Modul Computeralgebra mit Gröbnerbasen 9. Juni 2011
Sommersemester 2011
Schmale

Aufgabenblatt 9

Drei Übungsaufgaben aus der Algebra 2 im Wintersemester 2003/2004 geringfügig gekürzt:

(24) Seien $R = K[x_1, \ldots, x_n]$, h, $f_1, \ldots, f_r \in R$ und $I = \langle f_1, \ldots, f_r \rangle_R$. Mit Hilfe einer Gröbnerbasis für I und dem Divisionsalgorithmus können wir entscheiden, ob $h \in I$ oder nicht. Sei nun $U = K[f_1, \ldots, f_r]$ der von $f_1, \ldots, f_r$ in R über K erzeugte Unterring. In dieser Aufgabe geht es darum, zu entscheiden (vgl. als mögliches Beispiel etwa mit dem Hauptsatz über symmetrische Funktionen), ob $\boldsymbol{h \in U}$ **?**
Seien $x_1, \ldots, x_n$, $y_1, \ldots, y_r$ unabhängige Variable über K und

$$J = \langle f_1 - y_1, \ldots, f_r - y_r \rangle_S \ ,$$

wobei $S = K[x_1, \ldots, x_n, y_1, \ldots, y_r]$. Weiter sei $\leq$ eine Eliminierordnung bzgl. $\{x_1, \ldots, x_n\}$ und G eine Gröbnerbasis bzgl. $\leq$ für J.
Zeigen Sie:

- **(a)** Seien $u_1, v_1, \ldots, u_m, v_m$ Elemente eines kommutativen Ringes, dann ist $u_1 \cdots u_m - v_1 \cdots v_m$ in dem von $u_1 - v_1, \ldots, u_m - v_n$ erzeugten Ideal.
- **(b)** Sei $g \in K[y_1, \ldots, y_r]$. Dann ist $h = g(f_1, \ldots, f_r)$ genau dann, wenn $h - g \in J$.
- **(c)** $h \in U$ genau dann, wenn $\overline{h}^G \in K[y_1, \ldots, y_r]$.
- **(d)** Rechnen Sie Beispiele z.B. mit Maple.

(25) **Abhängige und unabhängige Substitution.**
Bezeichungen wie in Aufgabe (24).
Betrachtet werde die Abbildung $\Phi : K[y_1, \ldots, y_r] \to K[x_1, \ldots, x_n]$ mit $y_j \mapsto f_j$ für $1 \leq j \leq r$. Zeigen Sie (teilweise unter Benutzung von Aufgabe (24)):

- **(a)** Kern $\Phi = J \cap K[y_1, \ldots, y_r]$
- **(b)** $G \cap K[y_1, \ldots, y_r]$ ist Gröbnerbasis von Kern Φ.

Ausweitung auf den Ring $\mathcal{L} = K[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ der so genannten Laurentpolynome. Seien jetzt also $f_1, \ldots, f_r$ aus $\mathcal{L}$ und sei t eine weitere Unbestimmte.
Zeigen Sie:

- **(c)** Die Substitution $x_i \mapsto x_i, t \mapsto (x_1 \ldots x_n)^{-1}$ induziert einen Isomorphismus

$$\mathcal{L} \cong R[t]/_{\langle x_1 \cdots x_n \cdot t - 1 \rangle}.$$

Zu jedem $f \in \mathcal{L} \backslash \{0\}$ gibt es $f^{(t)} \in R[t]$ mit minimalem t-Grad und derart, dass

$$f^{(t)}\left(\frac{1}{x_1 \cdots x_n}\right) = f.$$

Sei $J^{(t)} = \langle f_1^{(t)} - y_1, \ldots, f_r^{(t)} - y_r, x_1 \cdots x_n \cdot t - 1 \rangle_{S[t]}$

- **(d)** Kern $\Phi = J^{(t)} \cap K[y_1, \cdots, y_r]$
- **(e)** Sei $G^{(t)}$ Gröbnerbasis von $J^{(t)}$ bzgl. einer $\{t, x_1, \ldots, x_n\}$ eliminierenden Monomordnung. Dann gilt

$$G^{(t)} \cap K[y_1, \ldots, y_r] \text{ ist Gröbnerbasis von Kern } \Phi.$$

(26) Die in dieser Aufgabe behandelten Ideale sind spezielle Binomideale, die auch „torische“ Ideale genannt werden. Zahlreiche Motivationen und eine gründliche Analyse binomischer Ideale findet man in Eisenbud/Sturmfels: Binomial Ideals, *Duke Math.J.*, **84** (1996) 1-45.

Seien U ein $\mathbb{Q}$-Untervektorraum von $\mathbb{Q}^n$, $R = K[x_1 \ldots, x_n]$,
$\mathcal{B} = \left\{x^\alpha - x^\beta : \ \alpha, \beta \in \mathbb{N}^n, \alpha \equiv \beta \mod U\right\}$ und $I_U = \langle \mathcal{B} \rangle_K$. Zeigen Sie:

(a) I_U ist ein Ideal und z. B. $I_{\{0\}} = \{0\}$ und $I_{\mathbb{Q}^n} = \langle x_1 - 1, \ldots, x_n - 1 \rangle_R$.

(b) Eine reduzierte Gröbnerbasis von I_U ist stets Teilmenge von $\mathcal{B}$.

(c) I_U ist ein Primideal.

[Anleitung zu (b): Es gibt eine endliche Teilmenge von $\mathcal{B}$, die I_U erzeugt; Buchbergeralgorithmus; beim Divisionsalgorithmus mit Binomen aus $\mathcal{B}$ ist stets Rest + Dividend $\in \mathcal{B}$.
Anleitung zu (c): direkt? mit folgendem Trick geht es für $\{0\} \neq U \neq \mathbb{Q}^n$ auf einem Umweg: Es gibt $A \in \mathbb{Z}^{n \times d}$ mit $n - d = \mathsf{dim}_{\mathbb{Q}} U$ und derart, dass Kern ${}^tA = {}^tU$. Seien $a^{(1)}, \ldots, a^{(n)}$ die Zeilen von A und $L = K[y_1, y_1^{-1}, \ldots, y_d, y_d^{-1}]$. Betrachte den K-Algebra-Morphismus $\varphi = R \to L$ mit $\varphi(x^\alpha) = y^{\alpha A}$. Insbesondere gilt: $\varphi(x_i) = y^{a^{(i)}}$.
Zu zeigen ist dann Kern $\varphi = I_U$, denn L nullteilerfrei. Der Nachweis von Kern $\varphi = I_U$ geht wohl am besten indirekt: betrachte dabei $f \in$ Kern $\varphi \backslash I_U$ in der Darstellung

$$f = \sum_{v \in \mathbb{Z}^d} h_v = \text{ und } h_v = \sum_{\substack{\alpha \in \mathbb{N}^n \\ \alpha A = v}} a_\alpha x^\alpha.$$

Auch die Teilsummen bzw. "Komponenten" h_v von f sind in Kern φ und müssen jeweils mindestens zwei Summanden $\neq 0$ haben. O. E. Anzahl der Summanden $\neq 0$ in h_v minimal; subtrahiere geeignetes Binom aus $\mathcal{B}$ um W! zu erhalten.]