

COURS DE MATHÉMATIQUES

TOME XI
GÉOMÉTRIE

Mathématiques générales

France ~ 2025

Écrit et réalisé par Louis Lascaud

Table des matières

1	Géométrie projective	7
1.1	Généralités de géométrie projective	7
1.1.1	Espaces projectifs	7
1.1.2	Changement de coordonnées projectif	11
1.1.3	Paramétrage des sous-espaces linéaires	12
1.2	Courbes affines, courbes projectives	12
1.2.1	Qu'est-ce qu'une courbe ?	12
1.2.1.1	Interprétation du degré d'une courbe plane projectif	15
1.2.2	Application : le théorème des 5 points	15
1.2.3	Notion de tangente (à une courbe, en un point)	17
1.2.3.1	Définitions de base sur la singularité et de la lissité	17
1.2.3.2	Quelques propriétés de base des singularités	18
1.2.4	Description des coniques projectives	19
1.2.5	Cubiques et courbes elliptiques	21
1.3	Quelques études de variétés projectives particulières	25
1.3.1	Quadriques	25
1.3.1.1	Topo sur les quadriques	25
1.3.1.2	Droites sur une quadrique	26
1.3.2	Surfaces cubiques	28
1.3.2.1	Théorème des 27 droites	28
2	Géométrie algébrique	33
2.1	Variétés algébriques et variétés affines	33
2.1.1	Polynômes, fonctions polynomiales	34
2.1.2	Sous-ensembles algébriques	35
2.1.3	La correspondance entre idéaux et variétés : le théorème du Nullstellensatz de Hilbert	39
2.1.4	Fonctions régulières	45
2.1.5	Topologie de Zariski	46
2.1.6	Applications polynomiales entre variétés	50
2.1.7	Fonctions sur une variété	50

2.1.7.1	L'algèbre de coordonnées d'une variété affine	51
2.1.7.2	Corps de fonctions d'une variété	53
2.1.7.3	Applications rationnelles, applications birationnelles	55
2.1.7.4	Image d'une variété affine	57
2.1.7.5	Définitions	57
2.1.7.6	Considérations fonctorielles	58
2.1.7.7	Applications sur le produit de variétés	60
2.1.7.8	Caractérisations classiques	61
2.1.7.9	Morphismes finis	62
2.1.8	Faisceaux de fonctions régulières	62
2.1.9	Variétés algébriques affines	66
2.1.10	Sous-variétés, immersions	67
2.1.11	Variétés algébriques abstraites	67
2.1.12	Construction des variétés par patching	68
2.1.13	Fonctions rationnelles	70
2.1.13.1	Applications birationnelles	72
2.1.13.2	Théorème de constructibilité de Chevalley	72
2.1.14	Le cas $k \neq \bar{k}$: comment se ramener à un corps algébriquement clos avec un peu de théorie de Galois	74
2.1.14.1	Variétés sur un corps parfait	74
2.2	Géométrie des variétés algébriques	77
2.2.1	Dimension des variétés algébriques	77
2.2.1.1	Rappels sur les degrés de transcendance	77
2.2.1.2	Théorie de la dimension algébrique	78
2.2.1.3	Application : existence de droites dans une surface cubique	83
2.2.2	Espace tangent, points singuliers en géométrie algébrique	84
2.2.3	Compléments en vrac	87
2.2.3.1	14 octobre 2024	88
2.3	Variétés projectives	90
2.3.1	Propriétés générales des variétés projectives	91
2.3.2	Plongement de Segre	92
2.3.3	Théorème de l'élimination	93
2.3.4	Grassmannienne	93
2.3.4.1	Grassmannienne de droites	95
2.3.4.2	Existence de droites contenues dans une hypersurface	95
2.3.4.3	Une autre application : coordonnées de Chow	95
2.3.4.4	Le grand théorème de Bézout	95

Chapitre 1

Géométrie projective

Résumé

La géométrie projective est une façon de voir la géométrie formalisant de manière technique les notions de perspective et d'horizon. En effet, un espace projectif n'est autre qu'un espace vectoriel dont on identifie les vecteurs ayant même direction. Cette construction admet, selon une propriété fondamentale, une structure qui permet de la ramener à peu de choses à un espace affine, de sorte que l'étude des courbes projectives n'est autre que l'étude des courbes affines définies par un polynôme homogène à une variable de plus que dans le cas affine, et le reste s'ensuit.

1.1 Généralités de géométrie projective

1.1.1 Espaces projectifs

Voilà une autre remarque heuristique. Les sous-espaces affines correspondent en géométrie aux équations de degré 1 (linéaires). Soient V_1, V_2 des sous-espaces affines d'un espace affine de dimension n . Alors $V_1 \cap V_2$ est encore un sous-espace affine de dimension $V_1 \cap V_2 \geq \dim V_1 + \dim V_2 - n$ (avec égalité dans les cas des espaces vectoriels) ou l'ensemble vide (ce qui n'arrive pas pour les ev). Ceci motive l'introduction de l'espace projectif qui corrige ce défaut.

Donnons un exemple : les droites affines dans \mathbb{A}^2 . On peut les définir par une équation de la forme

$$ax + by + c = 0$$

avec $(a,b) \neq (0,0)$ et $(a,b,c) \sim (\lambda a, \lambda b, \lambda c)$ dans l'équation ci-dessus pour $\lambda \neq 0$.

Définition. (*Espace projectif*)

Si V est un espace vectoriel de dimension $n+1$ sur un corps K , l'espace projectif $\mathbb{P}(V)$ est l'ensemble des droites vectorielles de V , *i.e.* des s.e.v de dimension 1 = $\{v \in V \setminus \{0\}\} / \sim$

où $v \sim v'$ si $v' = \lambda v$, $\lambda \in K^\times$.

Si $V = K^{n+1}$, on note $\mathbb{P}^n = \mathbb{P}(V)$, et ainsi $\mathbb{P}^n = (\mathbb{A}^{n+1} \setminus \{0\}) / \sim$.

On appelle n la *dimension de l'espace projectif* $\mathbb{P}(V)$. En particulier, $\mathbb{P}(V) = \dim(V) - 1$.

Pour $n = 1$, on parle de \mathbb{P}^1 la **droite projective**.

Pour $n = 2$, on parle de \mathbb{P}^2 le **plan projectif**.

Propriété. (Plongement d'espace projectif)

Soit L/K une extension de corps. Alors pour tout $n \in \mathbb{N}$, $\mathbb{P}^n(K) \hookrightarrow \mathbb{P}^n(L)$. On verra de plus que cette injection est polynomiale.

Remarque importante. On note $P = [x_0, \dots, x_n] = [\lambda x_0, \dots, \lambda x_n] \in \mathbb{P}^n$. Si $F \in K[x_0, \dots, x_n]$, $F(P)$ n'a aucun sens. Si F est homogène de degré d , par définition $F(\lambda x_0, \dots, \lambda x_n) = \lambda^d F(x_0, \dots, x_n)$, et alors $F(P) = 0$ ou $F(P) \neq 0$ a un sens. Par contre, la valeur en un point, si elle n'est pas nulle, n'a pas de sens.

Définition. (Sous-ensemble algébrique de l'espace projectif)

Les sous-ensembles algébriques de \mathbb{P}^n sont les $\{[x_0, \dots, x_n] \in \mathbb{P}^n \mid \forall i \in I \quad F_i(x_0, \dots, x_n) = 0\}$ avec les F_i homogènes.

Définition-propriété. (Idéal homogène)

Si I est l'idéal engendré par les F_i dans $K[X_0, \dots, X_n]$, on dit que c'est un *idéal homogène*. Il est équivalent de dire que I est un idéal de $K[X_0, \dots, X_n]$ et si $I \ni F = F_0 + \dots + F_d$ sa décomposition homogène, alors tous les $F_j \in I$.

Le sous-ensemble algébrique précédent est alors $\{[x_0, \dots, x_n] \in \mathbb{P}^n \mid \forall F \text{ homogène} \in I \quad F(x_0, \dots, x_n) = 0\}$.

▷ Supposons que l'idéal I aient un ensemble $\{f_\lambda\}_{\lambda \in \Lambda}$ de générateurs homogènes. Soit $g \in I$ et soit $g = \sum_i g_i$ sa décomposition homogène. Alors $g = \sum_{j=1}^m h_j f_{\lambda_j}$ pour un $m \in \mathbb{N}$ et $h_j \in K[X_0, \dots, X_n]$. Maintenant, décomposons $\sum h_j f_{\lambda_j}$ en composantes homogènes. Puisque f_{λ_j} est homogène, on peut voir que toute composante homogène de $\sum h_j f_{\lambda_j}$ sera de la forme $\sum_{k \in K} h'_k f_{\lambda_k}$ pour $K \subseteq \{1, \dots, m\}$. Puisque cette décomposition est unique, cela signifie que chaque g_i doit coïncider avec une expression du type $\sum_{k \in K} h'_k f_{\lambda_k}$, qui implique les $g_i \in I$.

Réciproquement, supposons que $f = \sum_i f_i$ implique $f_i \in I$ pour tout i . Soit $\{g_1, \dots, g_m\}$ un système de générateurs de I , fini par noéthérianité. Alors l'ensemble des $h \in K[X_0, \dots, X_n]$ tels que h soit une composante homogène de l'un des g_i est évidemment un système de générateurs de I . D'où le résultat. Remarquons que la finitude est inutile, mais elle permet la remarque suivante. ■



On remarque que ce dernier ensemble est fini ! On a donc montré que **si I est un idéal homogène, il a un système fini de générateurs homogènes.**

Définition-propriété. (*Sous-espace linéaire*)

Un *sous-espace linéaire (s.e.l)* de \mathbb{P}^n , ou *sous-espace vectoriel projectif*, est défini par des équations linéaires (homogènes).

C'est exactement le projeté $\mathbb{P}(W)$ d'un sous-espace vectoriel de \mathbb{A}^{n+1} .

On définit : $\dim(\mathbb{P}(W)) = \dim(W) - 1$.

▷ Prenons $V = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid L_1(x) = \dots = L_r(x) = 0\}$ avec les L_i des formes linéaires homogènes (pour qu'elles soient bien définies sur l'espace projectif). Si W est le sous-espace vectoriel $\{(x_0, \dots, x_n) \in \mathbb{A}^{n+1} \mid L_1 = \dots = L_r = 0\}$, alors $V = \mathbb{P}(W) = W \setminus \{0\} / \sim$, où $w_1 \sim w_2$ signifie $\exists \lambda \in K^\times \quad w_2 = \lambda w_1$. Réciproquement, on sait que tout espace vectoriel est défini par un système d'équations linéaires (que l'on peut même prendre linéairement indépendantes en se restreignant à $\text{rg}(S)$ équations) et donc définit un sous-espace linéaire projectif. ■

Propriété

L'intersection de deux sous-espaces linéaires est linéaire.

Théorème 1. (*Propriété d'incidence sur les droites*)

Soit D_1 et D_2 deux droites (projectives) dans \mathbb{P}^2 avec $D_1 \neq D_2$. Alors $D_1 \cap D_2$ est un point.

▷ $D_1 = \{[x, y, z] \in \mathbb{P}^2 \mid ax + by + cz = 0\}$, $D_2 = \{[x, y, z] \in \mathbb{P}^2 \mid a'x + b'y + c'z = 0\}$. Alors $D_1 \cap D_2 = \{[x, y, z] \in \mathbb{P}^2 \mid L_1 = L_2 = 0\}$. Puisque $D_1 \neq D_2$, (a, b, c) n'est pas équivalent à (a', b', c') : le rang du système linéaire est 2. Donc $W = \{(x, y, z) \in \mathbb{A}^3, L_1 = L_2 = 0\}$ est un sous-espace vectoriel de dimension 1. Ainsi $D_1 \cap D_2 = \mathbb{P}(W)$ est un point. ■

Plus généralement :

Théorème 2. (*Formule de Grassmann projective*)

Soient V_1, V_2 deux sous-espaces linéaires de \mathbb{P}^n . Si $\dim(V_1) + \dim(V_2) \geq n$, alors $V_1 \cap V_2 \neq \emptyset$ et $\dim(V_1 \cap V_2) \geq \dim(V_1) + \dim(V_2) - n$.

▷ \tilde{V}_1 est un s.e.v de \mathbb{A}^{n+1} avec $V_1 = \mathbb{P}(\tilde{V}_1)$, de même pour \tilde{V}_2 . Alors $V_1 \cap V_2 = \mathbb{P}(\tilde{V}_1 \cap \tilde{V}_2)$ et $\dim(\tilde{V}_j) = \dim(V_j) + 1$ donc $\dim \tilde{V}_1 \cap \tilde{V}_2 \geq (\dim V_1 + 1) + (\dim V_2 + 1) - (n + 1) = (\dim V_1 + \dim V_2 - n) + 1 \geq 1$ donc $\mathbb{P}(\tilde{V}_1 \cap \tilde{V}_2) \neq \emptyset$. Or $\dim(V_1 \cap V_2) = \dim \mathbb{P}(\tilde{V}_1 \cap \tilde{V}_2) = \dim(\tilde{V}_1 \cap \tilde{V}_2) - 1 \geq \dim V_1 + \dim V_2 - n$. D'où le résultat. ■

Ainsi, deux droites parallèles du plan affine se rencontrent dans un point du plan projectif qui n'est pas dans le plan affine. Nous étudions ainsi le lien entre \mathbb{A}^n et \mathbb{P}^n , qui ne sont pas du tout le même espace, mais l'on peut voir que l'un est inclus dans l'autre.

Propriété. (Lien entre \mathbb{A}^n et \mathbb{P}^n)

Dans \mathbb{P}^n , on peut définir l'*hyperplan projectif* $H_i = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid x_i = 0\}$ isomorphe à \mathbb{P}^{n-1} en un sens clair (que l'on précisera plus tard : en bijection par des polynômes). On pose $U_i = \mathbb{P}^n \setminus H_i$. Alors :

1. $\bigcup_{i=0}^n U_i = \mathbb{P}^n$ (en géométrie projective, le point 0 n'existe pas),
2. $U_i \simeq \mathbb{A}^n$.

En particulier, l'espace projectif contient plusieurs copies de l'espace affine. Par exemple, $\mathbb{P}^n = U_0 \cup H_0 \simeq \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$. On pourrait ainsi définir par récurrence l'espace projectif.

Plus précisément :

1. pour $n = 1$, $\mathbb{P}^1 = \mathbb{A}^1 \sqcup \{\star\}$ un point à l'infini ;
2. $\mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$ une droite à l'infini.

Remarque. Cette détermination du point à l'infini, d'une droite à l'infini, est un peu abusive ; en effet, par un changement de coordonnées projectives, comme on le verra, n'importe quel point, respectivement n'importe quelle droite, peut être prise à la place.

▷ Pour $i = 0$, $P = [x_0, \dots, x_n] \in U_0$ donc $x_0 \neq 0 = [1, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}]$. Remarquons que $\frac{x_i}{x_0}$ ne dépend pas des coordonnées projectives choisies, car $\frac{\lambda x_i}{\lambda x_0} = \frac{x_i}{x_0}$. On a obtenu une application ϕ de $U_0 \rightarrow \mathbb{A}^n$, définie par $[x_0, \dots, x_n] \mapsto (\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$, de réciproque $\psi : (y_1, \dots, y_n) \mapsto [1, y_1, \dots, y_n]$. Elle est bien définie par des polynômes. ■

Observation

On a $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \dots \sqcup \mathbb{A}^2 \sqcup \mathbb{A}^1 \sqcup \{\star\}$.

Exemples

1. Il y a deux types de droites projectives dans $\mathbb{P}^2 = \mathbb{A}^2 \cup D_\infty$: D_∞ , qui correspond à l'ensemble vide dans le plan affine, et les autres, qui correspondent à des droites affines (une à une).
2. (Deux droites affines qui ne se rencontrent pas.) Prenons D_1 définie par $ax + by + c = 0$ et $D_2 = ax + by + c' = 0$ où $c \neq c'$.

On pose ϕ de U_0 dans \mathbb{A}^2 définie par $[x_0, x_1, x_2] \mapsto (\frac{x_1}{x_0}, \frac{x_2}{x_0})$ de réciproque $(x, y) \mapsto [1, x, y]$. Alors $ax + by + c = 0$ ssi $ax_1/x_0 + bx_2/x_0 + c = 0$ où $x_0 \neq 0$, soit $ax_1 + bx_2 + cx_0 = 0$. Posons $\overline{D_1} = \{[x_0, x_1, x_2] \in \mathbb{P}^2 \mid ax_1 + bx_2 + cx_0 = 0\}$ droite projective. Alors $U_0 \cap \overline{D_1} = \{[1, x, y] \in \mathbb{P}^2 \mid ax + by + c = 0\} = \psi(D)$. De plus $\overline{D_1} = (U_0 \cap \overline{D_1}) \cup \{[-b, a, 0]\}$. D'autre part, $\overline{D_2} = (U_0 \cap \overline{D_2}) \cup \{[-b, a, 0]\}$ où ce premier terme égale $\psi(D_2)$, et voilà la méthode.

