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

SS 2003
Übungsblatt 3
7. Mai 2003

Algorithmische Algebra II

Abgabe: 12. Mai, in der Übung, MI03.09.011B

Aufgabe 1

Ein Polynome $f \in k[X_1, \ldots, X_n]$ heißt *Binom*, wenn f von der Form $f = cX^\alpha + dX^\beta$ $(c, d \in k,\ \alpha, \beta \in \mathbb{N}^n)$ ist.

(i) Sind f, g Binome, so ist auch das S-Polynom $S(f, g)$ ein Binom.

(ii) Ist f ein Binom und G ein m-Tupel von Binomen, so ist auch der Rest $\overline{f}^G$ der Division von f duch G ein Binom.

(iii) Sei $I = (f_1, \ldots, f_q)$ ein Ideal, das von Binomen $f_1, \ldots, f_q$ erzeugt wird (I heißt dann ein *binomiales Ideal*). Dann besteht die reduzierte Gröbner Basis von I ausschließlich aus Binomen. (Hinweis: Benutze (i), (ii) und den Buchberger-Algorithmus)

(iv) Sei $I \subset k[X_1, \ldots, X_n]$ ein binomiales Ideal (siehe (iii)) und $f = X^\alpha$ ein Monom. Dann ist die Normalform $\mathrm{NF}_{I,\sigma}(f)$ (siehe Satz/Def. 3.2.1) von f bzgl. I (und einer fixierten monomialen Ordnung σ) von der Form dX^β, $d \in k,\ \beta \in \mathbb{N}^n$.

Aufgabe 2

Sei $\varphi : k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_m]$ ein Ringhomomorphismus mit $\varphi(a) = a$ für alle $a \in k$, d.h. φ ist ein k-Algebrenhomomorphismus. Es sei $\varphi(Y_j) = f_j$ $(j = 1, \ldots, n)$.

(i) Für $g = \sum_\alpha c_\alpha Y^\alpha \in k[Y_1, \ldots, Y_n]$ ist $\varphi(g) = \sum_\alpha c_\alpha f_1^{\alpha_1} \cdots f_n^{\alpha_n}$. (Beachte, dass die Darstellung von $\varphi(g)$ i.a. nicht eindeutig ist)

(ii) Sei $>$ eine monomiale Ordnung auf $\mathbb{M}(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$, so dass jedes Monom, welches mindestens ein X_i enthält größer ist als jedes Monom aus $\mathbb{M}(Y_1, \ldots, Y_n)$ ($>$ ist eine Eliminationsordnung). Weiterhin sei G eine Gröbner Basis des Ideals $I = (Y_1 - f_1, \ldots, Y_n - f_n) \subset k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ bzgl. $>$, und $f \in k[X_1, \ldots, X_m] \subset k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$. Zeigen Sie:

$$f \in \mathrm{im}(\varphi) \iff \overline{f}^G \in k[Y_1, \ldots, Y_n].$$

Ist dies der Fall, so ist $f = \varphi(\overline{f}^G)$.

Aufgabe 3

In dieser Aufgabe beschäftigen wir uns mit dem Zusammenhang von Gröbner Basen und Linearen Diophantischen Gleichungen. Seien eine $m \times n$-Matrix $A = (a_{ij}) \in M(m \times n, \mathbb{N})$ und $b = (b_1, \ldots, b_m) \in \mathbb{N}^m$ (im folgenden stets als Spaltenvektor aufgefasst) gegeben. Wir suchen nach Lösungen $\alpha \in \mathbb{N}^n$ von $A\alpha = b$.

(i) Betrachte den k-Algebrenhomomorphismus $\varphi : k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_m]$ gegeben durch $\varphi(Y_j) = \prod_{i=1}^m X_i^{a_{ij}}$. Sei $\alpha \in \mathbb{N}^n$. Dann gilt:

$$A\alpha = b \iff \varphi(Y^\alpha) = X^b.$$

(ii) Seien $f_j = \prod_{i=1}^m X_i^{a_{ij}} \in k[X_1, \ldots, X_m]$, $(j = 1, \ldots, n)$. Sei $>$ eine monomiale Ordnung auf $\mathbb{M}(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$, so dass jedes Monom, welches mindestens ein X_i enthält größer ist als jedes Monom aus $\mathbb{M}(Y_1, \ldots, Y_n)$. Weiterhin sei G eine Gröbner Basis des Ideals $I = (Y_1 - f_1, \ldots, Y_n - f_n) \subset k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ bzgl. $>$. Zeigen Sie:

$$A\alpha = b \text{ hat eine Lösung } \alpha \in \mathbb{N}^n \iff g = \overline{f}^G \in k[Y_1, \ldots, Y_n], \text{ wobei } f = X^b$$

Ist dies der Fall, so ist $\alpha = \operatorname{multideg}(g)$ eine Lösung.

(iii) Überprüfen Sie mit Hilfe von (ii) (unter Verwendung von Singular) die Lösbarkeit folgender Diophantischer Gleichungssysteme und geben Sie ggf. eine Lösung an.

1) $A = \begin{pmatrix} 3 & 1 & 11 & 2 & 3 \\ 4 & 5 & 0 & 1 & 7 \\ 5 & 6 & 1 & 9 & 2 \end{pmatrix} \qquad b = \begin{pmatrix} 20 \\ 17 \\ 23 \end{pmatrix}$

2) A wie in 1) $\qquad b = \begin{pmatrix} 20 \\ 17 \\ 21 \end{pmatrix}$

3) $A = \begin{pmatrix} 3 & 1 & 11 & 2 & 3 & 5 & 3 \\ 4 & 5 & 0 & 1 & 7 & 4 & 6 \\ 5 & 6 & 1 & 9 & 2 & 3 & 3 \end{pmatrix} \qquad b = \begin{pmatrix} 31 \\ 27 \\ 38 \end{pmatrix}$