Théorème de Bézout en géométrie algébrique

Présenté par : ESSAMET Mahmoud

Encadré par : Pr. GMIRA Seddik

Année Universitaire : 2011/2012

Dédicace

... **À mes parents** ...

... **À mes frères et sœurs**...

... **À mes amis et amies**...

... **À ceux qui m'aiment**...

... **A ceux qui m'ont soutenue de près ou de loin à l'élaboration de ce travail**...

REMERCIEMENTS

Tout d'abord, Je tiens à présenter mes profondes gratitude à mon professeur Mr. GMIRA Seddik pour ses aides précieuses, son soutien, son encouragement et ses conseils fructueux tout au long de la période de la réalisation de mon projet, ce qui mérite toute la reconnaissance de ma part. Mes respectueux remerciements s'adressent aussi à tous les membres du jury qui m'ont fait l'honneur de bien vouloir examiner ce travail et de l'enrichir par leurs remarques importantes. Je leur présente mes remerciements les plus respectueux.

Je remercie le corps professoral de ma formation, savoir le Master en " Homologie, Algèbre et Sécurité de l'Information " de la Faculté des Sciences et Technique de Fès pour leur contribution dans ma formation.

Finalement, mes chaleureux remerciements sont adresses à toute personne, ayant aidé à la réalisation de ce projet de fin d'étude, qu'elle trouve l'expression de ma reconnaissance la plus chaleureuse.

TABLE DES MATIÈRES

Introduction

Dans ce rapport, notre intérêt est centré sur le théorème de Bézout en géométrie algébrique, il permet de calculer le nombre de points d'intersection entre deux courbes algébriques ce travail se divise en quatre chapitres.

Le premier chapitre est un ensemble de rappels fondamentaux sur la théorie des idéaux et les anneaux, quelques résultats importants ont été repris et explicités à l'occasion.

Le deuxième chapitre contient un bon nombre de notions et résultats essentiels des variétés algébriques. La topologie de Zariski a été introduite d'une manière naturelle sur ces variétés algébriques. Une variété affine irréductible sera tout simplement un fermé de Zariski. En fin le théorème des zéros de Hilbert est entièrement traité avec sa démonstration dans cette partie.

Quant au troisième chapitre, tous les résultats essentiels des variétés affines ont été transposés aux variétés projectives, y compris le théorème des zéros de Hilbert.

Le dernier chapitre est exclusivement consacré au théorème de Bézout et sa démonstration.

CHAPITRE 1

PRÉLIMINAIRES

Dans ce premier chapitre nous faisons un rappel de quelque concepts et notions qui seront utiles pour ce qui suit.

1.1 Anneaux

Définition 1.1 *(Anneau noethérien) Un anneau est dit noethérien si toute chaîne d'idéaux* $I_1 \subset I_2 \subset \cdots$ *se stabilise*

Proposiftion 1.1 *Soit R un anneau. On a les équivalences suivantes :*

- *(i) R est noethérien*
- *(ii) Toute collection non vide d'idéaux de R possède un élément maximal.*
- *(iii)Tout idéal est de génération finie.*

Preuve : $(i) \Rightarrow (ii)$ Soit $\mathcal{S}$ une collection non vide d'idéaux de R. Par l'absurde, supposons qu'elle ne possède pas d'élément maximal. Cela signifie que pour tout élément I de S on peut trouver un idéal $I' \subset \mathcal{S}$ tel que $I \subset I'$. L'axiome du choix nous assurer qu'il existe une suite $(I_n)_{n\in\mathbb{N}}$ telle que $I_n \subset I_{n+1}$ pour tout n, contredisant le fait que R est noethérien.

$(ii) \Rightarrow (iii)$ Soit $I \subset R$ un idéal et $S = \{J \subset I \setminus\ J$ est un idéal de génération finie$\}$ qui n'est pas vide. Par hypothèse, $\mathcal{S}$ contient un élément maximal M. Si $M \neq I$, on choisit un élément $m \in I \setminus M$ et on obtient un idéal $M + mR$ qui ne peut être de génération finie (car M est strictement inclue dans $M + mR$), contradiction.

$(iii) \Rightarrow (i)$ Soit $I_1 \subset I_2 \subset \cdots$ une suite d'idéaux de R et posons $I = \cup_{i \in \mathbb{N}} I_i$. Par hypothèse, ils existent $r_1, \ldots, r_n \in R$ tels que $I =< r_1, \ldots, r_n >$. Si $N \in \mathbb{N}$ tel que $r_1, \ldots, r_n \in I_N$, alors la suite se stabilise en I_N.

Corollaire 1.1 *Soient A un anneau noethérien et M un R-module de type fini, Alors M est noethérien.*

Théorème 1.1 *(Théorème de la base de Hilbert) Soit R un anneau commutatif unitaire. Si R est noethérien, alors $R[x]$ est noethérien.*

Preuve : Soit I un idéal non nul de $R[X]$. Soit D le sous-ensemble de R formé de 0 et des coefficients dominants des polynômes non nuls appartenant à I. On voit facilement que D est un idéal de R. Par hypothèse, il est engendré par des éléments $\alpha_1, \ldots, \alpha_r$. Pour tout $i = 1, \ldots, r$, soit P_i un élément de I dont le coefficient dominant est α_i, et soit $d_i = degP_i$. Soit d le plus grand des d_i, et soit M le sous-R-module de $R[X]$ engendré par les monômes $1, X, \ldots, X_{d-1}$. Alors M est noethérien, d'après le corollaire précédant. Soit $N = M \cap I$ c'est un sous R-module de M. Alors N est de type fini, donc engendré comme R-module par des éléments $Q_1, \ldots, Q_s$. Alors, I est égal à l'idéal J engendré par

$$P_1, \ldots, P_r, Q_1, \ldots, Q_s.$$

En effet, montrons par récurrence sur n que tout élément non nul de I, de degré n, appartient à J. C'est clair si $n < d$, car dans ce cas $P \in N$ donc est combinaison R-linéaire de $Q_1, \ldots, Q_s$. Soit donc $n > d$ et supposons l'assertion établie pour tout $n' < n$. Soit $P \in I\ \{0\}$, de degré n, et soit a son coefficient dominant. Alors $a \in D$ donc il existe $a_1, \ldots, a_r \in A$ tels que

$$\alpha = a_1\alpha_1 + \ldots + a_r\alpha_r$$

Alors,

$$a_1\alpha_1 X^{n-d_1}P_1 + \cdots + a_r\alpha_r X^{n-d_1}P_r$$

a pour terme dominant αX^n, et donc

$$P - \sum_{i=1}^{r} a_i\alpha_i X^{n-d_i}P_i$$

est un élément de I de degré < n. Il appartient donc à J, par hypothèse de récurrence. Enfin, comme les P_i sont dans J, on a aussi $P \in J$. Ceci preuve le théorème.

Corollaire 1.2 *Soit $\mathbb{K}$ un corps. Pour tout $n \in \mathbb{N}$, $\mathbb{K}[x_1, \ldots, x_n]$ est noethérien.*

Preuve *:* La preuve se fait par récurrence. L'anneau $\mathbb{K}[x]$ est noethérien d'après théorème de la base de Hilbert.

Définition 1.2 *soit A un anneau unitaire commutatif :*

- *Une unité $u \in A$ est un élément qui possède un inverse,*
- *On dit que $a \in A$ est premier si ce n'est pas une unité et si $a = b.c \Rightarrow b$ ou c est une unité.*

Définition 1.3 *(Anneau factoriel) L'anneau R est dit factoriel si tout élément $a \in A \setminus \{0\}$ possède une décomposition $a = a_1 \cdots a_N$, où les a_h sont premiers.*

Théorème 1.2 *Si R est factoriel, alors $R[x]$ est factoriel.*

Définition 1.4 *(Anneau principal) Un anneau est dit principal si tout idéal est principal, c'est-à-dire de la forme $< a >$ où $a \in A$.*

Pour tout corps K, l'anneau $K[X]$ est principal : si $I \subset K[x]$ est un idéal non nul, on prend un élément non nul $f \in I$ dont le degré est minimal parmi les degrés des éléments non nuls de I, et on montre que $I =< f >$.

