Calcul du résultant par l'algorithme d'Euclide

Jean-François Burnol, 6 février 2020 (2[e] version)

Définition et premières propriétés Soit $\mathbb{K}$ un corps, $\mathrm{A} \in \mathbb{K}[\mathrm{X}]$ un polynôme non nul de degré d, $\mathrm{B} \in \mathbb{K}[\mathrm{X}]$ un autre polynôme non nul, de degré e. Le résultant $\mathrm{R}(\mathrm{A}, \mathrm{B})$ est défini comme le déterminant dans les bases monomiales à puissances descendantes du morphisme $f : (\mathrm{U}, \mathrm{V}) \mapsto \mathrm{AU} + \mathrm{BV}$, $\deg \mathrm{U} < \deg \mathrm{B}$, $\deg \mathrm{V} < \deg \mathrm{A}$. Ce morphisme f va donc de $\mathbb{K}_{e-1}[\mathrm{X}] \times \mathbb{K}_{d-1}[\mathrm{X}]$ vers $\mathbb{K}_{d+e-1}[\mathrm{X}]$.

Je rappelle que $\mathbb{K}_n[\mathrm{X}]$ est le $\mathbb{K}$-espace vectoriel de dimension $n+1$ des polynômes de degrés au plus n, n donné dans $\mathbb{N}$. Et dans le paragraphe précédent (et suivant) on a besoin aussi de $\mathbb{K}_{-1}[\mathrm{X}]$ qui est $\{0\}$ puisque la constante nulle est le seul polynôme de degré au plus -1. La formule pour la dimension marche donc aussi pour $n = -1$.

Ce déterminant est non nul si et seulement le morphisme est surjectif. Ceci nécessite (attention, il y a une erreur corrigée dans le paragraphe suivant) qu'on puisse résoudre $\mathrm{AU} + \mathrm{BV} = 1$ avec $\deg \mathrm{U} < \deg \mathrm{B}$, $\deg \mathrm{V} < \deg \mathrm{A}$. On voit élémentairement que l'on peut laisser tomber la condition sur les degrés... blah blah blah

ATTENTION ! Si $d = e = 0$, il n'y a pas de « 1 » dans l'espace d'arrivée qui est l'espace vectoriel nul, donc NON, il n'est pas nécessaire de pouvoir résoudre $\mathrm{AU} + \mathrm{BV} = 1$ avec $\deg \mathrm{U} < \deg \mathrm{B}$, $\deg \mathrm{V} < \deg \mathrm{A}$ (heureusement d'ailleurs). Et à propos la matrice dont on veut calculer le déterminant... elle a disparu, elle est de taille 0×0 ! Ennuyeux. On conviendra que le résultant vaut 1 dans ce cas. Quelle autre valeur donner au déterminant d'une matrice qui n'existe pas ?

En fait ce que je voulais dire c'est que le résultant est non nul si et seulement si A et B sont premiers entre eux. Ça marche si les deux sont constants. Si un seul est constant, par exemple $\mathrm{B} = b \neq 0$, alors la matrice est la matrice diagonale de taille $\deg \mathrm{A} \times \deg \mathrm{A}$ avec b sur la diagonale (car $\mathbb{K}_{-1}[\mathrm{X}] = \{0\}$), le résultant $b^{\deg \mathrm{A}}$ est non nul, et il est vrai que A et B (constante non nulle) sont premiers entre eux.

Il reste donc à étudier le cas véritablement sérieux, c'est-à-dire $\deg A > 0$, $\deg B > 0$. Nous n'allons pas faire ici le raisonnement classique que vous trouverez partout pour valider « résultant non nul si et seulement si premiers entre eux », mais passer par une voie reliant le résultant à la division euclidienne et en particulier à l'algorithme d'Euclide pour le calcul du PGCD. Addendum : on va le voir aussi par extension de corps.

Le résultant est donc le déterminant de la matrice $(X^{e-1}A, \cdots, A, X^{d-1}B, \cdots, B)$ où chaque polynôme donne par ses coefficients dans $(X^{d+e-1}, \dots, X, 1)$ la colonne correspondante. Il en résulte les propriétés élémentaires suivantes :

1. $R(A, B) = (-1)^{\deg A \deg B} R(B, A)$,
2. $R(xA, yB) = x^{\deg B} y^{\deg A} R(A, B)$,
3. et le résultant est invariant par extension du corps $\mathbb{K}$.

