Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 2. Dezember 2008

Algebra

8. Übung mit Lösungshinweisen

Aufgabe 36

(a) Zeige, daß $\mathbb{Z}[X]$ kein Hauptidealring ist.

(b) Sei R ein Integritätsbereich und $c \in R$ irreduzibel. Zeige, daß $R[X]$ kein Hauptidealring ist.

(c) Zeige, daß für jeden Körper $\mathbb{K}$ der Polynomring in $n \in \mathbb{N}$ Unbestimmten $\mathbb{K}[X_1, ..., X_n]$ für $n > 1$ kein Hauptidealring ist.

LÖSUNG: Da diese Aufgabe nur ein Spezialfall von Aufgabe 31 ist, könnten wir diese Aufgabe vollständig lösen, indem wir zeigen, daß Körper keine irreduziblen Elemente enthalten können. Allerdings schadet es auch nicht, den konkreten Grund für das Scheitern der Hauptidealeigenschaft in den angegebenen Fällen zu kennen. Gerade die Aussage aus (c) ist nicht uninteressant.

(a) Wir betrachten das Ideal $I := (X, 2)$ in $\mathbb{Z}[X]$. Dieses Ideal ist nicht von einem Element erzeugbar. Angenommen, es gilt

$$I = (z),$$

dann hätten wir zum einen ein Element $a \in \mathbb{Z}[X]$ mit $a \cdot z = X$, also, da X irreduzibel ist, gilt $z = \pm 1$ und $a = X$, dann wäre aber $I = \mathbb{Z}[X]$, was falsch ist, oder es gilt $a = \pm 1$ und $z = X$.
Da jedoch nun aus $\deg(b \cdot X) \geq \deg(X) = 1$ folgt, daß die Gleichung $b \cdot X = 2$ keine Lösung haben kann, kann (X) nicht mit I übereinstimmen, also ist I kein Hauptideal.

(b) Der Beweis funktioniert analog zu Teil (a), nur daß wir in der Argumentation $\mathbb{Z}$ durch R und 2 durch c ersetzen müssen.

(c) Da in $R := \mathbb{K}[X_1, ..., X_n]$ für jedes $1 \leq m \leq n$ und je zwei Polynome $f, g \in R$ die Gleichung

$$\deg_m(f \cdot g) = \deg_m(f) + \deg_m(g)$$

gilt, können wir leicht zeigen, daß X_1 und X_2 irreduzible Elemente in R sind. Hierbei bezeichnet $\deg_m(f)$ den Grad von f bezüglich X_m.
Angenommen es gilt

$$X_1 = f \cdot g,$$

dann gilt

$$1 = \deg_1(X_1) = \deg_1(f \cdot g) = \deg_1(f) + \deg_1(g),$$

also ist das eine Polynom des Produkts vom Grad 1 und das andere vom Grad 0 in X_1.
Aus

$$0 = \deg_m(X_1) = \deg_m(f) + \deg_m(g)$$

für $2 \leq m \leq n$ folgt, daß f und g Grad 0 in X_m haben müssen. Also ist eines der Polynome eine Einheit, da es in allen Variablen Grad 0 hat. Somit ist aber X_1 irreduzibel. Völlig analog

folgt, daß auch X_2 ein irreduzibles Element ist.
Betrachten wir nun $I := (X_1, X_2)$, so kann dieses Ideal kein Hauptideal eines Elementes $z \in R$ sein, denn wir haben einen Isomorphismus

$$R = (\mathbb{K}[X_1, X_3, ..., X_n])[X_2].$$

Mit $c = X_1$, Integritätsbereich $\mathbb{K}[X_1, X_3, ..., X_n]$ und Variable X_2 folgt mit (b) die Behauptung.

Aufgabe 37 Bestimme alle irreduziblen Polynome

(a) in $\mathbb{C}[X]$.

(b) in $\mathbb{R}[X]$.

(c) in $\mathbb{Z}_2[X]$ bis Grad 4.

LÖSUNG: (a) Alle Polynome vom Grad 0 sind Einheiten, also nicht irreduzibel. Alle Polynome vom Grad 1 sind, da $\mathbb{C}$ ein Körper ist, irreduzibel. Alle Polynome vom Grad $n > 1$ haben n (möglicherweise gleiche) Nullstellen und zerfallen in ein Produkt aus n Linearfaktoren, die irreduzibel sind. Somit können Polynome vom Grad $n > 1$ nicht irreduzibel sein.