On remarque que D_1 et D_2 se rencontrent dans l'espace projectif.

3. Avec des polynômes généraux, c'est la même chose : on homogénéise puis on déshomogénéise. Pour changer, partons du point opposé au point de vue précédent. Soit $\bar{V} = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid F(x_0, \dots, x_n) = 0\}$. Prenons F homogène de degré d . On note $H_0 = \{x_0 = 0\}$ hyperplan à l'infini et $U_0 = \{x_0 \neq 0\} = \mathbb{P}^n \setminus H_0$. Alors $\bar{V} \cap U_0 = \{[1, y_1, \dots, y_n] \in \mathbb{P}^n \mid F(1, y_1, \dots, y_n) = 0\}$ dans U_0 hypersurface de \mathbb{A}^n définie par $F(1, y_1, \dots, y_n) = 0$ polynôme de degré $\leq d$. On la note V . Alors $\bar{V} = (\bar{V} \cap U_0) \sqcup (\bar{V} \cap H_0)$. Or $\bar{V} \cap H_0 = \{[0, x_1, \dots, x_n] \in \mathbb{P}^n \mid F(0, x_1, \dots, x_n) = 0\}$ polynôme homogène de degré d . Remarque : si $F = x_0 F_1$, alors $F(0, x_1, \dots, x_n) \equiv 0$. Supposons que X_0 ne divise pas F . Alors $F(0, x_1, \dots, x_n) \not\equiv 0$. $\bar{V} \cap H_0$ est une hypersurface de $H_0 = \mathbb{P}^{n-1}$ de degré d . Alors $\bar{V} = \psi(V) \sqcup (\bar{V} \cap H_0)$ réunion d'une hypersurface affine dans \mathbb{A}^n et d'une hypersurface projective de \mathbb{P}^{n-1} . Si maintenant $F = X_0 F_1$, Alors $\bar{V} = (\bar{V} \cap U_0) \sqcup H_0$. Pour $F(x_0, \dots, x_n)$ donné (homogène), l'hypersurface affine associée est définie par $f(y_1, \dots, y_n) = F(1, y_1, \dots, y_n)$. Si $f(y_1, \dots, y_n) = 0$ définit $V \subseteq \mathbb{A}^n$, on veut $\bar{V} \subseteq \mathbb{P}^n$ telle que $\bar{V} \cap U_0 = \psi(V)$. On prend $F(x_0, \dots, x_n) = x_0^d f(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$ avec $d = \deg_{\text{total}}(f)$. Rappelons l'essence de ce procédé : d'une part $F(\lambda x_0, \dots, \lambda x_n) = \lambda^d F(x_0, \dots, x_n)$ et $F \in K[X_0, \dots, X_n]$ et x_0 ne divisant pas F , il existe un monôme $X_1^{i_0} \dots X_n^{i_n}$ de degré d avec son coefficient non nul ; d'autre part, $F(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$. Ces deux constructions ne sont pas rigoureusement identiques, mais presque, en ce sens qu'elles sont bijectives. On a bien finalement $\bar{V} \cap U_0 = Q(V)$.

1.1.2 Changement de coordonnées projectif

Définition. (*Changement de coordonnées projectives*)

Soit $n \in \mathbb{N}$ et soit $A = ((a_{i,j}))$ une matrice $(n+1) \times (n+1)$ inversible. On peut calculer pour tout vecteur projectif $X = [X_0, \dots, X_n]$, $Y_j = \sum_{i=0}^n a_{ji} X_i$ ce qui fournit une application :

$$\begin{aligned} \phi_A: \quad \mathbb{P}^n &\longrightarrow \mathbb{P}^n \\ [X_0, \dots, X_n] &\longmapsto [Y_0, \dots, Y_n]. \end{aligned}$$

Remarques.

1. On a $\phi_A = \phi_B \iff B = \lambda A, \lambda \in K^\times$. On peut donc remplacer le rôle de GL_{n+1} par $PGL_{n+1}(K) = GL_{n+1}(K)/K^\times$.
2. Si A n'est pas inversible, alors l'application ϕ_A n'est pas bien définie, car il existe un vecteur de coordonnées non toutes nulles qui donne un vecteur de coordonnées toutes nulles (revoir la définition d'espace projectif).

Par contre, si l'on pose $W = \text{Ker}(A)$, alors on peut définir ϕ_A sauf sur un sous-espace

linéaire : $\mathbb{P}^n \setminus \mathbb{P}(W) \longrightarrow \mathbb{P}^n$.

Proposition

On pose $U_0 = \mathbb{A}^1$. Soient les points $0 = [1,0]$, $1 = [1,1]$, $\infty = [0,1] \in \mathbb{P}^1$ et P, Q, R distincts dans \mathbb{P}^1 , alors il existe une unique transformation linéaire telle que $\phi(0) = P$, $\phi(1) = Q$ et $\phi(\infty) = R$.

▷ La preuve résulte totalement de la propriété affine correspondance. On écrit la preuve afin de manipuler. On a $\phi(X_0, X_1) = [aX_0 + bX_1, cX_0 + dX_1]$ avec $ad - bc \neq 0$. On peut même calculer :

$$\phi([1,0]) = [a,c] = P = [p_0, p_1]$$

$$\phi([1,1]) = [a+b, c+d] = Q = [q_0, q_1]$$

$$\phi([0,1]) = [b,d] = R = [r_0, r_1]$$

d'où $(a,c) = \lambda(p_0, p_1)$, $(b,d) = \mu(r_0, r_1)$ et $(a+b, c+d) = \nu(q_0, q_1)$. Les solutions (a,b,c,d) sont uniques à un scalaire près. ■

1.1.3 Paramétrage des sous-espaces linéaires

On voit comment ça marche sur un exemple.

Exemple. (Paramétrer un s.e.l)

Prenons une droite projective $D \subseteq \mathbb{P}^n$. On peut écrire :

$$\begin{aligned} \phi: \quad \mathbb{P}^1 &\longrightarrow \mathbb{P}^n \\ [U_0, U_1] &\longmapsto [a_0U_0 + b_0U_1, \dots, a_nU_0 + b_nU_1]. \end{aligned}$$

On a $\phi(\mathbb{P}^1) = D$, de plus, ϕ est une bijection entre \mathbb{P}^1 (toujours pris pour un paramétrage) et D .

On verra qu'on peut toujours paramétrer une droite, puis, dans un théorème fondamental, paramétrer une conique sous une hypothèse faible (existence d'un point rationnel, ou ce qui est suffisant, K algébriquement clos). Par contre, nous verrons qu'il est impossible de paramétrer les cubiques lisses.

1.2 Courbes affines, courbes projectives

1.2.1 Qu'est-ce qu'une courbe ?

On se place désormais dans \mathbb{P}^2 . Les droites, les coniques, les cubiques, etc., sont alors des courbes planes.

Définition. (Courbe projective)

Une *courbe de degré d* est un polynôme homogène non nul de degré d en (X,Y,Z) modulo la relation $F_1 \sim F_2 \iff \exists \lambda \in K^\times \quad F_2 = \lambda F_1$, qu'il faut voir dès lors comme correspondant au lieu d'annulation du polynôme, avec une certaine multiplicité.

Remarquons que si $V = K[X,Y,Z]_d$, l'ensemble des courbes de degré d est $\mathbb{P}(V)$.

Définition. (Courbe projective)

Une *courbe de degré d* est un polynôme homogène non nul de degré d en (X,Y) , qu'il faut voir dès lors comme correspondant au lieu d'annulation du polynôme, avec une certaine multiplicité.

Remarquons que si $V = K[X,Y]$, l'ensemble des courbes de degré d est V .

Reformulation pratique. (Courbe et ensembles algébriques)

Les ensembles algébriques sont les intersections quelconques de courbes.

VOC Le *degré* de la courbe C_F est le degré du *polynôme minimal* F_1, \dots, F_k où $F = F_1^{n_1} \dots F_k^{n_k}$ avec les F_i , $i \in \llbracket 1, k \rrbracket$, $k \in \mathbb{N}$ irréductibles, *i.e.*, dans le cas affine, si $F(x,y) = \sum_{r,s} c_{r,s} x^r y^s$, $\deg(C_F) = \max\{r+s \mid c_{r,s} \neq 0\}$.

Exemples. (Courbe)

1. $F_1 = X^d + Y^d + Z^d$ est une courbe.
2. $F_2 = X^d$. C'est la droite $X = 0$ avec la multiplicité d .

On énonce une première version du théorème de Bézout pour la géométrie algébrique, décrivant l'intersection d'une droite et d'une courbe algébrique.

Théorème. (Théorème de Bézout faible)

On suppose K algébriquement clos. Soit C une courbe de degré d dans \mathbb{P}^2 , D une droite de \mathbb{P}^2 , alors ou bien $D \subseteq C$, ou bien $D \cap C$ est composé de d points avec multiplicités.

▷ Soit $F(X,Y,Z) = 0$ équation de C , $L(X,Y,Z) = aX + bY + cZ = 0$ équation de D avec $(a,b,c) \neq (0,0,0)$. Dans le premier cas, L divise F . Dans le second, L ne divise pas F . On cherche les $x \in \mathbb{P}^2$ tels que $F(x) = L(x) = 0$. Disons $c \neq 0$ pour fixer les idées. Alors $Z = -\frac{a}{c}X - \frac{b}{c}Y$. Par suite, $G(X,Y) = F(X,Y, -\frac{a}{c}X - \frac{b}{c}Y)$ est homogène de degré d non nul. Or puisque K est algébriquement clos, le

théorème de d'Alembert-Gauss généralisé s'écrit : $G(X,Y) = \prod_{i=1}^d (\alpha_i X + \beta_i Y)$ avec $(\alpha_i, \beta_i) \neq (0,0)$ ¹ donc on obtient d points dans l'espace projectif : $[X,Y] = [-\beta_i, \alpha_i]$, soit $[X,Y,Z] = [-\beta_i, \alpha_i, +\frac{a}{c}\beta_i - \frac{b}{c}\alpha_i] \in \mathbb{P}^2$. En résumé : un polynôme homogène non nul est le produit de d formes linéaires en deux variables $G(X,Y) = \prod L_i(X,Y)$ est les L_i sont uniques à un scalaire près. ■

Conséquence. (Où une droite est contenue dans une courbe)

Si $D \cap C$ contient $d + 1$ points (au moins), alors $D \subseteq C$.

Propriété. (Dimension de l'espace des polynômes homogènes)

L'espace des polynômes homogènes de degré d en X_0, \dots, X_n est de dimension $\dim(S_{d,n}) = \binom{n+d}{n}$.

Proposition. (Conique, cubique, quadrique, etc.)

Dans le cas $n = 2$ du plan projectif, on obtient :

$$\dim(S_d) = \binom{d+2}{2} = \frac{(d+1)(d+2)}{2}.$$

En particulier :

1. l'espace des *coniques* S_2 est de dimension 6 ;
2. l'espace des *cubiques* S_3 est de dimension 10 ;
3. l'espace des *quadriques* S_4 est de dimension 15 ;
4. l'espaces des *quintiques* S_5 est de dimension 21 ;

etc. Ainsi :

1. l'espace des coniques de \mathbb{P}^2 s'identifie à \mathbb{P}^5 ;
2. l'espaces des cubiques de \mathbb{P}^2 s'identifie à \mathbb{P}^9 ;
3. l'espaces des quadriques de \mathbb{P}^2 s'identifie à \mathbb{P}^{14} ;

etc.

¹ En effet, si $H(U,V)$ est un polynôme homogène de degré d non nul, alors $H(u,1) = a_0 \prod_{j=1}^{d_1} (u - \alpha_j)$ car c'est

un polynôme à une variable de degré $d_1 \leq d$. Or $H(U,V) = V^d H(\frac{U}{V}, 1) = a_0 V^{d-d_1} \prod_{i=1}^{d_1} (U - \alpha_i V)$. Remarquons que la factorisation des polynômes homogènes à plusieurs variables en facteurs linéaires ne tient plus en dimension projective $n \geq 2$; il y a dans $\mathbb{P}^2(\mathbb{C})$ d'autres courbes que les réunions de droite (autrement dit : il existe des polynômes homogènes en trois variables qui ne sont pas des produits de formes linéaires).

1.2.1.1 Interprétation du degré d'une courbe plane projectif

Prenons l'exemple du corps \mathbb{C} pour changer. Une courbe $L \subseteq \mathbb{CP}^2$ est une *ligne* si elle est définie par $L = \{[x, y, z] \in \mathbb{CP}^2 \mid ax + by + cz = 0\}$. On considère l'action de $GL_{n+1}(\mathbb{C})$ sur \mathbb{CP}^n . Elle est transitive sur l'ensemble des lignes de \mathbb{CP}^2 . Fixons donc la ligne $L = \{[x, y, 0] \in \mathbb{CP}^2\}$. Alors $C_F \cap L = \{[x, y, 0] \in \mathbb{CP}^2 \mid F(x, y, 0) = 0\}$. Supposons que F est irréductible, en particulier z n'est pas un facteur de F . Alors $F(x, y, 0)$ est homogène, du même degré que $F(x, y, z)$, et $F(x, y, 0)$ se décompose en d termes linéaires. Pour un terme linéaire $(b_i x - a_i y)$, le point $(a_i, b_i) \in \mathbb{C}_F$ est l'intersection de C_F à la ligne. Ainsi, $\deg(C_F) = \#(C_F \cap L)$ en comptant la multiplicité. Si F est minimal, la même interprétation tient en décomposant $C_F = C_{F_1} \cup \dots \cup C_{F_k}$, en imposant $L \neq C_{F_i}$ pour chaque i . (On a utilisé que $\mathbb{CP}^2 = \mathbb{CP}^2 \sqcup \mathbb{CP}^1$.)

1.2.2 Application : le théorème des 5 points

De la propriété précédente, on déduit :

Proposition. (Théorème des cinq points projectif)

Soient $P_1, \dots, P_5 \in \mathbb{P}^2$. Il existe une conique passant par ces cinq points.

▷ On note $S_2(P_1, \dots, P_5) = \{Q \in S_2, Q(P_1) = \dots = Q(P_5) = 0\}$. Alors $\dim(S_2(P_1, \dots, P_5)) \geq 6 - 5 = 1$, où 6 est la dimension de S_2 et 5 le rang maximal du système, d'où le résultat. (Plus généralement, $\dim(S_2(P_1, \dots, P_n)) \geq 6 - n$.) ■



Il n'y a pas unicité de la conique passant par cinq points ! S'il n'y a pas unicité, il y a même une infinité de coniques qui satisfassent à la condition ; on précise ce fait dans le théorème suivant.

Théorème. (Théorème des cinq points projectif fort)

Soient P_1, \dots, P_5 cinq points distincts de \mathbb{P}^2 . Alors il existe une conique passant par les cinq points donnés. De plus, la conique est unique si et seulement si les points P_i sont quatre à quatre non alignés (autrement dit, aucun quadruplet de $\{P_1, \dots, P_n\}$ n'est *aligné*).

▷ La première partie a déjà été justifiée.

Montrons la condition d'unicité.

Si quatre points sont alignés, alors la réunion d'une droite passant par ces quatre points et d'une droite passant par l'autre est une conique ; il n'y a pas unicité.

Réciproquement, supposons que $P_1, \dots, P_3 \in D$. Soit C une conique passant par P_1, \dots, P_5 . Alors $P_1, P_2, P_3 \in C \cap D$. D'après le théorème de Bézout faible, $D \subseteq C$. Donc $C = D \cup D_1$ où $P_4, P_5 \notin D$ par hypothèse et D_1 est l'unique droite passant par P_4 et P_5 ; son existence peut être justifiée, un peu au (petit) marteau-pilon, par le théorème de Bézout.

Dans le deuxième cas, aucun triplet parmi les P_i n'est aligné. Supposons $\dim(S_2(P_1, \dots, P_5)) \geq 2$. Alors pour tout P_6 , $\dim(S_2(P_1, \dots, P_6)) \geq 1$. On fait le choix d'un $P_6 \in D_{P_1, P_2}$ où $P_6 \neq P_1, P_2$. Soit C une

conique passant par P_1, \dots, P_6 . Alors $P_1, P_2, P_6 \in C \cap D_{P_1, P_2}$ donc $C = D_{P_1, P_2} \cup D_1$, mais $P_3, P_4, P_5 \in D_1$, contradiction. Donc $\dim(S_2(P_1, \dots, P_5)) = 1$ et la conique est unique. ■

On se demande si l'on peut déduire de ce théorème le théorème des cinq points en géométrie affine.

Exercice 1 (Et dans \mathbb{A}^2 ?)

Soient $P_1, \dots, P_5 \in \mathbb{A}^2$. Peut-on déduire de ce qui précède le théorème des cinq points pour ceux-là ?

▷ Éléments de réponse.

L'existence, oui : il existe une conique affine telle que $ax^2 + by^2 + cxy + dx + ey + f = 0$ passant par les P_i , avec $(a, c, d, e, f) \neq (0, \dots, 0)$. Quant à l'unicité, on ne peut la déduire : la condition qu'aucun quadruplet projectif est aligné n'est pas caractérisante.

