LECTURES DIRIGÉES DE RECHERCHE
THÉORÈME DE BÉZOUT

MERCEDES HAIECH ET AUDE LE GLUHER
ENCADRÉES PAR JULIEN SEBAG

Table des matières

Introduction

Une question classique en géométrie est de décrire l'intersection des formes de la géométrie que l'on considère (différentielle, analytique ou algébrique). L'illustration la plus élémentaire en géométrie algébrique est celle de l'intersection d'une famille de variétés associées à la donnée de polynômes (*i.e.* une famille d'*hypersurfaces* de l'espace affine). Le théorème de Bézout fournit une réponse à ce problème. L'objet de ce mémoire est de présenter un énoncé et une preuve de ce résultant dans le cas des courbes, *i.e.* des hypersurfaces du plan ou, de manière équivalente, des polynômes en deux variables.

Si l'on voit une hypersurface comme l'ensemble des zéros d'un polynôme, alors la question revient à chercher les zéros communs de famille des polynômes associés. Cette question est une question très ancienne dans cette branche des mathématiques. Les résultats sur l'intersection entre des droites et des coniques dans le plan sont connus depuis longtemps. On sait, de même, que les solutions rationnelles de deux polynômes homogènes de degré deux ont le même comportement que les solutions d'un polynôme de trois variables de degré trois.

On ne sait pas vraiment qui a observé le premier que, en général, deux courbes planes de degré respectivement p et q s'intersectaient en pq points. Ce que l'on sait, c'est que vers 1680 I. Newton a développé une méthode d'élimination pour de telles équations, ce qui a produit le résultant : un polynôme en une variable de degré pq dont les zéros donnent l'abscisse des points d'intersections de deux courbes planes. La construction correspondante pour n polynômes en n variables fut faite en 1764 par E. Bézout. Le traitement qu'en fit E. Bézout était entièrement algébrique, bien qu'il en fit une interprétation pour $n = 2$ et $n = 3$. Le nombre d'intersections de deux courbes planes est au plus le produit de leur degré.

On peut en dire plus lorsqu'on se place, non plus dans le plan euclidien, mais dans le plan projectif. En associant à un point de la courbe un certain entier que l'on nommera *multiplicité d'intersection*, il est possible de démontrer que le nombre d'intersections de deux courbes, compté avec multiplicité, est exactement égal au produit de leur degré. C'est ce qu'on appelle le *théorème de Bézout* qui est l'objet de ce mémoire.

Par ailleurs, et bien que nous n'abordions pas ce point de vue dans ce texte, il est intéressant de noter qu'en géométrie algébrique moderne une courbe n'est plus définie de manière topologique comme l'ensemble des zéros d'un polynôme, mais de manière algébrique en tant qu'idéal engendré par un polynôme. Ce point de vue est plus riche car il permet, entre autre, de faire la distinction entre la courbe définie par l'idéal engendrée par le polynôme F, et celle engendrée par le polynôme F^2. Le théorème de Bézout reste valide dans ce cadre.

*

Pour ce mémoire, nous avons utilisé les références [1, 2, 3, 4].

1. Préliminaires

1.1. **Quelques propriétés de la localisation.**

Tout les anneaux considérés dans la suite seront supposés **commutatifs** et **unitaires**.

Soit A un anneau commutatif et S une partie multiplicative de A. On rappelle une construction de la localisation de A par S, notée $S^{-1}A$. Considérons la relation $\sim$ sur $S \times A$. On dit que $(s, a) \sim (s', a')$ si et seulement si il existe $t \in S$ tel que $t(as' - a's) = 0$. Cette relation est une relation d'équivalence sur l'ensemble $S \times A$. Une définition de l'anneau $S^{-1}A$ est donnée par $S^{-1}A = S \times A/\sim$. Cette construction vérifie la *propriété universelle de localisation.*

Définition 1.1. On dit qu'un anneau A est local s'il possède un unique idéal maximal.

Remarque. Souvent, nous dirons que le couple $(A, \mathfrak{M})$ est un anneau local, si l'anneau A a pour unique idéal maximal $\mathfrak{M}$.

Proposition 1.1. *Soit A un anneau. Les assertions suivantes sont équivalentes :*

(1) *L'anneau A est local.*

(2) *Il existe un idéal $\mathfrak{M}$ de l'anneau A tel que, pour tout élément $x \in A$, on a $x \notin \mathfrak{M}$ si et seulement si l'élément x est inversible.*

Preuve : On suppose que l'anneau A est local d'idéal maximal $\mathfrak{M}$. Soit alors un élément $x \notin \mathfrak{M}$. Supposons, par l'absurde, que l'élément x n'est pas inversible. Alors l'idéal engendré par x, noté (x) n'est pas égal à l'anneau A. Par le théorème de Krull, il existe un idéal maximal $\mathfrak{M}'$ tel que $(x) \subset \mathfrak{M}'$. Or l'anneau A est local, donc $\mathfrak{M} = \mathfrak{M}'$, et $x \in \mathfrak{M}$, ce qui est absurde. Donc l'élément x est inversible.

Réciproquement on suppose qu'il existe un idéal $\mathfrak{M}$ tel que si $x \notin \mathfrak{M}$ alors l'élément x est inversible. Soit un idéal L tel que $\mathfrak{M} \subset L \subset A$. Si $L \neq \mathfrak{M}$, alors il existe $x \in L$ tel que $x \notin \mathfrak{M}$. Cela impose, par hypothèse, que l'élément x est inversible. Donc $L = A$. On a montré que l'idéal $\mathfrak{M}$ est maximal. Supposons, par l'absurde, qu'il existe un autre idéal maximal $\mathfrak{M}'$ distinct de $\mathfrak{M}$. Alors il existe un élément $x \in \mathfrak{M}' \backslash \mathfrak{M}$. Cet élément est donc inversible et $\mathfrak{M}' = A$, ce qui est absurde, car l'idéal était supposé propre. Donc $\mathfrak{M}$ est l'unique idéal maximal de A. Ce qui montre bien que l'anneau A est local. ▫

Si A est un anneau et $\mathfrak{P}$, un idéal premier de A, on sait que le sous-ensemble $A \backslash \mathfrak{P}$ est une partie multiplicative de A.

Corollaire 1.1. *Soit A un anneau, et soit $\mathfrak{P}$ un idéal premier de A. Alors en notant $S = A \backslash \mathfrak{P}$, l'anneau $S^{-1}A$ est local d'idéal maximal $\mathfrak{P} \cdot (S^{-1}A)$.*

Preuve : La preuve s'appuie sur la proposition 1.1 précédente.

Considérons un élément $x \notin \mathfrak{P}$. La propriété de localisation rend inversible tout élément n'appartenant pas à $\mathfrak{P}$, donc dans l'anneau $S^{-1}A$, l'élément x est inversible. Donc l'anneau $(S^{-1}A, \mathfrak{P})$ est local. ▫

Remarque. Par convention, on note $A_{\mathfrak{P}}$ l'anneau localisé $S^{-1}A$ pour $S = A\backslash\mathfrak{P}$.

Lemme 1.1. *Soit A un anneau, soit I un idéal de A, soit S une partie multiplicative de A, soit J un idéal de $S^{-1}A$. On note $\varphi\colon A \to S^{-1}A$ le morphisme de localisation. Alors on a les propriétés suivantes :*

(1) *$I \cap S \neq \varnothing$ si et seulement si $I \cdot S^{-1}A = S^{-1}A$*

(2) *$\varphi^{-1}(J) \cdot S^{-1}A = J$*

Preuve : (1) On a les équivalences suivantes :

$$I \cdot S^{-1}A = S^{-1}A \Leftrightarrow 1 \in I \cdot S^{-1}A \Leftrightarrow (S^{-1})^{\times}A \cap (I \cdot S^{-1}A) \neq \varnothing$$

S'il existe $s \in I \cap S$, alors $(S^{-1})^{\times}A \cap (I \cdot S^{-1}A) \neq \varnothing$, car $\frac{s}{1} \in I \cdot S^{-1}A$. Réciproquement si $I \cdot S^{-1}A = S^{-1}A$, alors, en particulier, pour tout $s \in S$, l'élément $\frac{s}{1}$ est dans $I \cdot S^{-1}A$. Donc il existe $x \in I$ et $r \in S$ tel que $\frac{s}{1} = \frac{x}{r}$. Donc il existe $t \in S$ tel que $tsr = tx$. En notant z cet élément, on constate que $z \in I \cap S$.

(2) L'ensemble $\varphi^{-1}(J)$ est un idéal de A. De plus $\varphi(\varphi^{-1}(J)) \subset J$, donc l'idéal engendré par $\varphi(\varphi^{-1}(J))$, à savoir $\varphi^{-1}(J) \cdot S^{-1}A$ est inclu dans J. Réciproquement, soit $\frac{x}{s} \in J$, alors $\frac{x}{s} \cdot \frac{s}{1} = \frac{x}{1} \in J$. Donc $x \in \varphi^{-1}(J)$. ▫

1.2. **Quelques propriétés des corps algébriquement clos.**

Définition 1.2. On dit qu'un corps k est algébriquement clos si tout polynôme de degré supérieur ou égal à un, à coefficients dans k, admet au moins une racine dans k.

Exemple 1.1. Le corps $\mathbf{R}$ des nombres réels n'est pas algébriquement clos, car le polynôme $X^2 + 1$ n'admet pas de racine dans $\mathbf{R}$. Le corps $\mathbf{C}$ des nombres complexes est algébriquement clos.

Proposition 1.2. *Un corps algébriquement clos est infini.*

Preuve : Raisonnons par contraposée. Soit k un corps fini. Alors il existe $n \in \mathbf{N}$ tels que $k = \{a_1, a_2, ..., a_n\}$. Considérons dès lors le polynôme $P(X) = \prod_{i=1}^{n}(X - a_i) + 1_k$. Alors, pour tout $i \in [\![1, n]\!], P(a_i) = 1_k \neq 0_k$. C'est un polynôme non constant qui n'admet pas de racine dans k. Donc k n'est pas algébriquement clos. ▫

Théorème 1.1. *Un corps k est algébriquement clos si et seulement si tout polynôme homogène non constant $F \in k[X, Y]$ se décompose en un produit de polynômes de la forme $bX - aY$ avec $(a, b) \in k^2$.*

Preuve : On suppose le corps k algébriquement clos. Soit $F \in k[X,Y]$ un polynôme homogène de degré d. Il existe des éléments $a_{i,j} \in k$ tels que $F = \sum_i a_{i,d-i} X^i Y^{d-i}$. Alors, dans l'anneau $k(Y)[X]$, on a $F = Y^d \sum_i a_{i,d-i} (\frac{X}{Y})^i$.

Posons $F' = \sum_i a_{i,d-i} (X')^i \in k[X']$. C'est un polynôme en la variable X' de degré d. Il découle du fait que le corps k est algébriquement clos que le polynôme F' se factorise sous le forme $F' = \lambda \prod_{i=1}^{d} (X' - c_i)$. Nous en déduisons la formule suivante :

$$F = Y^d F'(X/Y) = \lambda \prod_{i=1}^{d} (\frac{X}{Y} \cdot Y - c_i Y) = \lambda \prod_{i=1}^{d} (X - c_i Y)$$

On a bien prouvé la première implication.

Prouvons la réciproque. Soit $F' \in k[X]$ un polynôme de degré d. Il existe des éléments $a_i \in k$ tels que $F' = \sum_{i=0}^{d} a_i X^i$. Construisons le polynôme suivant :

$$F = Y^d F'(\frac{X}{Y}) = \sum_{i=0}^{d} a_i X^i Y^{d-i}$$

Par hypothèse, le polynôme F se décompose de la manière suivante, $F = \prod_{i=1}^{d} (b_i X - a_i Y)$. Une factorisation par Y^d permet de réécrire le polynôme sous la forme $F = Y^d \prod_{i=1}^{d} (b_i \frac{X}{Y} - a_i)$. Nous pouvons en déduire la relation $Y^d \prod_{i=1}^{d} (b_i \frac{X}{Y} - a_i) = Y^d F'(\frac{X}{Y})$ dans l'anneau $k(Y)[X]$. Donc, comme l'anneau $k(Y)[X]$ est intègre, $F'(X) = \prod_{i=1}^{d} (b_i X - a_i)$. Le polynôme F' admet une décomposition en polynômes de degré un. Donc le corps k est algébriquement clos. ▫

Remarque. La preuve du théorème précédent est fondée sur un principe d'homogénéisation et de déshomogénéisation pour des polynômes en deux variables. Ce principe sera présenté en détail dans la partie 4.1 pour des polynômes en trois variables.

