Leçon 143
Résultant. Applications.

Riffaut Antonin

2013-2014

Table des matières

Introduction

Considérons, dans l'espace affine $\mathbb{R}^2$, les deux courbes γ_1 et γ_2, décrites par leurs équations cartésiennes respectives $x^3-3xy^2+y^3-1=0$ et $x^2+2y^2+x-8=0$. Les courbes γ_1 et γ_2 s'intersectent-elles ? le cas échéant, combien y a-t-il de points d'intersection, et quelles sont leurs coordonnées ? La figure ci-dessous, réalisée avec le logiciel GeoGebra, met en évidence les 6 points d'intersection de γ_1 et γ_2 :

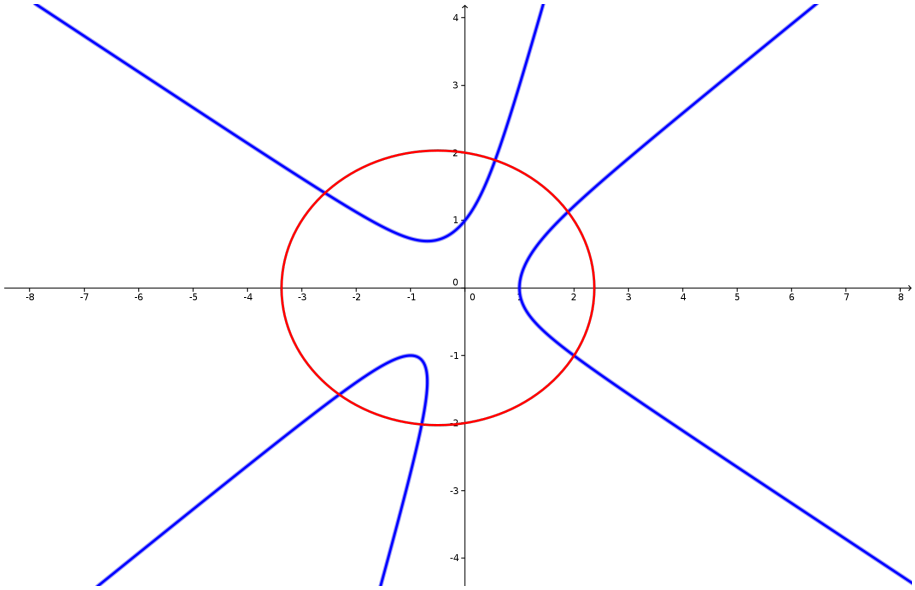

FIGURE 1 – Intersection des courbes γ_1 (en bleu) et γ_2 (en rouge)

Pouvait-on prévoir le nombre de points d'intersection de γ_1 et γ_2, ou, à défaut, en donner une borne ? Toutes ces questions s'inscrivent dans une problématique plus vaste : celle de la résolution des systèmes d'équations polynomiales. Si l'on définit les deux polynômes $P = X^3 - 3XY^2 + Y^3 - 1$ et $Q = X^2+2Y^2+X-8$ de $\mathbb{R}[X,Y]$, déterminer les points d'intersection de γ_1 et γ_2 revient à déterminer les *racines communes* de P et Q, c'est-à-dire les couples $(\alpha,\beta) \in \mathbb{R}^2$ tels que $P(\alpha,\beta) = Q(\alpha,\beta) = 0$.

De manière plus générale, si k désigne un corps quelconque, et $P_1,\dots,P_r$ des polynômes de $k[X_1,\dots,X_d]$, on s'intéresse au système d'équations polynomiales

$$\begin{cases} P_1(x_1,\dots,x_d) = 0 \\ \qquad\vdots \\ P_r(x_1,\dots,x_d) = 0 \end{cases},$$

d'inconnue $(x_1,\dots,x_d) \in k^d$. L'objectif de cette leçon est de développer la méthode dite *d'élimination*, via l'introduction de la notion de *résultant* de deux polynômes. Le principe de la méthode est de transformer le précédent système en un nouveau système, faisant intervenir moins d'inconnues, et potentiellement plus simple à traiter ; les informations obtenues à partir du nouveau système permettent alors d'apporter une solution partielle au système initial.

La première partie sera consacrée à la définition et aux propriétés fondamentales des résultants, ainsi qu'aux aspects élémentaires de la *théorie de l'élimination* ; nous détaillerons notamment la méthode d'élimination que l'on vient d'évoquer. Dans une deuxième partie, nous expliciterons une méthode effective de calcul de résultants, qui s'appuie sur l'algorithme d'Euclide, et les conséquences directes de cet algorithme sur le lien entre le résultant de deux polynômes et leurs racines, et sur le discriminant d'un polynôme. Enfin, au cours d'une troisième partie, nous développerons quelques applications pratiques des résultants. Les démonstrations proposées en développement figureront en

annexe, et viendront compléter la leçon : il s'agit des démonstrations des théorèmes de la borne de Bézout, de Kronecker, et de Rothstein-Trager, qui seront énoncés au cours de la leçon, et rappelés en annexe.

Dans toute cette leçon, A désigne un anneau unitaire, commutatif, et intègre : on pourra ainsi parler librement de son corps des fractions $\mathrm{Frac}(A)$, de la clôture algébrique $\overline{\mathrm{Frac}(A)}$ de ce corps, et donc, étant donné un polynôme de $A[X]$, de ses racines dans $\overline{\mathrm{Frac}(A)}$. On désignera également par P et Q deux polynômes de $A[X]$, avec les notations de la définition 1.1 à venir.

1 Théorie de l'élimination

1.1 Résultant de deux polynômes

Définition 1.1. Soient $P, Q \in A[X]$, de degrés respectifs n et m, avec $n+m>0$:

$$P = \sum_{i=0}^{n} a_i X^i, \quad Q = \sum_{i=0}^{m} b_i X^i.$$

La *matrice de Sylvester* de P et Q, notée $\mathrm{Syl}(P,Q)$, est la matrice carrée de taille $n+m$, à coefficients dans A, définie par :

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n & a_{n-1} & a_{n-2} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & b_m & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_m & b_{m-1} & b_{m-2} & \dots & b_0 \end{pmatrix} \in \mathcal{M}_{n+m}(A).$$

Le *résultant* de P et Q, noté $\mathrm{Res}(P,Q)$, est le déterminant de la matrice de Sylvester de P et Q :

$$\mathrm{Res}(P,Q) = \det(\mathrm{Syl}(P,Q)) \in A.$$

Remarques 1.2.

- Pour $N \geq 0$, notons $A_N[X]$ le sous-A-module de $A[X]$ constitué de l'ensemble des polynômes de $A[X]$ de degré au plus N, muni de sa base canonique $(X^N, X^{N-1}, \dots, X, 1)$. Le résultant de P et Q est alors le déterminant de l'application linéaire

$$\Phi_{P,Q} : \left\{ \begin{array}{ccc} A_{m-1}[X] \times A_{n-1}[X] & \longrightarrow & A_{n+m-1}[X] \\ (U,V) & \longmapsto & UP+VQ \end{array} \right.$$

  Plus précisément, la matrice de $\Phi_{P,Q}$, relativement aux bases $((X^{m-i},0)_{1\leq i\leq m}$, $(0,X^{n-j})_{1\leq j\leq n})$ de $A_{m-1}[X]\times A_{n-1}[X]$ et $(X^{m+n-i})_{1\leq i\leq m+n}$ de $A_{n+m-1}[X]$, n'est autre que la transposée de la matrice de Sylvester de P et de Q.
- En identifiant un polynôme $F = \sum_{i=0}^{n+m-1} f_i X^i \in A_{n+m-1}[X]$ avec le vecteur ligne $(f_{n+m-1}, f_{n+m-2}, \dots, f_1, f_0) \in A^{n+m}$ de ses coefficients, alors les m premières lignes de $\mathrm{Syl}(P,Q)$ sont respectivement les vecteurs lignes associés à $X^{m-1}P, X^{m-2}P, \dots, XP, P$, tandis que les n dernières lignes sont respectivement les vecteurs lignes associés à $X^{n-1}Q, X^{n-2}Q, \dots, XQ, Q$.
- Si $P, Q \in A[X_1, \dots, X_d]$, on notera $\mathrm{Res}_{X_i}(P,Q)$ le résultant de P et Q, vus comme polynômes en la variable X_i. Il s'agit d'un élément de $A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_d]$: la variable X_i est ainsi "éliminée"! L'objectif des prochains paragraphes sera de préciser le sens que nous donnons à cette élimination.

Exemple 1.3. Soient $P = X+3$ et $Q = 2X^2 - X + 1$ deux polynômes de $\mathbb{Z}[X]$.

$$\mathrm{Res}(P,Q) = \begin{vmatrix} 1 & 3 & 0 \\ 0 & 1 & 3 \\ 2 & -1 & 1 \end{vmatrix} = 22.$$

Insistons une dernière fois sur le fait que dans toute la suite, P et Q désignent deux polynômes de $A[X]$ tels qu'introduits dans la définition 1.1. Nous donnons à présent quelques résultats élémentaires concernant le calcul de résultants :

Proposition 1.4. *On suppose que* $\deg(Q) > 0$. *Soit* $\alpha \in A$.

a) $\operatorname{Res}(\alpha, Q) = \alpha^m$.

b) $\operatorname{Res}(Q, Q) = 0$.

c) $\operatorname{Res}(\alpha P, Q) = \alpha^m \operatorname{Res}(P, Q)$.

d) $\operatorname{Res}(P, Q) = (-1)^{mn} \operatorname{Res}(Q, P)$.

e) *Pour tout* $k \geq 0$, $\operatorname{Res}(X^k P, Q) = b_0^k \operatorname{Res}(P, Q)$.

