Notes de cours sur les courbes algébriques

Olivier Collin

Introduction

En rédigeant ces notes de cours j'espère aider les étudiants à s'introduire aux courbes algébriques, en français, en ayant un minimum de bagage algébrique. Il s'agit là de la base d'un cours de 45 heures en dernière année du premier cycle. Pour l'instant l'exposition se veut minimaliste avec les principales définitions ainsi que tous les résultats démontrés en classe et le lecteur trouvera certainement qu'il manque d'exemples et d'exercices. J'espère avoir le temps de peaufiner la présentation dans une version ultérieure.

Les courbes algébriques constituent le premier chapitre de la *Géométrie algébrique*, un sujet à la fois très vaste et sophistiqué des mathématiques contemporaines. S'il est vrai que les cours de Géométrie algébrique appartiennent foncièrement aux études de cycles supérieures, il m'apparait plus qu'opportun de ne pas attendre jusque là pour développer les parties les plus élémentaires ou *classiques* et l'étude ici proposée des courbes algébriques remplit au moins trois rôles importants dans la formation de premier cycle : (1) elle donne un exemple éclatant de la puissance des techniques algébriques dans un sujet intrinsèquement géométrique au départ (2) elle donne lieu à des résultats profonds qui seront grandement généralisés dans le contexte des variétés algébriques, avec des preuves élémentaires d'une grande beauté (3) elle laisse entrevoir comment des questions en apparence intuitives sont traitées de manière satisfaisante par des méthodes à caractère abstrait.

CHAPITRE 1

Courbes algébriques : exemples et motivation

Nous introduisons dans ce chapitre les espaces dans lesquels nous travaillerons pour l'étude des courbes algébriques et donnons les premiers exemples, définissant au passage certains concepts élémentaires.

1. Plan affine, plan projectif, leurs sous-espaces... et leurs transformations

L'étude des courbes commence par définir l'espace

$$\mathbb{A}^2(\mathbb{R}) = \{(x, y) \mid x, y \in \mathbb{R}\}$$

que l'on appelera dans ce cours le *plan affine*. Les éléments de cet ensemble sont appelés des *points*. Cet ensemble est naturellement muni d'une structure d'espace vectoriel, mais contrairement à ce qui se passe en *Algèbre linéaire* nous allons nous intéresser à des sous-ensembles linéaires plus généraux que les sous-espaces. Ceci est très naturel d'un point de vue géométrique puisque une opération aussi simple que la translation dans $\mathbb{A}^2(\mathbb{R})$ par un vecteur donné n'est pas une transformation linéaire (puisque l'origine n'est pas envoyée sur elle-même). Un autre exemple simple : la droite $\mathcal{L}$ d'équation $x+y = 1$ dans $\mathbb{A}^2(\mathbb{R})$ n'est pas un sous-espace vectoriel puisque $(0, 0) \notin \mathcal{L}$. Encore plus important : il peut être intéressant de considérer plusieurs modèles du plan affine. Par exemple dans $\mathbb{R}^3$, le sous-ensemble

$$\mathcal{P} = \{(x, y, z) \mid z = 1\}$$

n'est pas un sous-espace vectoriel puisque pour $p, q \in \mathcal{P}$ le vecteur $p + q$ a pour troisième coordonnée $z = 2$. Pourtant $\mathcal{P}$ partage plusieurs propriétés avec l'espace vectoriel défini par $z = 0$ au sens où la géométrie de $\mathcal{P}$ est modelée sur celle de $\mathbb{R}^2$.

Définition 1.1. *Un sous-ensemble $A \subset \mathbb{R}^n$ est dit affine si pour tous $u, v \in A$ et $\alpha, \beta \in \mathbb{R}$ satisfaisant $\alpha + \beta = 1$ on a $\alpha u + \beta v \in A$.*

Cette définition signifie que si $u, v \in A$, alors la droite de $\mathbb{R}^n$ qui relie u à v est également dans A puisque cette droite s'exprime en équation paramétrique comme

$$\{tu + (1 - t)v \mid t \in \mathbb{R}\}.$$

Une simple induction finie permet de donner une condition encore plus générale :

$$\sum_{i=1}^{k} \alpha_i u_i \in A \text{ si } \{u_1, u_2, ..., u_k\} \subset A \text{ et } \sum_{i=1}^{k} \alpha_i = 1.$$

EXERCICE 1.2. *Si $V \subset \mathbb{R}^n$ est un sous-espace vectoriel, pour tout $u \in \mathbb{R}^n$ l'ensemble $V + u = \{v + u \mid v \in V\}$ est un sous-espace affine de $\mathbb{R}^n$.*

PROPOSITION 1.3. *Tout sous-espace affine $A \subset \mathbb{R}^n$ est de la forme $V + u$ pour un certain sous-espace vectoriel $V \subset \mathbb{R}^n$ et $u \in \mathbb{R}^n$.*

DÉMONSTRATION. Soit $a \in A$ et montrons que $V = A - a$ est sous-espace vectoriel de $\mathbb{R}^n$. On a $0 \in V$ car $a - a \in V$ par définition de V. Pour $w - a \in V$ et $\lambda \in \mathbb{R}$, on aura

$$\lambda(w - a) \in V \iff \lambda(w - a) + a \in A \iff \lambda w + (1 - \lambda)a \in A.$$

Mais cette dernière condition est vraie car A est affine. De plus si $w_1 - a \in V$ et $w_2 - a \in V$, alors $(w_1 - a + w_2) \in A$ car A affine et donc $(w_1 - a) + (w_2 - a) \in A - a$ tel que demandé. □

EXERCICE 1.4. *Soit A un sous-espace affine et $a, b \in A$. Montrez qu'en tant qu'espaces vectoriels, on a $A - a = A - b$.*

On appelle *dimension* d'un sous-espace affine A la dimension du sous-espace vectoriel associé à A.

Les applications que l'on considère entre espaces affines préservent la propriété d'affinité et sont donc appelées applications affines. On dit que $f \colon A \to B$ est *affine* si elle satisfait

$$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v)$$

pour tous $u, v \in A$ et $\lambda + \mu = 1$. On remarque que cette condition dit implicitement que les droites dans A sont envoyées sur des droites de B. Comme pour les sous-espaces affines et vectoriels, il y a un lieu essentiel entre les transformations affines et linéaires.

PROPOSITION 1.5. *Si $f \colon A \to B$ est affine et $a \in A$, alors $L_f \colon A - a \to B - f(a)$ donnée par*

$$L_f(u) = f(u + a) - f(a)$$

est linéaire.

DÉMONSTRATION. On montre en premier lieu $L_f(u+v) = L_f(u) + L_f(v)$. On a $a, u+a, v+a \in A$ par hypothèse, donc $u+v+a = (u+a)+(v+a)-a \in A$ car A affine et $1+1-1=1$. Alors

$$\begin{aligned} L_f(u+v) &= f(u+v+a) - f(a) \\ &= f((u+a)+(v+a)-a) - f(a) \\ &= f(u+a) + f(v+a) - f(a) - f(a) \\ &= f(u+a) - f(a) + f(v+a) - f(a) \\ &= L_f(u) + L_f(v). \end{aligned}$$

Similairement, on a

$$\begin{aligned} L_f(\lambda u) &= f(\lambda u + a) - f(a) \\ &= f(\lambda(u+a) + (1-\lambda)a) - f(a) \\ &= \lambda f(u+a) + (1-\lambda)f(a) - f(a) \\ &= \lambda(f(u+a) - f(a)) \\ &= \lambda L_f(u). \end{aligned}$$

□

On note en particulier que pour une application affine $f\colon \mathbb{R}^n \to \mathbb{R}^n$ on a $f = L_f + f(0)$, c'est-à-dire que f est la composition d'une application linéaire suivie d'une translation. Ceci signifie que l'étude des applications affines de $\mathbb{R}^n$ se ramène essentiellement à de l'Algèbre linéaire.

Rappelons de l'Algèbre linéaire que l'ensemble

$$GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid A \text{ inversible}\}$$

forme un groupe sous multiplication matricielle. Ce groupe agit sur $\mathbb{R}^n$ par $(A, v) \mapsto Av$, où A est vue comme une transformation linéaire. Géométriquement, $GL_n(\mathbb{R})$ a la propriété d'envoyer des sous-espaces vectoriels de $\mathbb{R}^n$ sur d'autres sous-espaces vectoriels et de préserver la *dimension* des sous-espaces.
Les transformations qui nous intéresseront sur $\mathbb{A}^2(\mathbb{R})$ sont appelées *transformations affines* ou *affinitées*, $\varphi\colon \mathbb{A}^2(\mathbb{R}) \to \mathbb{A}^2(\mathbb{R})$, données par $\varphi(v) = Av + b$ où $A \in GL_2(\mathbb{R})$ et $b \in \mathbb{A}^2(\mathbb{R})$. On vérifie facilement que sous la composition cet ensemble forme un groupe, le *groupe des*

transformations affines en dimension 2. La *Géométrie affine* peut être vue comme l'étude des propriétés d'un espace affine qui sont invariantes sous l'action du groupe des affinités. Une des propriétés qui est clairement préservée par les transformations affines est celle exprimant que des points sont sur la même droite. Inversement, puisque les transformations affines sont inversibles, la propriété de ne pas être sur une même droite est également une propriété affine. Ceci mène à une caractérisation géométrique des affinités :

Théorème fondamental des affinités : Soient $p_1, p_2, p_3 \in \mathbb{A}^2(\mathbb{R})$ trois points non-alignés et $q_1, q_2, q_3 \in \mathbb{A}^2(\mathbb{R})$ trois autres points non-alignés dans le plan affine. Alors il existe une unique transformation affine $\varphi\colon \mathbb{A}^2(\mathbb{R}) \to \mathbb{A}^2(\mathbb{R})$ telle que $\varphi(p_i) = q_i$ pour $1 \leq i \leq 3$.

Nous nous spécialisons aux cas de petite dimension $n = 2, 3$ car ils seront utilisés pour l'étude des courbes algébriques. Les sous-espaces affines de $\mathbb{A}^2(\mathbb{R})$ sont très simples : en dimension 0 ce ne sont que des points isolés, alors qu'en dimension 1 ce sont des droites du plan, données par une équation de la forme

$$ax + by + c = 0$$

où $a, b \in \mathbb{R}$ et pas tous les deux nuls. Notons qu'une telle expression n'est pas unique : pour tout $\alpha \in \mathbb{R}^*$, l'équation $\alpha ax + \alpha by + \alpha c = 0$ décrit la même droite de $\mathbb{A}^2(\mathbb{R})$.
Par ailleurs la droite $ax + by = 0$ a un lien clair avec celle d'équation $ax + by + c = 0$: elle est confondue à cette dernière si $c = 0$ ou alors elle est *parallèle* distincte. En outre la droite $ax + by = 0$ est un sous-espace vectoriel de $\mathbb{A}^2(\mathbb{R})$. Lorsque l'on étudie l'intersection de deux droites quelconques on distingue deux cas en fonction des sous-espaces vectoriels associés à ces deux droites : (1) s'ils coïncident, les deux droites sont confondues ou n'ont pas d'intersection (2) s'ils diffèrent, les droites correspondantes ont un unique point d'intersection.

Conclusion : L'intersection de droites dans $\mathbb{A}^2(\mathbb{R})$ peut être vide ou pas, ce qui est un défaut majeur de $\mathbb{A}^2(\mathbb{R})$.

Ceci nous mène à considérer un espace plus vaste pour l'étude des courbes algébriques : le *plan projectif réel*, noté $\mathbb{R}P^2$, défini par

$$\mathbb{R}P^2 = \mathbb{R}^3 - \{0\} \ / \ \mathbb{R}^*$$

où $\mathbb{R}^*$ agit sur $\mathbb{R}^3$ par multiplication scalaire : deux éléments (x, y, z) et (x', y', z') de $\mathbb{R}^3 - \{0\}$ seront équivalents dans $\mathbb{R}P^2$ si et seulement si $\exists \lambda \in \mathbb{R}^* \mid (x', y', z') = \lambda(x, y, z)$. La classe d'équivalence dans $\mathbb{R}P^2$ d'un élément $u \in \mathbb{R}^3$ sera notée par le symbole $[u]$. On a donc $[u] = [v] \iff \exists \lambda \in \mathbb{R}^* \mid u = \lambda v$.
Il est important de bien réaliser que $\mathbb{R}P^2$ est très différent de $\mathbb{R}^3$, bien qu'il provienne de ce dernier après avoir quotienté par $\mathbb{R}^*$, et un travail important de base est de savoir distinguer ce qui se passe dans $\mathbb{R}^3$ et ce qui se passe dans le quotient $\mathbb{R}P^2$.

DÉFINITION 1.6. *On appelle droite projective dans* $\mathbb{R}P^2$ *un sous-ensemble*

$$\mathcal{L} = P(V) = \{[u] \in \mathbb{R}P^2 \mid u \in V \text{ où } V \subset \mathbb{R}^3 \text{ sous-espace vectoriel de dimension } 2\}.$$

Le gain est clair lorsque l'on passe de $\mathbb{A}^2(\mathbb{R})$ à $\mathbb{R}P^2$, tel qu'illustré par la symétrie parfaite entre les énoncés des deux propositions suivantes :

PROPOSITION 1.7. *Par deux points distincts de* $\mathbb{R}P^2$ *passe une unique droite projective.*

PROPOSITION 1.8. *Deux droites projectives distinctes de* $\mathbb{R}P^2$ *s'intersectent en un unique point.*

Les deux preuves sont basées sur des notions d'Algèbre linéaire dans $\mathbb{R}^3$. Pour la première, deux points distincts de $\mathbb{R}P^2$ définissent deux sous-espaces linéairement indépendants de $\mathbb{R}^3$, L_1 et L_2, qui engendrent ensemble un unique plan V passant par l'origine. Alors $\mathcal{L} = P(V)$ est l'unique droite projective passant par les deux points.
Pour la seconde, $\mathcal{L}_1 = P(V_1)$ et $\mathcal{L}_2 = P(V_2)$ sont deux droites distinctes, donc $V_1 \neq V_2$ dans $\mathbb{R}^3$. On sait par l'Algèbre linéaire que deux sous-espaces distincts de dimension 2 s'intersectent dans $\mathbb{R}^3$ en un sous-espace de dimension 1, ce qui définit bien l'unique point d'intersection entre $\mathcal{L}_1$ et $\mathcal{L}_2$.

Sur $\mathbb{R}P^2$ on peut introduire la notion de coordonnées homogènes, analogues aux coordonnées cartésiennes du plan $\mathbb{A}^2(\mathbb{R})$, de la façon suivante. Prenons $\{v_1, v_2, v_3\}$ une base de $\mathbb{R}^3$ et écrivons tout vecteur $v \in \mathbb{R}^3 - \{0\}$ comme

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3,$$

où les λ_i sont des réels pas tous nuls. Par rapport à cette base, on peut donc écrire v en coordonnées comme $v = (\lambda_1, \lambda_2, \lambda_3)$. Le point de $\mathbb{R}P^2$ définit par v est donc $[v]$ et on lui associe ses *coordonnées homogènes* $[\lambda_1, \lambda_2, \lambda_3]$.

Une des utilités des coordonnées homogènes est de faire rapidement le lien entre $\mathbb{A}^2(\mathbb{R})$ et $\mathbb{R}P^2$ de la façon suivante. On a

$$\begin{aligned}\mathbb{R}P^2 &= \{[X,Y,Z] \mid X,Y,Z \in \mathbb{R} \text{ pas tous nuls}\} \\ &= \{[X/Z, Y/Z, 1] \mid X,Y,Z \in \mathbb{R} \text{ avec } Z \neq 0\} \cup \{[X,Y,0] \mid X,Y \in \mathbb{R} \text{ pas tous nuls}\}\end{aligned}$$

L'ensemble $\{[X/Z, Y/Z, 1] \mid X,Y,Z \in \mathbb{R} \text{ avec } Z \neq 0\}$ peut être vu comme le plan affine $\mathbb{A}^2(\mathbb{R})$ que l'on a placé dans $\mathbb{R}^3$ comme $\{(x,y,z) \in \mathbb{R}^3 \mid z = 1\}$ en posant $x = X/Z, y = Y/Z$ et $z = Z$. De plus l'ensemble $\{[X,Y,0] \mid X,Y \in \mathbb{R} \text{ pas tous nuls}\}$ définit clairement une droite projective, obtenue à partir du sous-espace $Z = 0$ de $\mathbb{R}^3$. Cette droite projective peut être exprimée plus simplement comme $\mathbb{R}P^1 = \mathbb{R}^2 - \{0\} \,/\, \mathbb{R}^*$. Ceci donne une décomposition de $\mathbb{R}P^2$ en une partie affine et une droite dite à l'infini. Il est important toutefois de bien saisir que cette décomposition n'est pas intrinsèque à $\mathbb{R}P^2$. Par exemple outre $Z = 0$, on peut facilement décomposer selon les droites projectives $Y = 0$ ou $X = 0$. En fait n'importe quelle droite projective $\mathcal{L} \subset \mathbb{R}P^2$ donne lieu à une décomposition où $\mathcal{L}$ est considérée comme la droite à l'infini.

On peut donner plusieurs interprétations du plan projectif réel. Par exemple en termes d'Algèbre linéaire, $\mathbb{R}P^2$ est l'ensemble des sous-espaces vectoriels de dimension 1 dans $\mathbb{R}^3$: $\mathbb{R}P^2 = \{L \subset \mathbb{R}^3 \mid \dim L = 1 \ , \ L \text{ sous-espace vectoriel}\}$. On peut également prendre des représentants unitaires (c'est-à-dire de longueur 1 dans $\mathbb{R}^3$) pour chaque point de $\mathbb{R}P^2$, auquel cas le plan projectif réel est vu comme la sphère unitée de $\mathbb{R}^3$ quotientée par l'action antipodale de $\{\pm 1\}$: $\mathbb{R}P^2 = S^2/\{\pm 1\}$.

La classe de transformations de $\mathbb{R}P^2$ qui nous intéresse est celle des transformations projectives, qui seront une généralisation naturelle des transformations affines rencontrées plus tôt. Une telle transformation projective $\tau \colon \mathbb{R}P^2 \to \mathbb{R}P^2$ provient d'une transformation linéaire $T \in GL_3(\mathbb{R})$ (c'est-à-dire que T est inversible) en faisant la définition suivante :

Définition 1.9. *Une application $\tau \colon \mathbb{R}P^2 \to \mathbb{R}P^2$ est appelée transformation projective si elle est donnée par $\tau([v]) = [Tv]$ pour tout $[v] \in \mathbb{R}P^2$*

On note que τ est bien définie au sens où elle ne dépend pas du représentant v choisi dans $[Tv]$: si on a $[w] = [v]$, il s'en suit que $w = \lambda v$ pour un $\lambda \in \mathbb{R}^*$ et alors

$$\tau([w]) = \tau([\lambda v]) = [T(\lambda v)] = [\lambda T v] = [Tv] = \tau([v]).$$

Etant donné la définition adoptée pour les transformations projectives de $\mathbb{R}P^2$, il est facile de voir que l'ensemble des transformations projectives forme un groupe sous la composition, isomorphe au groupe de matrices $PGL_3(\mathbb{R}) = GL_3(\mathbb{R}) \,/\, \{\lambda I \mid \lambda \in \mathbb{R}^*\}$.

En utilisant la décomposition $\mathbb{R}P^2 = \mathbb{A}^2(\mathbb{R}) \cup \mathbb{R}P^1$, où le plan affine est vu comme le plan de $\mathbb{R}^3$ satisfaisant $Z = 1$, une transformation affine $\mathbb{A}^2(\mathbb{R}) \to \mathbb{A}^2(\mathbb{R})$ doit préserver la condition $Z = 1$. Ceci signifie que pour pouvoir représenter f par une matrice A de dimensions 3×3, il faut en particulier avoir

$$A \begin{pmatrix} \star \\ \star \\ 1 \end{pmatrix} = \begin{pmatrix} \star \\ \star \\ 1 \end{pmatrix}.$$

Mais comme on sait également qu'une transformation affine satisfait $f(u) = L_f(u) + b$, la matrice A sera une matrice 3×3 ayant les blocs suivants

$$A = \begin{pmatrix} L_f & b \\ 0\,0 & 1 \end{pmatrix}.$$

Ceci donne immédiatement la caractérisation suivante des transformations affines parmi les transformations projectives

PROPOSITION 1.10. *Une transformation projective $\tau\colon \mathbb{R}P^2 \to \mathbb{R}P^2$ peut être interprétée comme une transformation affine $\iff$ τ préserve la décomposition $\mathbb{R}P^2 = \mathbb{A}^2(\mathbb{R}) \cup \mathbb{R}P^1$, c'est-à-dire que $\tau(\mathbb{R}P^1) = \mathbb{R}P^1$.*

Ce résultat indique que les transformations projectives sont beaucoup plus vastes que la classe des transformations affines. Par exemple, contrairement aux affinités, on peut trouver une infinité de transformations projectives envoyant trois points non-alignés de $\mathbb{R}P^2$ sur trois autres points non-alignés. Par contre, on a le théorème suivant pour deux ensembles de points $\{X_1, X_2, X_3, X_4\}$ et $\{Y_1, Y_2, Y_3, Y_4\}$ dits en *position générale*, c'est-à-dire que tout sous-ensemble de 3 points parmi les X_i n'est pas constitué de points alignés et même chose pour les Y_j.

Théorème fondamental de la Géométrie projective : Etant donné $\{X_1, X_2, X_3, X_4\}$ et $\{Y_1, Y_2, Y_3, Y_4\}$ en position générale, il existe une unique transformation projective $\tau\colon \mathbb{R}P^2 \to \mathbb{R}P^2$ telle que $\tau(X_i) = Y_i$ $(1 \leq i \leq 4)$.

DÉMONSTRATION. Soient $X_i = [v_i]$ et $Y_i = [w_i]$ pour $1 \leq i \leq 4$ où $v_i, w_i \in \mathbb{R}^3 - \{0\}$ $(1 \leq i \leq 4)$. Par la condition de position générale, $\{v_1, v_2, v_3\}$ forment une base de $\mathbb{R}^3$ et donc on peut exprimer $v_4 = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3$, pour certains scalaires $\lambda_i \in \mathbb{R}$ $(1 \leq i \leq 3)$. A nouveau la condition de position générale impose que *aucun* des λ_i ne peut être nul. Puisque v_i représente $\lambda_i X_i$, on aurait pu choisir dès le début des représentants tels que $v_4 = v_1 + v_2 + v_3$. De plus ces v_i $(1 \leq i \leq 3)$ sont uniques une fois que l'on fixe v_4 car $\{v_1, v_2, v_3\}$ est une base de $\mathbb{R}^3$.
Le même raisonnement s'applique à Y_1, Y_2, Y_3 et Y_4, si bien que l'on peut choisir des représentants w_i $(1 \leq i \leq 4)$ tels que $w_4 = w_1 + w_2 + w_3$. Par l'Algèbre linéaire, on sait qu'il existe une unique $T \in GL_3(\mathbb{R})$ telle que $Tv_i = w_i$ $(1 \leq i \leq 3)$. De plus on aura

$$Tv_4 = T(v_1 + v_2 + v_3) = Tv_1 + Tv_2 + Tv_3 = w_1 + w_2 + w_3 = w_4$$

donc T induit bien une transformation projective τ telle que $\tau(X_i) = Y_i$ $(1 \leq i \leq 4)$.
Pour l'unicité de τ, si on a τ' une autre telle transformation projective définie à partir de $T' \in GL_3(\mathbb{R})$, on sait par l'hypothèse que $T'v_i = \alpha_i v_i$ $(1 \leq i \leq 4)$ pour certains $\alpha_i \in \mathbb{R}$ $(1 \leq i \leq 4)$. On a ainsi

$$\alpha_4 w_4 = T'v_4 = T'(v_1 + v_2 + v_3) = T'v_1 + T'v_2 + T'v_3 = \alpha_1 w_1 + \alpha_2 w_2 + \alpha_3 w_3$$

ce qui donne

$$w_4 = \frac{\alpha_1}{\alpha_4} w_1 + \frac{\alpha_2}{\alpha_4} w_2 + \frac{\alpha_3}{\alpha_4} w_3.$$

Mais comme on avait déjà la représentation unique $w_4 = w_1 + w_2 + w_3$, on sait dès lors que l'on doit avoir $\frac{\alpha_i}{\alpha_4} = 1$ $(1 \leq i \leq 3)$. Ceci implique que $T'v_i = \alpha_4 Tv_i$ $(1 \leq i \leq 3)$ si bien que $\tau' = \tau$ tel que voulu.