Corollaire 1.2. *Soit k un corps algébriquement clos, et soit $F \in k[X,Y] \backslash \{0\}$ un polynôme homogène. Soit $(a,b) \in k^2 \backslash (0,0)$ tel que $F(a,b) = 0$, alors le polynôme $bX - aY$ est un facteur de F.*

Preuve : En vertu du théorème 1.1, on sait que l'on peut écrire F sous la forme d'un produit $\prod_{i=1}^{d} (b_i X - a_i Y)$ de facteurs non nuls. Comme $F(a,b) = 0$, il existe un facteur de F, disons $b_j X - a_j Y$ tel que $b_j a - a_j b = 0$.

Autrement dit, nous avons

$$\begin{vmatrix} a & a_j \\ b & b_j \end{vmatrix} = 0.$$

Il existe donc un élément $\lambda_j \in k$ tel que $a_j = \lambda_j a$ et $b_j = \lambda_j b$, ce qui conclut la preuve. □

2. Le résultant

2.1. **Définition.**

Soit A un anneau et soient

$$f := \sum_{i=0}^{m} \alpha_i Y^i \in A[Y]$$
$$g := \sum_{i=0}^{n} \beta_i Y^i \in A[Y]$$

deux polynômes à coefficients dans A. Nous supposerons toujours les coefficients $\alpha_m, \beta_n \neq 0$ et $m, n \geqslant 1$.

Définition 2.1. On appelle résultant de f et g, et l'on note $\mathrm{Res}(f,g)$ l'élément de l'anneau A défini par :

$$\left.\begin{vmatrix}
\alpha_0 & 0 & \cdots & 0 & 0 & \beta_0 & 0 & \cdots & 0 & 0 \\
\alpha_1 & \alpha_0 & \ddots & \vdots & \vdots & \beta_1 & \beta_0 & \ddots & \vdots & \vdots \\
\vdots & \alpha_1 & \ddots & 0 & \vdots & \vdots & \beta_1 & \ddots & 0 & \vdots \\
\vdots & \vdots & \ddots & \alpha_0 & 0 & \vdots & \vdots & \ddots & \beta_0 & 0 \\
\alpha_{m-1} & \vdots & \vdots & \alpha_1 & \alpha_0 & \beta_{n-1} & \vdots & \vdots & \beta_1 & \beta_0 \\
\alpha_m & \alpha_{m-1} & \vdots & \vdots & \alpha_1 & \beta_n & \beta_{n-1} & \vdots & \vdots & \beta_1 \\
0 & \alpha_m & \ddots & \vdots & \vdots & 0 & \beta_n & \ddots & \vdots & \vdots \\
\vdots & 0 & \ddots & \alpha_{m-1} & . & \vdots & 0 & \ddots & \beta_{n-1} & 0 \\
\vdots & \vdots & \ddots & \alpha_m & \alpha_{m-1} & \vdots & \vdots & \ddots & \beta_n & \beta_{n-1} \\
0 & 0 & \cdots & 0 & \alpha_m & 0 & 0 & \cdots & 0 & \beta_n
\end{vmatrix}\right\} m{+}n \text{ lignes}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{n \text{ colonnes}} \quad \underbrace{\qquad\qquad\qquad\qquad}_{m \text{ colonnes}}$$

Remarque. Le fait que dans la matrice sous-jacente au déterminant présenté ci-dessus, appelée matrice de Sylvester, les coefficients α_m et β_n soient alignés n'est qu'un hasard.

Remarque. Par convention, si $n = m = 0$, alors on pose :

$$\mathrm{Res}(f,g) = \begin{cases} 0, & \text{si } f = g = 0, \\ 1, & \text{sinon.} \end{cases}$$

Il est possible de donner une définition alternative du résultant, vu comme le déterminant d'une certaine application linéaire.

On identifie l'ensemble des polynômes unitaires de degré n à coefficients dans A à l'espace A^n *via* la bijection

$$X^n + \sum_{i=0}^{n-1} a_{n-i} X^i \mapsto (a_1, \ldots, a_n).$$

Soit $m\colon A^p \times A^q \to A^{p+q}$ l'application qui au couple de polynômes (P, Q), de degré respectifs p, q, associe le produit PQ.

Proposition 2.1. *Le résultant de P, Q s'identifie au déterminant de la matrice jacobienne de m au point (P, Q).*

Preuve : Il existe des éléments $\alpha_i \in A$ et $\beta_j \in A$ tels que $P = X^p + \sum_{i=0}^{p-1} \alpha_{p-i} X^i$ et $Q = X^q + \sum_{j=0}^{q-1} \beta_{q-j} X^j$. L'application m associe aux éléments $(\alpha_1, \cdots, \alpha_p) \in A^p$ et $(\beta_1, \cdots, \beta_q) \in A^q$, l'élément $(\alpha_1 + \beta_1, \cdots, \sum_{i+j=k} \alpha_{p-i}\beta_{q-j}, \cdots, \alpha_p\beta_q)$ de A^{p+q}, pour $0 \leqslant k \leqslant p+q-1$.

L'application m est différentiable, car polynômiale composante par composante. On peut alors calculer la matrice jacobienne qui lui est associée :

$$\left(\frac{\partial}{\partial u_n}\Big(\sum_{i+j=k} \alpha_i \beta_j\Big)\right)_{0 \leqslant k \leqslant p+q-1,\ 0 \leqslant n \leqslant p+q-1} \text{où } u_n = \begin{cases} \beta_n & \text{pour } 0 \leqslant n \leqslant q-1 \\ \alpha_{n-q} & \text{pour } q \leqslant n \leqslant p+q-1 \end{cases}$$

Cette matrice est égale à :

$$\begin{pmatrix} \alpha_p & 0 & \cdots & 0 & \beta_q & 0 & \cdots & 0 \\ \alpha_{p-1} & \alpha_p & \ddots & \vdots & \beta_{q-1} & \beta_q & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \beta_1 & \vdots & \ddots & 0 \\ \alpha_1 & \vdots & \ddots & \alpha_p & 0 & \beta_1 & \ddots & \beta_q \\ \vdots & \alpha_1 & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_1 & 0 & 0 & \cdots & \beta_1 \end{pmatrix}$$

On reconnaît la matrice de Sylvester définissant le déterminant. Le déterminant de la matrice jacobienne de m est bien égal au résultant des polynômes P, Q. ▫

2.2. **Quelques propriétés importantes du résultant.**

Lemme 2.1. *Soit A un anneau intègre, et $f, g \in A[Y]$ deux polynômes non nuls. Alors les assertions suivantes sont équivalentes :*

(1) *On a* $\mathrm{Res}(f, g) = 0$.

(2) *Il existe* $P, Q \in A[Y]\backslash\{0\}$, $\deg(P) < m$ *et* $\deg(Q) < n$ *tels que* $fQ = gP$.

Preuve : On considère le système d'équations suivant :

$$(\sum_{i=0}^{m} \alpha_i Y^i) \cdot (\sum_{i=0}^{n-1} v_i Y^i) = (\sum_{i=0}^{n} \beta_i Y^i) \cdot (\sum_{i=0}^{m-1} u_i Y^i)$$

La condition (2) revient à l'existence d'une solution non triviale de ce système. En développant l'équation précédente et en identifiant coefficient coefficient, on obtient :

$$\begin{cases} \alpha_m v_{n-1} = & \beta_n u_{m-1} \\ \alpha_m v_{n-2} + \alpha_{m-1} v_{n-1} = & \beta_n u_{m-2} + \beta_{n-1} u_{m-1} \\ \cdots & \\ \alpha_0 v_0 = & \beta_0 u_0 \end{cases}$$

On peut réécrire ce système sous forme matricielle et on reconnait la transposée de la matrice de Sylvester définissant le résultant

$$0 = \begin{pmatrix} \alpha_0 & 0 & . & 0 & 0 & \beta_0 & 0 & . & 0 & 0 \\ \alpha_1 & \alpha_0 & . & . & . & \beta_1 & \beta_0 & . & . & . \\ . & \alpha_1 & . & 0 & . & . & \beta_1 & . & 0 & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & \alpha_0 & 0 & . & . & . & \beta_0 & 0 \\ \alpha_{m-1} & . & . & \alpha_1 & \alpha_0 & \beta_{n-1} & . & . & \beta_1 & \beta_0 \\ \alpha_m & \alpha_{m-1} & . & . & \alpha_1 & \beta_n & \beta_{n-1} & . & . & \beta_1 \\ 0 & \alpha_m & . & . & . & 0 & \beta_n & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & 0 & . & \alpha_{m-1} & . & . & 0 & . & \beta_{n-1} & 0 \\ . & . & . & \alpha_m & \alpha_{m-1} & . & . & . & \beta_n & \beta_{n-1} \\ 0 & 0 & . & 0 & \alpha_m & 0 & 0 & . & 0 & \beta_n \end{pmatrix} \cdot \begin{pmatrix} -u_0 \\ . \\ . \\ . \\ . \\ -u_{n-1} \\ v_{m-1} \\ . \\ . \\ . \\ . \\ v_{n-1} \end{pmatrix}$$

D'après les formules de Cramer sur la résolution de systèmes d'équations, l'existence d'une solution non triviale dans le corps des fractions de A, noté k, équivaut donc à la nullité de $\mathrm{Res}(f, g)$. Mais l'existence d'une solution non triviale dans k équivaut à l'existence d'une solution non triviale dans A. En effet, il suffit alors de multiplier les solutions par un dénominateur commun. ▫

Théorème 2.1. *Soit A un anneau factoriel. Soient $f, g \in A[Y]$ deux polynômes non nuls, alors les propriétés suivantes sont équivalentes :*

(1) *On a* $\mathrm{Res}(f, g) = 0$.

(2) *Les polynômes f et g ont un facteur commun non constant dans* $A[Y]$.

Preuve : On suppose (2), alors il existe $h \in A[Y]$ avec $\deg(h) > 0$ tel que $f = \tilde{f}h$ et $g = \tilde{g}h$. On déduit donc l'égalité $f\tilde{g} = g\tilde{f}$, avec $\deg(\tilde{f}) < n$ et $\deg(\tilde{g}) < m$. Le lemme 1.1 implique donc la nullité du résultant $\mathrm{Res}(f, g)$.

Réciproquement, si le résultant $\mathrm{Res}(f,g)$ est nul, d'après le lemme 1.1, il existe $P, Q \in A[Y]\backslash\{0\}$, avec $\deg(P) < m$ et $\deg(Q) < n$ tels que $fQ = gP$. Dans un anneau factoriel, tout élément non nul et non inversible admet une décomposition en irréductibles. Les facteurs irréductibles d'une décomposition de g apparaissent tous dans une décomposition de fQ. Or, ils ne peuvent pas tous apparaître dans une décomposition de Q car $\deg(Q) < \deg(g)$. Ceci prouve que l'un d'eux apparaît dans une décomposition du polynôme f. Donc les polynômes f et g possèdent un facteur commun. ▫

Lemme 2.2. *Soit k un corps, et soient $f, g \in k[X,Y,Z]$ des polynômes homogènes en trois variables. Alors l'égalité suivante est vérifiée :*

$$\mathrm{Res}_Z(f,g)(a,b) = \mathrm{Res}_Z(f(a,b,Z), g(a,b,Z))$$

Preuve : Notons $n = \deg(f) + \deg(g)$, et $S(x,y) = (u_{i,j}(x,y))_{1\leqslant i,j\leqslant n}$ la matrice de Sylvester associée au résultant par rapport à Z des polynômes f et g. Soit (a,b) un élément de k^2. Alors, on a les égalités suivantes :

$$\begin{aligned} \det(S(x,y))(a,b) &= (\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_i u_{i,\sigma(i)}(x,y))(a,b) \\ &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_i u_{i,\sigma(i)}(a,b) \\ &= \det(S(a,b)) \end{aligned}$$

Or $\det(S(x,y))(a,b) = \mathrm{Res}_Z(f,g)(a,b)$ et $\det(S(a,b)) = \mathrm{Res}_Z(f(a,b,Z), g(a,b,Z))$. On en déduit l'égalité voulue. ▫

Corollaire 2.1. *Soit k un corps algébriquement clos et soient $f, g \in k[X,Y,Z]$ des polynômes homogènes en trois variables. Soit $(a,b) \in k^2$ tel que le résultant $\mathrm{Res}_Z(f,g)(a,b)$ soit nul. Alors les polynômes $f(a,b,Z)$ et $g(a,b,Z)$ admettent une racine commune.*

Preuve : D'après le lemme 2.2, on a l'égalité suivante :

$$\mathrm{Res}_Z(f,g)(a,b) = \mathrm{Res}_Z(f(a,b,Z), g(a,b,Z))$$

D'après le théorème 2.1, on en déduit que les polynômes f et g possèdent un facteur commun, noté h. Comme le corps k est algébriquement clos, le polynôme h possède une racine dans k, noté c. Donc c est une racine commune de f et g. Ce qui conclut la preuve. ▫

Théorème 2.2. *Soit A un anneau, soient F et G deux polynômes homogènes dans $A[X_1,\ldots,X_s,Y]$ de degrés respectifs m et n. Si les degrés en Y de F et G, considérés comme des éléments de l'anneau $A[X_1,\ldots,X_s][Y]$, sont respectivement m et n, leur résultant est soit nul, soit un polynôme homogène de degré mn dans $A[X_1,\ldots,X_s]$.*

