Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 4. November 2008

Algebra

4. Übung mit Lösungshinweisen

Aufgabe 18 Es sei R ein faktorieller Ring. Zeige, daß jedes irreduzible Element $x \in R$ ein Primelement ist.

LÖSUNG: Sei x ein irreduzibles Element in R. Es teile zudem x das Produkt $a \cdot b$ mit $a, b \in R$, also $a \cdot b = x \cdot r$ für ein $r \in R$. Wir wissen, a, b und r haben eine bis auf Assoziiertheit eindeutige Darstellung als Produkt irreduzibler Elemente, also

$$a = \prod_{i=1}^{k} y_i^{e_i}, \quad b = \prod_{i=1}^{m} z_i^{f_i} \quad \text{und } r = \prod_{i=1}^{n} r_i^{g_i}.$$

Somit folgt

$$a \cdot b = \left(\prod_{i=1}^{k} y_i^{e_i}\right) \cdot \left(\prod_{i=1}^{m} z_i^{f_i}\right) = x \cdot r = x \cdot \left(\prod_{i=1}^{n} r_k^{g_k}\right).$$

Da aber die irreduziblen Faktoren bis auf eine Permutation assoziiert sein müssen, gilt also ist $x \approx y_d$ oder $x \approx z_d$ für ein $d \in \mathbb{N}$. Damit teilt x aber entweder a oder b und die Behauptung folgt.

Aufgabe 19 Bestimme in $\mathbb{Z}_8$ alle Einheiten, Primelemente und irreduziblen Elemente.

LÖSUNG: Am Einfachsten schreibt man sich die Multiplikationstabelle in $\mathbb{Z}_8$ auf.
Die Einheiten sind die Elemente $\{1, 3, 5, 7\}$, denn jede nicht durch 2 teilbare Zahl ist in $\mathbb{Z}_8$ invertierbar. Weiter ist die Einheitenmenge eine Gruppe, isomorph zu $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
Die Primelemente sind die Elemente $\{2, 6\}$, denn keine gerade Zahl in $\mathbb{Z}_8$ ist Produkt ungerader Zahlen und es gilt $6 = 2 \cdot 3$.
Die irreduziblen Elemente sind $\{2, 6\}$, denn jedes Produkt aus 2 nicht Einheiten ist durch 4 teilbar oder 0.

Aufgabe 20 Es sei R ein kommutativer Ring mit Eins. Wir wollen zeigen, daß in R die Menge

$$\mathcal{N} := \{x \in R : x \text{ ist ein Nullteiler oder } x = 0\}$$

ein Primideal enthält.

(a) Sei $P \subseteq R$ ein Primideal. Zeige, daß die Menge

$$S := \{x \in R : x \notin P\} = P^C$$

multiplikativ abgeschlossen ist, also

$$a \in S, b \in S \Rightarrow a \cdot b \in S.$$

(b) Sei umgekehrt $S \subseteq R$ multiplikativ abgeschlossen und es sei $P \subseteq R$ ein Ideal mit $P \subseteq S^C$, welches maximal ist unter allen Idealen im Komplement von S, dann ist P ein Primideal.

(c) Zeige, daß in R die Menge aller Nicht-Nullteiler S multiplikativ abgeschlossen ist und daß die Menge S^C ein Ideal von R enthält.

(d) Zeige nun die Behauptung.

LÖSUNG: (a) Dies ist lediglich eine Umformulierung der Primidealeigenschaft.

(b) Sei $a \cdot b \in P$, aber $a \notin P$ und $b \notin P$. Dann sind $I := (P, a)$ und $J := (P, b)$ echt größere Ideale als P, also enthalten I und J Elemente aus S. Somit finden wir in S Elemente der Form

$$i = p_1 + r \cdot a \quad \text{ und } j = p_2 + s \cdot b.$$

Damit folgt aus der multiplikativen Abgeschlossenheit von S:

$$i \cdot j = p_1 \cdot p_2 + p_1 \cdot s \cdot b + p_2 \cdot r \cdot a + r \cdot a \cdot s \cdot b \in S.$$

Offensichtlich ist jedoch jeder Summand ein Element des Ideals P, also folgt $i \cdot j \in P$, ein Widerspruch. Somit muß P ein Primideal gewesen sein.

(c) Ist b kein Nullteiler und $a \in R$, so ist $a \cdot b \neq 0$. Ist weiter $a \cdot b$ ein Nullteiler, so gibt es ein $x \in R$ mit $a \cdot b \cdot x = 0$, also muß a ein Nullteiler sein. Somit kann das Produkt von Nicht-Nullteilern kein Nullteiler sein, also ist besagte Menge mutliplikativ abgeschlossen. Die Menge (0) ist offensichtlich ein Ideal, welches in S^C liegt.

