Loi de réciprocité quadratique avec les résultants

Perrine Jouteur

Ce développement est inédit à ma connaissance. Je l'ai trouvé dans le livre *Nombres et algèbres* de Jean-Yves Mérindol. Son grand avantage est qu'il peut se placer dans plein de leçons d'algèbre : 120, 121, 123, 126, 140, 142, 144 et 152. Le prix à payer pour cette profusion de recasages est la longueur du développement, qui nécessite plusieurs entraînements avant de le maîtriser en quinze minutes. Je conseille d'ailleurs d'admettre toute la mise en place et de commencer la présentation à partir du lemme 0.3.

Remarque 0.1 Soient A un anneau, et $P, Q \in A[X, S, T]$. Alors

$$\mathrm{Res}_X(P,Q)(T,T) = \mathrm{Res}_X(P(X,T,T), Q(X,T,T)).$$

Lemme 0.1 Soient $P, Q \in \mathbb{Z}[X]$, unitaires, factorisés sur $\mathbb{C}$ en $P = \prod_{i=1}^{n}(X - a_i)$ et $Q = \prod_{j=1}^{m}(X - b_j)$. Alors on a

$$\mathrm{Res}(P,Q) = \prod_{i=1}^{n} Q(a_i) = (-1)^{nm} \prod_{j=1}^{m} P(b_j).$$

Démonstration
Considérons les indéterminées $S_1, \cdots, S_n$ et $T_1, \cdots, T_m$, et l'anneau $A = \mathbb{Z}[S_1, \cdots, S_n, T_1, \cdots, T_m]$. On va travailler avec les polynômes suivant :

$$\tilde{P}(X) = \prod_{i=1}^{n}(X - S_i) \text{ et } \tilde{Q}(X) = \prod_{j=1}^{m}(X - T_j).$$

On va déterminer le résultant en X de ces deux polynômes. Ce résultant est un élément de A, donc un polynôme en $S_1, \cdots, S_n, T_1, \cdots, T_m$. De plus, d'après la remarque 1, pour tout $i \in [\![1, n]\!]$, pour tout $j \in [\![1, m]\!]$,

$$\mathrm{Res}_X(\tilde{P}, \tilde{Q})(S_1, \cdots, S_{i-1}, T_j, S_{i+1}, \cdots, S_n, T_1, \cdots, T_m) = \mathrm{Res}_X(\hat{P}, \hat{Q})$$

où $\hat{P}, \hat{Q} \in \mathbb{Z}[S_1, \cdots, S_{i-1}, S_{i+1}, \cdots, S_n, T_1, \cdots, T_m]$ sont définis en remplaçant la variable S_i par T_j. Or $\hat{P}$ et $\hat{Q}$, en tant que polynômes en X, ont pour racine commune T_j, et donc leur résultant en X est nul. Donc T_j est racine du polynôme $\mathrm{Res}_X(\tilde{P}, \tilde{Q})$ quand on le voit comme un polynôme en S_i.
Finalement pour tout $i \in [\![1, n]\!]$, pour tout $j \in [\![1, n]\!]$, on a $S_i - T_j$ qui divise $\mathrm{Res}_X(\tilde{P}, \tilde{Q})$. Comme les éléments $S_i - T_j$ sont premiers entre eux deux à deux dans A, et que A est factoriel, on a finalement que $\prod_{i=1}^{n}\prod_{j=1}^{m}(S_i - T_j)$ divise $\mathrm{Res}_X(\tilde{P}, \tilde{Q})$ dans A, et donc il existe $a \in A$ tel que

$$\mathrm{Res}_X(\tilde{P}, \tilde{Q}) = a \prod_{i=1}^{n}\prod_{j=1}^{m}(S_i - T_j)$$

ce qui se réécrit :

$$\mathrm{Res}_X(\tilde{P}, \tilde{Q}) = a \prod_{i=1}^{n} \tilde{Q}(S_i) = a(-1)^{nm} \prod_{j=1}^{m} P(T_j).$$

