Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 18. November 2008

Algebra

6. Übung mit Lösungshinweisen

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* $z := \frac{b}{c} + \frac{a}{c} \cdot i$.

LÖSUNG: (a) Sind a und b ungerade, so gilt $c^2 = a^2 + b^2 \equiv 2 \mod 4$, also wäre c^2 keine Quadratzahl. Somit muß eine der Zahlen a, b gerade sein. O.B.d.A ist a gerade.
Da $a^2 = (-a)^2$ gilt, reicht es, sich positive Zahlen a, b, c anzuschauen.
Ist (a, b, c) ein pythagoreisches Tripel und $d = \mathrm{ggT}(a, b, c)$, so ist d ein Teiler von a, also teilt d^2 auch a^2. Da d auch b und c teilt, erhalten wir, daß $a^2 + b^2 = c^2 \Leftrightarrow d^2(r^2 + s^2) = d^2t^2$ für $a = d \cdot r, b = d \cdot s$ und $c = d \cdot t$. Damit ist das Tripel lediglich ein gestrecktes teilerfremdes Tripel.

(b) Sind a^2 und b^2 gerade, so auch c^2, also sind a, b, c gerade und das Tripel ist nicht mehr primitiv. Analog können a^2 und c^2 in einem primitiven pythagoreischen Tripel nicht gleichzeitig gerade sein.

(c) Die Richtung (1) $\Rightarrow$ (2) ist sofort durch Ausrechnen der multiplikativen Norm klar. Für die Rückrichtung unterscheiden wir zwei Fälle. Ist $z = -1$, dann folgt

$$z = \frac{i}{-i}.$$

Ist $z \neq -1$, dann folgt mit $N(z) = 1$

$$z \cdot (1 + \overline{z}) = z + z \cdot \overline{z} = 1 + z.$$

Somit gilt

$$z = \frac{1+z}{1+\overline{z}}$$

und mit $y = 1 + z$ folgt die Aussage.

(d) Nachrechnen liefert sofort die Aussage.

(e) Da $N(z) = 1$ ist, gilt

$$\frac{b}{c} + \frac{a}{c} \cdot i = \frac{\alpha + \beta \cdot i}{\alpha - \beta \cdot i} = \frac{\alpha^2 - \beta^2}{\alpha^2 + \beta^2} + \frac{2\alpha\beta}{\alpha^2 + \beta^2} \cdot i.$$

Durch geeignetes Erweitern von α und β erhalten wir positive ganzzahlige und teilerfremde Zahlen A und B mit

$$\frac{b}{c} + \frac{a}{c} \cdot i = \frac{A + B \cdot i}{A - B \cdot i} = \frac{A^2 - B^2}{A^2 + B^2} + \frac{2AB}{A^2 + B^2} \cdot i.$$

Nun klappern wir die Bedingungen ab.
Da $\frac{b}{c} > 0$ ist auch $A^2 - B^2 > 0$, also $A > B$.
Wären A und B gleichzeitig ungerade, so wäre $A^2 + B^2$ durch 2 teilbar und der Bruch

$$\frac{2 \cdot A \cdot B}{A^2 + B^2}$$

wäre durch 2 kürzbar. Vollständig gekürzt stünde im Zähler nun ein Teiler von $A \cdot B$ und dieser wäre ungerade, also auch a, also (a, b, c) kein primitives pythagoreisches Tripel.

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.*

Lösung: Betrachte $x \in \mathbb{Z}_{(p)} / \left(p \cdot \mathbb{Z}_{(p)}\right)$ mit Repräsentant $\frac{a}{b}$. Da p und b teilerfremd sind, existiert eine Lösung der Gleichung

$$m \cdot b + n \cdot p = a.$$

Somit folgt

$$\frac{a}{b} - \frac{n \cdot p}{b} = -m,$$

also besitzt x einen ganzzahligen Repräsentanten.
Nun betrachten wir φ. Der Ring $\mathbb{Z}_{(p)} / \left(p \cdot \mathbb{Z}_{(p)}\right)$ hat Charakteristik p und da $p \cdot \mathbb{Z}_{(p)}$ ein echtes Ideal ist, ist der Quotient nicht der Nullring. Somit enhält der Quotientenring eine isomorphe Kopie von $\mathbb{Z}_p$, welche von der Äquivalenzklasse der 1 erzeugt wird. Aus obiger Argumentation ist weiter klar, daß jedes Element des Quotientenringes einen Repräsentanten in diesem Unterring hat, also ist der Quotient isomorph zu $\mathbb{Z}_p$ und obige Abbildung φ ein Ismorphismus.