Par contre $K[X, Y]$ n'est pas principal car l'idéal $< x, y >$ ne peut être engendré par un seul polynôme.

Définition 1.5 *Soient A un anneau et I un sous ensemble de A. On dit que I est un idéal de A si :*

(i) $(I, +)$ *est un groupe commutatif.*

(ii) $\forall x \in I$, $\forall a \in A$, $ax \in I$.

Définition 1.6 *Soient A un anneau et P un idéal de A. On dit que P est premier si $P \neq A$ et $\forall x, y \in A$ on a :*

$$xy \in P \Longrightarrow x \in P \text{ ou } y \in P.$$

Définition 1.7 *(Radical d'un idéal et idéal radical) Soit I un idéal d'un anneau commutatif R.*

(i) *Le radical de I, noté $\sqrt{I}$, est $\sqrt{I} = \{r \in R \setminus \exists n \in \mathbb{N} \setminus \{0\}, r^n \in I\}$.*

(ii) *I est dit radical si $I = \sqrt{I}$.*

En particulier, $\sqrt{\{0\}}$ est l'ensemble des éléments nilpotents de R.

Définition 1.8 *(Anneau réduit) Un anneau est dit réduit s'il ne possède pas d'éléments nilpotents de R.*

Définition 1.9 *(Nilradical) Le nilradical d'un anneau R est l'ensemble des éléments nilpotents de R.*

Proposiftion 1.2 *Soit R un anneau commutatif et I son nilradical. Alors R/I est réduit.*

Preuve : Soit $r + I \in R/I$, $n \in \mathbb{N}$ tel que $(r + I)^n = 0$, c'est à dire $r^n \in I$. Ainsi, r est nilpotent et $r + I = \overline{0}$. Soit $\overline{r} \in R/I$. Supposons que $\overline{r}$ est nilpotent c'est à dire $\exists n \in \mathbb{N}$ tel que $(\overline{r})^n = \overline{0}$ i.e $\overline{r^n} = \overline{0}$ donc $r^n \in I$. puisque on a I le nilradical, alors $\exists m \in \mathbb{N}$ tel que $(r^n)^m = 0$ donc $r^{n.m} = 0$ alors $r \in I$ d'où $\overline{r} = \overline{0}$.

Définition 1.10 *(Ensemble multiplicatif) Soit R un anneau commutatif unitaire. Un sous-ensemble $S \subset R$ est dit multiplicatif si pour tous $s, s' \in S$ on a $ss' \in S$.*

Soit $S \subset R$ un ensemble multiplicatif. On définit une relation sur $R \times S$ comme suit :

$$(r,s) \sim (r',s') \Longleftrightarrow \exists s_0 \in S \text{ tel que } (rs' - sr')s_0 = 0$$

on montre qu'il s'agit bien d'une relation d'équivalence.

Notation : On écrit $\frac{r}{s}$ pour la classe d'équivalence de (r,s). L'ensemble des classes d'équivalence se note $S^{-1}R$.

Définition 1.11 *(Localisation) L'ensemble $S^{-1}R$ défini ci-dessus s'appelle localisation de R par rapport à S.*

Proposiftion 1.3 *Soit $S \subset R$ un ensemble multiplicatif. $S^{-1}R$ est un anneau commutatif unitaire pour les opérations définies par*

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \ \frac{r}{s}.\frac{r'}{s'} = \frac{rr'}{ss'}, \ \forall r, r' \in R, \ \ s, s' \in S$$

Proposiftion 1.4 *Soient A un anneau et P un idéal de A. On dit que P est premier si $P \neq A$ et :*

$$x.y \in P \Rightarrow x \in P \ ou \ y \in P.$$

Notation :Soient R un anneau, P un idéal premier et $S = R \setminus P$. Dans ce cas, on écrit R_P pour $S^{-1}R$.

Proposiftion 1.5 *R_p est un anneau local.*

Définition 1.12 *Soient R et S deux anneaux commutatifs unitaires tels que $R \subset S$. On dit que $v \in S$ est entier sur R s'il existe $a_1, ..., a_n \in R$ tels que :*

$$v^n + a_1 \cdot v^{n-1} + ... + a_n = 0$$

On dit que l'extension $R \subset S$ est entière si tout élément de S est entier sur R.

1.2 Anneaux gradués

Définition 1.13 *Un anneau gradué est un anneau R qui se décompose en une somme directe de sous groupes abolies $R = \bigoplus_{d \in N_0} R_d$ On demande de plus à ce que pour tous $d, e \in N_0$ on ait $R_d R_e \subset R_{d+e}$.*

Définition 1.14 *(Élément homogène) Dans la définition ci-dessus, un élément de R_d s'appelle élément homogène de degré d.*

Proposiftion 1.6 *Soient R un anneau gradué et I un idéal de R. Les conditions suivantes sont équivalentes :*

- $I = \bigoplus_{d \in N_0} (R_d \cap I)$
- *Il existe un ensemble générateur pour I constitué d'éléments homogènes.*

Définition 1.15 *(Idéal homogène) Un idéal d'un anneau gradué satisfaisant les deux conditions ci-dessus est appelé idéal homogène.*

Proposiftion 1.7 *Soient I et J deux idéaux homogènes d'un anneau gradué R. Alors : $I + J$, $I \cap J$ et IJ sont des idéaux homogènes.*

CHAPITRE 2

VARIÉTÉS AFFINES

On désignera par $\mathbb{K}$ un corps de caractéristique nulle, par exemple $\mathbb{R}$ ou $\mathbb{C}$. On notera $\mathbb{K}[X,Y]$ l'espace des polynômes en X et Y, à coefficients dans $\mathbb{K}$

2.1 Courbe algèbrique

Une courbe algèbrique plane est déterminée par une équation de la forme $f(x,y) = 0$ où $f \in \mathbb{K}[x,y]$. Notons que si on remplace f par $\lambda.f$, où $\lambda \in \mathbb{K}$, on obtient la même courbe. On note par $\sim$ la relation d'équivalence qui identifie $f, g \in \mathbb{K}[X,Y]\backslash\{0\}$ si elles sont sur une même droite passant par l'origine, c'est-à-dire s'il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $g = \lambda.f$.

Définition 2.1 *L'espace des courbes algèbriques est l'ensemble des classes définies par la relation $\sim$:*

$$\mathbb{P}(\mathbb{K}[x,y]) = \mathbb{K}[x,y] \setminus \{0\}/ \sim$$

Proposiftion 2.1 *Soit $\mathbb{K}[X,Y]_d$ le sous espace vectoriel de $\mathbb{K}[X,Y]$ des polynômes de degré plus petit ou égale à d*

$$dim(\mathbb{K}[X,Y]_d) = \binom{d+2}{2}$$

Preuve *:* Soit $P \in \mathbb{K}[X,Y]_d$ $(deg(P) \leq d)$ alors tous les monômes de P est inférieur ou égale à d c'est-à-dire $P(X,Y) = \sum_{i,j=0}^{d} a_{ij} X^i Y^j$ donc la famille $f := \{X^i Y^j\}_{0 \leq i,j \leq d, i+j \leq d}$ est un système générateur de $\mathbb{K}[X,Y]_d$.