Les différentes assertions se vérifient aisément en utilisant les propriétés élémentaires du déterminant.

1.2 Résultant et pgcd de deux polynômes

Nous allons expliciter le lien entre le résultant et le pgcd de deux polynômes. Commençons par énoncer le théorème au coeur de la théorie de l'élimination :

Théorème 1.5. *Il existe un couple* $(U, V) \in A_{m-1}[X] \times A_{n-1}[X]$ *tel que* $UP + VQ = \operatorname{Res}(P, Q)$.

Remarque 1.6. Concrètement, le théorème précédent signifie que le résultant de P et Q appartient à l'idéal de $A[X]$ engendré par P et Q. En particulier, si P et Q sont deux polynômes de $A[X_1, \ldots, X_d]$, alors $\operatorname{Res}_{X_i}(P, Q)$ appartient à l'idéal $(P, Q) \cap A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_d]$, qu'on appelle *idéal d'élimination*. C'est en ce sens qu'on peut parler d'élimination de la variable X_i.

Démonstration. Nous allons effectuer des transvections dans la dernière colonne de la matrice de Sylvester de P et Q, ce qui laisse invariant le déterminant, puis développer le déterminant par rapport à la dernière colonne, afin d'obtenir le résultat attendu. Notons $C_1, \ldots, C_{n+m}$ les colonnes de $\operatorname{Syl}(P, Q)$. Pour tout $j \in \{1, \ldots, n+m-1\}$, effectuons la transvection

$$C_{n+m} \leftarrow C_{n+m} + X^{n+m-j} C_j.$$

La dernière colonne de $\operatorname{Syl}(P, Q)$ devient alors

$$\begin{pmatrix} X^{m-1}P \\ X^{m-2}P \\ \vdots \\ P \\ X^{n-1}Q \\ X^{n-2}Q \\ \vdots \\ Q \end{pmatrix}.$$

En développant le déterminant par rapport à la dernière colonne, on obtient donc

$$\operatorname{Res}(P, Q) = \underbrace{(u_{m-1}X^{m-1} + u_{m-2}X^{m-2} + \ldots + u_0)}_{U} P + \underbrace{(v_{n-1}X^{n-1} + v_{n-2}X^{n-2} + \ldots + v_0)}_{V} Q,$$

avec $u_i, v_j \in A$, ce qui conclut la démonstration. ∎

Le théorème suivant donne une condition nécessaire et suffisante pour que le résultant de deux polynômes soit nul :

Théorème 1.7. *On suppose que A est factoriel. Alors* $\mathrm{Res}(P,Q)=0$ *si et seulement si P et Q ont un facteur commun non constant dans $A[X]$.*

Démonstration.

($\Rightarrow$) Supposons que $\mathrm{Res}(P,Q)=0$. L'application linéaire $\Phi_{P,Q}$, introduite aux remarques 1.2, est alors non injective (son déterminant est nul). Il existe donc un couple $(U,V)\in A_{m-1}[X]\times A_{n-1}[X]$ *non nul* tel que $\Phi_{P,Q}(U,V)=UP+VQ=0$ (le précédent théorème ne s'applique pas directement, puisqu'il ne garantit pas que les deux polynômes U et V sont non tous deux nuls dans ce cas de figure). Ainsi, $UP=-VQ$. Comme A est factoriel, alors $A[X]$ l'est également ; si aucun des facteurs irréductibles non constants de P ne divise Q, alors ils divisent tous V, ce qui implique que $\deg(V)\geq\deg(P)$ (car V est non nul), et contredit le fait que $V\in A_{n-1}[X]$. On en déduit que P et Q ont un facteur commun non constant dans $A[X]$.

($\Leftarrow$) Réciproquement, supposons que P et Q ont un facteur commun non constant dans $A[X]$. Soit D le pgcd de P et Q dans $A[X]$, qui est alors non constant. P et Q se factorisent respectivement en $P=D\widetilde{P}$ et $Q=D\widetilde{Q}$. En vertu du précédent théorème, il existe $(U,V)\in A_{m-1}[X]\times A_{n-1}[X]$ tel que $UP+VQ=\mathrm{Res}(P,Q)=D(U\widetilde{P}+V\widetilde{Q})$. Il s'ensuit que $\deg(\mathrm{Res}(P,Q))=\deg(D)+\deg(U\widetilde{P}+V\widetilde{Q})$; or, si $U\widetilde{P}+V\widetilde{Q}\neq 0$, alors $\deg(\mathrm{Res}(P,Q))\geq\deg(D)\geq 1$, ce qui est exclu puisque $\mathrm{Res}(P,Q)\in A$. Par conséquent, $U\widetilde{P}+V\widetilde{Q}=0$, et $\mathrm{Res}(P,Q)=0$. ■

Le corollaire essentiel qui servira de fil directeur à la méthode d'élimination décrite ci-après est le suivant :

Corollaire 1.8. $\mathrm{Res}(P,Q)=0$ *si et seulement si P et Q ont une racine commune dans* $\overline{\mathrm{Frac}(A)}$.

Démonstration.

($\Rightarrow$) Si $\mathrm{Res}(P,Q)=0$, alors P et Q ont un facteur commun non constant D dans $\mathrm{Frac}(A)[X]$. D possède une racine dans $\overline{\mathrm{Frac}(A)}$, qui est alors racine commune à P et Q.

($\Leftarrow$) Si P et Q ont une racine commune $\alpha\in\overline{\mathrm{Frac}(A)}$, alors $X-\alpha$ est un facteur commun non constant à P et Q dans $\overline{\mathrm{Frac}(A)}[X]$. Le résultant de P et Q, vus comme polynômes de $\overline{\mathrm{Frac}(A)}[X]$, est alors nul ; toutefois, $\mathrm{Res}(P,Q)$ se calcule de la même manière dans $A[X]$ et dans $\overline{\mathrm{Frac}(A)}[X]$, donc $\mathrm{Res}(P,Q)=0$. ■

Dans toute la suite, les anneaux seront toujours supposés factoriels.

1.3 Méthode d'élimination

Afin d'illustrer le principe de la méthode d'élimination, considérons dans un premier temps deux polynômes P et Q de $\mathbb{C}[X,Y]$, premiers entre eux dans $\mathbb{C}[X,Y]$, dont on cherche les racines communes, c'est-à-dire, d'un point de vue géométrique, les points d'intersection des courbes $\gamma_P=\{(x,y)\in\mathbb{C}^2\,|\,P(x,y)=0\}$ et $\gamma_Q=\{(x,y)\in\mathbb{C}^2\,|\,Q(x,y)=0\}$. Soit $(\alpha,\beta)\in\gamma_P\cap\gamma_Q$. Les polynômes $P(\alpha,Y)$ et $Q(\alpha,Y)$ de $\mathbb{C}[Y]$ admettent β comme racine commune, ce qui se traduit par $\mathrm{Res}(P(\alpha,Y),Q(\alpha,Y))=0$, en vertu du corollaire 1.8. Considérons à présent le polynôme $R(X)=\mathrm{Res}_Y(P(X,Y),Q(X,Y))\in\mathbb{C}[X]$. Nous venons exactement d'observer que α est racine de $R(X)$.

À la lumière de cette analyse, nous pouvons désormais mettre en oeuvre la méthode d'élimination, afin de rechercher les points d'intersection des courbes γ_P et γ_Q. La méthode se décompose essentiellement en trois étapes :

1. Calculer $R(X)=\mathrm{Res}_Y(P(X,Y),Q(X,Y))\in\mathbb{C}[X]$. Nous détaillerons dans la prochaine partie les méthodes effectives de calcul de résultants. Le fait que P et Q soient premiers entre eux dans $\mathbb{C}[X,Y]$ permet d'écarter le cas où $R(X)=0$.

2. Déterminer les racines de $R(X)$ dans $\mathbb{C}$.
3. Pour chaque racine $\alpha \in \mathbb{C}$ de $R(X)$, déterminer les racines de $P(\alpha, Y)$ et $Q(\alpha, Y)$ dans $\mathbb{C}$. Chaque racine commune $\beta \in \mathbb{C}$ à ces deux polynômes fournit alors un point d'intersection (α, β) des courbes γ_P et γ_Q.

Cette méthode garantit de trouver tous les points d'intersection de γ_P et γ_Q. La principale difficulté repose bien évidemment sur la recherche des racines complexes des polynômes qui entrent en jeu. L'étape 3 peut être légèrement améliorée en calculant plutôt le pgcd de $P(\alpha, Y)$ et $Q(\alpha, Y)$ dans $\mathbb{C}[Y]$ par l'algorithme d'Euclide, puis en déterminant les racines de ce pgcd.

Les étapes décrites ci-dessus se transposent immédiatement dans le cas de deux polynômes à coefficients dans un quelconque anneau A unitaire, commutatif, intègre, et factoriel, auquel cas les points d'intersection obtenus sont uniquement les points d'intersection dans A, mais il est bien entendu possible d'appliquer la méthode dans $\overline{\mathrm{Frac}(A)}$. Par exemple, dans le cas particulier où $A = \mathbb{Z}$, on sait déterminer aisément les racines entières d'un polynôme à coefficients entiers : il suffit de tester les diviseurs de son coefficient constant, ce qui peut se révéler intéressant pour déterminer les racines communes entières de deux polynômes à coefficients entiers.

