Résultant et discriminant

Exercice 1. [Calcul de résultants simples]
Calculer les résultants de P et Q pour les polynômes P et Q dans $K[X]$ suivants :
(*a*) $P = X^n - 1$, $Q = X^m - 1$. Qu'en déduire sur les résultants de polynômes cyclotomiques ?
(*b*) $P = X^3 + aX^2 + bX + c$, $Q = 2aX + b$.
(*c*) $P = X^2 + aX + b$, $Q = X^2 + a'X + b'$.
(*d*) $P = X^2 - a$ et $Q = X^{p-1} - 1$. Qu'en déduire sur le symbole de Legendre ?

Exercice 2. [Réciprocité quadratique et résultant]
On définit pour tout $n \geq 1$ le polynôme $H_n = X^{n-1} + \cdots + X + 1$.
(*a*) Montrer que pour tous $m, n \geq 1$, $\mathrm{Res}(H_m, H_n) = \pm 1$ si $\mathrm{pgcd}(m, n) = 1$ et 0 sinon.
(*b*) Montrer que pour n impair, il existe un unique polynôme $\psi_n \in \mathbb{Z}[X]$ tel que

$$H_n(X) = X^{\frac{n-1}{2}} \psi_n(X + X^{-1}).$$

(*c*) Montrer que pour tout nombre premier p impair, $\psi_p(2) = p$ et $\psi_p(X) \equiv (X-2)^{(p-1)/2}$ mod p.
(*d*) Montrer que pour tous nombres premiers p et q impairs distincts, $\mathrm{Res}(\psi_p, \psi_q) = \left(\frac{p}{q}\right)$ le symbole de Legendre associé à p et q.
(*e*) En déduire la loi de réciprocité quadratique.

Exercice 3. [Nombres algébriques] Donner des polynômes annulateurs des entiers algébriques $\sqrt{3} + \sqrt{5}$, $\sqrt[3]{5}(3 + i)$ et $7j + 3j^2 + 1$.

Exercice 4. [Courbes algébriques]
(*a*) Calculer l'intersection des courbes planes d'équations respectives $x^2 - xy + y^2 - 1 = 0$ et $2x^2 + y^2 - y - 2 = 0$, puis celle des courbes d'équations respectives $x^2 + y^2 + xy - 2x - y$ et $2y^2 + xy - x - 2y = 0$.
(*b*) Décrire par des équations polynomiales les courbes paramétrées $\mathcal{C} = \left\{(t^2, t^3 - t), t \in \mathbb{T}\right\}$ et $\mathcal{C}' = \left\{(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}), t \in \mathbb{R}\right\}$. Est-ce que toutes les solutions des équations polynomiales apparaissent sont paramétrées ?
(*c*) *(Formule de Héron)* Soit un triangle ABC avec pour longueurs $a = BC$, $b = AC$ et $c = AB$. On note H le pied de la hauteur partant de A et $x = BH, y = AH$. Donner des équations polynômiales satisfaites par a, b, c, x, y et l'aire S du triangle, puis par résultants successifs, en déduire la formule de Héron

$$S^2 = \frac{1}{16}(a+b+c)(a+b-c)(a-b+c)(-a+b+c).$$

Exercice 5. [Discriminant]

Par définition, le discriminant d'un polynôme $P = a\prod_{i=1}^{n}(X-\alpha_i)$ est

$$D(P) = a^{2n-1}\prod_{i<j}(\alpha_i-\alpha_j)^2$$

(a) Écrire $D(P)$ en fonction d'un résultant bien choisi, et en déduire que $D(P)$ est un polynôme à coefficients entier en les coefficients de P.

(b) Donner la formule du discriminant en fonction des coefficients pour les polynômes de degré 3 et 4.

(c) Montrer que l'intérieur de l'ensemble des matrices diagonalisables de $M_n(\mathbb{C})$ est l'ensemble des matrices diagonalisables à valeurs propres distinctes.

(d) Déterminer l'ensemble des nombres premiers p tels que X^4+3X+2 est sans facteurs carrés modulo p.

(e) Écrire $D(PQ)$ en fonction des discriminants et du résultant de P et Q.

(f) Calculer le discriminant du polynôme cyclotomique ϕ_p pour p premier, puis ϕ_{p^n}.

Exercice 6. [Nullstellensatz effectif]

La forme du Nullstellensatz que nous allons prouver énonce que sur un corps K algébriquement clos, si des polynômes $P_1,\cdots,P_m \in K[X_1,\cdots,X_n]$ sont sans zéro commun, alors il existe $Q_1,\cdots Q_m$ d'autres polynômes tels que

$$P_1Q_1+\cdots+P_mQ_m = 1.$$

(a) Montrer que pour tout $P \in K[X_1,\cdots,X_n]$ non nul de degré total d, il existe $(a_1,\cdots,a_{n-1}) \in K^{n-1}$ tel que

$$P(X_1+a_1X_n,\cdots,X_{n-1}+a_{n-1}X_n,X_n) = cX_n^d+R$$

avec R de degré $< d$ en X_n et $c \neq 0$.

(b) On va maintenant montrer le Nullstellensatz par récurrence sur n. Prouver qu'il est vrai pour $n=1$.

Supposons que le Nullstellensatz est vrai pour $n>1$, on peut de plus supposer que tous les P_i sont non nuls et que P_1 est sous la forme du (a), avec $c=1$. On définit, pour une variable supplémentaire T,

$$Q(T,X_1,\cdots,X_n) = P_2+P_3T+\cdots+P_mT^{m-2}.$$

et

$$\mathrm{Res}_{X_n}(P_1,Q) = D_k(X_1,\cdots,X_{n-1})T^k+\cdots+D_0(X_1,\cdots X_{n-1}).$$

(c) En utilisant les propriétés du résultant, prouver que les $D_0,\cdots,D_k$ sont dans l'idéal engendré par $P_1,\cdots P_m$.

(d) Montrer que les $D_0,\cdots,D_k$ sont sans zéro commun, et conclure par récurrence.

(e) En quoi cette preuve est-elle explicite ?