On a f est une sous famille de $\{X^i Y^j\}_{i,j \in \mathbb{N}}$, et $\{X^i Y^j\}_{i,j \in \mathbb{N}}$ est une base de $\mathbb{K}[X,Y]$ alors f est libre.

Donc f est une base de sous-espace vectoriel $\mathbb{K}[X,Y]_d$ c'est-à-dire, $dim(\mathbb{K}[X,Y]_d) = card(f)$

$\forall i_0 \in \{0, \cdots, d\}$ on a $deg(X^{i_0} Y^j) \leq d$ c'est-à-dire $j \leq d - i_0$, alors $j \in \{0, \ldots, d - i_0\}$ donc le nombre des valeurs possible pour j est $d - i_0 + 1$, donc :

$$card(f) = (d+1) + d + (d-1) + \cdots + 1 = \frac{(d+2)(d+1)}{2} = \binom{d+2}{2}$$

.

Définition 2.2 $\mathbb{P}(\mathbb{K}[X,Y]_d) = \mathbb{K}[X,Y]_d \setminus \{0\}/\sim$ *est L'espace des courbes algèbriques de degré plus petit ou égal d :*

2.2 Topologie de Zariski

Ensembles algèbriques affines

Soit f un élément de $\mathbb{K}[X_1, \cdots, X_n]$. On dit qu'un point $x = (x_1, \cdots, x_n)$ de $\mathbb{K}^n$ est un zéro de f si $f(x) = 0$.

Définition 2.3 *Soit S une partie de l'anneau du polynômes $\mathbb{K}[X_1, \cdots, X_n]$. On note $\mathcal{V}(S)$ le sous-ensemble de $\mathbb{K}^n$ formé des zéros communs à tous les éléments de S. Les sous-ensembles de $\mathbb{K}^n$ de ce type sont les ensembles algèbriques affines (sous-variétés affines) de $\mathbb{K}^n$.*

Exemple 2.1 *:*

1. *On a $\mathcal{V}(1) = \emptyset$ car l'ensemble des zéro du polynôme $1(x_1, \cdots, x_n) = 0$ est $\emptyset$ et $\mathcal{V}(0) = \mathbb{K}^n$, car tout élément de $\mathbb{K}^n$ est une racine c nul.*

2. Dans $\mathbb{K}^2$ on a $\mathcal{V}(X_1^2) = \mathcal{V}(X_1)$ c'est l'axe des Y. Des parties différentes peuvent donner le même ensemble algèbrique.

Remarques :

- Pour S et S' deux parties de $\mathbb{K}[x_1, \ldots, x_n]$, $S \subset S'$ entraîne $\mathcal{V}(S') \subset \mathcal{V}(S)$ (les inclusions changent de sens).
- D'autre part si $< S >$ est un idéal engendré par S, on a $\mathcal{V}(S) = \mathcal{V}(< S >)$, l'anneau $\mathbb{K}[X_1, \cdots, X_n]$ étant noethérien, l'idéal $< S >$ est engendré par un nombre fini des polynômes $f_1, \ldots, f_r$, de sorte que $\mathcal{V}(S) = \mathcal{V}(< S >) = V(f_1, \ldots, f_r)$ En d'autre terme, tout ensemble algèbrique affine de $\mathbb{K}^n$ peut être défini par un nombre fini d'équations.

Définition 2.4 *Soit V un sous-ensemble de $\mathbb{K}^n$. On appelle idéal de V, l'ensemble des polynômes nuls sur V, et on le note $\mathcal{I}(V)$.*

Remarque : On a $S \subset \mathcal{I}(\mathcal{V}(S))$, mais il n'y a en général pas égalité, même lorsque S est un idéal ; par exemple $\mathcal{I}(\mathcal{V}(X^2)) =< X >$. La relation entre I et $\mathcal{I}(\mathcal{V}(I)$ est l'objet de Nullstellensatz.

Proposiftion 2.2 *:*

- *a) Toute intersection d'ensembles algèbriques affines de $\mathbb{K}^n$ est un ensemble algèbrique affine.*
- *b) Toute réunion finie d'ensembles algèbriques affines de $\mathbb{K}^n$ est un ensemble algèbrique affine*

Preuve :

- a) Il suffit de remarquer que $\bigcap_\alpha V(S_\alpha) = V(\bigcup_\alpha S_\alpha)$
- b) Il suffit de montrer que $V(S_1) \cup V(S_2)$ est égal à $V(S_1S_2)$ où S_1S_2 désigne l'ensemble des produits d'un élément de S_1 avec un élément de S_2

  si $x \notin V(S_1) \cup V(S_2)$, il existe F_1 dans S_1 et F_2 dans S_2 avec $F_1(x)$ et $F_2(x)$ non nuls, de sorte que $F_1F_2(x)$ est non nul, et $x \notin V(S_1S_2)$.

Topologie de Zariski sur $\mathbb{K}^n$

On définit cette topologie en prenant comme ensembles fermés les ensembles algèbriques, qu'on appelle aussi fermés de Zariski. En effet :

1. L'ensemble vide $\emptyset$ et $\mathbb{K}^n$ peuvent être considérés comme ensembles algèbriques :

$$\emptyset = \mathcal{V}(< 1 >),\ \mathbb{K}^n = \mathcal{V}(< 0 >)$$

2. proposition (4.2) montre que la réunion finie et l'intersection quelconque de fermés de Zariski est encore un fermé de Zariski.

les ouverts de cette topologie sont comme d'habitude, les complémentaires des fermés de Zariski, qu'on appelle ouverts de Zariski.

Proposiftion 2.3 *Toute suite décroissante de fermés est stationnaire.*

Preuve : Soit $(S_i)_{i\in\mathbb{N}}$ une suite décroissante de fermés de zariski. On a $S_i \subset S_{i+1}$, $\forall i \in \mathbb{N}$, alors $\mathcal{I}(S_{i+1}) \subset \mathcal{I}(S_i)$ donc $(\mathcal{I}(S_i))_{i\in\mathbb{N}}$ est une suite croissante des idéaux de $\mathbb{K}[x_1, \cdots, x_n]$ puisque l'anneau $\mathbb{K}[x_1, \cdots, x_n]$ est noethérien alors $(\mathcal{I}(S_i))_{i\in\mathbb{N}}$ est stationnaire, donc $\exists N_0 \in \mathbb{N}$ tel que $\forall i \geqslant N_0$ on a $\mathcal{I}(S_i) = \mathcal{I}(S_{N_0})$ comme les S_i sont des ensembles algèbriques on a $\mathcal{V}(\mathcal{I}(S_i)) = \mathcal{V}(\mathcal{I}(S_{N_0})) \Rightarrow S_i = S_{N_0}$, $\forall i \in \mathbb{N}$. Donc $(S_i)_{i\in\mathbb{N}}$ est stationnaire.

Topologie de Zariski et topologie transcendante

Dans ce paragraphe $\mathbb{K} = \mathbb{C}$ ou $\mathbb{R}$, on a donc une autre topologie sur $\mathbb{K}^n$, induite par la métrique euclidienne. Dans ce contexte, on l'appelle topologie transcendante. Puisque les polynômes sont des fonctions continues pour la topologie transcendante, les fermés de Zariski sont aussi fermés pour la topologie transcendante.

Si $x \in \mathbb{K}^n$ et $r \in \mathbb{R},\ r > 0$, on désignera par $B(x, r)$ la boule de centre x et de rayon r :

$$B(x, r) = \{y \in \mathbb{K}^n \ \mid \parallel x - y \parallel < r\}$$

On va établir quelques résultats qui lient ces deux topologies, par exemple les ouverts de Zariski non vides sont "très gros".

