Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Dr. Peter Ullrich
Dipl.Math. Dipl.-Ing. Thomas Bayer

SS 2003
Übungsblatt 6
27. Mai 2003

Algorithmische Algebra II

Abgabe: 2. Juni, in der Übung, MI03.09.011B

Es seien $R = k[X_1, \ldots, X_n]$ ein Polynomring (k ein Körper), und $>$ eine monomiale Ordnung auf R^q.

Aufgabe 1

Der Ring $k[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]$ der *Laurent-Polynome* ist definiert als die Menge aller formalen (endlichen) Summen $\sum_{\alpha \in \mathbb{Z}^m} c_\alpha X^\alpha$, $c_\alpha \in k$ (für fast alle α ist $c_\alpha = 0$), wobei Addition und Multiplikation defininiert sind wie im Polynomring, d.h. $\sum_\alpha c_\alpha X^\alpha + \sum_\alpha d_\alpha X^\alpha = \sum_\alpha (c_\alpha + d_\alpha) X^\alpha$ und $\sum_\alpha c_\alpha X^\alpha \cdot \sum_\beta d_\beta X^\beta = \sum_\gamma e_\gamma X^\gamma$ mit $e_\gamma = \sum_{\alpha+\beta=\gamma} c_\alpha d_\beta$. (Z.B. ist $f = X^2 Y^{-3} + X^{-1}$ ein Laurent-Polynom).
Durch die Abbildung $k \to k[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]$, die jedem $c \in k$ das konstante Laurent Polynom cX^0 zuordnet, wird $k[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]$ zu einer k-Algebra. Zeigen Sie, dass folgende k-Algebrenhomomorphismen bijektiv sind. Zeigen Sie insbesondere: Zu jedem Monom X^β, ($\beta \in \mathbb{Z}^m$) gibt es $\alpha \in \mathbb{N}^m$ und $e \in \mathbb{N}$ (bzw. $e_1, \ldots, e_m \in \mathbb{N}$) mit $\psi(t^e X^\alpha \bmod I) = X^\beta$ (bzw. $\chi(t_1^{e_1} \cdots t_m^{e_m} X^\alpha \bmod J) = X^\beta$).

(i) $\psi : k[X_1, \ldots, X_m, t]/I \to k[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]$, $X_i \bmod I \mapsto X_i$ $(i = 1, \ldots, m)$ und $t \bmod I \mapsto X_1^{-1} \cdots X_m^{-1}$, wobei I das von $tX_1 \cdots X_m - 1$ im Polynomring $k[X_1, \ldots, X_m, t]$ erzeugte Ideal ist.

(ii) $\chi : k[X_1, \ldots, X_m, t_1, \ldots, t_m]/J \to k[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]$, $X_i \bmod J \mapsto X_i$, $t_i \bmod J \mapsto X_i^{-1}$ $(i = 1, \ldots, m)$, wobei J das von $t_1 X_1 - 1, \ldots, t_m X_m - 1$ in $k[X_1, \ldots, X_m, t_1, \ldots, t_m]$ erzeugte Ideal ist.

Aufgabe 2

Sei $k[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]$ der Ring der Laurent-Polynome (vgl. Aufgabe 1), und seien $A = (a_{ij}) \in M(m \times n, \mathbb{Z})$, $b = (b_i) \in \mathbb{Z}^m$. Wir suchen nach Lösungen $\alpha \in \mathbb{N}^n$ der linearen Diophantischen Gleichung $A\alpha = b$. Bisher (vgl. A3, Blatt 3) mussten die Koeffizienten von A und b auf nicht-negative ganze Zahlen beschränkt werden. In dieser Aufgabe soll nun gezeigt werden, wie der allgemeine Fall gelöst werden kann.

(i) Definiere einen Homomorphismus $\varphi : k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_m, t]$ wie folgt: Wähle (nach A1(i)) $e_j \in \mathbb{N}$ und $a'_{ij} \in \mathbb{N}$ mit $\psi(t^{e_j} \prod_i X_i^{a'_{ij}} \bmod I) = \prod_i X_i^{a_{ij}}$ (ψ wie in A1(i))

und setze $\varphi(Y_j) = t^{e_j} \prod_i X_i^{a'_{ij}}$ $(j = 1, \ldots, n)$. Wähle zudem $e \in \mathbb{N}$ und $b' = (b'_j) \in \mathbb{N}^m$ mit $\psi(t^e X^{b'} \bmod I) = X^b$. Dann gilt für ein $\alpha \in \mathbb{N}^n$:

$$A\alpha = b \qquad \Longleftrightarrow \qquad \varphi(Y^\alpha) \equiv t^e X^{b'} \bmod I, \ (\text{d.h. } \varphi(Y^\alpha) - t^e X^{b'} \in I)$$

mit $I = (tX_1 \cdots X_m - 1) \subset k[X_1, \ldots, X_m, t]$.

