Due date: 3.11.2020

15. Exercise

Given a Euclidean domain E, prove the following claims:

(a) Let $m_1, \dots, m_n \in E \setminus \{0\}$, where $n \in \mathbb{Z}^+$, be pairwise relatively prime an define

$$\overline{m}_i := \prod_{\substack{j=1 \\ j \neq i}}^{n} m_j.$$

Then m_i and $\overline{m}_i$ are relatively prime for all $1 \leq i \leq n$.

(b) Let $r, s \in E$ and $m, n \in E \setminus \{0\}$ such that m and n are relatively prime. Then $r \equiv s \bmod m$ and $r \equiv s \bmod n$ if and only if $r \equiv s \bmod m\,n$.

16. Exercise

The following is a famous (resolved) problem from the field of algebraic geometry asking for a relation between geometric objects and algebraic structures. We will give an answer to a special case in this exercise.

Problem (Nullstellensatz)**.** *Given a set of polynomials $S \subseteq F[x_1, \dots, x_n]$ over an algebraically closed base field F. Is there a relation between the ideal $\langle S \rangle$ and $\mathbf{I}(\mathbf{Z}(S))$?*

The notation $\mathbf{Z}(\cdot)$ and $\mathbf{I}(\cdot)$ stand for the subsequent constructions. Let $S \subseteq F[x_1, \dots, x_n]$ and define

$$\mathbf{Z}(S) := \{(a_1, \dots, a_n) \in F^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in S\},$$

i.e. the set of all common roots of the polynomials in S. A set which is defined by the zero-locus of a collection of polynomials is called an *affine algebraic set*. For an affine algebraic set $A \subseteq F^n$ we denote by

$$\mathbf{I}(A) := \{f \in F[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in A\}$$

the ideal of all polynomials which vanish on all points in A.

Consider the case where the polynomial ring is $\mathbb{C}[x]$. Since this is a principal ideal domain every ideal is generated by a single polynomial. Furthermore, every complex polynomial $f \in \mathbb{C}[x]$ factors completely into linear polynomials, i.e.

$$f = c\,(x - r_1)^{e_1} \cdots (x - r_k)^{e_k}, \tag{1}$$

where $r_1, \dots, r_k \in \mathbb{C}$ are the distinct roots of f, the exponents e_i are positive numbers denoting the multiplicities of the roots and $c \in \mathbb{C}$.

Let $f \in \mathbb{C}[x]$ be a non-zero polynomial with a factorization as in Equation (1).

(a) Show that

$$\langle f_{\mathrm{sfp}} \rangle = \mathbf{I}(\mathbf{Z}(\{f\})),$$

where $f_{\mathrm{sfp}} = c\,(x - r_1) \cdots (x - r_k)$ is called the *square-free part* of f.

(b) The square-free part of the polynomial f can be computed efficiently. Show that

$$f_{\mathrm{sfp}} = \frac{f}{\gcd(f, f')}.$$

(c) Find a single generator of the ideal $\mathbf{I}(\mathbf{Z}(\{f, g\})) \subseteq \mathbb{C}[x]$, where

$$f = x^6 - x^5 - 2\,x^4 + 2\,x^3 + x^2 - x \quad \text{and} \quad g = x^5 + x^4 - 2\,x^3 - 2\,x^2 + x + 1.$$

17. Exercise

Implement the algorithm `SQFR_FACTOR` from the lecture notes in a CAS and compute the square-free factors of the polynomial

$$f = x^9 + 7\,x^8 + 17\,x^7 + 12\,x^6 - 17\,x^5 - 37\,x^4 - 21\,x^3 + 10\,x^2 + 20\,x + 8.$$

What is the difference between the square-free factors and the irreducible factors in $\mathbb{Z}[x]$ of the polynomial f?

18. Exercise

Prove Theorem 2.3.3 from the lecture notes: Let F be a field of characteristic zero and $f \in F[x_1, \dots, x_n] \setminus \{0\}$. The polynomial f is square-free if and only if

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right) = 1.$$

Does the theorem hold for fields of positive characteristic?