Expression comme déterminant d'un endomorphisme Nous allons calculer le résultant après des opérations de colonnes (on suppose $\deg A = d > 0$, $\deg B = e > 0$ pour éviter des confusions liées à la manipulation de choses vides). Pour cela faisons la division euclidienne de $X^{d-1}B$ par A :

$$X^{d-1}B = Q_{d-1}A + R_{d-1}, \deg R_{d-1} < d$$

Le polynôme Q_{d-1} est de degré au plus $d - 1 + e - d = e - 1$ (en fait il est exactement de degré $e - 1$ mais nous ne voulons pas nous encombrer de préciser les degrés lorsque nous appliquerons la procédure aux colonnes qui suivent).

On peut alors en soustrayant à la colonne $X^{d-1}B$ la combinaison linéaire des colonnes $X^{e-1}A, \dots, A$ qui correspond aux coefficients de Q dans la base monomiale (descendante) remplacer $X^{d-1}B$ par la colonne des coefficients de R_{d-1}.

On procède ainsi non seulement pour la colonne $X^{d-1}B$ mais pour toutes les d colonnes $(X^{d-1}B, \dots, B)$ de la droite de la matrice, les transformant dans ce processus en les colonnes donnant les coefficients de certains polynômes $R_{d-1}, R_{d-2}, \dots, R_0$. Tous ces polynômes sont de degré au plus $d - 1$ et donc la nouvelle matrice a une forme par bloc avec un bloc en haut à gauche triangulaire inférieur à diagonale constante et un bloc en haut à droite identiquement nul. Son déterminant vaut

$$R(A, B) = \nu(A)^{\deg B} \det_{d\times d}(R_{d-1}, R_{d-2}, \dots, R_0) \qquad (d = \deg A)$$

On a noté $\nu(A)$ le coefficient dominant de A et cette notation $\nu(P)$ sera utilisée pour tout polynôme non nul P.

Mais cette matrice $d \times d$ est exactement celle de la multiplication par B dans $\mathbb{K}[X]/(A)$, dans la base monomiale descendante. Cela vaut le coup donc d'énoncer notre résultat comme un théorème :

Théorème 1. $\mathrm{R}(\mathrm{A},\mathrm{B}) = \nu(\mathrm{A})^{\deg \mathrm{B}} \det_{\mathbb{K}[\mathrm{X}]/(\mathrm{A})}(\mathrm{P} \mapsto \mathrm{BP} \pmod{\mathrm{A}})$.

Corollaire 1. *La relation suivante existe :*

$$\nu(\mathrm{A})^{\deg \mathrm{B}} \det_{\mathbb{K}[\mathrm{X}]/(\mathrm{A})}(\mathrm{P} \mapsto \mathrm{BP}) = (-1)^{\deg \mathrm{A} \deg \mathrm{B}} \nu(\mathrm{B})^{\deg \mathrm{A}} \det_{\mathbb{K}[\mathrm{X}]/(\mathrm{B})}(\mathrm{P} \mapsto \mathrm{AP})$$

Démonstration. En effet nous avons juste utilisé $\mathrm{R}(\mathrm{A},\mathrm{B}) = (-1)^{\deg \mathrm{A} \deg \mathrm{B}} \mathrm{R}(\mathrm{B},\mathrm{A})$. ◻

Calcul par factorisation Fixons pour le moment A, $\deg \mathrm{A} = d > 0$. Pour chaque $\mathrm{B} \in \mathbb{K}[\mathrm{X}]$ (pour l'instant même $\mathrm{B} = 0$ est autorisé) notons ϕ_B le morphisme de multiplication par B sur l'espace vectoriel $\mathrm{V} = \mathbb{K}[\mathrm{X}]/(\mathrm{A})$ de dimension d. Il est clair que $\phi_{\mathrm{B}_1\mathrm{B}_2} = \phi_{\mathrm{B}_1} \circ \phi_{\mathrm{B}_2} = \phi_{\mathrm{B}_2} \circ \phi_{\mathrm{B}_1}$. Donc si l'on calcule les déterminants, c'est multiplicatif. Et bien sûr $\deg(\mathrm{B}_1\mathrm{B}_2) = \deg \mathrm{B}_1 + \deg \mathrm{B}_2$. En combinant avec le Théorème 1, on peut donc affirmer :

