Due date: 16.11.2021

Exercise 15. Take your favourite CAS and implement the algorithm `SQFR_FACTOR` from the lecture notes. Use your implementation to compute the square-free factors of the polynomial

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

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

Exercise 16. In this exercise, we will give an answer to a special case of the following famous (resolved) problem in algebraic geometry.

Problem (Nullstellensatz)**.** Let $S \subseteq K[x_1, \dots, x_n]$ be a set of polynomials over an algebraically closed field K. What is the relation between the ideals $\langle S \rangle$ and $\mathbf{I}(\mathbf{Z}(S))$?

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

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

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 $A \subseteq K^n$, let

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

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

Consider the case where the polynomial ring is the principal ideal domain $\mathbb{C}[x]$. Recall that 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 integers 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 $\langle f_{\text{sfp}} \rangle = \mathbf{I}(\mathbf{Z}(\{f\}))$, where $f_{\text{sfp}} = c\,(x - r_1) \cdots (x - r_k)$ is called the *square-free part* of f.

(b) Show that the square-free part of the polynomial f can be computed efficiently by[1]

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

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

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

[1] f' denotes the derivative of f.

Exercise 17. Prove Theorem 2.3.3 from the lecture notes: Let K be a field of characteristic zero and $f \in K[x_1, \dots, x_n]$ be a non-zero polynomial. Then f is square-free if and only if

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