Proposiftion 2.4 *Soit $U \subset \mathbb{K}^n$ un ouvert de Zariski non vide. Alors, pour tout $x \in \mathbb{K}^n$ et tout $r > 0$ on a :*

$$B(x, r) \cap U \neq \emptyset$$

En d'autre terme, l'adhérence de U dans la topologie transcendante est $\mathbb{K}^n$ tout entier, ce qui s'exprime encore en disant que U est dense dans $\mathbb{K}^n$ pour la topologie transcendante.

Preuve : Supposons qu'il existerait $x \in \mathbb{K}^n$ et $r > 0$ tel que $B(x, r) \cap U = \emptyset$. En posant $F = \mathbb{K}^n \backslash U$, ceci implique que $B(x, r) \subset F$, qui est un fermé de Zariski, donc lieu de zéros du polynômes : $F = \mathcal{V}(< f_1, \cdots, f_k >)$. Mais ces f_i doivent s'annuler sur toute la boule $B(x, r)$, donc ils sont identiquement nuls, ce qui impliquerait que $F = \mathbb{K}^n$ et donc $U = \emptyset$.

Corollaire 2.1 *: Si $U_1, \ldots, U_k \subset \mathbb{K}^n$ sont des ouverts de Zariski non vides, alors leur intersection $U_1 \cap \ldots \cap U_k$ est un ouvert de Zariski non vide.*

Preuve : il suffit de faire la preuve pour $k = 2$. comme U_1 est non vide, il existe $x \in U_1$ et $r > 0$ tel que $B(x, r) \subset U_1$. U_2 est ouvert pour la topologie transcendante d'après (2.3) $B(x, r) \cap U_2 \neq \emptyset$ donc $\emptyset \neq B(x, r) \cap U_2 \subset U_1 \cap U_2$.

2.3 Décomposition en composantes irréductibles

Définition 2.5 *: Soit $Y \in \mathbb{K}^n$ un fermé de Zariski. On dit qu'il est irréductible si : $Y = Y_1 \cup Y_2$, Y_1 et Y_2 fermés de Zariski de $\mathbb{K}^n$ alors $Y_1 = Y$ ou $Y_2 = Y$.*

Définition 2.6 *On appelle variété affine un fermé de Zariski irréductible de $\mathbb{K}^n$.*

Exemple 2.2 *:*

1. *Soit $f(x, y) = y^2 - x^2$, Alors $V(f) = V(y - x) \cup V(y + x)$ n'est pas irréductible.*
2. *Soit $f(x, y) = x$ alors $V(f) = \{0\} \times \mathbb{K}$ est une variété affine de $\mathbb{K}^2$*

Théorème 2.1 *: Pour un fermé de Zariski soit irréductible, il faut et il suffit que son idéal soit premier.*

Preuve : Soit V un fermé de Zariski irréductible. Considérons des polynômes F et G tels que FG s'annule sur V, on a $V \subset \mathcal{V}(FG) = \mathcal{V}(F) \cup \mathcal{V}(G)$ de sorte que V est réunion des fermés $V \cap \mathcal{V}(F)$ et $V \cap \mathcal{V}(G)$. Comme V est irréductible, l'un d'eux est égal à V, de sorte que soit F, soit G s'annule sur V.

Supposons que l'idéal de V, $\mathcal{I}(V)$ est premier et que V est réunion de deux fermés propres V_1 et V_2. Comme $V_i \subsetneq V$, $i = 1, 2$, il existe un polynôme F_i nul sur V_i mais pas sur V, de sorte que $F_i \notin \mathcal{I}(V)$, et puisque $F_1F_2 \in \mathcal{I}(V)$, ceci contredit le fait que $\mathcal{I}(V)$ est premier.

Proposiftion 2.5 *: Soit $Y \subset \mathbb{K}^n$ un fermé de Zariski, si Y est irréductible et $U \subset Y$ un ouvert de Zariski non vide, alors $\overline{U} = Y$ où $\overline{U}$ désigne l'adhérence de Zariski de U dans Y.*

Preuve : On pose $Y_1 = Y \setminus U$ et $Y_2 = \overline{U}$, alors Y_1 et Y_2 sont des fermés de Zariski, et $Y = Y_1 \cup Y_2$. Si $Y = Y_1$, cela implique que $U = \emptyset$, donc on a $Y_2 = \overline{U} = Y$.

Corollaire 2.2 *:*

Si $\mathbb{K}$ est infini, alors $\mathbb{K}^n$ est irréductible.

Preuve : Puisque $\mathbb{K}$ est infini, tout polynôme nul sur $\mathbb{K}^n$ est nul, de sorte que $\mathcal{I}(\mathbb{K})^n =< 0 >$, et on a $\mathbb{K}[x_1, \ldots, x_n]$ anneau intègre, alors $< 0 >$ est premier donc $\mathbb{K}^n$ est irréductible.

Théorème 2.2 *:*

Toute sous-variété affine non vide se décompose de façon unique (à permutation près) en une réunion finie de sous-variétés affines irréductibles non contenues l'une dans l'autre.

Preuve : Existence : Supposons qu'il existe une sous-variété V non vide qui ne se décompose pas en une réunion finie d'irréductibles, d'après proposition 2.3, l'ensemble de ces sous-variétés admet un élément minimal V qui est forcément réductible. On écrit $V = V_1 \cup V_2$, avec V_i fermé non vide distinct de V . Par minimalité, V_i est réunion finie d'irréductibles, d'où la contradiction.

L'unicité : Supposons d'avoir deux décompositions incompressibles :

$$V = V_1 \cup \cdots \cup V_M = V'_1 \cup \cdots \cup V'_N$$

alors, pour $i \in \{1, \ldots, N\}$, on a :

$$V_i = \bigcup_{j=1}^{N} V_i \cap V'_j$$

et puisque Y_i est irréductible, il existe j_i tel que $V_i = V_i \cap V'_{j_i}$, ce qui entraîne que $V_i \subset V'_{j_i}$. De même, il existe un i' tel que $V'_{j_i} \subset V_{i'}$. Donc, puisque ces décomposition sont incompressibles :

$$V_i \subset V'_{j_i} \subset V_{i'} \Rightarrow i = i' \; et \; V_i = V'_{j_i}$$

De même, pour tout $j \in \{1, \ldots, N\}$, il doit exister i_j tel que $V'_j = V_{i_j}$.

2.4 Théorème des Zéros de Hilbert (Nullstellensatz)

Lorsqu'on définit un ensemble algèbrique $X \subset \mathbb{K}^n$ par des équations polynômiales :

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, & \\ f_2(x_1, \ldots, x_n) = 0, & f_1, \ldots, f_n \in \mathbb{K}[X_1, \ldots, X_n] \\ \qquad \ldots & \\ f_k(x_1, \ldots, x_n) = 0, & \end{cases}$$

Il n'est pas vrai en général que $\mathcal{I}(X) =< f_1, \ldots, f_k >$, par exemple si l'on prend l'équation $f(X_1) = X_1^2$ on a $\mathcal{I}(\mathcal{V}(X_1^2)) =< X_1 > \neq < X_1^2 >$, le théorème des Zéros de Hilbert nous dit comment retrouver $\mathcal{I}(X)$ à partir des équations $f_1, \ldots, f_n$.

Lemme 2.1 *(Lemme de normalisation de Noether) Soit $\mathbb{K}$ un corps, que l'on suppose infini. Soit $A \neq 0$ une $\mathbb{K}$-algèbre de génération finie sur $\mathbb{K}$, il existe $x_1, \ldots, x_n \in A$ tels que $A = \mathbb{K}[x_1, \ldots, x_n]$. Alors il existe des éléments $y_1, \ldots, y_r \in A$ qui sont algèbriquement indépendants sur $\mathbb{K}$ et tels que A soit entière sur $\mathbb{K}[y_1, \ldots, y_r]$. De plus, on peut choisir les $y_1, \ldots, y_r$ comme combinaisons $\mathbb{K}$-linéaires des $x_1, \ldots, x_n$.*

preuve : Quitte à renuméroter les $x_1, \ldots, x_n$, on peut supposer que $x_1, \ldots, x_r$ sont algèbriquement indépendants sur $\mathbb{K}$, et que $x_{r+1}, \ldots, x_n$ sont algèbriques sur $K[x_1, \ldots, x_r]$.

