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

SS 2003
Übungsblatt 5
19. Mai 2003

Algorithmische Algebra II

Abgabe: 26. Mai, in der Übung, MI03.09.011B

Es sei stets $R = k[X_1, \ldots, X_n]$ der Polynomring (k ein Körper).

Aufgabe 1

(i) Implementieren Sie eine Prozedur `IPSolve`, die auf Eingabe einer Matrix $A \in M(m \times n, \mathbb{N})$ und Vektoren $b = (b_1, \ldots, b_m)$, $c = (c_1, \ldots, c_n)$, $b_i, c_j \in \mathbb{N}$ zunächst checkt, ob $A\alpha = b$ ($\alpha \in \mathbb{N}^n$) eine Lösung hat, und im positiven Fall eine Lösung $\alpha \in \mathbb{N}^n$ berechnet, die $\ell(\beta) = \sum_i c_i\beta_i$ minimiert. (Hinweis: Benutzen Sie $c = (c_1, \ldots, c_n)$ als Gewichtsvektor zur Definition einer für (A, b, ℓ) passenden monomialen Ordnung (vgl. A2, Blatt 4)).

(ii) Testen Sie Ihre Prozedur `IPSolve` anhand folgender Eingaben:

1. A und b wie in A3(iii),1. , Blatt 3, mit $c = (23, 15, 6, 7, 1)$
2. A und b wie in A3(iii),3. , Blatt 3, mit $c = (23, 15, 67, 1, 53, 4)$

Aufgabe 2

Sei $>$ eine monomiale Ordnung auf R^q. Sei $\bar{\mathcal{M}}$ eine Menge von Monomen in R^q, und sei U der von $\bar{\mathcal{M}}$ erzeugte R-Untermodul von R^q. Sei weiter $\bar{N}$ ein Monom in R^q. Dann gilt: $\bar{N} \in U \iff \exists\ \bar{M} \in \bar{\mathcal{M}} \quad \bar{M} \mid \bar{N}$.

Aufgabe 3

Sei U ein R-Untermodul von R^q. Zeigen Sie: Genau dann ist U monomial, wenn es monomiale Ideale $I_1, \ldots, I_q$ von R mit $U = \oplus_i I_i\bar{e}_i$ gilt. ($\bar{e}_1, \ldots, \bar{e}_q$ ist die kanonische R-Basis von R^q).

Aufgabe 4

Beweisen Sie Korrektheit und Terminierung des Divisions-Algorithmus in R^q aus der Vorlesung (Theorem 7.2.7)
Der Divisions-Algorithmus liefert auf die Eingabe $\bar{G} = (\bar{g}_1, \ldots, \bar{g}_t)$, $\bar{g}_i \in R^q$, $\bar{f} \in R^q$, sowie einer monomialen Ordnung auf R^q eine Darstellung $f = \sum_i a_i\bar{g}_i + \bar{r}$ mit $\mathrm{LT}(\bar{f}) \geq \mathrm{LT}(a_i\bar{g}_i)$ ($1 \leq i \leq t$), und $\bar{r} = 0$ oder kein Monom von $\bar{r}$ ist durch eines der Monome $\mathrm{LM}(\bar{g}_1), \ldots, \mathrm{LM}(\bar{g}_t)$ teilbar.