Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 11. November 2008

Algebra

5. Übung mit Lösungshinweisen

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.

LÖSUNG: (1) $\Rightarrow$ (2) Sei u eine Einheit. Dann folgt aus der Eigenschaft der Bewertung

$$\varphi(u) = \varphi(u \cdot 1) \geq \varphi(1) = \varphi(u \cdot u^{-1}) \geq \varphi(u).$$

(2) $\Rightarrow$ (1) Gilt umgekehrt $\varphi(u) = \varphi(1)$, so existiert eine Darstellung

$$1 = a \cdot u + b,$$

wobei b entweder gleich 0 ist, woraus die Aussage folgt, oder die Bewertung auf b einen kleineren Wert annimmt, als auf u. Dies kann aber nicht sein, da $\varphi(u) = \varphi(1)$ und für alle $x \in R$ gilt $\varphi(x) = \varphi(x \cdot 1) \geq \varphi(1)$.

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.

LÖSUNG: (a) Wir wissen, daß Hauptidealringe faktoriell sind. Somit ist die Abbildung wohldefiniert, da bis auf Assoziiertheit die Zerlegung in Irreduzible eindeutig ist, und der Wert von β auf Grund der Multiplikativität für assoziierte Elemente gleich ist. Weiter existiert der Wert von β nach genau dieser Argumentation für alle Elemente ungleich Null.
Solch ein β ist in jedem faktoriellen Ring definierbar, allerdings wird in faktoriellen Ringen nicht unbedingt die Eigenschaft aus (b) gültig bleiben.

(b) Betrachte das Ideal (x, y) in R. Auf Grund der Hauptidealeigenschaft existiert ein $z \in R$ mit $(z) = (x, y)$. Wir zeigen, daß für x, y mit y teilt nicht x dieses z der Kandidat ist, denn $z = a \cdot x + b \cdot y$, da $(z) = (x, y)$.
1. Fall: x teilt y, dann besitzt y mindestens einen irreduziblen Faktor mehr als x, also folgt $\beta(y) > \beta(x) = \beta(1 \cdot x + 0 \cdot y)$ und wir sind fertig.
2. Fall: x teilt y nicht, dann ist z weder in (x) noch in (y), also folgt $y = r \cdot z$ für ein $r \in R$, welches keine Einheit ist. Damit besitzt y mindestens einen irreduziblen Faktor mehr als z, woraus $\beta(y) > \beta(z)$ folgt. Da $(z) = (a, b)$ gilt, folgt die Aussage, denn z ist von der Form $a \cdot x + b \cdot y$.

(c) (1) $\Rightarrow$ (2) Diese Richtung ist in (a) und (b) gezeigt worden. (2) $\Rightarrow$ (3) Das ist offensichtlich. (3) $\Rightarrow$ (1) Sei I ein Ideal in R. Wir müssen zeigen, daß es ein Element $z \in R$ gibt mit $I = (z)$. Wie im Beweis, daß euklidische Ringe Hauptidealringe sind, nutzen wir, daß es ein Element $r \in I - \{0\}$ gibt, auf welchem β minimal wird unter allen Elementen aus $I - \{0\}$. Alle Elemente, die von diesem r geteilt werden, liegen in (r). Ist $s \in I - \{0\}$, so daß r das Element s nicht teilt, dann erhalten wir, daß es Ringelemente $a, b \in R$ gibt mit $\beta(a \cdot s + b \cdot r) < \beta(r)$. Da $a \cdot s + b \cdot r$ wieder im Ideal liegt, nimmt β offensichtlich nicht auf r sein Minimum an, ein Widerspruch nach Wahl von r. Somit kommt dieser Fall nie vor, und wir erhalten $I = (r)$.