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.

LÖSUNG: (a) Mittels Polynomdivision oder anderen Verfahren erhalten wir

$$X^5 + 41 = (X^4 + X^3 + X^2 + X + 1)(X - 1) + 42$$

und

$$3X^4 + 9X^2 + X + 6 = (3X^2 + 6)(X^2 + 1) + X.$$

(b) Das Produkt $(3X^2+6)(X^2+1)$ ist ein Produkt irreduzibler Elemente, denn X^2+1 und X^2+2 haben in $\mathbb{Q}$ keine Nullstelle. Somit können sie nicht in Polynome von Grad 1 faktorisieren.

(c) Wir betrachten $R = \prod_{n\in\mathbb{N}} \mathbb{Z}_2$, dann ist jedes Element Nullstelle von $X^2 - X$, insbesondere hat das Polynom unendlich viele Nullstellen.

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).*

LÖSUNG: (1) $\Rightarrow$ (2) Sei $x \in R$ keine Einheit. Entweder ist x nilpotent, dann ist nichts zu zeigen, oder x ist nicht nilpotent. In diesem Fall ist die Menge $S := \{x, x^2, x^3, x^4, ...\}$ eine multiplikativ abgeschlossene Menge, welche die Null nicht enthält. Somit existiert in S^C nach Aufgabe 20 ein Primideal.
Andererseits ist (P, x) ein Ideal, welches größer ist, als P, P muß aber maximal sein, denn, da $1 \in R$, gäbe es sonst ein maximales echt größeres Ideal und dieses wäre ein Primideal, also folgt $x \in P$ und somit $S \subseteq P$. Damit erhalten wir aber ein Primideal in R, welches nicht mit P übereinstimmt, nämlich das Primideal in S^C, so ein Fall kann aber nach Vorraussetzung nicht auftreten.
(2) $\Rightarrow$ (3) Nach Aufgabe 20 existiert ein Primideal in den Nullteilern. Wir brauchen nur zu zeigen, daß jede Nicht-Einheit in P liegt. Dies folgt für $a \in (R^\times)^C$ leicht aus

$$0 = a^n \in P \Rightarrow a \in P.$$

Somit liegt $a \in P$, da a eine beliebige Nicht-Einheit war, folgt die Behauptung.
(3) $\Rightarrow$ (1) Das minimale Primideal ist gleichzeitig maximales Ideal, da jedes echt größere Ideal eine Einheit enthält und damit mit ganz R übereinstimmt.

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.

Lösung: (a) Der Polynomring ist so konstruiert, daß die angegeben Elemente unterschiedlich sind. Das die Auswertungshomomorphismen Polynome nicht unterscheiden können, ist hier klar, da $\mathbb{Z}_2$ nur endlich viele Elemente, $\mathbb{Z}_2[X]$ aber unendlich viele Elemente besitzt. Die endlich vielen Auswertungsabbildungen können demnach nicht punktetrennend sein.

(b) Polynomdivision liefert $X^6 - X^2 = (X^5 - X^4 + X^3 - X^2)(X + 1) + 0$.

(c) Polynomdivision liefert $X^3 + X^2 + 1 = (X + 1)(X^2 + 1) + X$.

(d) Wir stellen fest, daß $X^4 + 1$ keine Nullstelle in $\mathbb{Q}$ hat, also kann kein Linearfaktor $X - a$ das Polynom teilen, und damit ist es entweder irreduzibel oder in ein Produkt zweier Polynome vom Grad 2 zerlegbar. Somit brauchen wir nur den zweiten Fall auszuschliessen, um die Irreduzibilität nachzuweisen.
Leider war der Hinweis nicht glücklich formuliert, auch wenn der nun bestrittene Weg ihn verwendet.
Ausrechnen liefert

$$X^4 + 1 = (a \cdot X^2 + b) \cdot (c \cdot X^2 + d) = ac \cdot X^4 + (ad + bc) \cdot X^2 + bd.$$