(b) Alle Polynome vom Grad 0 sind Einheiten, also nicht irreduzibel. Alle Polynome vom Grad 1 sind, da $\mathbb{R}$ ein Körper ist, irreduzibel. Polynome vom Grad $2n + 1$ für $n > 0$ haben nach dem Zwischenwertsatz eine Nullstelle, sind demnach nicht irreduzibel.
Wir betrachten zunächst alle Polynome vom Grad $2n$ mit $n > 1$. Wir wollen einsehen, warum diese Polynome nicht irreduzibel sein können. Sei also f ein reelles Polynom vom Grad $2n$. Dieses zerfällt in $\mathbb{C}$ in $2n$ Linearfaktoren, da es $2n$ Nullstellen hat. Hat es eine reelle Nullstelle, so ist es bereits nicht irreduzibel. Hat es keine reelle Nullstelle, so sind alle Nullstellen imaginär. Sei $\lambda \in \mathbb{C} - \mathbb{R}$ eine Nullstelle von f, dann folgt

$$f(\overline{\lambda}) = \sum_{k=0}^{2n} a_k \cdot \overline{\lambda^k} = \sum_{k=0}^{2n} \overline{a_k \cdot \lambda^k} = \overline{\sum_{k=0}^{2n} a_k \cdot \lambda^n} = \overline{f(\lambda)} = 0,$$

somit ist auch $\overline{\lambda}$ eine Nullstelle von f und es gilt $\lambda \neq \overline{\lambda}$. Wir erhalten somit für f komplexe Nullstellen

$$\lambda_1, \overline{\lambda_1}, ..., \lambda_n, \overline{\lambda_n}$$

und eine Produktdarstellung

$$f = \prod_{i=1}^{n} \left((X - \lambda_i) \cdot (X - \overline{\lambda_i}) \right).$$

Ausmultiplizieren der inneren Terme liefert

$$f = \prod_{i=1}^{n} \left((X - \lambda_i) \cdot (X - \overline{\lambda_i}) \right) = \prod_{i=1}^{n} \left(X^2 - 2 \cdot \Re(\lambda_i) \cdot X + |\lambda_i|^2 \right).$$

Damit haben wir aber eine Zerlegung von f in ein Produkt aus rellen Polynomen, welche keine Einheiten sind, also war f nicht irreduzibel.
Wir brauchen also nur noch Polynome vom Grad 2 auf Irreduzibiltät zu prüfen. Dabei stellen wir fest, daß ein Polynom $f(X) = aX^2 + bX + c$ genau dann irreduzibel ist, wenn es keine reelle Nullstelle hat. Nach der guten aus der Schule bekannten abc-Formel ist das genau dann der Fall, wenn

$$b^2 - 4ac < 0$$

gilt.

(c) Eine gute Strategie ist es, alle Produkte von Polynomen mit Produktgrad kleiner 5 auszurechnen. Da es nur 32 solcher Polynome gibt, ist das etwas mühsam, aber in endlicher Zeit durchführbar.
Folgende Polynome stellen sich als die Irreduziblen heraus:

$$X, \quad X+1,$$

$$X^2+X+1,$$

$$X^3+X+1, \quad X^3+X^2+1,$$

$$X^4+X+1, \quad X^4+X^3+1 \quad \text{und} \quad X^4+X^3+X^2+X+1.$$

Aufgabe 38 Zeige mittels eines geeigneten Kriteriums, daß folgende Polynome in $\mathbb{Q}[X]$ irreduzibel sind. Welche dieser Polynome sind auch in $\mathbb{Z}[X]$ irreduzibel?

$$\begin{aligned} f_1(X) &= X^2-2X+2, \\ f_2(X) &= 3X^2-9X-27, \\ f_3(X) &= X^4-6X^3+12X^2-3X+9, \\ f_4(X) &= 5X^4-42X^3-42X+42. \end{aligned}$$

Lösung: Nach Eisenstein ist für die Wahl von $p=2$ das Polynom f_1 irreduzibel in $\mathbb{Q}[X]$ und, da es primitiv ist, auch in $\mathbb{Z}[X]$.
Reduktion modulo 2 des Polynoms f_2 liefert X^2+X+1, was in $\mathbb{Z}_2[X]$ irreduzibel ist nach voriger Aufgabe. Somit ist f_2 in $\mathbb{Q}[X]$ irreduzibel, aber nicht in $\mathbb{Z}[X]$, da es nicht primitiv ist.
Reduktion modulo 2 des Polynoms f_3 liefert X^4+X+1, ein in $\mathbb{Z}_2[X]$ irreduzibles Polynom. Also ist f_3 als primitives Polynom irreduzibel in $\mathbb{Q}[X]$ und $\mathbb{Z}[X]$.
Nach Eisenstein für $p=2$, $p=3$ oder $p=7$ ist f_4 irreduzibel in $\mathbb{Q}[X]$ und als primitives Polynom auch in $\mathbb{Z}[X]$.