(d) Ist φ die euklidische Bewertung, dann setze $\beta := \varphi$, wobei β nur auf $R - \{0\}$ definiert sei. Sind nun $x, y \in R$, so folgt aus der Eigenschaft, daß R euklidisch ist:

$$x = b \cdot y + z,$$

wobei $\varphi(z) < \varphi(y)$ oder $z = 0$ gilt. Teilt nun y nicht x, so ist $z \neq 0$, also folgt mit $z = 1 \cdot x - b \cdot y$ die Existenz eines Elements mit $\beta(z) < \beta(y)$. Damit folgt sofort, daß R ein Hauptidealring ist.
Natürlich braucht die auf R existierende Abbildung β aus (2) nichts mit der euklidischen Bewertung zu tun haben, diese hat in der Regel nicht die Eigenschaft, multiplikativ zu sein oder die Anzahl der irreduziblen Faktoren multiplikativ zu zählen.

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.

LÖSUNG: (a) (1) $\Rightarrow$ (2) Aus der Multiplikativität der Norm folgt, $N(u)$ ist in $\mathbb{Z}$ invertierbar, also gilt $N(u) = \pm 1$. (2) $\Rightarrow$ (1) Ist $N(u) = N(a+b\cdot\sqrt{10}) = 1$, so folgt $(a+b\cdot\sqrt{10})\cdot(a-b\cdot\sqrt{10}) = 1$. Somit steht das Inverse von u direkt da. Ist $N(u) = -1$, so ist $(a + b \cdot \sqrt{10}) \cdot (a - b \cdot \sqrt{10})^2$ das offensichtliche Inverse.

(b) Ausrechnen der 9 Quadrate in $\mathbb{Z}_{10}$ liefert, daß Quadratzahlen immer auf $0, 1, 4, 5, 6$ oder 9 enden. Somit haben diese Elemente in $\mathbb{Z}_{10}$ Quadratwurzeln, alle anderen nicht.

(c) Ausrechnen der Norm liefert $N(2) = 4$, $N(3) = 9$ und $N(4 + \sqrt{10}) = N(4 - \sqrt{10}) = 6$. Wir zeigen exemplarisch, warum $4 + \sqrt{10}$ irreduzibel sein muß, alle anderen Fälle laufen analog. Ist $4 + \sqrt{10}$ reduzibel, so existieren Zahlen $a, b \in R$ mit $a \cdot b = 4 + \sqrt{10}$, wobei weder a noch b eine Einheit wäre. Damit muß aber $N(a) \neq 1$ und $N(b) \neq 1$ gelten. Somit folgt $6 = N(a \cdot b) = N(a) \cdot N(b)$, also $N(a) \in \{\pm 2, \pm 3\}$. Dies kann aber nicht sein, da weder 2 noch 3 noch 8 in $\mathbb{Z}_{10}$ Quadratzahlen sind, denn wir sehen leicht den Widerspruch:

$$N(a) = (a_1 + \sqrt{10} \cdot a_2) \cdot (a_1 - \sqrt{10} \cdot a_2) = a_1^2 - 10a_2^2 \equiv a_1^2 \mod 10.$$

(d) Nachrechnen liefert $2 \cdot 3 = 6 = (4 + \sqrt{10}) \cdot (4 - \sqrt{10})$. Offensichtlich teilen die 4 Zahlen die 6 aber 2 oder 3 teilen keinen Faktor von $(4 + \sqrt{10}) \cdot (4 - \sqrt{10})$. der Rest der Argumentation läuft analog.

(e) Wir beobachten, daß für ein nicht irreduzibles Element $r \in R$ mit Produktdarstellung $r = a \cdot b$ auch gilt $N(r) = N(a) \cdot N(b)$ und weiter gilt $\max\{|N(a)|, |N(b)|\} < |N(r)|$. Da eine ganze Zahl nicht beliebig oft faktorisiert werden kann durch Faktoren ungleich ± 1 folgt daraus die Behauptung, beachte (a) und $2 \cdot 3 = 6 = (4 + \sqrt{10}) \cdot (4 - \sqrt{10})$.

