Géométrie algébrique

§6. Multiplicité d'intersection, théorème de Bézout

Soient C et D deux courbes algébriques affines dans $\mathbf{C}^2$ et soit $p \in \mathbf{C}^2$. On va définir la *multiplicité d'intersection* $Int_p(C \cap D)$ de C et D en p. On dit que C et D intersecte *proprement* en p si C et D n'ont aucune composante commune qui contient p. La multiplicité d'intersection est caractérisée par les propriétés suivantes :

1. $Int_p(C \cap D)$ est un entier non-négatif pour tout p, C, D tels que C et D intersectent proprement en p. $Int_p(C \cap D) = \infty$ si C et D n'intersecte pas proprement en p.

2. $Int_p(C \cap D) = 0$ si et seulement si $p \notin C \cap D$; $Int_p(C \cap D)$ ne dépend que sur les composantes de C et de D qui contient p et $Int_p(C \cap D) = 0$ si C ou D est constante.

3. $Int_p(C \cap D)$ est indépendante d'un changement affine des coordonnées : soit $T : \mathbf{C}^2 \to \mathbf{C}^2$ une telle transformation et soit C^T et D^T les images réspectives de C et de D, alors $Int_p(C \cap D) = Int_{T(p)}(C^T \cap D^T)$.

4. $Int_p(C \cap D) = Int_p(D \cap C)$.

On dit que deux courbes algébriques C et D intersectent *transversalement* en p si p est non-singulier et si les droites tangentes à C et D en p sont distinctes. On veut que la multiplicité d'intersection soit 1 lorsque deux courbes intersectent transversalement en p ; plus généralement :

5. $Int_p(C \cap D) \geq m_p(C)m_p(D)$ où $m_p(C), m_p(D)$ sont les multiplicités réspectives en p, avec égalité si et seulement si C et D n'ont aucune droite tangente commune en p.

6. Soient C_1 et C_2 définies par polynômes P_1 et P_2 et soit C définie par P_1P_2, alors

$$Int_p(C \cap D) = Int_p(C_1 \cap D) + Int_p(C_2 \cap D)\,.$$

7. Soit C irréductible définie par un polynôme P et soit D définie par Q, alors $Int_p(C \cap D)$ ne dépend que sur l'image de Q dans l'anneau des coordonnées $A(C)$:

$$Int_p(C \cap D) = Int_p(C \cap E)\,,$$

où E est définie par le polynôme $Q + RP$ pour tout $R \in \mathbf{C}[x, y]$.

Théorème 1 : Il existe un nombre unique $Int_p(C \cap D)$ vérifiant les propriétés 1-7. Il est donné par

$$Int_p(C \cap D) = \dim(\mathcal{O}_{\mathbf{C}^2,p}/I(C, D))\,,$$

où $\mathcal{O}_{\mathbf{C}^2,p}$ est l'anneau local de $\mathbf{C}^2$ en p et $I(C, D)$ est l'idéal déterminé par C et D.

On omet la preuve de ce théorème.

Exemple : On calcule $Int_p(C \cap D)$ où C est déterminée par $P = (x^2+y^2)^2 + 3x^2y - y^3$ et D est déterminé par $Q = (x^2+y^2)^3 - 4x^2y^2$ et $p = (0,0)$.

On remplace Q par $Q - (x^2+y^2)P = y[(x^2+y^2)(y^2-3x^2) - 4x^2y] = yR$, disons. Ensuite on remplace R par $R + 3P = y(5x^2 - 3y^2 + 4y^3 + 4x^2y) = yS$. Alors $Int_p(C \cap D) = 2Int_p(C \cap \{y = 0\}) + Int_p(C \cap \{S = 0\})$. Mais $Int_p(C \cap \{y = 0\}) = Int_p(\{x^4 = 0\} \cap \{y = 0\}) = 4$ par les propriétés 6 et 7 et $Int_p(C \cap \{S = 0\}) = m_p(C)m_p(\{S = 0\}) = 6$ par la propriété 5. D'où $Int_p(C \cap D) = 14$. On va recalculer ci-dessous ce nombre par une autre méthode.

La définition et le théorème s'adapte au cas des courbes projectives en supposant qu'après une transformation projective que $p \in U \cong \mathbf{C}^2$. Puis la multiplicité d'intersection est celle des courbes affines corréspondantes. Pour la propriété 7, on la remplace par

7'. Soient C et D définies par des polynômes homogènes $P(x,y,z)$ et $Q(x,y,z)$ de degrés m et n avec $n \geq m$ et soit E définie par $PR + Q$ où $R(x,y,z)$ est homogène de degré $n - m$ alors

$$Int_p(C \cap D) = Int_p(C \cap E)\,.$$

Théorème 2 (Bézout) Soient C et D deux courbes projectives dans $\mathbf{C}P^2$ de degrés m et n réspectivement qui n'ont aucune composante commune, alors elles ont exactement mn points d'intersection comptant multiplicités :

$$\sum_{p \in C \cap D} Int_p(C \cap D) = nm\,.$$

Il existe une méthode parfois plus pratique pour calculer la multiplicité d'intersection qu'on va explorer.