Exemple 1.9. Soient $P, Q \in \mathbb{Q}[X]$, définis par

$$\begin{cases} P = X^2 + 2X - XY + 2Y - 6, \\ Q = 3X^2 - 5X + 5 + XY - 2Y. \end{cases}$$

Le calcul du résultant de P et Q par rapport à l'indéterminée X donne $R(Y) = \mathrm{Res}_X(P, Q) = (36Y - 103)(Y - 3)$. Les racines de $R(Y)$ sont donc 3 et $\frac{103}{36}$.

- Pour $\beta = 3$, $P(X, 3) = X^2 - X = X(X - 1)$, et $Q(X, 3) = 3X^2 - 2X - 1$, dont la seule racine commune est $\alpha = 1$.
- De même, pour $\beta = \frac{103}{36}$, la seule racine commune obtenue est $\alpha = -\frac{1}{4}$.

Par conséquent, les courbes γ_P et γ_Q possèdent deux points d'intersection : $(1, 3)$ et $\left(-\frac{1}{4}, \frac{103}{36}\right)$.

Remarque 1.10. Il est également possible de procéder de la manière suivante :

1. Calculer d'une part $R(X) = \mathrm{Res}_Y(P, Q)$, d'autre part $S(Y) = \mathrm{Res}_X(P, Q)$.
2. Déterminer les racines de $R(X)$ et $S(Y)$.
3. Pour chaque racine α de $R(X)$ et chaque racine β de $S(Y)$, tester si $P(\alpha, \beta) = Q(\alpha, \beta) = 0$.

Il est aisé de s'assurer comme précédemment que cette méthode fournit toutes les racines communes de P et Q.

1.4 Théorème de la borne de Bézout

Nous nous intéressons désormais au nombre de racines communes que possèdent deux polynômes P et Q de $A[X, Y]$. Dans le cas général, il n'est pas possible d'estimer de manière exacte le nombre de racines communes. Toutefois, il est possible d'en donner une borne : c'est l'objet du théorème de la borne de Bézout. On rappelle que le degré total d'un monôme de la forme $X^a Y^b \in A[X, Y]$ est $a + b$, et que le degré total d'un polynôme $P \in A[X, Y]$ est le maximum des degrés totaux de ses monômes.

Théorème 1.11 (Borne de Bézout)**.** *Soient k un corps infini, et $P, Q \in k[X, Y]$ deux polynômes de degrés totaux respectifs d et d'. On suppose que P et Q sont premiers entre eux. Alors les courbes $\gamma_P = \{(x, y) \in k^2 \mid P(x, y) = 0\}$ et $\gamma_Q = \{(x, y) \in k^2 \mid Q(x, y) = 0\}$ ont au plus dd' points d'intersection.*

Remarque 1.12. Il n'est pas nécessaire de supposer que k est infini, ni même que k est un corps. Le théorème reste vrai dans un anneau A quelconque, puisqu'il suffit alors d'appliquer l'énoncé précédent dans $\overline{\mathrm{Frac}(A)}$, qui est bien un corps infini.

La démonstration du théorème de la borne de Bézout fait l'objet de l'annexe A.

Donnons une application immédiate de ce théorème :

Application 1.13. Deux coniques distinctes du plan ont au plus 4 points d'intersection. En effet, une conique du plan peut être interprétée comme l'ensemble des points d'annulation d'un polynôme $P \in \mathbb{R}[X,Y]$ de degré total 2, et le théorème fournit directement la borne. En conséquence, par 5 points distincts du plan ne peut passer au plus qu'une seule conique.

Remarque 1.14. La borne du théorème de la borne de Bézout est optimale. Par exemple, avec les deux polynômes $P, Q \in \mathbb{R}[X,Y]$ de l'introduction, de degrés totaux respectifs 3 et 2, les courbes s'intersectent bien en exactement $6 = 3 \times 2$ points.

1.5 Théorème d'extension

Pour simplifier, considérons un corps k algébriquement clos (il est toujours possible de se ramener à ce cas en considérant $\overline{\mathrm{Frac}(A)}$), et $P, Q \in k[X,Y]$. Rappelons que si $(\alpha, \beta) \in k^2$ est une racine commune de P et Q, alors α est racine de $R(X) = \mathrm{Res}_Y(P,Q) \in k[X]$. Si $\alpha \in k$ est une racine de $R(X)$, il est alors naturel de se demander s'il est possible de "remonter" α en une racine commune de P et Q, c'est-à-dire, en termes plus mathématiques, s'il existe $\beta \in k$ tel que (α, β) soit une racine commune de P et Q. Le théorème d'extension donne une condition suffisante d'existence d'un tel β.

Avant d'y parvenir, nous allons commencer par démontrer le théorème suivant :

Théorème 1.15. *Soit $\phi : A \longrightarrow B$ un morphisme d'anneaux intègres, étendu à $\phi : A[X] \longrightarrow B[X]$ ($\phi(X) = X$). On suppose que $\deg \phi(P) = \deg P$, et que $\deg \phi(Q) = \deg Q - s$, avec $s \geq 0$. Alors*

$$\phi(\mathrm{Res}(P,Q)) = \phi(a_n)^s \,\mathrm{Res}(\phi(P), \phi(Q)).$$

Démonstration. Puisque le déterminant d'une matrice M est une application polynomiale en les coefficients de M, on a

$$\phi(\mathrm{Res}(P,Q)) = \begin{vmatrix} \phi(a_n) & \phi(a_{n-1}) & \dots & \phi(a_1) & \phi(a_0) & 0 & \dots & 0 \\ 0 & \phi(a_n) & \dots & \phi(a_2) & \phi(a_1) & \phi(a_0) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \phi(a_n) & \phi(a_{n-1}) & \phi(a_{n-2}) & \dots & \phi(a_0) \\ \phi(b_m) & \phi(b_{m-1}) & \dots & \phi(b_1) & \phi(b_0) & 0 & \dots & 0 \\ 0 & \phi(b_m) & \dots & \phi(b_2) & \phi(b_1) & \phi(b_0) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \phi(b_m) & \phi(b_{m-1}) & \phi(b_{m-2}) & \dots & \phi(b_0) \end{vmatrix}$$

Or, par hypothèse, $\phi(a_n) \neq 0$, $\phi(b_m) = \phi(b_{m-1}) = \cdots = \phi(b_{m-s+1}) = 0$, et $\phi(b_{m-s}) \neq 0$. Le résultat s'en déduit immédiatement, en développant le déterminant. ∎

Muni de cette relation, nous pouvons désormais démontrer le théorème d'extension :

Théorème 1.16 (d'extension)**.** *Soient $P, Q \in k[X_1, \dots, X_d]$, que l'on écrit*

$$P = \sum_{i=0}^{n} a_i X_d^i, \quad Q = \sum_{i=0}^{m} b_i X_d^i,$$

avec $a_i, b_j \in k[X_1, \dots, X_{d-1}]$.

a) *Si $(\alpha_1, \dots, \alpha_d) \in k^d$ est une racine commune de P et Q, alors $(\alpha_1, \dots, \alpha_{d-1})$ est racine de $\mathrm{Res}_{X_d}(P,Q)$.*

b) *Réciproquement, si* $\mathrm{Res}_{X_d}(P,Q)(\alpha_1,\dots,\alpha_{d-1})=0$*, et si* $(\alpha_1,\dots,\alpha_{d-1})$ *n'est pas racine commune de* a_n *et* b_m*, alors il existe* $\alpha_d\in k$ *tel que* $(\alpha_1,\dots,\alpha_d)$ *soit une racine commune de* P *et* Q*.*

Démonstration. Le a) résulte de l'analyse menée au début du paragraphe 1.3. Pour le b), on applique le théorème précédent, avec le morphisme $\phi : k[X_1,\dots,X_{d-1}]\longrightarrow k$ défini par $\phi(t)=t$, pour tout $t\in k$, et $\phi(X_i)=\alpha_i$, pour tout $i\in\{1,\dots,d-1\}$, étendu à $\phi : k[X_1,\dots,X_d]\longrightarrow k[X_d]$ ($\phi(X_d)=X_d$). Par hypothèse, $(\alpha_1,\dots,\alpha_{d-1})$ n'est pas racine commune de a_n et b_m ; sans perte de généralité, supposons que $(\alpha_1,\dots,\alpha_{d-1})$ n'est pas racine de a_n, de sorte que $\deg\phi(P)=\deg P$ ($\phi(a_n)=a_n(\alpha_1,\dots,\alpha_{d-1})\neq 0$), et $\deg\phi(Q)=\deg Q-s$, avec $s\geq 0$. D'où finalement :

$$\phi(\mathrm{Res}_{X_d}(P,Q))=\phi(a_n)^s\,\mathrm{Res}(\phi(P),\phi(Q)).$$

Or $\phi(\mathrm{Res}_{X_d}(P,Q))=\mathrm{Res}_{X_d}(P,Q)(\alpha_1,\dots,\alpha_{d-1})=0$, donc $\mathrm{Res}(\phi(P),\phi(Q))=0$, ce qui signifie que $\phi(P)=P(\alpha_1,\dots,\alpha_{d-1},X_d)$ et $\phi(Q)=Q(\alpha_1,\dots,\alpha_{d-1},X_d)$ possèdent une racine commune $\alpha_d\in k$: c'est exactement le résultat recherché. ■

Exemple 1.17. Reprenons l'exemple 1.9 avec les polynômes $P,Q\in\mathbb{Q}[X]$ définis par

$$\begin{cases} P=X^2+2X-XY+2Y-6,\\ Q=3X^2-5X+5+XY-2Y. \end{cases}$$

Nous avons établi que les racines de $R(Y)=\mathrm{Res}_X(P,Q)$ sont 3 et $\frac{103}{36}$. Le terme de tête en X de P est 1, et celui de Q est 3, qui n'ont bien entendu aucune racine commune. Ainsi, le théorème d'extension garantit l'existence de $\alpha_1,\alpha_2\in\overline{\mathbb{Q}}$ tels que $(\alpha_1,3)$ et $\left(\alpha_2,\frac{103}{36}\right)$ soient racines communes de P et Q. En l'occurrence, $\alpha_1=1$ et $\alpha_2=-\frac{1}{4}$.