Plus généralement :

Proposition. (Théorème des neuf points)

Soient $P_1, \dots, P_9 \in \mathbb{P}^2$. Il existe une cubique passant par ces neuf points.

Plus généralement encore :

Proposition. (Théorème des quelques points)

Soient $P_1, \dots, P_{\frac{d(d+3)}{2}} \in \mathbb{P}^2$. Il existe une courbe de degré d passant par ces points.

On retiendra l'inégalité fondamentale :

Formule

$$\dim(S_d(P_1, \dots, P_r)) = \dim\{Q \in S_d, Q(P_1) = \dots = Q(P_r) = 0\} \geq \frac{(d+1)(d+2)}{2} - r.$$

Attention ! Il contient toujours la courbe pleine, définie par le polynôme homogène nul de tout degré, qui définit tout l'espace. (Alors il ne compte pas vraiment...)

1.2.3 Notion de tangente (à une courbe, en un point)

1.2.3.1 Définitions de base sur la singularité et de la lissité

Définition. (*Tangente ou droite exceptionnelle*)

Soit C une courbe, $P_0 \in C$ et D une droite passant par P_0 . On dit que D est *tangente*, ou *exceptionnelle*, si D rencontre C en P_0 avec multiplicité ≥ 2 .

Lemme

Soit $f = 0$ l'équation de $C \ni P = (x_0, y_0)$ et $f = f_0 + \dots + f_d$ la décomposition homogène de f en $(x - x_0, y - y_0)$ avec les notations évidentes, soit $f = f(x_0, y_0)(= 0) + a(x - x_0) + b(y - y_0) + f_2(x - x_0, y - y_0) + \dots$. Premier cas, $(a, b) \neq (0, 0)$. La seule droite exceptionnelle $T_{P_0}(C) : a(x - x_0) + b(y - y_0) = 0$. Deuxième cas : $(a, b) = (0, 0)$. Alors toutes les droites passant par P_0 sont exceptionnelles (fait purement conventionnel).

Remarque. $(a, b) = \left(\frac{\partial f}{\partial x}(x_0, y_0), \frac{\partial f}{\partial y}(x_0, y_0) \right)$ par la formule de Taylor polynomiale.

Définition. (*Point lisse, point singulier*)

Soit C une courbe, $P_0 \in C$. On dit que P_0 est *lisse* ou bien *non singulier* s'il admet une tangente (unique), soit $\left(\frac{\partial f}{\partial x}(x_0, y_0), \frac{\partial f}{\partial y}(x_0, y_0) \right) \neq (0, 0)$.

Remarque. Si C est définie par $F(X, Y, Z) = 0$ dans \mathbb{P}^2 , $P_0 = [X_0, Y_0, Z_0]$ est lisse si et seulement si une des dérivées $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ est non nulle en $[X_0, Y_0, Z_0]$, ce qui a du sens puisque la dérivée d'un polynôme homogène est homogène.

VOC Plus généralement, en un point singulier, le premier polynôme non nul de la décomposition homogène de Taylor définit l'ordre de la singularité et le *polynôme homogène associé à la singularité*.



Tous les points d'une courbe ne sont pas lisses, en particulier les points par laquelle la courbe passe deux fois, et également les points de rebroussements.

Exemples. (*Points singuliers*)

1. La courbe plane définie par $F(x, y) = y^2 - x^3 - x^2$ admet un point singulier du second ordre en $(0, 0)$. Le polynôme homogène associé est $y^2 - x^2 = (y - x)(y + x)$.

Définition. (*Singularité ordinaire*)

On considère une courbe plane (et donc un polynôme à deux variables). Une *singularité ordinaire* est une singularité dont les facteurs linéaires de la décomposition, qui existe par théorème, du polynôme homogène associé sont tous distincts.

Définition. (*Nœud*)

Une singularité ordinaire du second ordre d'une courbe plane est appelée un *nœud*.

Définition. (*Sécante*)

Une *sécante* d'une courbe plane est une ligne contenant au moins de points de cette courbe. Intuitivement, ce n'est pas une tangente, ni une ligne disjointe.

1.2.3.2 Quelques propriétés de base des singularités**Proposition. (*Singularité des courbes réductibles*)**

Une courbe non irréductible est singulière.

▷ On écrit l'équation de la courbe sous la forme $FG = 0$ où $F(x_0, y_0, z_0) = G(x_0, y_0, z_0) = 0$. Le point $[x_0, y_0, z_0]$ est singulier sur C , car $\frac{\partial}{\partial X}(FG) = \frac{\partial}{\partial X}F \cdot G + F \frac{\partial G}{\partial X}$ vaut 0 en (x_0, \dots, z_0) . ■

Proposition. (*Lissité des coniques*)

Une conique est irréductible si et seulement si elle est lisse.

▷ D'après la proposition précédente, une conique lisse est irréductible. Réciproquement, soit C une conique et P_0 un point singulier. On choisit $Q \in C$ tel que $Q \neq P_0$. Alors $D = D_{PQ}$ rencontre C en Q et en P_0 , mais avec multiplicité en P_0 supérieure à 2. Par le théorème de Bézout, $D \subseteq C$ donc $C = D \cup D_1$. ■

Proposition. (*Lissité des cubiques*)

Une cubique irréductible est soit lisse, soit a un unique point singulier.

▷ Soit C une cubique. Il suffit de montrer que si P, Q sont deux points singuliers distincts, $D = D_{P,Q}$ coupe C en P et Q avec une multiplicité ≥ 2 ; par le théorème de Bézout, $D \subseteq C$. ■

Exercice 2

Montrer que, sur une cubique dite *de Weierstrass* $F = -Y^2Z + X^3 + AXZ^2 + BZ^3 = 0$, le point à l'infini est lisse : $O = [0, 1, 0]$. Effectuer le calcul en coordonnées affines.

▷ **Éléments de réponse.**

Il suffit de remarquer que $\frac{\partial F}{\partial Z}(0,1,0) = -1 \neq 0$.

1.2.4 Description des coniques projectives

On peut décrire, comme dans les petites classes, l'ensemble des coniques : deux droites, éventuellement confondues, et les coniques irréductibles (sur \mathbb{R} , dans \mathbb{A}^2) : ellipses, hyperboles, paraboles. Citons également l'ensemble vide d'équation $x^2 + y^2 + 1 = 0$ sur \mathbb{R} . On peut préciser ces descriptions.

Théorème. (*Description des coniques projectives*)

Soit C une conique irréductible, *i.e.* non dégénérée.

1. Si K est algébriquement clos, posons $C_0 : XY - Z^2 = 0$. Alors il existe $\phi : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$ linéaire projective telle que $\phi(C) = C_0$. Autrement dit, toutes les coniques sont les mêmes.
2. Toujours si K est algébriquement clos, grâce à l'application $f : \mathbb{P}^1 \longrightarrow \mathbb{P}^2$ qui à $(U_0, U_1) \mapsto (U_0^2, U_1^2, U_0 U_1)$, on a même un isomorphisme (bijection bidéfinie par des polynômes) $\mathbb{P}^1 \simeq C_0$.
3. Si K est quelconque, si la conique C a un point à coordonnées rationnelles (autrement dit, dans K , donc si $C(K) \neq \emptyset$), alors $\mathbb{P}^1 \xrightarrow{\sim} C$ où $\mathbb{P}^1 \simeq$ l'ensemble des droites passant par P_0 dans \mathbb{P}^2 .

▷ En caractéristique 2, le résultat tient mais il faut construire une démonstration ad hoc, laissée en exercice. On suppose donc $\text{car}(K) \neq 2$. Soit $Q(X, Y; Z) = aX^2 + bY^2 + cZ^2$ un polynôme homogène ; il est irréductible si et seulement si $abc \neq 0$. En effet, on a déjà vu le sens réciproque ; on peut vérifier à la main le sens direct. En changeant de coordonnées de façon évidente, par exemple : $X^2 - Y^2 - Z^2 = (X - Y)(X + Y) - Z^2 \sim X'Y' - Z'^2$.

Pour le deuxième point, on prend l'isomorphisme proposé, dit *de Veronese*, où clairement $\phi(\mathbb{P}^1) \subseteq C := C_0$. Montrons que ϕ est injective. Supposons $[U_0^2, U_1^2, U_0 U_1] = [V_0^2, V_1^2, V_0 V_1]$. On peut supposer $U_0 \neq 0$, d'où $[U_0, U_1] = [1, x]$ et ce vecteur égale $[1, x^2, x]$ où $x = U_1/U_0$, donc $V_0 \neq 0$ et $[V_0, V_1] = [1, y] = [1, y^2, y]$ où $y = V_1/V_0$. Donc $x = y$. Montrons que ϕ est surjective. Soit $P = [X, Y, Z]$ avec $XY - Z^2 = 0$. Si $X = 0$, alors $P = [0, 1, 0] = \phi([0, 1])$. Si $X \neq 0$, $P = [1, y, z]$ avec $y = Y/X$ et $z = Z/X$. Alors $y = z^2$ et $\phi([1, z]) = [1, z^2, z] = P$. On observe que la bijection réciproque est bien définie par des polynômes.

On a $\mathbb{P}^2 = \mathbb{P}(V)$ où $V = \mathbb{A}^3$. Ainsi $D = \mathbb{P}(W)$ où W est un sev de V de dimension 2, et $P \in \mathbb{P}(U)$ où U est une droite vectorielle dans V . Alors $P \in D \iff U \subseteq W$. On a donc une bijection entre les plans contenant U et les droites (vectorielles) de V/U donné par $W \mapsto$ image de W dans le quotient et réciproquement : droite $\mapsto \pi^{-1}(\text{droite})$, en notant la projection canonique $\pi : V \longrightarrow V/U$, donc comme $\mathbb{P}(V/U) = \mathbb{P}^1$, on a une bijection entre les droites de \mathbb{P}^2 contenant P_0 et \mathbb{P}^1 . On peut donc, en notant \mathcal{D}_{P_0} l'ensemble des droites de \mathbb{P}^2 passant par P_0 , on introduit une application ϕ de $\mathcal{D}_{P_0} \longrightarrow C$ qui à D fait correspondre le second point d'intersection de D avec C , car $D \cap C = \{P_0, \phi(D)\}$ d'après le théorème

de Bézout faible (éventuellement, dans le cas tangent, $\phi(D) = P_0$). Cette application est injective, car si $\phi(D) = \phi(D')$, alors D et D' ont deux points en commun P_0 et $\phi(D)$, d'où $D = D'$, ou alors par unicité de la tangente. Pour la surjectivité, on remarque $P_0 = \phi(T_{P_0}C)$, notation pour la tangente, et $P = \phi(D_{P_0P})$, notation pour la droite passant par deux points. Il suffit de donner maintenant une écriture explicite polynomiale de ϕ . On peut supposer $P_0 = [0,0,1]$. La droite projective $aX + bY + cZ = 0$ contient P_0 si et seulement si $c = 0$. On peut identifier $D_{P_0} = \{[a,b] \mid [a,b] \in \mathbb{P}^1\}$. La conique C a pour équation $AX^2 + BXY + CY^2 + DXZ + EYZ = 0$. Cherchons $\mathcal{D}_{[a,b]} \cap C_0$. Disons $a \neq 0$ par non-dégénération ; alors $X = -\frac{b}{a}Y$. On peut donc récrire $A\frac{b^2}{a^2}Y^2 - B\frac{b}{a}Y^2 + CY^2 - D\frac{b}{a}YZ + EYZ = 0$. Cela revient à $X = -\frac{b}{a}Y$ et $(A\frac{b^2}{a^2} - B\frac{b}{a} + c)Y + (-D\frac{b}{a} + E)Z = 0$. ■

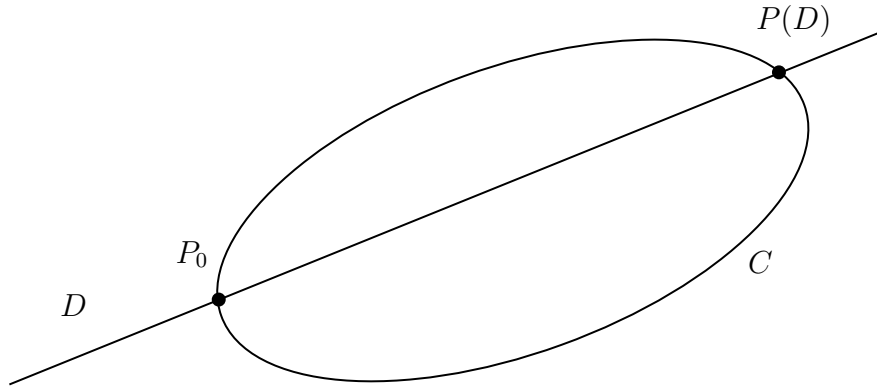


FIGURE 1.2.1 : *Description des coniques projectives.* —
Illustration du cas non algébriquement clos, par exemple $\mathbb{P}^2(\mathbb{R})$.

Corollaire. (Théorème de Bézout pour les coniques)

Soit C_1 une conique et C_2 une courbe de degré d dans \mathbb{P}^2 sans composante commune (c'est-à-dire que les polynômes qui la définissent sont premiers entre eux). Alors $\#C_1 \cap C_2 = 2d$ comptés avec multiplicités. En particulier, l'intersection d'une conique et d'une courbe de degré d est de cardinal au plus $2d$ ou alors l'une est incluse dans l'autre ou alors encore elles ont une droite commune.

▷ Si $C_1 = D_1 \cup D_2$, c'est le théorème de Bézout faible. Si C_1 est irréductible, on peut supposer que $C_1 = \phi(\mathbb{P}^1) = \{[X,Y,Z] \in \mathbb{P}^2 \mid XY - Z^2 = 0\}$ et $\phi([U_0,U_1]) = [U_0^2,U_1^2,U_0U_1]$. Soit $F = 0$ l'équation de C_2 . Alors $C_2 \cap C_1 = \{\phi([U_0,U_1]) \mid [U_0,U_1] \in \mathbb{P}^1 \text{ et } F \circ \phi(U_0,U_1) = 0\}$. Ainsi $F \circ \phi(U_0,U_1) = F(U_0^2,U_1^2,U_0U_1)$ est homogène de degré $2d$ non nul, donc s'écrit $\prod_{i=1}^{2d} (\alpha_i U_0 + \beta_i U_1)$. ■

Heuristique

Si la droite est distincte de la conique projective, c'est une ellipse ; sécante, hyperbole ; tangente, parabole.

On termine par une considération qui ne nous sera pas utile tout de suite.

Lemme. (*Caractérisation des coniques dégénérées*)

Soit $C : AX^2 + BXY + CY^2 + DX + EY + F = 0$. Alors C est dégénérée si et seulement si $4ACF + BDE - AE^2 - B^2F - CD^2 = 0$.

▷ En effet, le déterminant de la matrice symétrique de la forme quadratique s'écrit

$$4 \det \begin{vmatrix} A & B/2 & D/2 \\ B/2 & C & E/2 \\ D/2 & E/2 & F \end{vmatrix}. \blacksquare$$

1.2.5 Cubiques et courbes elliptiques

Nous allons voir qu'avec une petite condition, les cubiques lisses sont munies d'une loi de groupe, ce qui n'était pas le cas des coniques.

On rappelle que $\dim(S_3) = 10$. Alors S_3 est composé des conique + droite, des triplets de droites et des cubiques irréductibles (ou *lisses*, ou *non singulières*) venant de $y^2 = x^3 + x^2$ avec $(0,0) \in C$, d'où l'équation projective :

$$ZY^2 = X^3 + X^2Z \text{ irréductible singulière.}$$

Les courbes coniques du plan projectif peuvent prendre des formes très diverses : à deux composantes connexes par arcs (comme pris en exemple dans la preuve ci-dessous), une courbe à deux méandres, éventuellement très inégaux, des courbes relativement « droites », à l'inverse, des trous de serrure, puis, parmi les cubiques non lisses, avec des points doubles, des points de rebroussement, puis, parmi les cubiques dégénérées, une conique et une droite, ou encore la réunion trois droites dans toutes configurations possibles.