Soient $P(x) = a_m x^m + \cdots + a_1 x + a_0$ et $Q(x) = b_n x^n + \cdots + b_1 x + b_0$ deux polynômes de degré m et n. Alors le *résultant* $\mathcal{R}_{P,Q}$ est le déterminant de la $(m+n) \times (m+n)$-matrice :

$$\mathcal{R}_{P,Q} = \begin{vmatrix} a_0 & a_1 & \cdots & a_m & 0 & 0 & & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_m & 0 & & \cdots & 0 \\ \vdots & \vdots & & & \cdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_m \\ b_0 & b_1 & & \cdots & & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & & \cdots & & b_n & 0\ \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & \cdots & b_0 & b_1 & \cdots & & \cdots & b_n \end{vmatrix}$$

Soient $P(x,y,z) = a_m(y,z)x^m + \cdots + a_0(y,z)$ et $Q(x,y,z) = b_n(y,z)x^n + \cdots + b_0(y,z)$ deux polynômes en trois variables, alors le résultant $\mathcal{R}_{P,Q}(y,z)$ est le polynôme en y et z où on remplace a_j et b_k par $a_j(y,z)$ et $b_k(y,z)$ dans $\mathcal{R}_{P,Q}$.

On a les propriétés suivantes :

1. Soient $P(x)$ et $Q(x)$ deux polynômes en x. Alors P et Q ont un facteur non-constant commun si et seulement si $\mathcal{R}_{P,Q} = 0$ (c'est la raison d'être du résultant).
Preuve : Alors P et Q ont un facteur en commun ssi $P(x) = R(x)\varphi(x)$ et $Q(x) = R(x)\psi(x)$ ssi il existent polynômes $\varphi(x) = \alpha_{m-1}x^{m-1} + \cdots + \alpha_0$ et $\psi(x) = \beta_{n-1}x^{n-1} + \cdots + \beta_0$ de degré au plus $m-1$ et $n-1$ tels que

$$P(x)\psi(x) = Q(x)\varphi(x)\,.$$

On compare les coefficients de x^k pour $k = 0, \ldots, n-1$ pour en déduire le système d'équation linéaires :

$$\begin{array}{rcl} a_0\beta_0 & = & b_0\alpha_0 \\ a_0\beta_1 + a_1\beta_0 & = & b_1\alpha_0 + b_0\alpha_1 \\ \vdots & & \vdots \\ a_m\beta_{n-1} & = & b_n\alpha_{m-1} \end{array}$$

L'existence d'une solution non-triviale est équivalente à l'annulation de $\mathcal{R}_{P,Q}$.

2. Soient $P(x,y,z)$ et $Q(x,y,z)$ deux polynômes homogènes non-constants tels que

$$P(1,0,0) \neq 0 \neq Q(1,0,0)\,.$$

Alors P et Q ont un facteur en commun ssi le polynôme $\mathcal{R}_{P,Q}(y,z)$ est identiquement nul (il faut la condition sur $P(1,0,0)$ et $Q(1,0,0)$ afin que le degré reste le même en tant que polynômes en x avec coefficients dans $\mathbf{C}[y,z]$ qu'en tant que polynômes en x,y,z).
Preuve : C'est une conséquence du lemme précédant lorsqu'on considère P et Q comme polynômes en x avec coefficients dans $\mathbf{C}[y,z]$. Les détails sont un peu encombrant dont on les omet.

3. Si $P(x,y,z)$ et $Q(x,y,z)$ sont homogène de degré m et n réspectivement, alors le résultant $\mathcal{R}_{P,Q}(y,z)$ est homogène de degré mn en y et z.

4. Soient $P(x) = (x-\lambda_1)\cdots(x-\lambda_m)$ et $Q(x) = (x-\mu_1)\cdots(x-\mu_n)$. Alors

$$\mathcal{R}_{P,Q} = \prod_{1\leq j\leq m,\, 1\leq k\leq n} (\mu_k - \lambda_j)\,.$$

En particulier $\mathbf{R}_{P,QR} = \mathcal{R}_{P,Q}\mathcal{R}_{P,R}$. De même si P, Q et R sont polynômes en (x,y,z).