□

Notons pour finir que nous pouvons abstraire un peu les constructions faites ici en changeant le corps de base sur lequel on travail, en passant de $\mathbb{R}$ à $\mathbb{C}$. Ceci donne d'une part $\mathbb{A}^2(\mathbb{C})$ le *plan affine complexe*. Cet espace est difficile à visualiser puisqu'il est de dimension réelle 4, mais nous verrons qu'à plusieurs titres il est plus naturel pour l'étude des courbes algébriques que $\mathbb{A}^2(\mathbb{R})$. D'autre part le passage de $\mathbb{R}$ à $\mathbb{C}$ dans la construction que nous avons faite du plan projectif réel $\mathbb{R}P^2$ permet de construire le *plan projectif complexe*

$$\mathbb{C}P^2 = \mathbb{C}^3 - \{0\} \ / \ \mathbb{C}^*.$$

Cet espace $\mathbb{C}P^2$ sera en quelque sorte le *nec plus ultra* pour l'étude des courbes algébriques. On a encore une décomposition $\mathbb{C}P^2 = \mathbb{A}^2(\mathbb{C}) \cup \mathbb{C}P^1$, mais elle est difficile à visualiser convenablement. Les calculs en coordonnées homogènes y sont toutefois aussi faciles que pour $\mathbb{R}P^2$. Les transformations projectives qui nous intéressent sont obtenues comme $PGL_3(\mathbb{C}) = GL_3(\mathbb{C}) \ / \ \{\lambda I \mid \lambda \in \mathbb{C}^*\}$.

2. Premiers exemples de courbes algébriques

Il y aura 4 types de courbes algébriques dans ce cours : (1) réelles affines (2) complexes affines (3) réelles projectives (4) complexes projectives. Commençons par les courbes algébriques affines en traitant les deux cas simultanément en posant $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On dit que $\mathcal{C}$ est une *courbe algébrique affine* s'il existe un polynôme $f \in \mathbb{K}[x, y]$ tel que

$$\mathcal{C} = \{(x, y) \in \mathbb{A}^2(\mathbb{K}) \mid f(x, y) = 0\}.$$

C'est donc dire qu'une courbe algébrique affine est tout simplement le lieu d'annulation d'un polynôme en deux variables défini sur $\mathbb{K}$. Une première ambiguïté doit ici être soulignée : le polynôme f définissant la courbe $\mathcal{C}$ n'est pas unique... Si on définit

$$V(f) = \{(x, y) \in \mathbb{A}^2(\mathbb{K}) \mid f(x, y) = 0\}$$

alors on a immédiatement que $V(\alpha f) = V(f)$ pour tout $\alpha \in \mathbb{K}^*$ et $V(f^k) = V(f)$ pour tout $k \in \mathbb{N}$. Lorsque $\mathbb{K} = \mathbb{C}$ on verra qu'il s'agit là de la seule ambiguïté pour une courbe algébrique affine complexe, mais voyons dès maintenant à travers un exemple que la situation est désespérée pour le cas $\mathbb{K} = \mathbb{R}$:

Dans $\mathbb{A}^2(\mathbb{R})$, l'origine (0.0) peut s'exprimer comme $V(x^2 + y^2)$, ou encore $V(x^4 + y^6)$ ou même $V(x^{12} + y^{72})$. Bref, le lien entre le lieu géométrique $(0, 0)$ et les polynômes ci-dessus est loin d'être évident. Un autre problème illustré par l'exemple ci-dessus est que certaines courbes algébriques définies sur $\mathbb{R}$ possèdent un nombre *fini* de points dans $\mathbb{A}^2(\mathbb{R})$ alors que d'autres en ont un nombre infini, comme par exemple le cercle unité du plan $\mathbb{A}^2(\mathbb{R})$, $\mathcal{C} = \{(x, y) \mid x^2 + y^2 = 1\}$. Pour ces raisons, le cas des courbes algébriques réelles sera surtout couvert pour développer une intuition géométrique autour des notions définies dans le cours - car on peut dessiner dans $\mathbb{A}^2(\mathbb{R})$! - mais la théorie sera développée essentiellement en utilisant le corps des nombres complexes.

Exercice 1.11. *Démontrez que toute courbe algébrique dans* $\mathbb{A}^2(\mathbb{C})$ *possède un nombre infini de points.*

Après les droites étudiées précédemment, les courbes algébriques les plus simples dans $\mathbb{A}^2(\mathbb{K})$ sont les *coniques*. Dans $\mathbb{A}^2(\mathbb{K})$ celles-ci sont données par une équation polynomiale de degré 2 en x et y, dont la forme générale est

$$f(x,y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

où a, b, c, d, e et f sont des scalaires dans $\mathbb{K}$, pas tous nuls pour que la courbe ait un sens. En posant $x = X/Z$ et $y = Y/Z$ et en réécrivant l'équation ci-dessus on peut considérer l'équation

$$F(X,Y,Z) = aX^2 + 2bY^2 + cY^2 + 2dXZ + 2eYZ + fZ^2 = 0$$

qui définit une *conique projective*, c'est-à-dire une courbe algébrique de degré 2 dans $\mathbb{K}P^2$. Notons au passage que la forme du polynôme $F(X,Y,Z)$ définissant une conique de $\mathbb{K}P^2$ ne peut être quelconque puisque dans cet espace on a la relation $[X,Y,Z] = [\lambda X, \lambda Y, \lambda Z]$ pour tout $\lambda \in \mathbb{K}^*$, si bien que si l'on a $F(X,Y,Z) = 0$ on doit également avoir $F(\lambda X, \lambda Y, \lambda Z) = 0$ pour tout $\lambda \in \mathbb{K}^*$. On vérifiera, par exemple, que l'équation $X^2 + YZ - X$ ne définit pas une conique projective à cause de cette restriction. Il est également important de remarquer que ceci constitue une généralisation des coniques affines, qui sont ré-obtenues comme cas particulier en posant $Z = 1$, car alors $X = x$, $Y = y$ et les équations ci-dessus deviennent identiques.

En bref, nous savons classifier toutes les coniques possibles et en fait nous avons 4 classifications, selon que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$ et selon que l'on travaille dans le plan affine ou dans le plan projectif. Pour les coniques affines, le terme important pour la classification est

$$ax^2 + 2bxy + cy^2.$$

Ceci peut être écrit de manière matricielle comme

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

On sait alors par l'Algèbre linéaire que cette matrice symétrique 2×2 est diagonalisable, ce qui correspond géométriquement à une transformation affine de $\mathbb{A}^2(\mathbb{K})$ ramenant l'équation de la conique à

$$\alpha x^2 + \beta y^2 + 2dx + 2ey + f = 0$$

où les termes d, e et f sont peut-être différents des précédents mais cela n'a aucune importance pour la classification. Sur $\mathbb{R}$ la classification dépend des cas $\alpha\beta > 0$, $\alpha\beta < 0$ ou

$\alpha\beta = 0$, où dans chaque cas on procède essentiellement à une complétion de carrés des équations pour finalement obtenir :

PROPOSITION 1.12. *A équivalence affine près dans $\mathbb{A}^2(\mathbb{R})$, l'équation générale d'une conique se réduit à :*

$$\begin{aligned}
&x^2 + y^2 = 1 && \textit{(ellipse réelle)}\\
&x^2 + y^2 = -1 && \textit{(ellipse imaginaire)}\\
&x^2 - y^2 = 1 && \textit{(hyperbole)}\\
&y = x^2 && \textit{(parabole)}\\
&x^2 = y^2 && \textit{(droites non-parallèles)}\\
&x^2 = -y^2 && \textit{(droites non-parallèles imaginaires)}\\
&x^2 = 1 && \textit{(droites parallèles)}\\
&x^2 = -1 && \textit{(droites parallèles imaginaires)}\\
&x^2 = 0 && \textit{(droites confondues)}
\end{aligned}$$

La classification sur $\mathbb{C}$ découle de ceci, à la différence près que l'utilisation de $i^2 = -1$ permet de changer des termes quadratiques du type x^2 ou xy en $-x^2$ ou $-xy$. Ceci fait, par exemple, disparaître la distinction entre les *ellipses* et les *hyperboles* lorsque l'on travaille dans $\mathbb{A}^2(\mathbb{C})$ et on obtient :

PROPOSITION 1.13. *A équivalence affine près dans $\mathbb{A}^2(\mathbb{C})$, l'équation générale d'une conique se réduit à :*

$$\begin{aligned}
&x^2 - y^2 = 1 && \textit{(conique générique)}\\
&y = x^2 && \textit{(parabole)}\\
&x^2 = y^2 && \textit{(droites non-parallèles)}\\
&x^2 = 1 && \textit{(droites parallèles)}\\
&x^2 = 0 && \textit{(droites confondues)}
\end{aligned}$$

La classification projective des coniques est encore plus simple car, rappelons-le, les transformations projectives proviennent de transformations linéaires de $\mathbb{R}^3$, ce qui est beaucoup plus vaste que les transformations affines du plan $\mathbb{A}^2(\mathbb{K})$. Une conique projective d'équation

$$aX^2 + 2bY^2 + cY^2 + 2dXZ + 2eYZ + fZ^2 = 0$$

peut s'écrire en langage matriciel comme

$$\begin{pmatrix} X & Y & Z \end{pmatrix} \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = 0.$$

En se souvenant que le groupe des transformations projectives est

$$PGL_3(\mathbb{K}) = GL_3(\mathbb{K}) \ / \ \{\lambda I \mid \lambda \in \mathbb{K}^*\}$$

on peut trouver une transformation projective pour réécrire dans la nouvelle base cette matrice 3×3 comme

$$\begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}$$

et dans ces nouvelles coordonnées la conique s'exprime comme

$$\alpha_1 X^2 + \alpha_2 Y^2 + \alpha_3 Z^2 = 0.$$

Le reste dépend du corps de base :

THÉORÈME 1.14. *La classification projective des coniques est donnée par :*

(1) *Dans $\mathbb{R}P^2$ toute conique est équivalente à une des suivantes :*

$X^2 + Y^2 + Z^2 = 0$	*(conique irréductible vide)*
$X^2 - Y^2 - Z^2 = 0$	*(conique irréductible)*
$X^2 + Y^2 = 0$	*(droites non-parallèles imaginaires)*
$X^2 - Y^2 = 0$	*(droites non-parallèles)*
$X^2 = 0$	*(droites confondues)*

(2) *Dans $\mathbb{C}P^2$ toute conique est équivalente à une des suivantes :*

$X^2 + Y^2 + Z^2 = 0$	*(conique irréductible)*
$X^2 + Y^2 = 0$	*(droites non-parallèles)*
$X^2 = 0$	*(droites confondues)*

Les coniques et leurs classifications offrent déjà la possibilité d'illustrer deux notions qui reviendront plus tard dans le cours lorsque l'on développera la théorie générale : la notion de *point singulier* et la notion de *courbe réductible*. Intuitivement une courbe sera réductible si elle peut être décomposée en une union de plusieurs courbes algébriques et les coniques réductibles sont donc celles qui sont données comme réunion de droites (réelles ou imaginaires) dans les diverses classifications ci-dessus. Par exemple dans $\mathbb{C}P^2$ la conique définie par $X^2+Y^2=0$ est également décrite comme $0=X^2+Y^2=(X+iY)(X-iY)$ et les équations $X+iY=0$ et $X-iY=0$ définissent chacune une droite projective de $\mathbb{C}P^2$. On note bien sûr que lorsque l'on a une telle décomposition, le degré total (ici 2) doit se décomposer en une somme de degrés donnant le degré total (ici $1+1$).

La notion de point singulier est obtenue en regardant les dérivées partielles du polynôme définissant la courbe algébrique. Dans $\mathbb{A}^2(\mathbb{K})$ une courbe définie par $f(x,y)=0$ aura comme point singulier $P\in\mathbb{A}^2(\mathbb{K})$ si l'on a

$$\frac{\partial f}{\partial x}(P)=\frac{\partial F}{\partial y}(P)=0.$$

Pour une courbe de $\mathbb{K}P^2$ donnée par $F(X,Y,Z)=0$ la condition implique plutôt trois dérivées partielles

$$\frac{\partial F}{\partial X}(P)=\frac{\partial F}{\partial Y}(P)=\frac{\partial F}{\partial Z}(P)=0.$$

Nous ne ferons une étude systématique des points singuliers pour l'instant, mais observons qu'il peut y avoir un lien entre la notion de réductibilité et celle de point singulier de courbes algébriques à partir de notre exemple des coniques dans $\mathbb{C}P^2$. En effet pour une conique réductible $F(X,Y,Z)=0$ se décompose en $G(X,Y,Z)\cdot H(X,Y,Z)=0$ où G et H sont des polynômes de degré 1. Puisque $G(X,Y,Z)=0$ et $H(X,Y,Z)=0$ définissent des droites projectives, on sait que dans $\mathbb{C}P^2$ leur intersection sera non-vide. Soit donc $P\in\{G(X,Y,Z)=0\}\cap\{H(X,Y,Z)=0\}$. Par la règle de dérivation d'un polynôme produit, on a

$$\begin{aligned}\frac{\partial F}{\partial X}(P) &= \frac{\partial G}{\partial X}(P)H(P) + G(P)\frac{\partial H}{\partial X}(P) = 0\\ \frac{\partial F}{\partial Y}(P) &= \frac{\partial G}{\partial Y}(P)H(P) + G(P)\frac{\partial H}{\partial Y}(P) = 0\\ \frac{\partial F}{\partial Z}(P) &= \frac{\partial G}{\partial Z}(P)H(P) + G(P)\frac{\partial H}{\partial Z}(P) = 0\end{aligned}$$

où chaque ligne est égale à 0 car P satisfait $G(P) = 0$ et $H(P) = 0$. On en conclut que P est un point singulier de la conique réductible. Ce qui est plus surprenant à priori c'est que la réciproque est vraie : si une courbe conique possède des points singuliers, alors elle est réductible ! En effet, l'équation de la conique est

$$F(X, Y, Z) = aX^2 + 2bY^2 + cY^2 + 2dXZ + 2eYZ + fZ^2 = 0$$

et le calcul pour les points singuliers donne

$$\begin{aligned}\frac{\partial F}{\partial X}(P) &= 2aX + 2bY + 2dZ\\ \frac{\partial F}{\partial Y}(P) &= 2bX + 2cY + 2eZ\\ \frac{\partial F}{\partial Z}(P) &= 2dX + 2eY + 2fZ\end{aligned}$$

Ceci peut s'exprimer sous forme matricielle par

$$\begin{pmatrix}\frac{\partial F}{\partial X}(P)\\ \frac{\partial F}{\partial Y}(P)\\ \frac{\partial F}{\partial Z}(P)\end{pmatrix} = 2 \cdot \begin{pmatrix}a & b & d\\ b & c & e\\ d & e & f\end{pmatrix}\begin{pmatrix}X\\ Y\\ Z\end{pmatrix}.$$

La recherche d'un point singulier dans $\mathbb{C}P^2$ revient donc à trouver des solutions à ce système linéaire dans $\mathbb{R}^3$ puis à prendre les classes d'équivalence projective correspondantes. Or on sait par l'Algèbre linéaire qu'un tel système possède une solution $\iff \det A = 0$, où A désigne la matrice 3×3 ci-dessus. Puisque la condition $\det A = 0$ n'est pas affectée par un changement de base, on peut donc simplement se reporter au Théorème de classification des coniques dans $\mathbb{C}P^2$ et vérifier dans quels cas a-t-on $\det A = 0$. On constate que cela se produit exactement lorsque la conique est réductible.

Il est à noter que la définition de point singulier par l'annulation des dérivées partielles semble supposer que si les dérivées partielles de F sont nulles en $P \in \mathbb{C}P^2$, alors forcément $F(P) = 0$ (c'est-à-dire que P est *sur* la courbe). Ceci n'est point évident mais découle des faits suivants d'Algèbre des polynômes. D'une part pour une courbe algébrique de $\mathbb{C}P^2$ donnée par un polynôme de degré k, ce polynôme $F(X, Y, Z)$ satisfait la *relation d'homogénéité*

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^k F(X, Y, Z)$$

pour tout $\lambda \in \mathbb{C}^*$. Ensuite pour de tels polynômes dits *homogènes de degré k* on a la

Formule d'Euler : $k \cdot F(X, Y, Z) = \frac{\partial F}{\partial X}(X, Y, Z) \cdot X + \frac{\partial F}{\partial Y}(X, Y, Z) \cdot Y + \frac{\partial F}{\partial Z}(X, Y, Z) \cdot Z.$

Il s'en suit que lorsque le point est singulier, toutes ses dérivées partielles sont nulles et ainsi la formule d'Euler dit que le point est sur la courbe $F(X, Y, Z) = 0$.

Un objet qui sera particulièrement important dans ce cours est la *droite tangente* à une courbe algébrique. Etant donné une courbe projective donnée par $F(X, Y, Z) = 0$ homogène, au voisinage d'un point $[a, b, c] \in \mathbb{K}P^2$, on peut écrire

$$F(X,Y,Z) = F(a,b,c)+(X-a)\frac{\partial F}{\partial X}(a,b,c)+(Y-b)\frac{\partial F}{\partial Y}(a,b,c)+(Z-c)\frac{\partial F}{\partial Z}(a,b,c)+R(X,Y,Z)$$

où $\deg R \geq 2$. Ceci n'est rien d'autre que la formule de Taylor rencontrée en Calcul différentiel (valable pour les polynômes) mais l'équation peut également être dérivée algébriquement en utilisant la notion de dérivée formelle des polynômes en plusieurs variables. Puisque $[a, b, c]$ est sur la courbe on a $F(a, b, c) = 0$, l'approximation linéaire autour du point $[a, b, c]$ est donnée par

$$(X - a)\frac{\partial F}{\partial X}(a, b, c) + (Y - b)\frac{\partial F}{\partial Y}(a, b, c) + (Z - c)\frac{\partial F}{\partial Z}(a, b, c) = 0$$

mais la formule d'Euler permet de simplifier ceci à

$$\frac{\partial F}{\partial X}(a, b, c)\ X + \frac{\partial F}{\partial Y}(a, b, c)\ Y + \frac{\partial F}{\partial Z}(a, b, c)\ Z = 0,$$

ce qui est appelé *équation de la droite projective tangente* à la courbe en $[a, b, c]$. Il est à noter que cette équation n'a de sens que lorsqu'au moins une des trois dérivées est non-nulle en $[a, b, c]$, auquel cas on dit que $[a, b, c]$ est un *point régulier* de la courbe $\mathcal{C}$.

Dans le cas d'une courbe affine $\mathcal{C}$ donnée par $f(x,y)=0$, où f est un polynôme de degré n, la formule de Taylor en 2 variables donne plutôt comme équation de la tangente à la courbe en un point régulier (a,b)

$$\frac{\partial f}{\partial x}(a,b)(x-a)+\frac{\partial f}{\partial y}(a,b)(y-b)=0.$$

Il sera intéressant de donner une autre interprétation de la tangente en un point d'une courbe, vue parmi toutes les droites du plan affine passant par ce point (a,b). Pour cela, considérons l'équation générale d'une droite affine passant par (a,b) :

$$L=\{x=a+\alpha t\ ,\ y=b+\beta t \mid \alpha,\beta\in\mathbb{K} \text{ fixes},\ t\in\mathbb{K} \text{ variable}\}.$$

Définissons les termes

$$T_k(\alpha,\beta)=\sum_{i=0}^{k}\binom{k}{i}\frac{\partial^k f}{\partial x^{k-i}\,\partial y^i}(a,b)\ \alpha^{k-i}\beta^i.$$

La formule de Taylor peut être interprétée comme

$$f(a+\alpha t,b+\beta t)=f(a,b)+T_1(\alpha,\beta)\ t+\frac{1}{2!}T_2(\alpha,\beta)\ t^2+...+\frac{1}{n!}T_n(\alpha,\beta)\ t^n+r(t).$$

La partie polynomiale obtenue à partir de f ne dépend que d'une variable, appelons le polynôme $h(t)$. La première observation évidente est que, comme $f(a,b)=0$ et $(a,b)\in L$, on a que $t=0$ est racine de $h(t)$. Si la droite L n'est pas confondue avec la courbe $\mathcal{C}$, le polynôme $h(t)$ sera *non-nul*. Si l'on suppose que le point (a,b) n'est pas singulier, les valeurs α et β pour lesquelles $T_1(\alpha,\beta)=0$ correspondent à

$$\frac{\partial f}{\partial x}(a,b)\ \alpha+\frac{\partial f}{\partial y}(a,b)\ \beta=0$$

ce qui est exactement la droite tangente à $\mathcal{C}$ en (a,b). Pour ces valeurs précises de α et β, on a que $t=0$ est *au moins* racine double de $h(t)$. Si $T_2(\alpha,\beta)=0$, la racine $t=0$ est au moins racine *triple* de $h(t)$ et on pose :

DÉFINITION 1.15. *$(a,b)\in\mathcal{C}$ dont la tangente donnée par $T_1(\alpha,\beta)=0$ satisfait également $T_2(\alpha,\beta)=0$ est appelé un point d'inflexion de $\mathcal{C}$.*

Nous verrons plus tard qu'il y a peu de points d'inflexions sur une courbe algébrique donnée dès que la courbe est de degré au moins 3, mais que ceux-ci existent néanmoins *toujours*. On peut également montrer que la notion est préservée sous transformations affines. Finalement on peut généraliser le concept aux courbes projectives et montrer que le résultat est invariant sous transformations projectives. Pour ces courbes projectives, donnons une

caractérisation utile de ces points d'inflexion, appelée *caractérisation Hessienne*. Pour simplifier les notations, on prendra des coordonnées $[X_1, X_2, X_3]$ sur $\mathbb{K}P^2$ et autour d'une point $P \in \mathbb{K}P^2$ sur une courbe $\mathcal{C}$ donnée par $F(X_1, X_2, X_3) = 0$ on écrit le développement de Taylor comme

$$F(X_1, X_2, X_3) = F(P) + \sum_{i=1}^{3} F_i(P)X_i + \sum_{i,j=1}^{3} F_{ij}(P)X_iX_j + R(X_1, X_2, X_3)$$

où on utilise la notation $F_i = \frac{\partial F}{\partial X_i}$ et $F_{ij} = \frac{\partial^2 F}{\partial X_i \partial X_j}$. Pour la suite il sera plus parlant d'utiliser les notations F_X, F_Y, F_Z ainsi que $F_{XX}, F_{XY}, F_{XZ}, F_{YZ}, F_{ZZ}$ pour ces dérivées. On suppose que P est un point régulier de la courbe (c'est-à-dire non-singulier), auquel cas $F(P) = 0$ et le second terme du membre droit de l'équation donne la tangente à la courbe en P. Le terme d'ordre 2 peut s'écrire comme

$$\begin{pmatrix} X & Y & Z \end{pmatrix} \begin{pmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

On appelle la matrice 3×3 ci-dessus la matrice Hessienne H_F de F en P.

