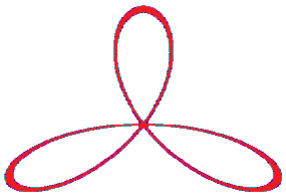
COURBES ALGEBRIQUES PLANES

Loïc Gaillard

9 mai 2012



Encadré par Catherine Labeye-Voisin

Table des matières

Introduction L'objet de cet article est de présenter une preuve du théorème de Bézout sur les courbes algébriques planes, qui stipule que deux courbes algébriques s'intersectent exactement en autant de points que le produit des degrés qui des polynômes qui les définissent. Nous allons donc parler d'ensembles algébriques sous différents aspects afin de pouvoir établir cet énoncé et d'en comprendre la démonstration :
Nous allons devoir définir les ensembles algébriques d'un $\mathbb{K}$ espace vectoriel où $\mathbb{K}$ est algébriquement clos, définir les multiplicités d'intersections de courbes affines pour que le résultat reste vrai lorsque les polynômes considérés ont des facteurs multiples, et définir les points d'intersection à l'infini pour créer les points d'intersections manquants dans $\mathbb{K}^2$.

Pour commencer, une approche très générale des ensembles algébriques dans le cadre de la géométrie algébrique classique : on étudiera des ensembles de zéros de polynômes de $\mathbb{K}[X_1, ..., X_n]$ où $\mathbb{K}$ est algébriquement clos. Nous énoncerons des propriétés diverses de ces ensembles algébriques.
Ce sera l'objet de la section 1, nous introduirons l'idéal d'un ensemble de points, quelques résultats concernant les radicaux d'idéaux, et en particulier le Nullstellensatz de Hilbert, théorème crucial de l'étude des ensembles algébriques.

Pour que le théorème de Bézout soit vrai en toute généralité, on doit aussi donner un sens aux multiplicités d'intersection de deux courbes, on introduira pour cela des anneaux locaux, les anneaux à valuation discrète, les anneaux de fonctions en section 2. On en déduira un isomorphisme important pour le théorème de Bézout.

Nous allons ensuite appliquer cela au cas du plan $\mathbb{K}^2$ et des polynômes de $\mathbb{K}[X, Y]$. Nous énoncerons des résultats géométriques en section 3 comme le nombre d'intersections de deux courbes en un point.

Ensuite nous parlerons des points à l'infini et introduirons les espaces projectifs afin de leur donner un sens mathématique en section 4.

Pour finir nous appliquerons les résultats des 4 sections précédentes aux courbes planes projectives, et cela permettra d'établir le théorème de Bézout.

La plupart de ce que j'ai écrit est tiré de "Algebraic curves" de William Fulton [1].

1 Ensembles algébriques

1.1 Préliminaires

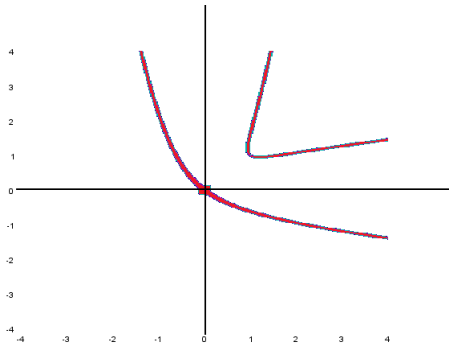
Commençons par introduire quelques notions qui serviront fréquemment :
Soit A un anneau.
On note $A[X_1, ..., X_n]$ l'anneau des polynômes à n indéterminées à coefficients dans A.
Soit $\mathbb{K}$ un corps, on note $\mathbb{K}(X_1, ..., X_n)$ l'ensemble de ses fractions rationnelles.
Si S est une partie de $\mathbb{K}[X_1, ..., X_n]$ l'idéal engendré par S est noté (S)
$\mathbb{K}^n$ est vu comme un espace affine.
Soit $P \in \mathbb{K}[X_1, ..., X_n]$, on dit que $x \in \mathbb{K}^n$ est un zéro de P si $x = (x_1, ..., x_n)$ vérifie $P(x_1, ..., x_n) = 0$.
Un anneau A est noethérien si ses idéaux sont de type fini. Cette définition équivaut à dire que toute suite croissante d'idéaux de A est stationnaire.

Définition 1. *Soit* $P \in \mathbb{K}[X_1, ..., X_n]$.

$$V(P) = \{x \in \mathbb{K}^n, P(x) = 0\}$$

C'est l'hypersurface de P notée V(P)
Une hypersurface de $\mathbb{K}^2$ *est appelée une courbe algébrique.*

Exemple. *Courbe V(P) pour* $P = X^3 + Y^3 - 2X^2Y^2$



Définition 2. *Soit* $S \subset \mathbb{K}[X_1, ..., X_n]$.

$$V(S) = \{x \in \mathbb{K}^n, \forall P \in S, P(x) = 0\}$$

V(S) est l'ensemble algébrique de S.
$V(S) = \bigcap_{P \in S} V(P)$

Proposition 1. *(i) Si I=(S) Alors V(I)=V(S)*
(ii) Soit $(I_\alpha)_{\alpha \in A}$ *collection d'idéaux, alors* $V(\bigcup_{\alpha \in A} I_\alpha) = \bigcap_{\alpha \in A} V(I_\alpha)$
(iii) Soient I,J idéaux, $I \subset J \Rightarrow V(J) \subset V(I)$
(iv) Soient P,Q polynômes, $V(PQ) = V(P) \cup V(Q)$
(v) $V(0) = \mathbb{K}^n; V(1) = \emptyset$

Démonstration. (iii) : Soit $x \in V(J)$, alors $\forall P \in J, P(x) = 0$. Soit $Q \in I \subset J$ alors $Q \in J$ donc Q(x)=0. Ainsi $x \in V(I)$.

(i) : Par (iii) $V(I) \subset V(S)$. Pour l'autre inclusion, un élément $P \in I$ s'écrit $P = \sum_{k=1}^{N} \alpha_k S_k$ avec $\forall k, S_k \in S$. $\forall x \in V(S)$, $P(x) = \sum_{k=1}^{N} \alpha_k S_k(x) = 0$. Donc V(I)=V(S).

(ii) : $x \in V(\bigcup_{\alpha \in A} I_\alpha) \Leftrightarrow \forall P \in \bigcup_{\alpha \in A} I_\alpha, P(x) = 0$

$\Leftrightarrow \forall \alpha \in A, \forall P \in I_\alpha, P(x) = 0 \Leftrightarrow x \in \bigcap_{\alpha \in A} V(I_\alpha)$

(iv) : Le produit PQ est nul en x si et seulement si P ou Q s'annule en x. Donc
$x \in V(PQ) \Leftrightarrow x \in V(P)$ ou $x \in V(Q) \Leftrightarrow x \in V(P) \cup V(Q)$

(v) : $\{x \in \mathbb{K}^n, 0 = 0\} = \mathbb{K}^n$

$\{x \in K^n, 1 = 0\} = \emptyset$ □

1.2 Idéal d'un ensemble de points

Définition 3. *Soit $X \subset K^n$,*

$$I(X) = \{P \in \mathbb{K}[X_1, ..., X_n], \forall x \in X, P(x) = 0\}$$

I(X) est l'idéal de X.

Proposition 2. *(i) I(X) est un idéal de $\mathbb{K}[X_1, ..., X_n]$*
(ii) $X \subset Y \Rightarrow I(Y) \subset I(X)$
(iii) $I(\emptyset) = \mathbb{K}[X_1, ..., X_n]$ et $I(\mathbb{K}^n) = (0)$
(iv) $I(\{(x_1, ..., x_n)\}) = (X_1 - x_1, ..., X_n - x_n)$
(v) $\forall X \subset \mathbb{K}^n, I(V(I(X))) = I(X)$; $\forall J \subset \mathbb{K}[X_1, ..., X_n], V(I(V(J))) = V(J)$

Démonstration. (i) :$\forall x \in \mathbb{K}^n$, on a :
$ev_x : \mathbb{K}[X_1, ..., X_n] \longrightarrow \mathbb{K}$ est un morphisme d'anneaux
· $P \longmapsto P(x)$
$I(X) = \bigcap_{x \in X} Ker(ev_x)$ c'est donc un idéal comme intersection d'idéaux.

(ii) :$I(Y) = \bigcap_{x \in Y} Ker(ev_x) = \bigcap_{x \in X} Ker(ev_x) \cap \bigcap_{x \in Y \setminus X} Ker(ev_x) \subset I(X)$

(iii) : $\{P \in \mathbb{K}[X_1, ..., X_n], \forall x \in \emptyset, P(x) = 0\} = \mathbb{K}[X_1, ..., X_n]$
$\{P \in \mathbb{K}[X_1, ..., X_n], \forall x \in \mathbb{K}^n, P(x) = 0\} = \{0\}$

(iv) : $(X_1 - x_1, ..., X_n - x_n) \subset I(\{x\})$ est évident car chaque $X_i - x_i$ est nul en x, donc les polynômes de l'idéal engendré aussi. Soit $P \in I(\{x\})$. P vu comme un polynôme de $\mathbb{K}[(X_i)_{i<n}]$, on le divise par $(X_n - x_n)$, $P = (X_n - x_n)Q_n + R_n$, on recommence en divisant $R_n \in \mathbb{K}[(X_i)_{i<n-1}]$ par $(X_{n-1} - x_{n-1})$, et ainsi de suite, on divise R_k par $(X_{k-1} - x_{k-1})$. Alors $P = \sum_{k=1}^{n} (X_k - x_k)Q_k + R_1$. $R_1 = 0$ sinon P ne s'annule pas en x. Ainsi $P \in ((X_1 - x_1), ..., (X_n - x_n))$. Donc $I(\{x\}) = ((X_1 - x_1), ..., (X_n - x_n))$.

(v) : On traite juste la première égalité, l'autre se montre de façon similaire.
$I(V(I(X))) = \bigcap_{x \in V(I(X))} Ker(ev_x) \subset I(X)$ par (ii) car $X \subset V(I(X))$
Soit $P \in I(X)$, soit $x \in V(I(X))$, P(x)=0 par définition de V(). Donc on a l'autre inclusion. Ainsi I(V(I(X)))=I(X). □

Cela établit une correspondance entre les ensembles algébriques et les idéaux provenant d'un ensemble de points :
Si X est un ensemble algébrique, V(I(X))=X
Si J provient d'un ensemble de points, I(V(J))=J
On va avoir bientôt une caractérisation plus précise des idéaux en question.

Définition 4. *Soit J un idéal, on note $\sqrt{J}$ le radical de J :*

$$\sqrt{J} = \{P \in \mathbb{K}[X_1, ..., X_n], \exists N \in \mathbb{N}, P^N \in J\}$$

.
On dit que J est radiciel si $J = \sqrt{J}$

Exemple. *Un idéal premier est radiciel :*
si $P^N \in \mathfrak{p}$ alors $P \in \mathfrak{p}$ ou $P^{N-1} \in \mathfrak{p}$, par récurrence on a donc $P \in \mathfrak{p}$
$(P) = ((X-1)(Y-2))$ est radiciel dans $\mathbb{K}[X,Y]$
$(Q) = ((X-1)^2(Y-2))$ n'est pas radiciel dans $\mathbb{K}[X,Y]$
$\sqrt{(P)} = (P) = \sqrt{(Q)}$. Cette figure représente V(P) ou V(Q). Les radicaux de (P) et (Q) sont

égaux, leurs hypersurfaces aussi ; on verra plus tard (avec le Nullstellensatz) que ce résultat est toujours vrai : les courbes géométriques sont caractérisées par le radical des idéaux.

La propriété suivante permet de mieux se figurer la structure du radical d'un idéal. J'ai trouvé et adapté la preuve de cette propriété dans [2]

Proposition 3.

$$\sqrt{J} = \bigcap_{\mathfrak{p}\ premier \supset J} \mathfrak{p}$$

Démonstration. On note I= $\bigcap_{\mathfrak{p}\ premier \supset J} \mathfrak{p}$
Soit $R \in \sqrt{J}, \forall \mathfrak{p}$ premier $\supset J$ $R^N \in J \subset \mathfrak{p}$.
Ainsi $\forall \mathfrak{p}, R^N \in \mathfrak{p}$ qui est radiciel. Donc $\forall \mathfrak{p}$ premier $\supset J, R \in \mathfrak{p}$.
On a donc $\sqrt{J} \subset I$

L'autre inclusion est plus difficile et nécessite l'axiome du choix dans un anneau quelconque. Elle va être vraie ici sans le lemme de Zorn car $\mathbb{K}[X_1, ..., X_n]$ est noethérien, ce que nous établirons plus tard. On va le prouver par contraposée.

Soit $R \notin \sqrt{J}$. Soit S=$\{R^k, k \in \mathbb{N}\}$. Par hypothèse on a donc S et J disjoints.
Étape 1 : $\exists \mathfrak{p}$ premier contenant J vérifiant aussi $\mathfrak{p} \cap S = \emptyset$:
$E = \{\mathfrak{a}\ ideal \subset \mathbb{K}[X_1, ..., X_n], J \subset \mathfrak{a},\ \mathfrak{a} \cap S = \emptyset\}$. E admet un élément maximal pour

l'inclusion dans E, sinon on peut construire une suite strictement croissante d'idéaux de $\mathbb{K}[X_1, ..., X_n]$ par :
$J_{k+1} \supsetneq J_k$ puisque J_k n'est pas maximal dans E. Cela contredit $\mathbb{K}[X_1, ..., X_n]$ est noethérien.
Soit $\mathfrak{p}$ un élément maximal de E. Montrons qu'il est premier :
Si $PQ \in \mathfrak{p}, P \notin \mathfrak{p}, Q \notin \mathfrak{p}$, on a
$I \subset \mathfrak{p} \subsetneq \mathfrak{p} + (P)$
$I \subset \mathfrak{p} \subsetneq \mathfrak{p} + (Q)$.
Donc ces idéaux intersectent S par maximalité de $\mathfrak{p}$.
Soient P_0, Q_0 dans ces intersections, $P_0Q_0 \in S$. Mais P_0Q_0 est aussi dans $\mathfrak{p}$:
$P_0Q_0 = (Pa_1 + \gamma_1)(Qa_2 + \gamma_2) = PQa_1a_2 + a_1P\gamma_2 + a_2Q\gamma_1 + \gamma_1\gamma_2$. Les 4 termes sont dans $\mathfrak{p}$, donc $\mathfrak{p} \cap S \neq \emptyset$ ce qui contredit l'hypothèse $\mathfrak{p} \in E$.
Donc $\mathfrak{p}$ est premier, n'intersecte pas S et contient J.
Étape 2 : On conclut en disant que R était supposé dans $A \setminus \sqrt{J}$ donc aucune de ses puissances ne peut être dans J. Si R était dans I, en particulier on aurait $R \in \mathfrak{p}$ où $\mathfrak{p}$ est un idéal comme construit dans l'étape 1. Donc on contredirait l'hypothèse $\mathfrak{p} \cap S = \emptyset$.
Donc $R \notin \sqrt{J} \Rightarrow R \notin I$, ou encore :

$$I \subset \sqrt{J}$$

□

1.3 Propriétés des ensembles algébriques

Lemme. *Soit A un anneau noethérien, Alors A[X] est noethérien.*

Démonstration. Étape 1 : soit I idéal de A[X]. L'ensemble J des coefficients dominants des polynômes de I forme un idéal de A :
Soient $j_1, j_2 \in J$, $a \in A$. j_1 est le coefficient de P_1, j_2 le coefficient de P_2, on va dire $d_1 = deg(P_1) > deg(P_2) = d_2$.
$X^{d_1-d_2}P_2 + P_1 \in I$, son coefficient dominant est $j_1 + j_2$ donc $j_1 + j_2 \in J$. De plus $aP_1 \in I$ donc $aj_1 \in J$.

Étape 2 : famille génératrice des éléments de faible degré.
J idéal de A donc il est engendré par $(a_1, .., a_p)$, qui sont les coefficients de $(P_1, ..., P_p)$. Soit $N = \max_{1 \leq k \leq n} deg(P_k)$.
On note maintenant J_m l'ensemble des coefficients dominants des polynômes de I de degrés inférieur à m.
Pour m≤N on note $\{P_{m,j}, j \leq N_m\}$ une famille de polynômes générant J_m.
Soit I'=($\{(P_i)_{1 \leq i \leq p}, (P_{m,j})_{1 \leq j \leq N_m}\}_{1 \leq m \leq N}$)
$I' \subset I$ est clair.
Soit $P \in I \setminus I'$ qu'on prend de degré minimal. Si deg(P)>N, $\exists (Q_k)_{1 \leq k \leq p} \subset I'$, P et $S = \sum_{k=1}^{p} Q_k P_k$ ont le même coefficient dominant. Alors $P - X^a S$ est de degré inférieur et cela contredit la minimalité de P.
Si deg(P)≤N, les $(F_{m,j})$ permettent de baisser son degré de la même façon. L'ensemble I\I' est donc vide. I est donc de type fini.