(d) Ist I ein Ideal in S^C und

$$I \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq S^C$$

eine Kette von Idealen, welche ganz im Komplement von S liegen, so ist

$$\bigcup_{n \in \mathbb{N}} I_n$$

ein Ideal und eine obere Schranke der Kette, welche I enthält und in S^C liegt. Folglich ist die Menge aller Ideale in S^C nicht leer und besitzt ein maximales Element. Dieses ist nach (b) ein Primideal, woraus die Behauptung folgt.

Aufgabe 21 Sei R ein kommutativer Ring und $S \subseteq R$ eine Teilmenge. Die Menge S heißt *gesättigt*, falls aus $x \in S$ und $x = a \cdot b$ folgt, daß $a \in S$ und $b \in S$ gilt. Enthält eine gesättigte Teilmenge eines Rings ein Element, dann auch jeden Teiler des Elementes.
Wir verschärfen das Resultat aus Aufgabe 20 (b). Zeige, daß folgende Aussagen für einen kommutativen Ring äquivalent sind:

(1) Die Menge $S \subseteq R$ ist eine gesättigte und multiplikativ abgeschlossene Teilmenge.

(2) Die Menge S^C ist die Vereinigung von Primidealen in R.

Hinweis: Zeige, daß unter der Vorraussetzung aus (1) mit $x \in S^C$ auch $(x) \subseteq S^C$ gilt.

LÖSUNG: (1) $\Rightarrow$ (2) Ist $x \in S^C$, so ist $r \cdot x \in S^C$ für jedes $r \in R$, denn andernfalls, wäre $r \cdot x \in S$, so auch r und x. Somit können wir ein maximales Ideal in S^C finden, welches (x) enthält und dieses ist prim. Damit, da $x \in S^C$ beliebig war, folgt die Behauptung.
(2) $\Rightarrow$ (1) Diese Implikation ist leicht, denn der Schnitt multiplikativ abgeschlossener Teilmengen ist wieder multiplikativ abgeschlossen.

Aufgabe 22

(a) Zeige, daß für einen kommutativen Ring R mit Eins folgende Aussagen äquivalent sind.

(1) Ist $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ eine aufsteigende Kette von Idealen in R, so gibt es ein $n_0 \in \mathbb{N}$ mit $I_n = I_{n_0}$ für alle $n > n_0$.

(2) In jeder nicht leeren Teilmenge von Idealen in R gibt es bezüglich der Inklusionsordnung ein maximales Element.

(3) Jedes Ideal I in R ist endlich erzeugbar, es gibt also $a_1, ..., a_n \in R$ mit $I = (a_1, ..., a_n)$.

Wir sagen auch, eine Kette mit der Eigenschaft in (1) wird *stationär* und nennen einen kommutativen Ring mit Eins, der obige Eigenschaften hat, *noethersch*.
Einen nicht kommutativen Ring nennen wir *noethersch*, wenn jedes Linksideal endlich erzeugbar ist.

(b) Zeige, daß jeder kommutative Hauptidealring ein noetherscher Ring ist.

(c) Finde ein Beispiel für einen nicht noetherschen kommutativen Ring R mit Eins. Gib ein Ideal in R an, welches nicht endlich erzeugbar ist.

LÖSUNG: (a) (1) $\Rightarrow$ (2) Ist M eine Menge von Idealen, welche kein maximales Element enthält, so gibt es Ideale $I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq ...$, wobei jede Inklusion echt ist. Somit erhalten wir eine Kette, welche nicht stationär wird.
(2) $\Rightarrow$ (3) Sei $I \subseteq R$ ein Ideal und es sei M die Menge aller Ideale in R, welche endlich erzeugbar sind und in I enthalten sind. Dann ist diese Menge M nicht leer, also existiert ein maximales Element J. Ist $a \in I$, so ist $J + (a)$ ein Ideal, welches J enthält, in I enthalten ist und $J + (a)$ ist endlich erzeugbar. Aus der Maximalität von J folgt $I = J$, also ist I endlich erzeugbar.
(3) $\Rightarrow$ (1) Ist $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ eine aufsteigende Kette von Idealen, so ist auch $I := \bigcup_{n\in\mathbb{N}} I_n$ ein Ideal in R. Nach Vorraussetzung ist I endlich erzeugbar, also $I = (a_1, ..., a_m)$. Weiter existiert zu jedem $1 \leq i \leq m$ ein $n_i \in \mathbb{N}$ mit $a_i \in I_{n_i}$. Es sei n das Maximum der Menge $\{n_{i_1}, ..., n_{i_m}\}$, dann gilt $I = I_n$ und die Kette wird stationär.

