Exercise sheet 11

1. The *Sylvester matrix* of two polynomials $f(X) := \sum_{i=0}^{m} a_i X^i$ and $g(X) := \sum_{j=0}^{n} a_j X^j$ over a ring R is given by the $(m+n) \times (m+n)$ matrix

$$\mathrm{Sylv}_{f,g} := \begin{pmatrix} a_m & \dots & \dots & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_m & \dots & \dots & \dots & a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & a_1 & a_0 \\ b_n & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_n & \dots & \dots & b_1 & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & b_1 & b_0 \end{pmatrix}.$$

The determinant of the Sylvester matrix is called the *resultant of f and g* and is denoted by $\mathrm{Res}_{f,g} \in R$.

(a) Compute the resultant of the polynomials $X^3 - X + 1$ and $X^2 + X + 3$.

(b) For two arbitrary polynomials f, g over a ring R prove that

$$\mathrm{Res}_{g,f} = (-1)^{mn} \, \mathrm{Res}_{f,g}$$

(c) For K a field, let $f, g \in K[X]$ be two polynomials. Prove: the resultant of f and g is equal to zero if and only if the two polynomials have a common root.

(d) For polynomials $f(X) = a_m \prod_{i=1}^{m}(X - \alpha_i)$ and $g(X) = b_n \prod_{j=1}^{n}(X - \beta_j)$ prove:

$$\mathrm{Res}_{f,g} = a_m^n \cdot b_n^m \cdot \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

(e) Let $f(X) = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m$ be a polynomial over a ring R. Let $\Delta(f)$ denote its discriminant (see exercise sheet 10). Show that

$$\Delta(f) = (-1)^{\frac{m(m-1)}{2}} \, \mathrm{Res}_{f,f'},$$

where f' denotes the derivative of f.

(f) Determine a general formula for the discriminant of an arbitrary polynomial of degree $2, 3$ and 4.

2. Let n be a positive integer, and $P \in \mathbb{Z}[X]$ a monic irreducible factor of $X^n - 1 \in \mathbb{Q}[X]$. Suppose that ζ is a root of P.

(a) Show that for each $k \in \mathbb{Z}_{\geqslant 0}$ there exists a unique polynomial $R_k \in \mathbb{Z}[X]$ such that $\deg(R_k) < \deg(P)$ and $P(\zeta^k) = R_k(\zeta)$. Prove that $\{R_k | k \in \mathbb{Z}_{\geqslant 0}\}$ is a finite set. We define

$$a := \sup\{|u| : u \text{ is a coefficient of some } R_k\}$$

(b) Show that for $k = p$ a prime, p divides all coefficients of R_p, and that when $p > a$ one has $R_p = 0$ (*Hint:* $P(\zeta^p) = P(\zeta^p) - P(\zeta)^p$).

(c) Deduce that if all primes dividing some positive integer m are strictly greater then a, then $P(\zeta^m) = 0$.

(d) Prove that if r and n are coprime, then $P(\zeta^r) = 0$ (*Hint:* Consider the quantity $m = r + n\prod_{p \leqslant a, p \nmid r} p$).

(e) Recall the definition of n-th cyclotomic polynomial Φ_n for $n \in \mathbb{Z}_{>0}$: we take $W_n \subseteq \mathbb{C}$ to be the set of primitive n-th roots of unity, and define

$$\Phi_n(X) := \prod_{x \in W_n} (X - x).$$

Prove the following equality for $n \in \mathbb{Z}_{>0}$:

$$\prod_{0<d|n} \Phi_d(X) = X^n - 1,$$

and deduce that $\Phi_n \in \mathbb{Z}[X]$ for every n.

(f) Prove that the n-th cyclotomic polynomial is irreducible. (*Hint:* Take $\zeta := \exp(2\pi i/n)$ and P its minimal polynomial over $\mathbb{Q}$. Check that P satisfies the required hypothesis to deduce that $\Phi_n(X)|P$ (using parts (a)-(d)). Then irreducibility of P together with part (e) allow you to conclude.)

3. Let L be a splitting field of the polynomial $X^6 - 5$ over $\mathbb{Q}$. Determine all intermediate fields of $L : \mathbb{Q}$ together with their inclusions.