Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Dr. Peter Ullrich
Dmytro Chibisov

SS 2005
Übungsblatt 3
27. April 2005

Algorithmische Algebra I

Abgabe: 4. Mai, in der Vorlesung, MI 00.04.011

Aufgabe 1
Sei R ein Ring. Bezeichne mit $\tilde{R}$ die Menge aller Folgen $(a_i)_{i\in\mathbb{N}_0}$, so dass nur endlich viele Folgenglieder von 0 verschieden sind, d.h. es existiere eine endliche Menge $I \subset \mathbb{N}_0$ mit $a_i = 0$ für alle $i \in \mathbb{N}_0 \backslash I$. Auf $\tilde{R}$ seien wie folgt Verknüpfungen gegeben:

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i + b_i)_{i\in\mathbb{N}_0}$$

$$(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} = (c_i)_{i\in\mathbb{N}_0}, \text{ wobei } c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

Zeigen Sie:

(a) $(\tilde{R}, +, \cdot)$ ist ein kommutativer Ring mit 1; es ist $\tilde{R} = R[x]$ der Polynomring in X über R

(b) Sei $X = (x_i)$, wobei $x_1 = 1$ und $x_i = 0$ für alle $i \neq 1$. Dann hat jedes $f \in \tilde{R}$ eine eindeutige Darstellung der Form $f = \sum_i a_i X^i$ mit $a_i \in R$, wobei $a(b_i) = (ab_i)$ für $a \in R$ und $b_i \in \tilde{R}$ definiert ist. (Beachte: Die Summe ist hier nicht formal definiert, sondern die Addition in $\tilde{R}$.)

Aufgabe 2
In der Vorlesung wurde gezeigt, dass $\mathbb{Z}$ und $\mathbb{Q}[X]$ Hauptidealringe sind. In dieser Aufgabe soll nun gezeigt werden, dass es Ringe gibt, die nicht Hauptidealringe sind Dazu betrachten wir den Ring $R = \mathbb{Q}[X,Y]$ aller Polynome in zwei Unbestimmten X, Y mit Koeffizienten in $\mathbb{Q}$. Zeigen Sie, dass R kein Hauptidealring ist. (Hinweis: Betrachten Sie das Ideal $I = (X, Y)$)

Aufgabe 3
Sei $R = k[x]$ ein Polynomring (k Körper) und y eine neue Variable. Zeigen Sie, dass im Polynomring $R[y]$ gilt: Seien $f, g \in R[y]$ Polynome, $g \neq 0$ normiert, d.h. $g = y^n + a_{n-1}y^{n-1} + ... + a_0$, $a_i \in R$, so existieren eindeutige $q, r \in R[y]$ mit

1. $f = qg + r$
2. $deg(r) < deg(g)$

Aufgabe 4

Sei $I = \{f \in \mathbb{F}_2[x,y] \mid f(a,b) = 0 \ \forall a,b \in \mathbb{F}_2\}$. Ziel dieser Aufgabe ist zu zeigen, dass $I = \langle x^2 - x, y^2 - y\rangle$ gilt.

(a) Zeigen Sie : I ist ein Ideal von $\mathbb{F}_2[x,y]$.

(b) Zeigen Sie, dass jedes Polynom $f \in \mathbb{F}_2[x,y]$ in der Form $f = A(x^2-x)+B(y^2-y)+axy+bx+cy+d$ dargestellt werden kann, wobei $A, B \in \mathbb{F}_2[x,y]$ und $a,b,c,d \in \mathbb{F}_2$. Hinweis: Benutzen Sie Polynomdivision aus Aufgabe 3.

(c) Zeigen Sie, dass $axy + bx + cy + d \in I$ genau dann gilt, wenn $a = b = c = d = 0$ ist.

(d) Zeigen Sie nun $I = \langle x^2 - x, y^2 - y\rangle$.

(e) Stellen Sie $x^2y + y^2x$ als lineare Kombination von $x^2 - x$ und $y^2 - y$ mit Koeffizienten in $\mathbb{F}_2[x,y]$ dar. Hinweis: $2 = 1 + 1 = 0$ in $\mathbb{F}_2$.