoms.

(a) Finde für Polynome f_i und g_i geeignete Polynome q_i und r_i mit $f_i = q_i \cdot g_i + r_i$ und $\deg(r_i) < \deg(g_i)$ oder $r_i = 0$:

$$f_1 = X^5 + 41, \quad g_1 = X - 1,$$

$$f_2 = 3X^4 + 9X^2 + X + 6, \quad g_2 = X^2 + 1.$$

(b) Zerlege das Polynom $f_2 - X$ in irreduzible Faktoren.

(c) Finde einen kommutativen Ring R mit Eins, so daß das Polynom $X^2 - X$ unendlich viele Nullstellen hat.

Aufgabe 30 Zeige, für einen kommutativen Ring R mit Eins sind äquivalent:

(1) Der Ring R besitzt ein eindeutiges Primideal P.

(2) Ein Element $x \in R$ ist entweder eine Einheit oder nilpotent.

(3) Der Ring R besitzt ein minimales Primideal, welches alle Nullteiler enthält und jedes Element $x \in R - \{0\}$ ist entweder eine Einheit oder ein Nullteiler.

Hinweis: (1) $\Rightarrow$ (2) : *Betrachte* $S := \{x, x^2, x^3 ...\}$ *und verwende Aufgabe 20 (b), falls* x *nicht nilpotent war.*
Um in den Nullteilern von R *ein Primideal zu finden, verwende Aufgabe 20 (d).*

Hausübungen

Aufgabe H11 (Zerlegung von Polynomen)

(a) In $\mathbb{Z}_2[X]$ stimmen die Polynome $p := X^2 + X + 1$ und $q := X^3 + X^2 + 1$ als Funktionen auf $\mathbb{Z}_2$ überein. Gilt in $\mathbb{Z}_2[X]$ deshalb $p = q$? Begründe Deine Antwort kurz.

(b) Es sei $p = X^6 - X^2$ und $q = X + 1$ zwei Polynome aus $\mathbb{R}[X]$. Finde eine Zerlegung $p = a \cdot q + b$ mit $a, b \in \mathbb{R}[X]$ und $\deg(b) < \deg(q)$ oder $b = 0$.

(c) Es sei $p = X^3 + X^2 + 1$ und $q = X^2 + 1$ zwei Polynome aus $\mathbb{Z}_2[X]$. Finde eine Zerlegung $p = a \cdot q + b$ mit $a, b \in \mathbb{Z}_2[X]$ und $\deg(b) < \deg(q)$ oder $b = 0$.

(d) Entscheide, ob $X^4 + 1$ in $\mathbb{Q}[X]$ irreduzibel ist.
Hinweis: *Überlege zuerst, warum es ausreicht, für* $a, b, c, d \in \mathbb{Q}$ *den Ansatz*

$$X^4 + 1 = (a \cdot X^2 + b) \cdot (c \cdot X^2 + d)$$

zu untersuchen.

Aufgabe H12 (Ringe der Brüche)

(a) Sei R ein Integritätsbereich und $S \subseteq R$ eine mutliplikativ abgeschlossene Teilmenge. Zeige, daß dann auch $S^{-1}R$ ein Integritätsbreich ist.

(b) Bestimme die Ringe der Brüche $R_1 = S_1^{-1}\mathbb{Z}_6$ und $R_2 = S_2^{-1}\mathbb{Z}_6$ mit $S_1 := \{2, 4\}$ und $S_2 := \{1, 5\}$.