Théorème 2. *Soit* $\mathrm{B} = \mathrm{B}_1^{k_1} \cdots \mathrm{B}_n^{k_n}$ *un produit quelconque de polynômes non nuls de* $\mathbb{K}[\mathrm{X}]$ *et* A *un polynôme non nul fixé. Alors*

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = \mathrm{R}(\mathrm{A},\mathrm{B}_1)^{k_1} \cdots \mathrm{R}(\mathrm{A},\mathrm{B}_n)^{k_n} \tag{1}$$

Démonstration. Il ne reste plus qu'à traiter le cas avec $\mathrm{A} = a$ une constante. Mais en revenant à la définition de départ $\mathrm{R}(a,\mathrm{B}) = a^{\deg \mathrm{B}}$. La formule vaut donc aussi pour de tels A. ◻

Corollaire 2. *Soit* $\mathrm{A} = \mathrm{A}_1^{k_1} \cdots \mathrm{A}_n^{k_n}$ *un produit quelconque de polynômes non nuls de* $\mathbb{K}[\mathrm{X}]$. *Alors, pour tout* $\mathrm{B} \in \mathbb{K}[\mathrm{X}]$*, non nul :*

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = \mathrm{R}(\mathrm{A}_1,\mathrm{B})^{k_1} \cdots \mathrm{R}(\mathrm{A}_n,\mathrm{B})^{k_n} \tag{2}$$

Démonstration du corollaire. On a $\mathrm{R}(\mathrm{A}_j,\mathrm{B}) = (-1)^{\deg \mathrm{A}_j \deg \mathrm{B}} \mathrm{R}(\mathrm{B},\mathrm{A}_j)$, $\mathrm{R}(\mathrm{A},\mathrm{B}) = (-1)^{\deg \mathrm{A} \deg \mathrm{B}} \mathrm{R}(\mathrm{B},\mathrm{A})$, et $\deg \mathrm{A} = \sum_i k_i \deg \mathrm{A}_i$. C'est donc une conséquence (équivalente) de Théorème 2. ◻

Corollaire 3. *Supposons que* $\mathrm{A} = \nu(\mathrm{A})\,(\mathrm{X}-\lambda_1) \cdots (\mathrm{X}-\lambda_n)$ *est factorisé sur* $\mathbb{K}$*, certaines racines pouvant apparaître plusieurs fois. Alors*

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = \nu(\mathrm{A})^{\deg \mathrm{B}} \prod_{1 \leqslant i \leqslant \deg \mathrm{A}} \mathrm{B}(\lambda_i)$$

La formule est encore valable si A *est une constante (non-nulle), en considérant qu'un produit vide vaut* 1.

Démonstration. On doit calculer $R(X-\lambda, B)$ mais par ce qui précède c'est le déterminant de l'endomorphisme de multiplication par B sur $\mathbb{K}[X]/(X-\lambda)$. Donc c'est $B(\lambda)$, puisque multiplier par B modulo $X-\lambda$ c'est la même chose que multiplier par $B(\lambda)$. □

Corollaire 4. *Supposons que* A *et* B *sont deux polynômes non nuls factorisés sur* $\mathbb{K}$*, de racines respectives (possiblement répétées)* λ_i*,* $1 \leqslant i \leqslant \deg A$*, et* μ_j*,* $1 \leqslant j \leqslant \deg B$*. Alors*

$$R(A, B) = \nu(A)^{\deg B}\nu(B)^{\deg(A)} \prod_{\substack{1\leqslant i\leqslant \deg A\\ 1\leqslant j\leqslant \deg B}} (\lambda_i - \mu_j)$$

Démonstration. Immédiate après ce qui précède. □

Corollaire 5. *Le résultant* $R(A, B)$ *est non nul si et seulement si* A *et* B *sont premiers entre eux.*

Démonstration. Le résultant est invariant par extension de corps et le fait pour deux polynômes d'être premiers entre eux aussi. En effet l'algorithme d'Euclide qui calcule le PGCD se déroule identiquement sur $\mathbb{K}$ ou toute extension de corps. On peut donc supposer que A et B sont entièrement factorisés et la conclusion vient alors de la formule précédente. □