Preuve : On peut écrire F et G sous la forme

$$F = A_m + A_{m-1}Y + \ldots + A_0 Y^m$$

$$G = B_n + B_{n-1}Y + \ldots + B_0 Y^n$$

avec A_i, B_i des polynômes homogènes de degré i dans $A[X_1, \ldots, X_s]$. De plus $A_0 \neq 0$ et $B_0 \neq 0$ par hypothèse. Le résultant $\mathrm{Res}(tX_1, \ldots, tX_s)$ est alors égal à :

$$\begin{pmatrix}
t^m A_m & 0 & . & 0 & 0 & t^n B_n & 0 & . & 0 & 0 \\
t^{m-1} A_{m-1} & t^m A_m & . & . & . & t^{n-1} B_{n-1} & t^n B_n & . & . & . \\
. & t^{m-1} A_{m-1} & . & 0 & . & . & t^{n-1} B_{n-1} & . & 0 & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & t^m A_m & 0 & . & . & . & t^n B_n & 0 \\
tA_1 & . & . & t^{m-1} A_{m-1} & t^m A_m & tB_1 & . & . & t^{n-1} B_{n-1} & t^n B_n \\
A_0 & tA_1 & . & . & t^{m-1} A_{m-1} & B_0 & tB_1 & . & . & t^{n-1} B_{n-1} \\
0 & A_0 & . & . & . & 0 & B_0 & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & 0 & . & tA_1 & . & . & 0 & . & tB_1 & 0 \\
. & . & . & A_0 & tA_1 & . & . & . & B_0 & tB_1 \\
0 & 0 & . & 0 & A_0 & 0 & 0 & . & 0 & B_0
\end{pmatrix}$$

En multipliant la $i^{\text{ème}}$ colonne par t^{n-i+1} pour $1 \leqslant i \leqslant n$, et la $(n+j)^{\text{ème}}$ colonne par t^{m-j+1} pour $1 \leqslant j \leqslant m$, on obtient :

$$t^p R(tX_1, \ldots, tX_s) = t^q R(X_1, \ldots, X_s)$$

où $p = \frac{n(n+1)}{2} + \frac{m(m+1)}{2}$ et $q = \frac{(m+n)(m+n+1)}{2}$, d'où, on déduit que $R(tX_1, \ldots, tX_s) = t^{mn} R(X_1, \ldots, X_s)$. Ce qui conclut la preuve. ▫

Théorème 2.3. *Soit A un anneau intègre et soient F, G deux polynômes **unitaires** de $A[X]$ de degrés respectifs n et m. On note $(\lambda_1, \cdots, \lambda_n)$ (*resp. *$(\mu_1, \ldots, \mu_m)$) les racines de F (*resp. *G) dans une clôture algébrique du corps des fractions de A. Alors le résultant de F, G est égal à* $\mathrm{Res}(F, G) = \prod_{i,j}(\lambda_i - \mu_j)$.

Preuve : Dans la mesure où les coefficients de F et G s'expriment en fonction des λ_i, respectivement μ_j, il est légitime de considérer le résultant de F, G comme un polynôme dépendant des λ_i et des μ_j. En considérant le résultant comme un polynôme en les variables $(\lambda_1, \cdots, \mu_m)$ le théorème 2.2 nous assure qu'il est de degré mn. De plus ce polynôme s'annule s'il existe i, j tels que $\lambda_i = \mu_j$. En effet, s'il existe i, j tels que $\lambda_i = \mu_j$, alors les polynômes F et G ont une racine commune, donc un facteur commun. D'après le théorème 2.1, le résultant de F et G est donc nul. Donc le polynôme $\mathrm{Res}(F, G)$ est un multiple du polynôme $\prod_{i,j}(\lambda_i - \mu_j)$. Il existe $a \in A$ tel que $\mathrm{Res}(\lambda_1, \cdots, \mu_m) = a \prod_{i,j}(\lambda_i - \mu_j)$. En évaluant en un point, on peut montrer que $\mathrm{Res}(F, G) = \prod_{i,j}(\lambda_i - \mu_j)$.

Remarque. Pour des polynômes $F, G \in k[X]$ de coefficients dominants α_n et β_m, on a l'égalité $\mathrm{Res}(F, G) = \alpha_n^m \beta_m^n \prod_{i,j}(\lambda_i - \mu_j)$

Corollaire 2.2 (Multiplicativité du résultant)**.** *Le résultant est multiplicatif. C'est-à-dire que, pour tous polynômes $F, G, H \in A[X]$, l'égalité suivante est vérifiée :* $\mathrm{Res}(F, GH) = \mathrm{Res}(F, G) \cdot \mathrm{Res}(F, H)$.

Preuve : C'est un corollaire du théorème 2.3, car les zéros du polynôme GH sont exactement les zéros de G et les zéros de H.

Corollaire 2.3. *Soit A un anneau et soient F et G deux polynômes de $A[X]$. Soit $p \in \mathbf{N}$. Alors il existe $c \in A$ tel que* $\mathrm{Res}(X^p F, G) = c\mathrm{Res}(F, G)$.

Preuve : Notons n le degré de F, m celui de G et $(\lambda_1, \cdots, \lambda_n)$ (*resp.* $(\mu_1, \ldots, \mu_m)$) les racines de F (*resp.* G) dans une clôture algébrique du corps des fractions de A. Les racines de $X^p F$ sont alors $(\lambda_1, \cdots, \lambda_{n+1}, \cdots, \lambda_{n+p})$ où pour tout $i \in [\![n+1, n+p]\!]$, $\lambda_i = 0$. Le théorème 2.3 assure donc que :

$$\mathrm{Res}(X^p F, G) = \prod_{i=1}^{n}\prod_{j=1}^{m}(\lambda_i - \mu_j) \times \prod_{j=1}^{m}(-\mu_j)^p = \prod_{j=1}^{m}(-\mu_j)^p \times \mathrm{Res}(F, G)$$

Théorème 2.4. *Soit A un anneau et soient F et G deux polynômes de $A[X]$ de degrés respectifs m et n tels que $n \geqslant m$. Alors, pour tout polynôme $U \in A[X]$ de degré inférieur ou égal à $m - n$, l'égalité suivante est vérifiée :* $\mathrm{Res}(F, G) = \mathrm{Res}(F, G + UF)$.

Preuve : *La preuve de théorème est calculatoire. Elle sera admise.* Cependant l'idée de la preuve consiste à effectuer des opérations élémentaires sur les colonnes du déterminant. Notons M la matrice de Sylvester associée au résultant de F et G et M' celle associée au résultant de F et $G + UF$. Passer de M à M' se fait en ajoutant à chaque colonne de M une combinaison linéaire des autres colonnes de M.

3. L'espace projectif

3.1. Définition de l'espace projectif.

Définition 3.1 (Définition d'un espace projectif)**.** Soit k un corps et E un espace vectoriel sur k.
On introduit une relation d'équivalence notée $\sim$ sur $E\backslash\{0\}$:

$$x \sim y \Leftrightarrow \exists \lambda \in k^*, x = \lambda y$$

On définit alors l'espace projectif sur E comme étant l'ensemble quotient $E/\sim$.
On note cet ensemble $\mathbf{P}(E)$ et on lui associe l'application $\pi : E \to \mathbf{P}(E)$ induite par la propriété universelle du quotient.

Remarque. Si la dimension de l'espace vectoriel E est n, alors la dimension de $\mathbf{P}(E)$ est $n - 1$.

Remarque. Pour un espace vectoriel E sur k de dimension finie il existe $n \in \mathbf{N}\backslash\{0\}$ tel que E s'identifie à k^n. Dans ce cas, nous noterons $\mathbf{P}^{n-1}(k)$ pour $\mathbf{P}(k^n)$.

3.2. **Repères de l'espace projectif.**

Définition 3.2 (Repère dans un espace projectif)**.** Lorsque E est de dimension finie n, on nomme repère projectif de $\mathbf{P}(E)$ tout $(n+1)$-uplet $(p_1, \ldots, p_{n+1})$ de $\mathbf{P}(E)$ tel qu'il existe une base $(e_1, \ldots, e_n)$ de E vérifiant :
(i) $\pi(e_i) = p_i$, $\forall i \in [\![1, n]\!]$
(ii) $\pi(\sum_{k=1}^{n} e_k) = p_{n+1}$.
Si $x \in E$ a pour coordonnées $(x_1, \ldots, x_n)$ dans la base $(e_1, \ldots, e_n)$, on note $[x_1 : \ldots : x_{n+1}]$ les coordonnées dites homogènes de $\pi(x)$ associées à cette base.

Cette définition fait sens. En effet, si $(p_1, ..., p_{n+1})$ est un repère de $\mathbf{P}(E)$ provenant de deux bases $(e_1, \ldots, e_n)$ et $(e'_1, \ldots, e'_n)$ de E alors $\pi(e_i) = \pi(e'_i)$ et $\pi(e_1 + \ldots + e_n) = \pi(e'_1 + \ldots + e'_n)$ pour tout $i \in [\![1, n]\!]$.
Les n premières égalités impliquent que pour tout $i \in [\![1, n]\!]$, il existe $\lambda_i \in k^*$ tel que $e_i = \lambda_i e'_i$.
La dernière se réécrit donc $\pi(\lambda_1 e'_1 + \ldots + \lambda_n e'_n) = \pi(e'_1 + \ldots + e'_n)$ ce qui signifie qu'il existe $\lambda \in k^*$ tel que $\lambda_1 e'_1 + \ldots + \lambda_n e'_n = \lambda(e'_1 + \ldots + e'_n)$.
Comme $(e'_1, \ldots, e'_n)$ est une base de E, on a finalement $\lambda_i = \lambda$ pour tout $i \in [\![1, n]\!]$. Les coordonnées homogènes d'un élément de $\mathbf{P}(E)$ ne dépendent donc pas de la base de E dont on se sert pour construire le repère projectif.

Proposition 3.1 (Changement de repère dans le plan projectif)**.** *Soient E un espace vectoriel et $\mathbf{P}(E)$ l'espace projectif associé. Soient $(p_1, \ldots, p_{n+1})$ et $(p'_1, \ldots, p'_{n+1})$ deux repères projectifs de $\mathbf{P}(E)$. Alors il existe une application $v : \mathbf{P}(E) \to \mathbf{P}(E)$ qui transforme le repère $(p_1, \ldots, p_{n+1})$ en le repère $(p'_1, \ldots, p'_{n+1})$.*

Preuve : D'après la définition 1.3 il existe deux bases $(e_0, \ldots, e_n)$ et $(e'_0, \ldots, e'_n)$, vérifiant respectivement :
(i) $\pi(e_i) = p_i$, $\forall i \in [\![1, n]\!]$
(ii) $\pi(\sum_{k=1}^{n} e_k) = p_{n+1}$.
(i') $\pi(e'_i) = p'_i$, $\forall i \in [\![1, n]\!]$
(ii') $\pi(\sum_{k=1}^{n} e'_k) = p'_{n+1}$.
Alors il existe un automorphisme de E noté $u \in \mathbf{GL_n}(E)$ qui transforme la base $(e_0, \ldots, e_n)$ en la base $(e'_0, \ldots, e'_n)$.
On considère l'application $\tilde{u} : E\backslash\{0\} \to \mathbf{P}(E)$ qui à x associe $\pi(u(x))$. Cette application est telle que pour tout $x \in E\backslash\{0\}$ et $\lambda \in k$, on ait $\tilde{u}(\lambda x) = \tilde{u}(x)$. Ainsi, par propriété universelle de factorisation, l'application $\tilde{u}$ induit une application $v : \mathbf{P}(E) \to \mathbf{P}(E)$ qui transforme le repère $(p_1, \ldots, p_{n+1})$ en le repère $(p'_1, \ldots, p'_{n+1})$. En effet, pour tout $1 \leqslant i \leqslant n+1$, le calcul montre $v(p_i) = \pi \circ u(e_i) = \pi(e'_i) = p'_i$. □

Remarque. L'application v est indépendante du choix des bases $(e_0, \ldots, e_n)$ et $(e'_0, \ldots, e'_n)$.

Proposition 3.2. *Soit E un espace vectoriel de dimension finie. Soit $P \in \mathbf{P}(E)$. On peut compléter P en un repère projectif.*

Preuve : Comme $\pi : E\backslash\{0\} \to \mathbf{P}(E)$ est surjective, il existe $e \in E\backslash\{0\}$ tel que $\pi(e) = P$. Comme $e \neq 0$ et que E est de dimension finie, on peut compléter e en une base $(e, e_2, ..., e_n)$ de E. Cette base induit un repère projectif dont la première composante est P. □

4. Courbes planes

4.1. Définition.

Définition 4.1 (Courbe affine plane)**.** Soit k un corps. On appelle *courbe affine plane* $\mathcal{C}$ le sous-ensemble de k^2 défini par $\mathcal{C} = \{x \in \mathbf{P}^2(k); F(x) = 0\}$ où $F \in k[X, Y]$ est un polynôme non constant. Le *degré* de la courbe $\mathcal{C}$ est le degré du monôme de plus haut degré de F.

