Loi de réciprocité quadratique par le résultant

Original page 361

Si $P(X) = \prod_{i=1}^{m}(X - a_i) \in A_m[X]$ et $Q \in A_n[X]$, alors

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

Corrigé

Si $P(X) = \prod_{i=1}^{m}(X - a_i) \in A_m[X]$ et $Q \in A_n[X]$, alors

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

Original page 362

Supposons qu'il existe $V \in A[X]$ telle que $P(X) = V(X + \frac{1}{X})$. On note $V(X) \stackrel{\text{def}}{=} \sum_{k=0}^{m} b_k X^k$ avec $b_m \neq 0$. On a alors

$$V(X + \frac{1}{X}) = b_m X^m + b_m X^{-m} + Q_1(X) + Q_2(X^{-1}),$$

où Q_1 et $Q_2 \in A[X]$ sont deux polynômes de degré strictement plus petit que m. Or $V(X + \frac{1}{X}) = P(X)$, ce qui donne $m = n$ et $b_n = a_n$ par identification des coefficients. Donc tout polynôme qui convient est de degré n et de coefficient dominant a_n.

Unicité : Soient V et U deux polynômes de $A[X]$ qui conviennent. On a alors $(V - U)(X + \frac{1}{X}) = P(X) - P(X) = 0$. Donc, par identification, le coefficient dominant de $V - U$ est nul ce qui est exclu à moins que $V - U = 0$. On a donc $V = U$, ce qui prouve l'unicité.

Existence : on procède par récurrence sur n. Si $n = 0$, alors $P = a_0$ et donc $V = a_0 \in A[X]$ convient. Soit n tel que la propriété soit vraie pour $n - 1$. Alors $P(X) - a_n(X + \frac{1}{X})^n$ est de la forme $\sum_{k=n-1}^{n-1} \alpha_k X^k$ avec $\alpha_k = \alpha_{-k}$ pour tout $k \in [\![1, n-1]\!]$. Ainsi, par hypothèse de récurrence, il existe $U \in A[X]$ tel que $U(X + \frac{1}{X}) = P(X) - a_n(X + \frac{1}{X})^n$. Ainsi $P(X) = U(X) + a_n X^n$ convient.

Corrigé

Unicité : Soient V et U deux polynômes de $A[X]$ qui conviennent. On a alors $(V - U)(X + \frac{1}{X}) = P(X) - P(X) = 0$. Donc, par identification, le coefficient dominant de $V - U$ est nul ce qui est exclu à moins que $V - U = 0$. On a donc $V = U$, ce qui prouve l'unicité.

Existence : on procède par récurrence sur n. Si $n = 0$, alors $P = a_0$ et donc $V = a_0 \in A[X]$ convient. Soit n tel que la propriété soit vraie pour $n - 1$. Alors $P(X) - a_n(X + \frac{1}{X})^n$ est de la forme $\sum_{k=n-1}^{n-1} \alpha_k X^k$ avec $\alpha_k = \alpha_{-k}$ pour tout $k \in [\![1, n-1]\!]$. Ainsi, par hypothèse de récurrence, il existe $U \in A[X]$ de degré $n - 1$ tel que $U(X + \frac{1}{X}) = P(X) - a_n(X + \frac{1}{X})^n$. Ainsi $V(X) = U(X) + a_n X^n$ convient car de degré n et de coefficient dominant a_n.

En effet, la partie originale en rouge est inutile car le polynôme créé dans la preuve d'existence est clairement de degré n et de coefficient dominant a_n. La partie supprimée peut par contre être utilisée pour préciser la preuve de l'unicité lorsque l'on montre que $V - U = 0$. En effet pour être plus précis il faudrait écrire $(V - U)(X)$ sous la forme $\sum_{k=0}^{m} b_k X^k$ pour bien voir ce qu'il se passe lorsqu'on dit que $(V - U)(X + \frac{1}{X}) = 0$.

Original page 363

Montrons que $\mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) = \left(\frac{p}{q}\right)$.

[...]

On a donc $A = \pm 1$ et $A = \left(\frac{p}{q}\right) \mod p$, d'où $A = \left(\frac{p}{q}\right)$.

On conclut à l'aide d'une propriété du résultant vis-à-vis de l'échange de ses arguments :

$$\begin{aligned}\left(\frac{p}{q}\right) &= \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)\\ &= (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \cdot \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_q, V_p)\\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right).\end{aligned}$$

Corrigé

Montrons que $\mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) = \left(\frac{q}{p}\right)$.

[...]

On a donc $A = \pm 1$ et $A = \left(\frac{q}{p}\right) \mod p$, d'où $A = \left(\frac{q}{p}\right)$.

On conclut à l'aide d'une propriété du résultant vis-à-vis de l'échange de ses arguments :

$$\begin{aligned}\left(\frac{q}{p}\right) &= \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)\\ &= (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \cdot \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_q, V_p)\\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).\end{aligned}$$