Réduction du résultant par division euclidienne Faisons la division euclidienne (encore, mais ici c'est un tout autre contexte) de A par B : $A = BQ + R$ (désolé pour le clash de notation avec la lettre R utilisée aussi pour le résultant). Le morphisme $P \mapsto AP$ sur $\mathbb{K}[X]/(B)$ c'est exactement le même que $P \mapsto RP$. Par conséquent :

$$R(A, B) = (-1)^{\deg A \deg B}\nu(B)^{\deg A} \det_{\mathbb{K}[X]/(B)}(P \mapsto RP) \tag{3}$$

Mais par ailleurs d'après le théorème, et à condition que le reste R ne soit pas le polynôme nul (car je n'ai pas pris la peine jusqu'à présent de définir le résultant si l'un des deux polynômes est nul) :

$$R(B, R) = \nu(B)^{\deg R} \det_{\mathbb{K}[X]/(B)}(P \mapsto RP) \tag{4}$$

D'où notre second (non énième) théorème (encore désolé pour le clash de notation avec la lettre R utilisée aussi pour le résultant) :

Théorème 3. *Soit* A *et* B *deux polynômes non nuls, et* R *le reste dans la division euclidienne de* A *par* B.

— *Si* R *n'est pas le polynôme nul, alors*

$$R(A, B) = (-1)^{\deg A \deg B}\nu(B)^{\deg A-\deg R}R(B, R)$$

— *Si* $\mathrm{R} = 0$,

— *si* $\mathrm{B} = b$ *est un polynôme constant,* $\mathrm{R}(\mathrm{A}, \mathrm{B}) = b^{\deg \mathrm{A}}$,

— *si* $\deg \mathrm{B} > 0$ *alors* $\mathrm{R}(\mathrm{A}, \mathrm{B}) = 0$.

Démonstration. Si R n'est pas le polynôme nul, alors B n'est pas un polynôme constant. Et le résultat vient de la comparaison des équations (3) et (4). Si R est le polynôme nul, c'est-à-dire si B divise A, il faut faire bien attention et traiter à part le cas de $\mathrm{B} = b$ une constante. Si $\mathrm{R} = 0$ et $\deg \mathrm{B} > 0$ (alors A n'est pas une constante) on peut utiliser la formule avec le déterminant de la multiplication par A sur $\mathbb{K}[\mathrm{X}]/(\mathrm{B})$, qui est donc le morphisme nul, et conclure que $\mathrm{R}(\mathrm{A}, \mathrm{B}) = 0$. Si $\mathrm{B} = b$ est une constante on a sans doute déjà dit quelque part que $\mathrm{R}(\mathrm{A}, \mathrm{B}) = b^{\deg \mathrm{A}}$. Et on est à nouveau contents d'avoir défini $\mathrm{R}(\mathrm{A}, \mathrm{B}) = 1$ lorsqu'à la fois A et B sont des constantes ; autrement dit tout morphisme d'un espace vectoriel nul vers un autre espace vectoriel nul doit être considéré comme ayant déterminant 1 pour n'importe quel choix de bases ; ça tombe bien car on n'a pas beaucoup de choix.

Se souvenir que les histoires de résultant sont piégeuses en ce qui concerne les polynômes constants (sans même parler des polynômes nuls), qui cependant sont indispensables à la discussion approfondie. □

Calcul du résultant comme corrélat à celui du PGCD par l'algorithme d'Euclide Nous suivons maintenant l'algorithme d'Euclide pour le calcul de $\mathrm{PGCD}(\mathrm{A}, \mathrm{B})$. Notons R_1 le 1er reste (notre ancien R). On posera aussi $\mathrm{R}_0 = \mathrm{B}$ et $\mathrm{R}_{-1} = \mathrm{A}$. Puis R_2 le reste dans la division de B par R_1, etc..., jusqu'au dernier reste non nul R_k. Attention que le $\mathrm{PGCD}(\mathrm{A}, \mathrm{B})$ est souvent normalisé comme étant unitaire c'est donc $\mathrm{R}_k/\nu(\mathrm{R}_k)$.