Remarque. Soit un polynôme $F \in k[X, Y]\backslash k$. Nous noterons $V(F)$ la courbe affine plane associée.

Définition 4.2 (Courbe projective plane)**.** Soit k un corps. On appelle *courbe projective plane* $\mathcal{C}$ le sous-ensemble de $\mathbf{P}^2(k)$ défini par la donnée de $\mathcal{C} = \{x \in \mathbf{P}^2(k); F(x) = 0\}$ où $F \in k[X, Y, Z]$ est un polynôme homogène non constant. Le *degré* de la courbe $\mathcal{C}$ est le degré commun à tous les monômes de F.

Remarque. Soit un polynôme $F \in k[X, Y, Z]\backslash k$. Nous noterons $V_+(F)$ la courbe projective plane associée.

4.2. Homogénéisation et déshomogénéisation.

Soit $\tilde{P}$ un polynôme de $k[X, Y]$. Le principe d'homogénéisation est une application de $k[X, Y]$ dans $k[X, Y, Z]$, qui au polynôme $\tilde{P}(X, Y)$ associe le polynôme $P(X, Y, Z) := Z^d \tilde{P}(\frac{X}{Z}, \frac{Y}{Z})$, où $d = \deg(\tilde{P})$. Le polynôme $P \in k[X, Y, Z]$ ainsi obtenu est homogène de degré d.

Remarque. Il nous semble important de noter que ce polynôme P est a priori un élément de l'anneau $k(Z)[X, Y]$. Il s'agit de vérifier qu'il appartient à l'image de $k[X, Y, Z]$ par la localisation. Si tel est le cas, comme $k[X, Y, Z]$ est intègre, le morphisme de localisation est injectif, et donc il est légitime d'identifier P à son antécédent dans $k[X, Y, Z]$.

Preuve : Il existe des entiers $n, m \in \mathbf{N}$ et $a_{i,j} \in k$, avec $n+m=d$, tels que $\tilde{P}(X,Y) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{i,j}X^iY^j$. Par définition $P(X,Y,Z) = Z^d \sum_{i=0}^{n}\sum_{j=0}^{m} a_{i,j}(\frac{X}{Z})^i(\frac{Y}{Z}^j)$.

$$P(X,Y,Z) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{i,j}X^iY^jZ^{d-i-j} \text{ avec } d-i-j \geqslant 0$$

Donc le polynôme P est bien un élément de l'image de $k[X,Y,Z]$ par la localisation.

De plus, pour tout élément $\lambda \in k$:

$$P(\lambda X, \lambda Y, \lambda Z) = (\lambda Z)^d \tilde{P}(\frac{\lambda X}{\lambda Z}, \frac{\lambda Y}{\lambda Z}) = \lambda^d Z^d \tilde{P}(\frac{X}{Z}, \frac{Y}{Z}) = \lambda^d P(X,Y,Z)$$

Ainsi, le polynôme P de $k[X,Y,Z]$ est homogène de degré d.

Définition 4.3 (Homogénéisé)**.** Le polynôme P construit ci-dessus est appelé l'*homogénéisé* de $\tilde{P}$.

Exemple 4.1 (Homogénéisation)**.** Considérons la courbe affine de degré deux définie par $P(X,Y) = XY - 1$. C'est une hyperbole. On plonge cette courbe dans le plan projectif en multipliant par $Z^{\deg(P)} = Z^2$ le polynôme P pris en $(\frac{X}{Z}, \frac{Y}{Z})$. Le polynôme décrivant notre hyperbole dans l'espace projectif est donc $Q(X,Y,Z) = Z^2(\frac{X}{Z}\frac{Y}{Z} - 1) = XY - Z^2$

Soit P un polynôme homogène de $k[X,Y,Z]$. Le principe de deshomogénéisation est une application des polynômes homogènes de $k[X,Y,Z]$ dans $k[X,Y]$, qui au polynôme $P(X,Y,Z)$ associe le polynôme $\tilde{P} := P(X,Y,1)$.

Définition 4.4 (Deshomogénéisé)**.** Le polynôme $\tilde{P} \in k[X,Y]$ ainsi défini se nomme le déshomogénéisé de P.

Exemple 4.2 (Déshomogénéisation)**.** Réciproquement, on considère la courbe projective définie par le polynôme homogène de degré deux $Q(X,Y,Z) = XY - Z^2$. La courbe en question est l'ensemble des points de $[x:y:z] \in \mathbf{P}^2(k)$ tels que $xy - z^2 = 0$. On souhaite se replacer dans le plan affine qui est en bijection avec $\{(x,y,1); (x,y) \in k^2\}$. Diviser l'égalité précédente par $z^{\deg(Q)} = z^2$ est donc loisible. On obtient alors que dans le plan affine, notre courbe est l'ensemble des points $(x',y') \in k^2$ tels que

$$\underbrace{\frac{x}{z}}_{x'}\underbrace{\frac{y}{z}}_{y'} - 1 = 0.$$

Proposition 4.1. *L'homogénéisation et la deshomogénéisation sont des applications réciproques l'une de l'autre.*

Preuve : Notons $k_h[X,Y,Z]$ l'ensemble des polynômes homogènes de $k[X,Y,Z]$,

$$\varphi : \begin{cases} k[X,Y] & \to & k_h[X,Y,Z] \\ \tilde{P}(X,Y) & \mapsto & P(X,Y,Z) = Z^d P(\frac{X}{Z}, \frac{Y}{Z}) \text{ où } d = \deg(\tilde{P}) \end{cases}$$

et

$$\psi : \begin{cases} k_h[X,Y,Z] & \to & k[X,Y] \\ P(X,Y,Z) & \mapsto & \tilde{P}(X,Y) = P(X,Y,1) \end{cases}$$

Soit $\tilde{P} \in k[X,Y]$. $\psi(\varphi(\tilde{P}(X,Y))) = 1^{\deg(\tilde{P})}\tilde{P}(\frac{X}{1}, \frac{Y}{1}) = \tilde{P}(X,Y)$ donc $\psi \circ \varphi = \mathrm{Id}_{k[X,Y]}$.

Soit $P \in k_h[X,Y,Z]$. $\varphi(\psi(P(X,Y,Z))) = Z^{\deg P(X,Y,1)}\tilde{P}(\frac{X}{Z}, \frac{Y}{Z}) = P(X,Y,Z)$ donc $\varphi \circ \psi = \mathrm{Id}_{k_h[X,Y,Z]}$.

Donc homogénéisation et déshomogénéisation sont deux procédés réciproques l'un de l'autre.

4.3. **Composantes irréductibles.**

Soit A un anneau factoriel. Soit $P \in A[X,Y]$ un polynôme non constant. Comme l'anneau $A[X,Y]$ est factoriel, le polynôme P admet une décomposition en produit de facteurs irréductibles. Cette remarque permet de définir la notion de composantes irréductibles des courbes planes projectives ou affines.

Définition 4.5 (Composante irréductible)**.** Soit k un corps.

(1) Soit $\mathcal{C}$ une courbe affine plane définie par un polynôme non constant $f \in k[X,Y]$. Les composantes irréductibles de $\mathcal{C}$ sont les courbes affines planes associées aux facteurs irréductibles de f.

(2) Soit $\mathcal{C}$ une courbe projective plane définie par un polynôme homogène non constant $F \in k[X,Y,Z]$. Les composantes irréductibles de $\mathcal{C}$ sont les courbes projectives planes associées aux facteurs irréductibles de F.

Remarque (Composante irréductible commune). Soit $A \in \{k, k[Z]\}$ et $F, G \in A[X,Y]$. On dit que les courbes $V(F)$ (ou $V_+(F)$) et $V(G)$ (ou $V_+(G)$) ont une *composante irréductible commune* s'il existe un facteur irréductible commun aux polynômes F et G.

Théorème 4.1. *Soit $\mathcal{C}, \mathcal{D}$ deux courbes projectives planes définies respectivement par $F, G \in k[X,Y,Z]$. Les courbes $\mathcal{C}, \mathcal{D}$ ont une composante commune si et seulement si* $\mathrm{Res}(F,G) = 0$.

Preuve : C'est une reformulation dans un cadre plus restreint du théorème 2.1.

Lemme 4.1. *Soient F et G deux polynômes homogènes de $k[X,Y,Z]$. Définissons les polynômes $\tilde{F}(X,Y) := F(X,Y,1)$ et $\tilde{G}(X,Y) := G(X,Y,1)$, qui correspondent aux polynômes F et G deshomogénéisés. Si les polynômes F et G sont sans facteur commun, alors il en va de même pour les polynômes $\tilde{F}$ et $\tilde{G}$.*

Preuve : Nous allons démontrer le résultat par contraposée. Supposons que les polynômes $\tilde{F}$ et $\tilde{G}$ possèdent un facteur commun noté $\tilde{Q}$ de degré supérieur à 1. Il existe alors des polynômes $\tilde{F}'$ et $\tilde{G}'$ dans $k[X,Y]$ tels que :

$$\left\{ \begin{array}{lrcl} (i) & \tilde{F}(X,Y) & = & \tilde{Q}(X,Y)\tilde{F}'(X,Y) \\ (ii) & \tilde{G}(X,Y) & = & \tilde{Q}(X,Y)\tilde{G}'(X,Y) \end{array} \right.$$

Nous noterons $n = \deg(\tilde{F})$, $m = \deg(\tilde{G})$, $d = \deg(\tilde{Q})$, $n' = \deg(\tilde{F}')$ et $m' = \deg(\tilde{G}')$. On déduit des égalités (i) et (ii) que $n = d+n'$ et $m = d+m'$.

$$\left\{ \begin{array}{lrcccl} (i') & F(X,Y,Z) & = & Z^n\tilde{F}(\frac{X}{Z},\frac{Y}{Z}) & = & Z^d\tilde{Q}(\frac{X}{Z},\frac{Y}{Z})Z^{n'}\tilde{F}'(\frac{X}{Z},\frac{Y}{Z}) \\ (ii') & G(X,Y,Z) & = & Z^m\tilde{G}(\frac{X}{Z},\frac{Y}{Z}) & = & Z^d\tilde{Q}(\frac{X}{Z},\frac{Y}{Z})Z^{m'}\tilde{G}'(\frac{X}{Z},\frac{Y}{Z}) \end{array} \right.$$

Le polynôme défini par $Q(X,Y,Z) = Z^d\tilde{Q}(\frac{X}{Z},\frac{Y}{Z})$ est un élément non constant de $k[X,Y,Z]$. C'est donc un facteur commun des polynômes F et de G.

Nous avons ainsi démontré, par contraposée, que si les polynômes F et G sont sans facteurs communs alors il en va de même pour les polynômes $\tilde{F}$ et $\tilde{G}$. ▫

Proposition 4.2. *Soit $\tilde{F}$ un polynôme de $k[X,Y]$, d'homogénéisé F. Si $\tilde{Q}$ est un facteur non constant de $\tilde{F}$, alors l'homogénéisé Q de $\tilde{Q}$ est un facteur de F.*

Preuve : Soit $\tilde{Q}$ un facteur non constant du polynôme $\tilde{F}$. Il existe alors un polynôme $\tilde{F}'$ dans $k[X,Y]$ tel que :

$$\tilde{F}(X,Y) = \tilde{Q}(X,Y)\tilde{F}'(X,Y)$$

Nous noterons $n = \deg(\tilde{F})$, $d = \deg(\tilde{Q})$, et $n' = \deg(\tilde{F}')$. On déduit de l'égalité ci-dessus que $n = d + n'$.

$$F(X,Y,Z) = Z^n\tilde{F}(\frac{X}{Z},\frac{Y}{Z}) = Z^d\tilde{Q}(\frac{X}{Z},\frac{Y}{Z})Z^{n'}\tilde{F}'(\frac{X}{Z},\frac{Y}{Z})$$