DÉFINITION 1.16. *On appelle déterminant Hessien de F en P la quantité $\mathcal{H}_F(P) = \det H_F$.*

On montre facilement (Exercice) que la condition $\mathcal{H}_F(P) = 0$ est préservée par une transformation projective quelconque : si $\varphi \colon \mathbb{K}P^2 \to \mathbb{K}P^2$ est transformation projective, $G = F \circ \varphi$ et $Q = \varphi^{-1}(P)$, alors $\mathcal{H}_F(P) = 0 \iff \mathcal{H}_G(Q) = 0$.

PROPOSITION 1.17. *Un point régulier $P \in \mathcal{C}$ est un point d'inflexion $\iff \mathcal{H}_F(P) = 0$.*

DÉMONSTRATION. On peut utiliser une transformation projective pour se ramener au cas où : (1) $P = [0, 0, 1]$ (2) la tangente à $\mathcal{C}$ en P est d'équation $Y = 0$. Le polynôme de degré k définissant $\mathcal{C}$ est de la forme

$$F(X, Y, Z) = \lambda Y Z^{k-1} + (aX^2 + 2bXY + cY^2)Z^{k-2} + ...$$

Par hypothèse $\lambda \neq 0$ et l'intersection de $F = 0$ et la tangente $Y = 0$ en P correspond alors à la racine $[0, 1]$ de $F(X, 0, Z) = aX^2Z^{k-2} + ...$ et pour que P soit un point d'inflexion il est donc nécessaire et suffisant que la condition $a = 0$ soit vérifiée. On calcule alors le

Hessien de F en P comme

$$\mathcal{H}_F([0,0,1]) = \begin{vmatrix} 2a & 2b & 0 \\ 2b & 2c & \lambda(k-1) \\ 0 & \lambda(k-1) & 0 \end{vmatrix} = -2a\lambda^2(k-1)^2.$$

Si $k-1=0$ alors on a une droite et tous ses points seront forcément des points d'inflexion. Autrement, on a bien $a=0$ comme voulu. □

LEMME 1.18. *Si l'on a $d = \deg F > 1$, alors la relation suivante est satisfaite :*

$$Z^2 \cdot \mathcal{H}_F(X,Y,Z) = (d-1)^2 \begin{vmatrix} F_{XX} & F_{XY} & F_X \\ F_{YX} & F_{YY} & F_Y \\ F_X & F_Y & \frac{d}{d-1}F \end{vmatrix}$$

DÉMONSTRATION. Par la formule d'Euler, on a

$$d\ F(X,Y,Z) = XF_X(X,Y,Z) + YF_Y(X,Y,Z) + ZF_Z(X,Y,Z)$$

ainsi que les trois équations suivantes

$$\begin{aligned} (d-1)\ F_X &= XF_{XX} + YF_{YX} + ZF_{ZX} \\ (d-1)\ F_Y &= XF_{XY} + YF_{YY} + ZF_{ZY} \\ (d-1)\ F_Z &= XF_{XZ} + YF_{YZ} + ZF_{ZZ} \end{aligned}$$

En utilisant ces trois dernières relations, par une opération sur les lignes de $\mathcal{H}_F$ on obtient

$$Z \cdot \mathcal{H}_F(X,Y,Z) = (d-1) \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_X & F_Y & F_Z \end{vmatrix}$$

A partir de ceci, une opération sur les colonnes et l'identité d'Euler donnent le résultat. □

Une application de ces idées est obtenue lorsque l'on considère les courbes algébriques de degré 3. On appelle ces courbes des *cubiques* et leur étude remonte à Newton qui avait étudié le problème de leur classification. Pour conclure cette section donnant les premiers exemples de courbes algébriques, nous donnons quelques généralités sur les cubiques.

Commençons par quelques exemples. La *cubique nodale* de Newton $\mathcal{C}$ est donnée par l'équation affine

$$y^2 = x^2(x+1).$$

On peut en donner un croquis approximatif dans $\mathbb{A}^2(\mathbb{R})$ en considérant l'intersection avec les droites $x = k$ constante et on a :
- pour $k < -1$ aucune point du plan ne satisfait l'équation
- pour $k = -1$ on a le point $(-1, 0)$
- pour $0 < k < -1$ on a deux points $(k, \pm\sqrt{k^2(k+1)})$
- pour $k = 0$ on a le point $(0, 0)$
- pour $k > 0$ à nouveau deux points $(k, \pm\sqrt{k(k+1)})$

Notons que le point $(0, 0)$ est une point singulier de la cubique de Newton puisque les deux dérivées partielles y sont nulles. On utilise ce point singulier pour construire une paramétrisation de la cubique de la façon suivante : en posant $y = tx$, le polynôme définissant la cubique devient

$$t^2x^2 = x^2(x + 1).$$

Pour toute valeur $x \neq 0$ on peut écrire $x = t^2 - 1$ et donc $y = t^3 - t$. Ceci permet de décrire la cubique de Newton partout sauf en $(0, 0)$ par $\varphi\colon \mathbb{R} \to \mathcal{C}$ où

$$\varphi(t) = (t^2 - 1, t^3 - t).$$

La cubique admettant une telle paramétrisation partout sauf en un nombre fini de points en termes de fonctions rationnelles de t (dans ce cas-ci même des fonctions polynomiales !) on dit que la cubique de Newton est une *courbe rationnelle*.

Un autre exemple élémentaire est donné par la *cubique de Neil* dont la paramétrisation rationnelle est $\varphi(t) = (t^2, t^3)$. Ceci représente une courbe algébrique d'équation polynômiale $x^3 - y^2 = 0$ et à nouveau $(0, 0)$ est point singulier de la courbe. Essayons de voir la cubique de Neil dans une famille de *déformations* en considérant

$$\mathcal{C}_\epsilon = \{(x, y) \mid y^2 = x^2(x + \epsilon)\}.$$

Lorsque $\epsilon = 0$ on a bien la cubique de Neil, lorsque $\epsilon > 0$ on tombe sur une cubique ayant le même type que la cubique de Newton, alors que lorsque $\epsilon < 0$ on voit que pour $x < 0$ et $0 < x < -\epsilon$ on n'a aucun point sur $\mathcal{C}_\epsilon$ si bien que la cubique n'est pas connexe dans $\mathbb{A}^2(\mathbb{R})$.

Après ces quelques exemples, nous nous intéressons au problème de classification des cubiques dans $\mathbb{C}P^2$. Premièrement il y a les cubiques réductibles, dont le polynôme se réduit à un produit de polynômes de degrés 1 et 2 ou de degrés 1, 1 et 1. Dans chaque cas, cela nous ramène à étudier les coniques et/ou les droites, donc nous considérons ces cas

bien compris. Ensuite on peut se demander quelles sont les cubiques non-singulières. Nous avons le

LEMME 1.19. *Si $\mathcal{C}$ est une cubique non-singulière elle est forcément irréductible.*

DÉMONSTRATION. On montre la contraposée : si $\mathcal{C}$ est réductible, alors elle possède au moins un point singulier. Soit donc $F(X,Y,Z) = G(X,Y,Z) \cdot H(X,Y,Z)$ avec, disons, $\deg G = 2$ et $\deg H = 1$. On a par conséquent

$$\begin{aligned}\frac{\partial F}{\partial X} &= \frac{\partial G}{\partial X}\, H + G\, \frac{\partial H}{\partial X}\\ \frac{\partial F}{\partial Y} &= \frac{\partial G}{\partial Y}\, H + G\, \frac{\partial H}{\partial Y}\\ \frac{\partial F}{\partial Z} &= \frac{\partial G}{\partial Z}\, H + G\, \frac{\partial H}{\partial Z}\end{aligned}$$

Ainsi tout point dans l'intersection

$$\{[X,Y,Z] \in \mathbb{C}P^2 \mid G(X,Y,Z) = 0\} \cap \{[X,Y,Z] \in \mathbb{C}P^2 \mid H(X,Y,Z) = 0\}.$$

Il reste ainsi à montrer qu'une telle intersection est toujours non-vide. Ceci découle du fait que $\deg H = 1$, donc on peut isoler une des variables X, Y ou Z en fonction des deux autres, si bien que l'intersection est décrite par un polynôme *homogène* en deux variables. Une application du Théorème fondamental de l'Algèbre donne le résultat. □

LEMME 1.20. *Toute cubique non-singulière non-singulière possède un point d'inflexion.*

Nous n'avons pas encore l'outil requis (le résultant de polynômes) pour la preuve de ce lemme, donc nous l'acceptons sans preuve pour l'instant. Mais le résultat est important car il nous permet la classification des cubiques non-singulières : il n'existe en fait qu'une unique cubique non-singulière à transformation projective près :

THÉORÈME 1.21. *Soit $\mathcal{C}$ une cubique non-singulière de $\mathbb{C}P^2$. Par une transformation projective, on peut ramener l'équation de $\mathcal{C}$ à la forme canonique*

$$Y^2Z = X(X-Z)(X-\lambda Z).$$

DÉMONSTRATION. Par le lemme précédent, on sait que la cubique $\mathcal{C}$ possède au moins un point d'inflexion. Par une transformation projective, on peut supposer qu'il s'agit du

point $[0,1,0]$ et que la tangente à $\mathcal{C}$ en ce point est donnée par l'équation $Z=0$. Alors la cubique $\mathcal{C}$ est donnée par un polynôme $F(X,Y,Z)$ homogène de degré 3 satisfaisant

$$F(0,1,0)=\frac{\partial F}{\partial X}(0,1,0)=\frac{\partial F}{\partial Y}(0,1,0)=\mathcal{H}_F(0,1,0)=0.$$

En effet le premier terme est nul car $[0,1,0]\in\mathcal{C}$, les deux suivants le sont également par l'hypothèse sur la tangente en $[0,1,0]$, alors que $\mathcal{H}_F(0,1,0)=0$ puisque $[0,1,0]$ est point d'inflexion de $\mathcal{C}$. Puisque $\mathcal{C}$ est non-singulière, on doit avoir

$$\frac{\partial F}{\partial Z}(0,1,0)\neq 0.$$

Par le Lemme 1.18 et selon une écriture légèrement différente, on a

$$Y^2\cdot\mathcal{H}_F(X,Y,Z)=4\begin{vmatrix} F_{XX} & F_X & F_{XZ}\\ F_X & \frac{3}{2}F & F_Z\\ F_{ZX} & F_Z & F_{ZZ}\end{vmatrix}$$

évaluée au point $[0,1,0]$ on obtient

$$0=\mathcal{H}_F(0,1,0)=4\begin{vmatrix} F_{XX} & 0 & F_{XZ}\\ 0 & 0 & F_Z\\ F_{ZX} & F_Z & F_{ZZ}\end{vmatrix}=-4(F_Z(0,1,0))^2F_{XX}(0,1,0).$$

On en déduit que l'on doit avoir $F_{XX}(0,1,0)=0$ puisque l'on sait que $F_Z(0,1,0)\neq 0$. Cette condition sur F_{XX} garantit que F n'a pas de terme de la forme YX^2 et ceci nous permet d'écrire

$$F(X,Y,Z)=YZ(\alpha X+\beta Y+\gamma Z)+\phi(X,Z).$$

Mais ceci implique que l'on a $\beta=\frac{\partial F}{\partial Z}(0,1,0)\neq 0$.

Ce qui précède nous permet de définir une transformation projective $\mathbb{C}P^2\to\mathbb{C}P^2$ par

$$[X,Y,Z]\mapsto[X,Y+\frac{\alpha X+\gamma Z}{2\beta},Z]$$

pour laquelle l'équation de $\mathcal{C}$ devient

$$\begin{aligned}0&=(Y-\frac{\alpha X+\gamma Z}{2\beta})\ Z\ (\alpha X+\beta(Y-\frac{\alpha X+\gamma Z}{2\beta})+\gamma Z)+\phi(X,Z)\\ &=(Y-\frac{\alpha X+\gamma Z}{2\beta})\ Z\ (\beta Y+\frac{\alpha X+\gamma Z}{2})+\phi(X,Z).\end{aligned}$$

En développant cette dernière expression, on constate que l'on a une équation de la forme

$$\beta Y^2 Z + \psi(X, Z) = 0$$

pour un certain polynôme homogène de degré 3 $\psi(X, Z)$. Par le Théorème Fondamental de l'Algèbre, on sait que ce polynôme homogène est produit de trois facteurs linéaires et qu'en outre le coefficient de X^3 est non-nul : autrement $\psi(X, Z)$ serait divisible par Z et ainsi $\mathcal{C}$ serait réductible, contredisant l'hypothèse voulant que $\mathcal{C}$ soit non-singulière en vertu du Lemme 1.19. Il s'en suit qu'après une autre transformation projective on peut écrire l'équation de la cubique $\mathcal{C}$ sous la forme

$$Y^2 Z = (X - aZ)(X - bZ)(X - cZ)$$

où $a, b, c \in \mathbb{C}$ doivent être distincts pour que $\mathcal{C}$ n'ait pas de points singulier, comme le montre un calcul simple. Une autre transformation projective permet d'obtenir la forme $Y^2 Z = X(X - Z)(X - \lambda Z)$, où $\lambda \neq 0, 1$, tel que voulu. □

La classification projective des cubiques peut être complétée en considérant le cas des cubiques ayant des points singuliers. Dans ce cas il faut distinguer les cas où F est réductible ou irréductible.

Si F est réductible, il s'écrit sous la forme $F = G \cdot H$ avec $\deg G = 2$ et $\deg H = 1$, ce qui signifie que la conique est réunion d'une conique (donnée par $G(X, Y, Z) = 0$) et d'une droite projective d'équation $H(X, Y, Z) = 0$. On applique ensuite la classification des coniques à G pour obtenir tous les cas possibles.

Le cas où F est irréductible mais possède un point singulier requiert des outils que nous n'avons pas encore développés dans le cours (tangentes multiple à une courbe en un point singulier, multiplicité d'intersection) mais en bref voici les deux uniques types projectifs dans ce cas (Voir le chapitre 15 de [**Gib**] pour les détails) :

$$X^3 + Y^3 - XYZ = 0 \qquad \text{(cubique nodale)}$$
$$Y^2 Z = X^3 \qquad \text{(cubique cuspidale).}$$

CHAPITRE 2

Interlude d'Algèbre

Nous faisons ici un bref survol des propriétés des anneaux $\mathbb{K}[X]$ et $\mathbb{K}[X_1, X_2, ..., X_n]$ dont nous aurons besoin pour systématiser notre étude des courbes algébriques. Pour plus de détails, on pourra consulter les ouvrages classiques de Lang [**Lan**] ou de van der Waerden [**vdW**].

1. Décomposition de polynômes

On a vu a Chapitre 1 des exemples suggérant qu'il y a probablement un lien entre la décomposition des courbes algébriques en *composantes* et la décomposition de polynômes, du moins lorsque l'on travaille sur $\mathbb{C}$. Ces exemples ne sont pas le fruit du hasard et nous verrons plus tard toute l'importance pour l'étude de la géométrie des courbes algébriques qu'il y a à étudier la divisibilité des polynômes. On sait déjà par l'Algèbre élémentaire que la décomposition polynômiale dépend du corps de base : un polynôme peut être factorisable dans $\mathbb{C}[X]$ sans l'être dans $\mathbb{R}[X]$. Par exemple le polynôme à coefficients réels $X^2 + 1$ se factorise comme $(X - i)(X + i)$ dans $\mathbb{C}[X]$ alors qu'il ne se factorise pas en deux polynômes de degré 1.

La propriété de base la plus importante de $\mathbb{K}[X]$ est qu'il satisfait l'algorithme de division euclidienne :

THÉORÈME 2.1. *Etant donné deux polynômes $f, g \in \mathbb{K}[X]$, il existe des polynômes $q, r \in \mathbb{K}[X]$ uniquement déterminés tels que l'on ait $f = q \cdot g + r$ avec $\deg r < \deg g$.*

DÉMONSTRATION. On écrit $f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$ ainsi que $g(X) = b_k X^k + b_{k-1} X^{k-1} + ... + b_0$ où $n = \deg f$ et $k = \deg g$ et on procède par induction complète sur n. Si $n = 0$ le résultat est clairement vrai. Supposons le résultat vrai pour tout polynôme de degré inférieur à n. On peut supposer que $\deg g \leq \deg f$ (autrement on conclut la preuve en posant $q = 0$ et $r = f$). On peut alors écrire $f(X) = a_n b_k^{-1} X^{n-k} g(X) + f_1(X)$ où

$\deg f_1 < n$. Par l'hypothèse d'induction on sait trouver q_1 et r tels que

$$f(X) = a_n b_k^{-1} X^{n-k} g(X) + q_1(X)g(X) + r(X)$$

avec $\deg r < \deg g$. On pose $q(X) = a_n b_k^{-1} X^{n-k} + q_1(X)$ pour conclure la preuve de l'existance de q et r tel que voulus. Pour l'unicité, supposons que l'on ait $q_1 g + r_1 = f = q_2 g + r_2$, avec $\deg r_1 < \deg g$ et $\deg r_2 < \deg g$. Ceci implique que

$$(q_1 - q_2) \cdot g = r_2 - r_1.$$

Mais alors puisque $\deg(q_1 - q_2) \cdot g = \deg(q_1 - q_2) + \deg g$ et que par hypothèse $\deg(r_1 - r_2) < \deg g$ on doit forcément avoir $q_1 - q_2 = 0$ et cette condition implique également $r_1 = r_2$ tel que voulu. □

PROPOSITION 2.2. *Si $\mathbb{K}$ est un corps quelconque, l'anneau $\mathbb{K}[X]$ est intègre : $f \cdot g = 0(X) \Rightarrow f = 0(X)$ ou $g = 0(X)$.*

DÉMONSTRATION. Ceci découle essentiellement du fait que $\mathbb{K}$ est un anneau intègre : supposons que $f, g \neq 0(X)$ de degré n et m avec terme de plus haut degré $a_n \neq 0$ et $b_m \neq 0$ respectivement. Alors dans $\mathbb{K}$ on a $a_n b_m \neq 0$ et $a_n b_m X^{n+m}$ est l'unique terme de degré $m + n$ de $f \cdot g$, si bien que l'on a $f \cdot g \neq 0(X)$ tel que voulu.

□

COROLLAIRE 2.3. *Si $\mathbb{K}$ est un corps quelconque, l'anneau $\mathbb{K}[X]$ est euclidien.*

DÉMONSTRATION. En effet $\mathbb{K}[X]$ est intègre et satisfait l'algorithme de division euclidienne. □

COROLLAIRE 2.4. *Si $\mathbb{K}$ est un corps quelconque, l'anneau $\mathbb{K}[X]$ est principal.*

DÉMONSTRATION. En effet l'anneau $\mathbb{K}[X]$ est intègre par la proposition précédente et en utilisant l'algorithme de division euclidienne dans $\mathbb{K}[X]$ tout idéal sera principal : en prenant un élément de degré minimal a dans un idéal $A \subset \mathbb{K}[X]$, on aura pour tout $f \in A$ que $f = q \cdot a + r$ et donc A est engendré par a.

□

Une des conséquences importantes de l'algorithme d'Euclide dans $\mathbb{K}[X]$ est la proposition suivante dont la preuve est facile :

PROPOSITION 2.5. *Soit $\alpha \in \mathbb{K}$ une racine de $f \in \mathbb{K}[X]$. Alors $X - \alpha$ est un facteur du polynôme f : $f = (X - \alpha) \cdot q(X)$, où $\deg q = \deg f - 1$.*

PROPOSITION 2.6. *Si $f \in \mathbb{K}[X]$ est de degré n, ce polynôme possède au plus n racines distinctes dans $\mathbb{K}$.*

DÉMONSTRATION. Soient $\alpha_1, \alpha_2, ..., \alpha_n$ racines distinctes de f. Alors par le résultat précédent, on a $f(X) = (X - \alpha_1) \cdot g(X)$. Comme α_2 est racine de f, on a également $0 = f(\alpha_2) = (\alpha_2 - \alpha_1) \cdot g(\alpha_2)$ si bien que α_2 est racine de $g(X)$ puisque $\alpha_2 \neq \alpha_1$ par hypothèse. Ceci permet d'écrire

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdot h(X).$$

En répétant le processus jusqu'à α_n, on obtient $f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$ et dnc f ne peut avoir plus que n racines. □

COROLLAIRE 2.7. *Si un polynôme $f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$ possède au moins $n + 1$ racines dans $\mathbb{K}$, alors $f = 0(X)$.*

REMARQUE 2.8. *Dans $\mathbb{Z}_9[X]$ le polynôme $f(X) = X^2$ possède 3 racines distinctes : $0, 3$ et 6. Pourquoi la preuve précédente ne fonctionne-t-elle pas dans ce cas ?*

Une autre utilité de l'algorithme d'Euclide est de trouver le plus grand commun diviseur de deux polynômes $f_1, f_2 \in \mathbb{K}[X]$: en appliquant l'algorithme d'Euclide de manière itérative, on a

$$\begin{aligned} f_1 &= q_1 f_2 + f_3 \\ f_2 &= q_2 f_3 + f_4 \\ f_3 &= q_3 f_4 + f_5 \\ &\vdots \\ f_{k-2} &= q_{k-2} f_{k-1} + f_k \end{aligned}$$

où le processus se termine lorsque $\deg f_k = 0$. La remarque simple mais cruciale est que si un polynôme g divise f_1 et f_2, alors la première ligne ci-dessus dit que g divise également f_3. Mais il s'en suit que g divise f_2 et f_3 , donc également f_4 par la seconde ligne de la division longue. Dans le cas où $f_k = 0$, on peut remonter l'algorithme de division et obtenir que f_{k-1} est le plus grand diviseur commun entre f_1 et f_2, noté (f_1, f_2). Réciproquement, si $f_k \neq 0$, les polynômes f_1 et f_2 n'ont pas de facteur en commun, on dit que f_1 et f_2 sont relativement premiers et on écrit $(f_1, f_2) = 1$.
L'algorithme peut également être interprété en termes d'algèbre linéaire : la première ligne dit que f_3 est combinaison linéaire (avec coefficients dans $\mathbb{K}[X]$) de f_1 et f_2. La seconde

ligne dit que f_4 jouit de la même propriété, mais alors f_5 est également combinaison linéaire de f_1 et f_2 selon la troisième ligne... On poursuit ainsi de suite la division pour obtenir que le plus grand commun diviseur de f_1 et f_2 dans $\mathbb{K}[X]$ sera combinaison linéaire de f_1 et f_2 : pour certains $\alpha, \beta \in \mathbb{K}[X]$, on a

$$h = \alpha f_1 + \beta f_2.$$

Notons que le cas où $(f_1, f_2) = 1$ dit alors qu'il existe $\alpha, \beta \in \mathbb{K}[X]$ tels que $\alpha f_1 + \beta f_2 = 1$.

