**UNIVERSITÄT DES SAARLANDES**
**Fachrichtung Mathematik**
**Prof. Dr. Frank-Olaf Schreyer**

Universität des Saarlandes - Campus E2 4 - D-66123 Saarbrücken

## Computer Algebra Summer Term 2019

**Exercise Sheet 6.** Hand in by Tuesday, May 28.

**Exercise 1.** Let $K = \mathbb{F}_p(t)$ be the field of rational function over $\mathbb{F}_p$. Consider

$$f = x^p - t$$

and its splitting field $L \supset K$. Prove that f has only one root in $L$ and conclude that $Gal(f) = Aut(L/K)$ is trivial.

**Exercise 2.** Let $d = d_1^{e_1} \cdots d_k^{e_k}$ be an integer with its prime factorisation and let $p$ be a prime number. Prove:

$$\frac{1}{d} \sum_{S \subset \{1,\ldots,k\}} (-1)^{|S|} p^{d/\prod_{i \in S} d_i}$$

is the number of monic irreducible polynomials of degree $d$ in $\mathbb{F}_p[x]$. Can you prove that this number is an integer without using finite fields?

**Exercise 3.** Prove:

(1) Let $f \in K[x]$ be an irreducible polynomial of degree $r$. One arithmetic operation in $L = K[x]/\langle f \rangle$, i.e. addition, multiplication or division by an invertible element, can be done in $O(r^2)$ arithmetic operations in $K$.
(2) One arithmetic operation in $\mathbb{Z}/\langle m \rangle$ can be done in $O((\log m)^2)$ bit operations.
(3) One arithmetic operation in the finite field $\mathbb{F}_q$ can be done in $O((\log q)^2)$ bit operations.

**Exercise 4.** Design an algorithm to factor polynomials in $\mathbb{Z}[x]$ based on interpolation of polynomials and factorization in $\mathbb{Z}$. Illustrate your algorithm by factoring $3x^4 + 12x^3 + 5x^2 - 4x - 2 \in \mathbb{Z}[x]$.