Resultant, number fields and trace forms

Exercise 1. [Resultant of two polynomials]

Let k be a field, $P := \sum_{i=0}^{n} a_i X^i, Q := \sum_{i=0}^{m} b_i X^i \in k[X]$ with $a_n, b_m \neq 0$. The *Sylvester matrix* of P and Q is the $(n+m)\times(n+m)$-matrix

$$\mathrm{Sylv}(P,Q) := \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & \dots & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \\ 0 & 0 & \dots & a_n & a_{n-1} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 & \dots & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \\ 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_1 & b_0 \end{pmatrix}$$

and their resultant is $\mathrm{Res}(P,Q) := \det(\mathrm{Sylv}(P,Q))$.

1. Show that ${}^t\,\mathrm{Sylv}(P,Q)$ is the matrix of the k-linear map $\Phi_{P,Q} : (U,V) \mapsto UP + VQ$ in suitable bases $k_{m-1}[X] \times k_{n-1}[X]$ and $k_{n+m-1}[X]$.
2. Show that $\mathrm{Res}(P,Q) = 0$ if and only if P and Q have a common root in an algebraic closure of k.
3. Let $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in \overline{k}$ be the roots of P and Q. Let $P_Y := P(Y - X) \in k[X][Y]$. Show that $\mathrm{Res}(P_Y, Q(Y))$ is a polynomial in $k[X]$ whose roots in $\overline{k}$ are the $\alpha_i + \beta_j$. Deduce that the sum of two algebraic numbers is an algebraic number.
   Remark : Similarly, $\mathrm{Res}_Y(X^n P(Y/X), Q(Y))$ has the $\alpha_i\beta_j$ as roots in $\overline{k}$, and the product of two algebraic numbers is an algebraic number.
4. **Fact :** We have $\mathrm{Res}(P,Q) = a_n^m \prod_{i=1}^{n} Q(\alpha_i)$.

   Show that $\mathrm{disc}(P) := \prod_{i<j}(\alpha_i - \alpha_j)^2 = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n^{2n-1}} \mathrm{Res}(P, P')$. Show that $\mathrm{disc}(P) \neq 0$ if and only if P is separable.

Exercise 2. [Embeddings and trace forms]

1. Let $K = \mathbb{Q}(\alpha)$, with $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$.
   (a) Show that $P_\alpha := X^3 - X^2 - 2X - 8$ is irreducible over $\mathbb{Q}$.
   (b) Determine the values of r_1 and r_2 (the numbers of real and pairs of complex embeddings of K, respectively).
2. Let $K = \mathbb{Q}(\alpha)$, where α is a root of an irreducible polynomial $P_\alpha := X^3 + pX + q \in \mathbb{Q}[X]$, with $p > 0$. Determine the values of r_1 and r_2 in this case.
3. If K is a number field of degree n and $(\omega_1, \dots, \omega_n) \in K^n$, the *discriminant* of $(\omega_1, \dots, \omega_n)$ is

$$\Delta(\omega_1, \dots, \omega_n) = \det\left(\left(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)\right)_{1\le i,j\le n}\right).$$

   In both previous cases, compute $\Delta(1, \alpha, \alpha^2)$.

Exercise 3. [Discriminant of a number field]

Let K be a number field with embeddings $\sigma_1, \dots, \sigma_n$. Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be such that $\mathcal{O}_K = \oplus_{i=1}^n \mathbb{Z}\alpha_i$. The *discriminant* of K is defined as $D_K = \Delta(\alpha_1, \dots, \alpha_n)$. You will see in class that such a family $(\alpha_1, \dots, \alpha_n)$ exists and that D_K does not depend on $\alpha_1, \dots, \alpha_n$.

1. Show that $\Delta(\alpha_1, \dots, \alpha_n) = \det((\sigma_i(\alpha_j))_{1\le i,j\le n})^2$.
2. Compute D_K when $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 0, 1$ square-free.
3. Show that $D_K \in \mathbb{Z}$ and $D_K \equiv 0, 1 \bmod 4$ (Stickleberger's criterion). *Hint : Write the determinant as the difference between two algebraic integers.*
4. Show that D_K is of sign $(-1)^{r_2}$ where r_2 is the number of pairs of complex embeddings of K.

Exercise 4. [Number of roots of a monic polynomial]

Let P be a monic separable polynomial in $\mathbb{R}[X]$ and $A = \mathbb{R}[X]/(P)$. Denote by r (respectively s) the number of distinct real roots of P (respectively of non-real roots of P).

1. Show that the signature (p, q) of the bilinear form $(x, y) \mapsto \mathrm{Tr}_{A/\mathbb{R}}(xy)$ on A^2 satisfies $r = p - q$ and $s = 2q$.
2. Determine r and s when P is not necessarily separable.

Exercise 5. Let $\alpha = \sqrt[4]{2}$ and $K = \mathbb{Q}(\alpha)$. Let p be an odd prime number, and assume for a contradiction that there exist $a, b, c, d \in \mathbb{Q}$ such that $\sqrt{p} = a + b\alpha + c\alpha^2 + d\alpha^3$.

1. Show that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{p}) = 0$. Deduce that $a = 0$.
2. By considering $\frac{\sqrt{p}}{\alpha}$, show that $b = 0$.
3. By considering $\frac{\sqrt{p}}{\alpha^2}$, deduce a contradiction.

Exercise 6. [A ring of integers with no power basis]

Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$. We will show that $\mathcal{O}_K$ is not of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Therefore, assume for a contradiction that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha \in \mathcal{O}_K$ has minimal polynomial P over $\mathbb{Q}$.

1. For every $Q \in \mathbb{Z}[X]$, show that $3 \mid Q(\alpha)$ in $\mathcal{O}_K$ if and only if $\overline{P} \mid \overline{Q}$ in $\mathbb{F}_3[X]$.
2. Let
$$\alpha_1 := (1+\sqrt{7})(1+\sqrt{10}), \alpha_2 := (1+\sqrt{7})(1-\sqrt{10}), \alpha_3 := (1-\sqrt{7})(1+\sqrt{10}), \alpha_4 := (1-\sqrt{7})(1-\sqrt{10}).$$
Show that $3 \mid \alpha_i\alpha_j$ in $\mathcal{O}_K$ for $i \neq j$.
3. Compute $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i)$ for $1 \le i \le 4$.
4. Let $P_i \in \mathbb{Z}[X]$ be such that $P_i(\alpha) = \alpha_i$ for $1 \le i \le 4$. Show that $\overline{P} \mid \overline{P_i P_j}$ but $\overline{P} \nmid \overline{P_i^n}$ in $\mathbb{F}_3[X]$, for $1 \le i \neq j \le 4$ and $n \ge 1$.
5. Deduce that for $1 \le i \neq j \le n$, there exists an irreducible polynomial of $\overline{P}$ dividing $\overline{P_i}$ but not $\overline{P_j}$. Deduce that $\overline{P}$ has four distinct roots in $\mathbb{F}_3$ and derive a contradiction.