(ii) Seien $\varphi : k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_m, t]$ der Homomorphismus, $I \subset k[X_1, \ldots, X_m, t]$ das Ideal aus (i) und $f_j = \varphi(Y_j)$, $(j = 1, \ldots, n)$. Sei $>$ eine monomiale Ordnung auf $\mathbb{M}(X_1, \ldots, X_m, t, Y_1, \ldots, Y_n)$, so dass jedes Monom, welches mindestens ein X_i oder t enthält größer ist, als jedes Monom in $Y_1, \ldots, Y_n$. Sei G eine Gröbner Basis des Ideals $J = (tX_1 \cdots X_m - 1, Y_1 - f_1, \ldots, Y_n - f_n)$ von $k[X_1, \ldots, X_m, t, Y_1, \ldots, Y_n]$ bzgl. $>$, und sei $f \in k[X_1, \ldots, X_m, t] \subset k[X_1, \ldots, X_m, t, Y_1, \ldots, Y_n]$. Zeigen Sie:

$$\exists\ g \in k[Y_1, \ldots, Y_n] \text{ mit } \varphi(g) \equiv f \bmod I \iff \overline{f}^G \in k[Y_1, \ldots, Y_n].$$

Ist dies der Fall, so gilt $\varphi(g) \equiv f \bmod I$ mit $g = \overline{f}^G$.

(iii) Mit den Bezeichnungen aus (i) und (ii) gilt nun:

$$A\alpha = b \text{ hat eine Lösung } \alpha \in \mathbb{N}^n \qquad \Longleftrightarrow \qquad g = \overline{f}^G \in k[Y_1, \ldots, Y_n] \text{ mit } f = t^e X^{b'}.$$

Ist dies der Fall, so ist $g = \overline{f}^G$ von der Form $g = Y^\alpha$, und α ist eine Lösung.

(iv) Es gelten die Bezeichnungen von (i) und (ii). Sei $\ell(\alpha) = \sum_i c_i \alpha_i$ die lineare Abbildung definiert durch $(c_1, \ldots, c_n) \in \mathbb{N}^n$. Es sei $>$ eine monomiale Ordnung auf $\mathbb{M}(X_1, \ldots, X_m, t, Y_1, \ldots, Y_n)$ wie in (ii) mit der zusätzlichen Eigenschaft, dass für alle $\alpha, \beta \in \mathbb{N}^n$ mit $\varphi(Y^\alpha) \equiv \varphi(Y^\beta) \bmod I$ und $\ell(\alpha) > \ell(\beta)$ gilt: $Y^\alpha > Y^\beta$. Zeigen Sie: Ist G eine Gröbner Basis von J bzgl. $>$ und $g = \overline{f}^G \in k[Y_1, \ldots, Y_n]$ mit $f = t^e X^{b'}$, so ist $\alpha = \text{multideg}(g)$ eine Lösung von $A\alpha = b$, die ℓ minimiert.

(v) Finde eine Lösung $\alpha = (\alpha_1, \ldots, \alpha_4) \in \mathbb{N}^4$ von

$$\begin{aligned} 3\alpha_1 - 2\alpha_2 + \alpha_3 &= -1 \\ 4\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 &= 5 \end{aligned}$$

die $\ell(\alpha) = \alpha_1 + 1000\alpha_2 + \alpha_3 + 100\alpha_4$ minimiert.

Aufgabe 3

Sei $0 \neq U$ ein R-Untermodul von R^q, und sei $V = \text{span}_R\text{LT}(U) (= \text{span}_R\text{LM}(U))$. Zeigen Sie:

(i) $\text{LM}(U) = \text{LM}(V)$.

(ii) Die Abbildung $\text{span}_k B_U \to R^q/V$, $\bar{r} \mapsto \bar{r} \bmod V$ ist ein Isomorphismus von k-Vektorräumen. $(B_U = \{\bar{M} : \bar{M} \notin \text{LM}(U)\})$.