□

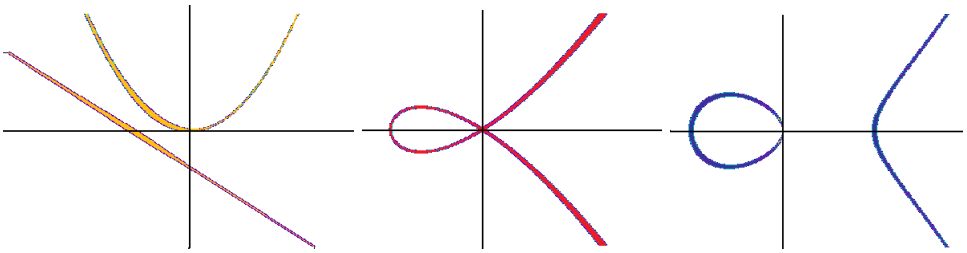
Corollaire. $\mathbb{K}[X_1, ..., X_n]$ *est noethérien.*

Démonstration. $\mathbb{K}[X_1, ..., X_n] = \mathbb{K}[X_1, ..., X_{n-1}][X_n]$. Par récurrence sur n, le résultat tombe par le fait $\mathbb{K}[X_1]$ est principal donc noethérien. □

Théorème 1. *Tout ensemble algébrique est l'intersection d'un nombre fini d'hypersurfaces.*

Démonstration. Soit V un ensemble algébrique. $V = V(I)$ pour un certain idéal I de $\mathbb{K}[X_1, ..., X_n]$. Comme $\mathbb{K}[X_1, ..., X_n]$ est noethérien, $I = (P_1, ..., P_k)$. Donc $V(I) = \bigcap_{i=1}^{k} V(P_i)$. C'est donc une intersection d'hypersurfaces. □

Définition 5. *Soit V un ensemble algébrique. On dit que V est irréductible si il n'est pas la réunion de 2 sous ensembles algébriques stricts.*
V irréductible $\Leftrightarrow \forall (V_1, V_2), V = V_1 \cup V_2 \Rightarrow (V_1 = V$ ou $V_2 = V)$, V_1 et V_2 étant des ensembles algébriques.
Un ensemble algébrique irréductible est appelé une variété algébrique (affine).



Exemple. *$P = (X + Y + 1)(Y - X^2)$. La figure à gauche représente V(P). Celle ci est l'union de $V(X+Y+1)$ (droite) et $V(Y-X^2)$ (parabole). Donc V(P) n'est pas irréductible.*
$Q = Y^2 - X^2(X + 1)$. V(Q) est représentée au milieu, elle est irréductible.
$R = Y^2 - X(X^2 - 1)$. V(R) est représentée à droite, elle est tout aussi irréductible même si elle semble dis-connexe :
mes représentations sont dans $\mathbb{R}^2$ qui n'est pas algébriquement clos, donc on pourrait penser que la courbe est réductible mais ce n'est pas le cas. Aucune des deux composantes connexes n'est possible à écrire de la forme V(R).

Proposition 4. *V est irréductible $\Leftrightarrow$ I(V) est un idéal premier.*

Démonstration. Soit V une hypersurface. Si $I(V)$ n'est pas premier, alors $I(V) = (P_1, ..., P_k)$ et l'un des P_j n'est pas irréductible.
Quitte à échanger l'ordre des P_j, on choisit $P_1 = PQ$, de sorte que
$V(PQ) \cap \bigcap_{i=2}^{k} V(P_i) = V$. On note

$$V_1 = V(P) \cap \bigcap_{i=2}^{k} V(P_i)$$

$$V_2 = V(Q) \cap \bigcap_{i=2}^{k} V(P_i)$$

$$V = V(I(V)) = V(PQ) \cap \bigcap_{i=2}^{k} V(P_i) = (V(P) \cup V(Q)) \cap \bigcap_{i=2}^{k} V(P_i) = V_1 \cup V_2$$

$V_1 \neq V$ et $V_2 \neq V$. Donc V n'est pas irréductible.
Si $V = V_1 \cup V_2$ est une décomposition non triviale, $P \in I(V_1) \setminus I(V)$ et $Q \in I(V_2) \setminus I(V)$, alors $PQ \in I(V)$. En effet, $x \in V \Rightarrow (x \in V_1$ et $P(x) = 0)$ ou $(x \in V_2$ et $Q(x) = 0)$. Donc I(V) n'est pas premier. □

Théorème 2. *Soit V un ensemble algébrique. Alors V se décompose de façon unique en ensembles algébriques irréductibles.*

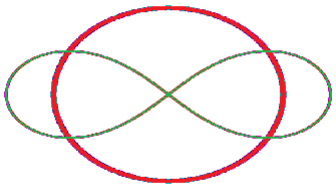
Démonstration. Existence : Soit V un ensemble algébrique. Si V n'est pas irréductible, il a une décomposition non triviale $V = V_1 \cup V_1'$.
On itère le procédé : si les deux sont irréductibles on a une écriture de V en union d'irréductibles, sinon, quitte à les échanger, on dit que V_1 est réductible, on l'écrit $V_1 = V_2 \cup V_2'$, et de même $V_n = V_{n+1} \cup V_{n+1}'$
Si $\forall n \in \mathbb{N}, V_n$ est réductible, on crée alors une suite d'idéaux : $(I(V_n))_{n\in\mathbb{N}}$ telle que $V_{n+1} \supsetneq V_n$. Mais une suite strictement croissante d'idéaux ne peut pas exister car $\mathbb{K}[X_1, ..., X_n]$ est noethérien. Donc V est décomposable en union d'irréductibles.
Unicité : supposons que $V = \bigcup_{i=1}^{k} V_i = \bigcup_{j=1}^{m} W_j$ admet deux décompositions irréductibles. Alors $\forall i$
$V_i = V_i \cap V = V_i \cap \bigcup_{j=1}^{m} W_j = \bigcup_{j=1}^{m} (V_i \cap W_j)$. Par ailleurs $V_i \cap W_j$ est un sous ensemble algébrique de W_j irréductible. Donc il est vide ou égal à W_j. Ainsi $V_i = W_{j(i)}$. Donc une permutation des éléments permet de conclure $k = m$ et $\forall i, V_i = W_i$. □

Proposition 5. *Soient P et Q polynômes de $\mathbb{K}[X, Y]$ sans facteurs en commun. Alors $V(P, Q) = V(P) \cap V(Q)$ est un ensemble fini.*

Démonstration. Comme P et Q n'ont pas de facteur en commun dans $\mathbb{K}[X, Y]$ ils n'en ont pas non plus dans $\mathbb{K}(X)[Y]$:
Supposons $U \in \mathbb{K}(X)[Y]$, $U \mid P$ et $U \mid Q$. $\exists V \in \mathbb{K}[X]$ de degré minimal, $VU \in \mathbb{K}[X, Y]$. Alors $VU \mid VP$ et $VU \mid VQ$ dans $\mathbb{K}[X, Y]$. Comme V est de degré minimal, VU est premier avec V dans $\mathbb{K}[X, Y]$. D'après le lemme de Gauss, $VU \mid P$ et $VU \mid Q$, ce qui est impossible. Donc Ils n'ont pas de facteur commun dans $\mathbb{K}(X)[Y]$.

$\mathbb{K}(X)[Y]$ est principal, donc pgcd(P,Q)=1 se traduit par $P\mathbb{K}(X)[Y] + Q\mathbb{K}(X)[Y] = (1)$.
Donc $\exists (R, S) \in \mathbb{K}(X)[Y], RP + SQ = 1$.

On multiplie par les dénominateurs (en X) et on a :
$\exists (A, B) \in \mathbb{K}[X, Y], AP + BQ = D$. $D \in \mathbb{K}[X]$
Si $(x, y) \in V(P, Q)$, alors $D(x) = 0$. Donc x prend un nombre fini de valeurs.
Avec un même raisonnement y prend un nombre fini de valeurs.
Ainsi V(P,Q) est fini. □



Exemple. *Intersection entre $V((X^2 + Y^2) - 1)$ (cercle) et $V((X^2 + Y^2)^2 - (X^2 - Y^2))$ (lemniscate). On ne voit que 4 points d'intersection.*

Corollaire. *Si P est irréductible de $\mathbb{K}[X, Y]$ et V(P) infini, alors I(V(P))=(P). De plus V(P) est irréductible.*

Démonstration. Soit $Q \in I(V(P))$, V(P,Q) est infini donc $P \mid Q$. Cela donne l'inclusion non triviale. Comme (P) est un idéal premier I(V(P)) est premier. Donc V(P) est irréductible. □

Corollaire. *Les ensembles algébriques irréductibles de* $\mathbb{K}[X,Y]$ *sont*
(i) $\mathbb{K}^2$
(ii) $\emptyset$
(iii)Les $\{(x,y)\}$ *du plan*
(iv) Les ensembles de la forme V(P) infinis tels que P irréductible.

Démonstration. Soit V variété algébrique. Si V n'est ni un point, ni trivial, alors $I(V)$ est un idéal premier. Donc $\exists P$ irréductible, $I(V) = (P)$. En effet si $Q \in I(V) \setminus (P)$, V(P,Q) est un ensemble fini, ce qu'on a exclu car V n'est pas un point, ni vide. □

1.4 Nullstellensatz

Lemme. *Soit* $\mathbb{K}$ *algébriquement clos.*
Les idéaux maximaux de $\mathbb{K}[X_1,...,X_n]$ *sont de la forme* $(X_1 - a_1, ..., X_n - a_n)$.

Démonstration. Ces idéaux sont maximaux car $ev_{(a_1,...,a_n)}$ est un morphisme surjectif de $\mathbb{K}[X_1,...,X_n]$ sur $\mathbb{K}$ dont le noyau est $(X_1 - a_1, ..., X_n - a_n)$. Ainsi $\mathbb{K}[X_1,...,X_n]/(X_1 - a_1, ..., X_n - a_n) \simeq \mathbb{K}$. Le premier est donc un corps, ainsi l'idéal est maximal.

Réciproque : On le montre quand $\mathbb{K}$ est indénombrable : soit $\mathfrak{m}$ idéal maximal de $\mathbb{K}[X_1,...,X_n]$. $\mathbb{K}[X_1,...,X_n]/\mathfrak{m}$ est un $\mathbb{K}$ espace vectoriel engendré par une famille dénombrable :

$$\mathbb{K}[X_1,...,X_n]/\mathfrak{m} =< \{\prod_{i=1}^{n} \overline{X_i}^{k_i}, (k_i)_{1\leq i\leq n} \in \mathbb{N}^n\} >$$

Donc toute famille libre est de cardinal au plus dénombrable.
On note $\mathbb{L} = \mathbb{K}[X_1,...,X_n]/\mathfrak{m}$. Comme $\mathbb{K}$ est algébriquement clos, une extension algébrique de $\mathbb{K}$ est triviale. Si on suppose par l'absurde $\mathbb{L} \supsetneq \mathbb{K}$ alors c'est une extension non algébrique qui admet donc des éléments non algébriques sur $\mathbb{K}$. Soit x un élément non algébrique de $\mathbb{L}$. On a donc :

$$\begin{array}{ll} \mathbb{K}[T] \to \mathbb{L} & \text{est injective donc} \quad \mathbb{K}(T) \to \mathbb{L} \quad \text{est injective.} \\ P \mapsto P(x) & \qquad\qquad \frac{P}{Q} \mapsto \frac{P(x)}{Q(x)} \end{array}$$

On utilise $\mathbb{L}$ est un corps pour définir la seconde application. On a donc une "inclusion" $\mathbb{K}(T)$ dans $\mathbb{L}$. Une famille libre de $\mathbb{K}(T)$ est donc envoyée vers une famille libre de $\mathbb{L}$. On aura donc une contradiction si on trouve une famille libre indénombrable de $\mathbb{K}(T)$.
$\{\frac{1}{(T-z)}_{z\in\mathbb{K}}\}$ est une telle famille :
$\sum_{i=1}^{p} \lambda_i \frac{1}{(T-z_i)} = 0 \Rightarrow \sum_{i=1}^{p} \lambda_i \prod_{j\neq i}(T - z_i) = 0$ et l'évaluation en z_i permet de voir $\lambda_i = 0$.
Donc la famille est libre et indénombrable quand $\mathbb{K}$ est indénombrable. Donc l'extension $\mathbb{L}$ ne peut pas être transcendante, elle est donc triviale (égale à $\mathbb{K}$). Il s'agit de montrer que l'idéal est de la forme $(X_1 - a_1, ..., X_n - a_n)$
L'image par l'isomorphisme de $\overline{X_i}$ est notée a_i. Alors $\forall i, (X_i - a_i) \in \mathfrak{m}$.
$(X_1 - a_1, ..., X_n - a_n) \subset \mathfrak{m}$ et $(X_1 - a_1, ..., X_n - a_n)$ est maximal.
Donc $\mathfrak{m} = (X_1 - a_1, ..., X_n - a_n)$ □

Théorème 3. *(Nullstellensatz 1.0 de Hilbert) Soit J idéal non trivial de* $\mathbb{K}[X_1, ..., X_n]$ *avec* $\mathbb{K}$ *algébriquement clos. Alors*

$$V(J) \neq \emptyset$$

.

Démonstration. Par le théorème de Krull, il existe un idéal maximal $\mathfrak{m}$ contenant J. $\mathfrak{m}$ est de la forme $(X_1 - a_1, ..., X_n - a_n)$, donc $(a_1, ..., a_n) \in V(\mathfrak{m}) \subset V(J)$. Donc $V(J) \neq \emptyset$ □

Théorème 4. *(Nullstellensatz 2.0 de Hilbert) Soit J idéal de* $\mathbb{K}[X_1, ..., X_n]$ *avec* $\mathbb{K}$ *algébriquement clos. Alors*

$$I(V(J)) = \sqrt{J}$$

.

Démonstration. $\sqrt{J}$ s'annule sur V(J) donc on a $\sqrt{J} \subset I(V(J))$.
Soit $Q \in I(V(J))$. On veut montrer que pour un certain $N \in \mathbb{N}$, $Q^N \in J$. $J = (P_1, .., P_m)$, on sait que Q s'annule là où chacun des P_i s'annule, on veut en déduire que $Q^N = \sum_{i=1}^{m} A_i P_i$ pour une famille $(A_i)_{1 \leq i \leq m}$ de polynômes.
Soit $J' = (P_1, .., P_m, X_{n+1}Q - 1) \subset \mathbb{K}[X_1, ..., X_n, X_{n+1}]$. Comme Q s'annule partout où les P_i sont nuls, $V(J') = \emptyset$. On applique le Nullstellensatz 1.0, on voit alors que J' est trivial.
$J' = \mathbb{K}[X_1, ..., X_{n+1}] = (1)$. Donc $\exists (A_i)_{0 \leq i \leq m} \in \mathbb{K}[X_1, ..., X_{n+1}]^{m+1}$,
$1 = \sum_{i=1}^{m} A_i(X_1, .., X_{n+1})P_i + A_0(X_1, ..., X_{n+1})(X_{n+1}Q - 1)$
On remplace X_{n+1} par $1/Q$ dans l'équation, puis en multipliant par une certaine puissance de Q assez grande pour que les fonctions soient des polynômes, on obtient :
$Q^N = \sum_{i=1}^{m} A_i(X_1, .., \frac{1}{Q})Q^N P_i + A_0(X_1, ..., \frac{1}{Q})(1 - 1)Q^N$
$Q^N = \sum_{i=1}^{m} A'_i P_i$. Donc $Q^N \in J$. □

Corollaire. *Si J est radiciel, I(V(J))=J*

Le Nullstellensatz de Hilbert permet d'établir une correspondance bijective entre les idéaux radiciels de $\mathbb{K}[X_1, ..., X_n]$ et les courbes algébriques de $\mathbb{K}^n$.

$$\begin{array}{c} \{\text{idéaux radiciels}\} \longleftrightarrow \{\text{ensembles algébriques}\} \\ I \longmapsto V(I) \\ I(V) \longleftarrow V \end{array}$$

Corollaire. *I premier ⇒ V(I) est irréductible.*

Démonstration. I=I(V(I)) car I est premier donc radiciel. Donc I(V(I)) est premier, ainsi V(I) est irréductible.

□

Corollaire. $P = \prod_{i=1}^{r} P_i^{n_i}$ *décomposition en irréductibles, alors* $V(P) = \bigcup_{i=1}^{r} V(P_i)$

Démonstration. V(P)=V(I(V(P))) ; $I(V(P)) = \sqrt{(P_1^{n_1} P_r^{n_r})} = (P_1 P_2 ... P_r)$. Donc

$$V(P) = \bigcup_{i=1}^{r} V(P_i)$$

□

Corollaire. *Soit $\mathbb{K}$ algébriquement clos et I idéal de $\mathbb{K}[X_1, ..., X_n]$.*
$V(I)$ est fini $\Leftrightarrow \mathbb{K}[X_1, ..., X_n]/I$ est de dimension finie. Dans ce cas,

$$\sharp V(I) \leq dim_{\mathbb{K}}\mathbb{K}[X_1, ..., X_n]/I$$

.