On procède par induction sur n. Si $n = r$, il n'y a rien à démontrer. On peut donc supposer que $n > r$ et que le résultat est vrai pour les $\mathbb{K}$-algèbres avec $n-1$ générateurs. Le générateur x_n est algèbrique sur $\mathbb{K}[x_1, \ldots, x_{n-1}]$, soit donc $f \in \mathbb{K}[x_1, \ldots, x_{n-1}][X_n]$ son polynôme minimal, que l'on peut regarder comme polynôme en $x_1, \ldots, x_n$. Soit $F(x_1, \ldots, x_n)$ la partie homogène de degré maximale de f, comme $\mathbb{K}$ est infini, il existe $\lambda_1, \ldots, \lambda_{n-1} \in \mathbb{K}$ tels que $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Posons $x'_i = x_i - \lambda_i.x_n, i = 1, \ldots, n-1$.

Supposons que F soit de degré d et soit $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$ un monôme apparaissant dans F, en termes des $x'_i, i = 1, \ldots, n-1$, il s'écrit :

$$x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n} = (x'_1 + \lambda_1.x_n)^{\alpha_1} \cdots (x'_1 + \lambda_1.x_n)^{\alpha_1}.x_n^{\alpha_n} = \lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n}.x_n^d + \rho$$

où ρ est un polynôme en $x'_1, \ldots, x'_{n-1}, x_n$ de degré strictement inférieur à d en x_n. On en déduit que,

$$f(x_1, \ldots, x_n) = x_n^d.F(\lambda_1, \ldots, \lambda_{n-1}, 1) + x_n^{d-1}.a_1(x'_1, ..., x'_{n-1}) + ... + a_d(x'_1, ..., x'_{n-1}) = 0$$

et donc x_n est entier sur l'anneau $A' = \mathbb{K}[x'_1, \ldots, x'_{n-1}]$. Il s'ensuit que l'anneau A est entier sur A', par hypothèse d'induction, il existe des combinaisons linéaires $y_1, ..., y_r$ des $x'_1, \ldots, x'_{n-1}$ (qui sont finalement des combinaisons linéaires des $x_1, \ldots, x_n$), telles que les $y_1, \ldots, y_r$ sont algèbriquement indépendants sur $\mathbb{K}$ et que A' soit entier sur $\mathbb{K}[y_1, \ldots, y_r]$, puisque A est entier sur A', il est aussi entier sur $\mathbb{K}[y_1, \ldots, y_r]$.

Lemme 2.2 *Soit L un corps,$A \subset L$ un sous-anneau et supposons que L soit entier sur A. Alors A est un corps.*

Preuve : Soit $a \in A, a \neq 0$. Alors $a^{-1} \in L$ est entier sur A, donc satisfait une équation du type :

$$a^{-n} + a^{-(n-1)}.a1 + \ldots + a_n = 0, a_1, \ldots, a_n \in A$$

d'où on tire, en multipliant par a^{n-1} :

$$a^{-1} = -a_1 - \ldots - a^{n-2}.a_{n-2} - a_n.a^{n-1} \text{ et donc } a^{-1} \in A.$$

Théorème 2.3 *(Forme faible du Nullstellensatz). Soient $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_n]$. Si l'ensemble $\mathcal{V}(f_1, \ldots, f_k)$ des zéros communs aux f_i est vide, alors il existe $a_1, \ldots, a_k \in \mathbb{K}[X_1, \ldots, X_n]$ tels que $a_1 f_1 + \ldots + a_k f_k = 1$.*

Preuve : Supposons que l'idéal $< f_1, \ldots, f_k >$ engendré par $f_1, \ldots, f_k$ ne soit pas $\mathbb{K}[X_1, \ldots, X_n]$ tout entier. Alors il est contenu dans un idéal maximal $\mathcal{M}$ et il suffit de montrer que $\mathcal{V}(\mathcal{M}) \neq \emptyset$, puisque $\mathcal{V}(\mathcal{M}) \subset \mathcal{V}(f_1, \ldots, f_k)$. Puisque $\mathcal{M}$ est maximal, le quotient $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$ est un corps, on notera $x_1, \ldots, x_n$ les images des X_i dans $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$. On applique le lemme de normalisation alors quitte à renuméroter les X_i, le corps $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$ est entier sur $\mathbb{K}[x_1, \ldots, x_r]$ et les $x_1, \ldots, x_r$ sont algèbriquement indépendants sur $\mathbb{K}$, pour un certain $r \leq n$. Alors, d'après le lemme précédent, $\mathbb{K}[x_1, \ldots, x_r]$ est aussi un corps, donc la seule possibilité est que r $= 0$ et que $\mathbb{K}[x_1, \ldots, x_r] = \mathbb{K}$. Donc $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$ est une extension algèbrique finie de $\mathbb{K}$, qui est algèbriquement clos, donc l'inclusion naturelle $\mathbb{K} \subset \mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$ est un isomorphisme. Si on appelle $a_1, \ldots, a_n \in \mathbb{K}$les éléments qui correspondent aux classes des X_i, les images des $X_i - a_i$ par le passage au quotient :

$$\mathbb{K}[X_1, \ldots, X_n] \longrightarrow \mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$$

sont nulles, $i = 1, \ldots, n$, donc on a l'inclusion

$$\mathcal{M}' < X_1 - a_1, \ldots, X_1 - a_1 > \subset \mathcal{M}$$

mais l'idéal $\mathcal{M}'$ est aussi maximal, puisque $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{M}$. Il s'ensuit que $\mathcal{M} = \mathcal{M}'$, et donc $\mathcal{V}(\mathcal{M}) = \{(a_1, \ldots, a_n)\} \neq \emptyset$, donc $< f_1, \ldots, f_k >= \mathbb{K}[X_1, \ldots, X_n]$

Théorème 2.4 *: (Nullstellensatz) Soit $\mathbb{K}$ un corps algèbriquement clos. Pour tout idéal I de $\mathbb{K}[X_1, \ldots, X_n]$, on a $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. En particulier, $\mathcal{V}(I)$ est vide si et seulement si $I =< 1 >$.*

Preuve*(Nullslellensatz)* : Soit $\mathcal{A} \subset \mathbb{K}[X_1, \ldots, X_n]$ un idéal, $f_1, \ldots, f_r \in \mathbb{K}[X_1, \ldots, X_n]$ des générateurs de cet idéal. Supposons que $f \in \mathbb{K}[X_1, \ldots, X_n]$ s'annule sur les zeros communs aux $f_i, i = 1, \ldots, r$. Construisons un nouvel idéal $\mathcal{B}$ dans $\mathbb{K}[X_1, \ldots, X_n, X_{n+1}]$:

$$\mathcal{B} =< f_1, \ldots, f_r, f \cdot x_{n+1} - 1 >$$

On voit que $V(\mathcal{B}) = \emptyset$ donc d'après Nullslellensatz faible on peut trouver $A_i, i = 1, \ldots, r$ et $\mathcal{B}$ dans $\mathbb{K}[X_1, \ldots, X_n, X_{n+1}]$ tels que :

$$(*) \sum_{i=1}^{r} A_i.f_i + 0 = 1$$

On travaille maintenant dans $\mathbb{K}(X_1, \ldots, X_n, X_{n+1})$; on substitue X_{n+1} par $\frac{1}{f}$ dans (*) et on obtient une expression de la forme :

$$\textstyle\sum_{i=1}^{n} \frac{A'_i(X_1, \ldots, X_n)}{f^{n_i}} = 1$$

et en la multipliant par f^N avec N suffisamment grand pour chasser tous les dénominateurs, on obtient une expression de la forme :

$$\textstyle\sum_{i=1}^{n} A_i"(X_1, \ldots, X_n) = f^N avec A_i" \in \mathbb{K}[X_1, \ldots, X_n]$$