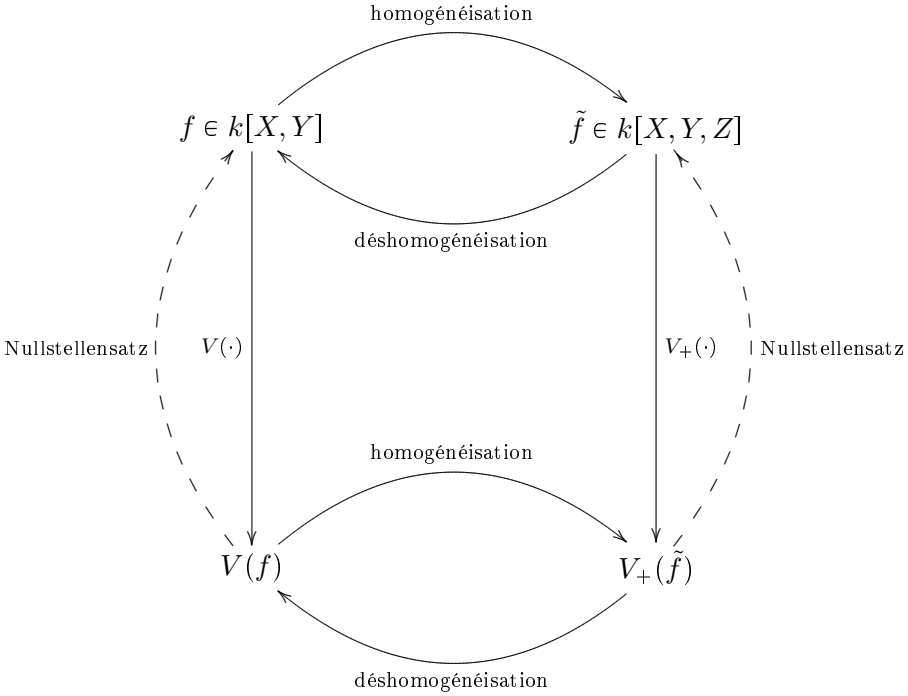
Le polynôme défini par $Q(X,Y,Z) = Z^d\tilde{Q}(\frac{X}{Z},\frac{Y}{Z})$ est un élément non constant de $k[X,Y,Z]$. C'est donc un facteur du polynôme F. ▫

Proposition 4.3. *Soient F un polynôme homogène de $k[X,Y,Z]$ définissant une courbe projective plane notée $V_+(F)$. Si le point $[a:b:c] \in \mathbf{P}^2(k)$ est tel que $F(a,b,c) = 0$, et si $[a:b:c]$ n'est pas un point à l'infini (i.e. $c \neq 0$). Alors $(\frac{a}{c},\frac{b}{c}) \in k^2$ est un zéro du déshomogénéisé de F.*

Preuve : Soit F un polynôme homogène de $k[X,Y,Z]$ de degré d. Il existe des éléments $a_{i,j} \in k^2$ tels que $F(X,Y,Z) = \sum_{i,j} a_{i,j}X^iY^jZ^{d-i-j}$. Soit, de plus, un élément $[a:b:c]$ de $\in \mathbf{P}^2(k)$ tel que $F(a,b,c) = 0$. Dans ce cas $\sum_{i,j} a_{i,j}a^ib^jc^{d-i-j} = 0$. On obtient après factorisation par c^d l'égalité

$c^d \sum_{i,j} a_{i,j} (\frac{a}{c})^i (\frac{b}{c})^j = 0$. Comme c est non nul, on en déduit que $F(\frac{a}{c}, \frac{b}{c}, 1) = 0$, *i.e* l'élément $(\frac{a}{c}, \frac{b}{c})$ est un zéro du déshomogénéisé de F. ▫

Pour conclure, nous résumons ce paragraphe sur les opérations d'homogénéisation et de déshomogénéisation en présentatnt un diagramme qui explique leur compatibilité au niveau des polynômes et des points. Soit $f \in k[X,Y] \backslash k$ un polynôme, supposé sans facteur irréductible multiple.



Remarque. Le théorème du *Nullstellensatz* n'est valable que dans un corps k algébriquement clos.

Notons enfin que l'on a :

$$V_+(\tilde{f}) = \{[a:b:1];\ f(a,b) = 0\} \cup \{[a:b:0];\ \tilde{f}(a,b,0) = 0\}.$$

Les éléments du sous-ensemble $\{[a:b:0];\ \tilde{f}(a,b,0) = 0\}$ de $V_+(\tilde{f})$ son appelés points à l'infini de la courbe $V(f)$.

5. Définition de la multiplicité d'un point d'intersection de deux courbes

Dans cette section, nous allons introduire la notion de *multiplicité d'intersection* de deux courbes.

5.1. **Quelques définitions préliminaires.**

Soient $F, G \in k[X,Y]\backslash k$ deux polynômes. Soient $\mathcal{C}, \mathcal{D}$ les courbes affines planes qui leur sont respectivement associées. Soit $P = (a,b) \in k^2$ un point tel que $F(a,b) = 0$. Dans ce paragraphe, nous allons introduire des notions utiles pour la suite.

Définition 5.1. Soit P un point du plan euclidien k^2. On dit que les courbes $\mathcal{C}, \mathcal{D}$ *s'intersectent proprement* en P si les polynômes F, G n'ont pas de facteur (irréductible) commun non constant $H \in k[X,Y]$ tel que $H(P) = 0$.

Soit $P = (0,0)$ l'origine de k^2. Il existe une famille $(F_i)_{m \leqslant i \leqslant n}$ de polynômes, unique, telle que, pour tout entier i, le polynôme $F_i \in k[X,Y]$ soit homogène de degré i, et $F = F_m + F_{m+1} + \ldots + F_n$. Rappelons que, pour tout entier i, le polynôme F_i est appelé *composante homogène de degré* i de F. La courbe affine plane associée au polynôme F_m est appelé *cône tangent* de $\mathcal{C}$.

Définition 5.2 (Multiplicité au point P)**.**

(1) Si $P = (0,0)$, la *multiplicité à l'origine* du polynôme F est le nombre m est défini ci-dessus. Nous le noterons $m =: m_{(0,0)}(F)$. C'est aussi le degré du *cône tangent* de $\mathcal{C}$.

(2) Si $P = (a,b) \in k^2$, la *multiplicité au point* P du polynôme F est définie par $m_P(F) := m_{(0,0)}(F^T)$, où $F^T(X,Y) = F(X+a, Y+b)$.

Décomposons le polynôme sous la forme $F^T(X,Y) := F(X+a, Y+b) = G_m + G_{m+1} + \ldots + G_n$. De même, d'après le théorème 1.1, le polynôme G_m se décompose sous la forme $G_m = \prod L_i^{r_i}$, où $L_i = \alpha_i X + \beta_i Y$, avec $\alpha_i, \beta_i \in k^2$.

Définition 5.3 (Droites tangentes)**.** Les droites $\alpha_i(X-a) + \beta_i(Y-b)$ sont appelées les *droites tangentes* de F en $P = (a,b)$.

Définition 5.4. Soit T est un changement de repère du plan affine. Notons F^T et G^T les polynômes définissant respectivement les deux courbes $\mathcal{C}^T := \{x \in k^2; F(T(x)) = 0\}$ et $\mathcal{D}^T := \{x \in k^2; G(T(x)) = 0\}$.

5.2. **Une approche axiomatique de la multiplicité d'intersection.**

Soient F et G deux polynômes de $k[X,Y]$ non constants qui définissent des courbes planes affines, notées $\mathcal{C}$ et $\mathcal{D}$. Nous souhaitons définir la multiplicité d'intersection de ces deux courbes en un point $P \in k^2$. Nous introduisons les axiomes suivants pour définir une application I de l'ensemble $k^2 \times (k[X,Y]\backslash k)^2$ dans $\mathbf{N} \cup \{\infty\}$. Pour tout $P \in k^2$, et tout couple $(F,G) \in (k[X,Y]\backslash k)^2$, nous définissons :

(1) $I(P,(F,G))$ est un entier positif, pour tous polynômes F, G, et point P tels que les courbes $\mathcal{C}$ et $\mathcal{D}$ s'intersectent proprement en P. Si les courbes $\mathcal{C}$ et $\mathcal{D}$ ne s'intersectent pas proprement en P alors $I(P,(F,G)) = \infty$.

(2) $I(P,(F,G)) = 0$ si et seulement si le point $P \notin \mathcal{C} \cap \mathcal{D}$.

(3) Si T est un changement de coordonnées du plan affine tel que, pour $Q \in k^2$, $T(Q) = P$, alors $I(Q,(F^T,G^T)) = I(P,(F,G))$.

(4) $I(P,(F,G)) = I(P,(G,F))$.

(5) $I(P,(F,G)) \geqslant m_P(F)m_P(G)$ avec égalité si et seulement si F et G n'ont pas de droites tangentes communes au point P.

(6) Si $F = \prod F_i^{r_i}$ et $G = \prod G_j^{s_j}$. Alors $I(P,(F,G)) = \sum_{i,j} r_i s_j I(P,(F_i,G_j))$.

(7) Pour tout polynôme $A \in k[X,Y]$, $I(P,(F,G)) = I(P,(F,G+AF))$.

Théorème 5.1. *Pour tout couple $(F,G) \in (k[X,Y]\backslash k)^2$, pour tout point $P \in k^2$, il existe au plus un entier $I(P,(F,G))$ vérifiant les axiomes **(1)** à **(7)** précédents.*

Preuve : Il suffit de donner un algorithme constructif pour calculer $I(P,(F,G))$ en utilisant seulement les propriétés **(1)** à **(7)**. Comme la propriété **(3)** assure que les changements de coordonnées ne modifient pas la multiplicité d'intersection, on peut supposer que $P = (0,0)$. Par ailleurs, à moins que les polynômes F et G ne définissent la même courbe, on peut supposer qu'il existe un point où les courbes s'intersectent proprement. Nous supposerons donc, par la propriété **(1)** que le nombre $I(P,(F,G))$ est fini. La propriété **(2)** nous permet le calcul dans le cas où $I(P,(F,G)) = 0$, *i.e* lorsque $P \notin \mathcal{C} \cap \mathcal{D}$. Nous procéderons donc par récurrence, on suppose que $I(P,(F,G)) = n > 0$ et que l'on sait calculer $I(P,(F,G))$ lorsque $I(P,(F,G)) < n$.
Notons respectivement $r, s \in \mathbf{N}$, les degrés des polynômes $F(X,0), G(X,0) \in k[X]$. Comme la propriété **(4)** assure la symétrie de la multiplicité d'intersection par rapport à F et G, on peut supposer que $r \leqslant s$.

Premier cas : *Si* $r = 0$. Alors Y divise le polynôme F, et il existe $H \in k[X,Y]$ tel que $F = YH$. Par la propriété **(6)**, on en déduit l'égalité suivante : $I(P,(F,G)) = I(P,(H,G)) + I(P,(H,G))$. Le polynôme G s'écrit sous la forme $G(X,Y) = X^m(a_0 + a_1X + \ldots + a_nX^n) + YQ(X,Y)$, avec $a_0 \neq 0$, et $Q(X,Y) \in k[X,Y]$. Par la propriété **(7)**, nous en déduisons l'égalité $I(P,(Y,G)) = I(P,(Y,(X^m(a_0 + a_1X + \ldots + a_nX^n)))$. De plus, par la propriété **(6)**, l'entier $I(P,(Y,(X^m(a_0 + a_1X + \ldots + a_nX^n)))$ s'exprime comme :

$$I(P,(Y,X^m)) + I(P,(Y,(a_0 + a_1X + \ldots + a_nX^n)))$$

Or le point $P = (0,0)$ n'appartient pas à l'intersection de Y avec le polynôme $(a_0 + a_1X + \ldots + a_nX^n)$, car $a_0 \neq 0$. Nous en déduisons donc que la multiplicité d'intersection $I(P,(Y,(a_0 + a_1X + \ldots + a_nX^n)))$ est nulle, par la propriété **(2)**. Enfin, comme les polynômes X^m et Y n'ont pas de droites tangentes communes, alors d'après la propriété **(5)**, la multiplicité d'intersection $I(P,(Y,X^m)) = m_P(Y)m_P(X^m) = m$. Ainsi $I(P,(Y,G)) = m$. Or comme P est sur la courbe définie par le polynôme G, le nombre m est strictement positif. Donc $I(P,(H,G)) < n$. On peut donc conclure le calcul par récurrence.

Deuxième cas : *Si* $r > 0$. Nous allons nous ramener au premier cas en utilisant les propriétés **(7)** et **(4)**.

Posons $H = G - X^{s-r}F$. Alors d'après la propriété **(7)**, la multiplicité d'intersection $I(P,(F,G)) = I(P,(F,H))$. De plus $\deg(H(X,0)) = t < s$. En itérant le processus, quitte à intervertir le rôle de F et H, par la propriété **(4)**, si $t < r$, ce calcul nous fournit deux polynômes $A, B \in k[X,Y]$ tels que $I(P,(A,B)) = I(P,(F,G))$, et $\deg(A(X,0)) = 0$.
Nous nous sommes ainsi ramené au premier cas, ce qui conclut la preuve de l'unicité. ▫

Définition 5.5. Soient $P \in k^2$ et $\mathcal{C}, \mathcal{D}$ deux courbes affines planes, définies respectivement par les polynômes non constants $F, G \in k[X,Y]$. S'il existe, l'entier $I_P(\mathcal{C},\mathcal{D}) := I(P,(F,G))$ est appelé *multiplicité d'intersection* des courbes $\mathcal{C}$ et $\mathcal{D}$ au point P.