Définition. (*Addition de points sur une courbe cubique*)

On définit une loi de composition sur les points d'une cubique lisse. On note O = point à l'infini. Par le théorème de Bézout, on peut bien définir une loi qui à deux points P, Q d'une cubique, fait correspondre la construction suivante : on trouve l'unique $S = P \star Q$ troisième point d'intersection de la droite $D_{P,Q}$ avec la cubique, qui est éventuellement un point à l'infini. Dans le cas où $P = Q = R$, on considère la tangente $T_R(C)$ à la place (d'après la section consacrée, elle existe toujours pour une cubique lisse). Alors on pose pour $P + Q = O \oplus S$, le troisième point d'intersection à C de (OS) . Autrement dit,

$$P + Q = O \oplus (P \oplus Q).$$

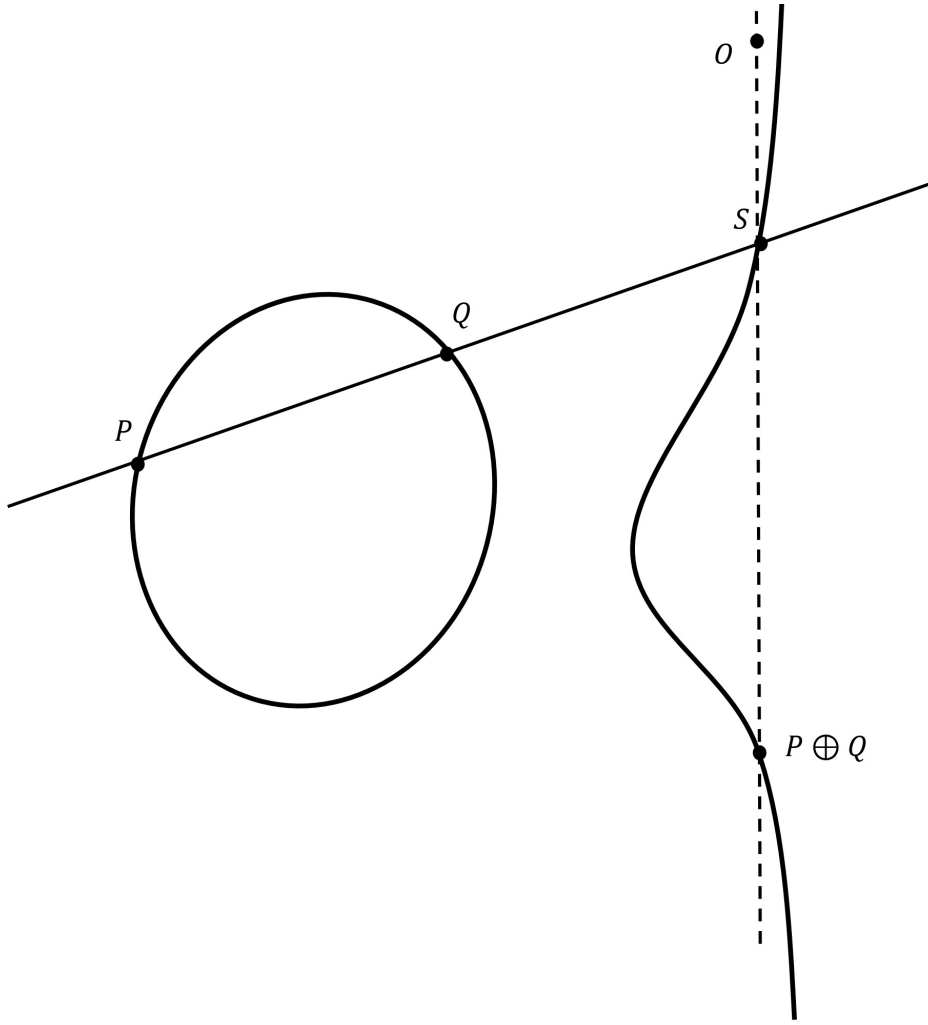


FIGURE 1.2.2 : Addition de deux points d'une cubique. —

Définition d'une loi de groupe sur une cubique à deux composantes connexes. Notons que le point O est égal en projectives au point à l'infini de l'autre branche.

Théorème. (Groupe d'une cubique lisse)

(C, \oplus) est un groupe abélien. De plus, la loi de groupe est algébrique, *i.e.* définie par des polynômes.

▷ $P \oplus Q = Q \oplus P$ de façon immédiate.

Vérifions que O est élément neutre : montrons que $P \oplus O = P$ pour P arbitraire. Dans le cas $P \neq O$, $D_{P,O} \cap C = \{P, O, P'\}$. Or $D_{P',O} = D_{P,O}$ donc $D_{P',O} \cap C = \{P', O, P\}$ donc $P \oplus O = P$. Dans le cas $P = O$, par définition $D_{O,O} = T_O(C)$ donc $T_O(C) \cap C = \{O, O, O'\}$. Or $D_{O,O'} = T_O(C)$ donc $D_{O,O'} \cap C = \{O, O', O\}$, d'où $O \oplus O = O$.

Cherchons l'inverse de P . On a $D_{O,P} \cap C = \{O, P, P'\}$ et $D_{O',P'} \cap C = \{O', P', P''\}$. D'autre part $D_{O',P} \cap C = \{O', P, P''\}$ d'où $P'' \oplus P = O$, car $D_{P,P''} = D_{O',P}$, $D_{P,P''} \cap C = \{O', P, P''\}$ et $D_{O,O'} = T_O(C)$ d'où $D_{O,O'} \cap C = \{O, O', O\}$.

On peut essayer d'intuiter l'associativité sur un dessin, mais les imprécisions graphiques s'accumulent trop pour qu'il soit convaincant. Précisément : pour

$$\begin{aligned} L_1 &= D_{PQ}, L_1 \cap C = \{P, Q, S\}, M_1 = D_{QR}, M_1 \cap C = \{Q, R, V\} \\ L_2 &= D_{OS}, L_2 \cap C = \{O, S, S'\}, M_2 = D_{OV}, M_2 \cap C = \{O, V, V'\} \\ L_3 &= D_{RS'}, L_3 \cap C = \{R, S', T\}, M_3 = D_{V'P}, M_3 \cap C = \{V', P, W\} \\ L_4 &= D_{OT}, L_4 \cap C = \{O, T, T'\}, M_4 = D_{OW}, M_4 \cap C = \{O, W, W'\}, \end{aligned}$$

on pose $T' = (P \oplus Q) \oplus R$ et $W' = P \oplus (Q \oplus R)$. On veut montrer $W' = T'$, c'est-à-dire, $W = T$. Il est possible de faire un dessin de tout cela, mais c'est rapidement atroce.

Pour montrer l'associativité, on aura besoin du fait suivant :

Proposition. (*Principe de prolongement des identités algébriques*)

Soient P_1, P_2 et $Q \neq 0$ sur $K[X_1, \dots, X_n]$. Si pour tout $x \in \mathbb{A}^n$ et tel que $Q(x) \neq 0$, on a $P_1(x) = P_2(x)$, alors $P_1 = P_2$.

▷ En effet, $Q(P_1 - P_2)(x) = 0 \ \forall x$ donc la composition $Q(P_1 - P_2) = 0$, d'où $P_1 = P_2$. Remarquons que sur \mathbb{R} ou \mathbb{C} , on aurait pu invoquer un argument de continuité; en général, c'est possible en se munissant de la topologie de Zariski. ■

Reprenons la preuve.

La stratégie est la suivante : l'égalité $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ est une identité, notée (\star) , polynomiales en les coordonnées de P, Q, R . Il suffit de démontrer (\star) pour P, Q, R dont une configuration intuitivement non dégénérée par le principe de prolongement; nous allons donner une démonstration géométrique.

Pour cela, nous utiliserons les résultats suivants :

Lemme. (*Lemme des huit points*)

Soient P_1, \dots, P_8 distincts dans \mathbb{P}^2 . On suppose qu'il n'y a pas parmi eux sept points sur une même conique ni quatre points sur une droite. Alors $\dim(S_3(P_1, \dots, P_8)) = 2$.

▷ Remarquons que ≥ 2 est immédiat.

Dans le premier cas, P_1, P_2 et P_3 sont alignés. On choisit $Q \in D_{P_1 P_2}$ distinct d'eux trois, de sorte que $\dim(S_3(P_1, \dots, P_8, Q)) \geq 1$, donc il existe une cubique C passant par P_1, \dots, P_8 et Q . On a $\{P_1, P_2, P_3, Q\} \subseteq C \cap D$, donc par le théorème de Bézout, $C = D \cup C_0$ conique, donc $P_4, P_5, P_6, P_7, P_8 \in C_0$. Or C_0 est unique, donc $\dim(S_3(\dots, Q)) = 1$, donc $\dim(S_3(P_1, \dots, P_8)) \leq 2$, donc elle est égale à 2.

Dans le second cas, $P_1, \dots, P_6 \in C_0$ conique (irréductible). On choisit Q distinct d'eux six et $Q \in C_0$. Alors $\dim(S_3(P_1, \dots, P_8, Q)) \geq 1$. Soit C une cubique dans cet espace. Alors $\{P_1, \dots, P_6, Q\} \subseteq C \cap C_0$. Par le théorème de Bézout, $C = C_0 \cup D$ mais forcément $D = D_{P_7, P_8}$, donc $\dim(S_3(P_1, \dots, P_8, Q)) = 1$, et l'on conclut de même.

Enfin, supposons qu'il n'y a aucun triplet aligné, aucun sextuplet conconique. Supposons que $\dim(S_3(P_1, \dots, P_8)) \geq 3$. On choisit $Q, R \in D_{P_1 P_2}$ distincts. Alors $\dim(S_3(P_1, \dots, P_8, Q, R)) \geq 3 - 2 = 1$; il existe donc une cubique C passant par ces 10 points. Alors $\{P_1, P_2, Q, R\} \subseteq C \cap D_{P_1 P_2}$, donc $C = D_{P_1 P_2} \cup C_0$ conique. Ainsi $P_3, \dots, P_8 \in C_0$, mais donc six des points sont sur la conique, ou la conique contient une droite : contradiction. ■

Corollaire. (*Unicité de la cubique passant par neuf points*)

Soit C une cubique irréductible et C_1 une cubique. Si $\{P_1, \dots, P_9\} = C \cap C_1$ avec P_1, \dots, P_8 distincts, alors si un troisième conique C_2 passe par P_1, \dots, P_8 , elle passe par P_9 .

▷ Si P_1, \dots, P_4 étaient alignés sur D , on aurait $\{P_1, \dots, P_4\} \subseteq C \cap D$, donc $C = D \cup C_0$, absurde. Si P_1, \dots, P_7 étaient conconiques dans C_0 , $\{P_1, \dots, P_7\} \subseteq C \cap C_0$, donc C est non irréductible; absurde. Soit F l'équation de C , F_1 celle de C_1 . Ainsi $S_3(P_1, \dots, P_8) = \text{vec}(F, F_1)$ de dimension 2. Soit F_2 l'équation définissant C_2 . On obtient $F_2 \in S_3(P_1, \dots, P_8)$, donc $F_2 = aF + bF_1$, donc $F_2(P_9) = 0$. ■

On peut combiner ces arguments.

Ainsi, on applique ce lemme à C notre cubique lisse, $C_1 = L_1 \cup M_2 \cup L_3$ et $C_1 \cap C = \{P, Q, S, O, V, V', R, S', T\}$ et $C_2 = M_1 \cup L_2 \cup M_3$, $C_2 \cap C = \{Q, R, V, O, S, S', V', P, W\}$.

Afin de conclure, il reste à montrer que la loi de groupe $P \oplus Q$ est définie par des polynômes; on pourra ainsi appliquer le principe de prolongement et conclure sur l'associativité, et la preuve sera terminée. On le fait sur une cubique de la forme suivante de Weierstrass : $ZY^2 = X^3 + AXZ^3 + BZ^3$. On prétend que toute cubique se ramène à cette forme; ainsi, les formules sont semblables, mais plus longues, pour une cubique générale. On se place en caractéristique $\neq 2, 3$ et l'on prétend également que la lissité de la cubique équivaut à $4A^3 + 27B^2 \neq 0$. On pose $O = [0, 1, 0]$ qui est le point à l'infini si on place la droite à l'infini D_∞ avec $Z = 0$; dans ce cas, $D_\infty \cap C = 3(\infty)$ et le point à l'infini est un point d'inflexion. Ainsi $C \cap \mathbb{A}^2 = \mathbb{P}^2 \setminus \{z = 0\}$ et l'on peut à l'équation $y^2 = x^3 + Ax + B$. Posons $P = (x_1, y_1)$, $Q = (x_2, y_2)$ et $P \oplus Q = (x_3, y_3)$, et calculons. La droite $D_{P, Q}$ est d'équation $y = \lambda x + \mu$. Par un simple calcul, si $x_1 \neq x_2$, $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ et sinon grâce à l'équation de la tangente $\lambda = \frac{3x_1^2 + A}{2y_1}$ et $\mu = y_1 - \lambda x_1$. En injectant les points P, Q dans la nouvelle équation, on a $(y_1 + y_2)(y_1 - y_2) = x_1^3 - x_2^3 + A(x_1 - x_2)$ et l'on obtient $\lambda = \frac{x_1^2 + x_1 x_2 + x_2^2 + A}{y_1 + y_2}$ si $x_1 = x_2$ et $y_2 \neq -y_1$, c'est-à-dire $P = Q$, $Q \neq -P$; remarque, si $Q = -P$, on a $P \oplus Q = O$. Alors $C \cap D_{P, Q}$ se détermine par $y = \lambda x + \mu$ et $x^3 + Ax + B - (\lambda x + \mu)^2 = (x - x_1) \dots (x - x_3) = 0$, d'où $\lambda^2 = x_1 + x_2 + x_3$ en identifiant le coefficient de x^2 . Alors $x_3 = \lambda^2 - x_1 - x_2$ et $y_3 = -(\lambda x_3 + \mu)$. Ceci termine la preuve. ■

Exemple fondamental. (*Inversion sur une cubique de Weierstrass*)

Détaillons avec une cubique de Weierstrass le calcul de $-P$. On pose $D = D_{OP}$ et $D \cap C = \{O, P, -P\}$ (en général : $D_{PQ} \cap C = \{P, Q, -P - Q\}$). De plus $P = [x, y, 1]$ et $O = [0, 1, 0]$. Alors $D = \{X - x_1 Z = 0\}$. Par suite, $D \cap C$ est déterminée par $X - x_1 Z = 0$ et $ZY^2 = X^3 + AXZ^2 + BZ^3$ qui contient par $Z = 0$ le point O . Si $Z \neq 0$, on résout

$x - x_1 = 0$ et $y^2 = x^3 + Ax + B$, dont on déduit si $P = (x_1, y_1)$, $\boxed{-P = (x_1, -y_1)}$.
Ainsi, l'inversion sur les cubiques de Weierstrass s'exprime très simplement.

On mentionne le résultat suivant :

Proposition. (*Paramétrisation des cubiques lisses*)

Soit C une cubique irréductible. Alors si C est lisse, elle n'est pas paramétrisable, autrement dit, il n'existe pas d'application rationnelle $\mathbb{P}^1 \rightarrow C$ non constante telle que $C = \{f(x, y) = 0\}$.

Contre-exemple. (*Paramétrisation de cubiques singulières*)

Soit C_2 la cubique d'équation $y^2 = x^3$. Elle est paramétrée par $t \mapsto (t^2, t^3)$.

Soit encore C_1 la cubique d'équation $y^2 = x^3 + x^2$. On remarque que $(\frac{y}{x})^2 = x + 1$. Si on pose $t = \frac{y}{x}$, $x = t^2 - 1$ et $y = tx = t(t^2 - 1)$, donc $t \mapsto (t^2 - 1, t(t^2 - 1))$ paramétrise C_1 . \square

1.3 Quelques études de variétés projectives particulières

1.3.1 Quadriques

1.3.1.1 Topo sur les quadriques

Définition. (*Quadrique*)

Une *quadrique* est une sous-variété de dimension 2 de \mathbb{P}^3 , c'est-à-dire, une « courbe » de \mathbb{P}^3 définie par une équation de la forme $Q(X, Y, Z, T)$ où Q est un polynôme homogène de degré 2.

Proposition. (*Dimension de l'espace des quadriques*)

L'espace vectoriel des quadriques est de dimension 10.

▷ Déjà vu : l'espace vectoriel des formes quadratiques éventuellement nulles en quatre variables est de dimension $\binom{5}{2} = 10$. ■

■ On suppose, à partir d'ici, que K est algébriquement clos et que $\text{car}(K) \neq 2$.

Définition-propriété. (*Description des quadriques*)

Sous ces hypothèses, après changement de coordonnées, une quadrique est toujours de la forme $Q = aX^2 + bY^2 + cZ^2 + dT^2$.

On pose $\text{rg}(Q)$ le nombre des coefficients $\{a, b, c, d\}$ non nuls.

▷ C'est le théorème de réduction de Gauss pour les formes quadratiques. ■

Exemple. (Quadrique de Segre)

La quadrique $Q = XT - YZ$ est appelée *quadrique de Segre* pour l'avoir déjà rencontrée dans ce contexte.

Théorème. (Classification des quadriques, droites contenues dans une quadrique)

On suppose K algébriquement clos et de caractéristique différente de 2. Soit Q une quadrique. On note $r = \text{rg}(Q)$.