(b) Jedes Ideal eines kommutativen Hauptidealringes ist von einem Element, also insbesondere endlich, erzeugbar.

(c) Betrachte $R := \prod_{n\in\mathbb{N}} \mathbb{Z}$. Dieser Ring ist nicht noethersch, denn die Kette

$$0 \times 0 \times 0 \times ... \subseteq \mathbb{Z} \times 0 \times 0 \times ... \subseteq \mathbb{Z} \times \mathbb{Z} \times 0 \times 0 \times ...$$

wird nicht stationär.
Das Ideal aller Folgen von Zahlen, die nur endlich viele Einträge ungleich Null besitzen, ist ein nicht endlich erzeugbares Ideal. Dies ist eine obere Schranke für obige aufsteigende Folge von Idealen.

Hausübungen

Aufgabe H7 Es sei a ein ganzzahliger Parameter. Gibt es eine ganze Zahl $b \in \mathbb{Z}$, so daß $b-1$ durch 3 teilbar, $b-3$ durch 4 teilbar und $b-a$ durch 5 teilbar ist? Wenn ja, bestimme für $a = 2$ und $a = 4$ die kleinste positive ganze Zahl mit dieser Eigenschaft.

LÖSUNG: Wir haben folgendes System von Kongruenzen:

$$\begin{aligned} b &\equiv 1 \mod 3 \\ b &\equiv 3 \mod 4 \\ b &\equiv a \mod 5 \end{aligned}$$

Da die Zahlen $3, 4, 5$ paarweise ggT 1 haben, sind die Vorraussetzungen für den chinesischen Restsatz erfüllt. Wir basteln:

$$\begin{aligned} N &= 3 \cdot 4 \cdot 5 = 60 \\ N_3 &= 4 \cdot 5 = 20 \\ N_4 &= 3 \cdot 5 = 15 \\ N_5 &= 3 \cdot 4 = 12. \end{aligned}$$

Weiter lösen wir die Kongruenzen

$$\begin{aligned} 20 \cdot x_3 = N_3 \cdot x_3 &\equiv 1 \mod 3 \\ 15 \cdot x_4 = N_4 \cdot x_4 &\equiv 1 \mod 4 \\ 12 \cdot x_5 = N_5 \cdot x_5 &\equiv 1 \mod 5 \end{aligned}$$

mit Lösungen $x_3 = 2, x_4 = 3$ und $x_5 = 3$. Wir erhalten

$$\begin{aligned} b &= 1 \cdot N_3 \cdot x_3 + 3 \cdot N_4 \cdot x_4 + a \cdot N_5 \cdot x_5 \\ &= 40 + 135 + 36 \cdot a \\ &= 175 + 36 \cdot a. \end{aligned}$$

Da b bis auf $N \cdot \mathbb{Z} = 60 \cdot \mathbb{Z}$ eindeutig bestimmt ist, erhalten wir für $a = 2$ die Lösung $b = 7$ und $a = 4$ die Lösung $b = 19$.

Aufgabe H8 Es sei R ein faktorieller Ring und $a, b, c, d, x \in R$.

(a) Sind a und b teilerfremd, so gilt $a|bc \Rightarrow a|c$.

(b) Ist $d \neq 0$, so gibt es nur endlich viele Hauptideale (x) in R mit $(d) \subseteq (x)$.

LÖSUNG: (a) Ist $a \cdot x = b \cdot c$, so existiert eine bis auf Assoziiertheit und Permutation eindeutige Zerlegung in ein Produkt irreduzibler Elemente von $a \cdot x$ und $b \cdot c$. Analog zu den Überlegungen in der Gruppenübung müssen alle Faktoren der Produktdarstellung von a in der Produktdarstellung von $b \cdot c$ und damit von c mit mindestens dem gleichen Exponenten vorkommen. Somit folgt die Behauptung.

(b) Die Aussage $(d) \subseteq (x)$ ist äquivalent zu x teilt d. Angenommen, wir haben für jedes $i \in \mathbb{N}$ die Inklusion $(d) \subseteq (a_i)$ für oBdA irreduzible und paarweise nicht assoziierte $a_i \in R$, dann ist jedes a_i ein Faktor der Produktdarstellung von d, welche endlich ist, ein Widerspruch. Somit kann es keine unendliche Menge irreduzibler Elemente geben.
Da die Menge aller irreduziblen Teiler von d endlich ist, ist auch die Menge aller Produkte dieser irreduziblen Teiler bis auf Assoziiertheit endlich und es folgt die Aussage.