En théorie des anneaux on introduit naturellement les deux notions suivantes : Soit $f \in \mathbb{A}$ non-nul et qui n'est pas une unité. On dit que f est *irréductible* dans $\mathbb{A}$ si $f = g \cdot h \Rightarrow g$ ou h unité de $\mathbb{A}$. On dit que f est *premier* dans $\mathbb{A}$ si $f \mid g \cdot h \Rightarrow f \mid g$ ou $f \mid h$. Il est facile de voir que tout élément premier est forcément irréductible : si $f = g \cdot h$ et que f divise un des deux facteurs, disons $g = k \cdot f$, on obtient immédiatement que $k \cdot h = 1$ et donc h est une unité tel que demandé par la condition de réductibilité de f. En général la réciproque est fausse : il y a des anneaux où certains irréductibles ne sont pas premiers (Exercice).
Dans la théorie des anneaux euclidiens, la notion d'éléments irréductibles permet de décomposer tout élément f en facteurs irréductibles, en procédant par des factorisations successives et en utilisant la propriété de la fonction degré dans un anneau euclidien pour s'assurer que le processus se termine après un nombre fini d'étapes. De son côté la notion d'élément premier permet de s'assurer d'une forme d'unicité de décomposition dans un anneau intègre : si l'on a deux décompositions en éléments premiers $f_1 f_2 \cdots f_n = f = g_1 g_2 \cdots g_m$, alors $m = n$ et les facteurs sont les mêmes à permutation et unités près [1].

Pour nos besoins dans l'étude des courbes algébriques, il nous sera important d'avoir à la fois la propriété de décomposition et d'unicité, donc nous nous restreindrons à travailler sur des anneaux dits *factoriels*, dans lesquel on a la décomposition unique en facteurs irréductibles.

THÉORÈME 2.9. *Si $\mathbb{K}$ est un corps quelconque, l'anneau $\mathbb{K}[X]$ est factoriel.*

DÉMONSTRATION. L'existance d'une décomposition en facteurs irréductibles est facile par induction sur le degré des polynômes. Il s'agit donc de démontrer que tout polynôme irréductible est premier. Soit donc $f \mid g \cdot h$ et tel que $f \nmid g$. Comme f es irréductible, la

1. pour alléger la terminologie on ne répète constamment "à permutation et unités près".

condition $f \nmid g$ signifie que g et f sont relativement premiers et donc il existe $\alpha, \beta \in \mathbb{K}[X]$ tels que $\alpha g + \beta f = 1$. Mais en multipliant cette équation par h, on a alors $\alpha gh + \beta fh = h$. Comme f divise clairement le membre de gauche, on doit avoir $f \mid h$ tel que demandé pour que f soit premier. □

Ce qui précède résume les propriétés de $\mathbb{K}[X]$ qui seront importantes. Du point de vue de l'algèbre abstrait, l'essentiel de ce que nous avons fait aurait pu être déduit de la suite d'inclusions

$$\{\text{Anneaux euclidiens}\} \subset \{\text{Anneaux principaux}\} \subset \{\text{Anneaux factoriels}\}.$$

Lorsque que l'on passe de l'anneau des polynômes $\mathbb{K}[X]$ à un anneau de polynômes en plusieurs variables, noté $\mathbb{K}[X_1, X_2, ..., X_n]$, on ne peut malheureusement exploiter cette suite d'inclusions d'anneaux pour obtenir la factorialité de $\mathbb{K}[X_1, X_2, ..., X_n]$. En effet on se convainc aisément que l'anneau $\mathbb{K}[X_1, X_2, ..., X_n]$ ne peut être eucliden dès que $n \geq 2$: prenons par exemple $f(X, Y) = Y^3$ et $g(X, Y) = XY$. Il est clairement impossible d'appliquer l'algorithme de division d'Euclide *dans* $\mathbb{K}[X, Y]$ et d'exprimer le polynôme f comme $f = q \cdot g + r$ avec $\deg r < \deg g$, puisque f ne dépend pas de X alors que g en dépend.
En fait l'anneau $\mathbb{K}[X_1, X_2, ..., X_n]$ n'est même pas un anneau principal dès que $n \geq 2$: prenons l'idéal $\mathcal{I} = \{f \in \mathbb{K}[X, Y] \mid f(0, 0) = 0\}$ (vérifiez qu'il s'agit bien d'un idéal) et montrons qu'il ne peut être engendré par un unique élément. En effet, on a que les polynômes $f = X$ et $g = Y$ sont dans $\mathcal{I}$ et pour avoir que $\mathcal{I} = < h >$ pour un certain $h \in \mathbb{K}[X, Y]$ on doit, en particulier, trouver $a, b \in \mathbb{K}[X, Y]$ tels que $f = a \cdot h$ et $g = b \cdot h$. Mais f et g sont de degré 1 et, pour engendrer $\mathcal{I}$, le polynôme h ne peut être de degré 0 (pourquoi ?), donc on doit avoir $\deg a = 0 = \deg b$. Ceci implique à la fois que $h = h(X)$ et $h = h(Y)$, ce qui est impossible.

Malgré ces lacunes l'anneau $\mathbb{K}[X_1, X_2, ..., X_n]$ partage tout de même avec $\mathbb{K}[X]$ la propriété d'être factoriel. La décomposition en facteurs irréductibles est facilement démontrée par une induction sur le degré des polynômes. La difficulté principale est de montrer que

$$\mathbb{A} \text{ factoriel } \Rightarrow \mathbb{A}[X] \text{ factoriel.}$$

Une preuve de ceci peut être trouvée dans le livre de Walker [**Wal**] (Section 6.2, théorème 6.1) mais afin de garder les pré-requis d'Algèbre à un niveau minimal, nous accepterons simplement ce résultat sans preuve. Une fois ceci démontré on obtient la factorialité de

$\mathbb{K}[X_1, X_2, ..., X_n]$ grâce à une induction finie, en remarquant que

$$\mathbb{K}[X_1, X_2, ..., X_n] \simeq \mathbb{K}[X_1, X_2, ..., X_{n-1}][X_n].$$

Résumons l'essentiel de ce qui a été discuté au fil des pages précédentes :

THÉORÈME 1. *Tout polynôme non constant $f(X_1, X_2, ..., X_n)$ défini sur un corps $\mathbb{K}$ peut être écrit de manière unique (à permutation de facteurs et multiplication scalaire près) sous la forme $f = \alpha f_1^{r_1} \cdot f_2^{r_2} \cdots f_k^{r_k}$, où $\alpha \in \mathbb{K}$, les facteurs $f_1, f_2, ..., f_k$ sont irréductibles et pour tous $i \neq j$ f_i n'est pas un facteur de f_j.*

Cette décomposition unique en facteurs irréductibles existe donc en théorie, mais on doit prévenir le lecteur ou la lectrice que la recherche explicite d'une telle décomposition est pas toujours facile... en fait il s'agit d'un des problèmes de base de l'*Algèbre commutative*.

2. Un outil important : le résultant de deux polynômes

Une question algébrique de base qui aura un impact pour l'étude des courbes algébriques est de savoir quand est-ce que deux polynômes ont un facteur en commun. Dans $\mathbb{C}[X]$ cette question a une réponse simple en apparence : les deux polynômes ont une racine commune (Proposition 2.5). Dans le cas de polynômes dans $\mathbb{A}[X]$ la réponse n'est pas aussi immédiate et nous allons définir un objet classique, le *résultant* de deux polynômes qui donne une réponse simple à la question.

Soient $f = a_0X^m + a_1X^{m-1} + ... + a_m$ et $g = b_0X^n + b_1X^{n-1} + ... + b_n$ deux éléments dans l'anneau de polynômes $\mathbb{A}[X]$.

DÉFINITION 2.10. *On appelle résultant de f et g l'expression*

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & ... & ... & ... & a_m & 0 & ... & ... & 0 \\ 0 & a_0 & a_1 & ... & ... & ... & a_m & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & ... & 0 & a_0 & a_1 & ... & ... & ... & ... & a_m \\ b_0 & b_1 & ... & b_n & 0 & ... & ... & ... & ... & 0 \\ 0 & b_0 & b_1 & ... & b_n & 0 & ... & ... & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & ... & ... & 0 & b_0 & b_1 & ... & ... & ... & b_n \end{vmatrix}$$

Par définition, $R(f,g)$ est un déterminant $(n+m)\times(n+m)$ obtenu en :

(1) répétant les coefficients $a_0, a_1, ..., a_m$ du polynôme f dans les entrées des n premières lignes en décalant d'une entrée vers la droite à chaque passage à la ligne suivante.

(2) répétant les coefficients $b_0, b_1, ..., b_n$ du polynôme g dans les entrées des m dernières lignes en décalant vers la droite à chaque passage à la ligne suivante.

LEMME 2.11. *Lorsque $\mathbb{A}$ est un anneau intègre et que $f, g \in \mathbb{A}[X]$, on a* $R(f,g) = 0$ *dans* $\mathbb{A}$

$$\iff \exists\ \phi, \psi \in \mathbb{A}[X] \text{ non nuls } |\ \deg\phi < \deg f, \deg\psi < \deg g \text{ et } \psi f + \phi g = 0 \text{ dans } \mathbb{A}[X].$$

DÉMONSTRATION. On peut travailler dans le corps de fractions $\mathbb{K}$ de l'anneau intègre $\mathbb{A}$ puisque l'on peut multiplier les coefficients de ϕ et ψ par leurs dénominateurs commun. Dans l'espace vectoriel V des polynômes de $\mathbb{K}[X]$ ayant un degré inférieur à $m+n$, on considère les éléments

$$X^{n-1}f\ \ ,...\ ,\ Xf\ ,\ f\ ,\ X^{m-1}g\ ,\ ...\ ,\ Xg\ ,\ g. \qquad (\dagger)$$

Si l'on considère la base $\{X^{m+n-1}, ..., X, 1\}$ de V, on observe que les rangées du résultant expriment exactement les coordonnées des vecteurs (†) dans cette base . Donc la condition $R(f,g) = 0$ exprime le fait que les vecteurs (†) sont linéairement dépendants dans V : on a une relation de dépendance linéaire de la forme

$$\mu_0 X^{n-1}f + \mu_1 X^{n-2}f + ... + \mu_{n-1}f + \lambda_0 X^{m-1}g + \lambda_1 X^{m-2}g + ... + \lambda_{m-1}g = 0.$$

Mais cette expression est exactement de la forme $\psi f + \phi g = 0$ où $\deg\psi < \deg g$ et $\deg\phi < \deg f$ tel qu'annoncé. □

Ce lemme permet de démontrer le résultat suivant qui s'avère fondamental puisqu'il permet de réduire le problème de l'existence de facteurs communs à deux polynômes dans $\mathbb{A}[X]$ à une question purement calculatoire dans $\mathbb{A}$.

THÉORÈME 2. **(Théorème du résultant)** *Soit $\mathbb{A}$ un anneau factoriel et $f, g \in \mathbb{A}[X]$ tels que $a_0 \neq 0$ et $b_0 \neq 0$. Alors f et g ont un facteur commun non-constant dans $\mathbb{A}[X]$ si et seulement si $R(f,g) = 0$ dans $\mathbb{A}$.*

DÉMONSTRATION. On exploite le lemme précédent et on montre en fait que f et g ont un facteur non-constant en commun $\iff$ $\exists\ \phi, \psi \in \mathbb{A}[X]$ non nuls tels que $\psi f + \phi g = 0$, avec $\deg\phi < \deg f$ et $\deg\psi < \deg g$.

Si f et g ont un facteur en commun h, on peut écrire $f = f_1 h$ et $g = g_1 h$, avec $\deg h \geq 1$. En posant $\phi = f_1$ et $\psi = -g_1$, on obtient immédiatement que

$$\psi f + \phi g = -g_1 f_1 h + f_1 g_1 h = 0,$$

ainsi que les conditions requises sur les degrés de ϕ et ψ.
Réciproquement, prenons une décomposition en facteurs premiers de $f\psi = -g\phi$:

$$(f_1\ f_2\ \cdots\ f_r)(\psi_1\ \psi_2\ \cdots\ \psi_k) = -(g_1\ g_2\ \cdots\ g_s)(\phi_1\ \phi_2\ \cdots\ \phi_l).$$

Alors modulo les unités, l'expression $g_1\ g_2\ \cdots\ g_s$ doit aussi apparaitre dans le membre de gauche puisque l'anneau $\mathbb{A}[X]$ est factoriel. Mais l'hypothèse $\deg \psi < \deg g$ implique qu'au moins un des facteurs g_i est de degré au moins 1 et figure parmi les facteurs premiers $f_1, f_2, ..., f_r$ du polynôme f tel que voulu. □

Il est utile de remarquer que nous avons travaillé avec un anneau $\mathbb{A}$ qui n'est pas forcément un corps dans le Théorème du résultant pour la raison suivante : nous pourrons appliquer le résultat au cas de polynômes dans $\mathbb{K}[X_1, X_2, ..., X_n]$ en utilisant l'isomorphisme d'anneaux $\mathbb{K}[X_1, X_2, ..., X_n] \simeq \mathbb{K}[X_1, X_2, ..., X_{n-1}][X_n]$, en exploitant le fait que $\mathbb{K}[X_1, X_2, ..., X_{n-1}]$ est intègre et factoriel.

Corollaire 2.12. *Si $f, g \in \mathbb{C}[X]$ polynômes non-constants, ils ont une racine commune si et seulement si $R(f, g) = 0$ dans $\mathbb{C}$.*

Démonstration. Sur $\mathbb{C}$ les facteurs premiers sont linéaires et correspondent aux racines d'un polynôme. Le résultat est donc une conséquence immédiate du résultat précédent. □

Avant d'étudier le problème de l'existence de facteurs premiers répétés pour un polynôme à l'aide du résultant, nous prenons quelques instants pour formaliser d'une manière purement algébrique la notion de dérivée dans $\mathbb{A}[X]$. Soit $f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$ un polynôme dans $\mathbb{A}[X]$ et définissons la *dérivée formelle* $D_X(f) = f' \in \mathbb{A}[X]$, où l'on a

$$f' = n \cdot a_n X^{n-1} + (n-1) \cdot a_{n-1} X^{n-2} + ... + a_1.$$

Il découle facilement de cette définition que $D_X \colon \mathbb{A}[X] \to \mathbb{A}[X]$ est un opérateur linéaire au sens où

$$D_X(\alpha f + \beta g) = \alpha D_X(f) + \beta D_X(g)$$

et qu'il satisfait en outre la règle de Leibniz pour un produit

$$D_X(f \cdot g) = D_X(f) \cdot g + f \cdot D_X(g).$$

DÉFINITION 2.13. *On appelle discriminant de $f \in \mathbb{A}[X]$, la quantité $R(f, f') \in \mathbb{A}$.*

PROPOSITION 2.14. *Soit $\mathbb{A}$ un anneau factoriel de caractéristique 0 et $f \in \mathbb{A}[X]$ un polynôme non-constant. Alors f possède un facteur premier répété si et seulement si son discriminant $R(f, f')$ est égal à 0.*

DÉMONSTRATION. On se place en caractéristique 0 pour pouvoir appliquer le Théorème du résultant à f et f'. On sait alors que $R(f, f') = 0 \iff f = h \cdot g_1$ et $f' = h \cdot g_2$ pour un certain h irréductible dans $\mathbb{A}[X]$. Mais on a par la règle de Leibniz que

$$h \cdot g_2 = f' = (h \cdot g_1)' = h \cdot g_1' + h' g_1.$$

Comme $h | f'$ et que $\deg h' < \deg h$ a a forcément $h | g_1$ et ainsi $h^2 | f$ tel qu'annoncé. □

CHAPITRE 3

Théorie élémentaire des courbes algébriques

Dans ce chapitre nous établissons les fondements de la théorie des courbes algébriques. A partir de maintenant nous travaillons exclusivement sur $\mathbb{C}$ pour définir les objets de notre étude.

1. Courbes affines et courbes projectives

Plusieurs notions du cours seront développées en parallèle pour les courbes affines et pour les courbes projectives, si bien qu'il nous importe de commencer par étudier le lien entre la notion de courbe algébrique affine et celle de courbe algébrique projective. Historiquement les courbes algébriques ont premièrement été étudiées dans le plan $\mathbb{A}^2(\mathbb{C})$, mais ici nous allons commencer par les courbes algébriques projectives.

DÉFINITION 3.1. *On appelle courbe algébrique projective un sous-ensemble de* $\mathbb{C}P^2$ *donné par*

$$\mathcal{C} = \{[X, Y, Z] \in \mathbb{C}P^2 |\ F(X, Y, Z) = 0\}$$

où $F(X, Y, Z)$ *est un polynôme homogène.*

Il est important de comprendre pourquoi nous demandons que F soit homogène dans la définition d'une courbe algébrique projective : pour avoir un objet dans l'espace projectif $\mathbb{C}P^2 = \mathbb{C}^2 - \{0\}\ /\ \mathbb{C}^*$ défini comme lieu d'annnulation d'un polynôme F, il faut absolument avoir que $F(X, Y, Z) = 0 \iff F(tX, tY, tZ) = 0$ pour tout $t \in \mathbb{C}^*$, ce qui revient exactement à requérir la condition d'homogénéité $F(tX, tY, tZ) = t^k \cdot F(X, Y, Z)$ sur le polynôme F.

La décomposition $\mathbb{C}P^2 = \mathbb{A}^2(\mathbb{C}) \cup \mathbb{C}P^1$ interprétée comme une partie affine donnée par la condition $Z = 1$ et une partie à l'infini donnée par la condition $Z = 0$ permet de voir les courbes algébriques affines comme restriction de courbes algébriques projectives, obtenues tout simplement en considérant le polynôme en deux variables $x = X$ et $y = Y$ donné par $f(x, y) = F(X, Y, 1)$.

On peut également faire le chemin inverse : partir d'un polynôme quelconque $g(x, y)$ définissant une courbe algébrique affine $\mathcal{C}$ pour construire une courbe projective lui correspondant en procédant à l'*homogénéisation* du polynôme g : en posant $x = X/Z$ et $y = Y/Z$, on obtient une fonction rationnelle $g(X/Z, Y/Z)$. En mettant le tout sur le même dénominateur $Z^{\deg g}$, on obtient alors

$$g(X/Z, Y/Z) = \frac{G(X, Y, Z)}{Z^{\deg g}},$$

pour un certain polynôme homogène de degré identique à celui de g. On peut définir la courbe algébrique projective $\widehat{\mathcal{C}}$ donnée par $G(X, Y, Z) = 0$. Puisque l'on a que $G(X, Y, 1) = g(x, y)$, la courbe $\widehat{\mathcal{C}}$ a bien comme partie affine la courbe $\mathcal{C}$.

Une question naturelle dans ce contexte est de se demander combien de points à l'infini ajoute-t-on à une courbe algébrique affine par le processus d'homogénéisation ? Cette question nous donne aussi l'occasion de faire une observation sur les polynômes homogènes en deux variables qui sera fort utile par la suite. Soit donc $g(x, y)$ un polynôme de degré n définissant une courbe affine $\mathcal{C}$ et prenons l'homogénéisation $G(X, Y, Z)$ de g, définissant $\widehat{\mathcal{C}}$. Les points ajoutés à $\mathcal{C}$ en passant à $\widehat{\mathcal{C}}$ satisfont donc la condition $G(X, Y, 0) = 0$. Puisque G est homogène de degré n, on aura que $G(X, Y, 0)$ sera également homogène de degré n (pourquoi ?). Mais alors on utilise le

LEMME 3.2. *Tout polynôme homogène $G(X, Y)$ de degré n dans $\mathbb{C}[X, Y]$ est décomposable en produit de n facteurs linéaires comptés avec multiplicité.*

DÉMONSTRATION. Le polynôme homogène s'écrit comme $G(X, Y) = \sum_{k=0}^{n} a_k X^k Y^{n-k}$. En divisant par Y^n chaque terme de cette somme, on obtient

$$\sum_{k=0}^{n} a_k \frac{X^k Y^{n-k}}{Y^n} = \sum_{k=0}^{n} a_k \left(\frac{X}{Y}\right)^k.$$

En posant $W = X/Y$ cette dernière expression définit un polynôme h de degré n [1] dans $\mathbb{C}[W]$. Par le Théorème Fondamental de l'Algèbre, h se décompose en facteurs linéaires en W et ainsi en remplaçant W par X/Y on obtient la factorisation

$$G(X, Y) = (b_1 X - a_1 Y)^{k_1} (b_2 X - a_2 Y)^{k_2} \cdots (b_i X - a_i Y)^{k_i},$$

où $k_1 + k_2 + ... + k_i = n$ et $[a_k, b_k] \in \mathbb{C}P^1$ $(1 \leq k \leq i)$. □

1. Si ce n'est pas le cas, il faut plutôt prendre $W = Y/X$

Le lemme précédent implique directement que les points ajoutés à $\mathcal{C}$, qui sont donnés par l'homogénéisation sous la forme de la condition $G(X, Y, 0) = 0$ existent en nombre fini : ce sont les points $[a_i, b_i, 0]$ $(1 \leq i \leq n)$. Si peu en nombre soient-ils, comme on le verra tout au long du cours, l'ajout de ces points lors du passage de $\mathcal{C}$ dans $\mathbb{A}^2(\mathbb{C})$ à $\widehat{\mathcal{C}}$ dans $\mathbb{C}P^2$ s'avère d'une importance fondamentale.

EXERCICE 3.3. *(Pour ceux ayant des notions de topologie) Démontrez qu'une courbe algébrique affine $\mathcal{C}$ dans $\mathbb{A}^2(\mathbb{C})$ n'est jamais compacte, mais qu'une courbe algébrique projective est toujours compacte.*

On dit que $\widehat{\mathcal{C}}$ construite ci-dessus est la *compactification* de la courbe affine $\mathcal{C}$.

2. Composantes irréductibles d'une courbe algébrique

Nous avons défini une courbe algébrique affine comme $\mathcal{C} = V(f)$ pour un certain polynôme $f \in \mathbb{C}[x, y]$. S'il arrive que le polynôme f peut être décomposé en facteurs non-constants et distincts $f = g \cdot h$, alors on a que $V(g) \subseteq V(f)$ et $V(h) \subseteq V(f)$, si bien que l'on a en fait $V(f) = V(g) \cup V(h)$, puisque $\mathbb{C}[x, y]$ est anneau intègre. C'est-à-dire que lorsque $f = g \cdot h$, la courbe algébrique $\mathcal{C} = V(f)$ se *décompose* en deux courbes algébriques $V(g)$ et $V(h)$: l'algèbre des polynômes a une conséquence sur la géométrie/topologie des courbes algébriques affines.

DÉFINITION 3.4. *Une courbe algébrique affine $\mathcal{C}$ est dite réductible s'il existe une décomposition $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ avec $\mathcal{C}_1 \neq \mathcal{C}_2$. Dans le cas contraire, on dit que $\mathcal{C}$ est irréductible.*

Le résultat suivant est fondamental puisqu'il nous permettra d'obtenir une solution purement algébrique au problème de décomposition d'une courbe algébrique en composantes irréductibles.