On a la suite d'équations :

$$\begin{aligned}
\mathrm{R}(\mathrm{A}, \mathrm{B}) &= (-1)^{\deg \mathrm{A} \deg \mathrm{B}} \nu(\mathrm{B})^{\deg \mathrm{A} - \deg \mathrm{R}_1} \mathrm{R}(\mathrm{B}, \mathrm{R}_1) \\
\mathrm{R}(\mathrm{B}, \mathrm{R}_1) &= (-1)^{\deg \mathrm{B} \deg \mathrm{R}_1} \nu(\mathrm{R}_1)^{\deg \mathrm{B} - \deg \mathrm{R}_2} \mathrm{R}(\mathrm{R}_1, \mathrm{R}_2) \\
\ldots &= \ldots \\
\mathrm{R}(\mathrm{R}_j, \mathrm{R}_{j+1}) &= (-1)^{\deg \mathrm{R}_j \deg \mathrm{R}_{j+1}} \nu(\mathrm{R}_{j+1})^{\deg \mathrm{R}_j - \deg \mathrm{R}_{j+2}} \mathrm{R}(\mathrm{R}_{j+1}, \mathrm{R}_{j+2}) \\
\ldots &= \ldots \\
\mathrm{R}(\mathrm{R}_{k-2}, \mathrm{R}_{k-1}) &= (-1)^{\deg \mathrm{R}_{k-2} \deg \mathrm{R}_{k-1}} \nu(\mathrm{R}_{k-1})^{\deg \mathrm{R}_{k-2} - \deg \mathrm{R}_k} \mathrm{R}(\mathrm{R}_{k-1}, \mathrm{R}_k)
\end{aligned}$$

Et R_k divise R_{k-1}. D'après le théorème précédent si R_k n'est pas une constante, le résultant $\mathrm{R}(\mathrm{R}_{k-1}, \mathrm{R}_k)$ est nul, donc $\mathrm{R}(\mathrm{A}, \mathrm{B}) = 0$. Par contre si R_k est une constante $r_k \neq 0$, alors le résultant $\mathrm{R}(\mathrm{R}_{k-1}, \mathrm{R}_k)$ est non nul, en fait il vaut $r_k^{\deg \mathrm{R}_{k-1}}$.

Nous concluons que $\mathrm{R}(\mathrm{A}, \mathrm{B})$ est nul si et seulement si $\deg \mathrm{R}_k > 0$ c'est-à-dire si et seulement si $\deg \mathrm{PGCD}(\mathrm{A}, \mathrm{B}) > 0$.

Nous savions déjà cela. La méthode suivie nous donne une formule exacte qui est beaucoup plus efficace numériquement qu'un calcul de déterminant.

Théorème 4. *Soit* A *et* B *deux polynômes non nuls et* $\mathrm{R}_{1} = \mathrm{A}$*,* $\mathrm{R}_0 = \mathrm{B}$*, puis* R_1 *le reste dans la division euclidienne de* A *par* B*,* R_2 *celui dans la division de* B *par* R_1*, et ainsi de suite jusqu'au dernier reste non nul* R_k*,* $k \geqslant 0$*. Le résultant de* A *et* B *est nul si* $\deg \mathrm{R}_k > 0$*, sinon il est non nul et donné par la formule suivante :*

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = (-1)^{\sum_{0\leqslant j<k} \deg \mathrm{R}_{j-1} \deg \mathrm{R}_j} \prod_{0\leqslant j<k} \nu(\mathrm{R}_j)^{\deg \mathrm{R}_{j-1} - \deg \mathrm{R}_{j+1}} \nu(\mathrm{R}_k)^{\deg \mathrm{R}_{k-1}} \tag{5}$$

On peut la reformuler sous cette forme :

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = \nu(\mathrm{B})^{\deg \mathrm{A} - \deg \mathrm{B}} (-1)^{\sum_{0\leqslant j<k} \deg \mathrm{R}_{j-1} \deg \mathrm{R}_j} \prod_{0\leqslant j<k} \Big(\nu(\mathrm{R}_j)\nu(\mathrm{R}_{j+1})\Big)^{\deg \mathrm{R}_j - \deg \mathrm{R}_{j+1}} \tag{6}$$

