Définition. *Soit $\mathcal{A}$ un anneau (commutatif et unitaire) et soient*

$$P(T) = a_p T^P + a_{p-1}T^{p-1} + \cdots a_0, \quad Q(T) = b_q T^q + b_{q-1}T^{q-1} + \cdots + b_0$$

deux polynômes non-nuls de $\mathcal{A}[X]$ tel que $a_p \neq 0$, $b_q \neq 0$ et $p + q > 0$. ***La matrice de Sylvester associée à P et Q*** *est la matrice carrée $(p+q) \times (p+q)$ définie ainsi*

$$S_{P,Q} = \begin{pmatrix} a_p & a_{p-1} & a_{p-2} & \dots & 0 & 0 & 0 \\ 0 & a_p & a_{p-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & a_2 & a_1 & a_0 \\ b_q & b_{q-1} & b_{q-2} & \dots & 0 & 0 & 0 \\ 0 & b_q & b_{q-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{pmatrix}$$

(Il y a q lignes avec les coefficients de P.)
Le déterminant de la matrice $S_{P,Q}$ est appelé ***résultant de P et Q*** *et sera noté* $\operatorname{res}_T(P, Q)$.

Remarque. Le resultant des polynômes à coefficients dans un anneau intègre $\mathcal{A}$, pourrais toujours être calculé dans le corps des fraction $Fr(\mathcal{A})$ de $\mathcal{A}$, où dans la clôture algébrique de $Fr(\mathcal{A})$, puisque $\mathcal{A} \subset \overline{Fr(\mathcal{A})}$.

Théorème 1. *Si $\mathcal{A}$ est intègre alors les conditions suivantes sont équivalentes :*

1. $\operatorname{res}_T(P, Q) = 0$.
2. *il existe des polynômes non-nuls U, V de $\mathcal{A}[T]$ tels que* $\deg U < q$, $\deg V < p$ *et*

$$U(T)P(T) + V(T)Q(T) = 0.$$

Si, en plus, $\mathcal{A}$ est factoriel alors elles sont équivalentes à

3. $\deg \operatorname{pgcd}(P, Q) > 0$.

Théorème 2. *Supposons $\mathcal{A}$ intègre et designons par $\alpha_1, \dots, \alpha_p$, resp. $\beta_1, \dots, \beta_q$, les racines de P, resp. Q, dans la clôture algébrique du corps des fractions de $\mathcal{A}$. Alors*

$$\operatorname{res}_T(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j).$$

Notons que la matrice transposée ${}^tS_{P.Q}$ est la matrice du morphisme des $\mathcal{A}$-modules

$$\mathcal{R} : \mathcal{A}_{q=1}[T] \times \mathcal{A}_{p-1}[T] \to \mathcal{A}_{p+q-1}[T], \quad (U, V) \to UP + VQ$$

dans les bases $(T^{q-1}, 0), (T^{q-2}, 0), \ldots, (1, 0), (0, T^{p-1}), (0, T^{p-2}), \ldots, (0, 1)$ et $T^{p+q-1}, \ldots, 1$.

Identité de Bezout :
Dans l'anneau $\mathbb{Z}[A_p, \ldots, A_0, B_q, \ldots, B_0][T]$ considérons la matrice de Sylvester $S_{P.Q}$ des polynômes

$$P(A, T) = A_p T^P + A_{p-1} T^{p-1} + \cdots A_0, \quad Q(T) = B_q T^q + B_{q-1} T^{q-1} + \cdots + B_0,$$

où $A_p, \ldots, A_0, B_q, \ldots, B_0$ sont des indéterminées. Dans cette matrice on fait réapparaître les polynômes P et Q dans la dernière colonne en mulipliant la j-ème colonne par T^{p+q-j} et en l'ajoutant à la dernière colonne. On obtient

$$\begin{pmatrix}
A_p & A_{p-1} & A_{p-2} & \ldots & 0 & 0 & T^{q-1}P(T) \\
0 & A_p & A_{p-1} & \ldots & 0 & 0 & T^{q-2}P(T) \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & A_1 & A_0 & TP(T) \\
0 & 0 & 0 & \ldots & A_2 & A_1 & P(T) \\
B_q & B_{q-1} & B_{q-2} & \ldots & 0 & 0 & T^{p-1}Q(T) \\
0 & B_q & B_{q-1} & \ldots & 0 & 0 & T^{p-2}Q(T) \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & B_1 & B_0 & TQ(T) \\
0 & 0 & 0 & \ldots & B_2 & B_1 & Q(T)
\end{pmatrix}$$

En développant le long de la dernière colonne on obtient une relation

$$\mathrm{res}_T(P, Q) = U(A, B, T)P(A, T) + V(A, B, T)Q(B, T),$$

où $U, V \in \mathbb{Z}[A_p, \ldots, A_0, B_q, \ldots, B_0, T]$.