LEMME 3.5. **(Lemme de Study)** *Soient $f, g \in \mathbb{C}[x, y]$ avec f irréductible et $\deg f \geq 1$. Si l'on a que $V(f) \subseteq V(g)$, on a que f divise g dans $\mathbb{C}[x, y]$.*

DÉMONSTRATION. L'idée de la preuve est de réduire le résultat au Théorème fondamental de l'Algèbre grâce au résultant. Ecrivons les deux polynômes comme éléments de $\mathbb{C}[x][y]$:

$$f = a_0 y^m + a_1 y^{m-1} + ... + a_m$$
$$g = b_0 y^n + b_1 y^{n-1} + ... + b_n$$

où $a_i, b_j \in \mathbb{C}[x]$ $(1 \leq i \leq m\ ,\ 1 \leq j \leq n)$ avec $a_0, b_0 \neq 0$. Quitte à remplacer x par y, on peut supposer que $m \geq 1$. Considérons $V(f) \subseteq V(g)$ que l'on intersecte avec les droites verticales $x = \alpha$ pour tous $\alpha \in \mathbb{C}$. Affirmation : on doit avoir $n > 0$. Sinon on aurait $g = b_0$ et alors pour tout α_0 tel que $a_0(\alpha_0) \neq 0$ et $b_0(\alpha_0) \neq 0$, $V(f)$ intersecterait la droite $x = \alpha_0$ (Théorème fondamental de l'Algèbre par rapport à la variable y) mais par construction $V(g)$ n'intersecterait pas cette même droite $x = \alpha_0$, ce qui contredirait $V(f) \subseteq V(g)$.
Considérons maintenant le résultant $R(f, g) \in \mathbb{A} = \mathbb{C}[x]$. Comme f est irréductible, la condition $R(f, g) = 0$ est équivalente à dire que f divise g par le Théorème du résultant. On montrera que $R(f, g) = 0$ en montrant que l'on a $R(f, g)(\alpha) = 0$ pour un nombre infini de $\alpha \in \mathbb{C}$. Comme a_0, b_0 sont non-nuls dans $\mathbb{C}[x]$, on a $a_0(\alpha) \neq 0$ et $b_0(\alpha) \neq 0$ pour presque tout $\alpha \in \mathbb{C}$. Si on pose $x = \alpha$, alors f et g définissent des polynômes f_α et g_α dans $\mathbb{C}[y]$. Par $V(f) \subseteq V(g)$ on sait que si $c \in \mathbb{C}$ est un zéro de f_α, alors c'est également un zéro de g_α et donc $(y - c)$ est facteur commun de f_α et g_α dans $\mathbb{C}[y]$. Mais pour de telles valeurs $\alpha \in \mathbb{C}$, on a

$$R(f, g)(\alpha) = R(f_\alpha, g_\alpha) = 0,$$

où la dernière égalité est obtenue en appliquant le Théorème du résultant dans $\mathbb{C}$. Ceci conclut la preuve du Lemme de Study. □

Le Lemme de Study nous permet de faire correspondre à la décomposition algébrique en facteurs irréductibles d'un polynôme $f \in \mathbb{C}[x, y]$, $f = f_1^{k_1} f_2^{k_2} \cdots f_r^{k_r}$, une décomposition géométrique $V(f) = V(f_1) \cup V(f_2) \cup ... \cup V(f_r)$, où chaque membre de droite est courbe irréductible. On appelle les $V(f_k)$ $(1 \leq k \leq r)$ les *composantes irréductibles* de $V(f)$.

PROPOSITION 3.6. *Une courbe algébrique affine $\mathcal{C} = V(f) \subset \mathbb{A}^2(\mathbb{C})$ est irréductible $\iff$ $\exists k \in \mathbb{N}$ et $\exists g \in \mathbb{C}[x, y]$ irréductible tels que $f = g^k$.*

DÉMONSTRATION. On procède par contraposition dans les deux directions. Soit $\mathcal{C} = V(f)$ une courbe et $f = f_1 \cdot f_2$ une décomposition en facteurs relativement premiers. Alors si h est facteur irréductible de f_1, on a $V(h) \subseteq V(f_1)$ et comme h ne divise pas f_2, la contraposée du Lemme de Study implique que $V(h) \nsubseteq V(f_2)$, si bien que $V(f_1) \neq V(f_2)$ et la courbe $\mathcal{C}$ est réductible.
Réciproquement, si $\mathcal{C} = V(f)$ est réductible, on a $V(f) = V(f_1) \cup V(f_2)$, avec $V(f_1) \neq V(f_2)$. Par la condition de réductibilité, il y a au moins un facteur irréductible h_i d'un des f_i pas partagé par l'autre polynôme (autrement on aurait $V(f_1) \subseteq V(f_2)$ et $V(f_2) \subseteq V(f_1)$) et donc $f \neq g^k$ pour tout $g \in \mathbb{C}[x, y]$ et tout $k \in \mathbb{N}$. □

Nous avons maintenant tous les outils nécessaires pour démontrer le résultat de décomposition suivant pour les courbes algébriques :

THÉORÈME 3. *Toute courbe algébrique affine $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ admet une décomposition $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup ... \cup \mathcal{C}_r$, où les $\mathcal{C}_i$ $(1 \leq i \leq r)$ sont des courbes algébriques affines irréductibles. Cette décomposition est unique modulo l'ordre.*

DÉMONSTRATION. Soit $\mathcal{C} = V(f)$. L'existence découle directement de la décomposition en facteurs irréductibles de polynômes dans $\mathbb{C}[x, y]$ et de la proposition ci-dessus. Pour l'unicité, si $\mathcal{C}' \subseteq \mathcal{C}$ est irréductible, on doit montrer que $\mathcal{C}' = \mathcal{C}_k$ pour un certain $1 \leq k \leq r$. On a $\mathcal{C}' = V(f')$ pour un certain f' irréductible. Par le Lemme de Study, comme $V(f') \subseteq V(f)$, on a que f' est facteur irréductible de f, ce qui termine la preuve. □

COROLLAIRE 3.7. *Soit $\mathcal{C} = V(f) \subset \mathbb{A}^2(\mathbb{C})$ avec $f = f_1^{k_1} f_2^{k_2} \cdots f_r^{k_r}$ décomposition en facteurs irréductibles. Si l'on peut exprimer $\mathcal{C}$ comme $V(g)$ pour un autre polynôme $g \in \mathbb{C}[x, y]$, alors $g = \lambda f_1^{l_1} f_2^{l_2} \cdots f_r^{l_r}$ pour certains $\lambda \in \mathbb{C}^*$ et l_i $(1 \leq i \leq r)$ entiers.*

Ce corollaire permet de définir sans ambiguïté le *polynôme minimal* de la courbe algébrique affine $\mathcal{C} = V(f)$, en posant $\tilde{f} = f_1 f_2 \cdots f_r$. Ce polynôme est unique à multiplication par une unité près et il peut être interprété comme le polynôme de degré minimal définissant le lieu géométrique occupé par $\mathcal{C}$ dans $\mathbb{A}^2(\mathbb{C})$. Ceci découle de l'observation voulant que $V(f_i) = V(f_i^{k_i})$ puisque $\mathbb{C}[x, y]$ est intègre. En particulier on note que $\mathcal{C} = V(f)$ est courbe irréductible $\iff$ $\tilde{f}$ est polynôme irréductible.

DÉFINITION 3.8. *On définit le degré d'une courbe algébrique $\mathcal{C} = V(f)$ comme étant le degré de son polynôme minimal $\tilde{f}$.*

Nous tournons maintenant notre attention vers le cas des courbes algébriques projectives $\mathcal{C} \subset \mathbb{C}P^2$ pour ce qui est de la question de la réductibilité. La définition pour les courbes projectives est exactement la même que celle donnée à la Définition 3.4. Etant donné le lien étroit entre une courbe algébrique affines et sa compactification obtenue par le processus d'homogénéisation, nous allons tout simplement pouvoir transposer le travail fait dans $\mathbb{A}^2(\mathbb{C})$ vers $\mathbb{C}P^2$ au moyen des quelques résultats algébriques auxiliaires suivants :

LEMME 3.9. *Si $F \in \mathbb{C}[X, Y, Z]$ est homogène et se décompose en $F = G \cdot H$, alors G et H sont également homogènes.*

DÉMONSTRATION. Exercice. □

LEMME 3.10. *Soit $f \in \mathbb{C}[x,y]$ et $F \in \mathbb{C}[X,Y,Z]$ son polynôme homogène associé. Alors on a f irréductible si et seulement si F est irréductible.*

DÉMONSTRATION. Si F est réductible, on a $F = G \cdot H$ avec G et H homogènes par le lemme précédent. On a donc que

$$f(x,y) = F(X,Y,1) = G(X,Y,1) \cdot H(X,Y,1)$$

est décomposition en facteurs non-constants (pourquoi ?). Réciproquement, si on a $f = g \cdot h$, alors

$$\begin{aligned} F(X,Y,Z) &= f(X/Z, Y/Z) Z^{\deg f} \\ &= g(X/Z, Y/Z) Z^{\deg g} \cdot h(X/Z, Y/Z) Z^{\deg h} \\ &= G(X,Y,Z) \cdot H(X,Y,Z). \end{aligned}$$

□

PROPOSITION 3.11. *Soit $f = f_1 \cdots f_r$ décomposition en facteurs irréductibles, F polynôme homogène associè à f et F_i polynômes homogènes associés aux f_i $(1 \leq i \leq r)$. Alors $F = F_1 \cdots F_r$ et cette décomposition est unique à unités près.*

DÉMONSTRATION. Si g (resp. h) est associé à G (resp. H) par homogénéisation, alors $g \cdot h$ est associé à $G \cdot H$. Une induction finie nous permet donc de conclure que l'homogénéisé de $f = f_1 \cdots f_r$ est $F = F_1 \cdots F_r$. Le lemme précédent et l'hypothèse d'irréductibilité des f_i $(1 \leq i \leq r)$ nous disent qu'il s'agit d'une décomposition en facteurs irréductibles, donc unique modulo unités. □

On peut dès lors montrer que la notion d'irréductibilité des courbes algébriques est la même dans $\mathbb{A}^2(\mathbb{C})$ et dans $\mathbb{C}P^2$:

THÉORÈME 3.12. *Soit $\mathcal{C}$ une courbe algébrique de $\mathbb{A}^2(\mathbb{C})$ et $\widehat{\mathcal{C}}$ sa compactification. Alors on a $\mathcal{C}$ irréductible $\iff$ $\widehat{\mathcal{C}}$ irréductible.*

DÉMONSTRATION. Soient $\mathcal{C} = V(f)$ et $\widehat{\mathcal{C}} = V(F)$ définies chacune par leur polynôme minimal, où F homogénéisé de f. Puisque $\widehat{\mathcal{C}} = \mathcal{C} \cup \{\text{nombre fini de points à l'infini}\}$, on a immédiatement que $\mathcal{C}$ irréductible implique $\widehat{\mathcal{C}}$ également irréductible (on se souvient que toute composante d'une courbe algébrique sur $\mathbb{C}$ a un nombre infini de points).
Pour l'autre direction, on procède par contraposition. Soit $\mathcal{C}$ réductible, si bien qu'on peut décomposer $f = f_1 \cdot f_2$ en facteurs non-constants distincts et par le Lemme 3.10, on a une décomposition correspondante de l'homogénéisé $F = F_1 \cdot F_2$, si bien que $\widehat{\mathcal{C}}$ est réductible. □

Notons que le Théorème 3.12 n'affirme pas tout à fait qu'une courbe algébrique projective est irréductible si et seulement si sa partie affine est irréductible, car il n'est pas vrai que toute courbe algébrique projective est compactification d'une courbe algébrique affine. Par exemple la courbe algébrique projective d'équation $XZ = 0$ n'est pas la compactification d'une courbe affine (pourquoi ?). Dans ce cas, la partie affine ($Z \neq 1$) est donnée par la droite $x = 0$ (donc une courbe irréductible de $\mathbb{A}^2(\mathbb{C})$) et pourtant la courbe projective est réductible en deux composante d'équations respectives $X = 0$ et $Z = 0$.
Ceci dit l'analogue du Théorème 3 pour les courbes projectives est facilement obtenu en ajoutant possiblement une composante irréductible à l'infini ($Z = 0$ selon les coordonnées employées usuellement) qui n'aurait pas été détectée en prenant les parties irréductibles affines et en les compactifiant. Algébriquement ceci correspond à l'unique décomposition en facteurs irréductibles $F = F_1^{k_1} \cdots F_r^{k_r}$. On obtient au final pour une courbe algébrique projective $\mathcal{C} \subset \mathbb{C}P^2$ un décomposition unique en composantes irréductibles

$$\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup ... \cup \mathcal{C}_r,$$

définie par le polynôme minimal de la courbe algébrique projective $\tilde{F} = F_1 \cdots F_r$.

Exercice 3.13. *Démontrez que la notion de degré et d'irréductibilité d'une courbe algébrique projective est invariante sous l'action du groupe de transformations projectives* $PGL_3(\mathbb{C})$.

Bien que la notion de polynôme minimal soit la bonne pour décrire algébriquement le lieu défini par une courbe algébrique dans $\mathbb{A}^2(\mathbb{C})$ ou dans $\mathbb{C}P^2$, il y a tout de même un certain intérêt à traduire géométriquement l'information offerte par un polynôme $f = f_1^{k_1} f_2^{k_2} \cdots f_r^{k_r}$ ou $F = F_1^{k_1} \cdots F_r^{k_r}$ définissant $V(f) \subset \mathbb{A}^2(\mathbb{C})$ ou $V(F) \subset \mathbb{C}P^2$. Ceci est fait à l'aide de la notion de *diviseur* que nous définissons ici dans $\mathbb{C}P^2$ seulement, mais il est facile de faire la même chose dans $\mathbb{A}^2(\mathbb{C})$. L'idée de base est de définir une addition formelle sur l'ensemble des courbes de $\mathbb{C}P^2$ de manière à que ce : (1) pour des courbes différentes $\mathcal{C}_1$ et $\mathcal{C}_2$, le diviseur $\mathcal{C}_1 + \mathcal{C}_2$ représente la courbe $\mathcal{C}_1 \cup \mathcal{C}_2$ (2) si $\mathcal{C} = V(F)$, alors $k\mathcal{C}$ est le diviseur associé à $V(F^k)$. Ce faisant, on arrive à distinguer géométriquement $V(F_1^{k_1} \cdots F_r^{k_r})$ de $V(F_1 \cdots F_r)$ bien que, en tant que lieux de $\mathbb{C}P^2$, ils soient identiques. En effet, en posant $\mathcal{C}_i = V(F_i)$ ($1 \leq i \leq r$), le premier donne lieu au diviseur $k_1\mathcal{C}_1 + k_2\mathcal{C}_2 + ... + k_n\mathcal{C}_r$, alors que le second définit le diviseur $\mathcal{C}_1 + \mathcal{C}_2 + ... + \mathcal{C}_r$. Comme ce fut le cas pour une courbe algébrique, on peut définir le *degré* d'un diviseur comme étant l'entier $k_1 \deg F_1 + k_2 \deg F_2 + ... + k_r \deg F_r$, qui est bien sûr exactement le degré du polynôme F ci-dessus. Par ailleurs, un diviseur est dit *efficace* lorsque tous les entiers sont non-nuls.

3. Multiplicité d'intersection entre une courbe et une droite

La théorie générale de l'intersection des courbes algébriques sera développée au chapitre suivant, mais avec les moyens développés précédemment, nous pouvons déjà étudier en détail le cas particulier de l'intersection d'une courbe algébrique avec une droite. Nous plaçons dès le début notre étude dans le cadre projectif.

Soit donc $\mathcal{C} \subset \mathbb{C}P^2$ une courbe algébrique de degré n donnée par $F(X,Y,Z) = 0$ et $\mathcal{L}$ une droite projective. Pour étudier $\mathcal{C} \cap \mathcal{L}$, on note que cette intersection est invariante sous l'action de $PGL_3(\mathbb{C})$ et donc peut simplifier le calcul en effectuant une transformation projective pour se ramener au cas où l'équation de $\mathcal{L}$ est $Z = 0$. Le calcul de $\mathcal{C} \cap \mathcal{L}$ se fait donc en obtenant les zéros du polynôme homogène $G(X,Y) = F(X,Y,0)$. Ecrivons F comme un élément de $\mathbb{C}[X,Y][Z]$:

$$F(X,Y,Z) = F_0 Z^n + F_1 Z^{n-1} + ... + F_{n-1} Z + F_n,$$

où les $F_k \in \mathbb{C}[X,Y]$ $(1 \leq k \leq n)$ sont polynômes homogènes avec $\deg F_k = k$ si F_k est polynôme non-nul.
Sous cette décomposition de F, on constate que $G = F_n$. Si l'on a $F_n \equiv 0$, alors le polynôme F est divisible par le facteur irréductible Z, ce qui est équivalent à dire que $\mathcal{L}$ est une *composante* de $\mathcal{C}$, par le Lemme de Study et sa réciproque. L'autre possibilité est que l'on ait $\deg G = \deg F_n = n$. Par la version homogène du Théorème fondamental de l'Algèbre , on a

$$G(X,Y) = (b_1 X - a_1 Y)^{k_1} (b_2 X - a_2 Y)^{k_2} \cdots (b_m X - a_m Y)^{k_m},$$

où les $[a_i, b_i] \in \mathbb{C}P^1$ sont distincts et uniques et $k_1, k_2, ..., k_m \in \mathbb{N}$.

Exercice 3.14. *Montrez que les coefficients $k_1, k_2, ..., k_m$ dépendent seulement de $\mathcal{C}$ et $\mathcal{L}$ et non pas du choix de coordonnées utilisées ci-dessus pour le calcul.*

Définition 3.15. *On appelle multiplicité d'intersection locale de $\mathcal{C}$ et $\mathcal{L}$ en $p \in \mathcal{C} \cap \mathcal{L}$, le nombre* $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = k$, *où $k = k_l$ pour $p = [a_l, b_l, 0]$ et $k = 0$ pour tout autre point de $\mathbb{C}P^2$.*

Exercice 3.16. *Montrez que* $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = k_l$ *en $p = [a_l, b_l, 0]$ si et seulement si $G^{(k_l)}(a_l, b_l) \neq 0$ mais $G^{(i)}(a_l, b_l) = 0$ pour tout $1 \leq i < k_l$, où $G^{(i)}$ dénote la $i^{ème}$ dérivée formelle de G.*

Avec cette terminologie, on obtient le résultat suivant :

THÉORÈME 4. *Si $\mathcal{C} \subset \mathbb{C}P^2$ est une courbe de degré n et $\mathcal{L}$ une droite projective qui n'est pas composante de $\mathcal{C}$, alors le nombre total d'intersections entre $\mathcal{C}$ et $\mathcal{L}$, comptées avec multiplicité, est égal à n.*

DÉMONSTRATION. En effet la discussion ci-dessus, la définition de multiplicité d'intersection en un point et le fait que $k_1 + k_2 + ... + k_m = n$ donnent le résultat. □

Nous ne saurions assez insister sur le fait que le Théorème 4 dépend crucialement à la fois du fait que nous travaillons sur $\mathbb{C}$ pour l'étude des courbes, mais aussi de l'espace dans lequel on travaille : $\mathbb{C}P^2$. En restreignant l'étude aux courbes algébriques *réelles*, la discussion ci-dessus ne peut être complétée car le Théorème fondamental de l'Algèbre est faux si on travaille sur $\mathbb{R}$. Ainsi par exemple dans $\mathbb{A}^2(\mathbb{R})$ l'intersection entre la courbe algébrique $x^2 + y^2 - 1 = 0$ et la droite $y = 2$ est *vide*. Pour ce qui est de la différence entre l'intersection de courbes dans $\mathbb{A}^2(\mathbb{C})$ versus $\mathbb{C}P^2$, la non-compacité de $\mathbb{A}^2(\mathbb{C})$ fait en sorte que des intersections auxquelles on s'attendrait d'un point de vue algébrique peuvent se *perdre à l'infini...* Donnons un exemple pour illustrer l'idée générale :

Dans $\mathbb{A}^2(\mathbb{C})$ considérons le Folium de Descartes, une cubique donnée par l'équation $f(x, y) = x^3 + y^3 - 3xy = 0$, que l'on cherche à intersecter avec la droite d'équation $x + y + 1 = 0$. En éliminant la variable y en utilisant le fait que $y = -x - 1$ pour être sur la droite, on cherche donc à résoudre l'équation $f(x, -x - 1) = 0$. Mais nous avons

$$f(x, -x - 1) = x^3 + (-x - 1)^3 - 3x(-x - 1) = x^3 - x^3 - 3x^2 - 3x - 1 + 3x^2 + 3x = -1.$$

Il n'y a donc *aucune* intersection dans $\mathbb{A}^2(\mathbb{C})$ entre ces deux courbes !
Si nous considérons plutôt les compactifications dans $\mathbb{C}P^2$ de ces deux courbes affines, nous obtenons les courbes projectives d'équations $X^3 + Y^3 - 3XYZ = 0$ et $X + Y + Z = 0$. Pour trouver les intersections, on doit résoudre $G(X, Y) = 0$, où $G(X, Y) = F(X, Y, -X - Y)$. Mais on a

$$X^3 + Y^3 - 3XY(-X - Y) = (X + Y)^3,$$

donc l'unique racine de ce polynôme est $[1, -1]$. L'intersection consiste donc en l'unique pour $[1, -1, 0]$, avec multiplicité d'intersection égale à 3, ce qui était prévisible par le Théorème 4.

COROLLAIRE 3.17. *Etant donné une courbe algébrique $\mathcal{C}$ de degré n et une droite générique $\mathcal{L}$ de $\mathbb{C}P^2$:* **(1)** *les points d'intersection sont simples, au sens où* $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = 1$. **(2)** *$\mathcal{C} \cap \mathcal{L}$ contient n points.*

DÉMONSTRATION. On a la décomposition du polynôme décrivant l'intersection $\mathcal{C} \cap \mathcal{L}$: $G(X,Y) = (b_1X - a_1Y)^{k_1}(b_2X - a_2Y)^{k_2} \cdots (b_nX - a_nY)^{k_m}$, et on veut montrer que pour une droite projective générique, on a $k_1 = k_2 = \cdots = k_m = 1$. C'est-à-dire que l'on ne veut pas avoir de racines multiples de G. On se souvient que G aura des racines multiples si et seulement si le discriminant $R(G, G')$ est identiquement nul. Comme le discriminant est obtenu par calcul d'un déterminant, qui sera fonction continue des coefficients de G et G', la condition $R(G, G') \neq 0$ est effectivement générique.
Pour la seconde assertion, par la première partie on a $k_1 = k_2 = \cdots = k_m = 1$ dans le cas d'une droite projective générique et donc $\mathcal{C} \cap \mathcal{L}$ consiste de n points distincts. □

Il peut être utile de considérer un contexte plus général non pas d'intersection entre une courbe et *une* droite, mais plutôt d'étudier l'intersection entre une courbe et une famillle de droites passant toutes par un point de la courbe. Afin de développer une certaine facilité à passer de $\mathbb{C}P^2$ à $\mathbb{A}^2(\mathbb{C})$ et vice versa, nous développons ce qui suit dans le contexte affine. Soite $p = (x_0, y_0)$ un point arbitraire de $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ donnée par un polynôme minimal $f(x, y)$ et considérons une droite $\mathcal{L}$ passant par p : son équation paramétrique sera

$$\begin{cases} x = x_0 + at \\ y = y_0 + bt \end{cases}$$

où $a, b \in \mathbb{C}$ pas tous nuls sont fixés, correspondant l'équation $b(x - x_0) - a(y - y_0) = 0$. Pour trouver l'intersection $\mathcal{C} \cap \mathcal{L}$ on doit trouver les solutions en t de l'équation $g(t) = f(x_0 + at, y + bt) = 0$. On peut considérer le développement de MacLaurin algébrique

$$g(t) = g(0) + \frac{g'(0)}{1!}t + \frac{g''(0)}{2!}t^2 + ... + \frac{g^{(n)}(0)}{n!}t^n.$$

Etant donné les Exercices 3.14 et 3.16, on a que $\mathcal{L}$ intersecte $\mathcal{C}$ en $p = (x_0, y_0)$ avec multiplicité k si et seulement si $g^{(k)}(0) \neq 0$ mais $g^{(l)}(0) = 0$ pour tout $1 \leq l < k$. Si l'on suppose que la multiplicité d'intersection est au moins 2, on a ainsi $g'(0) = 0$. Par la règle de dérivation en chaine formelle, pour $g(t) = f(x + 0 + at, y_0 + bt)$ on a

$$\frac{\partial f}{\partial x}(p) \cdot a + \frac{\partial f}{\partial y}(p) \cdot b = 0.$$

En supposant qu'une de ces deux dérivées est non-nulle (c'est-à-dire que p est un point régulier), disons $\partial f/\partial x(p) \neq 0$, alors en prenant $b = 1$ (rappel : les coefficients a et b sont définis à un scalaire commun près), on a donc

$$a = -\frac{\partial f/\partial y(p)}{\partial f/\partial x(p)}$$

et on tire de cela que l'équation linéaire de $\mathcal{L}$ donnée comme $b(x-x_0)-a(y-y_0)=0$ devient

$$\frac{\partial f}{\partial x}(p)\cdot(x-x_0)+\frac{\partial f}{\partial y}(p)\cdot(y-y_0).$$

On a donc montré

PROPOSITION 3.18. *Une droite $\mathcal{L}$ passant par un point régulier p d'une courbe $\mathcal{C}$ dans $\mathbb{A}^2(\mathbb{C})$ est tangente à $\mathcal{C}$ en p si et seulement* $\text{mult}_p(\mathcal{C}\cap\mathcal{L})\geq 2$.

