Dans tout ce problème, $\mathbb{K}$ désigne un corps commutatif quelconque.

Soient m, n deux entiers naturels non-nuls. Si $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{j=0}^{m} b_j X^j$ sont deux éléments de $\mathbb{K}[X]$ de degrés respectifs n et m, on appelle résultant de P et Q, noté $\mathrm{Res}_{\mathbb{K}}(P,Q)$ (ou bien $\mathrm{Res}(P,Q)$ si aucune confusion n'est possible) le déterminant de la matrice carrée à coefficients dans $\mathbb{K}$ de taille $(n+m, n+m)$:

$$\begin{vmatrix}
a_0 & 0 & \cdots & \cdots & 0 & b_0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
a_1 & a_0 & \ddots & & & b_1 & \ddots & \ddots & & & & \vdots & \vdots \\
\vdots & \ddots & \ddots & \ddots & & \vdots & \ddots & \ddots & \ddots & & & \vdots & \vdots \\
\vdots & & \ddots & \ddots & 0 & \vdots & & \ddots & \ddots & \ddots & & \vdots & \vdots \\
\vdots & & & \ddots & a_0 & b_{m-1} & & & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & & & & a_1 & b_m & & & & \ddots & \ddots & 0 & \vdots \\
\vdots & & & & \vdots & 0 & \ddots & & & & \ddots & b_0 & 0 \\
a_{n-1} & a_{n-2} & \cdots & \cdots & a_{n-m} & \vdots & \ddots & \ddots & & & & b_1 & b_0 \\
a_n & a_{n-1} & & & \vdots & \vdots & & \ddots & \ddots & & & b_2 & b_1 \\
0 & \ddots & & & \vdots & \vdots & & & \ddots & \ddots & & \vdots & \vdots \\
\vdots & \ddots & \ddots & & \vdots & \vdots & & & & \ddots & \ddots & \vdots & \vdots \\
\vdots & & \ddots & \ddots & \vdots & \vdots & & & & & \ddots & b_m & b_{m-1} \\
0 & \cdots & \cdots & 0 & a_n & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_m
\end{vmatrix}$$

La matrice dont le résultant est le déterminant est appelée *matrice résultante*. On la notera $R(P,Q)$. Ces m premières colonnes contiennent les coefficients de P (décalés vers le bas à chaque colonne) ; les n colonnes suivantes contiennent les coefficients de Q (décalés vers le bas à chaque colonne).

Par exemple si $P = 1 - 2X + 5X^2 + 4X^3$ et $Q = -1 + 3X + 2X^2$

$$\mathrm{Res} = \begin{vmatrix}
1 & 0 & -1 & 0 & 0 \\
-2 & 1 & 3 & -1 & 0 \\
5 & -2 & 2 & 3 & -1 \\
4 & 5 & 0 & 2 & 3 \\
0 & 4 & 0 & 0 & 2
\end{vmatrix}$$

Enfin, si A est un sous-anneau de $\mathbb{K}$, on notera $A[X]$ le sous-anneau de l'anneau des polynômes $\mathbb{K}[X]$, constitué des polynômes dont tous les coefficients sont dans A.

I. Résultats préliminaires :

Soit A un sous-anneau d'un corps commutatif k.

(1) Vérifier que $A[X]$ est bien un sous anneau de $k[X]$.

(2) Montrer que si P, Q sont deux éléments de $A[X]$, alors $\mathrm{Res}_k(P,Q)$ est un élément de A.

(3) On se place dans le cas particulier $A = \mathbb{K}[X]$ et $k = \mathbb{K}(X)$ avec $\mathbb{K}$ un corps. On considère donc $\mathbb{K}[X][Y]$ le sous-anneau de l'anneau $\mathbb{K}(X)[Y]$ des polynômes sur le corps des fractions rationnelles $\mathbb{K}(X)$. Montrer que tout élément P de $\mathbb{K}[X][Y]$ s'écrit de façon unique sous la forme $P(X,Y) = \sum_{i,j \geq 0} a_{i,j} X^i Y^j$ avec $a_{ij} \in \mathbb{K}$ nul sauf pour un nombre fini de couples (i,j).

(4) En déduire que si $P \neq 0$ est un élément de $k[X][Y]$ s'écrivant comme ci-dessus, alors le nombre $d(P) = \max\{i + j \ / \ a_{i,j} \neq 0\}$ est un entier naturel bien défini, appelé degré total de P.

II. Propriété fondamentale du résultant :

Soient $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{j=0}^{m} b_j X^j$ deux polynômes de $\mathbb{K}[X]$ de degrés n et m.

(1) Montrer que les polynômes P et Q ne sont pas premiers entre eux dans $\mathbb{K}[X]$ si et seulement si il existe deux polynômes A et B non-nuls de $\mathbb{K}[X]$, de degrés $\deg A < m$ et $\deg B < n$, tels que $AP = BQ$.