2 Calcul effectif de résultants et conséquences

Dans cette partie, nous portons un intérêt particulier à la méthode de calcul de résultants liée à l'algorithme d'Euclide, que nous allons dans un premier développer, puis exploiter afin d'expliciter davantage le lien entre le résultant de deux polynômes et leurs racines.

En préliminaire, rappelons que le résultant n'est autre qu'un déterminant, et qu'en conséquence, les méthodes de calcul de déterminants peuvent être mises à profit. Ainsi, par exemple, si $P,Q\in A[X]$ sont deux polynômes de degrés respectifs n et m, l'algorithme du pivot de Gauss permet de calculer $\mathrm{Res}(P,Q)$ avec une complexité en $\mathcal{O}((n+m)^3)$ opérations sur A. Néanmoins, l'algorithme d'Euclide est en pratique beaucoup plus efficace, et doit donc être privilégié pour les calculs.

2.1 Algorithme d'Euclide

La méthode repose sur la proposition suivante :

Proposition 2.1. *Soient* $P,Q\in A[X]$*. On suppose que le coefficient dominant de* Q *est inversible. Soit* $R\in A[X]$ *le reste de la division euclidienne de* P *par* Q*. Si* $R=0$*, alors* $\mathrm{Res}(P,Q)=0$ *; sinon, en notant* $r=\deg R$*, on a*

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

L'égalité s'obtient en procédant à des opérations élémentaires sur la matrice de Sylvester de P et Q. L'algorithme qui découle de cette proposition est donc identique à l'algorithme d'Euclide, au coefficient multiplicatif près qui apparaît lors de chaque division. L'algorithme s'interrompt dès lors que $\deg(R)=0$ ou $R=0$, la proposition 1.4 permettant alors d'expliciter immédiatement le résultant de Q et R.

Toutefois, cet algorithme est confronté à la difficulté suivante (que l'on rencontre également pour le calcul du pgcd de deux polynômes) : l'anneau $A[X]$ n'est en général pas euclidien, et il est donc nécessaire que le coefficient dominant de Q soit inversible afin de procéder à la division euclidienne de P par Q dans $A[X]$, ce qui n'est bien entendu pas toujours garanti au cours de l'algorithme. Deux solutions permettent de contourner cet obstacle :

- la première consiste à effectuer les calculs dans $\mathrm{Frac}(A)[X]$, qui est bien un anneau euclidien puisque $\mathrm{Frac}(A)$ est un corps ;
- la seconde s'appuie sur le principe de la *pseudo-division* dans $A[X]$, que l'on ne développe pas ici.

Exemple 2.2. Reprenons de nouveau l'exemple 1.9, avec les polynômes $P, Q \in \mathbb{Q}[X]$ définis par

$$\begin{cases} P = X^2 + 2X - XY + 2Y - 6, \\ Q = 3X^2 - 5X + 5 + XY - 2Y, \end{cases}$$

et appliquons la première solution afin de calculer $\mathrm{Res}_X(P, Q)$:

- le reste de la division euclidienne de P par Q est $R_1 = \left(\frac{11}{3} - \frac{4}{3}Y\right) X - \frac{23}{3} + \frac{8}{3}Y$;
- le reste de la division euclidienne de Q par R_1 est $R_2 = 3\dfrac{309 - 211Y + 36Y^2}{(4Y - 11)^2}$;
- le degré de R_2 en X est égal à 0, donc l'algorithme s'interrompt.

On en déduit que

$$\mathrm{Res}_X(P, Q) = 3\,\mathrm{Res}_X(Q, R_1) = \frac{1}{3}(4Y - 11)^2\,\mathrm{Res}_X(R_1, R_2) = 309 - 211Y + Y^2.$$

2.2 Lien résultant-racines

Le théorème suivant fournit une nouvelle expression du résultant de deux polynômes en fonction de leurs racines :

Théorème 2.3. *Soient k un corps, et $P, Q \in k[X]$. Écrivons*

$$\begin{cases} P = a_n(X - \alpha_1)\dots(X - \alpha_n), \\ Q = b_m(X - \beta_1)\dots(X - \beta_m), \end{cases}$$

avec $\alpha_i, \beta_j \in \overline{k}$. Alors

$$\begin{aligned} \mathrm{Res}(P, Q) &= b_m^n a_n^m \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \\ &= a_n^m \prod_{i=1}^{n} Q(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} P(\beta_j). \end{aligned}$$

Démonstration. Définissons l'application

$$\theta : \begin{cases} k[X] \times k[X] & \longrightarrow & \overline{k} \\ (P, Q) & \longmapsto & a_n^m \displaystyle\prod_{i=1}^{n} Q(\alpha_i) \end{cases}$$

avec les notations du théorème. On vérifie que

- $\theta(P, Q) = (-1)^{nm}\theta(Q, P)$;
- $\theta(\alpha, Q) = \alpha^m$ si $\alpha \in k$;
- si R est le reste de la division euclidienne de P par Q dans $k[X]$, et si $R \neq 0$, alors, en notant $r = \deg(R)$, on a $\theta(P, Q) = (-1)^{nm} b_m^{n-r}\theta(Q, R)$; si $R = 0$, alors $\theta(P, Q) = 0$.

Ainsi, $\theta(P,Q)$ et $\mathrm{Res}(P,Q)$ se calculent de la même manière via l'algorithme d'Euclide, de sorte que $\theta(P,Q) = \mathrm{Res}(P,Q)$. Les autres égalités se vérifient par un calcul direct. ■

Cette nouvelle expression du résultant a plusieurs conséquences, parmi lesquelles le théorème de Kronecker, qui constitue le développement abordé dans l'annexe B :

Théorème 2.4 (Kronecker)**.** *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, de degré $n \geq 1$. On suppose que les racines de P dans $\mathbb{C}$ sont de module inférieur ou égal à 1, et que 0 n'est pas racine. Alors les racines de P sont des racines de l'unité.*

Enfin, cette expression du résultant permet de relier le discriminant d'un polynôme P avec le résultant de P et P', comme nous allons l'étudier au cours du paragraphe suivant.

2.3 Discriminant d'un polynôme

Rappelons tout d'abord ce qu'est le discriminant d'un polynôme :

Définition 2.5. Soient k un corps, $P \in k[X]$, et soient $\alpha_1, \ldots, \alpha_n \in \overline{k}$ ses racines. Le *discriminant* de P, noté $\Delta(P)$, est défini par

$$\Delta(P) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Remarques 2.6.

- À partir de la définition, il est immédiat que $\Delta(P) = 0$ si et seulement si P possède une racine double.
- A priori, $\Delta(P)$ est un élément de $\overline{k}$. Il s'agit en fait d'un élément de k ; la prochaine proposition va permettre de le vérifier directement.

Proposition 2.7. *On a*

$$\Delta(P) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} \mathrm{Res}(P, P').$$

Remarque 2.8. Comme annoncé, $\Delta(P) \in k$, puisque $\mathrm{Res}(P, P') \in k$.

Démonstration. En dérivant $P = a_n \prod_{i=1}^{n} (X - \alpha_i)$, on obtient

$$P' = a_n \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_j),$$

d'où, par le théorème 2.3,

$$\mathrm{Res}(P, P') = a_n^{n-1} \prod_{i=1}^{n} P'(\alpha_i).$$

Il suffit alors de remarquer que $P'(\alpha_i) = a_n \prod_{j \neq i} (\alpha_i - \alpha_j)$ afin de conclure. ■

Mentionnons une application de ce dernier résultat afin de conclure cette partie :

Application 2.9. L'ensemble Ω_p des matrices de $\mathcal{M}_p(\mathbb{C})$ à p valeurs propres distinctes forme un ouvert de $\mathcal{M}_p(\mathbb{C})$ (pour la topologie usuelle d'espace vectoriel normé sur $\mathcal{M}_p(\mathbb{C})$). En effet, une matrice $M \in \mathcal{M}_p(\mathbb{C})$ possède p valeurs propres distinctes si et seulement si $\Delta(\chi_M) \neq 0$, où χ_M désigne le polynôme caractéristique de M, donc si et seulement si $\mathrm{Res}(\chi_M, \chi_M') \neq 0$. Comme l'application $\mu : M \in \mathcal{M}_p(\mathbb{C}) \longmapsto \mathrm{Res}(\chi_M, \chi_M')$ est continue, car polynomiale en les coefficients de M, alors $\Omega_p = \mu^{-1}(\mathbb{C}^*)$ est ouvert dans $\mathcal{M}_p(\mathbb{C})$.

3 Quelques applications des résultants

Au cours de cette dernière partie, nous nous intéressons à divers problèmes de nature tantôt purement algébrique, tantôt géométrique, observés du point de vue des résultants et de l'élimination.