Corollaire 2.3 *:*

L'application $V \to \mathcal{I}(V)$ réalise une bijection décroissante de réciproque $I \to \mathcal{V}(I)$ entre :

- *a) Les sous-variétés affines de $\mathbb{K}^n$ et les idéaux radicaux de $\mathbb{K}[X_1, \ldots, X_n]$;*
- *b) Les sous-variétés affines irréductibles de $\mathbb{K}^n$ et les idéaux premiers de $\mathbb{K}[X_1, \ldots, X_n]$.*
- *c) Les points de $\mathbb{K}^n$ et les idéaux maximaux de $\mathbb{K}[X_1, \ldots, X_n]$*

Définition 2.7 *: On appelle hypersurface de $\mathbb{K}^n$ toute sous-variété affine définie par un polynôme non constant.*

2.5 Produits de variétés affines

Soient $X \subset \mathbb{A}^n$ et $Y \subset \mathbb{A}^m$ deux variétés algèbriques affines sur un corps $\mathbb{K}$.

Proposiftion 2.6 *L'espace $X \times Y = \mathbb{A}^{n+m}$, muni de la topologie induite, est irréductible.*

Démonstration : Supposons que Z_1 et Z_2 soient deux fermés tels que $X \times Y = Z_1 \cup Z_2$, On définit

$$X_i = \{x \in X : \{x\} \times Y \subset Z_i\},\ i = 1, 2.$$

et l'on aimerait montrer que $X = X_1 \cup X_2$. Si l'on considère, pour $x \in X$ fixé, l'application

$$i_x : Y \longrightarrow X \times Y \ y \longmapsto (x, y)$$

on constate que l'une des préimages $i_x^{-1}(Z_i)$ doit être vide (puisque Y est irréductible). Soit maintenant $x \in X$. Si x n'appartient pas à $X_1 \cup X_2$, il existe $y_1, y_2 \in Y$ tels que $(x, y_i) \notin Z_i$, ce qui implique que $(x, y_1) \in Z_2$ et $(x, y_2) \in Z_1$, contredisant le fait que l'une des préimages doit être vide. Pour $y \in Y$, on définit une application $i_y : X \longrightarrow X \times Y$ comme ci-dessus et l'on constate que

$$X_i = \bigcap_{y \in Y} i_y^{-1}(Z_i)$$

ce qui implique que X_i est fermé. Puisque X est irréductible, on obtient $X_1 = \emptyset$ ou $X_2 = \emptyset$, ce qui implique que l'un des Z_i est vide, comme désiré.

Corollaire 2.4 *Le produit direct de deux variétés affines algèbriques affines est une variété affine.*

On peut remarquer que la topologie sur $\mathbb{A}^{n+m}$ n'est pas celle du produit de $\mathbb{A}^n$ et $\mathbb{A}^m$.

CHAPITRE 3

VARIÉTÉS PROJECTIVES

Le but de cette section est de transposer les résultats précédents aux espaces projectifs. La première différence se situe au niveau de l'évaluation des polynômes : selon le représentant choisi, le résultat ne sera pas le même. On remarque cependant que dans le cas d'un polynôme homogène, puisque notre anneau des polynôme est intègre, la question de savoir si un polynôme s'annule ou pas ne dépend pas du choix du représentant d'une classe d'équivalence. Afin de réaliser cette généralisation aux espaces projectifs, nous allons utiliser les idéaux homogènes de l'anneau gradué des polynômes.

3.1 Espace projectif

Un espace projectif est défini en mathématique comme l'ensemble des droites vectorielles d'un espace vectoriel.

soit E un $\mathbb{K}$-espace vectoriel, on définit sur $E \setminus \{0\}$ la relation d'équivalence suivant :

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

Définition 3.1 *On appelle espace projectif sur E l'ensemble quotient de $E \setminus \{0\}$ par la relation d'équivalence $\sim$:*

$$\mathbb{P}(E) = E \setminus \{0\}/ \sim$$

Soit $\pi : \mathbb{K}^{n+1} \setminus \{0\} \longrightarrow \mathbb{PK}^n$ *la projection canonique, celle qui à* $x = (x_0, \ldots, x_n) \in \mathbb{K}^{n+1} \setminus \{0\}$ *associe la classe d'équivalence de* $x = (x_0, \ldots, x_n)$.

Définition 3.2 *On la note* $\pi(x_0, \ldots, x_n) = [x_0 : \ldots : x_n]$ *et on appelle* $(x_0, \ldots, x_n)$ *les coordonnés homogènes de* $\pi(x)$.

On défini $\varphi_i : \mathbb{K}^n \longrightarrow \mathbb{PK}^n$, $(x_1, \ldots, x_n) \rightsquigarrow [x_1 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_n]$
qui est une bijection sur $U_i = \{[x_1 : \ldots : x_n] \setminus x_i \neq 0\}$. Notons que la réunion des U_i recouvre $\mathbb{PK}^n$.

Définition 3.3 *On appelle les* φ_i *cartes affines sur* $\mathbb{PK}^n$.

3.2 Ensembles algèbriques projectifs :

On veut une définition analogue à celle des variétés affines. Le problème est que les coordonnées (homogènes) d'un point n'étant pas uniquement définies, on ne peut parler de la valeur d'un polynôme en un point. En fait, seuls les zéros des polynômes nous intéressent. Ceux-ci seront définis pour une certaine catégorie du polynômes.

Définition 3.4 *(polynôme homogène) Un polynôme* $f \in \mathbb{K}[x_0, \cdots, x_n]$ *est dit homogène de degré* d *si pour tout élément* $\lambda \in \mathbb{K}$, *on a :*

$$f(\lambda.x_0, \ldots, \lambda.x_n) = \lambda^d.f(x_0, \ldots, x_n)$$

On reconnaît facilement un polynôme homogène de degré d : tous ses monômes non nuls sont de même degré d. Il est clair que tout polynôme $f \in \mathbb{K}[x_0, \cdots, x_n]$ se décompose de façon unique en somme du polynômes homogènes.

$$f(x_0, \ldots, x_n) = \sum_{h=0}^{d} f_h(x_0, \ldots, x_n)$$

où f_h est un polynôme homogène de degré h qui s'appelle la composante homogènes de degré $h$de f.

Définition 3.5 *(Idéal homogène) L'idéal $\mathcal{A} \subset \mathbb{K}[x_0, \ldots, x_n$ est dit homogène si :*

$$f \in \mathcal{A} \Longrightarrow f_h \in \mathcal{A} \; \forall h = 0, \cdots, d$$

Définition 3.6 *Soit $S \in \mathbb{K}[x_0, \cdots, x_n]$ un ensemble des polynôme homogènes. On définit $\mathcal{V}(S) = \{x \in \mathbb{P}^n ; f(x) = 0, \; \forall f \in S\}$.*

Si I est un idéal homogène, on pose $\mathcal{V}(I) = \mathcal{V}(hom(I))$ où $hom(I)$ est l'ensemble des éléments homogènes de I la réciproque est claire.