Lemme. *Soient $(x_1, ..., x_m)$ des points distincts de $\mathbb{K}^n$. Alors $\exists (P_1, .., P_m) \in \mathbb{K}[X_1, ..., X_n]^m$,*

$$\forall j, i, P_j(x_i) = \delta_i^j$$

Démonstration. (lemme) : Soit V ensemble algébrique et $y \notin V$. Alors $I(V \cup \{y\}) \neq I(V)$.
Donc $\exists P$ nul sur V non nul en y.
On divise P par sa valeur en y, on a donc P nul sur V et valant 1 en y.
On choisit de cette façon une famille de polynômes $(P_i)_{1 \leq i \leq m}$, $\forall i, P_i(x_i) = 1$ et P_i s'annule sur $V_i = \bigcup_{j \neq i} \{x_j\}$. □

Démonstration. (corollaire) : ($\Leftarrow$) Soient $(x_1, ..., x_m)$ une famille de points de V(I) distincts.
On prend une famille $(P_i)_{1 \leq i \leq m}$ comme dans le lemme.
Si on suppose $\sum_{i=1}^{m} \lambda_i \overline{P_i} = 0$ alors $\sum_{i=1}^{m} \lambda_i P_i \in I$. Donc $\forall j, \sum_{i=1}^{m} \lambda_i P_i(x_j) = 0$.
Par définition des P_i, cette somme vaut λ_j.
Donc $\forall j, \lambda_j = 0$. Comme les $\overline{P_i}$ sont linéairement indépendants dans $\mathbb{K}[X_1, ..., X_n]/I$ on a donc $m \leq dim_{\mathbb{K}}\mathbb{K}[X_1, ..., X_n]/I$.
($\Rightarrow$) On suppose $V(I) = \{x_1, ..., x_m\}$. Par le Nullstellensatz, $I(V(I)) = \sqrt{I}$. Pour chaque x_i on note $(a_{i,j})_{1 \leq j \leq n}$ ses coordonnées dans $\mathbb{K}^n$.
$\forall j$, on appelle $P_j = \prod_{i=1}^{m} (X_j - a_{i,j})$. On voit bien que P_j s'annule à la fois sur tous les x_i. Donc $P_j \in I(V(I))$.
Ainsi, $\exists N \in \mathbb{N}, \forall j, P_j^N \in I$. Alors $\overline{P_j^N} = \overline{0}$, donc $\overline{X_j}^{rN}$ est une combinaison $\mathbb{K}$-linéaire de $\{1, \overline{X_j}, ..., \overline{X_j}^{rN-1}\}$. Ainsi $\mathbb{K}[X_1, ..., X_n]/I$ est engendré par les ensembles
$\{X_i^{m_i}, 1 \leq i \leq n, 0 \leq m_i \leq rN - 1\}$ donc il est de dimension finie sur $\mathbb{K}$ □

2 Variétés affines

On rappelle qu'une variété affine est un ensemble algébrique irréductible. On verra plus tard des variétés projectives d'où le qualificatif "affine".
Dans cette partie, $\mathbb{K}$ est fixé et algébriquement clos. n est fixé et les variétés qu'on considère sont dans $\mathbb{K}^n$.

2.1 Anneau local et valuation....discrète !

Définition 6. *Soit V une variété affine. $\Gamma(V) = \mathbb{K}[X_1, ..., X_n]/I(V)$ est appelé l'anneau coordonné de V. Les éléments de $\Gamma(V)$ sont des classes de polynômes égaux sur V*

$\Gamma(V)$ est intègre car I(V) est premier.
$\mathcal{F}(V, \mathbb{K})$ est l'ensemble des fonctions de V dans $\mathbb{K}$. C'est une algèbre pour le produit des fonctions. $\mathbb{K}$ s'identifie aux fonctions constantes.

Définition 7. *Une fonction f de $\mathcal{F}(V, \mathbb{K})$ est polynômiale si*
$\exists P \in \mathbb{K}[X_1, ..., X_n]$, $\forall x \in V, P(x) = f(x)$.

On remarque que P,Q déterminent la même fonction sur V si et seulement si $\overline{P} = \overline{Q}$ dans $\Gamma(V)$. Donc $\Gamma(V)$ peut s'identifier aux fonctions polynômiales sur V.
On peut généraliser la notion d'application polynômiale pour $f : V \to W$ où $V \subset \mathbb{K}^n$ et $W \subset \mathbb{K}^m$ sont des variétés algébriques. On dit que f est polynômiale si chacune de ses coordonnées est polynômiale.
On note $\mathbb{K}(V)$ le corps des fractions de $\Gamma(V)$, appelé le corps des factions rationnelles sur V.
On dit que $f \in \mathbb{K}(V)$ est définie au point x si $\exists (p, q) \in \Gamma(V)^2$, $f = p/q$ et $q(x) \neq 0$.

Définition 8. *L'anneau local $\mathcal{O}_x(V)$ de V au point $x \in V$ est défini par :*
$\mathcal{O}_x(V) = \{f \in \mathbb{K}(V)$ *définies au point x* $\}$

$$\mathbb{K} \subset \Gamma(V) \subset \mathcal{O}_x(V) \subset \mathbb{K}(V)$$

Proposition 6. $\Gamma(V) = \bigcap_{x \in V} \mathcal{O}_x(V)$

Démonstration. $(\subset)$: Si f est polynômiale sur V, elle est définie en chaque point de V.
$(\supset)$: Soit f définie en tout point de V.
Soit $J = \{P \in \mathbb{K}[X_1, ..., X_n], f\overline{P} \in \Gamma(V)\}$. J est un idéal de $\mathbb{K}[X_1, ..., X_n]$ contenant $I(V)$. En effet $Q \in I(V) \Rightarrow \overline{Q}f \equiv 0_{\mathbb{K}(V)} \in \Gamma(V)$.
V(J) est inclus dans l'ensemble des pôles de f : soit $x \in V(J)$ on écrit $f = \frac{p}{q}$ localement, avec $q(x) \neq 0$. Donc $q \in J$ car $p \in \Gamma(V)$, et $x \in V(J)$ donc $q(x) = 0$ (impossible). Ainsi $V(J) = \emptyset$, par le Nullstellensatz, on a donc $J = \mathbb{K}[X_1, ..., X_n] = (1)$. Donc $f \in \Gamma(V)$. □

On a utilisé le lemme suivant, qui servira encore par la suite :

Lemme. *si $f \in \mathcal{O}_x(V)$ alors $\exists Q \in \mathbb{K}[X_1, ..., X_n], Q(x) \neq 0$ tel que $fQ \in \Gamma(V)$*

Définition 9. *L'idéal maximal de V en x noté* $\mathfrak{m}_x(V)$ *est le noyau de*
$ev_x : \mathcal{O}_x(V) \to \mathbb{K}$
$\cdot \qquad f \longmapsto f(x)$.

Définition 10. *On se place dans le cadre d'anneaux intègres :*
Un anneau local est un anneau avec un unique idéal maximal.
Un anneau à valuation discrète est un anneau local noethérien d'idéal maximal principal.

Proposition 7. *Soit A un anneau.*
$A \setminus A^\times$ *est un idéal* $\Leftrightarrow$ *A admet un unique idéal maximal* $\mathfrak{m}$ *contenant tous les idéaux non triviaux de A.*
En particulier pour A=$\mathcal{O}_x(V)$, $\mathfrak{m}_x(V)$ *est un tel idéal ; donc* $\mathcal{O}_x(V)$ *est local.*

Démonstration. ($\Rightarrow$) Soit $\mathfrak{m} = A \setminus A^\times$. On voit bien qu'il contient tous les idéaux non triviaux car il contient tout sauf les unités.
($\Leftarrow$) Soit $a \in A \setminus A^\times$. $(a) \subset \mathfrak{m}$ donc $a \in \mathfrak{m}$. Comme $\mathfrak{m}$ est maximal il ne contient pas d'unités donc $\mathfrak{m} = A \setminus A^\times$ qui est donc un idéal.
Pour A=$\mathcal{O}_x(V)$, $A^\times = \{f, f(x) \neq 0\}$ donc $A \setminus A^\times = \mathfrak{m}_x(V)$. □

Proposition 8. *Soit J idéal de* $\mathcal{O}_x(V)$, *et* $(P_1, ..., P_m)$ *générateurs de* $\pi^{-1}(J \cap \Gamma(V))$ *comme idéal de* $\mathbb{K}[X_1, ..., X_n]$. *Alors*

$$J = P_1\mathcal{O}_x(V) + ... + P_m\mathcal{O}_x(V)$$

En particulier $\mathcal{O}_x(V)$ *est noethérien.*

Démonstration. $x \in V$, $\Gamma(V) \subset \mathcal{O}_x(V)$.
$\Gamma(V)$ est la projection de $\mathbb{K}[X_1, ..., X_n]$ par
$\pi : \mathbb{K}[X_1, ..., X_n] \to \mathbb{K}[X_1, ..., X_n]/I(V)$. $J \cap \Gamma(V)$ correspond (par π^{-1}) avec un idéal de $\mathbb{K}[X_1, ..., X_n]$ contenant I(V) qu'on note par le même nom J.
Donc si J est un idéal de $\mathcal{O}_x(V)$ il correspond à un unique idéal de $\mathbb{K}[X_1, ..., X_n]$. On l'engendre avec une famille $(P_1, ..., P_m)$ de polynômes. On a clairement la première inclusion :
$P_1\mathcal{O}_x(V) + ... + P_m\mathcal{O}_x(V) \subset \mathcal{O}_x(V)$ car les polynômes sont définis au point x.
Pour un polynôme P_i on note $p_i = \overline{P_i}$ classe dans $\Gamma(V)$ de P_i.
Soit $f \in J$, $\exists Q \in \mathbb{K}[X_1, ..., X_n], Q(x) \neq 0$ et $Qf \in \Gamma(V)$.
$Qf = \sum_{i=1}^{m} a_i p_i$ où les a_i sont des polynômes. Comme Q non nulle en x on a
$\forall i, \frac{a_i}{Q} \in \mathcal{O}_x(V)$. Donc $f = \sum_{i=1}^{m} (a_i/Q)p_i$. On identifie les p_i aux polynômes P_i car vus comme des fonctions ils sont similaires. Ainsi

$$f \in P_1\mathcal{O}_x(V) + ... + P_m\mathcal{O}_x(V)$$

. □

Proposition 9. *On a une correspondance bijective :*
$\{$*idéaux premiers de* $\mathcal{O}_x(V)\} \leftrightarrow \{$*variétés affines de V passant par x*$\}$

Démonstration. Étape 1 : Correspondance bijective :
{idéaux premiers de $\mathcal{O}_x(V)$} $\longleftrightarrow$ {idéaux premiers $\subset \mathfrak{m}_x(V)$ de $\Gamma(V)$}
Soit $I \subset \mathfrak{m}_x(V)$ un idéal premier de $\Gamma(V)$. Il est engendré par les polynômes $(P_1, .., P_m)$. On appelle $I' = P_1\mathcal{O}_x(V) + ... + P_m\mathcal{O}_x(V) \subset \mathcal{O}_x(V)$.

Les P_i sont nuls en x, donc $I' \subset \mathfrak{m}_x(V)$ donc I' est non trivial. La primalité de I confère à I' une structure d'idéal premier.
Réciproquement, soit $I \subset \mathcal{O}_x(V)$ idéal premier. $I = f_1\mathcal{O}_x(V) + ... + f_r\mathcal{O}_x(V)$.
I est non trivial donc inclus dans $\mathfrak{m}_x(V)$. Donc $\forall i, f_i(x) = 0$.
On écrit $f_i = P_i/Q_i$ (écriture unique). On a donc $P_i(x) = 0$. Alors
$P_i = Q_i f_i \in \Gamma(V) \cap \mathfrak{m}_x(V)$.
Soit $I' = \sum_{i=1}^{r} P_i\Gamma(V)$, c'est un idéal premier de $\Gamma(V)$ contenu dans $\mathfrak{m}_x(V)$.
De plus on a $I' \cap \Gamma(V) = I$ et $(I \cap \Gamma(V))' = I$, ce sont donc des bijections.

Étape 2 : Correspondance bijective :
{idéaux premiers $\subset \mathfrak{m}_x(V)$ de $\Gamma(V)$} $\longleftrightarrow$ {variétés de V passant par x}
Soit $\overline{I}$ idéal de $\Gamma(V)$, $\overline{I} \subset \mathfrak{m}_x(V)$.
$I = \pi^{-1}(\overline{I})$ est un idéal de $\mathbb{K}[X_1, ..., X_n]$ contenant $I(V)$ (correspondance bijective par un théorème classique d'algèbre). On applique V :
$V(\mathfrak{m}_x(V) \cap \mathbb{K}[X_1, ..., X_n]) \subset V(I) \subset V(I(V)) = V$
On a déjà prouvé que $V(\mathfrak{m}_x(V) \cap \mathbb{K}[X_1, ..., X_n]) = \{x\}$ car l'idéal est maximal. Ainsi, V(I) est un sous ensemble algébrique de V contenant x et est irréductible.
Soit W variété affine avec $\{x\} \subset W \subset V$.
Alors $I(W) \supset I(V)$ donc correspond à un idéal J de $\mathbb{K}[X_1, ..., X_n]/I(V)$.
J est premier car W irréductible $\Rightarrow$ I(W)=J premier dans $\mathbb{K}[X_1, ..., X_n]$ et donc dans $\mathbb{K}[X_1, ..., X_n]/I(V)$.
A fortiori, dans $\mathcal{O}_x(V)$, le localisé de J est premier car il est inclus dans $\mathfrak{m}_x(V)$ donc non trivial dans $\mathcal{O}_x(V)$.
I(V(I))=I par le Nullstellensatz car I est premier ; V(I(V))=V prouvé en section 1.
On a donc établi une bijection. □

Proposition 10. *A est un anneau à valuation discrète* $\Leftrightarrow$

$$\exists T \in A, \forall z \in A, \exists! u \in A^\times, \exists! N \in \mathbb{N}, z = uT^N$$

Définition 11. *Un tel élément $T \in A$ est alors appelé un paramètre uniformisant de A. Il est unique à multiplication par un inversible près.*
L'unique $N(z)$ répondant à cette description est l'ordre de z dans A.

Démonstration. On note $\mathfrak{m}$ l'idéal maximal, alors soit T tel que $\mathfrak{m} = (T)$.
existence : Si z est une unité c'est une relation triviale car T non inversible. Soit z non unité de A. $z \in (T)$ donc $z = z_1T$. on itère le procédé, de même $z_k = z_{k+1}T$. Si aucun des z_k n'est inversible alors on a une suite strictement croissante d'idéaux $(z) \subsetneq (z_1) \subsetneq (z_2) \subsetneq ... \subsetneq (z_k) \subsetneq ...$ c'est impossible car A est noethérien. Donc on a l'existence.
unicité : $uT^m = vT^k \Rightarrow uT^{m-k} = v \in A^\times$. Cela impose m=k car T est non inversible. Il en suit u=v.
D'après ce qu'on suppose, on voit que $A \setminus A^\times = (T)$. Donc A est un anneau local d'idéal maximal (T) principal. A est noethérien et même principal car ses idéaux sont de la forme (T^m). □

On a prouvé au passage que un anneau local A dont l'idéal $\mathfrak{m}$ est principal est noethérien si et seulement si il est principal.

2.2 Homogénéité, produits d'idéaux

Définition 12. *$P \in \mathbb{K}[X_1, ..., X_n]$ est homogène si $\forall \lambda \in \mathbb{K}, P(\lambda X) = \lambda^k P(X)$*
k est alors le degré de P.
Si $P \in \mathbb{K}[X_1, ..., X_{n+1}]$ est homogène on définit $P_* \in \mathbb{K}[X_1, ..., X_n]$ par :
$P_*(X_1, ..., X_n) = P(X_1, ..., X_n, 1)$; c'est le dés-homogénéisé de P.
Réciproquement, $p \in \mathbb{K}[X_1, ..., X_n]$, l'homogénéisé p^* de p est :

$p^*(X_1, ..., X_{n+1}) = X_{n+1}^d p_0 + ... + X_{n+1} p_{d-1} + p_d$ *où d est le degré de p et $p = \sum_{i=0}^{d} p_i$ est la décomposition de p en homogènes.*

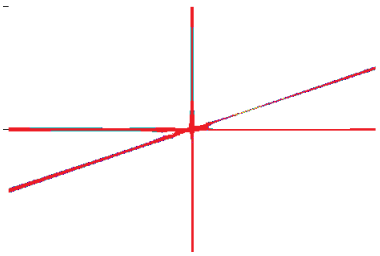
Proposition 11. *(i) $(PQ)_* = P_* Q_*$ et $(pq)^* = p^* q^*$*
(ii) $(p^*)_* = p$
(iii)$X_{n+1}^r (P_*)^* = P$, où r est le plus grand entier tel que $X_{n+1}^r \mid P$
(iv) $(P + Q)_* = P_* + Q_*$
(v) $X_{n+1}^t (p + q)^* = X_{n+1}^r p^* + X_{n+1}^s p^*$

Démonstration. (i) $PQ(X_1, .., X_n, 1) = P(X_1, .., X_n, 1) Q(X_1, .., X_n, 1)$.
$pq = \sum_{k=0}^{d_p+d_q} \sum_{i+j=k} p_i q_j$; $\quad (pq)^* = \sum_{k=0}^{d_p+d_q} \sum_{i+j=k} p_i q_j X_{n+1}^{d_p+d_q-k} = p^* q^*$.
(ii) est évident
(iii)$(P_*)^*(X_1, ..., X_{n+1}) = \frac{P(X_1, ..., X_{n+1})}{X_{n+1}^r}$
Les autres se montrent de façon similaire et sont intuitivement faciles à prouver. □

Corollaire. *Factoriser un polynôme homogène P revient à factoriser P_* avec une indéterminée de moins.*
En particulier, P homogène dans $\mathbb{K}[X, Y]$ et $\mathbb{K}$ algébriquement clos, alors P est décomposable en facteurs de degré 1.