3.1 Calcul de polynômes annulateurs

Soient k un corps, et $\alpha, \beta \in \overline{k}$, de polynômes minimaux distincts sur k. On suppose connu un polynôme annulateur $P \in k[X]$ de α sur k, et un polynôme annulateur $Q \in k[X]$ de β sur k. L'objectif est de déterminer un polynôme annulateur de la somme $\alpha+\beta$, ainsi que du produit $\alpha\beta$, sur k. Quitte à diviser P et Q par leur pgcd, on peut supposer que P et Q sont premiers entre eux. La proposition suivante répond à la problématique grâce aux résultants :

Proposition 3.1. a) *Le polynôme* $R(X) = \mathrm{Res}_Y(P(Y), Q(X-Y))$ *est un polynôme annulateur de* $\alpha+\beta$.

b) *Le polynôme* $S(X) = \mathrm{Res}_Y(P(Y), X^m Q\left(\frac{Y}{X}\right))$ *est un polynôme annulateur de* $\alpha\beta$.

Démonstration. Démontrons l'assertion a), l'assertion b) se traitant de manière similaire. On a $R(\alpha+\beta) = \mathrm{Res}_Y(P(Y), Q(\alpha+\beta-Y))$. Or les polynômes $P(Y)$ et $Q(\alpha+\beta-Y)$ admettent α comme racine commune, si bien que $R(\alpha+\beta) = 0$. ■

Remarque 3.2. Ce résultat n'a d'intérêt que si les résultants calculés sont non nuls. Sous l'hypothèse que P et Q sont premiers entre eux, c'est effectivement le cas : par exemple, si on avait $R(X) = 0$, alors $P(Y)$ et $Q(X-Y)$ auraient un facteur commun non constant dans $k[X][Y] = k[X,Y]$, qui serait nécessairement dans $k[Y]$ puisque le degré de $P(Y)$ en X est nul, et serait alors un facteur commun non constant à $P(Y)$ et $Q(Y)$ dans $k[Y]$ (en substituant $2Y$ à X).

Le corollaire immédiat de cette proposition et de la remarque précédente est le suivant :

Corollaire 3.3. *L'ensemble des éléments algébriques sur* k *est un anneau.*

Exemple 3.4. Déterminons un polynôme annulateur de $\sqrt{2}+\sqrt[3]{3}$ sur $\mathbb{Q}$. Le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $P = X^2-2$, tandis que celui de $\sqrt[3]{3}$ sur $\mathbb{Q}$ est $Q = X^3-3$ (tous deux sont bien irréductibles par le critère d'Eisenstein). Un polynôme annulateur de $\sqrt{2}+\sqrt[3]{3}$ sur $\mathbb{Q}$ est alors donné par

$$R(X) = \mathrm{Res}_Y(Y^2-2, (X-Y)^3-3) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1.$$

On peut vérifier qu'il s'agit même du polynôme minimal de $\sqrt{2}+\sqrt[3]{3}$ sur $\mathbb{Q}$, par exemple en calculant explicitement le degré de l'extension $\mathbb{Q}(\sqrt{2}+\sqrt[3]{3})/\mathbb{Q}$.

Remarque 3.5. Dans le cas général, le polynôme annulateur obtenu n'est pas le polynôme minimal, même si les polynômes annulateurs P et Q choisis sont respectivement les polynômes minimaux de α et β sur k. Toutefois, si P et Q sont les polynômes minimaux respectifs de α et β sur k, de degrés respectifs d et d', et si l'extension $k(\alpha+\beta)/k$ est de degré dd', alors le polynôme $R(X)$ est le polynôme minimal de $\alpha+\beta$: en effet, on peut montrer que le degré de $R(X)$ est inférieur à dd' (voir l'annexe A) ; comme le polynôme minimal de $\alpha+\beta$ divise $R(X)$ et est de degré dd', alors il s'agit de $R(X)$ (tous deux sont unitaires). Le raisonnement reste valable pour $S(X)$ si l'on suppose cette fois-ci que l'extension $k(\alpha\beta)/k$ est de degré dd'.

3.2 Formule de Héron

Le problème posé est le suivant : étant donné un triangle ABC (non plat) du plan, on désire exprimer son aire $\mathcal{A}$ en fonction des longueurs $a = BC$, $b = AC$ et $c = AB$ de ses côtés. La formule de Héron répond à cette problématique :

Proposition 3.6 (Formule de Héron). *En notant $p = \frac{1}{2}(a+b+c)$ le demi-périmètre de ABC, on a*

$$\mathcal{A} = \sqrt{p(p-a)(p-b)(p-c)}.$$

Ce problème élémentaire de géométrie peut être traité par une méthode d'élimination. Pour ce faire, nous devons commencer par décrire les contraintes polynomiales associées au problème étudié. Tout d'abord, fixons un repère affine orthonormé du plan, de sorte que le triangle ABC soit dans la configuration suivante :

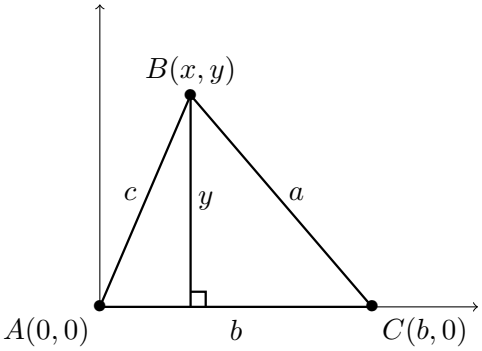

FIGURE 2 – Formule de Héron

On introduit ainsi deux nouvelles variables, x et y, qui désignent les coordonnées de B dans ce repère, et on trace la hauteur issue de B, de longueur y. L'aire s'obtient alors par la formule

$$\mathcal{A} - \frac{1}{2}by = 0. \tag{1}$$

Les deux autres contraintes polynomiales sur x et y correspondent au fait que AB est de longueur c, et que BC est de longueur a, soit respectivement

$$x^2 + y^2 - c^2 = 0 \tag{2}$$

et

$$(b-x)^2 + y^2 - a^2 = 0. \tag{3}$$

Il faut à présent éliminer les variables x et y des équations polynomiales (1), (2) et (3), afin d'en déduire $\mathcal{A}$ en fonction de a, b et c. En éliminant la variable x des équations (2) et (3), on obtient

$$a^4 - 2a^2b^2 - 2a^2c^2 + b^4 - 2b^2c^2 + 4b^2y^2 + c^4 = 0. \tag{4}$$

Puis, en éliminant la variable y des équations (1) et (4), on obtient

$$\frac{1}{4}b^4(16\mathcal{A}^2 - (a+b+c)(a+b-c)(a-b+c)(-a+b+c)) = 0, \tag{5}$$

ce qui fournit deux solutions pour $\mathcal{A}$, la seule positive correspondant bien à la formule de Héron ($b \neq 0$ pour un triangle non plat).

L'exemple de la formule de Héron illustre bien comment l'élimination permet d'aborder un problème simple de géométrie, en introduisant de nouvelles variables et en décrivant les contraintes polynomiales associées.

3.3 Équation implicite et paramétrisation rationnelle d'une courbe

On considère dans le plan $\mathbb{R}^2$ une courbe γ, tantôt définie implicitement par une équation de la forme $P(x, y) = 0$, avec $P \in \mathbb{R}[X, Y]$, tantôt décrite par une paramétrisation rationnelle, c'est-à-dire une équation paramétrique de la forme

$$\begin{cases} x(t) = F(t), \\ y(t) = G(t), \end{cases}$$

avec $F, G \in \mathbb{R}(T)$ deux fractions rationnelles. Au cours de ce paragraphe, nous nous attachons à expliciter comment transformer une équation implicite en une équation paramétrique rationnelle, et vice-versa. Selon la nature du problème posé, l'une ou l'autre de ces descriptions peut se révéler plus maniable que l'autre. Par exemple, le tracé d'une courbe est beaucoup plus aisé et précis lorsqu'on en connaît une paramétrisation rationnelle, ce qui n'est pas le cas avec une équation implicite.

Transformation d'une équation implicite en paramétrisation rationnelle

Toutes les courbes définies implicitement ne sont hélas pas descriptibles par une équation paramétrique rationnelle. Toutefois, dans le cas par exemple des coniques, il est possible de déterminer une paramétrisation rationnelle grâce à l'élimination. La méthode s'appuie sur le constat suivant : étant donné un point fixé A d'une conique γ, tout point de γ différent de A peut-être décrit par deux contraintes polynomiales en tant qu'unique point d'intersection différent de A d'une certaine droite passant par A avec γ.

En guise d'illustration, donnons une paramétrisation rationnelle du cercle unité $\mathcal{C}$. Fixons donc un point de $\mathcal{C}$, par exemple le point $A(-1, 0)$. Comme annoncé, on remarque que toute droite du plan passant par A, excepté la droite verticale d'équation $x = -1$, intersecte $\mathcal{C}$ en un unique point M autre que A, et que tout point de $\mathcal{C}$ autre que A peut être obtenu ainsi, de manière unique.