Cette Proposition suggère qu'il existe une approche purement algébrique de la notion de droite tangente à une courbe algébrique, définie à partir de la multiplicité d'intersection. Nous verrons à la section suivante que cela est bien le cas et la nouvelle approche aura le grand avantage de s'appliquer également dans le cas des points singuliers de courbes algébriques.

4. Singularités et notion d'ordre d'une courbe en un point

Rappelons qu'un point p sur une courbe $\mathcal{C}$ est dit singulier si les dérivées partielles du polynôme minimal évaluées en p sont toutes nulles. Ceci a un sens tant pour les courbes algébriques dans $\mathbb{A}^2(\mathbb{C})$ ou dans $\mathbb{C}P^2$. Il est important de travailler avec le polynôme minimal, car autrement on voit facilement que tout point est singulier.

EXERCICE 3.19. *Montrez que pour une courbe projective $\widehat{\mathcal{C}}$ ayant une partie affine $\mathcal{C}$, on a que $p\in\mathcal{C}$ est point singulier pour $\mathcal{C}$ si et seulement si il est point singulier de $\widehat{\mathcal{C}}$. (Indice : Identité d'Euler)*

DÉFINITION 3.20. *On appelle lieu singulier d'une courbe algébrique $\mathcal{C}$ l'ensemble*

$$\text{Sing}(\mathcal{C})=\{p\in\mathcal{C}\mid \mathcal{C} \text{ est singulière en } p\}.$$

Une fois que nous aurons vu le Théorème de Bézout, nous pourrons montrer que pour toute courbe algébrique, $\text{Sing}(\mathcal{C})$ est une ensemble fini. Pour l'instant nous nous intéressons à la description locale de la courbe autour d'un point singulier. Nous commençons par travailler avec des courbes dans $\mathbb{A}^2(\mathbb{C})$.
Soit $\mathcal{C}=V(f)$ une courbe de degré n et prenons un point quelconque $p=(x_0,y_0)$ sur la courbe. On peut écrire le développement de Taylor formel de f autour de p comme

$$f(x,y)=\sum_{k=1}^{n} f_{(k)}$$

où l'on a

$$f_{(k)} = \sum_{i+j=k}^{n} a_{ij}(x-x_0)^i(y-y_0)^j \quad \text{et} \quad a_{ij} = \frac{1}{i!j!}\frac{\partial^{i+j} f}{\partial x^i \partial y^j}(p).$$

DÉFINITION 3.21. *L'ordre du polynôme f au point p est l'entier*

$$\mathrm{ord_p}(f) = \min\{k \in \mathbb{N} \mid f_{(k)} \neq 0\}.$$

L'ordre d'une courbe algébrique $\mathcal{C} = V(f)$ au point p est donné par $\mathrm{ord_p}(\mathcal{C}) = \mathrm{ord_p}(f)$.

PROPOSITION 3.22. *L'ordre d'une courbe $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ en un point $p \in \mathbb{A}^2(\mathbb{C})$ satisfait :*

(1) $0 \leq \mathrm{ord_p}(\mathcal{C}) \leq \deg \mathcal{C}$.
(2) $p \in \mathcal{C} \iff \mathrm{ord_p}(\mathcal{C}) > 0$.
(3) *$\mathcal{C}$ est lisse en p* $\iff \mathrm{ord_p}(\mathcal{C}) = 1$.
(4) *$\mathcal{C}$ est singulière en p* $\iff \mathrm{ord_p}(\mathcal{C}) > 1$.
(5) $\mathrm{ord_p}(\mathcal{C}) = \deg \mathcal{C} = n \iff$ *$\mathcal{C}$ est réunion de n droites (pas forcément distinctes) passant par p.*

DÉMONSTRATION. (1) est évident à partir de la définition. Pour (2) on a $f_{(0)} \neq 0 \iff f(p) \neq 0 \iff p \notin \mathcal{C}$, puisque $f_{(k)}(p) = 0$ pour $1 \leq k \leq \deg \mathcal{C}$ par construction de $f_{(k)}$. Les items (3) et (4) découlent directement de la définition de a_{ij} et des définitions de point régulier et point singulier. Finalement, pour (5), on a par définition de l'ordre que $f = f_{(n)}$, si bien que f est polynôme homogène de degré n et se factorise en n facteurs linéaires (pas forcément distincts). Ceci arrive si et seulement si $\mathcal{C}$ est réunion de n droites passant par p. □

Nous avons jusqu'à maintenant introduit deux notions qui semblent avoir très peu en commun : l'ordre d'une courbe en un point et la multiplicité d'intersection locale entre une courbe et une droite. Nous allons voir qu'il y a en fait un lien à faire entre les deux notions. Nous reprenons la décomposition du développement de Taylor formel

$$f = \sum_{k=r}^{n} f_{(k)}$$

où $r = \mathrm{ord_p}(\mathcal{C})$ et $n = \deg f$. Par simplicité nous supposons en outre que $p \in \mathbb{A}^2(\mathbb{C})$ est placé à l'origine : $p = (0,0)$. Si $\mathcal{L}$ est une droite passant par p, elle est donnée par $\varphi(t) = (\lambda_1 t, \lambda_2 t)$ et déterminée par $[\lambda_1, \lambda_2] \in \mathbb{C}P^1$. Posons maintenant

$$g(t) = f(\varphi(t)) = \sum_{k=r}^{n} f_{(k)}(\lambda_1, \lambda_2)t^k.$$

PROPOSITION 3.23. **(Inégalité ordre-multiplicité)** *Pour une courbe algébrique $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ et $\mathcal{L}$ une droite passant par $p \in \mathcal{C}$, on a* $\mathrm{ord_p}(\mathcal{C}) \leq \mathrm{mult}_p(\mathcal{C} \cap \mathcal{L})$. *L'inégalité est stricte seulement pour un nombre fini de droites passant par $p \in \mathcal{C}$.*

DÉMONSTRATION. Pour le polynôme $g(t)$ défini ci-dessus, on peut définir son ordre par $\mathrm{ord_p}(g) = \min\{k \in \mathbb{N} \mid f_{(k)}(\lambda_1, \lambda_2) \neq 0\}$. On a alors clairement que $\mathrm{ord_p}(g) \geq \mathrm{ord_p}(f)$. Par ailleurs, en vertu de ce qui a été fait à la fin de la section précédente, on a que la multiplicité d'intersection locale en p entre $\mathcal{C}$ et $\mathcal{L}$ est donnée par $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = \mathrm{ord_p}(g)$. Ceci donne l'inégalité désirée.
Par définition de $\mathrm{ord_p}(g)$, l'inégalité sera stricte si et seulement si $f_{(r)}(\lambda_1, \lambda_2) = 0$. Comme $\mathrm{ord_p}(f) = \mathrm{ord_p}(\mathcal{C}) = r$, on sait que $f_{(r)}$ n'est pas identiquement nul, si bien qu'il existe un nombre fini de pentes pour lesquelles $f_{(r)}(\lambda_1, \lambda_2) = 0$ donnent l'inégalité stricte. Pour toutes les autres pentes on a l'égalité $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = \mathrm{ord_p}(\mathcal{C})$. □

On se souvient que l'on a défini la notion de tangente en un point p à une courbe algébrique $\mathcal{C}$ seulement dans le cas où p est un point régulier. Avec l'inégalité ordre-multiplicité on peut généraliser la notion de droite tangente de la manière suivante :

DÉFINITION 3.24. *On dit que $\mathcal{L}$ est tangente ła courbe algébrique $\mathcal{C}$ en $p \in \mathcal{C} \cap \mathcal{L}$ si l'on a* $\mathrm{ord_p}(\mathcal{C}) < \mathrm{mult}_p(\mathcal{C} \cap \mathcal{L})$.

Ceci est compatible avec la définition adoptée au début du cours lorsque p est un point régulier, puisqu'en vertu des Propositions 3.18 et 3.22, on a $\mathrm{ord_p}(\mathcal{C}) = 1 < 2 \leq \mathrm{mult}_p(\mathcal{C} \cap \mathcal{L})$. Donnons des exemples d'intersections de droites avec une courbe en un point singulier qui illustreront les gains faits avec une telle définition :

Pour premier exemple, nous considérons la cubique cuspidale dans $\mathbb{A}^2(\mathbb{C})$, donnée par l'équation $x^3 - y^2 = 0$. La cubique a un point singulier en $(0, 0)$ et soit $\mathcal{L}$ une droite passant par l'origine paramétrée par $t \mapsto (\lambda_1 t, \lambda_2 t)$, avec $[\lambda_1, \lambda_2] \in \mathbb{C}P^1$. Pour trouver $\mathcal{C} \cap \mathcal{L}$, on analyse

$$(\lambda_1 t)^3 - (\lambda_2 t)^2 = t^2(\lambda_1^3 t - \lambda_2^2) = 0.$$

La multiplicité d'intersection $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L})$ est obtenue en déterminant la multiplicité de la racine $t = 0$ de ce polynôme. Il y a deux cas à considérer : si $\lambda_2 \neq 0$, cette multiplicité est égale à 2, alors que si $\lambda_2 = 0$, elle est égale à 3. Notons que nous pouvons visualiser une partie de ce qui se passe en restreignant notre attention à $\mathbb{A}^2(\mathbb{R})$: les droites avec $\lambda_2 \neq 0$ sont non-horizontales, contrairement à la droite donnée par $\lambda_2 = 0$. Par ailleurs l'ordre de

$p = (0, 0)$ sur la courbe $\mathcal{C}$ est clairement égal à 2. Donc pour toutes les droites sauf une, on a $\mathrm{ord_p}(\mathcal{C}) = \mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = 2$. La seule droite pour laquelle $\mathrm{ord_p}(\mathcal{C}) < \mathrm{mult}_p(\mathcal{C} \cap \mathcal{L})$ est la droite donnée par $\lambda_2 = 0$ et c'est la droite tangente à $\mathcal{C}$ en p.

Le second exemple est celui du folium de Descartes, d'équation affine $x^3 + y^3 - 3xy = 0$. A nouveau l'origine $p = (0, 0)$ est point singulier de $\mathcal{C}$. L'équation de $\mathcal{C}$ donne directement que l'ordre de $\mathcal{C}$ en p est 2. Une paramétrisation de la droite $\mathcal{L}$ par $t \mapsto (\lambda_1 t, \lambda_2 t)$ permet de calculer $\mathcal{C} \cap \mathcal{L}$:

$$(\lambda_1 t)^3 + (\lambda_2 t)^3 - 3\lambda_1\lambda_2 t^2 = 0.$$

Si $\lambda_1\lambda_2 \neq 0$, on a alors $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = 2 = \mathrm{ord_p}(\mathcal{C})$ et c'est la situation générique. Dans le cas où $\lambda_1\lambda_2 = 0$, on obtient $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = 3 > \mathrm{ord_p}(\mathcal{C})$ et ceci nous donne *deux* droites tangentes a la courbe $\mathcal{C}$ en p : $\lambda_1 = 0$ ainsi que $\lambda_2 = 0$, visualisées dans $\mathbb{A}^2(\mathbb{R})$ comme la droite verticale et la droite horizontale passant par l'origine.

Une différence importante entre les deux exemples où la courbe est d'ordre 2 à l'origine est que dans le premier les (deux) tangentes sont confondues puisque données par la condition $\lambda_2^2 = 0$, alors que dans le second on a deux tangentes distinctes $\lambda_1 = 0$ et $\lambda_2 = 0$. On dit qu'un point singulier d'ordre r est *simple* s'il y a r tangentes distinctes à $\mathcal{C}$ en p. C'est donc dire que le polynôme homogène $f_{(r)}$ possède r zéros distincts $[\lambda_1, \lambda_2] \in \mathbb{C}P^1$ donnant les pentes des tangentes à $\mathcal{C}$ en p.

Passons maintenant au cas des courbes algébriques projectives. En bref, l'étude des tangentes, singularités, ordre ou multiplicité d'intersection de courbes $\mathcal{C} = V(F)$ dans $\mathbb{C}P^2$ se ramène à celle faite précédemment dans le cas affine. En effet pour tout point $p = [X_0, Y_0, Z_0] \in \mathcal{C} \subset \mathbb{C}P^2$, on sait qu'au moins une des coordonnées est non-nulle et on utilise la décomposition $\mathbb{C}P^2 = \mathbb{A}^2(\mathbb{C}) \cup \mathbb{C}P^1$ selon cette coordonnée, de façon à ce que l'on ait que le point p ne soit pas sur la droite à l'infini et donc ce sera un point sur la partie affine de $\mathcal{C}$ selon cette décomposition de $\mathbb{C}P^2$. On reprend la discussion algébrique ci-dessus en utilisant un des polynôme $F(X, Y, 1), F(X, 1, Z)$ ou $F(1, Y, Z)$ selon que l'on ait $Z_0 \neq 0, Y_0 \neq 0$ ou $X_0 \neq 0$. Tous les résultats établis dans cette section ont donc leur version projective.

CHAPITRE 4

Théorie de l'intersection des courbes algébriques

1. Multiplicité d'intersection et Théorème de Bézout

Au cours du chapitre précédent, nous avons étudié le cas particulier de l'intersection entre une courbe algébrique et une droite. Que ce soit dans $\mathbb{A}^2(\mathbb{C})$ ou dans $\mathbb{C}P^2$, l'équation d'une droite nous permettait d'isoler une variable en fonction de l'autre (cas affine) ou des deux autres (cas projectif) et, en remplaçant ceci dans l'équation définissant la courbe algébrique $\mathcal{C}$, nous avons facilement réduit le problème d'intersection à de l'algèbre élémentaire des polynômes en une variable (cas affine) ou des polynômes homogènes en deux variables (cas projectif).
Nous nous nous proposons d'étudier le problème de l'intersection $\mathcal{C}_1 \cap \mathcal{C}_2$ pour deux courbes algébriques quelconques dans $\mathbb{C}P^2$. Les idées algébriques (notamment le résultant) et géométriques développées plus tôt seront essentielles pour étudier en détail $\mathcal{C}_1 \cap \mathcal{C}_2$.

Inspirés par la preuve du Lemme de Study au chapitre précédent, nous chercherons à décrire $\mathcal{C}_1 \cap \mathcal{C}_2$ en voyant $\mathbb{C}P^2$ comme une famille de droites projectives. Dans un premier effort, nous cherchons à montrer que si $\mathcal{C}_1$ et $\mathcal{C}_2$ n'ont pas de composante irréductible commune, alors $\mathcal{C}_1 \cap \mathcal{C}_2$ est constitué d'un nombre *fini* de points de $\mathbb{C}P^2$. Sans perte de généralité, supposons que $\mathcal{C}_1, \mathcal{C}_2$ ne passent pas par le point $q = [0, 0, 1]$. Pour $x = [X, Y, 0] \in \mathbb{C}P^1$, posons L_x la droite projective joignant x à q. On a dès lors

$$\mathbb{C}P^2 = \bigcup_{x \in \mathbb{C}P^1} L_x,$$

réunion de droites se rencontrant toutes en q. Pour montrer que $\mathcal{C}_1 \cap \mathcal{C}_2$ est ensemble fini, on montre que chaque droite L_x intersecte $\mathcal{C}_1 \cap \mathcal{C}_2$ un nombre fini de fois et que parmi tous les $x \in \mathbb{C}P^1$, seul un nombre fini sont tels que L_x intersecte $\mathcal{C}_1 \cap \mathcal{C}_2$. La première affirmation est claire puisque l'on sait par le chapitre précédent que $\#(L_x \cap \mathcal{C}_1) \leq \deg \mathcal{C}_1$ ou bien que $\#(L_x \cap \mathcal{C}_2) \leq \deg \mathcal{C}_2$, car $\mathcal{C}_1$ et $\mathcal{C}_2$ n'ont pas de composante en commun. Ceci qui donne bien $\#(L_x \cap (\mathcal{C}_1 \cap \mathcal{C}_2)) \leq \max\{\deg \mathcal{C}_1, \deg \mathcal{C}_2\} < \infty$. La seconde affirmation demande un

peu plus de réflexion. Soient $\mathcal{C}_1 = V(F_1)$ et $\mathcal{C}_2 = V(F_2)$ et l'on voit $F_1, F_2 \in \mathbb{C}[X,Y][Z]$:

$$F_1 = a_0 Z^m + a_1 Z^{m-1} + ... + a_m$$
$$F_2 = b_0 Z^n + b_1 Z^{n-1} + ... + a_n$$

où $a_i, b_j \in \mathbb{C}[X,Y]$ homogènes avec $\deg a_i = i$ et $\deg b_j = j$, s'ils ne sont pas identiquement nuls. Comme $q \notin \mathcal{C}_1$ et $q \notin \mathcal{C}_2$, on sait que $a_0 \neq 0$ et $b_0 \neq 0$, puisque tous les autres termes de F_1 et F_2 s'annulent en $p = [0,0,1]$. Comme $\mathcal{C}_1$ et $\mathcal{C}_2$ n'ont pas de composante commune, on sait que $R(F_1, F_2)$ n'est pas identiquement nul dans $\mathbb{C}[X,Y]$ et ce sera donc un polynôme homogène de degré $m \cdot n$. En fixant X et Y, ce qui revient à choisir une droite L_x pour $x = [X,Y,0]$, on sait alors que $F_1(X,Y,Z)$ et $F_2(X,Y,Z)$ auront un zéro en commun $\iff$ $R(F_1,F_2) = 0$ dans $\mathbb{C}$. Ceci donne les valeurs de Z (en nombre fini, pourquoi ?) telles que $\mathcal{C}_1$ et $\mathcal{C}_2$ s'intersectent le long de L_x et on a bien que $\mathcal{C}_1 \cap \mathcal{C}_2$ est un ensemble fini.

Nous pouvons raffiner le résultat de finitude de $\mathcal{C}_1 \cap \mathcal{C}_2$, en démontrant ce qui est parfois appelé la *version faible* du Théorème de Bézout :

THÉORÈME 4.1. *Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ des courbes algébriques de $\mathbb{C}P^2$ sans composante commune. Alors on a $\#(\mathcal{C}_1 \cap \mathcal{C}_2) \leq \deg \mathcal{C}_2 \cdot \deg \mathcal{C}_2$.*

DÉMONSTRATION. Comme on sait que $\mathcal{C}_1 \cap \mathcal{C}_2$ est fini, il y aura également un nombre fini de droites projectives reliant les points d'intersection entre eux. Dans la construction ci-dessus, choisissons alors q tel que $q \notin \mathcal{C}_1 \cup \mathcal{C}_2$ et afin qu'il ne soit sur aucune des droites reliant les points de $\mathcal{C}_1 \cap \mathcal{C}_2$. Il s'en suit que chaque droite L_x contient *au plus* un point d'intersection de $\mathcal{C}_1$ et $\mathcal{C}_2$. Il y a donc au plus le même nombre de points d'intersection dans $\mathcal{C}_1 \cap \mathcal{C}_2$ qu'il y a de zéros au résultant G. Puisque G est homogène de degré $\deg \mathcal{C}_1 \cdot \deg \mathcal{C}_2$, on obtient bien le résultat. □

Notons que ce théorème implique en particulier le fait remarquable suivant : si deux courbes $\mathcal{C}_1$ et $\mathcal{C}_2$ s'intersectent en *plus* de $\deg \mathcal{C}_1 \cdot \deg \mathcal{C}_2$ points, elles ont forcément une composante en commun. En particulier, pour deux courbes *irréductibles*, soit elles ont au plus $\deg \mathcal{C}_1 \cdot \deg \mathcal{C}_2$ points d'intersection, ou alors on doit avoir $\mathcal{C}_1 = \mathcal{C}_2$. Ceci donne lieu à un argument de type *local/global* de la façon suivante : pour montrer que deux courbes algébriques irréductibles coïncident, il suffit de montrer qu'autour d'un unique point quelconque, elles coïncident partout dans $\mathbb{C}P^2$

Le résultat fondamental qu'est le Théorème de Bézout établit que l'inégalité du théorème précédent est en fait toujours une égalité si l'on compte les points d'intersection avec *multiplicité*, notion que nous devons maintenant définir. Soient $\mathcal{C}_1 = V(F_1)$ et $\mathcal{C}_2 = V(F_2)$ n'ayant pas de composante commune dans $\mathbb{C}P^2$. On suppose en outre que les deux courbes ne passent pas par $q = [0, 0, 1]$ et que sur chaque droite projective passant par q il y a au plus un point d'intersection entre $\mathcal{C}_1$ et $\mathcal{C}_2$. Soit $p = [X_0, Y_0, Z_0] \in \mathcal{C}_1 \cap \mathcal{C}_2$ et $p' = [X_0, Y_0]$.

DÉFINITION 4.2. *On définit la multiplicité d'intersection locale entre $\mathcal{C}_1$ et $\mathcal{C}_2$ en $p \in \mathcal{C}_1 \cap \mathcal{C}_2$ par* $\mathrm{mult}_p(\mathcal{C}_1 \cap \mathcal{C}_2) = \mathrm{ord}_{p'} R(F_1, F_2)$.