Démonstration. On note $Q = (P_*)^*$. $P = Y^r Q$.
On factorise $Q_* = \prod_{i=1}^{m} (X - \lambda_i)$; $Q = \prod_{i=1}^{m} (X - \lambda_i Y)$
Donc $P = Y^r \prod_{i=1}^{m} (X - \lambda_i Y)$ □

Exemple. *$P = X^2 Y - 2XY^2$ homogène. Ses facteurs sont de degré 1 : V(P) est une union de droites*



Définition 13. *Soit I,J deux idéaux, on note $IJ = (\{ij, i \in I, j \in J\})$*
I^m est engendré par les $a_1^{i_1} a_2^{i_2} ... a_k^{i_k}$ où $a_i \in I$ et $i_1 + i_2 + ... + i_k = m$

Proposition 12. *$IJ \subset I \cap J$ avec égalité quand I et J sont comaximaux.*

Démonstration. $IJ \subset I \cap J$ est trivial.
Soit $x \in I \cap J$
On a I+J=(1) donc $\exists i \in I, j \in J, i + j = 1$. Donc $x = xi + xj$. Alors, $xi \in IJ$ car $x \in J$ et $xj \in IJ$ car $x \in I$. Donc $x \in IJ$. □

Proposition 13. *$I \subset A$ noethérien, alors $\exists N \in \mathbb{N}, \sqrt{I}^N \subset I$.*

Démonstration. $\sqrt{I} = P_1A + ... + P_mA$ car A noethérien.
Chaque P_i est dans $\sqrt{I}$ donc $P_i^{a_i} \in I$ pour un certain $a_i \in \mathbb{N}$. Soit $N = \sum_{i=1}^{m} a_i$. Soit $P \in \sqrt{I}$, $P = \sum_{i=1}^{m} P_iA_i$.
$P^N = \sum_{k_1+...+k_m=N} (P_1A_1)^{k_1}..(P_mA_m)^{k_m} \frac{N!}{k_1!..k_m!}$ et on voit que chaque terme de la somme a au moins un élément P_iA_i élevé à une puissance suffisante (supérieure à a_i). Donc $P^N \in I$ □

Définition 14. *Soit I idéal de $\mathbb{K}[X_1, ..., X_n]$. On dit que I est homogène quand :*
$\forall P \in I$, chaque composante homogène de P est dans I.

Exemple. *$I = (X_1^2, X_2^2)$ est un idéal homogène de $\mathbb{K}[X_1, ..., X_n]$.*
Si $P \in I$, $P = X_1^2A + X_2^2B$, en décomposant A et B en sommes de polynômes homogènes on voit que chacun de leurs termes sont dans l'idéal I. Donc c'est un idéal homogène.
$I' = (X_1^2 - X_2)$ n'est pas homogène car $X_1^2 - X_2$ a pour termes homogènes X_1^2 et X_2 mais aucun des deux n'est dans I'
$I'' = (X_1^2, X_2)$ est homogène : $P \in I''$, $P = X_1^2A - X_2B$ on décompose A et B en sommes d'homogènes et il est clair que leurs termes sont dans I".

Proposition 14. *I est homogène si et seulement si il existe une famille de polynômes homogènes qui génère I.*

Démonstration. (⇐)Soit $P \in I$, $P = \sum_{i=0}^{k} Q_iA_i$ où $(Q_i)_{1\leq i\leq k}$ est la famille de polynômes homogènes générant I. En décomposant les A_i en sommes d'homogènes on voit que tous les termes sont dans I.
(⇒) I est noethérien, on choisit des générateurs $(P_i)_{1\leq i\leq k}$. Comme I est homogène chaque composante homogène de P_i est aussi dans I.
Donc $I = (\{P_i\}_{1\leq i\leq k}) = (\{P_{i,j}, P_i = \sum_{j=0}^{d_i} P_{i,j}\}_{1\leq i\leq k})$
L'inclusion (⊂) est triviale, (⊃) vraie car les $P_{i,j}$ sont dans I par homogénéité.
Donc I est engendré par des homogènes. □

Exemple. *$I = (X_1, ..., X_n)$ homogène de $\mathbb{K}[X_1, ..., X_n]$. De plus $\forall k \in \mathbb{N}$, I^k est un idéal homogène de $\mathbb{K}[X_1, ..., X_n]$.*
En effet, $I^k = (\{\prod_{k_1+...+k_n=k} X_i^{k_i}\})$. Ces polynômes sont homogènes de degré k.
I^k contient tous les polynômes de premier terme dont le degré est supérieur à k.

2.3 Isomorphisme

Théorème 5. *Soit I un idéal de $\mathbb{K}[X_1, ..., X_n]$ tel que V(I) est fini. $V(I) = \{x_1, ..., x_k\}$. On note $\mathcal{O}_{x_i}(\mathbb{K}^n) = \mathcal{O}_i$, alors*

$$\mathbb{K}[X_1, ..., X_n]/I \cong \prod_{i=1}^{k} \mathcal{O}_i/I\mathcal{O}_i$$

Démonstration. Je vais établir une preuve pour n=1. Elle n'a pas d'intérêt pour la démonstration générale mais permet de mieux comprendre cet énoncé.
Soit I idéal de $\mathbb{K}[X]$ tel que V(I) est fini. $\mathbb{K}[X]$ est principal donc I=(P) et $P \neq O$. On décompose P en irréductibles : $P = \prod_{i=1}^{k} (X - x_i)^{a_i}$ d'où $V(I) = \{x_1, .., x_k\}$
Le théorème des restes chinois nous donne :
$\mathbb{K}[X]/(P) \cong \prod_{i=1}^{k} \mathbb{K}[X]/(X - x_i)^{a_i}\mathbb{K}[X]$.On a $(P)\mathcal{O}_i = (X - x_i)^{a_i}\mathcal{O}_i$. En effet, les autres facteurs de P sont inversibles dans $\mathcal{O}_i$ donc ils ne changent pas l'idéal.
Il suffit d'établir $\mathcal{O}_i/I\mathcal{O}_i \cong \mathbb{K}[X]/(X - x_i)^{a_i}\mathbb{K}[X]$.
Soit $\phi : \mathbb{K}[X] \to \mathcal{O}_i/I\mathcal{O}_i$
. $P \mapsto \overline{P}$
$\phi = \pi \circ \psi$ où π est le morphisme de quotient, ψ est le morphisme de localisation. ϕ est surjectif : soit $f \in \mathcal{O}_i$, $f = \sum_{r=0}^{a_i-1} f^{(r)}(x_i)\frac{(X-x_i)^r}{r!} + g$. Les a_i premières dérivées de g sont nulles en x_i. Cela suffit à dire que $\overline{g} = 0$ dans $\mathcal{O}_i$ car $(X - x_i)^{a_i}$ divise alors le numérateur de g.
En effet, $g = P/Q$, $P = gQ$. Soit $r < a_i$
$(P)^{(r)}(x_i) = (Qg)^{(r)}(x_i) = \sum_{s=0}^{r} \alpha_s Q^{(r-s)}(x_i)g^{(s)}(x_i) = 0$ donc $(X - x_i)^{a_i} \mid P$
$g = \frac{(X-x_i)^{a_i}P_g}{Q_g}$ et $Q_g(x_i) \neq 0$, donc $g \in I\mathcal{O}_i$.
Donc $\overline{f} = \phi(Q)$ où $Q = \sum_{i=0}^{a_i-1} f^{(r)}(x_i)\frac{(X-x_i)^r}{r!} \in \mathbb{K}[X]$, ϕ est surjectif.
$R \in Ker(\phi) \Leftrightarrow$ les j premières dérivées de R en x_i sont nulles $\Leftrightarrow (X - x_i)^{a_i} \mid R$ dans $\mathbb{K}[X]$.
$Ker(\phi) = (X - x_i)^{a_i}$, donc
$\mathbb{K}[X]/(X - x_i)^{a_i} \cong \mathcal{O}_i/(X - x_i)^{a_i}\mathcal{O}_i$
Donc $\mathbb{K}[X]/(P) \cong \prod_{i=1}^{k} \mathcal{O}_i/P\mathcal{O}_i$ □

Démonstration. On note ici $I_i = I(\{x_i\}) \subset \mathbb{K}[X_1, ..., X_n]$.
Ces idéaux sont maximaux distincts, contenant I. On note $A = \mathbb{K}[X_1, ..., X_n]/I$ et $A_i = \mathcal{O}_i/I\mathcal{O}_i$. On note $\varphi_i : A \to A_i$ les morphismes naturels de la forme $\pi \circ \psi$ où ψ est la localisation $P \mapsto \frac{P}{1}$ et π le quotient $f \mapsto \overline{f}$.
Ces morphismes induisent $\varphi : A \to \prod_{i=1}^{k} A_i$.
D'après le Nullstellensatz, $\sqrt{I} = I(V(I)) = \bigcap_{i=1}^{k} I_i$.
Avec la propriété précédente, on choisit d tel que $(\bigcap_{i=1}^{k} I_i)^d \subset I$. De plus comme I_i et $\bigcap_{j\neq i} I_j$ sont comaximaux $(I_1 I_2 .. I_k)^d = \bigcap_{i=1}^{k} I_i^d = (\bigcap_{i=1}^{k} I_i)^d \subset I$
Grâce à un lemme déjà établi, on choisit une famille de polynômes $(P_1, .., P_k)$ telle que

$P_i(x_i) = 1$ et $P_i(x_j) = 0$ si $j \neq i$. $P_i \in I_j \forall j \neq i$
Soient $E_i = 1 - (1 - P_i^d)^d$; $E_i(x_i) = 1$ et $E_i(x_j) = 0$ si $j \neq i$
$E_i = P_i^d Q_i$ pour un certain Q_i donc $E_i \in I_j^d$ pour tout $j \neq i$
On a aussi $1 - \sum_{i=1}^{k} E_i = 1 - E_i - \sum_{j \neq i} E_i$ donc c'est un élément de $\bigcap_{i=1}^{k} I_i^d \subset I$.
On note en majuscule les polynômes, en minuscules les classes résiduelles sur I.
$e_i^2 = e_i$; $e_i e_j = 0$; $\sum_{i=1}^{k} e_i = 1$
Étape 1 : Soit Q un polynôme, $Q(x_i) \neq 0$, alors $\exists t \in \mathbb{K}[X_1, ..., X_n]/I, t * q = e_i$
On prend $Q(x_i) = 1$; Soit $R = 1 - Q$; Alors
$(1 - R) \sum_{j=0}^{d-1} R^j E_i = E_i - R^d E_i$. $R \in I_i$ donc $R^d E_i \in I$
En quotientant, $q \sum_{j=0}^{d-1} e_i r^j = e_i$. On a donc $t = \sum_{j=0}^{d-1} e_i r^j$ comme voulu, $tq = e_i$.
Étape 2 : φ est injective
On suppose $\varphi(p) = 0$. Alors $\forall i \exists Q_i$, $Q_i(x_i) \neq 0$ et $Q_i P \in I$. Par l'étape 1 on prend t_i, $t_i q_i = e_i$. Ainsi $p = \sum_{i=1}^{k} e_i p = \sum_{i=1}^{k} t_i g_i p = 0$. Donc φ est injective.
Étape 3 : φ est surjective
$E_i(x_i) = 1$ donc $\varphi_i(e_i)$ est une unité de A_i. Soit $j \neq i$ on a $\varphi_i(e_i)\varphi_i(e_j) = \varphi_i(e_i e_j) = \varphi_i(0) = 0$
donc $\varphi_i(e_j) = 0$. Ainsi $\varphi_i(e_i) = \varphi_i(\sum_{i=1}^{k} e_i) = \varphi_i(1) = 1$.
Soit $z = (\frac{p_1}{q_1}, .., \frac{p_k}{q_k}) \in \prod_{i=1}^{k} A_i$. P_i/Q_i est l'écriture polynômiale d'un représentant de p_i/q_i, $Q_i(x_i) \neq 0$; par l'étape 1, on choisit t_i tel que $t_i q_i = e_i$.
Dans l'anneau A_i, $p_i = p_i e_i = p_i q_i t_i$. Donc $p_i/q_i = p_i t_i$. Ainsi :
$\varphi_i(\sum_{j=1}^{k} t_j p_j e_j) = \varphi_i(t_i p_i) = p_i/q_i$.
Donc $z = \varphi(\sum_{j=1}^{k} t_j p_j e_j)$ donc φ surjective. □

Corollaire. $dim_{\mathbb{K}}(\mathbb{K}[X_1, ..., X_n]/I) = \sum_{i=1}^{k} dim_{\mathbb{K}}(\mathcal{O}_i/I\mathcal{O}_i)$

3 Courbes planes affines

3.1 Notions géométriques

On se place dans le cadre de $\mathbb{K}$ corps algébriquement clos. Par le Nullstellensatz, une courbe algébrique $\mathbb{K}^2$ correspond à un polynôme P non constant sans facteurs multiples de $\mathbb{K}[X,Y]$ unique à multiplication scalaire près.
Une courbe algébrique V(P) définie par P se note parfois $\{P=0\}$, le degré d'une courbe algébrique est le degré du polynôme P qui la détermine.

Exemple. *Une courbe algébrique de degré 1 est une droite de $\mathbb{K}^2$, $D=V(P)$, $P=aX+bY+c$, $D=\{x,y,ax+by+c=0\}$ est notée $aX+bY+c=0$*

On veut pour la suite permettre aux polynômes d'avoir des facteurs multiples pour plus de généralité et pour que $\sqrt{I}$ ne caractérise pas $V(I)$. L'ensemble algébrique déterminé est le même donc on doit étendre la définition.
On donne une nouvelle définition de V qu'on appellera V'.

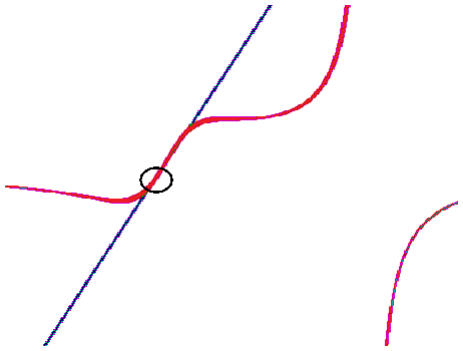
Définition 15. *Une courbe plane affine est une classe d'équivalence $\overline{P}$ pour la relation $P\sim Q \Leftrightarrow \exists\lambda\in\mathbb{K}^*, P=\lambda Q$. On la note V'(P).*
Le degré d'une courbe est le degré des polynômes dans sa classe d'équivalence.
Soit $P=\prod_{i=1}^{k} P_i^{e_i}$ décomposition factorielle, et V'(P) la courbe qu'il détermine :
Les $V'(P_i^{e_i})$ sont les composantes de V'(P) qu'on note $V'(P_i)$.
$V(P_i)$ est une composante simple si $e_i=1$, sinon c'est une composante multiple.
e_i est la multiplicité de la composante $V'(P_i)$.
Si P irréductible, V'(P) est une variété affine de $\mathbb{K}^2$.
On note alors $\Gamma(P)$, $\mathcal{O}_z(P)$, $\mathbb{K}(P)$, $\mathfrak{m}_z(P)$ les anneaux qu'on considérait précédemment au lieu de $\Gamma(V(P))$, $\mathcal{O}_z(V(P))$, $\mathbb{K}(V(P))$, $\mathfrak{m}_z(V(P))$.
Soit $z=(a,b)\in V(P)$. z est régulier si $\frac{\partial P}{\partial X}(z)\neq 0$ ou $\frac{\partial P}{\partial Y}(z)\neq 0$
La droite V'(L)=V(L), $L=\frac{\partial P}{\partial X}(z)(X-a)+\frac{\partial P}{\partial Y}(z)(Y-b)$ est la droite tangente en z.
Les points non réguliers sont singuliers ou multiples.
Une courbe est régulière quand tous ses points sont réguliers.

La courbe géométrique seule permet de déterminer les P_i mais pas leurs multiplicités. On remarque que les tangentes ainsi définies sont les tangentes géométriques de la courbe.

Exemple. $P=X^3Y-2(X+1)(Y-1)$. $z=(-1,0)\in V(P)$
$L=\frac{\partial P}{\partial X}(z)(X-a)+\frac{\partial P}{\partial Y}(z)(Y-b)=2(X+1)-Y=2X-Y+2$

On voit sur la figure que la courbe et la tangente coïncident.
Le point qu'on a choisi est régulier, cela se voit aussi géométriquement.