Il reste à montrer que $a = 1$. Pour cela, on va utiliser le fait que le résultant de deux polynômes est un polynôme en leurs coefficients, et procéder ainsi à une identification. Plus précisément, dans la suite on considère que $\mathrm{Res}_X(\tilde{P}, \tilde{Q})$ est un polynôme en les coefficients de $\tilde{Q}$.
Développons les polynômes $\tilde{P}$ et $\tilde{Q}$ en tant que polynômes en X à coefficients dans A :

$$\tilde{P} = x_n X^n + \cdots + x_1 X + x_0 \text{ et } \tilde{Q} = y_m X^m + \cdots + y_1 X + y_0.$$

Le résultant en X de ces deux polynômes s'écrit :

$$\begin{vmatrix} x_n & & \cdots & & x_0 & & \\ & \ddots & & & & \ddots & \\ & & x_n & & \cdots & & x_0 \\ y_m & \cdots & & y_0 & & & \\ & \ddots & & & \ddots & & \\ & & y_m & & \cdots & & y_0 \end{vmatrix}.$$

En particulier, la diagonale est composée de x_n et de y_0, et ces variables sont uniquement le long de la diagonale, donc dans l'écriture développée de $\mathrm{Res}_X(\tilde{P}, \tilde{Q})$ comme polynôme en les y_j, le coefficient devant y_0^n vaut x_n^m.
Mais comme $\tilde{P}$ est unitaire en tant que polynôme en X, on a $x_n = 1$ et donc le coefficient devant y_0^n vaut 1.
Enfin, grâce à l'écriture $\mathrm{Res}_X(\tilde{P}, \tilde{Q}) = a\prod_{i=1}^n \tilde{Q}(S_i) = a\prod_{i=1}^n (y_m S_i^m + \cdots + y_1 S_i + y_0)$, on sait que le coefficient devant y_0^n est a. Par identification, $a = 1$, ce qui conclut la preuve. ■

Remarque 0.2 On aurait aussi pu démontrer cela par récurrence sur $\deg(P) + \deg(Q)$.

Proposition 0.1 Réciprocité des résultants
Soient P, Q deux polynômes à coefficients dans $\mathbb{Z}$, de degrés n et m. Alors

$$\mathrm{Res}(P, Q) = (-1)^{nm}\,\mathrm{Res}(Q, P).$$

Démonstration
C'est un corollaire immédiat du lemme 1. Sinon, il s'agit simplement d'utiliser l'alternance du déterminant.■

Lemme 0.2 Soit $P \in \mathbb{Z}[X]$, de degré pair $n = 2d$. Supposons de plus que P soit symétrique, c'est-à-dire que son homogénéisé $\bar{P}$ vérifie $\bar{P}(X, Y) = \bar{P}(Y, X)$.
Alors il existe un polynôme $V \in \mathbb{Z}[T]$ de degré d tel que $V(X + X^{-1}) = X^{-d}P(X)$.

Démonstration
Considérons le polynôme homogène $\bar{P}$: par hypothèse, il est symétrique, et donc c'est un polynôme en $\sigma_1 = X + Y$ et $\sigma_2 = XY$. Donc il existe $Q \in \mathbb{Z}[\sigma_1, \sigma_2]$ tel que $\bar{P}(X, Y) = Q(X + Y, XY)$.
Écrivons $Q = \sum_{i,j} q_{i,j}\sigma_1^i\sigma_2^j$. On a

$$Q(X + Y, XY) = \sum_{i,j} q_{i,j} \sum_{k=0}^{i} \binom{i}{k} X^{k+j}Y^{i-k+j} = \overline{P}(X, Y).$$

Mais $\overline{P}$ est homogène de degré $2d$ donc pour tous i, j tels que $q_{ij} \neq 0$, $i + 2j = 2d$, et donc i est nécessairement pair.
Ainsi en réalité, $Q = \sum_{i,j} q_{2i,j}\sigma_1^{2i}\sigma_2^j$. Donc en fait Q est un polynôme en σ_1^2 et en σ_2, donc en $X^2 + Y^2$ et XY car σ_1^2 est un polynôme en $X^2 + Y^2$ et en σ_2. On note $\tilde{Q}$ ce polynôme en $X^2 + Y^2$ et en XY, de telle sorte que $\tilde{Q}(X^2 + Y^2, XY) = \overline{P}(X, Y)$ et $\tilde{Q}$ est un polynôme homogène de degré d.