Dans cette formule on rappelle que $\mathrm{R}_{-1} = \mathrm{A}$, $\mathrm{R}_0 = \mathrm{B}$, et R_k est une constante si A et B ont un résultant non nul. La formule fonctionne aussi si $\mathrm{A} = a$ et $\mathrm{B} = b$ sont deux constantes non nulles (un produit vide vaut 1, une somme vide vaut 0) et confirme que l'on pose $\mathrm{R}(a, b) = 1$ dans ce cas. Pour démontrer la deuxième formule on écrit $\deg \mathrm{R}_{j-1} - \deg \mathrm{R}_{j+1} = \deg \mathrm{R}_{j-1} - \deg \mathrm{R}_j + \deg \mathrm{R}_j - \deg \mathrm{R}_{j+1}$ et on regroupe deux à deux les termes successifs. Rappelons que $\deg \mathrm{R}_k = 0$ est supposé dans ces formules.

Génériquement (c'est-à-dire si on ne réfléchit pas trop) on s'attend à ce qu'à chaque étape le degré du reste diminue d'une unité. Donc pour $\mathrm{R}_0 = \mathrm{B}$ le degré est $\deg \mathrm{B} = e$, R_1 est attendu de degré $e - 1$ (à condition évidemment que $\deg \mathrm{A} \geqslant \deg \mathrm{B}$, sinon $\mathrm{R}_1 = \mathrm{A}$), R_2 de degré $e - 2$,...., R_e est probablement le dernier reste non nul et il est une constante. La formule devient donc, pour $\deg \mathrm{A} \geqslant \deg \mathrm{B}$ et si on est dans une situation générique :

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = \nu(\mathrm{B})^{\deg \mathrm{A} - \deg \mathrm{B} + 1} \cdot \Big(\prod_{1\leqslant j\leqslant k-1} \nu(\mathrm{R}_j)\Big)^2 \cdot \nu(\mathrm{R}_k)$$

La formulation alternative dans ce cas générique avec $\deg \mathrm{A} \geqslant \deg \mathrm{B}$ est :

$$\mathrm{R}(\mathrm{A},\mathrm{B}) = \nu(\mathrm{B})^{\deg \mathrm{A} - \deg \mathrm{B}} \prod_{0\leqslant j<k} \nu(\mathrm{R}_j)\nu(\mathrm{R}_{j+1})$$

Remarque : il n'est pas tout-à-fait trivial (mais pas bien compliqué non plus) à partir du Théorème 4 de retrouver la propriété élémentaire $\mathrm{R}(x\mathrm{A}, y\mathrm{B}) = x^{\deg \mathrm{B}} y^{\deg \mathrm{A}} \mathrm{R}(\mathrm{A},\mathrm{B})$. C'est un bon exercice.

Exemples Prenons $A = aX^2 + bX + c$ ($a \neq 0$), $B = A' = 2aX + b$, on calcule

$$aX^2 + bX + c = (2aX + b)(\frac{1}{2}X + \frac{b}{4a}) + c - \frac{b^2}{4a}$$

donc $k = 1$ et par la formule générale

$$R(A, A') = (-1)^{2\cdot 1}(2a)^2(c - \frac{b^2}{4a}) = -a(b^2 - 4ac)$$

C'est donc à peu près le *discriminant quadratique*. En fait on définit souvent le *discriminant* pour P de degré n par la formule :

$$\Delta(P) = \frac{(-1)^{n(n-1)/2}}{\nu(P)} R(P, P')$$

Pour $n = 2$, c'est fait pour donner $\Delta(A) = b^2 - 4ac$.

Considérons $A = P = X^3 + pX + q$, $B = P' = 3X^2 + p$. On calcule facilement : $R_1 = pX+q+X(-p/3) = (2pX+3q)/3$ puis $R_2 = 3(-3q/2p)^2+p = (4p^3+27q^2)/(4p^2)$. Bien sûr j'ai supposé $p \neq 0$ puis $4p^3 + 27q^2 \neq 0$ pour identifier le dernier reste non nul.

$$R(P, P') = (-1)^{3\cdot 2+2\cdot 1}3^{3-1}(2p/3)^{2-0}(4p^3 + 27q^2)/(4p^2) = 4p^3 + 27q^2$$

Attention que pour cette formule on a supposé $p \neq 0$, puis $4p^3+27q^2 \neq 0$. Cependant on sait que le résultat est un polynôme en p et q, donc la formule est valable généralement (par un raisonnement de densité sur les complexes, et nécessitant des techniques autres sur un corps quelconque). Et le calcul du déterminant de la matrice de Sylvester de taille 5×5 n'est pas si dantesque si on tient à vérifier à partir de la définition initiale.