Aufgabe 39 Es sei $\mathbb{K}$ ein Körper. Zeige mit dem Kriterium von Eisenstein, daß im Polynomring in 2 Unbestimmten $\mathbb{K}[X,Y]$ das Polynom

$$f(X,Y) := Y^3 + X^2 \cdot Y^2 + X^3 \cdot Y + X$$

irreduzibel ist.
Hinweis: *Die Ringe* $\mathbb{K}[X,Y]$ *und* $(\mathbb{K}[X])[Y]$ *sind isomorph.*

Lösung: Wir wissen, daß X ein irreduzibles Element im faktoriellen Ring $\mathbb{K}[X,Y]$ ist. Weiter teilt X in $(\mathbb{K}[X])[Y]$ nicht den führenden Koeffizienten, alle anderen Koeffizienten und X^2 teilt nicht den Koeffizienten mit Y^0. Bezeichnet $\mathbb{K}(X)$ den Quotientenkörper von $\mathbb{K}[X]$, so ist f irreduzibel in $\mathbb{K}(X)[Y]$ und, da es primitiv ist, sogar in $(\mathbb{K}[X])[Y] \cong \mathbb{K}[X,Y]$.

Aufgabe 40 Sei $\mathbb{K}$ ein endlicher Körper. Zeige, daß dann $|\mathbb{K}| = p^n$ für eine Primzahl p und ein $n \geq 1$ gilt.

Lösung: Wir wissen, daß $\mathbb{K}$ ein Vektorraum über seinem Primkörper P ist. Da $\mathbb{K}$ endlich ist, muß zum einen der Primkörper endlich sein, als auch die Dimension von $\mathbb{K}$ über P. Somit setze $p = |P|$ und $n := \dim_P(\mathbb{K})$.

Hausübungen

Aufgabe H15 (Automorphismen von Polynomringen) Sei $\mathbb{K}$ ein Körper und sei $c \in \mathbb{K}$ ein beliebiges Element.

(a) Zeige, daß jeder Ringautomorphismus $\Phi : \mathbb{K}[X] \to \mathbb{K}[X]$ irreduzible Polynome auf irreduzible Polynome abbildet.

(b) Zeige, daß die Abbildung

$$\Phi_c : \mathbb{K}[X] \to \mathbb{K}[X], \quad \Phi_c(f(X)) = \Phi_c\left(\sum_{k=0}^{\deg(f)} a_k \cdot X^k\right) := \sum_{k=0}^{\deg(f)} a_k \cdot (X-c)^k$$

ein Ringautomorphismus ist.

(c) Zeige, daß das Polynom

$$f(X) = \sum_{k=0}^{p-1} X^k = X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Q}[X]$$

für $p \in \mathbb{N}$ prim ein irreduzibles Polynom ist.
Hinweis: *In Teil (c) steht eine endliche geometrische Reihe.*

Lösung: (a) Ist Φ ein Automorphismus, f irreduzibel und $\Phi(f) = g \cdot h$, so gilt $\Phi^{-1}(\Phi(f)) = \Phi^{-1}(g) \cdot \Phi^{-1}(h)$, also ist entweder $\Phi^{-1}(g)$ oder $\Phi^{-1}(h)$ eine Einheit, also ist entweder g oder h eine Einheit, also ist auch $\Phi(f)$ irreduzibel.

(b) Wir rechnen nur die Multiplikativität nach, der Rest ist quasi klar. Sei $f(X) = \sum_{i=0}^{m} a_i X^i$ und $g = \sum_{j=0}^{n} b_j X^j$, dann folgt

$$\begin{aligned}
\Phi_c(f(X)) \cdot \Phi_c(g(X)) &= \left(\sum_{i=0}^{m} a_i \cdot (X-c)^i\right) \cdot \left(\sum_{j=0}^{n} b_j \cdot (X-c)^j\right) \\
&= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) \cdot (X-c)^k \\
&= \sum_{k=0}^{m+n} \Phi_c\left(\left(\sum_{i=0}^{k} a_i b_{k-i}\right) \cdot X^k\right) \\
&= \Phi_c(f(X) \cdot g(X)).
\end{aligned}$$

Da die Inverse von Φ_c offensichtlich durch den Homomorphismus Φ_{-c} gegeben ist, folgt die Behauptung.