Il y a plusieurs définitions que l'on peut faire de la notion de multiplicité. Celle donnée ici a l'avantage d'être élémentaire et ainsi nous permettre d'arriver rapidement au Théorème de Bézout. Elle a par contre le défaut de dépendre - en apparence - de certains choix que nous aurons faits dans la construction. On peut développer une approche axiomatique de $\mathrm{mult}_p(\mathcal{C}_1 \cap \mathcal{C}_2)$ qui met en valeur le fait qu'il s'agit en fait d'un invariant projectif des courbes algébriques. Ceci peut être fait de diverses manières, notamment en utilisant un peu d'Analyse complexe (voir le chapitre 14 de [**Gib**]) ou en développant une approche homologique de l'intersection (voir [**BK**]). A la fin du chapitre nous donnerons une construction proposée dans [**Kir**].
Pour l'instant nous allons supposer l'invariance sous transformations projectives de la multiplicité d'intersection et nous démontrons l'analogue de la Proposition 3.23 dans le cas de courbes de degrés quelconques :

THÉORÈME 4.3. **(Inégalité ordre-multiplicité)** *Soient $\mathcal{C}_1 = V(F)$ et $\mathcal{C}_2 = V(G)$ deux courbes de $\mathbb{C}P^2$ n'ayant pas de composante commune et $p \in \mathcal{C}_1 \cap \mathcal{C}_2$. Alors on a*

$$\mathrm{mult}_p(\mathcal{C}_1 \cap \mathcal{C}_2) \geq \mathrm{ord}_p(\mathcal{C}_1) \cdot \mathrm{ord}_p(\mathcal{C}_2).$$

DÉMONSTRATION. Soient $m = \deg F$ et $n = \deg G$ et supposons sans perte de généralité que $[0, 0, 1] \notin \mathcal{C}_1 \cup \mathcal{C}_2$ et que ce point n'est pas non plus sur une des droites reliant les points de $\mathcal{C}_1 \cap \mathcal{C}_2$. On suppose de plus que $p = [0, 1, 0]$. On se souvient que $\mathrm{mult}_p(\mathcal{C}_1 \cap \mathcal{C}_2) = \mathrm{ord}_{[0,1]} R(F, G)$, où $R(F, G)$ est vu comme un polynôme à coefficients dans $\mathbb{C}[X, Y]$. Puisque $p = [0, 1, 0]$, on considère $f(X, Y) = F(X, Y, 0)$ et $g(X, Y) = G(X, Y, 0)$ et ainsi le calcul de la multiplicité est obtenu en trouvant la multiplicité de la racine $X = 0$ de $R(f, g)$, polynôme vu comme élément de $\mathbb{C}[Y]$. Posons $\mathrm{ord}_p(\mathcal{C}_1) = r$ et $\mathrm{ord}_p(\mathcal{C}_2) = s$. On aura montré le résultat si l'on arrive à prouver que l'on peut mettre en facteur X^{rs} dans le résultant $R(f, g)$. Ceci sera accompli par des opérations astucieuses sur les lignes et colonnes de

$R(f,g)$. On peut écrire

$$f(X,Y) = [f_0X^r + f_1X^{r-1}Y + ... + f_rY^r] + f_{r+1}Y^{r+1} + f_{r_2}Y^{r+2} + ...$$
$$g(X,Y) = [g_0X^s + g_1X^{s-1}Y + ... + g_sY^s] + g_{s+1}Y^{s+1} + g_{s+2}Y^{s+2} + ...$$

où la fin de chaque expression ci-dessus n'est pas importante pour notre argument. Le résultant est alors exprimé comme

$$R(f,g) = \begin{vmatrix} f_0X^r & f_1X^{r-1} & ... & f_{r+1} & ... & f_m & ... & ... & ... & ... \\ 0 & f_0X^r & f_1X^{r-1} & f_r & ... & f_{m-1} & f_m & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ g_0X^s & g_1X^{s-1} & ... & ... & g_{s+1} & ... & ... & g_n & ... & ... \\ 0 & g_0X^s & g_1X^{s-1} & ... & ... & g_{s+1} & ... & ... & g_n & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \end{vmatrix}$$

Pour les termes de F, on multiplie la ligne 1 par X^s, la ligne 2 par X^{s-1}, ..., la ligne s par X. Ceci a pour effet de multiplier le déterminant par X^S, où $S = 1+2+3+...+s = \frac{1}{2}s(s+1)$. De même pour les termes de G, on multiplie la ligne 1 par X^r, la ligne 2 par X^{r-1}, ..., la ligne r par X. Ceci a pour effet de multiplier le déterminant par X^R, où $R = 1+2+...+r = \frac{1}{2}r(r+1)$. Une fois ceci accompli, on peut mettre en facteur : X^{r+s} dans la colonne 1, X^{r+s-1} dans la colonne 2, ..., X dans la colonne $r+s$. Donc ce déterminant a un facteur de la forme X^N, où $N = 1+2+...+(r+s) = \frac{1}{2}(r+s)(r+s+1)$. Tout ceci mis ensemble nous donne que le résultant $R(f,g)$ a un facteur de la forme X^{N-R-S}, avec $N-R-S = \frac{1}{2}(r+s)(r+s+1) - \frac{1}{2}r(r+1) - \frac{1}{2}s(s+1) = rs$, ce qui conclut la preuve. □

Passons maintenant à l' énoncé d'un des résultats majeurs de ce cours :

THÉORÈME 5. **(Théorème de Bézout)** *Pour deux courbes algébriques $\mathcal{C}_1$ et $\mathcal{C}_2$ de $\mathbb{C}P^2$ sans composante commune, on a*

$$\sum_{p \in \mathcal{C}_1 \cap \mathcal{C}_2} \text{mult}_p(\mathcal{C}_1 \cap \mathcal{C}_2) = \deg \mathcal{C}_1 \cdot \deg \mathcal{C}_2.$$

DÉMONSTRATION. En reprenant la discussion du début de la section, on a $R(F_1,F_2)$ polynôme homogène de degré $\deg \mathcal{C}_1 \cdot \deg \mathcal{C}_2$ et donc il se factorise en

$$R(F_1,F_2) = (\alpha_1X - \beta_1Y)^{k_1} \cdots (\alpha_nX - b_nY)^{k_n}.$$

Un $p' = [X_0, Y_0]$ racine de $R(F_1, F_2)$ provient d'un facteur $(\alpha_i X - \beta_i Y)^{k_i}$. Pour chaque tel p', il y a par construction un unique Z_0 tel que $p = [X_0, Y_0, Z_0] \in \mathcal{C}_1 \cap \mathcal{C}_2$. Selon la définition que nous avons faite pour la multiplicité d'intersection, on a ainsi

$$\sum_{p \in \mathcal{C}_1 \cap \mathcal{C}_2} \operatorname{mult}_p(\mathcal{C}_1 \cap \mathcal{C}_2) = \sum_{p \in \mathcal{C}_1 \cap \mathcal{C}_2} \operatorname{ord}_{p'} R(F_1, F_2) = \sum_{i=1}^{n} k_i = \deg R(F_1, F_2) = \deg \mathcal{C}_1 \cdot \deg \mathcal{C}_2.$$

□

Notons en particulier que pour des courbes ayant plusieurs composantes, c'est-à-dire que $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup ... \cup \mathcal{C}_n$ et $\mathcal{C}' = \mathcal{C}'_1 \cup \mathcal{C}'_2 \cup ... \cup \mathcal{C}'_m$ données par $F = F_1 \cdots F_n$ et $H = H_1 \cdots H_m$, cette formule implique en particulier que chacune des composantes de $\mathcal{C}$ intersecte chacune des composantes de $\mathcal{C}'$ et on a

$$\begin{aligned}\sum_{p \in \mathcal{C} \cap \mathcal{C}'} \operatorname{mult}_p(\mathcal{C} \cap \mathcal{C}') &= (\deg F_1 + ... + \deg F_n)(\deg H_1 + ... + \deg H_m) \\ &= \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\deg F_i) \cdot (\deg H_j).\end{aligned}$$

Sous cette forme on voit commen le Théorème de Bézout s'étend facilement des courbes algébriques de $\mathbb{C}P^2$ aux diviseurs de $\mathbb{C}P^2$: Si $\mathcal{C} = V(F_1^{k_1} F_2^{k_2} \cdots F_n^{k_n})$ définit le diviseur $k_1\mathcal{C}_1 + k_2\mathcal{C}_2 + ... + k_n\mathcal{C}_n$ et $\mathcal{C}' = V(H_1^{l_1} H_2^{l_2} \cdots H_m^{l_m})$ définit le diviseur $l_1\mathcal{C}'_1 + l_2\mathcal{C}'_2 + ... + l_m\mathcal{C}'_m$, alors un point dans $\mathcal{C} \cap \mathcal{C}'$ est un zéro commun d'un certain $F_i^{k_i}$ et d'un certain $H_j^{l_j}$. Mais on a $\deg F_i^{k_i} = k_i \deg F_i$ et $\deg H_j^{l_j} = l_j \deg H_j$, donc le terme dans le membre de droite de l'égalité de sommes ci-dessus est $(k_i l_j) \deg F_i \cdot \deg H_j$. De même pour le membre de gauche on a $\operatorname{mult}_p(k_i\mathcal{C}_i \cap l_j\mathcal{C}'_j) = (k_i l_j) \operatorname{mult}_p(\mathcal{C}_i \cap \mathcal{C}'_j)$, ce qui donne bien le résultat.

COROLLAIRE 4.4. *Toute courbe algébrique de $\mathbb{C}P^2$ qui est lisse, c'est-à-dire qui n'a pas de points singuliers, est forcément irréductible.*

DÉMONSTRATION. On montre la contraposée : si $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$, on a par le Théorème de Bézout que $\mathcal{C}_1 \cap \mathcal{C}_2 \neq \varnothing$. Mais chacun des points de cette intersection est un point singulier de $\mathcal{C}$ (pourquoi ?), ce qui montre que $\mathcal{C}$ ne peut être lisse si elle est réductible. □

2. Nombre de points singuliers d'une courbe algébrique

La première application du Théorème de Bézout est de mieux décrire l'ensemble $\operatorname{Sing}(\mathcal{C})$ pour une courbe algébrique quelconque $\mathcal{C}$ dans $\mathbb{C}P^2$. Nous commençons par montrer que cet ensemble est fini : une courbe algébrique définie par son polynôme minimal a toujours un nombre fini de points singuliers.

Pour la preuve de ceci, nous commençons par travailler dans $\mathbb{A}^2(\mathbb{C})$ et soient $\mathcal{C} = V(f), \mathcal{C}_x = V(\partial f/\partial x)$ et $\mathcal{C}_y = V(\partial F/\partial y)$. On note alors que $\mathrm{Sing}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}_x \cap \mathcal{C}_y$ dans $\mathbb{A}^2(\mathbb{C})$. On peut supposer que $\deg f \geq 2$ puisqu'une droite est lisse en tout point. On a alors $\deg \partial f/\partial x \geq 1$ ou encore $\deg \partial f/\partial y \geq 1$. Sans perte de généralité supposons que $\deg \partial f/\partial x \geq 1$. On a $\mathcal{C}_x$ courbe algébrique et $\mathrm{Sing}(\mathcal{C}) \subseteq \mathcal{C} \cap \mathcal{C}_x$. On aura donc fini si on montre que $\mathcal{C} \cap \mathcal{C}_x$ est un ensemble fini.
Pour ceci on a besoin du Théorème de Bézout pour les diviseurs : en effet, il se peut que $\partial f/\partial x$ ne soit pas polynôme minimal pour $\mathcal{C}_x$ (par exemple si $f = xy^2 + 1$). On doit également montrer que $\mathcal{C}$ et $\mathcal{C}_x$ n'ont pas de composante commune. Si on a $f = g \cdot h$ et $\partial f/\partial x = g \cdot h_1$, avec g irréductible, alors

$$g \cdot h_1 = h \cdot \frac{\partial g}{\partial x} + g \cdot \frac{\partial h}{\partial x},$$

et donc g divise $h \cdot \partial f/\partial x$. Si $\partial g/\partial x$ n'est pas polynôme nul, g divise h car on sait que g ne divise pas $\partial g/\partial x$. Mais ainsi on aurait que g^2 divise f, contredisant la minimalité de f. Si au contraire $\partial g/\partial x \equiv 0$, alors $g = y - a$. Mais on peut toujours choisir des coordonnées affines sur $\mathbb{A}^2(\mathbb{C})$ de façon à ce que $\mathcal{C}$ n'ait pas de composante parallèle aux axes de coordonnées, donc ce dernier cas est exclus également.
Par la version faible du Théorème de Bézout, on a immédiatement que

$$\#\,\mathrm{Sing}(\mathcal{C}) \leq \#(\mathcal{C} \cap \mathcal{C}_x) \leq \deg \mathcal{C} \cdot \deg \mathcal{C}_x < +\infty$$

pour la partie affine d'une courbe algébrique. Mais alors la partie à l'infini de $\mathcal{C}$ consiste soit en une composante donnée par la droite à l'infini (qui est lisse) ou alors il y a un nombre fini de points à l'infini et ainsi dans tous les cas de figure, on sait que $\mathrm{Sing}(\mathcal{C})$ est fini dans tout $\mathbb{C}P^2$.

Maintenant que nous savons que $\mathrm{Sing}(\mathcal{C})$ est toujours fini, nous nous attaquons au problème de trouver une borne supérieure à sa cardinalité.

PROPOSITION 4.5. *Soit $\mathcal{C}$ une courbe irréductible de degré n dans $\mathbb{C}P^2$ ayant $\{p_1, p_2, ..., p_k\}$ points singuliers. Alors*

$$\sum_{i=1}^{k} \mathrm{ord}_{p_i}(\mathcal{C})(\mathrm{ord}_{p_i}(\mathcal{C}) - 1) \leq n(n-1).$$

En particulier, on a $\#\,\mathrm{Sing}(\mathcal{C}) \leq \frac{1}{2}n(n-1)$.

DÉMONSTRATION. Puisque $\mathrm{Sing}(\mathcal{C}) \subseteq V(F) \cap V(\partial F/\partial X)$, on travaille sur l'ensemble $V(F) \cap V(\partial F/\partial X)$ et on applique le Théorème de Bézout. On suppose que $[1,0,0]$ n'est pas sur $\mathcal{C}$, donc le coefficient de X^n dans le développement de F est non-nul. La courbe $\mathcal{C}$ étant irréductible, elle ne peut avoir de facteurs en commun avec $V(\partial F/\partial X)$ puisque $\deg \partial F/\partial X = n-1 < n$.
Si p_i a un ordre k_i sur $\mathcal{C}$, alors il a un ordre au moins égal à $k_i - 1$ sur $V(\partial F/\partial X)$: toute $(k_i-2)^{\text{ème}}$ dérivée de $\partial F/\partial X$ est $(k_i-1)^{\text{ème}}$ dérivée de F et donc identiquement nulle.
En combinant la version faible du Théorème de Bézout et l'inégalité ordre-multiplicité, on a bien

$$\sum_{i=1}^{k} \mathrm{ord}_{p_i}(\mathcal{C})(\mathrm{ord}_{p_i}(\mathcal{C}) - 1) \leq n(n-1).$$

La seconde inégalité découle de la première une fois que l'on se rappelle que $\mathrm{ord}_{p_i}(\mathcal{C}) \geq 2$ $(1 \leq i \leq k)$ puisque ce sont des points singuliers de la courbe algébrique $\mathcal{C}$. □

Cette inégalité n'est cependant pas optimale. Par exemple, elle prédit qu'une conique irréductible a au plus un point singulier (alors qu'on sait qu'il n'y en a aucun par la classification projective des coniques) ou encore qu'une cubique irréductible a au plus trois points singuliers (alors que la classification complète dans $\mathbb{C}P^2$ du Chapitre 15 de [**Gib**] nous enseigne qu'il y en a au plus un). Nous allons donc chercher à améliorer la borne supérieure pour $\#\,\mathrm{Sing}(\mathcal{C})$.

Nous devons commencer par une digression sur le nombre de courbes algébriques passant par des points donnés dans $\mathbb{C}P^2$. Par exemple, par 2 points il passe exactement une courbe de degré 1 (droite) de $\mathbb{C}P^2$. De même on peut montrer (Exercice) que par 5 points de $\mathbb{C}P^2$ tels que 4 quelconques ne soient jamais alignés, il passe une unique courbe algébrique de degré 2 (conique).
Définissons $V_{k,n} = \mathbb{C}[X_0, X_1, ..., X_k]$ l'espace vectoriel des polynômes homogènes de degré (au plus) n en $k+1$ variables. On peut montrer par induction (Exercice) que l'on a $\dim V_{k,n} = \binom{n+k}{n}$. Si on considère $f, g \in V_{k,n}$ comme équivalents lorsque $f = \lambda g$ pour un certain $\lambda \in \mathbb{C}^*$, alors pour $k = 2$ ces classes d'équivalences sont représentées géométriquement par des diviseurs efficaces de degré n dans $\mathbb{C}P^2$. Par exemple le polynôme $27X^3 + 3XYZ + Z^3$ correspond à $3\mathcal{C}_1 + \mathcal{C}_2 + 3\mathcal{C}_3$, où $\mathcal{C}_1 = V(3X), \mathcal{C}_2 = V(3XYZ)$ et $\mathcal{C}_3 = V(Z)$. Notons par ailleurs que, par construction, l'espace quotient $V_{2,n}/\mathbb{C}^*$ est isomorphe à $\mathbb{C}P^N$, où $N = \binom{n+2}{n} - 1$.

Soit

$$F(X,Y,Z) = \sum_{i+j+k=n} a_{ijk} X^i Y^j Z^k$$

un polynôme homogène et $p = [p_0, p_1, p_2] \in \mathbb{C}P^2$ un point. Alors on a $p \in V(F) \iff F(p_0, p_1, p_2) = 0$ et si l'on voit les a_{ijk} comme variables, cette dernière équation donne une condition linéaire sur les $N+1$ coefficients a_{ijk} de F, donc sur les coordonnées homogènes dans $\mathbb{C}P^N$. Donc tout point de $\mathbb{C}P^2$ par lequel passe ce diviseur de degré n détermine un hyperplan de $\mathbb{C}P^N$. On peut montrer (exercice facile d'Algèbre linéaire) que l'intersection de N hyperplans dans $\mathbb{C}P^N$ contient au moins un point de $\mathbb{C}P^N$. On dit que des points $p_1, p_2, ..., p_N \in \mathbb{C}P^2$ sont en *position générale* si les hyperplans qu'ils déterminent dans $\mathbb{C}P^N$ s'intersectent exactement en un point.

LEMME 4.6. *Par $\frac{1}{2}n(n+3)$ points de $\mathbb{C}P^2$ il passe au moins une courbe algébrique de degré au plus n. Si les points sont en position générale, il y a exactement 1 diviseur efficace de degré n contenant ces points.*

DÉMONSTRATION. En effet on a l'identité algébrique $\binom{n+2}{n} - 1 = \frac{1}{2}n(n+3)$ qui est très facilement démontrée et ainsi, par ce qui précède, les $\frac{1}{2}n(n+3)$ points déterminent N hyperplans de $\mathbb{C}P^N$ et leur intersection (non-vide) correspond aux diviseurs de degré n passant par tous ces points. Ceci donne bien au moins une courbe algébrique de degré *au plus* n passant par ces points.
Si les points sont en position générale, l'intersection des N hyperplans dans $\mathbb{C}P^N$ donne lieu â un unique point de $\mathbb{C}P^N$, correspondant à un unique diviseur efficace (la condition "efficace" est nécessaire ici pour garantir l'unicité). □

Avec ces préliminaires établis, nous pouvons énoncer le résultat optimal pour ce qui est du nombre de points singuliers d'une courbe algébrique :

THÉORÈME 4.7. *Une courbe irréductible de $\mathbb{C}P^2$ possède au plus $\frac{1}{2}(n-1)(n-2)$ points singuliers.*

DÉMONSTRATION. Posons $\frac{1}{2}(n-1)(n-2) = \gamma(n)$. Les cas $n = 1$ et $n = 2$ du théorème sont connus par la géométrie élémentaire. Supposons donc que $n \geq 3$ et que la courbe $\mathcal{C}$ possède $\gamma(n)+1$ points singuliers. Nous chercherons à arriver à une contradiction. Ajoutons à ces $\gamma(n)+1$ points $n-3$ autres points sur $\mathcal{C}$ et appelons tous ces points *distingués*. On a alors $\gamma(n) + 1 + n - 3 = \frac{1}{2}(n-2)(n+1)$ points distingués. Par le Lemme précédent, on sait qu'il existe une courbe $\mathcal{C}'$ de degré $m \leq n-2$ passant par tous ces points. Intéressons-nous à la multiplicité d'intersection locale $\text{mult}_p(\mathcal{C} \cap \mathcal{C}')$: pour $p \in \mathcal{C}$ singulier, on sait que

$\mathrm{mult}_p(\mathcal{C} \cap \mathcal{C}') \geq 2$ par l'inégalité ordre-multiplicité, alors que pour les autres $n-3$ points, on a $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{C}') \geq 1$. Ceci donne

$$\sum_{p \in \mathcal{C} \cap \mathcal{C}'} \mathrm{mult}_p(\mathcal{C} \cap \mathcal{C}') \geq 2(\gamma(n)+1) + N - 3 = n(n-2) + 1.$$

Mais par ailleurs, comme $\mathcal{C}$ est irréductible par hypothèse, $\mathcal{C}'$ ne peut être composante de $\mathcal{C}$ et comme $\deg \mathcal{C}' < n$ par construction, on ne peut pas plus avoir que $\mathcal{C}$ est composante de $\mathcal{C}'$. Nous sommes dans les conditions d'application du Théorème de Bézout et on doit avoir

$$\sum_{p \in \mathcal{C} \cap \mathcal{C}'} \mathrm{mult}_p(\mathcal{C} \cap \mathcal{C}') = n \cdot m \leq n(n-2),$$

ce qui contredit l'inégalité de multiplicité obtenue il y a quelques lignes. □

COROLLAIRE 4.8. *Une courbe $\mathcal{C}$ de degré n possède au plus $\frac{1}{2}n(n-1)$ singularités, avec égalité exactement dans le cas où la courbe est réunion de n droites distinctes.*

DÉMONSTRATION. Exercice (Indice : induction finie sur le nombre de composantes irréductibles de la courbe).

□

3. Nombre de points d'inflexion d'une courbe algébrique

Revenons maintenant à la notion de *point d'inflexion* d'une courbe algébrique que nous avons brièvement introduite à la fin du Chapitre 1, maintenant que nous avons plus d'outils à notre disposition. On se souvient que pour $\mathcal{C} = V(F) \subset \mathbb{C}P^2$, on a introduit la matrice hessienne

$$H_F = \begin{pmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{pmatrix},$$

ainsi que le déterminant hessien de $\mathcal{C}$ au point $p \in \mathcal{C}$: $\mathcal{H}_F(p) = \det H_F$

DÉFINITION 4.9. *On appelle courbe hessienne de $\mathcal{C} = V(F)$ la courbe $\mathcal{H}(\mathcal{C}) = V(\mathcal{H}_F)$.*

Donnons rapidement quelques exemples :

(1) $F = X^2 + Y^2 + Z^2$ donne après un bref calcul $\mathcal{H}_F = 8$ et donc $\mathcal{H}(\mathcal{C}) = \varnothing$.

(2) $F = XY(X-Y)$ donne $\mathcal{H}_F = 0$ et donc $\mathcal{H}(\mathcal{C}) = \mathbb{C}P^2$.

(3) $F = XYZ$ implique que $\mathcal{H}_F = 2XYZ$ et donc on a $\mathcal{H}(\mathcal{C}) = \mathcal{C}$.

(4) $F = X(X^2 + Y^2 + Z^2)$ union d'une droite et d'une conique a pour Hessien $\mathcal{H}_F = 8X(3X^2 - Y^2 - Z^2)$, ce qui donne $\mathcal{H}(\mathcal{C})$ comme réunion d'une droite et une conique également.