- Si $n = 4$, c'est-à-dire, grosso modo, $Q = X^2 + Y^2 + Z^2 + T^2$, alors $X^2 + Y^2 = (X - \alpha Y)(X + \alpha Y)$ où $\alpha^2 = -1$ puis après changement de coordonnées $Q = XT - YZ$, et l'on a un isomorphisme de la quadrique à $\mathbb{P}^1 \times \mathbb{P}^1$ donné par le plongement de Segre $S_{1,1} = \phi : [x_0, x_1][y_0, y_1] \mapsto [x_0y_0, x_0y_1, x_1y_0, x_1y_1]$. La quadrique est lisse. Les droites contenues dans la quadrique sont de deux familles : $\phi([x_0, x_1] \times \mathbb{P}^1)$ et $\phi(\mathbb{P}^1 \times [y_0, y_1])$, qui forment à elles deux un réseau. (On peut démontrer qu'il n'y a pas d'autres droites.)
- Si $n = 3$, c'est-à-dire si $Q = X^2 + Y^2 + Z^2$, c'est un *cône sur une conique*. La quadrique est irréductible singulière. Les droites sur cette quadrique sont tendues du point $P_0 = [0, 0, 0, 1]$ à un point du plan $T = 0$, en particulier, elles se rencontrent toutes.
- Si $n = 2$, $Q = X^2 + Y^2$ puis après changement de coordonnées $Q = XY$. Il s'agit de deux plans projectifs sécants. Deux droites disjointes appartiennent l'une au plan $X = 0$, l'autre au plan $Y = 0$. Ainsi, trois droites ne peuvent pas être disjointes.
- Si $n = 1$, $Q = X^2$; c'est un plan double. Ses droites sont les droites du plan $X = 0$. Elles se rencontrent toutes.

Remarque. Une quadrique est non singulière si et seulement si elle est de rang 4.

1.3.1.2 Droites sur une quadrique

Corollaire

Si une quadrique contient trois droites qui se rencontrent, alors elle est non singulière.

▷ Simple combinatoire en observant la classification précédente. ■

Lemme. (*Existence d'une conique contenant trois droites*)

Soient L_1, L_2, L_3 trois droites de \mathbb{P}^3 . Alors :

1. Il existe une quadrique contenant $L_1 \cup L_2 \cup L_3$.
2. Si les L_i sont disjointes, alors la quadrique est non dégénérée.

▷ En effet, $\dim(S_2(X, Y, Z, T)) = 10$ et la condition Q nulle sur L impose trois conditions : $Q_{L_i} = 0$ pour $i = 1, 2, 3$ chacune équivalant à trois conditions linéaires, donc un système de rang ≤ 9 . Puisque $10 - 9 \geq 1$, le tour est joué. Le deuxième point est le corollaire précédent. ■

Proposition. (*Théoreme de Bézout pour les quadriques*)

Soit S une surface de degré d dans \mathbb{P}^3 , et L une droite. Alors $\#(L \cap S) \leq d$ ou S contient L .

En particulier, si une droite L de \mathbb{P}^3 rencontre trois droites contenues dans une quadrique S , alors S contient L .

Lemme. (*Quatre droites dans une quadrique*)

Soient L_1, \dots, L_4 des droites disjointes de \mathbb{P}^3 . Soit \mathcal{L} l'ensemble des droites rencontrant L_1, L_2, L_3 et L_4 . Alors \mathcal{L} est infini et alors en bijection avec \mathbb{P}^1 , ou bien $\#\mathcal{L} = 1$ ou 2.

▷ Soit S une quadrique contenant ces trois droites. Si $L_4 \subseteq S$, L_1, \dots, L_4 appartiennent à une des deux familles donc les droites appartenant à l'autre famille rencontrent L_1, \dots, L_4 et ce sont les seules, d'où l'infinité. Ainsi, \mathcal{L} est en bijection ensembliste avec \mathbb{P}^1 . Si maintenant $L_4 \not\subseteq S$, $S \cap L_4 = \{P_1, P_3\}$, avec éventuellement $P_1 = P_3$; soit L une droite de \mathbb{P}^3 qui rencontre ces quatre droites; on a vu que $L \subseteq S$. Alors $L \cap L_4 \neq \emptyset$ et $L \cap L_4 = \{P_1\}$ ou $\{P_2\}$. ■

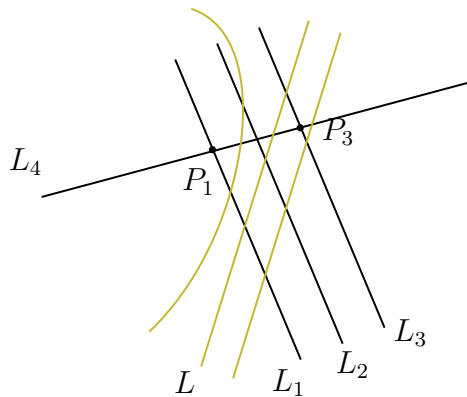


FIGURE 1.3.1 : Droites sur une quadrique. —

1.3.2 Surfaces cubiques

Définition. (*Surface cubique*)

L'ensemble des surfaces cubiques dans \mathbb{P}^3 est $\mathbb{P}(S_3(X,Y,Z,T)) = \mathbb{P}^N$.

Remarque. La variété projective $Z = \{(V,L) \in \mathbb{P}^N \times G(1,3) \mid L \subseteq V\}$ se projette sur \mathbb{P}^N par p et sur $G(1,3)$ par q . On utilise le théorème de la dimension des fibres. Or $q^{-1}(2) = \mathbb{P}^{N-4}$, donc $\dim(Z) = (N-4) + \dim(G(1,3)) = N$. On rappelle que si $L = \{Z = T = 0\}$, $L \subseteq \{F = 0\}$ si et seulement si ni X^3, XY^2, X^2Y, Y^3 dans F . Il existe V cubique avec un nombre fini de droites $XYZ - T^3 = 0$ d'où $\dim(p(Z)) = \dim(Z) = N$. Par l'élimination, $p(Z)$ est fermé donc $p(Z) = \mathbb{P}^N$.

Proposition. (*Description des surfaces cubiques*)

Une surface cubique est irréductible ($F = 0$ avec F irréductible), un plan et une quadrique (alors $F = LQ$), ou bien trois plans.

L'argument précédent montre qu'il existe $U \subseteq \mathbb{P}^N$ tel que pour toute surface cubique $S = V \in U$, $\#\{L \in G(1,3) \mid L \subseteq V\}$ est fini.

On a mieux.

1.3.2.1 Théorème des 27 droites

Théorème. (*27 droites*)

Si S est une surface cubique lisse dans \mathbb{P}^3 , condition bénigne, alors S contient exactement 27 droites (avec une configuration explicite).

Pour le démontrer, on y va pas à pas.

Contre-exemple. (*Pas 27 droites si pas lisse...*)

$XYZ - T^3 = 0$ contient trois droites. □

Contre-exemple. (*Pas 27 droites si pas lisse, encore*)

$X^2Y - Z^2T = 0$ contient une infinité de droites. □

Remarque. On sait déjà, grâce à la théorie de la grassmannienne, qu'il existe une droite sur S .

Soit L une droite $L \subseteq S$, S irréductible. Soit Π_α un plan de \mathbb{P}^3 contenant L , soit $\{\Pi_\alpha\} \simeq \mathbb{P}^1$. Alors $S \cap \Pi_\alpha = L \cup C_\alpha$ où $C_\alpha \subseteq \Pi_\alpha$ est une conique irréductible, ou $S \cap \Pi_\alpha = L \cup L' \cup L''$.

Lemme

Si S est lisse alors dans le second cas, les L, L', L'' sont distinctes.

▷ Supposons $S \cap \Pi = L \cup L' \cup L''$ avec $L = L'$. On peut supposer $\Pi = \{Z = 0\}$ sans perte de généralités. L'équation de S s'écrit $G(X, Y, Z, T) = ZQ(X, Y, Z, T) + L_1^2 L_2$ où les L_i sont des formes linéaires en X, Y, T . Soit P_0 appartenant à $Z = Q = L_1 = 0$. Alors $P_0 \in S$ est singulier ! En effet, $\frac{\partial G}{\partial X} = Z \frac{\partial Q}{\partial X} + 2L_1 \frac{\partial L_1}{\partial X} + L_1^2 \frac{\partial L_2}{\partial X}, \dots, \frac{\partial G}{\partial Z} = Q + Z \frac{\partial Q}{\partial Z}$. Toutes les dérivées partielles sont nulles en P_0 . ■

Remarque. Soient M_1, \dots, M_3 distinctes dans \mathbb{P}^2 . Alors, premier cas, elles forment un triangle non dégénéré ou, second cas, elles sont concourantes, ce qui correspond à une cubique $XYZ = 0$ ou $XY(Y + Z = 0)$. On note $m_i = 0$ l'équation de M_i .

Dans le premier cas, les formes linéaires m_1, m_2, m_3 sont linéairement indépendantes. On peut supposer $m_1 = X, m_2 = Y$ et $m_3 = Z$.

Dans le second cas, $\text{rg}(m_1, m_2, m_3) = 2$, d'où $m_3 = am_1 + bm_2$ et l'on peut supposer $m_1 = X, m_2 = Y, m_3 = X + Y$.

Proposition. (Cinq paires de droites)

Soit $L \subseteq S$, S lisse. Il y a 5 plans Π_1, \dots, Π_5 contenant L tels que pour tout $i \in \llbracket 1, 5 \rrbracket$, $\Pi_i \cap S = L \cup L_i \cup L'_i$ donc il y a exactement dix droites, soit cinq paires de droites, dans S qui rencontrent L .

▷ On peut supposer $L = \{Z = T = 0\} \subseteq S$. L'équation de la surface se réécrit alors $G = A(Z, T)X^2 + B(Z, T)XY + C(Z, T)Y^2 + D(Z, T)X + E(Z, T)Y + F(Z, T) = 0$ où A, B, C sont de degré 1, D, E de degré 2 et F est de degré 3. L'équation d'un plan Π_α contenant L s'écrit $Z = \alpha T$, avec $\Pi_\infty : T = 0$. De plus, $A(\alpha T, T) = TA(\alpha, 1)$ et $D(\alpha T, T) = T^2 D(\alpha, 1)$, etc. Ainsi, les équations de $\Pi_\alpha \cap S$ s'écrivent $Z = \alpha T$ et $T(\overbrace{A(\alpha, 1)X^2 + B(\alpha, 1)XY + C(\alpha, 1)Y^2 + D(\alpha, 1)XT + E(\alpha, 1)YT + F(\alpha, 1)T^2}^{C_\alpha}) = 0$ avec donc $\Pi_\alpha = L \cup C_\alpha$ où la conique C_α est donnée ci-dessus.

Par un lemme déjà vu, C_α est dégénérée si et seulement $\Delta(\alpha, 1) = 4ACF + BDE - AE^2 - B^2E - CD^2 = 0$. Le polynôme $\Delta(Z, T)$ est homogène de degré 5. Il y a donc cinq plans, comptés avec multiplicité, tels que $\Pi \cap S$ égale trois droites. Si S est lisse, ces cinq plans sont de plus distincts.

Montrons que si $Z \mid \Delta(Z, T)$, alors $Z^2 \nmid \Delta(Z, T)$. D'après la remarque préliminaire, $G(X, Y, Z, T) = ZQ(X, Y, Z, T) + TXY$ dans le cas où $\Pi_{Z=0} \cap S$ est un triangle, ou $G = ZQ(X, Z, T) + TX(X + T)$ dans le cas où $\Pi_{Z=0} \cap S$ est trois droites concourantes.

Dans le premier cas, $B(Z, T) = T + bZ$. On voit que Z divise A, C, D, E, F ainsi que B . On écrit $F = Z(f_0 T^2 + f_1 ZT + f_2 Z^2)$. On obtient directement que modulo Z^2 , $\Delta(Z, T) = -B^2 F = -(T + bZ)^2 Z(f_0 T^2 + \dots) \equiv f_0 T^4 Z$. Montrons que $f_0 \neq 0$. Il n'y a aucun point singulier : pour $P = (0, 0, 0, 1)$, $G = ZQ + XYT$, $\overrightarrow{\text{grad}} G(P) = (0, 0, Q(0, 0, 0, 1), 0) \neq (0, 0, 0, 0)$, donc $Q(0, 0, 0, 1) \neq 0$ le coefficient de ZT^2 pour G , qui est $f_0 \neq 0$. On conclut donc.

L'autre cas se traite un peu différemment, mais pas trop. On a maintenant $G = ZQ(X, Y, Z, T) + TX(X + T)$. Alors Z divise B, C, E, F , et là $C(Z, T) = c_1 Z$, $D(Z, T) = T^2 + d_1 ZT + d_2 Z^2$. Ainsi

$\Delta(Z, T) \equiv -CD^2 \equiv c_1 ZT^4$ modulo Z^2 , et $c_1 \neq 0$ grâce à la lissité en $P = (0, 1, 0, 0)$ et $\overrightarrow{\text{grad}} G(P) = (0, c_1, 0, 0)$. ■

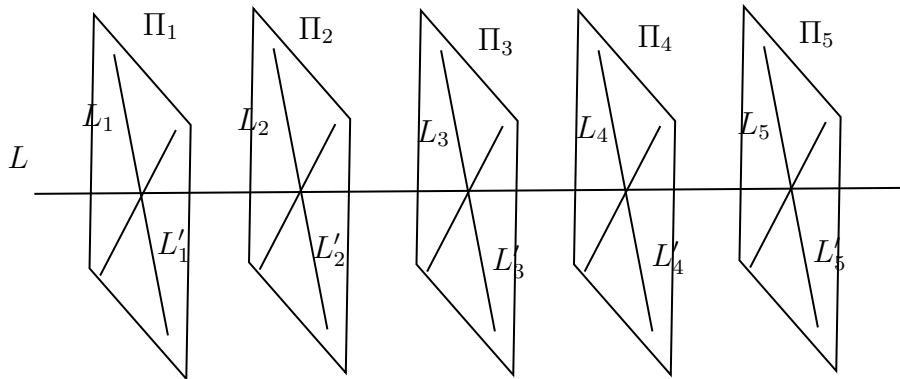


FIGURE 1.3.2 : Voici dix droites. —
C'est déjà ça.

Corollaire. (Existence de deux droites dans une surface cubique)

Une surface cubique lisse contient deux droites disjointes. On peut donc choisir L, M disjointes sur S .

Corollaire. (Configuration de 15 droites)

Il existe 15 droites contenues dans S et rencontrant L et M . De plus, la configuration est la suivante : on peut numérotter ces droites L_i, L'_i, L''_i pour $1 \leq i \leq 5$ de sorte que les droites L_i rencontrent L et M , les droites L'_i rencontrent seulement L et les droites L''_i rencontrent seulement M ; il y a des plans Π_i tels que $\Pi_i \cap V = L \cup L_i \cup L'_i$ ainsi que des plans $\Pi'_i \cap V = M \cup L_i \cup L''_i$; on a $L'_i \cap L''_i = \emptyset$ mais, si $i \neq j$, alors L'_i et L''_j se rencontrent, en un point.

▷ Un plan et une droite se rencontrent toujours. On a $\Pi_i \cap M = \text{un point}$ et l'on a vu que $L \cap M = \emptyset$, donc $M \cap L_i \neq \emptyset$ ou $M \cap L'_i \neq \emptyset$, et ces deux conditions s'excluent mutuellement. Quitte à échanger L_i et L'_i , on décide que $M \cap L_i \neq \emptyset$. Alors L_i rencontre L et M , soit $L'_i \cap (M \cup L''_i) = \emptyset$. $L'_i \cap L''_i = \emptyset$, mais $L'_i \cap L''_j = \text{un point}$. Si Π_i est un plan contenant L, L'_i, L_i , $\Pi_i \cap L''_j = \text{un point}$ et L''_j ne rencontre pas L , pas L_i , donc rencontre L'_i . ■

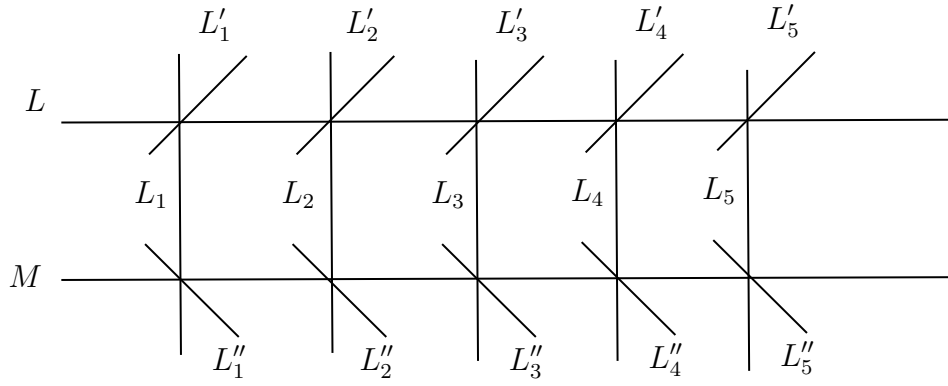


FIGURE 1.3.3 : *En voilà dix-sept autres.* —
Et le compte est bon.

Notons \mathcal{S} les 17 droites L, M, L_i, L'_i, L''_i et \mathcal{N} les autres droites.

Lemme. (*Lemme final*)

1. Soit $N \in \mathcal{N}$. Alors elle rencontre 3 des L_i .
2. Si $\{i, j, k\} \subseteq \{1, 2, 3, 4, 5\}$, il existe $N_{ijk} \in \mathcal{N}$ rencontrant L_i, L_j et L_k .

Preuve.