Définition 16. *$P=\sum_{i=m}^{d} P_i$ décomposition en homogènes.*
m est la multiplicité en 0 de P. On la note $m_0(P)$.
P_m est homogène dans $\mathbb{K}[X,Y]$, ses facteurs sont de degré 1 : $P_m=\prod_{i=1}^{r} L_i^{r_i}$
Les L_i sont les droites tangentes à V(P) en 0.
On dit que 0 est un point multiple ordinaire quand ses tangentes sont simples.
Sinon, 0 a au moins une tangente double.



$P = \prod_{i=1}^{k} P_i^{e_i}$, *alors* $m_0(P) = \sum_{i=1}^{k} e_i m_0(P_i)$
Soit $z \in \mathbb{K}^2$, T_z *la translation envoyant 0 sur* z. $z = (a, b)$
$T_z(x, y) = (x + a, y + b)$, *on définit* $m_z(P) = m_0(P \circ T_z)$

On remarque que z est un point simple de V'(P) si et seulement si :
(i) z n'appartient qu'à un composante P_i
(ii) P_i est un facteur simple de P
(iii) z est un point simple de P_i

V(P) est la courbe géométrique, caractérisée par le radical de P. V'(P) donne du poids aux composantes irréductibles multiples de P. Si P n'a que des facteurs simples V(P)=V'(P).

3.2 Notions algébriques

Soit V'(P) une courbe plane affine irréductible, $z \in V(P)$. Nous allons établir que la multiplicité est caractérisée par l'anneau local $\mathcal{O}_z(P)$.

Théorème 6. *z point simple de V'(P)$\Leftrightarrow$ $\mathcal{O}_z(P)$ anneau à valuation discrète.*
Quand tel est le cas, $\forall L$ droite non tangente à V(P) passant par z, l'image l de L dans $\mathcal{O}_z(P)$ est un paramètre uniformisant.

Démonstration. ($\Rightarrow$) On se ramène au cas $z = 0$, $L = V(X)$, $T = V(Y)$ la ligne tangente par changement de coordonnées affine. Il suffit de montrer que $\mathfrak{m}_0(P)$ est engendré par $x = \overline{X}$ vu comme une fonction définie en 0.
Soit $f \in \mathfrak{m}_0(P)$, f est définie en 0 non inversible dans $\mathcal{O}_0(P)$ donc nulle en 0.
Soit Q, $Q(0) \neq 0$ et $Qf \in \Gamma(P)$. On le divise par X :
$Qf = XQ' + R'$. $deg(R'(X, 0)) = 0$ si $R' \neq 0$, $Y \mid R'$ car f non inversible donc son coefficient constant est nul, donc $R' = YR$.
On revient dans $\mathcal{O}_0(P)$, $f = xh_0 + yg$. On a $\mathfrak{m}_0(P) = (x, y)$
On a P=Y+(...) termes de plus haut degré.
On peut donc écrire $P = YG - X^2H$, G=1+(...) et $H \in \mathbb{K}[X]$.
$yg = x^2h$ dans $\Gamma(P)$ et $g(0) \neq 0$. $y = x^2hg^{-1}$ et ainsi $\mathfrak{m}_0(P) = (x, y) = (x)$
La réciproque vient du théorème suivant. □

Définition 17. *Soit z un point de V(P) courbe plane affine.*
Pour $Q \in \mathbb{K}[X, Y]$ on note $ord_z^P(Q) = ord_z^P(q)$ est l'ordre de Q dans l'anneau à valuation discrète $\mathcal{O}_z(P)$.
On peut étendre cette définition aux composantes irréductibles de P si P est réductible. On notera toujours $ord_z^P(Q)$.

En particulier, si V(L) passe par z est une droite, $ord_z^P(L) = 1$ si V(L) n'est pas tangente à V(P) ; $ord_z^P(L) > 1$ si V(L) est tangente à V(P) ; (et $ord_z^P(L) = 0$ si L ne passe pas par z.) Donc L est un paramètre uniformisant quand V(L) n'est pas tangente à V(P)

Théorème 7. *Soit $z \in V(P)$, P irréductible.*
Alors pour N assez grand, $m_z(P) = dim_{\mathbb{K}}(\mathfrak{m}_z(P)^N/\mathfrak{m}_z(P)^{N+1})$

Démonstration. On note $O = \mathcal{O}_z(P)$ et $M = \mathfrak{m}_z(P)$.
$\forall n \geq m_z(P)$, la suite d'algèbres
$0 \to M^n/M^{n+1} \to O/M^{n+1} \to O/M^n \to 0$ est exacte
Il suffit donc de prouver $\exists s, \forall n \geq m_z(P), dim_{\mathbb{K}}(O/M^{n+1}) = nm_z(P) + s$
On se ramène à $z = 0$ donc $M^n = I^n O$ où I=(X,Y). $V(I^n) = \{0\}$ donc
$\frac{\mathbb{K}[X,Y]}{(I^n,P)} = \frac{\mathcal{O}_0(\mathbb{K}^2)}{(I^n,P)\mathcal{O}_0(\mathbb{K}^2)} = \frac{\mathcal{O}_0(P)}{I^n\mathcal{O}_0(P)} = O/M^n$
Cela revient à calculer la dimension de $\frac{\mathbb{K}[X,Y]}{(I^n,P)}$. On note $m = m_0(P)$
$0 \to \frac{\mathbb{K}[X,Y]}{I^{n-m}} \to \frac{\mathbb{K}[X,Y]}{I^n} \to \frac{\mathbb{K}[X,Y]}{I^n,P} \to 0$ est exacte donc :
$dim_{\mathbb{K}}(\mathbb{K}[X,Y]/(I^n,P)) = nm - \frac{m(m-1)}{2}$. Cela conclut le théorème.

□

Il est facile de voir que si $\mathcal{O}_z(P)$ est à valuation discrète, $m_z(P) = 1$ donc z est un point simple de V'(P) ce qui prouve la réciproque du théorème précédent.

3.3 Nombre d'intersections

Pour P et Q deux polynômes, on définit $I(z, P \cap Q)$ le nombre d'intersections de V'(P) et V'(Q) au point z. Géométriquement ce nombre vaut 1 ou 0 mais en pondérant par des multiplicités d'intersections il peut valoir plus.

Définition 18. *Soient P,Q dans $\mathbb{K}[X,Y]$ et V'(P),V'(Q) leurs courbes affines.*
V'(P) et V'(Q) s'intersectent strictement en z quand ils n'ont pas de composante commune passant par z.

Propriété 1. *$I(z, P \cap Q) \in \mathbb{N}$ si V'(P) et V'(Q) s'intersectent strictement en z*
$I(z, P \cap Q) = \infty$ si ils s'intersectent non strictement.

Propriété 2. *$I(z, P \cap Q) = 0 \Leftrightarrow z \notin V(P) \cap V(Q)$*
$I(z, P \cap Q)$ ne dépend que des composantes passant par z

Propriété 3. *Si T est un changement de coordonnées affine avec $T(u) = z$,*
$I(u, P \circ T \cap Q \circ T) = I(z, P \cap Q)$

Propriété 4. *$I(z, P \cap Q) = I(z, Q \cap P)$*

Propriété 5. *$I(z, P \cap Q) \geq m_z(P)m_z(Q)$*
L'égalité a lieu si et seulement si V(P) et V(Q) n'ont pas de tangente commune en z

Propriété 6. *$P = \prod_{i=1}^{n} P_i^{s_i}$ et $Q = \prod_{j=1}^{k} Q_j^{t_j}$*
alors $I(z, P \cap Q) = \sum_{i=1}^{n} \sum_{j=1}^{k} s_i t_j I(z, P_i \cap Q_j)$

Propriété 7. *$I(z, P \cap Q) = I(z, P \cap (Q + AP)$ pour tout $A \in \mathbb{K}[X,Y]$*

Théorème 8. *Il existe un unique $I(z, P \cap Q)$ vérifiant ces 7 propriétés.*

$$I(z, P \cap Q) = dim_{\mathbb{K}}(\mathcal{O}_z(\mathbb{K}^2)/(P, Q))$$

Démonstration. Unicité : preuve algorithmique.
On admet que $I(z, P \cap Q)$ vérifie les 7 propriétés. On suppose donc z=0 par la propriété 3 et $0 < I(z, P \cap Q) < \infty$ par les propriétés 1 et 2.
$I(z, P \cap Q) = n > 0$; On procède par récurrence sur n : l'hypothèse de récurrence étant que $\forall A, B, I(z, A \cap B)$ est unique s'il est inférieur à n.
On considère P(X,0) et Q(X,0) de degrés respectifs r et s, on peut supposer $r \leq s$ par la propriété 4.
Si r=0 : $Y \mid P$, $P = YR$ donc $I(0, P \cap Q) = I(0, R \cap Q) + I(0, Y \cap Q)$ par la propriété 6.
$Q(X, 0) = X^m(a_0 + ... + a_r X^r)$ avec $a_0 \neq 0$ on a donc
$I(0, Y \cap Q) = I(0, Y \cap Q(X, 0)) = I(0, Y \cap X^m) = m$. Comme $0 \in V(Q)$ on a $m > 0$ donc on rappelle $I(0, R \cap Q)$ qui est strictement inférieur à n.
Si $r \neq 0$: on considère que P et Q sont unitaires (la multiplication scalaire n'a pas d'influence).
Soit $R = Q - X^{s-r}P$. $I(0, P \cap R) = I(0, P \cap Q)$ et le degré de R(X,0) est strictement inférieur à s.
On itère cette opération et on échange P et Q quand l'ordre de leurs degrés s'inverse, on arrive fatalement au cas $r = 0$.
On a ainsi prouvé l'unicité d'un tel nombre d'intersections.

Existence : soit $I(z, P \cap Q) = dim_{\mathbb{K}}(\mathcal{O}_z(\mathbb{K}^2)/(P, Q))$
On doit montrer qu'il vérifie les 7 propriétés.
Les propriétés 2,4 et 7 se vérifient immédiatement.
$\mathcal{O}_z(\mathbb{K}^2)/(P) \cong \mathcal{O}_z(\mathbb{K}^2)/(P \circ T)$ suffit pour la propriété 3.

Si P,Q n'ont pas de facteurs communs, V(P,Q)=V(I) fini. On a alors :
$dim_{\mathbb{K}}(\mathbb{K}[X, Y]/(P, Q)) = \sum_{i=1}^{k} dim_{\mathbb{K}}(\mathcal{O}_{z_i}(\mathbb{K}^2)/(P, Q)) < \infty$. Si z est l'un des z_i (cas contraire trivial) $I(z, P \cap Q) < \infty$
Si P et Q ont R comme facteur commun, $(P, Q) \subset (R)$ donc $dim_{\mathbb{K}}(\mathcal{O}/(P, Q)) = I(z, P \cap Q) \geq dim_{\mathbb{K}}(\mathcal{O}/(R)) = \infty$. Ainsi on a établi la propriété 1.

On suppose maintenant P et QR n'ont pas de facteurs communs. On veut établir
$I(z, P \cap QR) = I(z, P \cap Q) + I(z, P \cap R)$. On considère le diagramme :

$$0 \longrightarrow \frac{\mathcal{O}}{(P,Q)} \xrightarrow{\psi} \frac{\mathcal{O}}{(P,QR)} \xrightarrow{\varphi} \frac{\mathcal{O}}{P,R} \longrightarrow 0$$

$\varphi : \mathcal{O}/(P, QR) \to \mathcal{O}/(P, R)$ est surjectif car c'est un quotient
$\psi : \mathcal{O}/(P, Q) \to \mathcal{O}/(P, QR)$.
$\overline{f} \longmapsto R\overline{f}$
La suite est exacte :
ψ est injectif : soit $\psi_0 : \mathcal{O} \to \mathcal{O}/(P, QR)$
$P, Q \in Ker(\psi)$ est évident. Supposons $\psi_0(\overline{f}) = 0$
$Rf = uP + vQR$ où $u, v \in \mathcal{O}$.
On veut prouver que $f = u'P + v'Q$ pour $u', v' \in \mathcal{O}$ Cette égalité s'écrit dans $\mathbb{K}[X, Y]$: soit $S \in \mathbb{K}[X, Y]$, $Su = A$, $Sv = B$, $Sf = C$, $S(z) \neq 0$ et $A, B, C \in \mathbb{K}[X, Y]$
$RC = AP + BQR$, $R(C - BQ) = AP$. P et R n'ont pas de facteurs en commun donc sont premiers entre eux. Ainsi $R \mid A$. $RA' = A$ alors

$C = BQ + PA'$; on divise par S, on note $v' = \frac{B}{S}$ et $u' = \frac{A'}{S}$
Alors $f = u'P + v'Q$. $Ker(\psi_0) = (P, Q)$ et donc $Ker(\psi) = (0)$
$Ker(\varphi) = \{Pf + Rg, (f, g) \in \mathcal{O}/(P, QR)\} = \{Rg, g \in \mathcal{O}/(P, Q)\} = Im(\psi)$
Ainsi $dim_{\mathbb{K}}(\mathcal{O}/(P, QR)) = dim_{\mathbb{K}}(\mathcal{O}/(P, Q)) + dim_{\mathbb{K}}(\mathcal{O}/(P, Q))$
Donc $I(z, P \cap QR) = I(z, P \cap Q) + I(z, P \cap R)$, on prouve ainsi (6).

La propriété (5) est plus difficile à établir.
On note $m = m_z(P)$ et $n = m_z(Q)$. Soit $I = (X, Y)$, on considère le diagramme :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{\mathbb{K}[X,Y]}{I^n} \times \frac{\mathbb{K}[X,Y]}{I^m} & \xrightarrow{\psi} & \frac{\mathbb{K}[X,Y]}{I^{n+m}} & \xrightarrow{\varphi} & \frac{\mathbb{K}[X,Y]}{I^{n+m},P,Q} & \longrightarrow & 0 \\ & & & & & & \downarrow \alpha & & \\ & & 0 & \longrightarrow & \frac{\mathcal{O}}{(P,Q)} & \xrightarrow{\pi} & \frac{\mathcal{O}}{I^{n+m},P,Q} & \longrightarrow & 0 \end{array}$$

φ est le morphisme (surjectif) de quotient.
π est le morphisme (surjectif) de quotient.
$\psi : (\overline{A}, \overline{B}) \longmapsto \overline{AP + BQ}$
Comme $V(I^{n+m}, P, Q) = \{z\}$ est fini, α est un isomorphisme.
La suite au dessus est exacte donc $dim_{\mathbb{K}}(\frac{\mathbb{K}[X,Y]}{(I^{n+m},P,Q)}) = dim_{\mathbb{K}}(\frac{\mathbb{K}[X,Y]}{I^{n+m}}) - dim_{\mathbb{K}}(Ker(\varphi))$
Cela nous indique donc
$I(z, P \cap Q) = dim_{\mathbb{K}}(\frac{\mathcal{O}}{(P,Q)})$
· $\geq dim_{\mathbb{K}}(\frac{\mathcal{O}}{(I^{n+m},P,Q)})$ car π surjectif
· $= dim_{\mathbb{K}}(\frac{\mathbb{K}[X,Y]}{(I^{n+m},P,Q)})$ car α bijectif
· $\geq dim_{\mathbb{K}}(\frac{\mathbb{K}[X,Y]}{I^{n+m}}) - dim_{\mathbb{K}}(\frac{\mathbb{K}[X,Y]}{I^n}) - dim_{\mathbb{K}}(\frac{\mathbb{K}[X,Y]}{I^m})$
· $= n * m$

L'égalité a lieu si et seulement si π et ψ sont injectifs.

Lemme. *ψ injectif $\Leftrightarrow$ V(P) et V(Q) ont des tangentes distinctes en z.*
Dans ce cas, $\forall t \geq n + m - 1$, on a $I^t \subset (P, Q)\mathcal{O}$

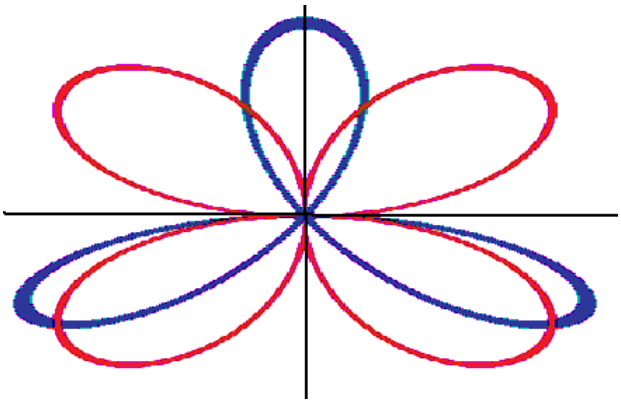
En admettant le lemme on constate que π est alors bijectif car il est surjectif et $Ker(\pi_0) = (I^{n+m}, P, Q) \subset (P, Q)$.
Donc $Ker(\pi) = (0)$ □

Démonstration. (lemme) On suppose que V(P),V(Q) ont $(L_i)_{1 \leq i \leq n}$ et $(M_j)_{1 \leq j \leq m}$ pour tangentes respectives (distinctes) en z.
$A_{i,j} = L_1 L_2 ... L_i M_1 ... M_j$, alors $\{A_{i,j}, i + j = t\}$ forment une base de l'espace des polynômes homogènes de degré t de $\mathbb{K}[X, Y]$.
On veut établir $A_{i,j} \in (P, Q)\mathcal{O}$ quand $i + j \geq n + m - 1$.
Quand tel est le cas, $i \geq m$ ou $j \geq n$. On va dire $i \geq m$, $A_{i,j} = A_{m_0} B$
$P = A_{m_0} + P'$, les termes de P' sont de degré supérieur à $m + 1$
$A_{i,j} = BP - BP'$, les termes de BP' sont de degré supérieur à $i + j + 1$
Il suffit donc de prouver $I^t \subset (P, Q)$ quand t assez grand.
$V(P, Q) = \{z, w_1, ..., w_s\}$. On choisit un polynôme R tel que
$\forall j, R(w_j) = 0$ et $R(0) \neq 0$. RX et RY sont dans I(V(P,Q)). Donc $\exists N \in \mathbb{N}$, $(RX)^N$ et $(RY)^N$ soient dans (P,Q) (Nullstellensatz).
Comme $(HX)^N, (HY)^N \in I$ et H unité de $\mathcal{O}$, on a $X^N, Y^N \in I$
Alors $I^{2N} \subset (P, Q)\mathcal{O}$ comme voulu.