Preuve du Théorème 1. Si $\mathrm{res}_T(P, Q) = 0$ alors l'équation $\mathcal{R}(U, V) = 0$ admet une solution non-nulle (dans $Fr(\mathcal{A})$ et donc dans $\mathcal{A}$). Si $U \neq 0$ alors $V \neq 0$. Ça montre que 1. donne 2.
Réciproquement, si $\mathrm{res}_T(P, Q) \neq 0$ alors par l'identité de Bezout, P et Q sont premiers entre eux dans $Fr(\mathcal{A})$. Donc l'équation $\mathcal{R}(U, V) = 0$ n'a pas de solutions non-nulles.
L'équivalence de 2. et 3. dans un anneau factoriel est classique.

Preuve du Théorème 2.
Considérons le résultant des deux polynômes de $\mathbb{Z}[A_p, B_q, T_1, \ldots, T_p, U_1, \ldots U_q][T]$

$$P(T) = A_p(T - T_1) \cdots (T - T_p), \quad Q(T) = B_q(T - U_1) \cdots (T - U_q).$$

Dans $\mathbb{Z}[A_p, B_q, T_1, \ldots, T_p, U_1, \ldots U_q]$, anneau factoriel, on considère l'élement

$$S = A_p^q B_q^p \prod_{i,j} (T_i - U_j).$$

Nous allons montrer que A_p^q, B_q^p et les $T_i - U_j$ divise chacune $res_T(P,Q)$. Le coefficient de T^k est $(-1)^{p-k} A_p \sigma_{p-k}(T_1, \ldots, T_p)$. Alors A_p divise chaque terme de q premières lignes de $S_{P,Q}$. Ainsi A_p^q divise $res_T(P,Q)$.
On divise $res_T(P,Q)$ par $T_i - U_j$ considéré comme polynome unitaire en T_i. Le reste de la division est le résultant des polynômes P et Q ou on remplace T_i par U_j. Ceux deux polynômes ont un facteur $T - U_j$ commun, est donc par Théorème 1 leur résultant est nul. Alors $res_T(P,Q)$ est divisible par S :

$$res_T(P,Q) = \lambda S$$

Le calcul du degré de $res_T(P,Q)$ par rapport aux T_i, resp. U_j, montre que ce degré ne depasse pas q, resp. p. Même pour A_p, resp. B_q. Alors $\lambda \in \mathbb{Z}$. Prénons comme exemple $P = (T+1)^p, Q = T^q$, pour calculer que, en fait $\lambda = 1$:

$$res_T(P,Q) = A_p^q B_q^p \prod_{i,j} (T_i - U_j).$$

Ça termine la démonstration du Théorème 2.

Références : R. Goblot, Algèbre commutative. Cours et exercices corrigés, Dunod)
Leçons concernées :
117 Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.
123 Déterminant. Exemples et applications..
140 Systèmes d'équations linéaires. Systémes échelonnés. Résolution. Exemples et applications.
146 Résultant de deux polynômes, application à l'intrsection de courbes ou de surfaces algébriques.

Exercice 1. Les propriétés du résultant peuvent se changer si on ne suppose plus que $a_p \neq 0$ et $b_q \neq 0$.

1. Montrer que si $\deg P < p$ et $\deg Q < q$ mais on les considère comme polynômes de degré p et q repectivement alors $\mathrm{res}(Q, P) = 0$.
2. Supposons que $\deg P = p$ et $\deg Q = q$. Pour $q' \geq q$ désignons par $\mathrm{res}_{p,q'}(Q, P)$ le résultant de P et Q considerés comme les polynômes de degré p et q' repectivement. Alors

$$\mathrm{res}_{p,q'}(Q, P) = a_p^{q'-q} \mathrm{res}_{p,q}(Q, P).$$

Exercice 2.