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 $q := m + \frac{1}{2} \cdot n(1 + \sqrt{d})$.*

LÖSUNG: Seien $z, w \in \mathcal{O}_d$ mit $w \neq 0$. Dann gilt in $\mathbb{Q}_d$:

$$z \cdot w^{-1} = u + v \cdot \sqrt{d} \text{ mit } u, v \in \mathbb{Q}.$$

Wähle nun eine ganze Zahl $n \in \mathbb{Z}$, so daß für folgendes β die Ungleichung $|\beta| \leq \frac{1}{4}$ gilt:

$$\beta := v - \frac{1}{2} \cdot n.$$

Wähle weiter ein $m \in \mathbb{Z}$, um

$$u - \frac{1}{2} \cdot n$$

zu approximieren, d.h. so daß gilt

$$|\alpha| \leq \frac{1}{2}$$

für

$$\alpha := u - m - \frac{1}{2} \cdot n.$$

Setze

$$q := m + \frac{1}{2} \cdot n \cdot (1 + \sqrt{d}),$$

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

dann gilt

$$z = w \cdot q + r,$$

wobei

$$r = w \cdot (\alpha + \beta \cdot \sqrt{d})$$

gilt. Entweder ist $r = 0$ oder wir erhalten eine Abschätzung

$$\begin{aligned} |N(r)| &= |N(w)| \cdot |N(\alpha - \beta \cdot \sqrt{d})| \\ &= |N(w)| \cdot |\alpha^2 - d \cdot \beta^2| \\ &< |N(w)|, \end{aligned}$$

da wir die Abschätzung

$$|\alpha^2 - d \cdot \beta^2| \leq \frac{1}{4} + \frac{11}{16} < 1$$

aus $|d| \leq 11$ folgern.

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) ⇒ (1) *die Bedingung als Kongruenz modulo p und verwende Teil (a).*

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

LÖSUNG: (a) Für ein Element der Ordnung 1 gilt $x^1 = 1$, also $x = 1$. Jedes Element der Ordnung 2 erfüllt $x^2 = 1$, also

$$0 = x^2 - 1 = (x - 1) \cdot (x + 1).$$

Damit ist -1 das einzige Element mit Ordnung 2, sofern $1 \neq -1$ gilt. Dies ist aber in allen Körpern ungerader Charakteristik erfüllt. Besitzt $\mathbb{K}$ Charakteristik 2, so gilt $1 = -1$, also gibt es kein Element der Ordnung 2, denn das Polynom $x^2 - 1$ hat hier in 1 eine doppelte Nullstelle.

(b) (1) ⇔ (2) Das sollten wir bereits wissen, denn Z_p ist genau dann ein Integritätsbereich, wenn p prim ist.
(2) ⇒ (3) Ist $p = 2$, so stimmt die Aussage offensichtlich. Ist $p > 2$, so ist die Charakteristik von $\mathbb{Z}_p$ ungerade, also besitzt die Einheitengruppe von Z_p genau ein einziges Element der Ordnung 2, nämlich -1. Somit gilt in $\mathbb{Z}_p$:

$$(p-1)! = \prod_{n \in \mathbb{Z}^\times} n = (-1) \cdot \prod_{n \in \mathbb{Z}^\times, n \neq \pm 1} n.$$

Da nun aber jedes Element im Produkt auch mit seinem Inversen multipliziert wird (Elemente sind genau dann in einer Gruppe selbstinvers, wenn ihre Ordnung die 2 teilt), ist das große Produkt rechts gleich 1 und wir erhalten

$$(p-1)! = -1.$$

Das ist äquivalent zu

$$(p-1)! + 1 \equiv 0 \mod p \text{ in } \mathbb{Z},$$

also teilt p die Zahl $(p-1)!+1$.
(3) $\Rightarrow$ (1) Ist p keine Primzahl, so besitzt p einen echten Teiler $m \in \mathbb{Z}$ mit $m < p$. Dieser kommt als Faktor in der Fakultät $(p-1)!$ vor, also teilt m die Zahl $(p-1)!$ und m teilt p. Damit kann p aber nicht die Zahl $(p-1)!+1$ teilen, da m nicht die 1 teilt. Somit folgt die Behauptung.