▷ \mathcal{N} est donc décrit par les parties à trois éléments de $\llbracket 1, 5 \rrbracket$. Ainsi, $\#\mathcal{N} = \binom{5}{3} = 10$. On a $17 + 10 = 27$, d'où le résultat. ■

Chapitre 2

Géométrie algébrique

Résumé

Historiquement, la géométrie algébrique a été introduite dans les complexes, pour des problèmes de calcul intégral (oui!). On se focalise ici sur l'étude des espaces affines, des espaces projectifs, et, plus généralement, des sous-ensembles algébriques de K^n où K est un corps, c'est-à-dire, des courbes (au sens intuitif du terme) définies par des équations, des surfaces, et leurs généralisations. L'aspect pratique devient alors clair. Cette introduction est sous-tendue par un pré-requis d'algèbre commutative à confirmer dans les exercices..

2.1 Variétés algébriques et variétés affines

Heuristique

La géométrie algébrique affine se ramène localement à l'algèbre commutative, de même que la géométrie différentielle se ramène localement à l'étude d'une boule euclidienne. Cela signifie aussi que la géométrie algébrique est plus difficile.

Dans toute la suite, k est un corps, que l'on supposera assez vite algébriquement clos¹, en particulier infini, et même parfait. Tous les anneaux sont supposés commutatifs, unitaires. On fixe un entier $n \in \mathbb{N}$.

Propriétés

L'anneau $K[X_1, \dots, X_n]$ est principal $\iff n = 1$. Même condition pour qu'il soit euclidien. Néanmoins, il est toujours factoriel.

¹ On verra plus tard comment, grâce à un peu de théorie de Galois, on se ramène au cas d'un tel corps. Expliquons brièvement l'idée : \mathbb{R} n'est pas algébriquement clos, et pour construire sa clôture, on a deux choix : $\mathbb{C} = \mathbb{R}(i)$ ou $\mathbb{R}(-i)$. Ce choix n'est pas canonique, et il en résulte que $\mathbb{Z}/2\mathbb{Z}$ agit sur \mathbb{C} (par conjugaison). La théorie de Galois émerge de cette action ; elle permet également de la maîtriser, au moyen de ses points fixes.

On conseille de s'intéresser d'ores et déjà aux considérations relatives à la LOCALISATION et au SPECTRE D'ANNEAU. Les notions de base de l'algèbre commutative sont supposées connues.

2.1.1 Polynômes, fonctions polynomiales

On conseille de relire la section sur les FONCTIONS POLYNOMIALES dans le cas des POLYNÔMES À PLUSIEURS VARIABLES.

Définition. (*Fonction polynomiale sur k^n*)

Une fonction $f : k^n \rightarrow k$ est *polynomiale* s'il existe $P \in k[X_1, \dots, X_n]$ telle que $f(x) = P(x)$ pour tout $x \in k^n$. On adopte la notation usuelle $x = (x_1, \dots, x_n)$ où $x_i \in k$ pour tout $i \in \llbracket 1, n \rrbracket$.

On note $\mathcal{O}(k^n)$ l'ensemble des fonctions polynomiales sur k^n .

On rappelle le théorème suivant :

Propriété. (*Théorème de transfert de Hilbert*)

$k[X_1, \dots, X_n]$ est noethérien. En particulier, $\mathcal{O}(k^n)$ est noethérien.

▷ En effet, on a un morphisme d'anneaux surjectif de $k[X_1, \dots, X_n] \longrightarrow \mathcal{O}(k^n)$, défini ci-dessous. ■

Définition-propriété. (*Morphisme évaluation en fonctions polynomiales*)

L'application $\text{EV} : k[X_1, \dots, X_n] \longrightarrow \mathcal{O}(k^n)$, dite *évaluation*, est un morphisme de k -algèbres.

$$P \longmapsto \text{EV}(P)$$

Fait. (*Morphisme évaluation sur un corps infini*)

Si k est infini, en particulier si k est algébriquement clos, alors k est un isomorphisme et l'on peut écrire $\mathcal{O}(k^n) \simeq k[X_1, \dots, X_n]$.

Exercice 1 (*Morphisme évaluation sur un corps fini*)

Redémontrer que, si k est un corps fini de cardinal q , $\text{Ker}(\text{EV}) = \langle X_i^q - X_i \rangle_{i \in \llbracket 1, n \rrbracket}$.

Propriété. (*Propriété universelle des fonctions polynomiales*)

Soit A une k -algèbre^a. Alors, il y a une bijection

$$A^n \xrightarrow{\sim} \text{Hom}_{k\text{-alg.}}(k[X_1, \dots, X_n], A)$$

donnée par $(a_1, \dots, a_n) \mapsto (P \mapsto P(a_1, \dots, a_n))$ et $(f(X_1), \dots, f(X_n)) \mapsto f$.

^a Dans ce cours, c'est un anneau A muni d'un morphisme $k \rightarrow A$.

Corollaire

On a une bijection

$$\underbrace{k^n}_{\text{« objets génériques } X \text{ »}} \xrightarrow{\sim} \text{Hom}_{k\text{-alg.}}\left(\underbrace{\mathcal{O}(k^n)}_{\text{« fonctions régulières sur } X \text{ »}}, k\right).$$

▷ On prend $A = k$. ■

2.1.2 Sous-ensembles algébriques

De même que dans le cas de la géométrie différentielle, on s'attache d'abord à définir la notion de variété plongée dans l'espace k^n avant de définir celle de variété abstraite.

→ *Notation.* On note $\mathbb{A}_k^n = \mathbb{A}^n(k) = \mathbb{A}^n := k^n$ l'espace affine de dimension n , qui est un k -espace vectoriel.

Définition. (*Sous-ensemble algébrique, variété algébrique*)

Un *sous-ensemble algébrique* de $\mathbb{A}^n(k)$ est un ensemble de la forme $V = \{x \in k^n \mid \forall i \in I \ P_i(x) = 0\}$ où $(P_i)_{i \in I} \in k[X_1, \dots, X_n]^I$, I un ensemble. On parle également de *variété algébrique*^a.

^a Convention non universelle. Dans ce cours, on réserve d'abord cette appellation aux sous-ensembles algébriques irréductibles, puis à une notion plus générale de variété algébrique abstraite, voir la section VARIÉTÉS ALGÈBRIQUES ABSTRAITES.

Fait

On observe immédiatement que si I est l'idéal engendré par les P_i , alors V est l'ensemble des zéros d'éléments de I .

Définition. (*Lieu d'annulation*)

À un idéal I de $K[X_1, \dots, X_n]$, on peut lui associer $\mathcal{V}(I) = \{x \in K^n \mid \forall P \in I \ P(x) = 0\}$ son *lieu commun d'annulation*

Définition. (Idéal annulateur)

Réciproquement, pour $S \subseteq K^n$, on peut lui associer $\mathcal{J}(S) = \mathcal{I}(S) = \{P \in K[X_1, \dots, X_n] \mid \forall x \in S \quad P(x) = 0\}$ son *idéal annulateur (multiple)*.

Ce n'est pas exagéré de dire que, par rapport à la géométrie différentiable, la géométrie algébrique n'étudie plus les ensembles définis par des fonctions différentiables, mais par des polynômes.

Notons tout de suite le fait suivant :

Propriété

Tout idéal de $K[X_1, \dots, X_n]$ est finiment engendré.

Heuristique

Prenons V l'ensemble des zéros de $P \in K[X_1, \dots, X_n]$ où $P = X_1^2 + \dots + X_n^2 + 1$. Si $K = \mathbb{R}$, on a $V = \emptyset$. Si P est irréductible, est-il vrai que si pour tout x tel que $P(x) = 0$, on a $Q(x) = 0$, alors P divise Q ? Cet exemple montre que non si le corps n'est pas supposé algébriquement clos; pour avoir une bonne correspondance entre idéaux et ensembles algébriques, il faudra faire cette hypothèse.

Propriété. (Décroissance du lieu d'annulation, de l'idéal annulateur)

1. Si $I_1 \subseteq I_2$, alors $\mathcal{V}(I_2) \subseteq \mathcal{V}(I_1)$.
2. Si $S_1 \subseteq S_2$, alors $\mathcal{J}(S_2) \subseteq \mathcal{J}(S_1)$.

Heuristique

On va chercher à résoudre les équations polynomiales ($y^2 = x$, par exemple) dans un corps quelconque.

Dans \mathbb{R} , l'équation $x^2 + y^2 = -1$ n'a pas de racines, autrement dit, l'ensemble de ses solutions est la courbe vide du plan. Mais il en est de même pour l'équation $x^2 + 3y^2 = -17$: autrement dit, la donnée de l'ensemble des solutions d'une équation polynomiale perd l'information sur l'équation.

Nous allons voir que ce fait ne provient que de ce que k n'est pas algébriquement clos, et que, si $k = \bar{k}$, on peut à bonne approximation près retrouver le système d'équation définitionnel d'un ensemble (« algébrique ») de points du plan.

Définition. (Lieu d'annulation)

Soit $F \subseteq \mathcal{O}(k^n)$. On note $\mathcal{V}_F = \mathcal{V}(F) := \{x = (x_1, \dots, x_n) \in k^n \mid \forall f \in F \quad f(x) = 0\}$ le *lieu des zéros communs à tous les éléments de f* , ou encore *lieu d'annulation* de F .

Exemples. (*Lieux d'annulation*)

1. Si $f \neq 0$ est dans $\mathcal{O}(k^n)$, alors $\mathcal{V}_{\langle f \rangle}$ est une *hypersurface*.
2. Si $x = (x_1, \dots, x_n) \in k^n$, alors $\{x\} = \mathcal{V}_{M_x}$ où $M_x = \langle X_1 - x_1, \dots, X_n - x_n \rangle$. En prenant la notation $\text{ev}_x: \mathcal{O}(k^n) \longrightarrow k$, alors $M_x = \text{Ker}(\text{ev}_x)$.

$$P \longmapsto P(x) = P(x_1, \dots, x_n)$$
3. (*On précise la remarque précédente.*) Si $n = 1$, alors $\mathcal{V}_{\langle X_1 \rangle} = 0 = \mathcal{V}_{\langle X_1^2 \rangle}$, or $\langle X_1 \rangle \neq \langle X_1^2 \rangle$, donc on ne peut jamais récupérer l'idéal I en fonction de \mathcal{V}_I . Mais, presque.

Propriété. (*Clôture du lieu d'annulation par l'idéal engendré*)

Soit $F \subseteq \mathcal{O}(k^n)$. Alors $\mathcal{V}_F = \mathcal{V}_{\langle F \rangle}$.

Définition. (*Idéal annulateur*)

Si $X \subseteq k^n$, $I(X) \subseteq \mathcal{O}(k^n)$ est $\{f \in \mathcal{O}(k^n) \mid f(x) = 0 \quad \forall x \in X\}$.

Propriété. (*Décroissance du lieu d'annulation, de l'idéal annulateur*)

Soient $I_1, I_2 \subseteq \mathcal{O}(k^n)$ (ou les idéaux qu'ils engendrent) et $S_1, S_2 \subseteq k^n$ (ou des ensembles algébriques).

1. Si $I_1 \subseteq I_2$, alors $\mathcal{V}(I_2) \subseteq \mathcal{V}(I_1)$.
2. Si $S_1 \subseteq S_2$, alors $\mathcal{I}(S_2) \subseteq \mathcal{I}(S_1)$.

Définition. (*Ensemble algébrique*)

Soit $F \subseteq k^n$. Tout ensemble de la forme \mathcal{V}_F est appelé *ensemble algébrique*.

Exemples. (*Ensembles algébriques*)

1. La réunion des n axes de coordonnées de $\mathbb{A}^n(k)$ est un ensemble algébrique.

Rappels variés. (*Radical d'un idéal*)

1. Par définition, $\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} \quad a^n \in I\}$.
2. Le radical est croissant.
3. Le radical est un opérateur de clôture. On dit qu'un idéal I est *réduit* ou *radiciel* si $\sqrt{I} = I$.
4. Un idéal I est radiciel si et seulement si A/I n'a pas d'éléments nilpotents non nul (*i.e.* il est *réduit*).
5. Tout idéal premier est réduit.

Remarque. Pour toute variété V , $\mathcal{I}(V)$ est radical. On en déduit que l'application $Z \mapsto \mathcal{I}(Z)$ de l'ensemble des parties de \mathbb{A}^n dans l'ensemble des idéaux de $\mathcal{O}(k^n) \cong K[X_1, \dots, X_n]$ n'est pas surjective. De plus, $\boxed{\mathcal{V}(I) = \mathcal{V}(\sqrt{I})}$, donc $I \subseteq \sqrt{I} \subseteq \mathcal{J}(\mathcal{V}(I))$. Depuis ce constat, on s'intéresse à :

On reprend les notations des prolégomènes. On fixe toujours un corps K et un entier naturel n . On rappelle que $\mathcal{V}(I)$ désigne le lieu d'annulation commun de l'idéal I , et $\mathcal{J}(S)$ désigne l'idéal annulateur de la partie S .

Proposition. (Topologie de Zariski)

L'ensemble des zéros commun à une famille donnée de polynômes, définit de façon duale une topologie sur $K^n = \mathbb{A}^n(K)$, explicitement donnés par $\{\mathcal{V}(I), I \text{ idéal de } K[X_1, \dots, X_n]\}$. Ainsi, les sous-ensembles algébriques sont les fermés d'une topologie (dite *de Zariski*).

$$\triangleright \text{ On a } \mathcal{V}(K[X_1, \dots, X_n]) = \emptyset \text{ et } \mathcal{V}(\{0\}) = K^n, \bigcap_{j \in J} \mathcal{V}(I_j) = \mathcal{V}(\sum_{j \in J} I_j), \text{ et } \mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2),$$

d'où le résultat. ■

On retiendra :

Proposition. (Lien fondamental entre l'algèbre et la géométrie)

Pour tous idéaux $I, J, (I_j)_{j \in J}$, pour tous ensembles algébriques $V, W, (V_i)_{i \in I}$,

1. $\mathcal{V}(IJ) = \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$ mais ceci ne s'étend pas à une famille infinie d'idéaux.
2. $\mathcal{V}(\sum_{j \in J} I_j) = \bigcap_{j \in J} \mathcal{V}(I_j)$.
3. $V \subseteq W \iff I(W) \subseteq I(V)$.
4. $V = W \iff I(V) = I(W)$.



Dans \mathbb{A}^2 , $V(X, Y) = V(X) \cap V(Y) = \mathbb{A}^2 \setminus \{0\} \neq V(XY) = V(X) \cup V(Y) =$ la réunion des deux axes !

Pour compléter ces formules, il faut aller plus avant.

Proposition. (Opérateurs de Zariski)

1. $S \subseteq \mathcal{V}(\mathcal{J}(S))$, avec égalité, si et seulement si, S est un sous-ensemble algébrique. Autrement dit, $\mathcal{V}(\mathcal{J}(S)) = \overline{S}$ l'adhérence de S pour la topologie de Zariski.
2. $I \subseteq \mathcal{J}(\mathcal{V}(I))$ mais il n'y a pas égalité en général. (On va voir que $\mathcal{J}(\mathcal{V}(I)) = \sqrt{I}$).

\triangleright Les inclusions proposées sont tautologiques. Soit S un sous-ensemble algébrique, soit $S = \mathcal{V}(I)$ pour un certain idéal I de $K[X_1, \dots, X_n]$. Or $I \subseteq \mathcal{J}(\mathcal{V}(I))$, soit ici $I \subseteq \mathcal{J}(S)$. En passant au \mathcal{V} , on obtient $\mathcal{V}(\mathcal{J}(S)) \subseteq \mathcal{V}(I) = S$, ce qu'il fallait encore vérifier. ■

Il y a deux obstacles à cette égalité, qui justifient à terme l'intervention du Nullstellensatz.

Contre-exemple

$P = 0$ et $P^2 = 0$ définissent le même sous-ensemble algébrique, donc l'égalité ne peut avoir lieu ci-haut, car a priori ils n'engendrent pas le même idéal ; prendre $P = X$. \square

Contre-exemple

Si K n'est pas algébriquement clos, si $P \in K[X]$ et non constant et sans zéros, $I = PK[X] \subsetneq \mathcal{J}(\mathcal{V}(I))$, car $\mathcal{V}(I) = \emptyset$ donc $\mathcal{J}(\mathcal{V}(I)) = K[X]$ et par hypothèse ce n'est pas I ! On n'a pas de correspondance. \square

Si le corps est algébriquement clos, ce deuxième obstacle disparaît. Pour éliminer le premier qui demeure, on utilise la notion de radical d'un idéal.

Rappels variés. (*Radical d'un idéal*)

1. Par définition, $\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} \quad a^n \in I\}$.
2. Le radical est croissant.
3. Le radical est un opérateur de clôture. On dit qu'un idéal I est *réduit* ou *radiciel* si $\sqrt{I} = I$.
4. Un idéal I est réduit si et seulement si A/I n'a pas d'éléments nilpotents non nul.
5. Tout idéal premier est réduit.