Posons alors $V(T) = \tilde{Q}(T, 1)$. On a

$$X^d V(X + X^{-1}) = X^d\tilde{Q}(X + X^{-1}, 1) = \tilde{Q}(X^2 + 1, X) = \overline{P}(X, 1) = P(X).$$

D'où le résultat. ■

Théorème 0.1 Soient p, q deux nombres premiers impairs distincts. Alors

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Démonstration
Soit p un nombre premier impair. Le polynôme $X^{p-1}+\cdots+X+1$ est symétrique de degré pair, donc par le lemme 2, il existe un polynôme $V_p(T) \in \mathbb{Z}[T]$ tel que $V_p(X+X^{-1}) = X^{\frac{p-1}{2}}+\cdots+X+1+X^{-1}+\cdots+X^{-\frac{p-1}{2}}$.
On pose alors

$$K_p(Y) = V_p(Y + 2).$$

Alors K_p vérifie :

— $K_p(0) = p$
— $K_p(Y) \cong Y^{\frac{p-1}{2}}[p]$

Montrons que $\mathrm{Res}(K_p, K_q) = \left(\frac{p}{q}\right)$ modulo p.

On a calculé que $K_p(Y) = Y^{\frac{p-1}{2}}$ modulo p. Donc $\mathrm{Res}(K_p, K_q) = \mathrm{Res}(Y^{\frac{p-1}{2}}, K_q)$ modulo p. Et même mieux, grâce à la formule du lemme 1, on a

$$\mathrm{Res}(K_p, K_q) = \prod_{i=1}^{\frac{p-1}{2}} K_q(0) = q^{\frac{p-1}{2}}.$$

Ainsi $\mathrm{Res}(K_p, K_q)$ a la même classe que $\left(\frac{q}{p}\right)$ dans $\mathbb{Z}/p\mathbb{Z}$.
Pour conclure, on va montrer que $\mathrm{Res}(K_p, K_q)$ est inversible dans $\mathbb{Z}$. Procédons par l'absurde : supposons que $\mathrm{Res}(K_p, K_q)$ ne soit pas inversible dans $\mathbb{Z}$. Alors il existe un nombre premier r qui divise $\mathrm{Res}(K_p, K_q)$. Donc dans tout corps de caractéristique r, $\mathrm{Res}(K_p, K_q) = 0$. Ainsi sur une extension E de $\mathbb{F}_r$, les polynômes K_p et K_q ont une racine y commune. On a vu que $K_p(0) = p$ et $K_q(0) = q$ dans $\mathbb{Z}$, donc au moins l'un de ces deux nombres est non nul modulo r, et donc y n'est pas nulle. Quitte à grossir l'extension E, l'équation $x + x^{-1} - 2 = y$ admet une solution non nulle dans E. Cette solution x vérifie alors $K_p(x + x^{-1} - 2) = 0$ c'est-à-dire

$$x^{-\frac{p-1}{2}}(x^{p-1} + \cdots + x + 1) = 0.$$

Or x est non nulle, donc $x^{p-1} + \cdots + x + 1 = 0$. De plus y est non nulle donc x n'est pas égale à 1, et ainsi x est une racine non triviale de $X^p - 1$, dans E. Mais x vérifie la même relation pour K_q et donc x est aussi racine non triviale de $X^q - 1$ dans E. Ceci est absurde (car p et q sont premiers entre eux et donc le seul nombre qui est à la fois racine $p$ième et racine $q$ième est 1).
Finalement, $\mathrm{Res}(K_p, K_q)$ est inversible dans $\mathbb{Z}$ donc égal à ± 1, et la réduction modulo p permet de conclure :

$$\mathrm{Res}(K_p, K_q) = \left(\frac{q}{p}\right).$$

Et voilà ! ■