1. Montrer que $\mathrm{res}(Q, P) = (-1)^{pq} \mathrm{res}(P, Q)$.
2. Calculer $\mathrm{res}(P, P)$.
3. Calculer $\mathrm{res}(Q, P)$ pour les polynômes de degré ≤ 2.
4. Sous les hypothèses du Théorème 2 montrer que

$$\mathrm{res}_T(P, Q) = a_p^q \prod_{i=1}^{p} Q(\alpha_i) = (-1)^{pq} b_q^p \prod_{j=1}^{q} P(\beta_j).$$

Exercice 3. Calculer le résultant $\mathrm{res}_Y(P, Q)$ des polynômes $P = X^2 - XY + Y^2 - 1$ et $Q = 2X^2 + Y^2 - Y - 2$ par rapport à la variable Y. Utiliser le résultat pour trouver les points d'intersection des ellipses d'équations $P = 0$ et $Q = 0$.

Exercice 4. Soient A et B deux polynômes scindé de $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps. Proposer un polynôme dont les racines sont les sommes d'une racine de A et d'une racine de B. (Quels sont les Y tels que le système $A(X) = B(Y - X) = 0$ ait une solution ?)
Proposer un polynôme à coefficients entiers qui a $\sqrt{2} + \sqrt{3}$ pour racine, et un autre qui a $\sqrt{2} + \sqrt[3]{7}$ comme racine.

Exercice 5. Soient $\mathbb{K}$ un corps, $f, g \in \mathbb{K}[X]$, $\deg f = n$, $\deg g = m$, et soient $\alpha_1, ..., \alpha_n$ les zéros de f et $\beta_1, ..., \beta_m$ les zéros de g. Construire (en termes de résultants) un polynôme dont les zéros sont :

1. $\alpha_i + \beta_j$ avec $i \in \{1, ..., n\}$ et $j \in \{1, ..., m\}$.
2. $\alpha_i - \beta_j$ avec $i \in \{1, ..., n\}$ et $j \in \{1, ..., m\}$.
3. $\alpha_i \beta_j$ avec $i \in \{1, ..., n\}$ et $j \in \{1, ..., m\}$.
4. α_i / β_j avec $i \in \{1, ..., n\}$ et $j \in \{1, ..., m\}$ (on suppose $g(0) \neq 0$).

On dit que $z \in \mathbb{C}$ est algébrique s'il est racine d'un polynôme non-nul à coefficients entiers. Montrer que les nombres algébriques forment un corps.

Exercice 6. Comment fabriquer l'équation de la courbe paramétrée par $x = A(t)/B(t), y = F(t)/G(t)$, où A, B, F, G sont des polynômes ? Exemple :$x = t^2 + t + 1, y = (t^2 - 1)/(t^2 + 1)$.

Exercice 7. [Théorème de Bezout]
Soient $P, Q \in \mathbb{C}[X, Y]$ premier entre eux. Montrer que le système d'équations $P(x, y) = Q(x, y) = 0$ admet au plus $\deg P \deg Q$ solutions.

Exercice 8. (Discriminant)
Soit

$$P(T) = a_p T^P + a_{p-1} T^{p-1} + \cdots a_0, \quad a_p \neq 0, p > 1$$

un polynôme à coefficients dans un corps $\mathbb{K}$ de caractéristique zéro. Soient $\alpha_1, ..., \alpha_p$ les p racines de P (comptées avec multiplicité) dans un corps algébriquement clos $\overline{\mathbb{K}}$ contenant $\mathbb{K}$. Le discriminant de P, noté $\text{disc}(P)$, est

$$\text{disc}(P) = a_p^{2p-2} \prod_{1 \leq i < j \leq p} (\alpha_i - \alpha_j)^2.$$

1. Montrer que
$$a_p \text{disc} P = (-1)^{p(p-1)/2} \text{res}(P, P').$$
2. Soient P_1 et P_2 deux polynômes unitaires. Exprimer $\text{disc}(P_1 P_2)$ en fonction de $\text{disc}(P_1)$, $\text{disc}(P_2)$ et $\text{res}(P_1, P_2)$.
3. Calculer le discriminant de $X^p + aX + b \in \mathbb{C}[X]$, $p > 1$, $a \neq 0$.