$\psi((\overline{A}, \overline{B})) = \overline{AP + BQ} = \overline{0} \Leftrightarrow$ AP+BQ n'a que des termes de degré supérieur à $n + m$.

On note A_r et B_s les termes homogènes de plus petit degré de A et B.
$A_rP + B_sQ = 0$, P et Q sont premiers entre eux ; ainsi $P \mid B_s$, $Q \mid A_r$.
Mais alors B_s est nul ou de degré supérieur à m, donc $\overline{B} = \overline{0}$
de même $\overline{A} = \overline{0}$. Donc ψ est injectif. □

On remarque que la preuve de l'unicité donne un algorithme (programmable) pour déterminer le nombre d'intersections en un point donné.
Par ailleurs, on peut remarquer que ces propriétés sont redondantes. On va en ajouter encore deux autres qui serviront par la suite.



Exemple. *Intersection entre* $V((X^2+Y^2)^3 - 4X^2Y^2)$ *(en rouge) et* $V((X^2+Y^2)^2 + 3X^2Y - Y^3)$ *(en bleu). Ces deux courbes ont 14 points d'intersection en 0.*

Propriété 8. *Si z est un point simple de V'(P),* $I(z, P \cap Q) = ord_z^P(Q)$

Démonstration. Supposons P irréductible et q=$\overline{Q}$ sa classe dans $\mathcal{O}_z(P)$.
$ord_z^P(Q) = dim_{\mathbb{K}}(\mathcal{O}_z(P)/(q))$. Comme $\mathcal{O}_z(P)/(q) \cong \mathcal{O}_z(\mathbb{K}^2)/(P,Q)$, sa dimension est $I(z, P \cap Q)$. □

Propriété 9. *Si P et Q n'ont pas de facteurs en commun, alors*

$$\sum_{z \in V(P) \cap V(Q)} I(z, P \cap Q) = dim_{\mathbb{K}}(\mathbb{K}[X,Y]/(P,Q))$$

Démonstration. $dim_{\mathbb{K}}(\mathbb{K}[X,Y]/I) = \sum_{z \in V(I)} dim_{\mathbb{K}}(\frac{\mathcal{O}_z(\mathbb{K}^2)}{I\mathcal{O}_z(\mathbb{K}^2)})$ d'après l'isomorphisme établi précédemment.
Donc on a bien le résultat avec I=(P,Q). □

4 Variétés projectives

On pourrait penser qu'on a ainsi trouvé toutes les intersections entre deux courbes algébriques, mais ce n'est pas le cas :
P=Y et Q=Y+1
Alors $V(P) \cap V(Q) = \emptyset$ car ce sont deux droites parallèles. Pourtant elles s'intersectent "à l'infini". C'est géométriquement visible, et pour l'établir algébriquement on doit voir cette intersection dans l'espace projectif.

4.1 Espaces projectifs

On définit la relation de colinéarité dans $\mathbb{K}^{n+1} \setminus \{0\}$ par :

$$x \sim x' \Leftrightarrow \exists \lambda \in \mathbb{K}^*, x = \lambda x'$$

On vérifie aisément que c'est une relation d'équivalence.

Définition 19. *On appelle $\mathbb{P}_n(\mathbb{K})$ l'espace projectif défini par :*

$$\mathbb{P}_n(\mathbb{K}) = \frac{\mathbb{K}^{n+1} \setminus \{0\}}{\sim}$$

P_n correspond à l'ensemble des droites vectorielles en dimension $n+1$.
Les points de P_n peuvent être représentés en coordonnées homogènes par
$z \in \mathbb{P}_n(\mathbb{K}) \Rightarrow z = (x_1 : x_2 : ... : x_{n+1})$ où $(x_1, ..., x_{n+1})$ est un point non nul de la droite de $\mathbb{K}^{n+1}$ déterminée par z.

Proposition 15. *$\mathbb{P}_n(\mathbb{K})$ a une structure de variété pure de dimension n :*

Démonstration. Soit $U_i = \{(x_1 : ... : x_{n+1}) \in \mathbb{P}_n(\mathbb{K}), x_i \neq 0\}$

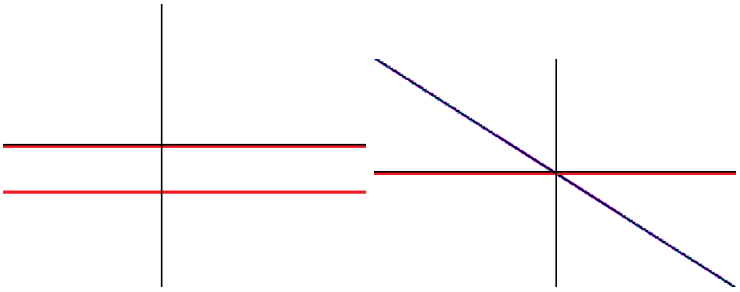
$$\varphi_i : U_i \longrightarrow \mathbb{K}^n$$
$$(x_1 : ... : x_{n+1}) \mapsto (\tfrac{x_1}{x_i}, ..., \tfrac{x_{i-1}}{x_i}, \tfrac{x_{i+1}}{x_i}, ..., \tfrac{x_{n+1}}{x_i})$$

φ_i est de classe C^∞ sur U_i
Elle est bijective : soit $z \in U_i$
$\exists!(x_1, .., x_{i-1}, 1, x_{i+1}, .., x_{n+1}) \in \mathbb{K}^{n+1}$ déterminant z
Il s'agit de l'intersection entre la droite déterminée par z et le plan affine d'équation $x_i = 1$.
Elle est non vide car $z \in U_i \Rightarrow$ la droite déterminée par z n'est pas dans le plan vectoriel d'équation $x_i = 0$
Les cartes sont au nombre de $n+1$ et sont compatibles. Les cartes recouvrent $\mathbb{P}_n(\mathbb{K})$ car $z = (x_1 : ... : x_{n+1}) \in \mathbb{P}_n(\mathbb{K}) \Rightarrow \exists i, x_i \neq 0$ donc $\exists i, z \in U_i$ □

En pratique on prend souvent U_{n+1} comme carte de référence ; On peut voir le plan projectif comme :
$\mathbb{P}_n(\mathbb{K}) = U_{n+1} \cup H_\infty$ où H_∞ correspond à un "hyperplan projectif à l'infini".
Le lien géométrique avec les courbes algébriques planes est le suivant :

Exemple. $\mathbb{P}_2(\mathbb{K}) = \{(x : y : 1), x, y \in \mathbb{K}^2\} \amalg \{(x : y : 0), (x : y) \in \mathbb{P}_1(\mathbb{K})\}$
Donc $\mathbb{P}_2(\mathbb{K}) \cong \mathbb{K}^2 \amalg \mathbb{P}_1(\mathbb{K})$
On voit ici que dans le plan projectif, on a ajouté une droite projective à l'infini à notre plan $\mathbb{K}^2$.

Exemple. *intersection de V(Y), V(Y+1) : on va faire une approche intuitive de l'intérêt des espaces projectifs dans la recherche de points d'intersections. On justifiera par la suite les méthodes utilisées dans cet exemple.*
On a déjà vu qu'elle est vide dans $\mathbb{K}^2$. *Mais* $\mathbb{K}^2$ *correspond dans le plan projectif à la carte* U_3 *définie par* $z = 1$.
Pour prolonger le cadre précédent, on doit avoir $\overline{P}$ *polynôme défini sur* $\mathbb{K}^3$:
$\overline{P}(X, Y, 1) = P(X, Y) = Y$
$\overline{Q}(X, Y, 1) = Q(X, Y) = Y + 1$
De plus le fait que $\overline{P}(x, y, z)$ *s'annule doit être indépendant du représentant dans* $\mathbb{K}^3$ *de* $(x : y : z)$. *La façon naturelle de garantir* $\forall \lambda \in \mathbb{K}^*$, $\overline{P}(\lambda x, \lambda y, \lambda z) = 0 \Leftrightarrow \overline{P}(x, y, z) = 0$ *est de prendre* $\overline{P}$ *homogène. La façon naturelle de choisir un tel homogène est de prendre l'homogénéisé de* P.
Ainsi $\overline{P} = Y$ *et* $\overline{Q} = Y + Z$. *On regarde l'intersection dans une autre carte :* $U_1 = \{(x : y : z), x = 1\}$. *On déshomogénéise* $\overline{P}$ *pour sa première variable, on étudie maintenant l'intersection de*
$P_0 = Y$ *et* $Q_0 = Y + Z$, *qui a un point d'intersection au point (0,0)*
Donc il y a un point projectif (1 :0 :0) qui est l'intersection de V(Y), V(Y+1).
Ce point est à l'infini car $z = 0$



Ce qu'il faut retenir et qu'on établira ensuite est : P définit une courbe V(P) de $\mathbb{K}^2$, alors $P^* \in \mathbb{K}[X, Y, Z]$ est l'équation correspondant dans K^3 à un cône dont l'intersection avec $\mathbb{K}^2 \times \{1\}$ est une translation de V(P).
Il est donc naturel de chercher les points de V(P) dans l'hyperplan à l'infini ; cela revient à dés-homogénéiser P pour une autre variable que Z et résoudre cette nouvelle équation.

4.2 Ensembles algébriques projectifs

Le cadre est le suivant : on prend des polynômes de $\mathbb{K}[X_1, ..., X_{n+1}]$ et on veut regarder leurs zéros dans $\mathbb{P}_n(\mathbb{K})$. Pour cela le fait qu'ils s'annulent en $z \in \mathbb{K}^{n+1} \setminus \{0\}$ doit donc être indépendant du représentant choisi sur la droite $\mathbb{K}z$.

Définition 20. $z \in \mathbb{P}_n(\mathbb{K})$ *est un zéro de* $P \in \mathbb{K}[X_1, ..., X_{n+1}]$ *si pour tout choix* $(x_1 : ... : x_{n+1})$ *de coordonnées homogènes de* z, $P(x_1, ..., x_{n+1}) = 0$
Si S *est un ensemble de polynômes de* $\mathbb{K}[X_1, .., X_{n+1}]$ *on appelle V(S) la variété projective de* S *définie par*

$$V(S) = \{z \in \mathbb{P}_n(\mathbb{K}), \forall P \in S, z \text{ est un zero de } P\}$$

Un ensemble algébrique projectif est un tel ensemble

De même soit $X \subset \mathbb{P}_n(\mathbb{K})$, l'idéal de X est

$$I(X) = \{P \in \mathbb{K}[X_1, ..., X_{n+1}], \forall z \in X, z \text{ est un zero de } P\}$$

Proposition 16. *(i) $I = (S) \Rightarrow V(I) = V(S)$*
(ii) $I(X)$ est un idéal homogène de $\mathbb{K}[X_1, ..., X_{n+1}]$

Démonstration. (i) $S \subset I$ donc $V(I) \subset V(S)$
Si $z \in V(S)$, $\forall P \in S, (z_1 : ... : z_n) = z \Rightarrow P(z_1, .., z_n) = 0$
$P \in I \Rightarrow P = \sum j = 1^k P_j A_j$ où les P_j sont dans S.
$(z_1 : ... : z_{n+1}) = z \Rightarrow P(z_1, ..., z_{n+1}) = \sum_{j=1}^{k} P_j(z_1, .., z_{n+1}) A_j(z_1, .., z_{n+1}) = 0$
Donc $z \in V(I)$, $V(I) = V(S)$
(ii) I est un idéal car P,Q s'annulent en $(z_1, ..., z_{n+1}) \Rightarrow$ P+Q et AP s'y annulent
Soit $P = \sum_{i=0}^{N} P_i$ écrit dans sa décomposition homogène.
$P(z) = 0 \Leftrightarrow \forall (z_1 : ... : z_{n+1}) = z,\ P(z_1, .., z_{n+1}) = 0$
$\cdot \quad \Leftrightarrow \forall (z_1 : ... : z_{n+1}) = z, \forall \lambda \in \mathbb{K}^*,\ P(\lambda z_1, ..., \lambda z_{n+1}) = 0$
$(\lambda \to \infty) \Rightarrow \forall (z_1 : ... : z_{n+1}) = z,\ P_N(z_1, .., z_{n+1}) = 0$
$\cdot \quad \Rightarrow P_N(z) = 0$
Cela prouve $P \in I(X) \Rightarrow P_N \in I(X)$
C'est un idéal donc $P - P_N \in I(X)$. On conclut par récurrence sur N que
$\forall i, P_i \in I(X)$ donc I(X) est homogène. □

La caractérisation des idéaux homogènes (section 2.2) permet donc d'établir la correspondance bijective suivante :
{idéaux homogènes de $\mathbb{K}[X_1, ..., X_{n+1}]$} $\leftrightarrow$ {ensembles algébriques de $\mathbb{P}_n(\mathbb{K})$}

Définition 21. *Soit V un ensemble algébrique projectif.*
V irréductible $\Leftrightarrow$ V n'est pas l'union de deux sous ensembles algébriques stricts.
On dit alors que V est une variété projective

Pour ne pas recommencer les démonstrations de toutes les propriétés affines on établit le lien entre les variétés affines et projectives par le cône.

Définition 22. *Soit V un ensemble algébrique projectif le cône sur V est*

$$C(V) = \{(z_1, ..., z_{n+1}) \in \mathbb{K}^{n+1}, (z_1 : ... : z_{n+1}) \in V\} \cup \{0\}$$

On note pour l'instant I_a et V_a les opérations I et V affines dans $\mathbb{K}[X_1, ..., X_{n+1}]$ et $\mathbb{K}^{n+1}$
On note donc I_p et V_p les opérations I et V projectives dans $\mathbb{K}[X_1, ..., X_{n+1}]$ et dans $\mathbb{P}_n(\mathbb{K})$

Proposition 17. *Si $V \neq \emptyset$ alors $I_a(C(V)) = I_p(V)$*
Si I idéal homogène tel que $V_p(I) \neq \emptyset$, alors $C(V_p(I)) = V_a(I)$

Démonstration. $P \in I_a(C(V)) \Leftrightarrow \forall (z_1 : ... : z_{n+1}) \in V, P(z_1, .., z_{n+1}) = 0$
$\cdot \quad \Leftrightarrow P \in I_p(V)$
$z \in C(V_p(I)) \Rightarrow (z_1 : ... : z_{n+1}) \in V_p(I)$
$\cdot \quad \Rightarrow \forall P \in IP(z_1, .., z_{n+1}) = 0$

$\cdot \quad \Rightarrow z \in V_a(I)$
$z \in V_a(I) \Rightarrow \forall P \in I, P(z_1, .., z_{n+1}) = 0$
$\cdot \quad \Rightarrow \forall P \in I$ homogène $P(z_1, .., z_{n+1}) = 0$ (car I homogène)
$\cdot \quad \Rightarrow \forall \lambda \in \mathbb{K}^*, \forall P \in I$ homogène $P(\lambda z) = 0$
$\cdot \quad \Rightarrow \forall P \in I$, P s'annule sur la droite $z\mathbb{K}$
$\cdot \quad \Rightarrow (z_1 : ... : z_{n+1}) \in V_p(I)$
$\cdot \quad \Rightarrow (z_1, ..., z_{n+1}) \in C(V_p(I))$ □

Cela permet de se ramener au cas affine.