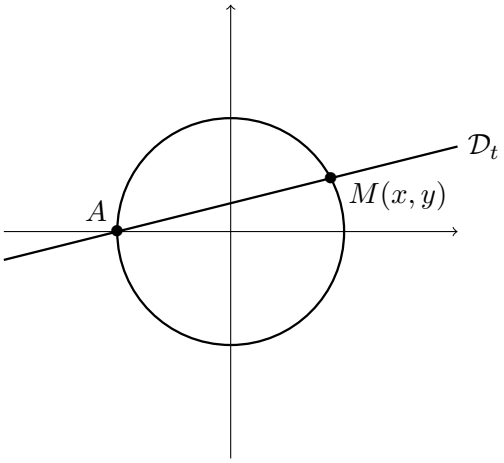

FIGURE 3 – Paramétrisation rationnelle du cercle unité

Sur la figure ci-dessus, on a noté $\mathcal{D}_t$ la droite passant par A de coefficient directeur $t \in \mathbb{R}$, ainsi que (x, y) les coordonnées du point d'intersection M autre que A de $\mathcal{D}_t$ avec $\mathcal{C}$. Les deux contraintes polynomiales proviennent de l'appartenance de M à $\mathcal{C}$ d'une part, et à la droite $\mathcal{D}_t$ d'autre part, soit respectivement

$$x^2 + y^2 - 1 = 0 \tag{6}$$

et

$$y - t(x + 1) = 0. \tag{7}$$

On procède alors en éliminant d'une part la variable x des équations (6) et (7), et d'autre part en éliminant la variable y, ce qui donne respectivement

$$y^2(1+t^2) - 2yt = 0 \tag{8}$$

et

$$x^2(t^2+1) + 2t^2x + t^2 - 1 = 0. \tag{9}$$

Il ne reste plus qu'à exprimer x et y en fonction de t. L'équation (8) fournit deux solutions $y_1 = 0$ et $y_2 = \dfrac{2t}{1+t^2}$, tandis que l'équation (9) fournit deux solutions $x_1 = -1$ et $x_2 = \dfrac{1-t^2}{1+t^2}$. Finalement, une paramétrisation rationnelle du cercle unité est donnée par

$$\begin{cases} x(t) = \dfrac{1-t^2}{1+t^2}, \\ y(t) = \dfrac{2t}{1+t^2}. \end{cases}$$

avec $t \in \mathbb{R}$. Cette paramétrisation décrit tous les points du cercle unité, à l'exception du point A, qui est cependant obtenu "à la limite", en faisant tendre t vers l'infini.

Cette paramétrisation rationnelle du cercle unité est très intéressante, puisqu'elle permet par exemple de déterminer les triplets pythagoriciens, c'est-à-dire les triplets $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$.

Transformation d'une paramétrisation rationnelle en équation implicite

La transformation d'une paramétrisation rationnelle en équation implicite est, quant à elle, toujours possible. En effet, considérons une courbe γ décrite par une équation paramétrique rationnelle de la forme

$$\begin{cases} x(t) = \dfrac{P_1(t)}{Q_1(t)}, \\ y(t) = \dfrac{P_2(t)}{Q_2(t)}, \end{cases}$$

avec $P_1, P_2, Q_1, Q_2 \in \mathbb{R}[X]$, et supposons pour simplifier que Q_1 et Q_2 ne s'annulent pas sur $\mathbb{R}$. Le système précédent est alors équivalent à

$$\begin{cases} Q_1(t)x(t) - P_1(t) = 0, \\ Q_2(t)y(t) - P_2(t) = 0. \end{cases}$$

En d'autres termes, pour tout $t \in \mathbb{R}$, le triplet $(x(t), y(t), t)$ est racine commune aux polynômes $Q_1(T)X - P_1(T)$ et $Q_2(T)Y - P_2(T)$ de $\mathbb{R}[X, Y, T]$. Il s'ensuit que $(x(t), y(t))$ est racine du polynôme $R(X, Y) = \mathrm{Res}_T(Q_1(T)X - P_1(T), Q_2(T)Y - P_2(T))$, ce qui fournit une équation implicite de γ. Néanmoins, il se peut que l'équation implicite obtenue ne décrive pas γ, mais une courbe γ' qui contienne γ, dans la mesure où il n'est pas toujours possible d'étendre une racine de $R(X, Y)$ en une racine commune à $Q_1(T)X - P_1(T)$ et $Q_2(T)Y - P_2(T)$.

Exemple 3.7. Effectuons la transformation inverse à partir de la paramétrisation rationnelle du cercle unité privé du point $A(-1, 0)$ obtenue précédemment. Le calcul de $R(X, Y)$ donne

$$R(X, Y) = \mathrm{Res}_T((1+T^2)X - (1-T^2), (1+T^2)Y - 2T) = 4X^2 + 4Y^2 - 4,$$

et l'on retrouve ainsi l'équation implicite $x^2 + y^2 - 1 = 0$ du cercle unité. La courbe obtenue par ce procédé contient un point de plus que la courbe initiale, à savoir le point A.

Exemple 3.8. Soit γ la courbe paramétrée par

$$\begin{cases} x(t) = t^2 + t + 1, \\ y(t) = \dfrac{t^2 - 1}{t^2 + 1}. \end{cases}$$

Dans cet exemple, le calcule de $R(X, Y)$ donne

$$\begin{aligned} R(X, Y) &= \mathrm{Res}_T(X - (T^2 + T + 1), (T^2 + 1)Y - (T^2 - 1) \\ &= X^2Y^2 - 2X^2Y + X^2 + 4XY - 4X + Y^2 + 3. \end{aligned}$$

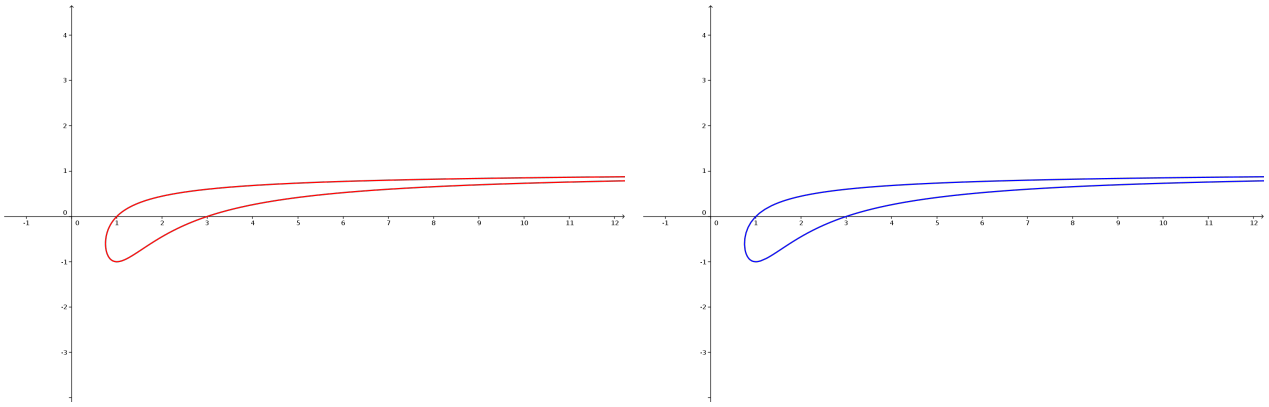

FIGURE 4 – Comparaison du tracé avec l'équation paramétrique (en bleu) et l'équation implicite (en rouge)

Les deux tracés sont rigoureusement identiques, comme le suggère la figure ci-dessus. Vérifions-le : le terme de tête en T du polynôme $X - (T^2 + T + 1)$ est -1, qui ne s'annule jamais ; en conséquence, grâce au théorème d'extension, toute racine (x, y) de $R(X, Y)$ peut être étendue en une racine commune (x, y, t) à $X - (T^2 + T + 1)$ et $(T^2 + 1)Y - (T^2 - 1)$, si bien que les équations paramétriques et implicites décrivent la même courbe.

3.4 Intégration de fractions rationnelles

Soit $\frac{P}{Q} \in \mathbb{Q}(X)$ une fraction rationnelle, que l'on suppose *propre*, c'est-à-dire telle que P et Q soient premiers entre eux, Q ne soit pas réduit à 1 et soit unitaire, et $\deg P < \deg Q$. Il est toujours possible de se ramener à cette situation, quitte à effectuer la division euclidienne de P par Q afin d'extraire la partie entière de $\frac{P}{Q}$. On souhaite expliciter une *primitive formelle* de $\frac{P}{Q}$: concrètement, il s'agit de trouver, dans une extension de $\mathbb{Q}(X)$ dans laquelle se prolonge la dérivation usuelle dans $\mathbb{Q}(X)$, un élément F tel que $F' = \frac{P}{Q}$. On ne s'attarde pas trop sur la construction d'une telle extension ; on sait néanmoins que, par le théorème de décomposition en éléments simples, si $\alpha_1, \ldots, \alpha_d$ sont les racines de Q dans le corps de décomposition K de Q sur $\mathbb{Q}$ (ou plus simplement si $K = \mathbb{C}$), alors $\frac{P}{Q}$ se décompose sous la forme

$$\frac{P}{Q} = \sum_{i=1}^{d} \sum_{j=2}^{r_i} \frac{m_{i,j}}{(X - \alpha_i)^j} + \sum_{i=1}^{d} \frac{c_i}{X - \alpha_i},$$

avec $m_{i,j}, c_i \in K$, de sorte qu'une primitive de $\frac{P}{Q}$ s'écrive sous la forme

$$\int \frac{P}{Q} = \sum_{i=1}^{d} \sum_{j=2}^{r_i} \frac{m'_{i,j}}{(X - \alpha_i)^{j-1}} + \sum_{i=1}^{d} c_i \log(X - \alpha_i),$$

avec $m'_{i,j} \in K$, où chaque $\log(X-\alpha_i)$ désigne un élément d'une extension de $K(X)$ de dérivée $\frac{1}{X-\alpha_i}$.