Définition 3.7 *:(Ensemble algèbrique projective) Un sous-ensemble $A \subset \mathbb{P}^n$ est dit algèbrique projectif (ou simplement algèbrique) s'il existe un ensemble d'éléments homogènes S tel que $A = \mathcal{V}(S)$.*

Proposiftion 3.1 *: (Propriétés de base de $\mathcal{V}$) Soient I, I', J des idéaux homogènes de $\mathbb{K}[x_0, \cdots, x_n]$ tels que $I \subset I'$ ainsi que $S, S' \subset \mathbb{K}[x_0, \cdots, x_n]$ deux ensembles du polynômes homogènes. On a les propriétés suivantes :*

(i) $\mathcal{V}(I) \supset \mathcal{V}(I')$

(ii) $\mathcal{V}(I.J) = \mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$

(iii) $\mathcal{V}(S \cup S') = \mathcal{V}(S) \cap \mathcal{V}(S')$

(iv) $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$

Peuve : En utilisant les propriétés de base de l'anneau gradué $\mathbb{K}[x_0, \cdots, x_n]$, on montre ces résultats de manière analogue au cas affine.

Exemple 3.1 *Quelques exemples d'ensembles algèbriques :*

(i) $\mathcal{V}(1) = \emptyset$

(ii) $\mathcal{V}(0) = \mathbb{P}^n$

(iii) *si* $a = (a_0, \ldots, a_n) \in \mathbb{P}^n$ *alors* $\{a\}$ *est algèbrique. En effet, le fait que* $a \in \mathbb{P}^n$ *entraîne qu'au moins une des composante n'est pas* 0*, disons* a_i*. On écrit alors :*

$$\{a\} = \mathcal{V}(x_0 - \tfrac{a_0}{a_i}x_i, \cdots, x_n - \tfrac{a_n}{a_i}x_i)$$

Proposiftion 3.2 *:*

(a) *Toute intersection des ensembles algèbriques projectifs de* $\mathbb{P}^n$ *est un ensemble algèbrique projectif*

(b) *Toute réunion finie des ensembles algèbriques projectives de* $\mathbb{P}^n$ *est un ensemble algèbrique projectif*

La proposition permet de définir la topologie de Zariski sur $\mathbb{P}^n$, en prenant comme fermés les ensembles algèbriques projectifs.

3.3 Idéal d'une variété projective

Définition 3.8 *Soit* V *un sous-ensemble de* $\mathbb{P}^n$ *; on appel idéal de* V *et l'on note* $\mathcal{I}(V)$*,l'idéal (homogène) engendré par les polynômes homogènes nuls sur* V*.*

Proposiftion 3.3 *(propriétés de base de* $\mathcal{I}$*)*

Soient $S \subset S' \subset \mathbb{P}^n$ *et* V *un ensemble algèbrique ainsi que* I *un idéal homogène de* $\mathbb{K}[x_0, \cdots, x_n]$.

(i) $\mathcal{I}(S) \supset \mathcal{S}'$

(ii) $\mathcal{V}\mathcal{I}(V) = V$

(iii) $I \subset \mathcal{I}\mathcal{V}(I)$

(iv) $\overline{S} = \mathcal{V}\mathcal{I}(S)$

Démonstration : analogue au cas affine.

Remarque :

On utilise la plupart du temps les notations pour $\mathcal{V}$ et $\mathcal{I}$ dans le cas affine et projectif. Cependant, si cela s'avère nécessaire, on écrira $\mathcal{V}_{aff}$ et $\mathcal{V}_p$ ainsi que $\mathcal{I}_{aff}$ et $\mathcal{I}_p$.

Une différence fondamentale entre le cas affine et le cas projectif est que même si l'on suppose $\mathbb{K}$ algèbriquement clos, $\mathcal{V}(I)$ peut être vide pour un idéal propre I.

Exemple 3.2 *: Si l'on note R_+ l'idéal $< x_0, \ldots, x_n >$ de $\mathbb{K}[x_0, \cdots, x_n]$, On trouve que $\mathcal{V}(R_+) = \emptyset$, puisque $0 \notin \mathbb{P}^n$. dans le cas affine, Nullstellensatz faible assure que cela ne peut pas se produire.*

Définition 3.9 *(cône d'un ensemble algèbrique projectif)*

Soit V un ensemble algèbrique projectif. Alors on définit le cône $\mathcal{C}(V)$ de V comme étant :

$$\mathcal{C}(V) = p^{-1}(V) \cup \{0\} \subset \mathbb{K}^{n+1}.$$

où $p : \mathbb{K}^{n+1} \longrightarrow \mathbb{P}^n$ est la projection canonique.

Remarque :

Soit $V = \mathcal{V}_p(I)$ un ensemble algèbrique projectif non vide. Alors on remarque que $\mathcal{C}(\mathcal{V}_p(I))$ coïncide avec $\mathcal{V}_{app}(I)$(à l'élément 0 près).

Théorème 3.1 *(Le théorème des zéros de Hilbert(cas projectif)) Soient $\mathbb{K}$ un corps algèbriquement clos et I un idéal homogène de $\mathbb{K}[x_0, \cdots, x_n]$. Alors :*

(i) *$\mathcal{V}_p(I)$ est vide si et seulement si I contient une puissance de R_+*

(ii) *si $\mathcal{V}_p(I)$ n'est pas vide $\mathcal{I}_p\mathcal{V}_p(I) = \sqrt{I}$*

Preuve :

(i) supposons que $\mathcal{V}_p(I)$ soit vide, c'est-à-dire $\mathcal{V}_{aff}(I) \subset \{0\}$ et donc

$$\sqrt{I} = \mathcal{I}_{aff}\mathcal{V}_{aff}(I) \supset \mathcal{I}_{aff}(\{0\}) = R_+$$

Ainsi, pour tout $i = 0, \ldots, n$, il existe $\lambda_i \in \mathbb{N}$ tel que $x_i^{\lambda_I} \in I$. On trouve alors que $(R_+)^{\lambda_0 + \cdots + \lambda_n} \subset I$. La réciproque est claire.

(ii) Supposons donc que $\mathcal{V}_p(I)$ ne soit pas vide. On remarque pour commencer que si f est un polynôme homogène, alors f est nul sur $\mathcal{V}_p(I)$ si et seulement s'il est nul sur $\mathcal{C}(\mathcal{V}_p(I)) \setminus \{0\}$ ce qui implique :

$$\mathcal{I}_p\mathcal{V}_p(I) \subset \mathcal{I}_{aff}(\mathcal{C}(\mathcal{V}_p(I))) = \mathcal{I}_{aff}\mathcal{V}_{aff}(I) = \sqrt{I}$$

où l'on a utilisé la remarque et le théorème des zéros de Hilbert du cas affine. L'autre inclusion est analogue au cas affine.

Corollaire 3.1 *L'application $V \longmapsto \mathcal{I}_p(V)$ réalise une bijection décroissante, de réciproque $I \longmapsto \mathcal{V}_p(I)$, entre les ensembles algèbriques projectifs de $\mathbb{P}^n$ et les idéaux radicaux homogènes de $\mathbb{K}[x_0, \cdots, x_n]$ distincts de R_+.*

Preuve : Cela découle de Nullstellensatz projectif, il suffit de remarquer que si un idéal radical contient une puissance de R_+, il contient R_+

CHAPITRE 4

THÉORÈME DE BÉZOUT

Dans ce chapitre on travaille sur le corps $\mathbb{C}$.

Définition 4.1 *Soient $\Gamma_F = \mathcal{V}_p(F)$ et $\Gamma_G = \mathcal{V}_p(G)$ deux courbes projectives planes, où $F, G \in \mathbb{C}[t, x, y]$ sont des polynômes homogènes de degré respectivement m et n. On dira que Γ_F et Γ_G sont transverses au point $P = [t_0 : x_0 : y_0] \in \mathbb{P}^2$ si : $P \in \Gamma_{_F} \cap \Gamma_{_G} \Longrightarrow dF_{(t_0,x_0,y_0)}$ et $dG_{(t_0,x_0,y_0)}$ sont linéairement indépendantes.*

Notons que puisque $dF_{\lambda(t_0,x_0,y_0)} = \lambda^{m-1} dF_{(t_0,x_0,y_0)}$, la condition ci-dessus ne dépend pas du représentant choisi (t_0, x_0, y_0) de P.