Théorème 9. *Nullstellensatz projectif :*
(i) $V_p(I) = \emptyset \Leftrightarrow \exists N \in \mathbb{N}$, *I contient tout P homogène tel que* $deg(P) \geq N$
(ii) $V_p(I) \neq 0$, *alors* $I_p(V_p(I)) = \sqrt{I}$

Démonstration. Soit I idéal de $\mathbb{K}[X_1, ..., X_{n+1}]$
(i)$V_p(I) = \emptyset \Leftrightarrow V_a(I) \subset \{0\}$
$\cdot \quad \Leftrightarrow I_a(V_a(I)) \supset (X_1, ..., X_{n+1})$
$\cdot \quad \Leftrightarrow \sqrt{I} \supset (X_1, ..., X_{n+1})$
$\cdot \quad \Leftrightarrow \exists N \in \mathbb{N}, (X_1, ..., X_{n+1})^N \subset I$
$\cdot \quad \Leftrightarrow$ I contient tous les homogènes de degré supérieur à N
(ii) $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \sqrt{I}$ □

Les conséquences du Nullstellensatz sont les mêmes que dans le cas affine mis à part qu'on doit considérer le cas particulier de l'idéal $(X_1, ..., X_{n+1})$
On a des correspondance bijectives :
{hypersurfaces V(P)} $\longleftrightarrow$ {P homogènes non constants à facteurs simples}
{hypersurfaces irréductibles} $\longleftrightarrow$ {P homogènes irréductibles}
{hyperplans irréductibles} $\longleftrightarrow$ {P homogènes de degré 1}

Les $V(X_i)$ sont les hyperplans coordonnés, ce sont les hyperplans projectifs à l'infini dans U_i. $n = 2$, les $V(X_i)$ sont les trois axes coordonnés

Définition 23. *Soit V variété projective, I(V) est premier*
$\Gamma_h(V) = \mathbb{K}[X_1, ..., X_{n+1}]$ *est l'anneau coordonné homogène (intègre).*
Plus généralement, si I homogène, $\Gamma = \mathbb{K}[X_1, ..., X_{n+1}]/I$
$p \in \Gamma$ *est homogène s'il existe* $P \in \mathbb{K}[X_1, .., X_{n+1}]$ *homogène,* $\overline{P} = p$.
Alors $deg(p) = \min_{\overline{P}=p}(deg(P))$
$\mathbb{K}_h(V)$ *est le corps des fractions de* $\Gamma_h(V)$
C'est le corps des fonctions homogènes de V.

Contrairement au cas affine les seuls éléments de $\Gamma_h(V)$ définissant des fonctions sur V sont les constantes. En revanche si $p, q \in \Gamma$ sont homogènes de degré d, p/q définit une fonction sur les points de V où $q \neq 0$:
$\frac{p}{q}(\lambda x) = \frac{p(\lambda x)}{q(\lambda x)} = \frac{\lambda^d}{\lambda^d}\frac{p}{q}(x) = \frac{p}{q}(x)$. Mais cela nécessite la proposition :

Proposition 18. $p \in \Gamma \Rightarrow p = \sum_{i=0}^{m} p_i$ *où les* p_i *sont homogènes de degré i.*
Cette écriture existe et est unique.

Démonstration. Soit P, $p = \overline{P}$, $deg(P) = deg(p) = m$
$P = \sum_{i=0}^{m} p_i$ donc $p = \sum_{i=0}^{m} \overline{P_i}$
unicité : Si $p = \sum_{i=0}^{m} \overline{P_i} = \sum_{i=0}^{m} \overline{Q_i}$ alors $P - \sum_{i=0}^{m} Q_i = \sum_{i=0}^{m} (P_i - Q_i) \in I$, comme I est homogène chaque $(P_i - Q_i) \in I$ donc $\forall i, \overline{P_i} = \overline{Q_i}$ □

Définition 24. *Le corps des fonctions sur V est* $\mathbb{K}(V)$ *défini par*
$\mathbb{K}(V) = \{f \in \mathbb{K}_h(V), \exists p, q \in \Gamma_h(V)$ *homogènes de même degré,* $f = \frac{p}{q}\}$
f est définie en z si il existe un tel représentant, $q(z) \neq 0$.
$\mathcal{O}_z(V) = \{f \in \mathbb{K}(V)$ *définies en z*$\}$
$\mathfrak{m}_z(V) = \{f \in \mathcal{O}_z(V), f(z) = 0\}$

C'est un sous corps strict de $\mathbb{K}_h(V)$. On n'a plus $\Gamma_h(V) \subset \mathbb{K}(V)$. Les seuls polynômes définissant une fonction sur un ensemble projectif sont constants.

4.3 Lien entre ensembles affines et projectifs

On voit désormais $\mathbb{K}^n$ comme un sous ensemble de $\mathbb{P}_n(\mathbb{K})$: on pourrait dire que c'est l'image de n'importe quel U_i par l'application φ_i. On choisit la $n+1$-ème :
$\varphi_{n+1} : U_{n+1} \longrightarrow \mathbb{K}^n$ c'est un homéomorphisme.
· $(z_1, ..., z_{n+1}) \mapsto (\frac{z_1}{z_{n+1}}, ..., \frac{z_n}{z_{n+1}})$
Donc on peut identifier $\mathbb{K}^n$ à $U_{n+1} = \{(z_1 : ... : z_{n+1}), z_{n+1} \neq 0\}$
Soit V un ensemble algébrique affine dans $\mathbb{K}^n$
Soit $I = I(V)$ idéal de $\mathbb{K}[X_1, ..., X_n]$ on note $I^* = (\{P^*, P \in I\})$
On définit pour V ensemble algébrique affine :

$$V^* = V(I^*) = V(I(V)^*)$$

De même soit V ensemble algébrique de $\mathbb{P}_n(\mathbb{K})$
$I = I(V)$ homogène dans $\mathbb{K}[X_1, ..., X_{n+1}]$, $I_* = (\{P_*, P \in I\})$
On définit pour V ensemble algébrique projectif :

$$V_* = V(I_*) = V(I(V)_*)$$

On remarque que $(V^*)_* = V$ pour V affine.

Pour la proposition, V,W désigneront toujours des ensembles algébriques, que ce soit de $\mathbb{K}^n$ ou de $\mathbb{P}_n(\mathbb{K})$ qu'on précisera. On note $H_\infty = \mathbb{P}_n(\mathbb{K}) \setminus U_{n+1}$

Proposition 19. *(i)*$V \subset \mathbb{K}^n$, *alors* $\varphi_{n+1}^{-1}(V) = V^* \cap U_{n+1}$
(ii) $V \subset W \subset \mathbb{K}^n \Rightarrow V^* \subset W^* \subset \mathbb{P}_n(\mathbb{K})$
· $V \subset W \subset \mathbb{P}_n(\mathbb{K}) \Rightarrow V_* \subset W_* \subset \mathbb{K}^n$
(iii)$V \subset \mathbb{K}^n$ *irréductible* $\Rightarrow V^* \subset \mathbb{P}_n(\mathbb{K})$ *irréductible*
(iv) $V = \bigcup_{i=1}^{N} V_i$ *décomposition irréductible* $\Rightarrow V^* = \bigcup_{i=1}^{N} V_i^*$ *décomposition de* V^*
(v) $V \subset \mathbb{K}^n \Rightarrow V^*$ *est le plus petit ensemble algébrique de* $\mathbb{P}_n(\mathbb{K})$ *contenant V.*
(vi)$V \subsetneq \mathbb{K}^n \Rightarrow$*aucune composante de* V^* *n'est incluse dans ou ne contient* H_∞
(vii)Si $V \subset \mathbb{P}_n(\mathbb{K})$ *et aucune composante de V ne contient* H_∞ *ni n'est incluse dans* H_∞, *alors* $V_* \subsetneq \mathbb{K}^n$ *et* $(V_*)^* = V$

Démonstration. (i) et (ii) découlent directement des définitions
(iii) : Soit V irréductible, $I = I(V)$ est premier. Un polynôme homogène P de $\mathbb{K}[X_1, ..., X_{n+1}] \in I^*$ si et seulement si $P_* \in I$ par définition.
Comme I est premier I^* est donc premier. Ainsi V^* irréductible.
(v) : Soit W ensemble algébrique de $\mathbb{P}_n(\mathbb{K})$ contenant $\varphi_{n+1}^{-1}(V)$. Si $P \in I(W)$, $P_* \in I(V)$ alors $P = X_{n+1}^r(P_*)^* \in I(V)^*$
Donc $I(W) \subset I(V)^*$ et donc $W \supset V^*$.
(iv) découle de (ii), (iii), et (v)
(vi) On suppose V irréductible. $V^* \not\subset H_\infty$ par (i).
Si $H_\infty \subset V^*$ on a $I(V)^* \subset I(V^*) \subset I(H_\infty) = (X_{n+1})$. Mais si $P \in I(V)$ non nul $P^* \in I(V)^*$ alors que $P^* \notin (X_{n+1})$. Donc $V^* \not\supset H_\infty$.
(vii) Soit $V \subset \mathbb{P}_n(\mathbb{K})$ irréductible. Il suffit de prouver que :
$\varphi^{-1}(V_*) \subset V \Rightarrow [V \subset (V_*)^*$ ou $I(V_*)^* \subset I(V)]$
Soit $P \in I(V_*), \exists N \in \mathbb{N}, P^N \in I(V)_*$ (Nullstellensatz). Donc $X_{n+1}^t(P^N)^* \in I(V)$. Comme I(V) premier, $X_{n+1} \notin I(V)$ et $(P^*)^N = (P^N)^*$, $P^* \in I(V)$ □

Pour V algébrique de $\mathbb{K}^n$ on appelle V^* la fermeture projective de V. On a une correspondance bijective entre les variétés projectives de $\mathbb{P}_n(\mathbb{K})$ non incluses dans H_∞ et les variétés algébriques de $\mathbb{K}^n$.
Si $V \subset \mathbb{K}^n$ et V^* sa fermeture projective, pour $p \in \Gamma_h(V^*)$ on définit p_* par : soit $P \in \mathbb{K}[X_1, ..., X_{n+1}]$ dont le $I(V^*)$ résidu est p, alors
$p_* \in \Gamma(V)$ est le (I(V)) résidu de P_*, ne dépend pas du choix de P.

$$\begin{array}{c} \Gamma_h(V^*) \xrightarrow{\sim} \Gamma(V) \\ p \longmapsto p_* \end{array}$$

De même on a

$$\begin{array}{c} \mathbb{K}(V) \xrightarrow{\sim} \mathbb{K}(V^*) \\ \frac{p}{q} \longmapsto \frac{p^*}{q^*} \end{array} \qquad\qquad \begin{array}{c} \mathcal{O}_z(V) \xrightarrow{\sim} \mathcal{O}_z(V^*) \\ \frac{p}{q} \longmapsto \frac{p^*}{q^*} \end{array}$$

5 Courbes planes projectives

En se servant des parties précédentes, nous allons appliquer les propriétés qu'on a établi au cas $n = 2$ des courbes algébriques planes. On prend $\mathbb{K}$ un corps algébriquement clos.

5.1 Préliminaires

On a déjà vu qu'une courbe projective plane est une hypersurface de $\mathbb{P}_2(\mathbb{K})$.
Mais cette définition ne permet que de connaître les points de la courbe et pas leurs multiplicités, leurs anneaux locaux...
On donne donc une nouvelle définition comme on l'a fait pour les courbes planes affines en section 3

Définition 25. *Une courbe plane projective est une classe d'équivalence de polynômes homogènes pour la relation* $P \sim Q \Leftrightarrow \exists \lambda \in \mathbb{K}^*, P = \lambda Q$
On note une courbe $V'(P) = \{Q \in \mathbb{K}[X, Y, Z] homogènes,\ P \sim Q\}$
Le degré d'une courbe est le degré des polynômes qu'elle contient.

On va noter à nouveau $\mathcal{O}_z(P)$ au lieu de $\mathcal{O}_z(V(P))$ où $z = (a : b : c)$ est un point projectif de $V(P)$ et P un polynôme homogène de $\mathbb{K}[X, Y, Z]$.

Proposition 20. *Quand* $z = (a : b : 1)$, $\mathcal{O}_z(P)$ *est isomorphe à* $\mathcal{O}_{(a,b)}(P_*)$

Démonstration. Il suffit de voir que $V(P_*)^* = V(P)$
Alors on a prouvé en section 4 que $\frac{f}{g} \mapsto \frac{f^*}{g^*}$ est une bijection de $\mathcal{O}_{(a,b)}(V(P_*))$ vers $\mathcal{O}_{(a,b,1)}(V(P))$ □

On a $V'(P(X, Y, 1)) = V'(P_*)$ est la courbe affine correspondant à V'(P).

En section 3 on a prouvé que la multiplicité d'un point sur une courbe affine ne dépend que de l'anneau local. La multiplicité d'un point sur la courbe projective V(P) est la multiplicité de ce point en dés-homogénéisant P :
$m_z(P) = m_{z'}(P_*)$. A priori cela varie selon l'indéterminée qu'on choisit constante.

Proposition 21. $m_z(P)$ *est indépendant de la façon de dés-homogénéiser P*

Démonstration. Soit $z = (a : b : c)$ et $m_z(P)_X = m_{(\frac{b}{a}, \frac{c}{a})}(P(1, Y, Z))$ si $a \neq 0$;
$m_z(P)_Y = m_{(\frac{a}{b}, \frac{c}{b})}(P(X, 1, Z))$ si $b \neq 0$;
$m_z(P)_Z = m_{(\frac{a}{c}, \frac{b}{c})}(P(X, Y, 1))$ si $c \neq 0$.
Si un seul des trois est défini, la propriété est triviale.
Si deux sont définis, on va dire $m_z(P)_X$ et $m_z(P)_Y$, la propriété précédente nous donne un isomorphisme entre les anneaux locaux. Les multiplicités correspondantes sont alors égales car ne dépendent que de l'anneau local (théorème prouvé en section 3). De même quand trois sont définis. □

Définition 26. $m_z(P)$ *est la multiplicité de z dans V'(P)*

Lemme. *Soient* $z_1, ..., z_m$ *des points distincts de* $\mathbb{P}_2(\mathbb{K})$.
Il existe $V(L)$ *une droite projective ne passant par aucun des* z_i

Démonstration. Soit L homogène de degré 1 noté $L = uX + vY + wZ$.
On note $z_i = (a_i : b_i : c_i) \in \mathbb{P}_2(\mathbb{K})$ et $z_i' = (a_i, b_i, c_i) \in \mathbb{K}^3 \setminus \{0\}$

$z = (a : b : c) \in V(L) \Rightarrow (a, b, c) \in C(V(L))$
. $\Rightarrow au + bv + cw = 0$
. $\Rightarrow (u, v, w) \in (a, b, c)^{\perp}$
Donc la négation du lemme signifierait :
$\forall L$ droite projective, $\exists i, z_i \in V(L)$. Donc
$\forall (u, v, w) \in \mathbb{K}^3 \setminus \{0\}$, $\exists i, (u, v, w) \in (a_i, b_i, c_i)^{\perp}$
Donc $\mathbb{K}^3 = \bigcup_{i=1}^{m} z_i'^{\perp}$ où $\forall i, z_i' \neq 0$. On voit une contradiction par exemple en disant que le terme de droite est d'intérieur vide dans $\mathbb{K}^3$, ou encore en disant qu'une telle union est V(P) pour $P = \prod_{i=1}^{m} (a_i X + b_i Y + c_i Z)$, le polynôme étant non nul elle est d'intérieur vide. □

Proposition 22. *Soient $(z_1, ..., z_m)$ points projectifs fixés*
(i)Il existe une carte de $\mathbb{P}_n(\mathbb{K})$ dans laquelle aucun des z_i n'est à l'infini.
(ii)$\mathbb{K}(\mathbb{K}^2) \cong \mathbb{K}(\mathbb{P}_2(\mathbb{K}))$

Démonstration. Une carte est la donnée d'une droite projective qui se retrouve à l'infini. Une telle carte existe d'après le lemme précédent.
(ii) Soient L et L' deux "droites" comme dans le lemme précédent. Soit P homogène de degré d. Alors
$P_* = P/L^d \in \mathbb{K}(\mathbb{P}_2(\mathbb{K}))$, cette dés-homogénéisation dépend de L. On a
$P/L'^d = (L'/L)^d P_*$. L'/L est une unité de $\mathcal{O}_{z_i}(\mathbb{P}_2(\mathbb{K}))$
Donc $\mathbb{K}(\mathbb{P}_2(\mathbb{K})) \cong \mathbb{K}(\mathbb{K}^2)$ s'identifient naturellement et le P_* ainsi défini correspond à P(X,Y,1) par la propriété précédente. □

Définition 27. *Soit $Q \in \mathbb{K}[X, Y, Z]$ homogène, z point simple de V'(P) tels que $Q_* \in \mathcal{O}_z(\mathbb{P}_2(\mathbb{K}))$ (avec une dés-homogénéisation comme précédemment). Alors $\mathcal{O}_z(P)$ est un anneau à valuation discrète donc on définit :*
$ord_z^P(Q) = ord_z^P(\overline{Q_*})$

Définition 28. *Soient V'(P),V'(Q) des courbes projectives, $z \in \mathbb{P}_2(\mathbb{K})$.*
$I(z, P \cap Q) = dim_K(\mathcal{O}_z(\mathbb{P}_2(\mathbb{K}))/(P_*, Q_*))$

$I(z, P \cap Q)$ est indépendant de la dés-homogénéisation et vérifie les 9 propriétés énoncées en section 3 mis à part que :
(3') $I(T(z), P \cap Q) = I(z, P \circ T \cap Q \circ T)$ est vrai pour tout changement T de coordonnées projectives
(7)$I(z, P \cap Q) = I(z, P \cap (Q + AP))$, A homogène et $deg(A) + deg(P) = deg(Q)$

Définition 29. *V(L) droite tangente à V(P) en z si $I(z, P \cap L) > m_z(P)$*
z point ordinaire multiple de V'(P) si V'(P) a $m_z(P)$ tangentes distinctes en z
P et Q sont projectivement équivalents si $Q = P \circ T$ pour un certain T changement projectif de coordonnées.