Preuve : On peut considérer P et Q comme polynômes homogène en $x, \lambda_1, \ldots, \lambda_m$ et en $x, \mu_1, \ldots, \mu_n$. En géneralisant la propriété 3, on voit que le résultant $\mathcal{R}_{P,Q}$ est homogène de degré mn en $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n$. En plus, par la propriété 1, ce polynôme s'annulle lorsque $\lambda_j = \mu_k$ pour un j et k ; il est donc divisible par

$$\prod_{1 \leq j \leq m, 1 \leq k \leq n} (\mu_k - \lambda_j) .$$

Il s'agit également d'un polynôme homogène de degré mn ; il est donc un multiple scalaire de $\mathcal{R}_{P,Q}$. On vérifie que si on pose $\mu_1 = \cdots = \mu_n = 0$ de sorte que $Q(x) = x^m$ on a

$$\prod_{j=1}^{m} (-\lambda_j)^m .$$

On en déduit la formule pour $\mathcal{R}_{P,Q}$.

Théorème 3 Soient C et D deux courbes projectives dans $\mathbf{C}P^2$, alors ils s'intersectent en au moins un points.

Preuve : Supposons C et D définies par polynômes homogènes P et Q de degrés m et n respectivement. Par la propriété 3, le résultant est un polynôme homogène de degré mn en y et z. Il s'ensuit que soit $\mathcal{R}_{P,Q}$ est identiquement nul, soit il est un produit de mn facteurs linéaires du type $bz - cy$ avec $b, c \in \mathbf{C}$ pas tous les deux nuls. Dans chaque cas il existe $(b, c) \in \mathbf{C}^2 \setminus \{0\}$ tel que $\mathcal{R}_{P,Q}$ s'annulle lorsque $y = b$ et $z = c$, d'où le résultant des deux polynômes en x : $P(x, b, c)$ et $Q(x, b, c)$ est nul et par la propriété 1, ils ont une racine commune $a \in \mathbf{C}$. Alors $P(a, b, c) = Q(a, b, c) = 0$ et $[a, b, c] \in C \cap D$. q.e.d.

Théorème 4 Si deux courbes projectives C et D dans $\mathbf{C}P^2$ de degrés m et n respectivement n'ont aucune composante commune alors elles s'intersectent en au plu mn points.

Preuve : Supposons que C et D ont au moins $mn + 1$ points d'intersection. On montre qu'elles ont une composantes commune. On choisit un ensemble S de $nm + 1$ points distincts dans $C \cap D$. Alors on peut choisir un point dans $\mathbf{C}P^2$ qui n'appartient ni à C ni à D ni aux droites dans $\mathbf{C}P^2$ passant par deux points distincts de S. En appliquant une tranformation projective on suppose que ce point est $[1, 0, 0]$. Alors C et D sont définies par des polynômes homogènes P et Q de degrés m et n tels que $P(1, 0, 0), Q(1, 0, 0) \neq 0$ (car $[1, 0, 0] \notin C \cup D$). Par la propriété 3, le résultant $\mathcal{R}_{P,Q}$ par rapport à x est un polynôme homogène de degré mn en y et z. Alors s' il n'est pas nul, il est un produit de mn facteurs linéaires du type $bz - cy$ où $(b, c) \in \mathbf{C}^2 \setminus \{0\}$.

En plus, pour $(b,c) \in \mathbf{C}^2 \setminus \{0\}$, $bz - cy$ est un facteur de $\mathcal{R}_{P,Q}(y,z)$ ssi le résultant des polynômes $P(x,b,c)$ et $Q(x,b,c)$ en x s'annulle, ce qui est le cas ssi il existe $a \in \mathbf{C}$ tel que $P(a,b,c) = Q(a,b,c) = 0$. Mais si $[a,b,c] \in S$ alors $P(a,b,c) = Q(a,b,c) = 0$ avec b et c pas tous les deux nuls (car $[1,0,0] \notin S$), d'où $bz - cy$ est un facteur de $\mathcal{R}_{P,Q}(y,z)$.

D'autre part, si $[\alpha,\beta,\gamma] \in S$ est distinct de $[a,b,c] \in S$ alors $\beta z - \gamma y$ n'est pas un multiple scalaire de $bz - cy$, sinon $[a,b,c], [\alpha,\beta,\gamma]$ et $[1,0,0]$ seront des points de la même droite définie par $bz - cy = 0$, ce qui contredit notre hypothèse sur $[1,0,0]$. Il s'ensuit que $\mathcal{R}_{P,Q}(y,z)$ possède au moins $mn+1$ facteurs linéaires distints ; il est donc identiquement nul. Par la propriété 2 il s'ensuit que C et D ont une composantes commune. q.e.d.