(c) Wir erhalten durch die Formel für die endliche geometrische Reihe

$$f(X) = \frac{X^p - 1}{X - 1}.$$

Betrachten wir $\Phi_{-1}(f(X))$, so erhalten wir

$$f(X+1) = \frac{(X+1)^p - 1}{X}.$$

Mit der Verallgemeinerung der binomischen Formel sehen wir

$$\begin{aligned} f(X+1) &= \frac{1}{X} \cdot \left(\left(\sum_{k=0}^{p} \binom{p}{k} X^k \right) - 1 \right) \\ &= \frac{1}{X} \cdot \left(\sum_{k=1}^{p} \binom{p}{k} X^k \right) \\ &= \sum_{k=1}^{p} \binom{p}{k} X^{k-1}. \end{aligned}$$

Nun ist dies ein normiertes Polynom mit konstantem Term p und jeder Koeffizient ist, da dieser ein Binomialkoeffizient mit p ist, durch p teilbar. Somit ist nach Eisenstein dieses Polynom und damit f irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$.

Aufgabe H16 (Die Grenzen des Reduktionsverfahrens) Wir wissen bereits, daß $f(X) = X^4 + 1 \in \mathbb{Q}[X]$ ein irreduzibles Polynom ist. Als primitives Polynom ist es somit auch in $\mathbb{Z}[X]$ irreduzibel. Wir wollen zeigen, daß für jede Primzahl p das reduzierte Polynom $f(X) = X^4 + 1 \in \mathbb{Z}_p[X]$ nicht irreduzibel ist.
Sei $p \in \mathbb{Z}$ eine Primzahl. Zeige:

(a) Gibt es ein $a \in \mathbb{Z}_p[X]$ mit $a^2 = -1$, dann ist $f \in \mathbb{Z}_p[X]$ nicht irreduzibel.

(b) Gibt es ein $b \in \mathbb{Z}_p[X]$ mit $b^2 = 2$, dann ist $f \in \mathbb{Z}_p[X]$ nicht irreduzibel.

(c) Gibt es ein $c \in \mathbb{Z}_p[X]$ mit $c^2 = -2$, dann ist $f \in \mathbb{Z}_p[X]$ nicht irreduzibel.

(d) In $\mathbb{Z}_p$ ist mindestens eine der drei Zahlen $-2, -1, 2$ eine Quadratzahl.

Somit gibt es Polynome in $\mathbb{Z}[X]$, welche nicht mit dem Reduktionskriterium als irreduzibel erkannt werden können, obwohl sie irreduzibel sind.

Hinweis: *In den Teilen (a),(b) und (c) ist es möglich, f als Produkt zweier normierter Polynome vom Grad 2 zu schreiben.*

LÖSUNG: (a) Wir rechnen aus:

$$\begin{aligned} (X^2 - a)(X^2 + a) &= X^4 + (a - a)X^2 - a^2 \\ &= X^4 + 1. \end{aligned}$$

Somit ist $X^4 + 1$ nicht irreduzibel.

(b) Wir rechnen aus:

$$\begin{aligned} (X^2 - bX + 1)(X^2 + bX + 1) &= X^4 + (b - b)X^3 + (1 + 1 - b^2)X^2 + (b - b)X + 1 \\ &= X^4 + 1. \end{aligned}$$

Somit ist $X^4 + 1$ nicht irreduzibel.

(c) Wir rechnen aus:

$$\begin{aligned} (X^2 - cX - 1)(X^2 + cX - 1) &= X^4 + (c - c)X^3 + (-1 - 1 - c^2)X^2 + (c - c)X + 1 \\ &= X^4 + 1. \end{aligned}$$

Somit ist $X^4 + 1$ nicht irreduzibel.

(d) Wir wissen, die Einheitengruppe von $\mathbb{Z}_p$ ist zyklisch. Somit gibt es einen Erzeuger c und Exponenten $r, s \in \mathbb{N}$ mit

$$-1 = c^r \quad \text{und} \quad 2 = c^s.$$

Da nun gilt

$$-2 = c^{r+s},$$

muß mindestens einer der auftretenden drei Exponenten gerade sein, also ist eine der drei Zahlen auf jedem Fall ein Quadrat. Somit folgt die Behauptung.