5.2 Théorème de Bézout

Proposition 23. $\sharp\{$*monômes unitaires de* $\mathbb{K}[X,Y,Z]\} = \frac{(d+1)(d+2)}{2}$

Démonstration. Un monôme unitaire de degré d de $\mathbb{K}[X,Y,Z]$ est la donnée de :
$X^iY^jZ^k$ où $i+j+k=d$
Il y en a autant que des entiers i,j,k vérifiant $i+j+k=d$:

$$N = \sharp\{(i,j,k), i+j+k=d\} = \sum_{i+j+k=d} 1 = \sum_{k=0}^{d} \sum_{i+j=d-k} 1$$
$$= \sum_{k=0}^{d} \sum_{i+j=k} 1 = \sum_{k=0}^{d} \sum_{j=0}^{k} 1 = \sum_{k=0}^{d} (k+1) = \sum_{k=1}^{d+1} k = \frac{(d+1)(d+2)}{2}$$ □

Se donner un polynôme homogène revient à avoir une famille $(a_i)_{1\leq i\leq N}$ non tous nuls avec $N = \frac{(d+1)(d+2)}{2}$
On note $(M_i)_{1\leq i\leq N}$ les N monômes unitaires de degré d. On a $N-1 = \frac{d(d+3)}{2}$
Une courbe projective plane est la donnée de $(a_i)_{1\leq i\leq N}$ non tous nuls définis à multiplication scalaire près, ainsi :

Proposition 24. *L'ensemble des courbes projectives planes de degré d est un* $\mathbb{K}$ *espace projectif de dimension (N-1),* $N = \frac{(d+1)(d+2)}{2}$

Théorème 10. *(théorème de Bézout) Soient V'(P),V'(Q) courbes projectives planes de degrés respectifs n et m. On suppose P et Q sans facteurs communs. Alors*

$$\sum_{z\in V(P,Q)} I(z, P\cap Q) = n * m$$

Démonstration. $V(P)\cap V(Q)$ est fini car tous les points d'intersection projectifs sont dans une des trois cartes et dans chaque carte le nombre d'intersections entre V(P) et V(Q) est fini.
D'après une proposition énoncée en section 5, on peut donc choisir une carte de $\mathbb{P}_2(\mathbb{K})$ contenant $V(P)\cap V(Q)$.
Dans cette carte, on se ramène donc à l'étude des ensembles affines $V'(P_*)$ et $V'(Q_*)$ qui ont les mêmes propriétés que V'(P) et V'(Q).
Donc $\sum_{z\in V(P,Q)} I(z, P\cap Q) = \sum_{z\in V(P_*,Q_*)} I(z, P_*\cap Q_*)$
Par la propriété 9 des nombres d'intersections énoncée en section 3, on a
$\sum_{z\in V(P_*,Q_*)} I(z, P_*\cap Q_*) = \sum_{z\in V(P_*,Q_*)} dim_{\mathbb{K}}(\mathbb{K}[X,Y]/(P_*,Q_*))$
Soit $\Gamma_* = \mathbb{K}[X,Y]/(P_*,Q_*)$
$\Gamma = \mathbb{K}[X,Y,Z]/(P,Q)$
On note R pour désigner $\mathbb{K}[X,Y,Z]$
Soit $R_d = \{$Polynômes homogènes de $\mathbb{K}[X,Y,Z]$ de degré d$\}$
Soit $\Gamma_d = \{\overline{P}, P\in R_d\}$
Il suffit de montrer $dim_{\mathbb{K}}(\Gamma_*) = dim_{\mathbb{K}}(\Gamma_d) = mn$ pour d suffisamment grand et on aura le résultat

Étape 1 : $dim_{\mathbb{K}}(\Gamma_d) = mn$ quand $d \geq m+n$
Soit $\pi : R \to \Gamma$ la surjection canonique

$\varphi : R \times R \to R$
. $(A, B) \mapsto (AP + BQ)$
$\psi : R \to R \times R$
. $C \mapsto (QC, -PC)$
La suite suivante est exacte :

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \longrightarrow 0$$

π surjective et ψ injective se voient facilement
$\varphi(A, B) = 0 \Leftrightarrow AP + BQ = 0 \Leftrightarrow AP = -BQ$ et P,Q sans facteurs communs
. $\Leftrightarrow Q \mid A$, $CQ = A$, $CQP = -BQ$
. $\Leftrightarrow (A, B) = (CQ, -PC) = \psi(C)$
Donc $Ker(\varphi) = Im(\psi)$
$\pi(D) = 0 \Leftrightarrow D = AP + BQ \Leftrightarrow D = \varphi(A, B)$
Donc $Ker(\pi) = Im(\varphi)$
La suite est exacte, on restreint les ensembles :

$$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-n} \times R_{d-m} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \longrightarrow 0$$

Elle reste exacte quand $d \geq m + n$ car $deg(P) = n$, $deg(Q) = m$. Donc
$dim(\Gamma_d) + dim(R_{d-n}) + dim(R_{d-m}) = dim(R_d) + dim(R_{d-m-n})$
$2 * dim(\Gamma_d) = (d+1)(d+2) + (d-m-n+1)(d-m-n+2) - (d-n+1)(d-n+2) - (d-m+1)(d-m+2)$
$= d^2(2-2) + 3d + 2 - 2dm - 2dn + 3d + 2mn - 3m - 3n + n^2 + m^2 + 2 + 3n + 2dn - 3d - n^2 - 2 - 2 + 3m - m^2 + 2dm - 3d$
$= 2mn$ Donc $dim_{\mathbb{K}}(\Gamma_d) = mn$

Étape 2 : on veut prouver : $ZC = AP + BQ \Rightarrow C = A'P + B'Q$
Soient $A, B \in \mathbb{K}[X, Y, Z]$
Pour $J \in \mathbb{K}[X, Y, Z]$ on note $J_0 = J(X, Y, 0) \in \mathbb{K}[X, Y]$
On suppose que Z=0 est la droite à l'infini donc disjointe avec les points de $V(P) \cap V(Q)$. Donc P_0 et Q_0 sont homogènes premiers entre eux dans $\mathbb{K}[X, Y]$. On suppose $ZC = AP + BQ$
$A_0P_0 + B_0Q_0 = 0$, $P_0 \mid B_0$ donc $P_0D = B_0$, on en déduit $A_0 = -Q_0D$
Soient $A_1 = A + QD$ et $B_1 = B - PD$ alors $(A_1)_0 = 0 = (B_1)_0$
Donc $Z \mid A_1$, $A_1 = ZA'$, $Z \mid B_1$ donc $B_1 = ZB'$
Alors $ZC = Z(A'P + B'Q)$ d'où $C = A'P + B'Q$ comme voulu.
Ainsi $\alpha : \Gamma \to \Gamma$ (où la barre est le reste modulo (P,Q)) est injective .
. $\overline{C} \mapsto \overline{ZC}$

Étape 3 : Base de Γ_*
Soit $d \geq m + n$ et $(A_1, ..., A_{mn}) \in R_d$ dont les résidus forment une base de Γ_d. $\forall i$ on note $(A_i)_* = A_i(X, Y, 1)$ le dés-homogénéisé de A_i et $a_i = \overline{(A_i)_*}$ son résidu dans Γ_*.
On remarque que le α de l'étape 2 se restreint à un isomorphisme de Γ_d sur Γ_{d+1} quand $d \geq m + n$ (α injective et les dimensions sont égales).
Donc $\forall r \geq 0$, les résidus des $(Z^r A_i)$ forment une base de Γ_{d+r}
(i) les a_i génèrent Γ_*
Soit $c = \overline{C} \in \Gamma_*$, $C \in \mathbb{K}[X, Y]$. Il existe $N \in \mathbb{N}$, $Z^N C^*$ est homogène de degré $d + r$ alors
$Z^N C^* = \sum_{i=1}^{mn} \lambda_i Z^r A_i + SP + TQ$ où les $\lambda_i \in \mathbb{K}$, $S, T \in \mathbb{K}[X, Y, Z]$
$H = (Z^N H^*)_* = \sum_{i=1}^{mn} \lambda_i (A_i)_* + S_*P_* + T_*Q_*$ et en réduisant modulo (P_*, Q_*)

on a $h = \sum_{i=1}^{mn} \lambda_i a_i$
(ii) Les a_i forment une famille libre :
Supposons $\sum_{i=1}^{mn} \lambda_i a_i = 0$ alors cela s'écrit
$\sum_{i=1}^{mn} \lambda_i (A_i)_* + BP_* + CQ_* = 0$ dans $\mathbb{K}[X,Y]$ puis
$Z^r \sum_{i=1}^{mn} \lambda_i (A_i) + Z^s B^* P + Z^t C^* Q = 0$ dans $\mathbb{K}[X,Y,Z]$, chaque de degré d+r. On réduit dans Γ_{d+r} modulo (P,Q)
$\sum_{i=1}^{mn} \lambda_i \overline{Z^r A_i} = 0$ mais ces derniers formant une base de Γ_{d+r} on en déduit que les λ_i sont tous nuls.
Ainsi $dim_{\mathbb{K}}(\Gamma_*) = dim_{\mathbb{K}}(\Gamma_{d+r}) = mn$
Donc

$$\sum_{z \in V(P,Q)} I(z, P \cap Q) = n * m$$

□

Corollaire. *Si $\sharp(V'(P) \cap V'(Q)) > nm$, P et Q ont un facteur commun.*

Corollaire. *Si P,Q n'ont pas de facteur commun, $\sum_z m_z(P) m_z(Q) \leq deg(P) deg(Q)$*

Corollaire. *Soient $P, Q \in \mathbb{K}[X,Y]$ de degrés n, m sans facteurs communs.*
Alors les courbes V'(P) et V'(Q) s'intersectent en nm points projectifs.
Ces points sont les intersections de $V'(P^*)$ et $V'(Q^*)$

5.3 Nombre d'intersections en pratique

Comme on l'a mentionné plus tôt, la preuve d'unicité du nombre d'intersection donne un algorithme à appliquer sur P et Q pour trouver leur nombre d'intersections en 0 :

Le voici programmé en scilab :

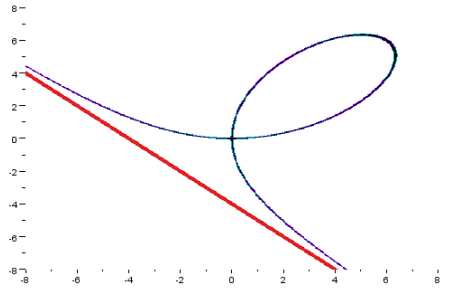
```
function z=inter0(P,Q)
.    n=0
.    while (P(1,1)==0 and Q(1,1)==0) do      cas plancher : 0 n'annule pas P, Q
.       p=degX(P)
.       q=degX(Q)
.       if p>q then
.          k=x
.          x=y
.          y=k
.          p=degX(P)
.          q=degX(Q)
.          end                    On met P en degre inferieur
.       if degX(P)==0 then
.          n=n+firstX(Q)                cas r = 0
.          P=divY(P)
```

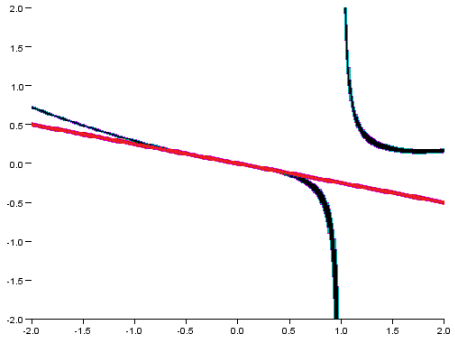
```
.            else
.            lambda=Q(1,q+1)/P(1,p+1)
.            Q=Q-mulX(q-p,lambda*P)          on reduit le degre de Q
.            end
.        end
.    z=n
endfunction
```

P(1,1) est le terme constant du polynôme P.
degX(P) renvoie le degré de P(X,0)
firstX(P) renvoie la plus haute puissance de X divisant P
mulX(P) renvoie XP
divY(P) renvoie P/Y

Le n retourné à la fin est le nombre voulu

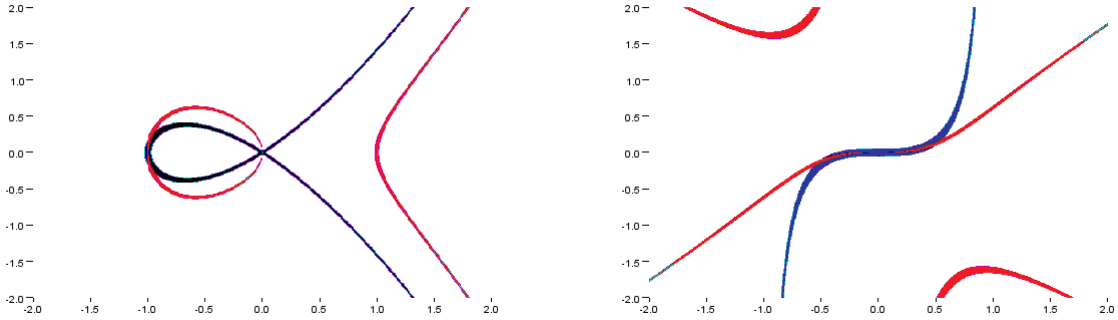
L'algorithme est écrit comme dans la preuve, et permet de trouver le nombre d'intersections du polynôme en 0, pour trouver les points d'intersection un calcul est nécessaire, l'algorithme permet juste de les compter en 0.





Exemple. $P = X + Y + 4$ *et* $Q = X^3 + Y^3 - 12XY$.
La figure de gauche représente V(P) (droite rouge) et V(Q) (courbe bleue) dans le plan complexe (carte $z = 1$*).*
On remplace Y *par* $'(X + 4)$ *dans l'équation de* Q*; on a alors l'équation* $-64 = 0$
Moralité : V(P) et V(Q) n'ont pas d'intersection complexe.
$P^* = X + Y + 4Z$ *on va les déshomogénéiser dans une autre carte :*
$Q^* = X^3 + Y^3 - 12XYZ$
carte $Y = 1$ *:* $P_0 = X + 1 + 4Z$ *et* $Q_0 = X^3 + 1 - 12XY$
La figure de droite représente V(P) (droite en rouge toujours) et V(Q) (courbe bleue) dans la carte $y = 1$.
L'analyse donne 1 point d'intersection : $z = 0; x = -1; y = 1$
On applique le programme après translation du polynôme : T(0,0)=(-1,0)
T(x,z)=(x-1,z)
$P_0 \circ T(X, Z) = X + 4Z$
$Q_0 \circ T(X, Z) = X^3 - 3X^2 + 3X - 12XZ + 12Z$

Le programme évalué en P_0, Q_0 donne $n = 3$
On représente à gauche les courbes dans la carte $z = 1$, à droite dans la carte $y = 1$.
Donc le seul point d'intersection de ces courbes est (-1 :1 :0) de multiplicité 3 et à l'infini dans la carte z=1 ; l'analyse de la troisième carte donne le même point d'intersection projectif car cela sort (1 :-1 :0) qui est bien sûr le même.



Exemple. *$P = Y^2 - X^3 + X = 0$ et $Q = Y^2 - X^3 - X^2 = 0$*
La figure de gauche est encore une fois la représentation de V(P) (en rouge) et V(Q) (en bleu) dans la carte $z = 1$.
La figure de gauche représente V(P) en bleu et V(Q) en vert dans la carte $y = 1$.
On cherche 9 points d'intersections par le théorème de Bézout.
L'analyse des points d'intersections complexes donne : (0,0) et (-1,0)
Chacun de ces deux points a un poids 2 : on exécute le programme pour ces deux polynômes tels quels et on a le nombre d'intersections en (0,0) ;
On exécute le programme pour les polynômes translatés de 1 en X :
$P_0 = Y^2 - X^3 + 3X^2 - 2X$ et $Q_0 = Y^2 - X^3 + 2X^2 - X$. Le nombre d'intersections en (-1,0) est alors 2 aussi. On a 4 points d'intersections complexes (figure de gauche).
On voit que celui de gauche (-1,0) est de multiplicité 2 car les courbes sont tangentes, l'autre est de multiplicité 2 car la courbe bleue passe deux fois en (0,0)
Il manque 5 points d'intersection : $P^* = Y^2Z - X^3 + XZ^2$ et $Q^* = Y^2Z - X^3 - X^2Z$ qu'on déshomogénéise dans la carte $y = 1$ (réprésenté sur la figure de droite) :
$p = Z - X^3 + XZ^2 = 0$ et $q = Z - X^3 - X^2Z = 0$; l'analyse donne une intersection en (0,0). On applique le programme et on constate que cette intersection est de multiplicité 5. Donc on a trouvé toutes les intersections de P et Q au nombre de 9.

Références

[1] William Fulton. *ALGEBRAIC CURVES*. 1969.

[2] Gaël Rémond. *Géométrie algébrique*. 2012.