Nous rappelons que la condition pour qu'un point régulier $p \in \mathcal{C}$ soit point d'inflexion a été donnée à la Définition 1.15 dans le cadre affine. En ayant développé la notion de multiplicité d'intersection entre une courbe et une droite, on peut réinterpréter cette condition condition en disant que $p \in \mathcal{C}$ est point d'inflexion $\iff$ $\text{mult}_p(\mathcal{C} \cap \mathcal{L}) \geq 3$, pour une certaine droite $\mathcal{L}$ passant par p. Notons qu'en vertu de la Proposition 3.18, la condition implique que $\mathcal{L}$ est droite tangente à $\mathcal{C}$ en p. On dit qu'un point d'inflexion est *simple* si l'on a exactement $\text{mult}_p(\mathcal{C} \cap \mathcal{L}) = 3$. Sous des hypothèses facilement remplies, le lemme suivant, qui découle facilement du développement de Mac Laurin pour $\mathcal{C}$, donne une forme pratique pour travailler avec le polynôme de $\mathcal{C}$:

LEMME 4.10. *Soit $\mathcal{C} = V(f) \subset \mathbb{A}^2(\mathbb{C})$ et $p = (0,0)$ point régulier avec tangente à $\mathcal{C}$ en p donnée par $\mathcal{L} = V(y)$. Alors si $k = \text{mult}_p(\mathcal{C} \cap \mathcal{L}) < \infty$, on a*

$$f(x,y) = x^k g(x) + yh(x,y),$$

où $g(0) \neq 0$ et $h(0,0) \neq 0$.

DÉMONSTRATION. La version homogène de ceci a été démontrée au chapitre 1 (Proposition 1.17), à partir de laquelle on obtient immédiatement la forme affine. □

LEMME 4.11. *Soit $\mathcal{C} \subset \mathbb{C}P^2$ une courbe algébrique irréductible de degré n. Alors tout point de $\mathcal{C}$ est point d'inflexion si et seulement si $n = 1$.*

DÉMONSTRATION. (Idée) Il est immédiat de voir que pour une courbe de degré 1 toutes les dérivées secondes sont identiquement nulles et donc $\mathcal{H}_F \equiv 0$. Par la Proposition 1.17 du premier chapitre et le fait que qu'une courbe algébrique de degré 1 n'a pas de point singulier, on obtient que tous les points de $\mathcal{C}$ sont points d'inflexion.
L'autre direction requiert plus d'idées et nous ne faisons qu'esquisser une approche ici, les détails étant fournis au Lemme 3.32 à la page 72 du livre [**Kir**]. On peut sans perte de généralité se restreindre au cas des courbes affines (pourquoi ?). Autour d'un point régulier p de $\mathcal{C} = V(f)$ dans $\mathbb{A}^2(\mathbb{C})$, le *Théorème des fonctions implicites* vu en Analyse complexe permet d'exprimer $f(x,y) = 0$ comme $y = \varphi(x)$ ou possiblement $x = \psi(y)$. Dans les deux cas on peut montrer que la condition pour n'avoir que des points d'inflexions autour de p est localement équivalente à dire que $d^2\varphi/dx^2 \equiv 0$, ou possiblement $d^2\psi/dy^2 \equiv 0$. Cela donne une forme affine pout φ ou ψ, si bien qu'autour de p la courbe $\mathcal{C}$ contien un morceau

de droite. La courbe étant irréductible, ce doit alors être une droite en vertu de la brève discussion après le Théorème 4.1. □

On peut dès lors donner le lien précis entre la notion de courbe hessienne et celle de point d'inflexion :

PROPOSITION 4.12. *Soit $\mathcal{C} = V(F) \subset \mathbb{C}P^2$ une courbe algébrique de degré n ne contenant pas de droite. Alors*

(1) *$\mathcal{H}(\mathcal{C})$ est une courbe algébrique de degré $3(n-2)$.*
(2) *$p \in \mathcal{C}$ point régulier est une point d'inflexion de $\mathcal{C} \iff p \in \mathcal{H}(\mathcal{C})$.*
(3) *$\mathcal{C}$ et $\mathcal{H}(\mathcal{C})$ n'ont pas de composante en commun.*
(4) *Si $p \in \mathcal{C} \cap \mathcal{H}(\mathcal{C})$ est point d'inflexion simple de $\mathcal{C}$, alors on a $\mathrm{ord}_p(\mathcal{H}(\mathcal{C})) = 1$ et $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{H}(\mathcal{C})) = 1$.*

DÉMONSTRATION. Pour (1) puisque $\mathcal{C}$ ne contient pas de droite, on a que $\mathcal{H}_F$ n'est pas identiquement nul en vertu du lemme précédent. Alors $\mathcal{H}(\mathcal{C})$ est donnée comme lieu d'annulation d'un polynôme, en vertu de la définition de $\mathcal{H}_F$ et c'est donc bien une courbe algébrique. La partie (2) a déjà été montré dans la discussion sur les cubiques (Proposition 1.17). On en déduit une preuve de (3) puisque si $\mathcal{C}$ et $\mathcal{H}(\mathcal{C})$ avaient une composante commune, alors le Lemme 4.11 et sa preuve impliqueraient que $\mathcal{C}$ contient une droite, contredisant une hypothèse de l'énoncé. La partie (4) requiert un peu plus de travail. On se place dans les hypothèses du Lemme 4.10 adaptées au contexte des courbes projectives : $\mathcal{C}$ est donnée par un polynôme de la forme

$$F(X,Y,Z) = X^k G(X,Z) + Y H(X,Y,Z),$$

et la tangente $\mathcal{L}$ à $\mathcal{C}$ en $p = [0,0,1]$ donnée comme $V(Y)$. Pour avoir $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{L}) = k$, on doit avoir $G(0,1) \neq 0$ et pour que p ne soit pas point singulier, on doit avoir $H(0,0,1) \neq 0$ (autrement F les dérivées s'annulent toutes en $[0,0,1]$). Alors la courbe $\mathcal{H}(\mathcal{C})$ est donnée comme lieu d'annulation du polynôme

$$\mathcal{H}_F(X,Y,Z) = X^{k-2}\widetilde{G}(Y,Z) + Y\widetilde{H}(X,Y,Z),$$

où l'on doit avoir $\widetilde{G}(0,1) \neq 0$ car $\mathcal{H}_F$ ne peut avoir que $k-2$ facteurs en X puisque F en a exactement k. Il s'ensuit que la multiplicité d'intersection entre $\mathcal{C}$ et $\mathcal{H}(\mathcal{C})$ satisfait en général $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{H}(\mathcal{C})) = k-2$. Dans le cas particulier où p est un point d'inflexion simple, on a $k = 3$ et donc $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{H}(\mathcal{C})) = 1$. L'inégalité ordre-multiplicité (Théorème 4.3) implique alors que $\mathrm{ord}_p(\mathcal{H}(\mathcal{C})) = 1$ tel que demandé. □

On peut alors combiner ceci au Théorème de Bézout et obtenir une borne supérieure sur le nombre de points d'inflexion d'une courbe algébrique dans $\mathbb{C}P^2$:

THÉORÈME 4.13. *Une courbe algébrique de degré n dans $\mathbb{C}P^2$ ne contenant pas de droite possède au plus $3n(n-2)$ points d'inflexion. il y a exactement $3n(n-2)$ points d'inflexion lorsque $\mathcal{C}$ ne possède pas de point singulier et que les points d'inflexion sont simples.*

DÉMONSTRATION. La première partie découle directement de la version faible de Bézout et de la partie (1) de la dernière proposition. Si en outre il n'y a pas de points singuliers pour $\mathcal{C}$ ont sait que l'intersection avec $\mathcal{H}(\mathcal{C})$ ne consistera qu'en des points d'inflexions et si ceux-ci sont simples, on aura bien $3n(n-2) = \deg \mathcal{C} \cdot \deg \mathcal{H}(\mathcal{C})$ points distincts dans $\mathcal{C} \cap \mathcal{H}(\mathcal{C})$. □

Regardons par exemple les points d'inflexion de la cubique de Fermat donnée par $F(X,Y,Z) = X^3 + Y^3 + Z^3$. On calcule facilement $\mathcal{H}_F = 6^3XYZ$, si bien que la courbe hessienne $\mathcal{H}(\mathcal{C})$ consiste des droites $X = 0$, $Y = 0$ et $Z = 0$. Sur la droite projective $Z = 0$ on a alors 3 points d'inflexion $[1,-1,0], [\xi,-1,0]$ et $[\xi^2,-1,0]$, où ξ est racine cubique de l'unité. Il en sera de même pour les deux autres droites, à chaque fois les 3 points d'inflexion étant obtenus en permutant la variable annulée. Ceci nous donne donc 9 points d'inflexion pour la cubique de Fermat, le maximum possible. On notera en outre les 3 points d'inflexion réels $[1,-1,0], [0,1,-1]$ et $[1,0,-1]$ qui sont alignés.

On peut voir cet exemple dans le contexte général des cubiques non-singulières :

COROLLAIRE 4.14. *Une cubique non-singulière possède forcément 9 points d'inflexion distincts.*

DÉMONSTRATION. Pour une tangente d'inflexion $\mathcal{L}$ on sait que l'on a $\text{mult}_p(\mathcal{C} \cap \mathcal{L}) \geq 3$. Comme $\mathcal{C}$ est de degré 3, il s'agit en fait d'une égalité si bien que tout point d'inflexion sur une cubique est simple. Comme $\mathcal{C}$ est non-singulière, on a que $\mathcal{C} \cap \mathcal{H}(\mathcal{C})$ ne contient que des points d'inflexion. On a la conclusion voulue en faisant appel au Théorème de Bézout. □

4. Une approche axiomatique de la multiplicité d'intersection

Pour la preuve du Théorème de Bézout, nous nous sommes contentés d'une définition de la multiplicité d'intersection locale entre deux courbes $\mathcal{C}_1$ et $\mathcal{C}_2$ qui faisait appel à des

choix particuliers et coordonnées sur $\mathbb{C}P^2$ et nous n'avons pas démontré que cette multiplicité est un invariant de $\mathcal{C}_1$ et $\mathcal{C}_2$. Nous nous tournons maintenant vers une approche axiomatique de la multiplicité d'intersection, exposée dans le livre [**Kir**], qui mettra un point final à cette discussion.

Dans $\mathbb{C}P^2$ soient $\mathcal{C} = V(F)$ une courbe algébrique de degré n et $\mathcal{D} = V(G)$ une courbe algébrique de degré m. Nous définissons ci-dessous un objet $I_p(\mathcal{C}, \mathcal{D})$ ayant les propriétés suivantes :

(1) Il est donné par 6 axiomes.

(2) Les axiomes suffisent pour le calculer (ceci donne l'unicité).

(3) Les axiomes sont préservés par les transformations projectives.

(4) Le nombre $\text{mult}_p(\mathcal{C}, \mathcal{D})$ introduit auparavant satisfait ces 6 axiomes.

Axiomatique pour $I_p(\mathcal{C}, \mathcal{D})$:

(1) $I_p(\mathcal{C}, \mathcal{D}) = I_p(\mathcal{D}, \mathcal{C})$.

(2) $I_p(\mathcal{C}, \mathcal{D}) = +\infty$ si p est sur une composante commune de $\mathcal{C}$ et $\mathcal{D}$. Autrement, $I_p(\mathcal{C}, \mathcal{D})$ est un entier positif ou nul.

(3) $I_p(\mathcal{C}, \mathcal{D}) = 0 \iff p \notin \mathcal{C} \cap \mathcal{D}$.

(4) Si $\mathcal{L}_1$ et $\mathcal{L}_2$ sont des droites projectives distinctes, alors $I_p(\mathcal{L}_1, \mathcal{L}_2) = 1$ pour l'unique $p \in \mathcal{L}_1 \cap \mathcal{L}_2$.

(5) $I_p(\mathcal{C}_1 \cup \mathcal{C}_2, \mathcal{D}) = I_p(\mathcal{C}_1, \mathcal{D}) + I_p(\mathcal{C}_2, \mathcal{D})$.

(6) Si on pose $\xi = V(F \cdot H + G)$, où $\deg H = m - n$, alors $I_p(\mathcal{C}, \mathcal{D}) = I_p(\mathcal{C}, \xi)$

On montre que (1)–(6) suffisent pour calculer $I_p(\mathcal{C}, \mathcal{D})$. Puisque ces 6 propriétés ne dépendent pas des coordonnées de $p \in \mathbb{C}P^2$, on suppose que $p = [0, 0, 1]$. On peut en outre se ramener au cas où les polynômes F et G sont irréductibles en appliquant (1) et (5). Il y a deux cas faciles. Si $I_p(\mathcal{C}, \mathcal{D}) = 0$, la condition (3) dit que $p \notin \mathcal{C} \cap \mathcal{D}$ et alors les 5 autres axiomes sont trivialement satisfaits. De même si $I_p(\mathcal{C}, \mathcal{D}) = +\infty$, l'axiome (2) dit que $F = F_1 \cdot F_2$ et $G = F_1 \cdot G_1$, et alors tous les axiomes sont satisfaits facilement.

On peut donc supposer pour la suite que $I_p(\mathcal{C}, \mathcal{D}) = k > 0$. L'idée de la preuve est de procéder par induction sur k, en supposant que tout $I_p(\mathcal{C}, \mathcal{D})$ inférieur à k peut être calculé de manière unique à partir de (1)–(6). Considérons les polynômes $F(X, 0, 1)$ et $G(X, 0, 1)$

dans $\mathbb{C}[X]$, de degrés respectivement r et s. Par l'axiome (1) on peut supposer que $r \leq s$.

Cas I : Supposons que $r = 0$. Alors $F(X, 0, 1)$ polynôme constant et donc $F(X, 0, 1) \equiv 0$ car $F(0, 0, 1) = 0$ ($p \in \mathcal{C} \cap \mathcal{D}$ puisque $I_p(\mathcal{C}, \mathcal{D}) = k > 0$). Puisque F est homogène, on a $F(X, 0, Z) \equiv 0$ dans $\mathbb{C}[X, Z]$. Ceci signifie que $F(X, Y, Z)$ est de la forme

$$F(X, Y, Z) = Y \cdot R(X, Y, Z),$$

pour un certain polynôme homogène R. On peut par ailleurs décomposer le polynôme homogène G comme

$$G(X, Y, Z) = G(X, 0, Z) + Y \cdot S(X, Y, R) = X^q \cdot T(X, Z) + Y \cdot S(X, Y, Z),$$

où $T(X, Z)$ satisfait $T(0, 1) \neq 0$ et $q > 0$ car $G(0, 0, 1) = 0$. La condition $T(0, 1) \neq 0$ signifie que $[0, 0, 1] \notin V(T)$ et donc par (3) on a $I_p(V(Y), V(T)) = 0$. Par ailleurs, par l'axiome (4) on sait que $I_p(V(Y), V(X)) = 1$. En appliquant l'axiome (5) on obtient

$$I_p(\mathcal{C}, \mathcal{D}) = I_p(V(Y), \mathcal{D}) + I_p(V(R), \mathcal{D}).$$

Ensuite en appliquant l'axiome (6) à $V(Y), V(G)$ et $V(G - YS)$, on trouve

$$I_p(V(Y), \mathcal{D}) = I_p(V(Y), V(X^q \cdot T(X, Z)).$$

En utilisant à nouveau (5) ainsi que le facteur $X^q \cdot T(X, Z)$ à répétition, il en découle que

$$I_p(V(Y), \mathcal{D}) = q \cdot I_p(V(Y), V(X)) + I_p(V(Y), V(T)) = q.$$

Ceci permet d'écrire

$$I_p(\mathcal{C}, \mathcal{D}) = q + I_p(V(R), \mathcal{D}),$$

et cette équation combinée à $q > 0$ donne $I_p(V(R), \mathcal{D}) < I_p(\mathcal{C}, \mathcal{D}) = k$ alors par l'hypothèse d'induction on sait que $I_p(V(R), \mathcal{D})$ est calculable de manière unique à partir de (1)–(6). Il s'en suit que $I_p(\mathcal{C}, \mathcal{D})$ lui-même est calculé uniquement à partir de (1)–(6).

Cas II : Supposons maintenant que $r > 0$. Dans ce cas $F(X, 0, 1)$ et $G(X, 0, 1)$ sont des polynômes non-nuls dans $\mathbb{C}[X]$ (rappel : $r \leq s$) et en les multipliant chacun par une constante, on les rend moniques en X. Définissons un nouveau polynôme homogène : si $n = \deg F$ et $m = \deg G$, soit

$$U(X, Y, Z) = Z^{n+s-r} \cdot G(X, Y, Z) - X^{s-r} \cdot Z^m \cdot F(X, Y, Z).$$

Notons que l'on ne peut avoir $U(X,Y,Z) \equiv 0$ car, par hypothèse, F et G sont irréductibles et distincts. Ce polynôme a en outre la propriété que le polynôme $U(X,0,1) \in \mathbb{C}[X]$ a un degré $t < s$ puisque

$$U(X,0,1) = G(X,0,1) - X^{s-r} \cdot F(X,0,1)$$

est différence de deux polynômes moniques de même degré s. Par l'axiome (6), on a $I_p(V(F),V(U)) = I_p(V(F),V(Z^{n+s-r} \cdot G))$ et donc

$$I_p(V(F),V(U)) = (n+s-r) \cdot I_p(V(F),V(Z)) + I_p(V(F),V(G)).$$

Le terme $I_p(V(F),V(Z))$ est nul puisque $p = [0,0,1] \notin V(Z)$, donc la conclusion de ce Cas II est que, pour calculer $I_p(\mathcal{C},\mathcal{D})$, on peut remplacer F et G par F et U, avec

$$\deg U(X,0,1) = t < s = \deg G(X,0,1).$$

En répétant cette étape pour F et U (si $r \leq t$) ou pour U et F (si $t < r$), après un nombre fini de fois, on se ramène au Cas I où $r = 0$, cas qui a déjà été traité.

Dans notre plan de preuve pour l'invariance projective de la multiplicité d'intersection, la partie la plus facile est de voir que le nombre $I_p(\mathcal{C},\mathcal{D})$ défini par les axiomes (1)–(6) est préservé par une transformation projective. Ceci repose sur le fait qu'une transformation projective $\tau\colon \mathbb{C}P^2 \to \mathbb{C}P^2$ préserve : la propriété d'intersection de deux courbes, le degré des courbes algébriques et la décomposition en composantes.

Il nous reste donc à voir que pour $p = [X_0,Y_0,Z_0]$ le nombre $\mathrm{mult}_p(\mathcal{C} \cap \mathcal{D})$ introduit précédemment comme

$$\mathrm{mult}_p(\mathcal{C} \cap \mathcal{D}) = \mathrm{ord}_{[X_0,Y_0]}(R(F,G))$$

satisfait les axiomes (1)–(6) :

(1) Découle de la propriété générale de changement de signe du déterminant lorsque l'on intervertit deux lignes, ce qui donne $R(F,G) = \pm R(G,F)$ et donc ne change pas les racines ni leurs multiplicités.
(2) Découle de la propriété du résultant voulant que $R(F,G) \equiv 0$ dans $\mathbb{C}[X,Y] \iff \mathcal{C}$ et $\mathcal{D}$ ont une composante en commun.
(3) On a $p = [a,b,c] \in \mathcal{C} \cap \mathcal{D} \iff F(X,b,c)$ et $G(X,b,c)$ ont une racine commune en $a \iff R(F,G) \in \mathbb{C}[X,Y]$ s'annulle pour $Y = b$ et $Z = c \iff (bZ - cY)$ est facteur de $R(F,G) \iff \mathrm{mult}_p(\mathcal{C} \cap \mathcal{D}) > 0$.

(4) C'est un calcul facile de résultant avec un déterminant 2×2 donnant $\text{mult}_p(\mathcal{L}_1, \mathcal{L}_2) = 1$ pour $p = \mathcal{L}_1 \cap \mathcal{L}_2$.
(5) et (6) Découlent de propriétés purement algébriques du résultant (voir [**Kir**] Section 3.1) : $R(F, G_1 \cdot G_2) = R(F, G_1) \cdot R(F, G_2)$ (donc les multiplicités s'additionnent) et $R(F, F \cdot H + G) = R(F, G)$ (opération sur les lignes).

5. Une application en Géométrie projective classique

PROPOSITION 4.15. *Soient deux courbes $\mathcal{C}$ et $\mathcal{D}$ de degré respectivement n et m, avec $n \geq m$, qui s'intersectent exactement en $n \cdot m$ points. On suppose que $n \cdot k$ de ces points sont sur une courbe algébrique irréductible $\mathcal{E}$ de degré $k < m$. Alors on peut trouver une courbe algébrique de degré au plus $n - k$ contenant les $n(m - k)$ autres points de $\mathcal{C} \cap \mathcal{D}$.*

DÉMONSTRATION. Soient $\mathcal{C} = V(F), \mathcal{D} = V(G)$ et $\mathcal{E} = V(H)$ et choisissons $[a, b, c] \in \mathcal{E}$ qui ne soit pas sur $\mathcal{C} \cap \mathcal{D}$. Alors la courbe $\mathcal{E}'$ de degré au plus n définie par

$$G(a, b, c)F(X, Y, Z) - F(a, b, c)G(X, Y, Z) = 0$$

intersecte $\mathcal{E}$ en au moins $n \cdot k + 1$ points : les $n \cdot k$ points de $\mathcal{C} \cap \mathcal{D}$ qui sont sur $\mathcal{E}$ et le point $[a, b, c]$. Par la version faible de Bézout, ceci implique que $\mathcal{E}'$ et $\mathcal{E}$ ont une composante en commun et cette composante doit être tout $\mathcal{E}$, puisque $\mathcal{E}$ est supposée irréductible. Au niveau polynomial, on a donc

$$G(a, b, c)F(X, Y, Z) - F(a, b, c)G(X, Y, Z) = H(X, Y, Z) \cdot K(X, Y, Z)$$

pour un certain polynôme K de degré au plus $n-k$. Alors les $n(m-k)$ points de $\mathcal{C} \cap \mathcal{D}$ qui ne sont pas sur $\mathcal{E} = V(H)$ sont sur la courbe de degré au plus $n-k$ définie par $K(X, Y, Z) = 0$ tel que voulu. □

On déduit de ce résultat sur les courbes algébriques le résultat classique de Pascal :

THÉORÈME 4.16. *Les paires de côtés opposés d'un hexagone de $\mathbb{C}P^2$ qui est inscrit dans une conique irréductible se rencontrent en 3 points alignés.*

DÉMONSTRATION. Soit $\mathcal{H}$ l'hexagone donné par $V(L_1 L_2 \cdots L_6)$ où $L_i = 0$ représente le $i^{\text{ème}}$ côté de $\mathcal{H}$. Les côtés opposés de l'hexagone sont $\{L_1, L_4\}$, $\{L_2, L_5\}$ et $\{L_3, L_6\}$. Définissons $\mathcal{C} = V(L_1 L_3 L_5)$ et $\mathcal{D} = V(L_2 L_4 L_6)$. Ce sont deux courbes de degré 3 chacune, s'intersectant par construction exactement en $3 \times 3 = 9$ points : les 6 sommets de $\mathcal{H}$ ainsi que les 3 points d'intersection des côtés opposés dans $\mathcal{H}$. Par hypothèse les 6 points sont sur

une courbe irréductible de degré 2. La proposition précédente appliquée au cas $n = 3 = m$ et $k = 2$ nous donne alors que les 3 points restants de $\mathcal{C} \cap \mathcal{D}$ sont sur une courbe de degré au plus $3 - 2 = 1$, c'est-â-dire que les 3 points sont alignés. □

Bibliographie

[BK] E. Brieskorn, H. Knörrer, *Plane algebraic curves*, Birkhäuser Verlag (1986)

[Fis] G. Fischer, *Plane algebraic curves*, Student Math. Library AMS (2001)

[Gib] C. G. Gibson, *Elementary geometry of algebraic curves*, Cambridge University Press (1998)

[Kir] F. Kirwan, *Complex algebraic curves*, Cabridge University Press (1992)

[Lan] S. Lang, *Algebra*, Springer Verlag (2004)

[vdW] B. van der Waerden, *Algebra*, Springer Verlag (1990)

[Wal] R. Walker, *Algebraic curves*, Springer Verlag (1978)