to be prepared for 05.11.2019

Exercise 1. Use the algorithm `SQFR_FACTOR` from the lecture notes to compute the square-free factors of the polynomial

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

You can do the computations by hand or implement the algorithm in a CAS of your choice. What is the difference between the square-free factors and the irreducible factors in $\mathbb{Z}[x]$ of the polynomial $f(x)$?

Exercise 2. The following is a famous (resolved) problem in algebraic geometry asking for a relation between geometric objects and algebraic structures. We will give an answer to a special case in this exercise. For the sake of brevity, the dependency on the variables is omitted here, i.e., instead of $f(x_1, \ldots, x_n)$ we write just f for a polynomial.

Problem 1 (Nullstellensatz)**.** Given polynomials $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ over an algebraically closed field F. Is there a relation between $\langle f_1, \ldots, f_m \rangle$ and $\mathbf{I}\big(\mathbf{V}(f_1, \ldots, f_m)\big)$?

Recall from exercise sheet 2 that $\langle f_1, \ldots, f_m \rangle$ denotes the ideal generated by the polynomials $f_1, \ldots, f_m$, i.e., the set of all polynomial linear combinations spanned by the f_i, $i \in 1 \ldots m$. We denote by

$$\mathbf{V}(f_1, \ldots, f_m) := \{\, (a_1, \ldots, a_n) \in F^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq m \,\}$$

the set of all common roots of the polynomials f_i. Such sets are called *affine algebraic sets*. Similarly, for $V = \mathbf{V}(f_1, \ldots, f_m)$ we denote by

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

the ideal of all polynomials which vanish on all points in V.
Now consider the case where the polynomial ring is $\mathbb{C}[x]$. Since this is a principal ideal domain, we can reduce the case of multiple generators of an ideal to a single generator, cf. exercise sheet 2. Getting to the point, we consider the problem of determining the generator of the ideal $\mathbf{I}(\mathbf{V}(f)) \subseteq \mathbb{C}[x]$, where $f \in \mathbb{C}[x]$ is a non-zero polynomial. Since f is a complex polynomial it factors completely into linear polynomials, i.e.,

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

where $r_1, \ldots, r_k \in \mathbb{C}$ are the distinct roots of f, the exponents are positive numbers denoting the multiplicities of the roots and $c \in \mathbb{C} \setminus \{0\}$. Now prove the following items:

1. Show that $\mathbf{V}(f) = \{\, r_1, \ldots, r_k \,\}$.
2. We call the polynomial $f_{\text{sfp}} = c\,(x - r_1) \cdots (x - r_k)$ the *square-free part* of f. Show that $\langle f_{\text{sfp}} \rangle = \mathbf{I}(\mathbf{V}(f))$.

Exercise 3. Compute a single generator of the ideal $\mathbf{I}(\mathbf{V}(f, g)) \subseteq \mathbb{C}[x]$, where

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

Exercise 4. Prove the following theorem.[1] Let K be a field of characteristic 0, and $a(x_1, \ldots, x_n) \in K[x_1, \ldots x_n]$. Then a is squarefree if and only if $\gcd\left(a, \frac{\partial a}{\partial x_1}, \ldots, \frac{\partial a}{\partial x_n}\right) = 1$.

[1] Theorem 4.4.2, F. Winkler, Polynomial Algorithms in Computer Algebra