Remarque. Pour toute variété V , $\mathcal{I}(V)$ est radiciel. On en déduit que l'application $Z \mapsto \mathcal{I}(Z)$ de l'ensemble des parties de \mathbb{A}^n dans l'ensemble des idéaux de $K[X_1, \dots, X_n]$ n'est pas surjective. De plus, $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$, donc $I \subseteq \sqrt{I} \subseteq \mathcal{J}(\mathcal{V}(I))$. Depuis ce constat, on s'intéresse à :

2.1.3 La correspondance entre idéaux et variétés : le théorème du Nullstellensatz de Hilbert

Théorème. (*Théorème des zéros de Hilbert, Nullstellensatz*)

On suppose K algébriquement clos.

1. (*Première forme*) $\sqrt{I} = \mathcal{J}(\mathcal{V}(I))$.
2. (*Deuxième forme*) On a une correspondance biunivoque entre les sous-ensembles algébriques de K^n et les idéaux réduits de $K[X_1, \dots, X_n]$ qui à un ensemble algébrique $S \mapsto \mathcal{J}(S)$ et de réciproque qui à $I \mapsto \mathcal{V}(I)$. En particulier, on peut identifier les deux.
3. (*Troisième forme*) (Un peu pompeusement, car c'est la réécriture de la première forme.) Pour $I = (P_1, \dots, P_r)$, $Q \in K[X_1, \dots, X_n]$, si $(P_1(x) = \dots = P_r(x) = 0 \implies Q(x) = 0)$ $\implies Q \in I$.

$Q(x) = 0$), alors il existe $M \geq 1$, $A_1, \dots, A_r \in K[X_1, \dots, X_n]$ avec $Q^M = \sum_{i=1}^r A_i P_i$.
 (Supplément) si $K_0 \subseteq K$ et les coefficients de P, Q sont dans K_0 , alors on peut choisir $A_i \in K_0[X_1, \dots, X_n]$.

Pour démontrer le théorème, nous allons nous intéresser à la proposition-clef suivante :

Proposition. (*Proposition-clef du théorème des zéros de Hilbert*)

Soit $L = K[t_1, \dots, t_n]$ une K -algèbre de type fini sur K . Si L est un corps, c'est une extension algébrique de K .

▷ (*Cas indénombrable*) Si le corps K est non dénombrable, par exemple $K = \mathbb{R}$ ou \mathbb{C} , on peut fournir une preuve simple de cette proposition. Supposons qu'il existe $x \in L$ transcendant sur K . Alors $K(x) \simeq K(x) \subseteq L$. Or L possède une partie génératrice dénombrable donnée par les monômes en t_1, \dots, t_n en tant que K -espace vectoriel ; seulement, $\{\frac{1}{x-a}, a \in K\}$ est une partie libre, problème, car le cardinal des familles libres ne peut excéder celui d'une famille génératrice. ■

▷ (*Cas général*) Pour le montrer, on aura besoin du résultat suivant :

Lemme. (*Lemme de normalisation de Noether*)

Soit $L = K[x_1, \dots, x_n]$ une algèbre de type fini. Il existe $y_1, \dots, y_r \in L$ algébriquement indépendants sur K tels que $L/K[y_1, \dots, y_r]$ soit entière (algébrique).

▷ Dans le cas où K est infini, soit x_1, \dots, x_r une famille algébriquement indépendante maximale. Tout élément de L est algébrique sur $K[x_1, \dots, x_r]$. Montrons qu'en remplaçant x_1, \dots, x_r par $y_i - a_i x_{r+1}$, l'élément x_{r+1} est entier sur $K[y_1, \dots, y_r]$. Par récurrence, cela suffit. Si $r = 0$, c'est immédiat ; de même, si $r = n$. Autrement $K[x_1, \dots, x_r] \subseteq K[x_1, \dots, x_{n-1}] \subseteq K[x_1, \dots, x_n]$ et l'on conclut par tour d'extensions entières.

Montrons donc cela. On a que x_{n+1} est algébrique sur $K(x_1, \dots, x_r)$, donc en prenant la décomposition homogène $F_d(x_1, \dots, x_{n+1}) + F_{d-1}(x_1, \dots, x_{n+1}) + \dots + F_1 = 0$. Alors $x_i = y_i + a_i x_{r+1}$ pour $1 \leq i \leq r$ et $a_i \in K$, $F_d \neq 0$. Par suite, $F_d(a_1, \dots, a_r, 1)x_{r+1}^d +$ termes de degré $\leq d-1$ en $x_{n+1} = 0$. Comme le corps est infini, il existe $a_1, \dots, a_r \in K$, $F_d(a_1, \dots, a_r, 1) \neq 0$. Donc x_{n+1} est un entier algébrique sur $K[y_1, \dots, y_r]$.

Dans le cas général, on fait le changement de variables $y_i = x_i - x_{r+1}^{k_{r+1}+1-i}$ pour k suffisamment grand. ■

On peut donc terminer la preuve de la proposition-clef :

Posons $L = K[x_1, \dots, x_n]$ un corps. Alors par le lemme, L est entier sur $K[y_1, \dots, y_r]$ où les y_i sont algébriquement indépendants. Par une propriété classique de théorie des nombres, $K[y_1, \dots, y_r]$ est un corps. Donc $r = 0$. Donc L/K est de degré de transcendance nul, donc L/K est algébrique. ■

Nous montrons que cette proposition-clef entraîne le Nullstellensatz (noté *NSS*). D'abord, elle entraîne une version faible du théorème :

Théorème. (*Théorème du Nullstellensatz faible*)

On suppose K algébriquement clos. Si l'idéal $I \subsetneq K[X_1, \dots, X_n]$, alors $\mathcal{V}(I) \neq \emptyset$.

▷ D'après le théorème de Krull, il existe $I \subseteq \mathfrak{M} \subsetneq K[X_1, \dots, X_n]$ où \mathfrak{M} est un idéal maximal. Introduisons $L = K[X_1, \dots, X_n]/\mathfrak{M}$. C'est un corps. Posons $x_i = X_i \bmod \mathfrak{M}$; on a $L = K[x_1, \dots, x_n]$. Par la proposition-clef, L/K est algébriquement, donc $L = K$, car K est algébriquement clos, donc $x_i \in K$ et pour tout $P \in \mathfrak{M}$, $P(x_1, \dots, x_n) = P(X_1 \bmod \mathfrak{M}, \dots, X_n \bmod \mathfrak{M}) = P(X_1, \dots, X_n) \bmod \mathfrak{M} = 0$. Ainsi $(x_1, \dots, x_n) \in \mathcal{V}(\mathfrak{M}) \subseteq \mathcal{V}(I)$, d'où $\mathfrak{M} = (X_1 - x_1, \dots, X_n - x_n)$. En effet : notons $\mathfrak{M}' = (X_1 - x_1, \dots, X_n - x_n)$. Si $P(x_1, \dots, x_n) = 0$, alors $P \in \mathfrak{M}'$. En effet, il suffit de diviser euclidiennement dans $K[X_1, \dots, X_{n-1}][X_n]$ où $\deg_{X_n} R < \deg(X_n - a_n) = 1$, donc $\deg_{X_n}(R) = 0$. Par induction, on peut écrire $P(X) = \sum Q_i(X_i - a_i)$. Réciproquement, si $P \in \mathfrak{M}$, alors on écrit que $P(x_1, \dots, x_n) = 0$ et la double inclusion est démontrée. ■

Remarque. Cette étape de la preuve fournit encore un supplément, encadré ci-dessus.

Nous pouvons conclure la preuve du théorème du Nullstellensatz général.

Preuve.

▷ On se place dans $K[X_1, \dots, X_n, T]$. Alors $P_1(X), \dots, P_r(X), 1 - TQ(X)$ n'ont aucun zéro commun. En effet, si $P_1(x) = \dots = P_r(x) = 0$, alors $1 - tQ(x) = 1 \neq 0$. D'après le théorème faible, l'idéal engendré par $P_1, \dots, P_r, 1 - TQ$ est égal à $K[X_1, \dots, X_n, T]$, c'est-à-dire qu'il existe $A_i(X, T) \in K[X_1, \dots, X_n, T]$ tels que $1 = A_1(X, T)P_1(X) + \dots + A_r(X, T)P_r(X) + B(X, T)(1 - TQ(X))$. Or $K[X_1, \dots, X_n, T] \subseteq K(X_1, \dots, X_n)[T]$. On pose $T = 1/Q(X)$. Ainsi $1 = \sum_{i=1}^r A_i(X, \frac{1}{Q(X)})P_i(X)$ dans $K(X_1, \dots, X_n)$. Posons $M = \max(\deg_T(A_i(X, T)))$, d'où $Q^M = \sum_{i=1}^r Q^M A_i(X, \frac{1}{Q})P_i(X)$ à coefficients dans $K[X_1, \dots, X_n]$, et le théorème est démontré. ■

Remarque. Toutes les preuves proposées requièrent l'axiome du choix. On pourrait s'en passer en convoquant la noéthérianité de l'anneau $K[X_1, \dots, X_n]$ dans la preuve complète.

Quelques conséquences du Nullstellensatz :

Corollaire. (*Existence d'un point d'annulation*)

Supposons K algébriquement clos. Tout idéal strict I de $K[X_1, \dots, X_n]$ a un lieu d'annulation $\mathcal{V}(I)$ non vide, autrement dit, il existe un point de K^n racine de tous les éléments de I à la fois (fou!). Merci la structure d'idéal qui fait le boulot toute seule dans $K[X_1, \dots, X_n]$.

Corollaire. (Théorème de d'Alembert-Gauss)

Tout polynôme de $\mathbb{C}[X]$ de degré ≥ 1 admet au moins une racine.

Corollaire. (Finitude de la génération des idéaux de $K[X_1, \dots, X_n]$)

Supposons K algébriquement clos. Tout idéal maximal de $K[X_1, \dots, X_n]$ est de type fini engendré par n éléments. Explicitement, $\mathfrak{M} = \langle f_1, \dots, f_r \rangle$ où $r = n$ et $f_i = X_i - x_i$ pour un certain $x \in V(\mathfrak{M})$.



Ne surtout pas dire que tout idéal de $K[X_1, \dots, X_n]$ est engendré par $\leq n$ polynômes ! Tout idéal de $K[X_1, \dots, X_n]$ est engendré par un nombre fini de polynômes, et tout idéal maximal J est engendré par n polynômes (et d'ailleurs pas par moins). Mais $K[X_1, \dots, X_n]$ n'étant pas principal pour $n \geq 2$, on ne peut pas faire mieux : que dire de (X^2, XY, Y^2) dans $\mathbb{C}[X, Y]$?

Corollaire. (Description du spectre maximal)

Supposons K algébriquement clos. Le spectre maximal de $K[X_1, \dots, X_n]$ est en bijection avec K^n .

Corollaire. (Description du radical d'un idéal dans une algèbre)

Supposons K algébriquement clos. Soit I un idéal d'une algèbre de type fini A sur K . Alors \sqrt{I} est l'intersection des idéaux maximaux de A contenant I .

Théorème

Soit k un corps quelconque. Soit $M \subseteq k[X_1, \dots, X_n]$ un idéal maximal. Alors $k[X_1, \dots, X_n]/M$ est une extension finie de k .

Théorème

Soit k un corps quelconque. Soit K une extension de corps de k , telle que K est une k -algèbre de type fini (beaucoup moins fort que (de dimension finie!)), alors K/k est finie.

Ces deux énoncés sont en fait équivalents¹ à la forme suivante :

Théorème

Pour $k = \mathbb{C}$, soit $M \subseteq \mathbb{C}[X_1, \dots, X_n]$ idéal maximal. Alors M est de corps résiduel \mathbb{C} . Autrement dit, $M = \langle X_1 - x_1, \dots, X_n - x_n \rangle$ avec $(x_1, \dots, x_n) \in \mathbb{C}^n$. Ainsi les idéaux maximaux de $\mathcal{O}(\mathbb{C}^n)$ sont en bijection avec \mathbb{C}^n .

¹ Et oui : si $k = \bar{k}$, et K/k est une extension de corps de type fini, alors $K = k$

Fait

$k(X)$ n'est pas une k -algèbre de type fini. Supposons $k(X) = k[f_1, \dots, f_n]$. Alors $\frac{1}{Q+1} \notin k[X, \frac{1}{Q}]$ où $f_i \in k(X)$ où $f_i = \frac{p_i}{Q}$, Q dénominateur commun non constant.

Comme on l'a vue, la preuve classique repose sur des moyens issus de l'algèbre commutative. On peut donner une preuve plus élémentaire.

Théorème. (Théorème des zéros)

Soit k un corps et K/k une extension de corps de type fini, i.e. $K = k[X_1, \dots, X_n]$. Alors $\dim_k(K) < \infty$.

Autrement dit, une k -algèbre de type fini qui est un corps est de dimension finie sur k en tant qu'espace vectoriel.

Si k est algébriquement clos, on a donc $K = k$.

▷ On raisonne par récurrence sur n . Si $K = k[x_1]$, si x_1 est algébrique, alors c'est gagné, et sinon, $k[X] = k(x)$, absurde.

On écrit $K = k(x_1)[x_2, \dots, x_n]$ et l'on note $l = k(x_1)$. En appliquant le théorème à l par hypothèse de récurrence, on obtient $\dim_l(K) < \infty$. Soit $(\beta_1 = 1, \dots, \beta_r)$ base de K sur l . On peut écrire $\beta_i \beta_j = \sum_{k=1}^r a_{i,j,k} \beta_k$ où les constantes de structure $a_{i,j,k} \in l$. De même $K \ni x_i = \sum_{k=1}^r b_{i,k} \beta_k$. Posons $A = k[a_{i,j,k}, b_{i,k}]$. C'est en particulier une k -algèbre de type fini. On a $k \subseteq A \subseteq l$. De plus, $K = l\beta_1 \oplus l\beta_2 \oplus \dots \oplus l\beta_r$. On définit $M := A\beta_1 \oplus A\beta_2 \oplus \dots \oplus A\beta_r$ le A -module engendré par β_1, \dots, β_r , avec $M \subseteq K$ par inclusion de tous les facteurs. Or M contient tous les x_i , et c'est un sous-anneau de K , donc $M = K$, donc $A = l$. Donc $k(x_1) = l$ est une k -algèbre de type fini. Or $k(X)$ n'est pas de type fini sur k . Donc x_i est algébrique sur k , donc $[K : k] = [K : l][l : k] < \infty$. ■

Corollaire. (Utile en géométrie algébrique)

Soit $\varphi : A \rightarrow A'$ un morphisme entre k -algèbres de type fini. Soit $\mathcal{M}' \subseteq A'$ un idéal maximal. Alors $\varphi^{-1}(\mathcal{M}') \subseteq A$ est maximal.

▷ On peut factoriser :

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ \downarrow \pi & & \downarrow \pi' \\ A/\mathcal{M} & \xrightarrow{\tilde{\varphi}} & A'/\mathcal{M}' \end{array}$$

de sorte que $\tilde{\varphi}$ est injectif et A'/\mathcal{M}' est une extension algébrique finie de k . Par le théorème des zéros, $\dim_k(A/\mathcal{M}) < \infty$. Donc $\mathcal{M} \subseteq A$ est un idéal premier, donc A/\mathcal{M} est une k -algèbre intègre de dimension finie sur k . Ainsi, par une propriété d'algèbre linéaire, A/\mathcal{M} est un corps, donc \mathcal{M} est maximal. ■

Heuristique

On verra que ce théorème assure que l'image d'un point fermé est un point fermé, autrement dit que les morphismes en géométrie algébrique font ce que l'on attend d'eux.

Propriété. (Radical d'un idéal dans une algèbre de TF)

Soit A une k -algèbre de type fini et I un idéal de A . Alors $\sqrt{I} = \bigcap_{I \subseteq \mathcal{M} \text{ maximal}} \mathcal{M}$.

▷ On se ramène à $I = 0$ en réduisant l'anneau, car alors la propriété se reformule ainsi : dans A/I , le nilradical $\sqrt{0} = \bigcap_{\mathcal{M}' \text{ maximal}} \mathcal{M}' := \mathcal{J}$. Clairement, $\sqrt{0} \subseteq \mathcal{J}$. Soit $f \in A$ non nilpotent. Alors le localisé A_f est non nul et A_f est une k -algèbre de type fini. Soit $\mathcal{M}' \subseteq A$ un idéal maximal (construit ici sans l'axiome du choix). Soit φ le plongement de A dans A_f . Appliquons le corollaire précédent : $\mathcal{M} = \varphi^{-1}(\mathcal{M}') \subseteq A$ est un idéal maximal. Alors $f \notin \mathcal{M}$. ■

Corollaire. (Théorème des zéros de Hilbert fort)

Soient $I, I' \subseteq \mathcal{O}(k^n)$ deux idéaux. On suppose $k = \bar{k}$. Alors

$$V_i = V_{I'} \iff \sqrt{I} = \sqrt{I'}.$$

▷ Le sens réciproque est clair. D'autre part, on a $\sqrt{I} = \bigcap_{I \subseteq \mathcal{M} \text{ maximal}} \mathcal{M}$. Par le théorème des zéros et le fait que k soit algébriquement clos, les idéaux maximaux de $\mathcal{O}(k^n)$ sont les $\langle X - x_1, \dots, X - x_n \rangle$ pour $(x_1, \dots, x_n) = k^n$. Ainsi, les $x \in V_i$ correspondent aux \mathcal{M} maximaux contenant I . ■

Remarque. (Base de Gröbner) On suppose k algébriquement clos. Si $f_1, \dots, f_r \in k[X_1, \dots, X_n]$. Alors $V_{\langle f_1, \dots, f_r \rangle} = \emptyset \iff \exists g_1, \dots, g_r \in k[x_1, \dots, x_n] \quad 1 = g_1 f_1 + \dots + g_r f_r$.

