Due date: 19.10.2021

Exercise 5. Implement the extended Euclidean algorithm `GCD_EUCLID` from the lecture notes for $K = \mathbb{Q}$. Test your implementation on the input:

(a) $f_1 = x^3 + 3x^2 + 2x + 1$ and $g_1 = x^2 + x + 1$,

(b) $f_2 = x^6 + x^5 - x^4 - x^2 - 4x - 2$ and $g_2 = x^5 - 3x^4 - x^3 + 3x^2 - 2x + 6$.

Note: You may use the field operations and the command for division with remainder offered by your CAS. You may NOT use any built-in GCD methods.

Exercise 6. Let U be a unique factorization domain. For non-zero polynomials $f, g \in U[x]$ we write $f \sim g$ if and only if there exists a unit $u \in U$ such that $f = ug$. Show that:

(a) $\operatorname{cont}(fg) \sim \operatorname{cont}(f) \cdot \operatorname{cont}(g)$,

(b) $\operatorname{pp}(fg) \sim \operatorname{pp}(f) \cdot \operatorname{pp}(g)$,

(c) $\operatorname{cont}(\gcd(f, g)) \sim \gcd(\operatorname{cont}(f), \operatorname{cont}(g))$,

(d) $\operatorname{pp}(\gcd(f, g)) \sim \gcd(\operatorname{pp}(f), \operatorname{pp}(g))$.

Hint: $U[x]$ is a unique factorization domain. Every non-zero non-unit polynomial can be factored uniquely (up to reordering and multiplication by units) into the product of finitely many irreducible (prime) elements. Let $f = up_1^{a_1} \cdots p_n^{a_n}$ and $g = vp_1^{b_1} \cdots p_n^{b_n}$ be prime factorizations of f and g, respectively, where $u, v \in U$ are units and the p_i denote distinct primes with corresponding exponents $a_i, b_i \geq 0$. What is $\gcd(f, g)$ in this case?

Exercise 7. Let us extend the definition of a greatest common divisor (GCD) from the lecture notes: A *greatest common divisor* of a finite number of polynomials $f_1, \dots, f_m \in K[x]$, where K is a field and $m > 1$, is a polynomial $g \in K[x]$ with the following properties:

- g divides all polynomials $f_1, \dots, f_m$ and
- if h is another polynomial which divides all $f_1, \dots, f_m$, then h divides g.

If g satisfies these properties, then we write $g = \gcd(f_1, \dots, f_m)$. Show that:

(a) The GCD of $f_1, \dots, f_m$ exists and is unique up to multiplication by elements of K^*.[1]

(b) The GCD generates the ideal spanned by $f_1, \dots, f_m$, i.e. $\langle \gcd(f_1, \dots, f_m) \rangle = \langle f_1, \dots, f_m \rangle$.

(c) For $m > 2$ we have that $\gcd(f_1, \dots, f_m) = \gcd(f_1, \gcd(f_2, \dots, f_m))$.

Hint: Use the fact that $K[x]$ is a principal ideal domain.

Exercise 8 (Membership problem)**.** Consider polynomials $f, f_1, \dots, f_m \in K[x]$, where K is a field and m is a positive integer. Develop an algorithm for deciding whether $f \in \langle f_1, \dots, f_m \rangle$ based on the algorithm `GCD_EUCLID` from the lecture notes.[2]

[1] Since GCDs are unique up to multiplication by units, we usually speak of *the* GCD instead of *a* GCD.
[2] You do not have to implement the algorithm, it suffices to provide pseudo-code.

Exercise 9. Consider the polynomials over the integers $f = 6x^5 + 2x^4 - 19x^3 - 6x^2 + 15x + 9$ and $g = 5x^4 - 4x^3 + 2x^2 - 2x - 2$. Find the GCD of f and g by a polynomial remainder sequence.