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 $\mathbb{Z}_4$.*

LÖSUNG: (a) Wir wissen nach Aufgabe H9, daß p die Zahl $(p-1)!+1$ teilt. Nach obigem Hinweis, zerfällt unsere Fakultät wie folgt:

$$\begin{aligned}
(p-1)! &= (4k)! = \prod_{n=1}^{2k} n \cdot \prod_{n=2k+1}^{4k} n \\
&\equiv \prod_{n=1}^{2k} n \cdot \prod_{n=2k+1}^{4k} (n-4k-1) \mod p \\
&\equiv \prod_{n=1}^{2k} n \cdot \prod_{n=2k+1}^{4k} (-1) \cdot (4k+1-n) \mod p \\
&\equiv (-1)^{2k} \cdot \prod_{n=1}^{2k} n \cdot \prod_{n=1}^{2k} n \mod p \\
&\equiv (-1)^{2k} \cdot \left(\prod_{n=1}^{2k} n\right)^2 \mod p \\
&\equiv 1 \cdot [(2k)!]^2 \mod p \\
&\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \mod p.
\end{aligned}$$

Da $(p-1)! \equiv -1 \mod p$ bekannt ist, folgt die Behauptung.
(1) $\Rightarrow$ (2) Da p eine Primzahl der Form $4k+1$ ist, teilt p die Zahl $1+x^2$ wie in (a). Somit folgt in $\mathcal{O}_{-1}$:

$$(1+x^2) = (1+i\cdot x)\cdot(1-i\cdot x).$$

Damit teilt p zwar das Produkt der rechten Seite, aber keinen der beiden Faktoren. Somit ist p im Ring der gaußchen Zahlen kein Primelement, also kein irreduzibles Element (Beachte, daß $\mathcal{O}_{-1}$ euklidisch, also insbesondere faktoriell ist). Es gibt somit eine Darstellung

$$p = (l+i\cdot m)\cdot(u+i\cdot v)$$

als Produkt von Nicht-Einheiten. Mit der Normabbildung erhalten wir somit

$$p^2 = N((l+i\cdot m)\cdot(u+i\cdot v)) = N(l+i\cdot m)\cdot N(u+i\cdot v).$$

Da die Norm genau dann 1 ist, wenn das Element eine Einheit ist, muß gelten

$$p = N(l+i\cdot m) = l^2+m^2$$

und der Satz ist gezeigt.
(2) $\Rightarrow$ (1) Damit p eine Primzahl ist, dürfen nicht beide Summanden gerade oder beide Summanden ungerade sein. Damit ist genau ein Summand gerade. Damit ist ein Summand durch 2 teilbar, also auch durch 4 teilbar, da die Summanden Quadratzahlen waren und 2 in $\mathbb{Z}$ ein Primelement ist. Rechnen wir modulo 4, verschwindet somit die gerade Quadratzahl. Die ungerade Quadratzahl ist natürlich auch modulo 4 ein Quadrat in $\mathbb{Z}_4$, mit $3^2 \equiv 1 \mod 4$ folgt die Behauptung, denn 3 ist keine Quadratzahl in $\mathbb{Z}_4$.
Der Zusatz folgt aus folgendem Argument: Die Norm von $(l+i\cdot m)$ ist eine Primzahl in $\mathbb{Z}$, also ist $(l+i\cdot m)$ prim in $\mathbb{Z}[i]$. Da weiter gilt

$$(l+i\cdot m)\cdot(l-i\cdot m) = (u+i\cdot v)\cdot(u-i\cdot v)$$

folgt, daß beide Seiten bis auf Assoziiertheit die gleichen Primelemente, also die gleichen irreduzible Faktoren, stehen haben, da $\mathcal{O}_{-1}$ ein faktorieller Ring ist. Damit ist die Wahl von l und m bis auf Vorzeichen und Vertauschen der Rolle von m und l eindeutig.