5.3. **Existence de la multiplicité d'intersection : acte I.**

Dans ce paragraphe, nous admettons certains passages de la preuve du théorème 5.2 qui définit la multiplicité d'intersection de deux courbes affines planes.

Soient $F, G \in k[X,Y]$ deux polynômes non constants. Soit $P = (a,b) \in k^2$. On définit l'anneau $\mathcal{O}_P(k^2)$ par la formule $\mathcal{O}_P(k^2) := k[X,Y]_{(X-a,Y-b)}$. Cet anneau est un anneau intègre qui contient $k[X,Y]$.

Proposition 5.1. *Soient $F, G \in k[X,Y]$ deux polynômes non constants, et $P \in k^2$. La k-algèbre $\mathcal{O}_P(k^2)/(F,G)$ est finie.*

Preuve : Pour plus de clarté, nous allons découper la preuve en plusieurs étapes.

∘ *Étape 1 : Montrons que l'anneau $\mathcal{O}_P(k^2)$ est local.* Pour cela, nous allons montrer que l'idéal $(X-a, Y-b)$ est premier dans $k[X,Y]$. Considérons le morphisme d'évaluation de l'anneau $k[X,Y]$ dans l'anneau k, qui à un polynôme $P(X,Y)$ associe l'élément $P(a,b)$. Ce morphisme est surjectif, et son noyau est l'idéal $(X-a, Y-b)$. Par le lemme de factorisation, nous en déduisons l'existence d'un isomorphisme d'anneau entre $k[X,Y]/(X-a, Y-b)$ et k. Comme k est un corps, l'idéal $(X-a, Y-b)$ est donc maximal. Cet idéal est donc, en particulier, premier. En appliquant le corollaire 1.1, on en déduit que l'anneau $\mathcal{O}_P(k^2)$ est local.

D'après le théorème de correspondance des idéaux, le passage au quotient ne modifie pas cette propriété, donc l'anneau $\mathcal{O}_P(k^2)/(F,G)$ est local.

∘ *Étape 2 : Montrons que l'anneau $\mathcal{O}_P(k^2)$ est noethérien.* Soit J un idéal de $\mathcal{O}_P(k^2)$. Si $J = \mathcal{O}_P(k^2)$, alors l'idéal J est engendré l'élément unité de l'anneau. Il est donc de type fini. On supposera désormais que $J \neq \mathcal{O}_P(k^2)$.

Notons $\varphi\colon k[X,Y] \to \mathcal{O}_P(k^2)$, le morphisme de localisation. D'après le lemme 1.1, l'idéal $\varphi^{-1}(J)$ est tel que $\varphi^{-1}(J) \cdot S^{-1}k[X,Y] = J$. Or d'après la proposition (1) de ce même lemme $\varphi^{-1}(J) \cdot S^{-1}k[X,Y] \neq S^{-1}k[X,Y]$ si et seulement si $\varphi^{-1}(J) \cap S = \varnothing$. Or ici $S = k[X,Y]\backslash(X-a, Y-b)$. Donc $\varphi^{-1}(J) \cdot S^{-1}k[X,Y] \neq S^{-1}k[X,Y]$ si et seulement si $\varphi^{-1}(J) \subset (X-a, Y-b)$. Ainsi $\varphi^{-1}(J) = (X-a, Y-b)$, ou $\varphi^{-1}(J) = (Y-b)$, ou $\varphi^{-1}(J) = (X-a)$, qui sont tous de type fini. Enfin, la proposition (2) du lemme 1.1 nous assure

que $J = \varphi^{-1}(J) \cdot S^{-1}k[X,Y]$ est de type fini. Donc l'anneau $\mathcal{O}_P(k^2)$ est noethérien.

Le passage au quotient ne modifie pas cette propriété, donc l'anneau $\mathcal{O}_P(k^2)/(F,G)$ est noethérien.

On rappelle que la dimension d'un anneau dans la théorie de la dimension de Krull est donnée par le supremum de la longueur des chaînes croissantes d'idéaux premiers.

Comme $\mathcal{O}_P(k^2)$ est un anneau local, dont l'idéal maximal est engendré par deux éléments, alors il est de dimension de Krull inférieure ou égale à deux. Par ailleurs, en appliquant le *Hauptidealsatz* succésivement à l'anneau local noetherien $\mathcal{O}_P(k^2)$, puis à l'anneau local noethérien $\mathcal{O}_P(k^2)/(F)$, on en déduit que $\dim(\mathcal{O}_P(k^2)/(F,G)) \leqslant \dim(\mathcal{O}_P(k^2)) - 2 \leqslant 0$.

Donc l'anneau $(\mathcal{O}_P(k^2)/(F,G))$ est de dimension de Krull nulle.

$\circ$ *Étape 3 : Conclusion.* Par un argument classique d'algèbre commutative, on en déduit alors que la k-algèbre l'anneau $(\mathcal{O}_P(k^2)/(F,G))$ est finie.

Théorème 5.2. *Soient $F,G \in k[X,Y]$ deux polynômes non constants, et $P \in k^2$. L'entier $\dim_k(\mathcal{O}_P(k^2)/(F,G))$ vérifie les axiomes **(1)** à **(7)** précédents. En particulier, $I(P,(F,G)) = \dim_k(\mathcal{O}_P(k^2)/(F,G))$.*

Remarque. La proposition 5.1 assure que cela a du sens de parler de la dimension de la k-algèbre $\mathcal{O}_P(k^2)/(F,G)$.

Preuve : Nous allons prouver partiellement ce théorème. Une preuve détaillée est donnée dans Algebraic Curves de W. Fulton [2].

$\circ$ **(2)** : La dimension de la k-algèbre $\mathcal{O}_P(k^2)/(F,G)$ est nulle si et seulement si $(F,G) = \mathcal{O}_P(k^2)$, si et seulement si $F(P) \neq 0$ ou $G(P) \neq 0$. En effet, l'idéal $(F,G) = \mathcal{O}_P(k^2)$ si et seulement si il existe $U,V,D \in k[X,Y]$ tels que $FU + GV = D$, avec D inversible dans $\mathcal{O}_P(k^2)$. Si $F(P) = G(P) = 0$, alors $D(P) = 0$, donc d'après le corollaire 1.2, le polynôme $bX - aY$ est un facteur de D. Or $bX - aY \in (X-a, Y-b)$. Donc D n'est pas inversible dans $\mathcal{O}_P(k^2)$. Donc par contraposée, si $(F,G) = \mathcal{O}_P(k^2)$ alors $F(P) \neq 0$ ou $G(P) \neq 0$.

Réciproquement montrons que si $F(P) \neq 0$ alors F est inversible dans $\mathcal{O}_P(k^2)$, par contraposée. Supposons que le polynôme F est non inversible. Alors il existe $A,B \in k[X,Y]$ tels que $F = (X-a)A + (Y-b)B$, donc $F(P) = 0$, ce qui conclut. Donc $(F,G) = \mathcal{O}_P(k^2)$.

Donc $(F,G) = \mathcal{O}_P(k^2)$, si et seulement si $F(P) \neq 0$ ou $G(P) \neq 0$.

Donc $\mathcal{O}_P(k^2)/(F,G) = 0$ si et seulement si $P \notin V(F) \cap V(G)$.

$\circ$ **(4)** : L'idéal (F,G) est égal à l'idéal (G,F). Nous en déduisons l'égalité $\dim_k(\mathcal{O}_P(k^2)/(F,G)) = \dim_k(\mathcal{O}_P(k^2)/(G,F))$

$\circ$ **(7)** : Pour tout polynôme $A \in k[X,Y]$, on a l'égalité entre les idéaux $(F,G) = (F, G + AF)$. Nous en déduisons que $\dim_k(\mathcal{O}_P(k^2)/(F,G)) = \dim_k(\mathcal{O}_P(k^2)/(F,G+AF))$.

Les théorèmes 5.1 et 5.2 garantissent que le graphe I précédent est une application.

5.4. **Existence de la multiplicité d'intersection : acte II.**

Nous présentons dans ce paragraphe la notion de multiplicité d'intersection de deux courbes projectives planes. Cette approche est moins théorique et plus effective.

Soit k un corps. Soient $F, G \in k[X,Y,Z]$ deux polynômes homogènes non constants représentant respectivement deux courbes projectives planes $\mathcal{C}$ et $\mathcal{D}$, supposées sans composante commune. On note $\mathrm{Res}_Z(F,G)$ le résultant de $F, G \in k[X,Y][Z]$. En vertu du corollaire 2.1, l'on conclut que l'ensemble des solutions de l'equation $\mathrm{Res}_Z(F(a,b,Z), G(a,b,Z)) = 0$ correspond à l'ensemble des points de $V_+(F) \cap V_+(G)$ de la forme $[a : b : c]$, avec $c \in k$. Autrement dit, il existe $[a : b : c] \in V_+(F) \cap V_+(G)$ si et seulement si $(bX - aY)$ divise $\mathrm{Res}_Z(F,G)$ d'après le théorème 1.1.

Soit $(a,b) \neq (0,0)$. On note $\iota_{(a:b)}(F,G)$ le plus grand élément $\ell \in \mathbf{N}$ tel que $(bX - aY)^\ell$ divise $\mathrm{Res}_Z(F,G)$. Soit $J\colon k^2 \times (k[X,Y]\backslash k)^2 \to \mathbf{N} \cup \{\infty\}$ l'application définie par

$$((a,b),(f,g)) \mapsto \iota_{(a:b)}(\tilde{f}, \tilde{g}),$$

si $\tilde{f}, \tilde{g}$ sont sans facteurs communs. Par convention, J prend la valeur ∞ si les courbes correspondantes ont une composante commune.

Théorème 5.3. *Pour tout point $(a,b) \in (k^*)^2$ et tout couple de polynômes $(f,g) \in (k[X,Y]\backslash k)^2$, l'élément $J((a,b),(f,g))$ vérifie les axiomes* ***(1)***, ***(3)*** *à* ***(7)*** *précédents, ainsi que l'axiome* ***(2')*** *suivant : $J((a,b),(f,g)) \neq 0$ si et seulement il existe $c \in k$ tel que $[a : b : c] \in V_+(\tilde{f}) \cap V_+(\tilde{g})$.*

Preuve : Nous allons vérifier un à un que les axiomes sont vérifiés.

Axiome 1 : $J((a,b),(f,g)) \geqslant 0$ est acquis. Si $\mathcal{C}$ et $\mathcal{D}$ ne s'intersectent pas proprement en P, alors les polynômes f et g ont un facteur commun, donc d'après la proposition 4.2, les polynômes $\tilde{f}$ et $\tilde{g}$ ont aussi un facteur commun. D'après le théorème 2.1 leur résultant est donc nul. L'on déduit que $J((a,b),(f,g)) = \infty$.

Axiome 2' : la preuve découle directement de la remarque du début du paragraphe.

Si $P = [a : b : c] \in \tilde{\mathcal{C}} \cap \tilde{\mathcal{D}}$, alors $f(a,b) = 0$ et $g(a,b) = 0$. Donc $\tilde{f}(a,b,1) = 0$ et $\tilde{g}(a,b,1) = 0$. Ainsi les polynômes $\tilde{f}(a,b,Z)$ et $\tilde{g}(a,b,Z)$ possèdent un facteur commun. D'après le théorème 2.1 et le lemme 2.2, nous en déduisons que $\mathrm{Res}(\tilde{f}, \tilde{g})(a,b) = 0$. Donc d'après le théorème 1.1 le polynôme $bX - aY$ est un facteur du polynôme $\mathrm{Res}(\tilde{f}, \tilde{g})$. Donc $\iota_{(a:b)}(\tilde{f}, \tilde{g}) \geqslant 1$. Ainsi $J((a,b),(f,g)) \neq 0$.

Réciproquement, si $J((a,b),(f,g) \geqslant 1$, alors $\iota_{(a:b)}(\tilde{f}, \tilde{g}) \neq 0$. Par définition, cela signifie que $bX - aY$ est un facteur de $\mathrm{Res}_Z(\tilde{f}, \tilde{g})$. Donc le nombre $\mathrm{Res}_Z(\tilde{f}(a,b,Z), \tilde{g}(a,b,Z))$ est nul. D'après le corollaire 2.1, nous en déduisons que les polynômes $\tilde{f}(a,b,Z)$ et $\tilde{g}(a,b,Z)$ ont une racine commune notée c. Cela conclut la preuve.

Axiome 3 : Soit T un changement affine de coordonnées tel que $T(Q) = P$. Notons $Q = (c, d)$ et $P = (a, b)$. Le polynôme noté f^T est tel que, pour tout $x \in k^2$, $f^T(x) = f(T(x))$.

Nous allons montrer que $\widetilde{f^T}(c, d, Z) = \tilde{f}(a, b, Z)$.