La difficulté de cette méthode repose sur la décomposition en éléments simples de la fraction $\frac{P}{Q}$, qui nécessite notamment de connaître les racines de Q dans $\mathbb{C}$. Toutefois, comme le montre l'exemple suivant, il n'est pas nécessaire de décomposer $\frac{P}{Q}$ en facteurs du premier degré :

Exemple 3.9. On considère la fraction rationnelle $\frac{X}{X^2-3} \in \mathbb{Q}(X)$; elle se décompose en éléments simples dans $\mathbb{C}$ de la manière suivante :

$$\frac{X}{X^2-3} = \frac{1}{2(X-\sqrt{3})} + \frac{1}{2(X+\sqrt{3})},$$

d'où

$$\int \frac{X}{X^2-3} = \frac{1}{2}\log(X-\sqrt{3}) + \frac{1}{2}\log(X+\sqrt{3}) = \frac{1}{2}\log(X^2-3).$$

Ainsi, l'introduction de $\sqrt{3}$ s'est résorbée au moment d'écrire le résultat final, si bien qu'il est naturel de se demander si l'on pouvait obtenir ce résultat sans décomposer la fraction en éléments simples.

Le théorème de Rothstein-Trager permet de pallier cette difficulté, en évitant de décomposer $\frac{P}{Q}$ en éléments simples :

Théorème 3.10 (Rothstein-Trager)**.** *Soient $P, Q \in \mathbb{Q}[X]$ deux polynômes premiers entre eux, avec $\deg P < \deg Q$ et Q sans facteur carré et unitaire. Soit K une extension de $\mathbb{Q}$ dans laquelle on puisse écrire*

$$\int \frac{P}{Q} = \sum_{i=1}^{r} c_i \log P_i,$$

où les c_i sont des constantes distinctes non nulles de K, et où les P_i sont des polynômes de $K[X]$ unitaires, non constants, sans facteur carré et deux à deux premiers entre eux. Alors les c_i sont les racines distinctes du polynôme

$$R(Y) = \mathrm{Res}_X(P - YQ', Q) \in K[Y],$$

et, pour chaque i, le polynôme P_i vaut

$$P_i = \mathrm{pgcd}(P - c_i Q', Q).$$

La démonstration de ce théorème est présentée en développement dans l'annexe C. Ainsi, la connaissance des racines de $R(Y)$ suffit à déterminer complètement une primitive de $\frac{P}{Q}$.

Exemple 3.11. En guise d'illustration, appliquons le théorème de Rothstein-Trager à l'exemple 3.9. Le résultant $R(Y)$ du théorème est égal à $-3(1-2Y)^2$, d'unique racine $c_1 = \frac{1}{2}$. Le polynôme P_1 correspondant est égal à X^2-3. On retrouve bien

$$\int \frac{X}{X^2-3} = \frac{1}{2}\log(X^2-3),$$

sans avoir eu besoin de décomposer la fraction rationnelle en éléments simples.

Annexe A

Théorème de la borne de Bézout

Théorème (Borne de Bézout)**.** *Soient k un corps infini, et $P, Q \in k[X,Y]$ deux polynômes de degrés totaux respectifs d et d'. On suppose que P et Q sont premiers entre eux. Alors les courbes $\gamma_P = \{(x,y) \in k^2 \,|\, P(x,y) = 0\}$ et $\gamma_Q = \{(x,y) \in k^2 \,|\, Q(x,y) = 0\}$ ont au plus dd' points d'intersection.*

Démonstration. Définissons $R(X) = \mathrm{Res}_Y(P,Q) \in k[X]$, ainsi que $S(Y) = \mathrm{Res}_X(P,Q) \in k[Y]$.

- Nous allons tout d'abord établir que γ_P et γ_Q ont un nombre fini de points d'intersection. Le résultat découle directement de la définition des polynômes $R(X)$ et $S(Y)$: en effet, si (α, β) est un point d'intersection de γ_P et γ_Q, alors $R(\alpha) = 0$ et $S(\beta) = 0$; or, puisque P et Q sont premiers entre eux, $R(X)$ et $S(Y)$ ne sont pas nuls, de sorte que chacun possède un nombre fini de racines, ce qui impose que les courbes s'intersectent en au plus $\deg(R)\deg(S)$ points.
- Nous allons montrer que le degré de $R(X)$ est inférieur ou égal à dd' (et, par symétrie du raisonnement, que le degré de $S(Y)$ est également inférieur ou égal à dd'). Notons p le degré en Y de P, et q le degré en Y de Q, de sorte que l'on puisse écrire

$$P(X,Y) = \sum_{k=0}^{p} P_k(X) Y^{p-k}, \quad Q(X,Y) = \sum_{k=0}^{q} Q_k(X) Y^{q-k},$$

avec

$$\begin{cases} \deg(P_k) \leq d - p + k, & 0 \leq k \leq p, \\ \deg(Q_k) \leq d' - q + k, & 0 \leq k \leq q. \end{cases}$$

Notons $M = (M_{i,j})_{1 \leq i,j \leq p+q}$ la matrice de Sylvester de P et Q comme polynômes en l'indéterminée Y. On a alors

$$M = \begin{pmatrix} P_0 & P_1 & \dots & P_{p-1} & P_p & 0 & \dots & 0 \\ 0 & P_0 & \dots & P_{p-2} & P_{p-1} & P_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & P_0 & P_1 & P_2 & \dots & P_p \\ Q_0 & Q_1 & \dots & Q_{q-1} & Q_q & 0 & \dots & 0 \\ 0 & Q_0 & \dots & Q_{q-2} & Q_{q-1} & Q_q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & Q_0 & Q_1 & Q_2 & \dots & Q_q \end{pmatrix}.$$

□ Pour $1 \leq i \leq q$,

$$M_{i,j} = \begin{cases} P_{j-i} & \text{si } 0 \leq j - i \leq p, \\ 0 & \text{sinon.} \end{cases}$$

Donc pour tout $j \in \{1, \dots, p+q\}$, $\deg(M_{i,j}) \leq d - p + j - i$.

□ De même, pour $q+1 \leq i \leq p+q$,

$$M_{i,j} = \begin{cases} Q_{j-i+q} & \text{si } 0 \leq j-i+q \leq q, \\ 0 & \text{sinon.} \end{cases}$$

Donc pour tout $j \in \{1, \ldots, p+q\}$, $\deg(M_{i,j}) \leq d' - q + j - i + q = d' + j - i$. On applique alors la formule du déterminant :

$$R = \sum_{\sigma \in \mathfrak{S}_{p+q}} \varepsilon(\sigma) \underbrace{\prod_{i=1}^{q} M_{i,\sigma(i)} \prod_{i=q+1}^{p+q} M_{i,\sigma(i)}}_{R_\sigma}.$$

Il suffit alors de montrer que pour tout $\sigma \in \mathfrak{S}_{p+q}$, $\deg(R_\sigma) \leq dd'$. En effet :

$$\begin{aligned} \deg(R_\sigma) &\leq \sum_{i=1}^{q} (d - p + \sigma(i) - i) + \sum_{i=q+1}^{p+q} (d' + \sigma(i) - i) \\ &= q(d-p) + pd' + \underbrace{\sum_{i=1}^{p+q} (\sigma(i) - i)}_{=0} \\ &= qd + pd' - pq \\ &= \underbrace{(p-d)(d'-q)}_{\leq 0} + dd' \\ &\leq dd'. \end{aligned}$$

Par conséquent, $\deg(R) \leq dd'$, et de même, $\deg(S) \leq dd'$.

- À ce stade, on en déduit que les courbes γ_P et γ_Q ont au plus $(dd')^2$ points d'intersection. Nous allons chercher à affiner cette borne. Notons $(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)$ les différents points d'intersection de γ_P et γ_Q. Choisissons $u \in k$ tel que

$$\alpha_i + u\beta_i \neq \alpha_j + u\beta_j, \quad \forall i, j \in \{1, \ldots, r\},\ i \neq j.$$

Un tel u existe, puisque les droites d'équation $y = \alpha_i + x\beta_i$, $x \in k$, ont deux à deux au plus un point d'intersection, et que k est supposé infini. Effectuons alors le changement de variables

$$\begin{cases} X = X' - uY', \\ Y = Y', \end{cases}$$

et notons $\widetilde{P}(X', Y') = P(X, Y)$, $\widetilde{Q}(X', Y') = Q(X, Y)$, ainsi que $\gamma_{\widetilde{P}}$ et $\gamma_{\widetilde{Q}}$ les courbes correspondantes. On a alors,

$$\begin{aligned} (\alpha, \beta) \in \gamma_P \cap \gamma_Q &\iff P(\alpha, \beta) = Q(\alpha, \beta) = 0 \\ &\iff \widetilde{P}(\alpha + u\beta, \beta) = \widetilde{Q}(\alpha + u\beta, \beta) = 0 \\ &\iff (\alpha + u\beta, \beta) \in \gamma_{\widetilde{P}} \cap \gamma_{\widetilde{Q}}. \end{aligned}$$

On en déduit que pour tout $x \in k$ qui est l'abscisse d'un point d'intersection de $\gamma_{\widetilde{P}}$ et $\gamma_{\widetilde{Q}}$, il existe un unique $y \in k$ tel que $(x, y) \in \gamma_{\widetilde{P}} \cap \gamma_{\widetilde{Q}}$, et de plus que $\operatorname{card}(\gamma_{\widetilde{P}} \cap \gamma_{\widetilde{Q}}) = \operatorname{card}(\gamma_P \cap \gamma_Q)$. Donc, quitte à effectuer le changement de variables ci-dessus, on peut supposer sans perte de généralité que les abscisses α_i des points d'intersection de γ_P et γ_Q sont deux à deux distinctes. Or, pour tout $i \in \{1, \ldots, r\}$, $R(\alpha_i) = 0$, et R est non nul de degré inférieur ou égal à dd'. Par conséquent, $r \leq dd'$, ce qui achève la démonstration. ■