Quant au discriminant le coefficient normalisateur est ici -1, donc $\Delta(P) = -4p^3 - 27q^2$.

Pour comprendre le coefficient normalisateur, on peut profiter de notre formule :

$$R(P, P') = \nu(P)^{\deg P - 1} \det_{\mathbb{K}[X]/(P)}(T \mapsto P'T)$$

Si $P = \nu(P) \prod (X - \lambda_i)$ est scindé à racines simples cela se calcule directement par l'isomorphisme des restes chinois (cette section a été rédigée avant d'ajouter le Théorème 2) et donne :

$$\begin{aligned} R(P, P') &= \nu(P)^{\deg P - 1} \prod_i P'(\lambda_i) \\ &= \nu(P)^{\deg P - 1} \prod_i \nu(P) \prod_{j \neq i} (\lambda_i - \lambda_j) \end{aligned}$$

$$= \nu(\mathrm{P})^{2\deg \mathrm{P}-1}(-1)^{n(n-1)/2}\prod_{i<j}(\lambda_i - \lambda_j)^2$$

donc le signe du coefficient normalisateur est choisi de sorte que pour un polynôme réel qui a toutes ses racines simples et réelles (et donc par continuité pour tout polynôme réel qui a toutes ses racines réelles) le discriminant

$$\Delta(\mathrm{P}) = \nu(\mathrm{P})^{2\deg \mathrm{P}-2}\prod_{i<j}(\lambda_i - \lambda_j)^2$$

est positif. La formule ci-dessus pour $\mathrm{R}(\mathrm{P}, \mathrm{P}')$ suppose que P a des racines distinctes mais si deux racines coïncident, P et P′ (P non constant !) ne sont pas premiers entre eux et le résultant $\mathrm{R}(\mathrm{P}, \mathrm{P}')$ est nul, donc la formule fonctionne aussi dans ce cas.

En fait on a depuis ajouté le Théorème 2 et ses corollaires ce qui rend inutiles certains arguments du paragraphe précédent.

Terminons avec le calcul du résultant de $\mathrm{A} = \mathrm{X}^4 + \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1$ et $\mathrm{B} = \mathrm{A}' = 4\mathrm{X}^3 + 3\mathrm{X}^2 + 2\mathrm{X} + 1$.

$$\begin{aligned}
\mathrm{A} &= \mathrm{X}^4 + \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1 \\
\mathrm{B} &= 4\mathrm{X}^3 + 3\mathrm{X}^2 + 2\mathrm{X} + 1 \\
\mathrm{R}_1 &= \frac{5}{16}\mathrm{X}^2 + \frac{10}{16}\mathrm{X} + \frac{15}{16} \\
\mathrm{R}_2 &= 16 \\
\mathrm{R}_3 &= 0 \\
\mathrm{R}(\mathrm{A}, \mathrm{B}) &= 4^1(-1)^{4\cdot 3+3\cdot 2}\left(4\frac{5}{16}\right)^1\left(\frac{5}{16}16\right)^2 = 5^3 = 125
\end{aligned}$$

Ça se calcule aussi très bien de tête par un déterminant 7×7 (j'ai mis sous forme transposée pour qu'il me soit plus simple d'écrire le déterminant ligne par ligne, puisque c'est sous cette forme que LaTeX l'attend) :

$$125 = \begin{vmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 \\
4 & 3 & 2 & 1 & 0 & 0 & 0 \\
0 & 4 & 3 & 2 & 1 & 0 & 0 \\
0 & 0 & 4 & 3 & 2 & 1 & 0 \\
0 & 0 & 0 & 4 & 3 & 2 & 1
\end{vmatrix}$$

Mais il faudrait réfléchir un peu plus au Théorème 4 car il fait passer par le corps des fractions (les coefficients dominants des restes peuvent être fractionnaires, comme on le voit sur l'exemple ci-dessus) alors qu'on sait que le résultat appartient à l'anneau des coefficients des polynômes A et B.