Définition 4.2 *On dit que Γ_F et Γ_G sont transverses s'elles sont transverses en tout point de $\Gamma_{_F} \cap \Gamma_{_G}$*

Définition 4.3 *l'espace tangent de Zariski à X en un point p comme l'espace vectoriel défini par les équations :*

$$\sum_{i=1}^{n} \frac{\partial F}{\partial x_i}(p) x_i$$

pour tout F dans $I(X)$. Il est noté $T_p(X)$.

Définition 4.4 *Soit X un espace topologique, la dimension de X est le maximum des entiers n pour lesquels il existe des parties irréductibles fermées $X_0, \ldots, X_n$ de X vérifiant $X_0 \subsetneq \cdots \subsetneq X_n$.*

Théorème 4.1 *Soient* $\Gamma_F = \mathcal{V}_p(F)$ *et* $\Gamma_G = \mathcal{V}_p(G)$ *deux courbes projectives planes transverses, où* $F, G \in \mathbb{C}[t, x, y]$ *sont des polynômes homogènes de degré respectivement* m *et* n. *Alors* $\Gamma_{_F} \cap \Gamma_{_G}$ *consiste en exactement* $m.n$ *points.*

Preuve : Nous allons utiliser les notations et les résultats du §2 de l'appendice. Posons $\mathbb{P}_m = \mathbb{P}(\mathbb{C}[t, x, y]_m)$,qui est l'espace des courbes de degré m. Considérons l'ensemble algèbrique :

$$W = \{([F], [G], [t, x, y]) \in \mathbb{P}_m \times \mathbb{P}_n \times \mathbb{P}^2 \setminus F(t, x, y) = G(t, x, y) = 0\}$$

et soit $\pi : W \to \mathbb{P}_m \times \mathbb{P}_n$ la restriction à W de la projection naturelle :$\pi([F], [G], [t, x, y]) = ([F], [G])$. Considérons le cône de W

$$CW = \{(F, G, v) \in \mathbb{C}[t, x, y]_m \times \mathbb{C}[t, x, y]_n \times \mathbb{C}^3 \setminus F(v) = 0, G(v) = 0\} \text{ (où } v = (t, x, y) =)$$

Définissons $\phi : (\mathbb{C}[t, x, y]_m \setminus \{0\}) \times (\mathbb{C}[t, x, y]_n \setminus \{0\}) \times (\mathbb{C}^3 \setminus \{0\}) \longrightarrow \mathbb{C}^2$ par :

$$\phi(F, G, v) = (F(v), G(v))$$

Alors sa dérivée s'écrit :

$$d\phi_{(F,G,v)}(\overline{F}, \overline{G}, \overline{v}) = (\overline{F}(v) + dF_v(\overline{v}), \overline{G}(v) + dG_v(\overline{v}))$$

et si $(\lambda, \mu) \in \mathbb{C}^2$, puisque $v \neq 0$ on peut trouver $\overline{F}$ et $\overline{G}$ tels que $\overline{F}(v) \neq 0, \overline{G}(v) \neq 0$ (par exemple, si $v = [v_0, v_1, v_2]$ avec $v_0 \neq 0$, on prend $\overline{F} = t^m, \overline{G} = t^n$), et alors

$$d\phi_{(F,G,v)}(\tfrac{\lambda}{\overline{F}(v)}.\overline{F}, \tfrac{\mu}{\overline{G}(v)}.\overline{G}, 0) = (\lambda, \mu)$$

ce qui montre que $d\phi_{(F,G,v)}$ est surjective. il en suit que W est lisse, de dimension égale à :

$$dim(\mathbb{P}_m \times \mathbb{P}_n \times \mathbb{P}^2) - 2 = dim(\mathbb{P}_m \times \mathbb{P}_n)$$

et que son espace tangent au point $z = ([F], [G], P)$ est donné par :

$$TW_z = \{[\overline{F}, \overline{G}, \overline{v}] \setminus \overline{F}(v) + dF_v(\overline{v}) = 0, \overline{G}(v) + dG(\overline{v}) = 0\}.$$

comme le noyau de la dérivée de π au point z est l'intersection de TW_z avec le noyau de la dérivée de la projection $\mathbb{P}_m \times \mathbb{P}_n \times \mathbb{P}^2 \to \mathbb{P}_m \times \mathbb{P}_n$, qui consiste en les $[0, 0, \overline{v}] \in T(\mathbb{P}_m)_{[F]} \times (\mathbb{P}_n)_{[F]}) \times \mathbb{P}^2_P$, on a :

$$Ker(d\pi_z) = \{[0, 0, \overline{v}] \setminus dF_P(\overline{v}) = 0, dG_p(\overline{v}) = 0\}.$$

Or dF_P et dG_P sont linéairement indépendantes si et seulement si $Ker(dF_P) \cap Ker(dG_P)$ et de dimension 1. Comme $dF_P(P) = m.F(P) = 0$ et $dG_P(P) = n.G(P) = 0$, on va dire que la dérivée de π au point $z = ([F], [G], P)$ n'est pas bijective revient à dire que $\mathcal{V}_p(F)$ et $\mathcal{V}_p(G)$ ne sont pas transverses au point P. Soit

$$\Sigma = \{z \in \mathbb{P}_m \times \mathbb{P}_n \times \mathbb{P}^2 \setminus d\pi_z \text{ n'est pas bijective}\}.$$

Alors $\pi(\Sigma)$, qui est une variété projective, est l'ensemble de paires de courbes non transverses. Si on prend

$$F_0 = (x - t).(x - 2t) \cdots (x - m.t), G_0 = (y - t).(y - 2t) \cdots (y - n.t)$$

On vérifie immédiatement que ces deux courbes se coupent transversalement, en les $m.n$ points $[i : j : 1], i = 1, \cdots, m, j = 1, \cdots, n$. En particulier $\pi(\Sigma) \subsetneq \mathbb{P}_m \times \mathbb{P}_n$, ce qui entraîne que $V = \mathbb{P}_m \times \mathbb{P}_n \setminus \pi(\Sigma)$ est connexe (la trace de $\pi(\Sigma)$ sur au moins un produit de cartes affaîne $U' \times U'', U'$ carte affine sur $\mathbb{P}_m$, U'' carte affine sur $\mathbb{P}_n$, doit être non vide, doit $U' \times U'' \setminus \pi(\Sigma)$ est connexe,et donc aussi $\mathbb{P}_m \times \mathbb{P}_n \setminus \pi(\Sigma)$, car il est contenu dans l'adhérence, dans la topologie transcendante, de $U' \times U'' \setminus \pi(\Sigma)$.) posons $M = \pi^{-1}(V) = W \setminus \pi^{-1}(\pi(\Sigma))$; parce que π est propre (dans la topologie transcendante), $\pi \setminus M : M \longrightarrow V$ l'est aussi. Il suit alors de la proposition $I.1.2$ page 51[Ron] (principe de la conservation du nombre) et du fait que la fibre de $\pi \setminus M$ au dessus de (F_0, G_0) consiste en $m.n$ point,que toutes les fibres de $\pi \setminus M : M \longrightarrow V$ consistent en $m.n$ point, ce qui démontre le théorème.

BIBLIOGRAPHIE

[Ron] RONGA Felice, Notes de géométrie algébrique, Genève, MMVI ap. J.-C.