Koeffizientenvergleich liefert

$$ac = bd = 1 \quad \text{und} \quad ad + bc = 0.$$

Nun erhalten wir aus

$$1 = ac = \frac{acd}{d} = -\frac{bc^2}{d} = -\frac{bdc^2}{d^2} = -\frac{c^2}{d^2}.$$

Diese Gleichung hat aber in $\mathbb{Q}$ keine Lösung, also kann solch eine Zerlegung nicht existieren. Wir brauchen nun nur noch den allgemeinen Fall

$$X^4 + 1 = (\lambda X^2 + aX + b)(\mu X^2 + cX + d)$$

auszuschliessen. Wir stellen zuerst fest, daß wir $\lambda = 1$ wählen dürfen, indem wir λ aus dem linken Faktor ausklammern und in den rechten Faktor reinrechnen. Somit erhalten wir oBdA das äquivalente Problem, ob die Zerlegung

$$X^4 + 1 = (X^2 + aX + b)(\mu X^2 + cX + d)$$

existiert. Ausrechnen der rechten Seite liefert mit Koeffizientenvergleich folgende Gleichungen:

$$\begin{aligned} \mu &= 1, \\ a+c &= 0, \\ b+ac+d &= 0, \\ ad+bc &= 0, \\ bd &= 1. \end{aligned}$$

Da a und c nicht beide verschwinden, können wir oBdA a als invertierbar annehmen, denn andernfalls befänden wir uns im Fall des Hinweises. Wir lösen auf:

$$\begin{aligned} a &= -c, \\ d = -ac - b &= a^2 - b, \\ d = -\frac{bc}{a} = b \cdot \frac{a}{a} &= b. \end{aligned}$$

Somit erhalten wir

$$a^2 - b = b \Leftrightarrow a^2 = 2b^2.$$

Weiter erhalten wir aus $b = d$ und $bd = 1$ die Gleichung

$$b^2 = d^2 = 1,$$

also $b = \pm 1$ und

$$a^2 = 2.$$

Diese Gleichung ist jedoch in $\mathbb{Q}$ nicht lösbar.
Somit haben wir alle Fälle in eine Produktzerlegung des Polynoms $X^4 + 1$ in Polynome von Grad größer 0 ausgeschlossen, also ist $X^4 + 1$ irreduzibel in $\mathbb{Q}[X]$.

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 $S_2 := \{1, 5\}$.

LÖSUNG: (a) Sind $x, y \in S^{-1}R$, dann gilt mit $x = \frac{a}{b}$ und $y = \frac{c}{d}$:

$$\frac{ac}{bd} \sim 0 \Leftrightarrow s \cdot ac = 0$$

für ein $s \in S$. Da $0 \notin S$, folgt $ac = 0$, also $a = 0$ oder $c = 0$. Damit ist entweder $x = 0$ oder $y = 0$, also ist $S^{-1}R$ ein Integritätsring.

(b) Im ersten Fall erhalten wir folgende drei Äquivalenzklassen

$$[0] := \left\{\frac{0}{2}, \frac{3}{2}, \frac{0}{4}, \frac{3}{4}\right\},$$

$$[2] := \left\{\frac{1}{2}, \frac{4}{2}, \frac{2}{4}, \frac{5}{4}\right\},$$

$$[1] := \left\{\frac{2}{2}, \frac{5}{2}, \frac{1}{4}, \frac{4}{4}\right\}.$$

Prüfe noch nach, daß diese Äquivalenzklassen eine zu $\mathbb{Z}_3$ isomorphe Ringstruktur tragen. Im zweiten Fall erhalten wir einen zu $\mathbb{Z}_6$ isomorphen Ring, da alle Elemente aus S_2 bereits in $\mathbb{Z}_6$ invertierbar waren. Wir erhalten somit

$$[0] := \left\{ \frac{0}{1}, \frac{0}{5} \right\},$$

$$[1] := \left\{ \frac{1}{1}, \frac{5}{5} \right\},$$

$$[2] := \left\{ \frac{2}{1}, \frac{4}{5} \right\},$$

$$[3] := \left\{ \frac{3}{1}, \frac{3}{5} \right\},$$

$$[4] := \left\{ \frac{4}{1}, \frac{2}{5} \right\},$$

$$[5] := \left\{ \frac{5}{1}, \frac{1}{5} \right\}.$$

Diese Elemente tragen die durch die Notation suggerierte Struktur.