Par définition, nous avons l'égalité suivante : $f^T(c, d) = f(a, b)$. Par ailleurs les degrés des polynômes f et f^T sont égaux ; en notant n ce degré commun, nous obtenons que : $Z^n f^T(\frac{c}{Z}, \frac{d}{Z}) = Z^n f(\frac{a}{Z}, \frac{b}{Z})$, ce qui revient à dire que $\widetilde{f^T}(c, d, Z) = \tilde{f}(a, b, Z)$.

Nous déduisons de l'égalité précédente, valable pour tout $f \in k[X, Y]$ et tous points $P, Q \in k^2$ tels que $T(Q) = P$, que $\mathrm{Res}_Z(\widetilde{f^T}, \widetilde{g^T})(Q) = \mathrm{Res}_Z(\tilde{f}, \tilde{g})(T(P))$. On déduit de cette égalité que $\iota_{(a:b)}(\tilde{f}, \tilde{g}) = \iota_{(c:d)}(\widetilde{f^T}, \widetilde{g^T})$. Donc $J((a, b)(f, g) = J((c, d)(f^T, g^T))$.

Axiome 4 : Notons m et n les degrés respectifs de $\tilde{f}$ et $\tilde{g}$. Passer de la matrice qui donne $\mathrm{Res}_Z(\tilde{f}, \tilde{g})$ à celle qui donne $\mathrm{Res}_Z(\tilde{g}, \tilde{f})$ se fait en permutant nm colonnes. Donc $\mathrm{Res}_Z(\tilde{f}, \tilde{g}) = (-1)^{mn}\mathrm{Res}_Z(\tilde{g}, \tilde{f})$. Donc $\mathrm{Res}_Z(\tilde{f}, \tilde{g}) = (-1)^{mn}\mathrm{Res}_Z(\tilde{g}, \tilde{f})$ ont les mêmes facteurs (irréductibles) $aX - bY$. Donc $\iota_{(a:b)}(C, D) = \iota_{(a:b)}(D, C)$. Donc $J((a, b)(f, g)) = J((a, b)(g, f))$

Axiome 5 : La démonstration de cet axiome est extrêmement fastidieuse, nous vous renvoyons au théorème 54.6 du livre *Algrebraic geometry for beginners* de C. Musili [4].

Axiome 6 : Soient $\tilde{h}, \tilde{g}_1, \tilde{g}_2$ des polynômes homogènes de $k[X, Y, Z]$. Par le corollaire 2.2, qui démontre la multiplicativité du résultant :

$$\mathrm{Res}_Z(\tilde{h}, \tilde{g}_1\tilde{g}_2) = \mathrm{Res}(\tilde{h}, \tilde{g}_1) + \mathrm{Res}(\tilde{h}, \tilde{g}_2)$$

Donc $\iota_{(a:b)}(\tilde{h}, \widetilde{g_1 g_2}) = \iota_{(a:b)}(\tilde{h}, \tilde{g}_1) + \iota_{(a:b)}(\tilde{h}, \tilde{g}_2)$, car $\widetilde{g_1 g_2} = \tilde{g}_1\tilde{g}_2$. Donc l'égalité suivante est vérifiée : $J((a, b)(h, g_1 g_2)) = J((a, b)(h, g_1)) + J((a, b)(h, g_2))$.

Décomposons alors les polynômes f et g sous la forme suivante $f = \prod_i f_i^{\alpha_i}$ et $g = \prod_j g_j^{\beta_j}$. Nous en déduisons par récurrence sur $\deg(f) + \deg(g)$ que $J((a, b)(f, g)) = \sum_{i,j} \alpha_i \beta_j J((a, b)(f_i, g_j))$.

Axiome 7 : Notons $m = \deg(f)$, $n = \deg(g)$. On peut supposer que $n \geqslant m$ grâce à l'axiome 4.

La démonstration de l'unicité de l'objet défini dans le théorème 5.1 n'utilise que le fait que le polynôme $A \in k[X, Y]$ *est de degré inférieur ou égal à* $n - m$. *Nous montrerons que, pour tout polynôme* $u \in k[X, Y]$, *tel que* $\deg(u) \leqslant n - m$, *on a l'égalité suivante :* $J((a, b), (f, g)) = J((a, b)(f, g + uf))$.

Notons $d = \deg(g + uf)$, et $l = \deg(u)$

Si $d = n$, alors $g + uf$ est de degré n, donc

$$\widetilde{g + uf} = Z^n(g(\frac{X}{Z}, \frac{Y}{Z}) + uf(\frac{X}{Z}, \frac{Y}{Z})) = \tilde{g} + \tilde{f} \cdot \tilde{u} Z^{n-l-m} \quad (1)$$

Comme le polynôme $\tilde{u}Z^{n-l-m}$ est de degré $n-m$, nous pouvons utiliser le théorème 2.4 qui assure que $\mathrm{Res}_Z(\tilde{f},\tilde{g}+\tilde{f}\cdot\tilde{u}Z^{n-l-m}) = \mathrm{Res}_Z(\tilde{f},\tilde{g})$. Donc en combinant avec l'égalité (1), on obtient le résultat : $\widetilde{\mathrm{Res}_Z(\tilde{f},\tilde{g})} = \mathrm{Res}_Z(\tilde{f},\widetilde{g+uf})$. Donc on en déduit que $\iota_{(a:b)}(\tilde{f},\tilde{g}) = \iota_{(a:b)}(\tilde{f},\widetilde{g+uf})$. Donc $J((a,b),(f,g)) = J((a,b)(f,g+uf))$.

Si $d<n$, alors on a toujours l'égalité : $Z^n(g(\frac{X}{Z},\frac{Y}{Z})+uf(\frac{X}{Z},\frac{Y}{Z})) = \tilde{g}+\tilde{f}\cdot\tilde{u}$. Par ailleurs, on a aussi $Z^{n-d}Z^d(g(\frac{X}{Z},\frac{Y}{Z})+uf(\frac{X}{Z},\frac{Y}{Z})) = Z^{n-d}\widetilde{g+uf}$. Nous utilisons l'égalité $\tilde{g}+\tilde{f}\cdot\tilde{u} = Z^{n-d}\widetilde{g+uf}$, pour en déduire que $\mathrm{Res}_Z(\tilde{f},\tilde{g}+\tilde{f}\cdot\tilde{u}) = \mathrm{Res}_Z(\tilde{f},Z^{n-d}\widetilde{g+uf})$. Par le théorème 2.4 et le corollaire 2.3, il existe $c\in k$ tel que l'égalité suivante soit vérifiée : $\mathrm{Res}_Z(\tilde{f},\tilde{g}) = c\mathrm{Res}_Z(\tilde{f},\widetilde{g+uf})$. L'on conclut par le même argument que précédemment que $J((a,b),(f,g)) = J((a,b)(f,g+uf))$.

Remarque. Dans la preuve des théorèmes de Bézout (formes faible et forte), nous montrerons comment l'on peut toujours supposer $(a,b)\neq(0,0)$ *via* un changement de coordonnées. Cette remarque implique en particulier que la construction prend un sens en général.

Définition 5.6. Soient k un corps. Soient $\mathcal{C},\mathcal{D}$ deux courbes projectives planes respectivement associées aux polynômes homogènes non constants $F,G\in k[X,Y,Z]$, supposés sans facteur irréductible commun. On appelle *multiplicité d'intersection* de $\mathcal{C}$ et $\mathcal{D}$ au point $P=[a:b:c]$, $c\neq 0$, l'entier $I_P(\mathcal{C},\mathcal{D}) := I((\frac{a}{c},\frac{b}{c}),(F(X,Y,1),G(X,Y,1))$.

Remarque. Si $a\neq 0$, on peut montrer que la définition ci-dessus est encore égale à $I((\frac{a}{c},\frac{b}{c}),(F(1,Y,Z),G(1,Y,Z))$. (Idem si $b\neq 0$.) Nous admettons ce point.

6. Énoncé et démonstration du théorème de Bézout

6.1. **Quelques résultats préliminaires.** Dans toute ce paragraphe, nous noterons k un corps algébriquement clos, et $\mathbf{P}^2(k) := k^3\backslash\{0\}/\sim$ le plan projectif, où $\sim$ est la relation d'équivalence définie dans la définition 3.1.

Lemme 6.1. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux courbes définies par des polynômes en deux variables F et G dans le plan euclidien. Si les polynômes F et G sont sans facteur commun, alors l'ensemble $\mathcal{C}\cap\mathcal{D}$ est fini.*

Preuve : Les polynômes F et G sont sans facteur commun dans $k[X][Y]$, ils n'ont donc pas de facteurs commun dans $k(X)[Y]$. Comme $k(X)$ est un corps, l'anneau $k(X)[Y]$ est euclidien. Donc le plus grand diviseur commun de F et G existe et vaut 1. Par conséquent, il existe $R,S\in k(X)[Y]$ tels que $RF+SG=1$. De plus il existe un polynôme non nul $D\in k[X]$ tel que $A:=DR\in k[X,Y]$ et $B:=DS\in k[X,Y]$. Ainsi $AF+BG=D$. Si $(a,b)\in\mathcal{C}\cap\mathcal{D}$, alors $D(a)=0$. Comme D a un nombre fini de zéros, la première coordonnée des éléments de $\mathcal{C}\cap\mathcal{D}$ ne peut prendre qu'un nombre fini de valeurs.

On peut appliquer le même raisonnement aux coordonnées selon Y. Donc il n'y a qu'un nombre fini d'éléments dans $\mathcal{C} \cap \mathcal{D}$. ▫

Proposition 6.1. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux courbes définies par des polynômes homogènes $F, G \in k[X, Y, Z]$. Si les polynômes F et G sont sans facteur commun, alors l'ensemble $\mathcal{C} \cap \mathcal{D}$ est fini.*

Preuve : Par le principe de deshomogénéisation, on transforme les polynômes F et G en des polynômes $\tilde{F}$ et $\tilde{G}$ de deux variables. D'après le lemme 4.1, ces polynômes restent sans facteur commun. On applique alors le lemme 6.1 à $\tilde{F}$ et $\tilde{G}$ et en déduit que l'ensemble $\tilde{\mathcal{C}} \cap \tilde{\mathcal{D}}$ est fini, où $\tilde{C}$ et $\tilde{D}$ sont les courbes du plan euclidien définies par la donnée des polynômes $\tilde{F}$ et $\tilde{G}$. On en déduit que l'ensemble $\mathcal{C} \cap \mathcal{D}$ est également fini, par le lemme 6.2 suivant. ▫

Lemme 6.2. *En gardant les notations précédentes, si l'ensemble $\tilde{\mathcal{C}} \cap \tilde{\mathcal{D}}$ est fini alors l'ensemble $\mathcal{C} \cap \mathcal{D} = \{x = [a : b : c] \in \mathbf{P}^2(k); F(x) = G(x) = 0\}$ est fini.*

Preuve : Si $c \neq 0$, alors $[a : b : c] \sim [\frac{a}{c} : \frac{b}{c} : 1]$. Pour les éléments x tels que c est non nul, dire que $x \in \mathcal{C} \cap \mathcal{D}$ revient à demander que $(\frac{a}{c}, \frac{b}{c}) \in \tilde{\mathcal{C}} \cap \tilde{\mathcal{D}}$.

Si $c = 0$, alors comme 0 n'est pas un élément du plan projectif, un des éléments a ou b est non nul. Sans perdre de généralité, on peut supposer que $b \neq 0$. Ainsi $[a : b : 0] \sim [\frac{a}{b} : 1 : 0]$. Dire que $x \in \mathcal{C} \cap \mathcal{D}$ avec $c = 0$ revient à demander à ce que $\frac{a}{b}$ soit racine commune des polynômes en une variable $F(X, 1, 0)$ et $G(X, 1, 0)$. Ces polynômes en une variable n'ont qu'un nombre fini de racines. Il n'y a donc qu'un nombre fini de points à l'infini dans $\mathcal{C} \cap \mathcal{D}$.

L'ensemble $\mathcal{C} \cap \mathcal{D}$ est donc fini, en tant que réunion de deux ensembles finis. ▫

6.2. **Enoncé et démonstration.**

Théorème 6.1 (Forme faible du théorème de Bézout)**.** *Soit k un corps algébriquement clos. Soit $\mathcal{C}$ (resp. $\mathcal{D}$) une courbe projective plane définie par la donnée d'un polynôme F (resp. G) homogène de degré $m \geqslant 1$ (resp. $n \geqslant 1$). Si les deux courbes n'ont pas de composante commune, i.e.* $\operatorname{pgcd}(F, G) = 1$*, alors les deux courbes s'intersectent en au plus mn points distincts.*

Preuve : Nous allons prouver le théorème 6.1 par l'absurde en découpant la preuve en différentes étapes. D'après la proposition 6.1, l'ensemble $\mathcal{C} \cap \mathcal{D}$ est fini. Supposons que $|\mathcal{C} \cap \mathcal{D}| \geqslant mn + 1$. Nous fixons un ensemble S de $mn + 1$ points choisis dans l'ensemble $\mathcal{C} \cap \mathcal{D}$.

