Chair of Symbolic Computation
Prof. Dr. Martin Kreuzer
Julian Danner

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

Computeralgebra – Sheet 2

Summer term 2025

Date: 02.05.2025
Discussion: 09.05.2025

Exercise 1 (**Bachelor**, The Degree-Lexicographic Term Ordering)**.**
Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $\mathbb{T}^n = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in P \mid \alpha_1, \ldots, \alpha_n \in \mathbb{N}\}$ be the set of all terms of P. We define a relation $\leq_{\mathtt{dl}}$ on $\mathbb{T}^n$ as follows:

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \ \leq_{\mathtt{dl}}\ x_1^{\beta_1} \cdots x_n^{\beta_n} \quad \Longleftrightarrow \quad \left[\begin{array}{l} \alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n, \text{ or} \\ \alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n \text{ and } \alpha_1 < \beta_1, \text{ or} \\ \alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n \text{ and } \alpha_1 = \beta_1, \alpha_2 < \beta_2, \text{ or} \\ \qquad\qquad \vdots \\ \alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n \text{ and} \\ \qquad\qquad \alpha_1 = \beta_1, \ldots, \alpha_{n-1} = \beta_{n-1}, \alpha_n \leq \beta_n. \end{array}\right.$$

Show that $\leq_{\mathtt{dl}}$ satisfies:

(a) $t_1 \leq_{\mathtt{dl}} t_2$ implies $t_1 t_3 \leq_{\mathtt{dl}} t_2 t_3$ for all $t_1, t_2, t_3 \in \mathbb{T}^n$.

(b) $1 \leq_{\mathtt{dl}} t$ for all $t \in \mathbb{T}^n$.

Exercise 2 (Squarefree Parts of Polynomials I)**.**
Let K be a field of characteristic 0 and $P = K[x]$. Let $f \in P \setminus \{0\}$ and write $f = c \prod_{i=1}^{s} p_i^{\alpha_i}$, where $c \in K \setminus \{0\}$ and $p_1, \ldots, p_s \in P$ are distinct irreducible polynomials. Show that

$$\gcd(f, f') \ = \ \prod_{i=1}^{s} p_i^{\alpha_i - 1}$$

and deduce that the squarefree part of f can be computed as

$$\operatorname{sqfree}(f) \ = \ \frac{f}{\gcd(f, f')}.$$

Exercise 3 (Squarefree Parts of Polynomials II)**.**
Let p be a prime and let $f \in P = \mathbb{F}_p[x]$ be a non-zero polynomial. Consider the following sequence of instructions.

(1) Compute $s_1 = \gcd(f, f')$. If $s_1 = 1$, then **return** f.

(2) If $s_1' = 0$, then $s_1 = g^p$ for some $g \in P$. Replace f by $\frac{fg}{s_1}$ and continue with step (1).

(3) Otherwise, compute $s_{i+1} = \gcd(s_i, s_i')$ for $i = 1, 2, \ldots$ until $s_{i+1}' = 0$. Then there is some $g \in P$ with $s_{i+1} = g^p$. Replace f by $\frac{fg}{s_1}$ and continue with step (1).

Show that this is an algorithm. It computes the squarefree part $\operatorname{sqfree}(f)$ of f.

Exercise 4 (**Master**)**.** Implement the algorithm from Exercise 3 as a function `SqFree` in `CoCoA`. Apply it to find the squarefree part of $f = x^{31}2x^{30}x^6 + 2x^5$ in $\mathbb{F}_5[x]$.

Exercise 5 (Minimal Polynomial)**.** Let $\alpha = \sqrt{2} + \sqrt[3]{3} + i \in \mathbb{C}$. Use `CoCoA` and the instructions given in the lecture to compute the minimal polynomial $\mu_\alpha(t) \in \mathbb{Q}[t]$ of α, i.e., the monic polynomial $\mu_a(t) \in \mathbb{Q}[t]$ of smallest degree such that $\mu_a(a) = 0$.

Hint: Start with `Use P::= QQ[x,y,z,t];`*, form the diagonal ideal, and apply the function* `Elim`*.*

Exercise 6 (Implicitization Problem and Heron's Formula)**.**

(a) Consider the following parametrized curve

$$C = \{\, (t^2, t^3, t^5) \in \mathbb{Q} \mid t \in \mathbb{Q} \,\}.$$

What are its defining equations?

Hint: Use the function `Elim(...)` *to compute the vanishing ideal* $I_C = \langle x - t^2, y - t^3, z - t^5 \rangle \cap \mathbb{Q}[x, y, z]$ *of* C*.*

(b) Using `CoCoA` to find Heron's formula for the area of a triangle in terms of the lengths a, b, c of its sides.