SS 2010 02.07.2010

Übungen zur Vorlesung Computeralgebra
Blatt 11

Prof. Dr. Klaus Madlener Abgabe bis 19.07.2010

Aufgabe 1:
Sei $f \in \mathbb{Z}[x]$ vom Grad n und die Maximumsnorm $\|f\|_\infty = A$ und $f = (ux+v)g$, wobei $u, v \in \mathbb{Z} \setminus \{0\}$ und $g = \sum_{0 \leq i < n} g_i x^i \in \mathbb{Z}[x]$.

1. Zeigen Sie, dass $|g_i| < (i+1)A/|v|$ für $0 \leq i < n-1$, falls $|u| = |v|$, und folgern Sie, dass dann $\|g\|_\infty \leq nA$.
2. Angenommen $\alpha = |u/v| < 1$. Zeigen Sie $|g_i| \leq A\frac{1-\alpha^{i+1}}{1-\alpha}/|v|$ für $0 \leq i < n-1$, und folgern Sie, dass dann $\|g\|_\infty \leq A$ gilt. Zeigen Sie, dass letzteres auch im Fall $|u/v| > 1$ gilt.

Aufgabe 2:
Betrachten Sie die deterministische Variante des Berlekamp-Algorithmus in Geddes et al. auf Seite 352 (Algorithm 8.4). Wieso genügt es im letzten Abschnitt, die größten gemeinsamen Teiler $\mathrm{ggT}(v^{[r]} - s, u)$ für die Basispolynome $v^{[2]}, \ldots, v^{[k]}$ der Nullraumbasis von $Q - I$ zu berechnen, um eine vollständige Faktorisierung zu erhalten?

Aufgabe 3:
Von Kronecker (1882) stammt folgende Methode, das Faktorisierungsproblem für multivariate Polynome über einem ZPE-Ring R auf das Faktorisierungsproblem für univariate Polynome über R zu reduzieren.

a) Sei die Abbildung $S_d : R[x_1, \ldots, x_n] \to R[y]$ durch

$$h(x_1, \ldots, x_n) \mapsto h(y, y^d, \ldots, y^{d^{n-1}})$$

definiert (für $d \in \mathbb{N}$). überzeugen Sie sich, dass S_d ein Homomorphismus ist, der für diejenigen Polynome invertiert werden kann, die in jeder Variablen einen Grad kleiner als d haben.

b) Wir wollen mit S_d^{-1} die additive Abbildung $R[y]/\langle y^{d^n} \rangle \to R[x_1, \ldots, x_n]$ bezeichnen, die

$$S_d^{-1}(c\, y^\alpha) = c\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

erfüllt, wobei $\alpha_1 + \alpha_2 d + \cdots + \alpha_n d^{n-1}$ die (positive) d-adische Darstellung von α sei.

Sei nun $f \in R[x_1, \ldots, x_n]$, $d > \max_{1 \leq i \leq n} \deg_{x_i}(f)$, und sei g ein Faktor von f. Zeigen Sie, dass es dann irreduzible Faktoren $g_1, \ldots, g_s$ von $S_d(f)$ gibt, so dass $g = S_d^{-1}(\prod_{j=1}^{s} g_j)$ ist.

c) Geben Sie nun einen Algorithmus an, der für ein $f \in R[x_1, \ldots, x_n]$ seine irreduziblen Faktoren $f_1, \ldots, f_s$ berechnet. Untersuchen Sie die Laufzeit Ihres Algorithmus.

d) Faktorisieren Sie das Polynom $f = -x^4y + x^3z + xz^2 + yz^2 \in \mathbb{F}_3[x, y, z]$ mit Ihrem Algorithmus.