∘ *Étape 1 : montrons que l'on peut supposer que les polynômes F, G sont non constants en la variable Z.*

L'idée est ici d'exprimer les données dans un « bon » système de coordonnées dans $\mathbf{P}^2(k)$. Considérons les lignes droites L_{PQ} qui joignent une paire de points $P, Q \in S$. On peut alors choisir un point P_0 qui n'est ni sur $\mathcal{C}$, ni

sur $\mathcal{D}$, ni sur une des lignes L_{PQ} car k est infini d'après la proposition 1.2 Par un changement de coordonnées, en se référant à la proposition 3.2, on peut supposer que $P_0 = [0:0:1]$.

On remarquera, en particulier, que pour tout $[a:b:c] \in S$, le couple (a,b) est non nul. En effet, si tel était le cas, alors le point $[0:0:c]$ appartiendrait à S, avec $c \neq 0$, car $[0:0:0]$ n'est pas un élément du plan projectif. Alors $[0:0:c] \sim [0:0:1]$, ce qui signifie que $P_0 \in S$; or ceci est absurde par hypothèse.

Comme $F(0,0,1) \neq 0$ et $G(0,0,1) \neq 0$, puisque le point P_0 n'appartient pas aux courbes $\mathcal{C}$ ou $\mathcal{D}$, la variable Z apparaît effectivement dans l'expression des polynômes des F et G.

∘ *Étape 2 : montrons que le résultant* $\mathrm{Res}_Z(F,G)$ *est un polynôme homogène non nul de degré* mn.

Écrivons F et G comme des polynômes en Z à coefficients dans $k[X,Y]$,

$$F = A_0 Z^m + A_1(X,Y)Z^{m-1} + \ldots + A_{m-1}(X,Y)Z + A_m(X,Y)$$

$$G = B_0 Z^n + B_1(X,Y)Z^{n-1} + \ldots + B_{n-1}(X,Y)Z + B_n(X,Y)$$

où chaque A_i (respectivement B_j) est soit nul, soit un polynôme homogène de degré i (respectivement j). On peut remarquer que les propriétés suivantes sont vérifiées :

$$\begin{cases} (i) & A_m \text{ ou } B_n & \neq & 0 \\ (ii) & A_0, B_0 & \in & k \\ (iii) & A_0 B_0 & \neq & 0 \end{cases}$$

En effet, si la propriété (i) était invalide, Z serait un facteur commun de F et G ; les propriétés (ii) et (iii) découlent directement du fait que le point $P_0 = [0:0:1]$ n'appartient pas à $\mathcal{C} \cap \mathcal{D}$. On en déduit, d'après le théorème 2.2, que $\mathrm{Res}_Z(F,G)$ le résultant de F et G par rapport à Z est soit nul, soit un polynôme homogène de $k[X,Y]$ de degré mn.

∘ *Étape 3 : Le résultant* $\mathrm{Res}_Z(F,G) \neq 0$ *(ainsi il est homogène de degré* mn*).*

Supposons que $\mathrm{Res}(F,G)(a,b) = 0$ pour tout $(a,b) \in k^2$. D'après le corollaire 2.1, les polynômes $F(a,b,Z)$ et $G(a,b,Z)$ ont une racine commune qui dépend de (a,b), notons-la $Z = c$. Cela signifie que, pour tout $(a,b) \in k^2 \backslash \{0\}$, il existe $c \in k$ tel que $(a,b,c) \in \mathcal{C} \cap \mathcal{D}$. L'ensemble $\mathcal{C} \cap \mathcal{D}$ serait donc infini, ce qui est absurde.

∘ *Étape 4 : concluons la preuve par l'absurde.*

On remarque que pour tout point $[a:b:c] \in \mathcal{C} \cap \mathcal{D}$, l'élément c est une racine commune de $F(a,b,Z)$ et $G(a,b,Z)$. Ainsi $\mathrm{Res}_Z(F(a,b,Z), G(a,b,Z))$ est nul, *i.e.* $\mathrm{Res}_Z(F,G)(a,b) = 0$. Ceci est vrai pour tout $[a:b:c] \in S$. En d'autres termes, pour tout $[a:b:c] \in S$ on montre que $(a,b) \neq 0$ et (a,b) est un zéro non trivial de $\mathrm{Res}_Z(F,G)$, *i.e.* $bX - aY$ est un facteur de $\mathrm{Res}_Z(F,G)$ par le corollaire 1.2. Cependant S contient au moins $mn+1$ points et $\mathrm{Res}_Z(F,G)$ est seulement de degré mn. On en déduit que l'ensemble $\{\frac{a}{b} \ ; [a:b:c] \in S\}$ peut prendre au plus mn valeurs distinctes. Ou, de manière équivalente, il existe $P_i = [a_i : b_i : c_i] \in S$ pour $i = 1,2$ avec

$P_1 \neq P_2$ tels que $\frac{a_1}{b_1} = \frac{a_2}{b_2}$. Cela signifie que P_1, P_2 et $P_0 = (0,0,1)$ sont sur une droite définie par $b_1X - a_1Y = 0$, ce qui est absurde dans la mesure où P_0 n'est sur aucune des lignes reliant deux points de S. ▫

Théorème 6.2 (Forme forte du théorème de Bézout)**.** *Soit k un corps algébriquement clos. Soit $\mathcal{C}$ (resp. $\mathcal{D}$) une courbe projective plane définie par la donnée d'un polynôme F (resp. G) homogène de degré $m \geqslant 1$ (resp. $n \geqslant 1$). Si les deux courbes n'ont pas de composante commune, alors elles ont exactement mn points d'intersections comptés avec multiplicité.*

Preuve : L'ensemble $\mathcal{C} \cap \mathcal{D}$ étant fini, il existe donc un entier $k \in \mathbf{N}$ tel que $\mathcal{C} \cap \mathcal{D} = \{P_1, \ldots, P_k\}$. On reprend des éléments de la preuve du théorème 6.1 : on choisit un point P_0 en dehors de $\mathcal{C}$, $\mathcal{D}$ et de toutes les droites $L_{P_iP_j}$ qui relient les points P_i et P_j pour $i \neq j$; on choisit un repère tel que $P_0 = [0:0:1]$. On considère F et G comme des polynômes en Z à coefficients dans $k[X,Y]$, le résultant de F et G est non nul, et c'est donc un polynôme homogène de degré mn. Si $P_i = [a_i : b_i : c_i]$, $1 \leqslant i \leqslant k$, nous avons vu que (i) $(a_i, b_i) \neq 0$, (ii) $\frac{a_i}{b_i} \neq \frac{a_j}{b_j}$ pour tout $i \neq j$, (iii) les zéros non triviaux de $\mathrm{Res}_Z(F,G)$ sont précisément les points communs de $\mathcal{C}$ et $\mathcal{D}$, c'est-à-dire que les éléments $(\frac{a_i}{b_i}, 1)$ sont exactement tous les zéros non triviaux distincts de $\mathrm{Res}_Z(F,G)$.

On remarque alors que, grâce à (ii) et au théorème 5.3, l'entier $\iota_{(a_i:b_i)}(F,G)$ vérifie l'axiome **(2)** du paragraphe 5.2, et donc que $\ell_i := \iota_{(a_i:b_i)}(F,G) = I_P(F,G)$ en vertu du théorème 5.1. En outre, on a :

$$\mathrm{Res}_Z(F,G) = \prod_{i=1}^{k} (b_iX - a_iY)^{\ell_i} \text{ avec } \ell_1 + \ldots + \ell_k = mn$$

Cette formule conclut la preuve du théorème. ▫

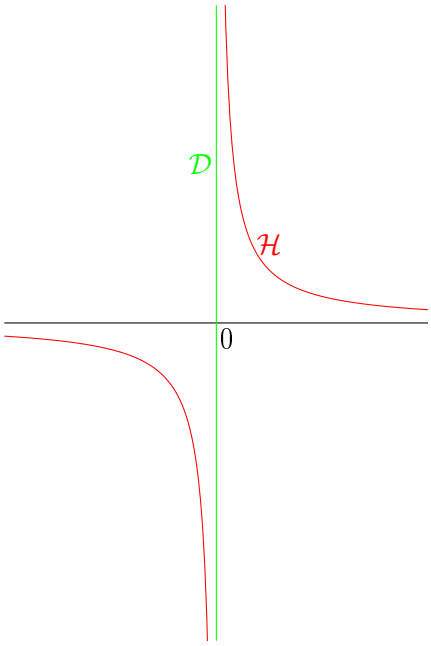
6.3. **Limites.**

a. Le théorème de Bézout est invalide si l'on se place dans le plan affine k^2.

Exemple 6.1. Considérons les courbes affines $\mathcal{H}$ et $\mathcal{D}$ définies respectivement par les polynômes $\tilde{P}(X,Y) = XY - 1$ et $\tilde{Q}(X,Y) = X$. Si le théorème de Bézout s'appliquait, ces deux courbes devraient s'intersecter en exactement deux points de k^2. Or, ces deux courbes ne s'intersectent pas puisque le système d'équations

$$\begin{cases} x = 0 \\ xy = 1 \end{cases}$$

n'admet aucune solution dans k^2 (car $0 \neq 1$).

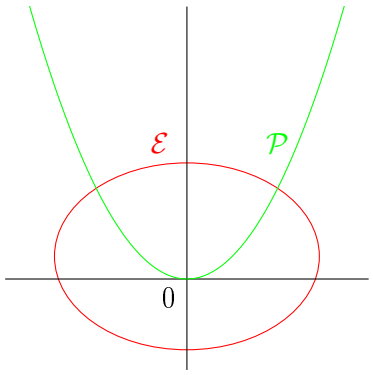


Cependant, graphiquement, ces deux courbes semblent s'intersecter "à l'infini", d'où la nécessité de se placer dans le plan projectif. Et en effet, en homogénéisant $\tilde{P}$ et $\tilde{Q}$, on trouve effectivement que les courbes projectives définies par les polynômes $P(X,Y,Z) = XY - Z^2$ et $Q(X,Y,Z) = Z$ s'intersectent en exactement deux points de $\mathbf{P}^2(k)$, à savoir celui de coordonnées $[1:0:0]$ et celui de coordonnées $[0:1:0]$.

b. Le théorème de Bézout est invalide si k n'est pas algébriquement clos.

Exemple 6.2.

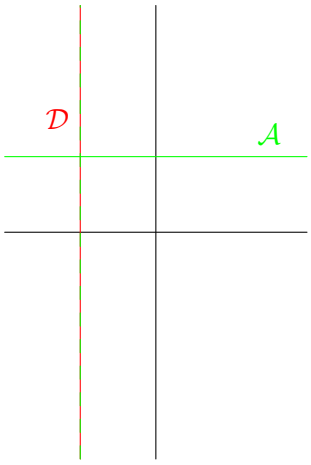
La parabole $\mathcal{P}$ décrite par le polynôme $P(X,Y) = Y - X^2$ et l'ellipse $\mathcal{E}$ décrite par le polynôme $Q(X,Y) = X^2 + 2Y^2 - Y - 2$ s'intersectent uniquement en deux points - à savoir $(1,1)$ et $(-1,1)$ - si l'on considère que P et Q sont des polynômes de $\mathbf{R}[X,Y]$.



Mais si ces polynômes sont vus comme appartenant à $\mathbf{C}[X,Y]$, on trouve deux points d'intersection supplémentaires : $(i,-1)$ et $(-i,-1)$. On trouve bien 4 points d'intersection, comme prévu par le théorème de Bézout.

c. Le théorème de Bézout ne tient plus lorsque les courbes considérées ont une composante commune.

Exemple 6.3.



Considérons les courbes affines $\mathcal{D}$ et $\mathcal{A}$ définies respectivement par $P(X,Y) = (X+1)$ et $Q(X,Y) = (X+1)(Y-1)$. Elles s'intersectent en une infinité de points non colinéaires dans le plan affine - à savoir la droite affine décrite par le polynôme $X+1$ - donc ont aussi une infinité de points d'intersection dans le plan projectif alors que si le théorème de Bézout s'appliquait il y en aurait exactement 2.

Références

1. Alain Chenciner, *Courbes algébriques planes*, Publications Mathématiques de l'Université Paris VII [Mathematical Publications of the University of Paris VII], vol. 4, Université de Paris VII, U.E.R. de Mathématiques, Paris, 1978.
2. William Fulton, *Introduction to intersection theory in algebraic geometry*, CBMS Regional Conference Series in Mathematics, vol. 54, Published for the Conference Board of the Mathematical Sciences, Washington, DC ; by the American Mathematical Society, Providence, RI, 1984.
3. _____, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.
4. C. Musili, *Algebraic geometry for beginners*, Texts and Readings in Mathematics, vol. 20, Hindustan Book Agency, New Delhi, 2001.