Corollaire : (i) Un courbe projective non-singulière C dans $\mathbf{C}P^2$ est irréductible.

(ii) Une courbe projective irréductible C dans $\mathbf{C}P^2$ possède un nombre fini de points singuliers.

Preuve : (i) Soit

$$C = \{[x,y,z] \in \mathbf{C}P^2 : P(x,y,z)Q(x,y,z) = 0\} \, ,$$

une courbe réductible dans $\mathbf{C}P^2$. Alors par Théorème 3, il existe au moins un point $[a,b,c] \in \mathbf{C}P^2$ tel que $P(a,b,c) = Q(a,b,c) = 0$. Il s'ensuit que $[a,b,c] \in C$ est singulier.

(ii) On suppose C définie par le polynôme homogène $P(x,y,z)$ de degré n. Sans perdre la généralité on peut supposer que $[1,0,0] \notin C$, d'où le coefficient $P(1,0,0)$ de x^n dans $P(x,y,z)$ n'est pas zéro. Il s'ensuit que

$$Q(x,y,z) = \frac{\partial P}{\partial x}(x,y,z) \, ,$$

est homogène non-identiquement nul de degré $n-1$, d'où il définit une courbe D dans $\mathbf{C}P^2$. Puisque C est irréductible et le degré de D est strictement inférieur de celui de C, les courbes C et D n'ont aucune composante commune. Par le théorème de Bézout C et D interesectent en au plus $n(n-1)$ points. Puisque tout point singulier de C appartient à $C \cap D$, le resultat s'ensuit. q.e.d.

Définition : Une conique est une courbe de degré deux dans $\mathbf{C}^2$ ou dans $\mathbf{C}P^2$.

Corollaire : Toute conique irréductible C dans $\mathbf{C}P^2$ s'identifie par transformation projective avec la conique:

$$x^2 = yz \, ,$$

et en particulière elle est non-singulière.

Preuve Par le corollaire précédant C possède un nombre fini de points singulier, donc par une transformation projective on peut supposer que $[0,1,0]$ est un point non-singulier dans C et que la droite tangente à C en $[0,1,0]$ est la droite $z = 0$. Il s'ensuit que C est définie par un polynôme de la forme

$$ayz + bx^2 + cxz + dz^2\,,$$

pour des nombres complexes a, b, c, d. Puisque C est irréductible, a et b sont non-nuls. La transformation projective

$$[x, y, z] \mapsto [\sqrt{b}\,x, ay + cx + dz, -z]\,,$$

applique C dans $x^2 = yz$. Puisque cette conique est non-singulière, il s'ensuit que C est non-singulière. q.e.d.

On remarque qu'il y a un homeomorphisme $\varphi : \mathbf{C}P^1 \to C$ définie par $x^2 = yz$ donnée par

$$\varphi[x, y] = [xy, y^2, x^2]\,,$$

avec application reciproque $g : C \to \mathbf{C}P^1$:

$$g[x, y, z] = [x, y] \text{ si } y \neq 0 \text{ et } [y, z] \text{ si } z \neq 0\,.$$

Il s'ensuit que toute conique irréductible dans $\mathbf{C}P^2$ est homeomorphe à $\mathbf{C}P^1$.

Théorème (Calcule de la multiplicité d'intersection) : Soient C et D définies par polynômes homogènes $P(x, y, z)$ et $Q(x, y, z)$ de degrés m et n. Supposons que C et D n'ont aucune composante commune et qu'on a choisit les coordonnées projectives de telle sorte que :

(i) $[1, 0, 0] \notin C \cup D$;

(ii) $[1, 0, 0]$ n'appartient à aucune droite joignant deux points distincts de $C \cap D$;

(iii) $[1, 0, 0]$ n'appartient à aucune droite tangente à C ou D en un point de $C \cap D$.

Alors la multiplicité d'intersection $Int_p(C \cap D)$ en un point $p = [a, b, c] \in C \cap D$ est le plus grand entier k tel que $(bz - cy)^k$ divise le résultant $\mathcal{R}_{P,Q}(y, z)$.

Exemple : On reprend l'exemple des courbes dans $\mathbf{C}^2$ ci-dessus. On projectivise :

$$\begin{aligned} P &= x^4 + 5x^2y^2 + 3x^2yz + y^4 - y^3z \\ Q &= x^6 + 3x^4y^2 + 3x^2y^4 - 4x^2y^2z^2 + y^6\,. \end{aligned}$$

On calcule la multiplicité d'intersection en $[0, 0, 1]$. Voir feuille annexe pour ce calcul.