On note $\mathbb{K}_d[X]$ le sous-espace vectoriel de $\mathbb{K}[X]$ constitué des polynômes de degré inférieur ou égal à d.

On pose ϕ l'application

$$\phi : \begin{cases} E = \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] & \to \mathbb{K}_{m+n-1}[X] \\ (A,B) & \mapsto AP + BQ \end{cases}.$$

(2) Montrer que ϕ est une application linéaire.

(3) On note $\mathcal{B} = ((1,0),(X,0),\ldots,(X^{q-1},0)(0,1),(0,X),\ldots,(0,X^{p-1}))$, base de E. Quelle est la matrice de ϕ dans les bases $\mathcal{B}$ et $\mathcal{B}_0$?

(4) Montrer que P et Q sont premiers entre eux dans $\mathbb{K}[X]$ si et seulement si ϕ est bijective.

(5) En déduire que P et Q sont premiers entre eux dans $\mathbb{K}[X]$ si et seulement si $\mathrm{Res}_{\mathbb{K}}(P,Q) \neq 0$.

III. **Autres expressions du résultant :**

(1) On peut remarquer que l'on peut définir $\mathrm{Res}(P,Q)$ dès lors que $m+n \in \mathbb{N}^*$ même si $m=0$ ou $n=0$. Que vaut $\mathrm{Res}(\alpha,Q)$ pour $\alpha \in \mathbb{K}$ non nul ?

(2) Relier $\mathrm{Res}(P,Q)$ et $\mathrm{Res}(Q,P)$.

(3) On suppose $n \geq m \geq 1$. Soit R le reste de la division euclidienne de P par Q. Montrer que $Res(P,Q)=0$ si $R=0$, et $Res(P,Q) = b_m^{n-r}\mathrm{Res}(R,Q)$ si $r=\deg(R)$.

(4) On suppose les deux polynômes scindés : $P = \alpha\prod_{i=1}^{n}(X-\lambda_i)$, $Q = \beta\prod_{j=1}^{m}(X-\mu_j)$. Montrer que

$$\mathrm{Res}(P,Q) = \beta^n \prod_{j=1}^{m} P(\mu_j) = \alpha^m\beta^n \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (\mu_j - \lambda_i).$$

(5) Montrer que pour tout λ non nul, on a

$$\mathrm{Res}(\lambda^n P(\frac{X}{\lambda}), \lambda^m Q(\frac{X}{\lambda})) = \lambda^{mn}\mathrm{Res}_{\mathbb{C}}(P(X),Q(X)).$$

IV. **Discriminant :**

On appelle discriminant d'un polynôme $P \in \mathbb{K}[X]$ (de degré supérieur ou égal à 2) le résultant $\mathrm{Res}(P,P')$.

(1) Calculer pour $P = aX^2+bX+c$ le discriminant de P, et le comparer avec le discriminant habituel $\Delta = b^2-4ac$.

(2) Montrer que $P \in \mathbb{C}[X]$ admet une racine multiple si et seulement si son discriminant est nul.

(3) Soit $P = X^3+pX+q \in \mathbb{C}[X]$. Calculer son discriminant et en déduire une condition sur $(p,q) \in \mathbb{C}^2$ pour que P admette une racine multiple. Comment aurait-on pu trouver cette condition (sans discriminant) ?

(4) Dans le cas d'un polynôme scindé sur $\mathbb{K}$ exprimer le discriminant en fonction de $\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)$ où les $(\alpha_i)_i$ désignent les racines de P.

(5) Sous ces mêmes hypothèses, l'exprimer en fonction du produit $\prod_{i=1}^{n} P'(\alpha_i)$.

V. **Entiers algébriques :**

On note $\mathcal{O}$ l'ensemble des nombres complexes z pour lesquels il existe un polynôme non-nul $P(X) \in \mathbb{Z}[X]$ (l'anneau des polynômes à coefficients dans $\mathbb{Z}$), qui soit *unitaire* (c'est-à-dire par définition de coefficient dominant égal à 1), et vérifiant $P(z)=0$.

(1) Soient z_1 et z_2 des éléments de $\mathcal{O}$, annulant les polynômes P_1 et P_2 de degrés respectifs n_1 et n_2. Montrer que le polynôme (en X) $R(X) = \mathrm{Res}_{\mathbb{Q}(X)}(P_1(X-Y),P_2(Y))$ est un élément de $\mathbb{Z}[X]$, unitaire de degré n_1n_2.

(2) Montrer que R annule la somme z_1+z_2.

(3) Procéder de même pour trouver un polynôme de $\mathbb{Z}[X]$ qui annule z_1z_2. En déduire que $\mathcal{O}$ est un sous-anneau de $\mathbb{C}$.

(4) Déterminer un polynôme à coefficients entiers de degré 4 ayant pour racine $\sqrt{3}+\sqrt{7}$. Quelles sont les autres racines de ce polynôme.