Annexe B

Théorème de Kronecker

Théorème (Kronecker)**.** *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, de degré $n \geq 1$. On suppose que les racines de P dans $\mathbb{C}$ sont de module inférieur ou égal à 1, et que 0 n'est pas racine. Alors les racines de P sont des racines de l'unité.*

Démonstration. Notons Ω_n l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$, de degré n, et dont toutes les racines dans $\mathbb{C}$ sont de module inférieur ou égal à 1, et distinctes de 0. Bien entendu, $P \in \Omega_n$. Démontrons que Ω_n est un ensemble fini : soit $F \in \Omega_n$,

$$F = X^n + \sum_{i=1}^{n} f_i X^{n-i},$$

et notons $\beta_1, \ldots, \beta_n$ les racines de F dans $\mathbb{C}$ (non nécessairement distinctes). Par les relations coefficients-racines, pour tout $p \in \{1, \ldots, n\}$,

$$|f_p| = \left| \sum_{1 \leq i_1 < \cdots < i_p \leq n} \prod_{j=1}^{p} \beta_{i_j} \right| \leq \sum_{1 \leq i_1 < \cdots < i_p \leq n} \underbrace{\prod_{j=1}^{p} |\beta_{i_j}|}_{\leq 1} \leq \binom{n}{p}.$$

Comme les coefficients de F sont entiers, alors chacun d'entre eux ne peut prendre qu'un nombre fini de valeurs (indépendamment de F), ce qui impose à l'ensemble Ω_n d'être fini, le degré des éléments de Ω_n étant fixé égal à n.

À présent, notons $\alpha_1, \ldots, \alpha_n$ les racines de P dans $\mathbb{C}$, et définissons, pour tout $k \geq 1$, $P_k = \prod_{i=1}^{n}(X - \alpha_i^k) \in \mathbb{C}[X]$, ainsi que $Q_k = X^k - Y \in \mathbb{Z}[X, Y]$. Commençons par montrer que $P_k \in \mathbb{Z}[X]$, puis que $P_k \in \Omega_n$. Pour ce faire, posons $R_k(Y) = \mathrm{Res}_X(P(X), Q_k(X, Y))$; R_k est un polynôme de $\mathbb{Z}[Y]$, puisque $P(Y)$ et $Q_k(X, Y)$ sont tous les deux des polynômes de $\mathbb{Z}[X, Y]$. De plus,

$$R_k(Y) = \prod_{i=1}^{n} Q_k(\alpha_i, Y) = \prod_{i=1}^{n} (\alpha_i^k - Y) = (-1)^n P_k(Y),$$

ce qui prouve que $P_k \in \mathbb{Z}[X]$. On vérifie immédiatement que P_k est unitaire, et que ses racines sont toutes de module inférieur ou égal à 1, et distinctes de 0, autrement dit que $P_k \in \Omega_n$.

Remarquons que, puisque Ω_n est un ensemble fini, l'ensemble Z_n de toutes les racines des polynômes de Ω_n est également un ensemble fini. Soit α une racine de $P = P_1$. Pour tout $k \geq 1$, α^k est une racine de P_k, de sorte que l'application $k \longmapsto \alpha^k$ définit bien une application de $\mathbb{N}^*$ dans Z_n. Cette application est nécessairement non injective, d'où l'existence de deux entiers $1 \leq r < s$ tels que $\alpha^r = \alpha^s$. Finalement, $\alpha^{s-r} = 1$, et donc α est bien une racine de l'unité. ■

Annexe C

Théorème de Rothstein-Trager

Théorème (Rothstein-Trager)**.** *Soient $P, Q \in \mathbb{Q}[X]$ deux polynômes premiers entre eux, avec* $\deg P < \deg Q$ *et Q sans facteur carré et unitaire. Soit K une extension de $\mathbb{Q}$ dans laquelle on puisse écrire*

$$\int \frac{P}{Q} = \sum_{i=1}^{r} c_i \log P_i,$$

où les c_i sont des constantes distinctes non nulles de K, et où les P_i sont des polynômes de $K[X]$ unitaires, non constants, sans facteur carré et deux à deux premiers entre eux. Alors les c_i sont les racines distinctes du polynôme

$$R(Y) = \mathrm{Res}_X(P - YQ', Q) \in K[Y],$$

et, pour chaque i, le polynôme P_i vaut

$$P_i = \mathrm{pgcd}(P - c_i Q', Q). \tag{C.1}$$

Démonstration. Pour tout $i \in \{1, \ldots, r\}$, définissons $U_i = \prod_{j \neq i} P_j \in K[X]$. Par hypothèse,

$$\frac{P}{Q} = \sum_{i=1}^{r} c_i \frac{P_i'}{P_i} = \frac{\sum_{i=1}^{r} c_i P_i' U_i}{\prod_{i=1}^{r} P_i},$$

en réduisant au même dénominateur, soit

$$P \prod_{i=1}^{r} P_i = Q \sum_{i=1}^{r} c_i P_i' U_i.$$

Ainsi, d'une part, Q divise $\prod_{i=1}^{r} P_i$, car P et Q sont premiers entre eux ; d'autre part, pour tout $i \in \{1, \ldots, r\}$, P_i divise $Q \sum_{j=1}^{r} c_j P_j' U_j$. Comme P_i divise U_j, pour tout $j \neq i$, et comme $c_i \neq 0$, alors P_i divise $Q P_i' U_i$; or P_i est premier avec chacun des P_j, $j \neq i$, donc avec U_i ; de plus, P_i est premier avec P_i', car P_i est sans facteur carré. Il s'ensuit que $P_i | Q$, pour tout $i \in \{1, \ldots, r\}$, et de nouveau, comme les P_i sont deux à deux premiers entre eux, que $\prod_{i=1}^{r} P_i$ divise Q. Par conséquent, Q et $\prod_{i=1}^{r} P_i$ sont associés, et finalement égaux, car tous deux unitaires :

$$Q = \prod_{i=1}^{r} P_i,$$

d'où

$$P = \sum_{i=1}^{r} c_i P_i' U_i.$$

À présent, démontrons que pour tout $i \in \{1, \dots, r\}$, P_i divise $P - c_i Q'$. On a

$$Q' = \sum_{j=1}^{r} P_j' U_j,$$

d'où

$$P - c_i Q' = \sum_{j=1}^{r} (c_j - c_i) P_j' U_j,$$

le terme en $j = i$ étant nul, de sorte que P_i divise bien $P - c_i Q'$. Reste à prouver que $P_i = \operatorname{pgcd}(P - c_i Q', Q)$. En effet,

$$\operatorname{pgcd}(P - c_i Q', Q) = \operatorname{pgcd}\left(P - c_i Q', \prod_{j=1}^{r} P_j\right) = \prod_{j=1}^{r} \operatorname{pgcd}(P - c_i Q', P_j),$$

puisque les P_j sont deux à deux premiers entre eux. Néanmoins, pour $j \neq i$,

$$\begin{aligned} \operatorname{pgcd}(P - c_i Q', P_j) &= \operatorname{pgcd}\left(\sum_{k=1}^{r} (c_k - c_i) P_k' U_k, P_j\right) \\ &= \operatorname{pgcd}((c_j - c_i) P_j' U_j, P_j) \\ &= 1, \end{aligned}$$

car $c_j - c_i \neq 0$ par hypothèse, et que P_j est premier avec P_j' et U_j. En conséquence, sachant que nous avons montré que P_i divise $P - c_i Q'$,

$$\operatorname{pgcd}(P - c_i Q', Q) = \operatorname{pgcd}(P - c_i Q', P_i) = P_i,$$

ce qui vérifie l'égalité (C.1).

Désormais, démontrons que les racines de $R(Y) = \operatorname{Res}_X(P - YQ', Q)$ sont exactement les c_i. Nous venons de montrer que pour tout $i \in \{1, \dots, r\}$, $P - c_i Q'$ et Q ont un facteur commun non constant dans $K[X]$, à savoir leur pgcd P_i, si bien que $R(c_i) = 0$.

Il s'agit alors de montrer que si c est une racine de $R(Y)$ dans le corps de décomposition L de $R(Y)$ sur K, alors c est l'un des c_i. Dire que c est une racine de $R(Y)$ signifie que le pgcd de $P_i - cQ'$ et Q est non constant dans $L[X]$, notons-le S. Considérons un facteur irréductible T de S dans $L[X]$. D'une part, T divise $Q = \prod_{i=1}^{r} P_i$, et comme les P_i sont deux à deux premiers entre eux, alors T divise l'un des P_i, disons P_{i_0}. Par ailleurs, T divise également $P - cQ' = \sum_{i=1}^{r} (c_i - c) P_i' U_i$, donc T divise $(c_{i_0} - c) P_{i_0}' U_{i_0}$; mais comme T est premier avec P_{i_0}' et U_{i_0} (car P_{i_0} l'est), alors T divise $c_{i_0} - c$, et pour des raisons de degrés, $c = c_{i_0}$. Le théorème est démontré. ■

Bibliographie

[1] Philippe Saux Picart, *Cours de calcul formel : Algorithmes fondamentaux*, Ellipses, 1999.

[2] Aviva Szpirglas, *Algèbre L3*, Pearson Education, 2009.

[3] Jean-Yves Mérindol, *Nombres et algèbre*, EDP Sciences, 2005.