Exercice 2 (Nullstellensatz version entière)

Soit $\mathcal{M} \subseteq \mathbb{Z}[X_1, \dots, X_n]$ un idéal maximal. Montrer que $\mathbb{Z}[X_1, \dots, X_n]/\mathcal{M}$ est un corps fini.

▷ On note $L = \mathbb{Z}[X_1, \dots, X_n]/\mathcal{M}$ et K son sous-corps premier. L'extension L/K est de type finie, donc finie par le Nullstellensatz. Si K est un corps fini, c'est donc terminé. Il s'agit d'éliminer le cas $K = \mathbb{Q}$. Heuristiquement, c'est impossible, car « on ne peut pas inverser tous les entiers avec un nombre fini de relations ». Soit $x \in L$. Si $x \in \mathbb{Q}$, alors $x = \frac{a}{b}$. Si $x \notin \mathbb{Q}$, alors $a_n x \in \mathcal{O}_L$ où a_n est le dominant d'une relation d'intégralité sur x . Soient x_1, \dots, x_n des générateurs de L comme \mathbb{Z} -algèbre. Alors $x_i = \frac{z_i}{N_i}$ pour tout i et en prenant $N = N_1 \dots N_n$ de sorte que $x_1, \dots, x_n \in \mathcal{O}_L[\frac{1}{N}]$ d'où $L = \mathbb{Z}[x_1, \dots, x_n] = \mathcal{O}_L[\frac{1}{N}]$. Soit p ne divisant pas N . L'inverse de p est dans $\mathbb{Q}_d \text{ dans } L = \mathbb{Q}[\frac{1}{N}]$, d'où $N^{\frac{1}{p}} \in \mathcal{O}_L \cap \mathbb{Q}$. Par clôture intégrale, $N^{\frac{1}{p}} \in \mathbb{Z}$, absurde. ■

Remarque. En formalisant un peu, on peut adapter la preuve du Nullstellensatz au cas de \mathbb{Z} , mais ce n'est pas dur.

Remarque. Soit A un anneau de Jacobson, i.e. un anneau « ayant beaucoup d'idéaux premiers », i.e. tout idéal premier est l'intersection des idéaux maximaux le contenant. En particulier l'ensemble de ses idéaux maximaux est dense dans l'ensemble des idéaux premiers pour la topologie de Zariski. Le théorème des zéros s'étend au cas d'un tel A à la place de k .

Exercice 3 (Théorème d'Ax)

On souhaite montrer le théorème suivant : soit $f \in \mathbb{C}^n \rightarrow \mathbb{C}^n$ polynomiale injective, alors f est surjective. L'énoncé fonctionne en remplaçant \mathbb{C} par un corps algébriquement clos de caractéristique nulle.

1. Si l'on remplace par une fonction de $f \in \mathbb{C}^n \rightarrow \mathbb{C}^m$, donner des contre-exemples pour $n \neq m$.
2. Montrer le théorème pour des corps finis.
3. En utilisant le théorème des zéros de Hilbert, en déduire le théorème pour \mathbb{C} .

Propriété

Si le TH0 s'applique, alors l'intersection des idéaux maximaux est nulle.

2.1.4 Fonctions régulières

Définition. (Restriction)

Soit $V \subseteq k^n$ un ensemble algébrique. On a un morphisme *restriction* $\text{res} : \mathcal{O}(k^n) \rightarrow \{\text{fonctions } V \rightarrow k\} = k^V$.

Définition. (Fonction régulière, polynomiale sur un ensemble algébrique)

On note $\mathcal{O}(V) = \text{Im}(\text{res})$. Une fonction $f \in \mathcal{O}(V)$ s'appelle *fonction régulière* ou *polynomiale sur V* .

Remarque importante. Donc $\mathcal{O}(V) = \mathcal{O}(k^n)/\text{Ker}(\text{res})$ où $\text{Ker}(\text{res}) = \mathcal{I}(V)$, d'où $\mathcal{O}(V) = \mathcal{O}(k^n)/\mathcal{I}(V)$

Proposition. (Opérateurs de Zariski)

1. $S \subseteq \mathcal{V}(\mathcal{I}(S))$, avec égalité, si et seulement si, S est un sous-ensemble algébrique. Autrement dit, $\mathcal{V}(\mathcal{I}(S)) = \overline{S}$ l'adhérence de S pour la topologie de Zariski.
2. $I \subseteq \mathcal{I}(\mathcal{V}(I))$ mais il n'y a pas égalité en général. (On va voir que $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$).

Corollaire

On a une bijection bien définie :

$$V \longleftrightarrow \text{Hom}_{k\text{-alg.}}(\mathcal{O}(V), k)$$

donnée par $v \mapsto (f \mapsto f(v))$ et $(\varphi(\overline{X_1}), \dots, \varphi(\overline{X_n})) \mapsto (\varphi : \mathcal{O}(V) \rightarrow k)$. On en déduit une bijection :

$$V \longleftrightarrow \{\text{idéaux maximaux } M \subseteq \mathcal{O}(V) \text{ de corps résiduel } k, \text{ i.e. tels que } \mathcal{O}(V)/M = k\}.$$

▷ Pour la deuxième, on a en effet $k \hookrightarrow \mathcal{O}(V) \rightarrow \mathcal{O}(V)/M \simeq k$. En effet, l'ensemble des idéaux maximaux M dans $\mathcal{O}(V)$ de corps résiduel k est $\text{Hom}_{k\text{-alg.}}(\mathcal{O}(V), k)$. ■

Exemple

On prend $k = \mathbb{R}$, $n = 1$. L'ensemble des idéaux maximaux de $\mathbb{R}[X]$, autrement dit le spectre maximal de $\mathbb{R}[X]$, est $\underbrace{\{X - a, a \in \mathbb{R}\}}_{\text{de corps résiduel } \mathbb{R}} \amalg \underbrace{\{X^2 + aX + b \mid b^2 - 4ac < c\}}_{\text{de corps résiduel } \mathbb{C}}$.

Remarque. Si $m_x = (X_1 - x_1, \dots, X_n - x_n) \subseteq \mathcal{O}(k^n)$ qui se restreint à $\mathcal{O}(V) = \mathcal{O}(k^n)/I(V)$, pour $x \in V$, alors $m_x \supseteq I(V)$.

2.1.5 Topologie de Zariski

On rappelle que les fermés de Zariski sont exactement les sous-ensembles algébriques.

Définition. (Sous-ensemble algébrique irréductible, variété algébrique affine)

Soit V un sous-ensemble algébrique de \mathbb{A}^n . Il est dit *irréductible* si pour tous V_1, V_2 fermés de Zariski, $V = V_1 \cup V_2 \implies V = V_1$ ou $V = V_2$.

En présence d'un sous-ensemble algébrique irréductible, on parle également de *variété algébrique (affine)* de K^n .

Théorème

Les variétés affines sont en correspondance bijective avec les idéaux premiers de $K[X_1, \dots, X_n]$.

En particulier, tout idéal maximal de $K[X_1, \dots, X_n]$ définit une variété.

▷ C'est le théorème du Nullstellensatz et la définition de primalité, qui correspond à celle d'irréductibilité des sous-ensembles algébriques. ■

Proposition

Tout sous-ensemble algébrique s'écrit comme réunion finie de sous-ensembles algébriques irréductibles.

▷ Comme on a une correspondance entre idéaux réduits et sous-ensembles algébriques, et que toute suite d'idéaux est stationnaire, car tout $K[X_1, \dots, X_n]$ est noethérien, toute suite décroissante de sous-ensembles algébriques est stationnaire. Ainsi, à partir de tout fermé de Zariski $V \subseteq \mathbb{A}^n$, ou bien V est irréductible, ou bien l'une de ses parties strictes est un fermé de Zariski. En recommençant, on obtient une suite décroissante de fermés qui est donc stationnaire. Plus fortement, on obtient même un arbre de décompositions de V qui ne peut contenir de branches infinies. Cette construction donne $V = W_1 \cup \dots \cup W_r$ avec les W_i irréductibles qui sont les racines de cet arbre. ■

Remarque importante. Si on impose que pour tout $i \neq j$, $W_i \not\subseteq W_j$ et $W_j \not\subseteq W_i$, la décomposition est unique, et l'on appelle les W_i les *composantes irréductibles* de V .

Exemples. (*Composantes irréductibles*)

1. Le lieu d'annulation d'un polynôme réductible ne peut être un sous-ensemble algébrique irréductible. En particulier, un point isolé dans \mathbb{R}^n muni de la topologie usuelle disjointement réuni à une variété, constitue une variété mais non irréductible. La réciproque est vraie.
2. Soit $V = \{(x, y) \in \mathbb{A}^2 \mid xy = 0\}$. Alors $V = \{(x, y) \in \mathbb{A}^2 \mid x = 0\} \sqcup \{(x, y) \in \mathbb{A}^2 \mid y = 0\}$. C'est la réunion de deux droites orthogonales.
3. Soit $S = \{(x, y, z, t) \in \mathbb{A}^4 \mid xt - yz = y^2 - xz = 0\}$. On note $D = \{x = y = 0\}$ et $C_1 = \{xt - yz = y^2 - xz = yt - z^2 = 0\}$ qui sont les composantes irréductibles de S . (On peut le vérifier par le calcul.)
4. Un point est toujours un ensemble irréductible.

Proposition. (*Densité des ouverts de Zariski*)

Soit K algébriquement clos. Tout ouvert de Zariski non vide est dense dans $\mathbb{A}^n(K)$ (pour la topologie de Zariski!).

▷ Soit U un ouvert de Zariski de \mathbb{A}^n . Il s'agit simplement de voir que l'intersection de deux ouverts non vides n'est jamais vide. Soient U_1, U_2 deux ouverts de Zariski, complémentaires de $\mathcal{V}(I_1)$ et $\mathcal{V}(I_2)$, $U_1 \cap U_2$ est le complémentaire de $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2)$. Par le Nullstellensatz, s'il était vide, on aurait $\sqrt{I_1 I_2} = (0)$ d'où $I_1 I_2 = 0$, impossible. ■

On peut même démontrer :

Proposition. (*Densité des ouverts relatifs de Zariski*)

Soit K algébriquement clos. Soit V une variété affine. Tout ouvert de Zariski non vide de V est dense dans V .

▷ En exercice (il suffit de rédiger proprement). ■

On renvoie au cours de TOPOLOGIE pour davantage sur la topologie de Zariski sur \mathbb{R}^n ou \mathbb{C}^n . On peut déjà remarquer que cette topologie, pour $n = 1$, n'est autre que la topologie co-finie. En particulier, elle n'est pas séparée au sens de Hausdorff.

Heuristique

En géométrie algébrique, le vocabulaire de la topologie de Zariski coexiste à celui de variétés et de leurs complémentaires, de même que la densité traduit un usage larvé du Nullstellensatz.

Un prérequis à cette section : ESPACES TOPOLOGIQUES IRRÉDUCTIBLES en TOPOLOGIE GÉNÉRALE.

Remarques.

1. $V_{(0)} = k^n$.
2. $V_1 = \emptyset$.

Voici une propriété importante pour simplifier les vérifications :

Propriété. (*Base de la topologie de Zariski*)

Soit $f \in \mathcal{O}(k^n)$, on note $U_f = V_f^c = \{x \in k^n \mid f(x) \neq 0\}$. Les U_f sont ouverts, dits *ouverts principaux*, et forment une base de la topologie de Zariski. Plus précisément, si $I \subseteq \mathcal{O}(k^n)$ est un idéal, alors $V_I^c = \bigcup_{i \in I} U_i$.

Exemples. (*Topologies de Zariski*)

1. Pour $n = 1$, les fermés (de Zariski) de k sont k et les sous-ensembles finis. C'est donc la topologie cofinie.
2. Si $k = \mathbb{C}$, un fermé de Zariski l'est pour la topologie usuelle de \mathbb{C}^n .
3. Dans le cas d'un corps fini, la topologie de Zariski est discrète.

Propriété. (*Compacité de k^n*)

$(k^n = X, \text{Zar})$ est quasi-compact.

▷

■

Corollaire

k^n est quasi-compact.



Attention ! La topologie de Zariski sur le produit est strictement plus fine que le produit des topologies de Zariski.

Propriété. (Produit de variétés affines)

Soient $V \subseteq k^n$ et $W \subseteq k^m$ algébriques. Alors $V \times W \subseteq k^{n+m}$ est algébrique.

▷ On note $V = V_I$, $I \subseteq \mathcal{O}(k^n)$ et $W = V_J$, $J \subseteq \mathcal{O}(k^m)$. On raisonne en termes de produit tensoriel. On observe que $\mathcal{O}(k^m) = k[X_1, \dots, X_m]$, $\mathcal{O}(k^n) = k[Y_1, \dots, Y_n] \hookrightarrow \mathcal{O}(k^{m+n}) = k[X_1, \dots, X_m, Y_1, \dots, Y_n]$ par ρ . Or $V_{\rho(I)} = k^m \times V$ et $V_{\rho(J)} = W \times k^n$ et $W \times V = V_{\rho(I)} \cap V_{\rho(J)} = V_{\rho(I)+\rho(J)}$. ■

Exemples

1. En dimension 1, deux cercles.

Lemme

Tout anneau de fonctions polynômes sur une variété est un anneau réduit.

▷ Soit V une variété affine. Alors $\mathcal{O}(V) \subseteq k^V$ qui est réduit, donc $\mathcal{O}(V)$ est réduit. ■

Proposition. (Décomposition en composantes irréductibles)

Soit X un ensemble algébrique. Alors... PRENDRE DANS TOPOLOGIE.

Corollaire

Les composantes irréductible de V_I correspondent aux idéaux premiers minimaux contenant I .

Les éléments de V_I correspondent aux idéaux maximaux contenant I , soit les idéaux maximaux de $\mathcal{O}(V)$.

Exemples

1. La courbe cubique tordue $C = \{(t, t^2, t^2), t \in k\} \subseteq \mathbb{A}^3(k)$ est un ensemble algébrique irréductible. Question : trouver des générateurs de l'idéal $I(C)$.
2. L'ensemble $V = V(X^2 - YZ, XZ - X)$ est constitué de trois ensembles algébriques irréductibles et déterminer les idéaux premiers correspondants.

Propriété

Soit $f \in k[X_1, \dots, X_n]$ un polynôme non constant. Soit $f = \prod_{i=1}^r f_i^{n_i}$ la décomposition de f en irréductibles. Alors $\sqrt{(f)} = (f_1 \dots f_r)$ et les composantes irréductibles de $V(f)$ sont les $V(f_i)$.



Dans \mathbb{A}^2 muni de la topologie de Zariski, $V(Y^2 - X^3 + X)$ est irréductible et donc connexe, mais ce n'est pas le cas pour la topologie usuelle.

Ce qu'il faut retenir

- Au bout de trois, les opérateurs V et I n'agissent plus.
- On a des bijections réciproques données par V et I entre les idéaux radiciels de $\mathcal{O}(k^n)$ et les sous-ensembles algébriques $V \subseteq k^n$; de même, entre les idéaux premiers de $\mathcal{O}(k^n)$ et les sous-ensembles algébriques irréductibles $V \subseteq k^n$.

2.1.6 Applications polynomiales entre variétés**2.1.7 Fonctions sur une variété**

Dès lors, on supposera tacitement le corps K algébriquement clos afin d'utiliser librement le théorème des zéros de Hilbert. Remarquons que dans nombre de résultats, cette hypothèse est superflue. L'analyse de sa nécessité est laissée à la perspicacité du lecteur.

2.1.7.1 L'algèbre de coordonnées d'une variété affine

Définition. (*Algèbre des coordonnées*)

Soit V une variété algébrique affine. On note $K[V] = K[X_1, \dots, X_n]/I_V$, où $I_V = \mathcal{J}(V)$ est l'idéal définissant V , et l'on appelle *algèbre des coordonnées* de V cet ensemble, qui est conceptuellement l'ensemble des fonctions polynômes « qui sont égales » sur V , i.e. de \mathbb{A}^n dans $K = \mathbb{A}^1$ qui à $x \mapsto P(x)$, soit $P : V \rightarrow \mathbb{A}^1$, et $\bar{f} = \bar{g}$ si et seulement si $f = g + u$ où u est nulle sur V .

Lemme. (*Correspondance entre idéaux maximaux et variétés*)

V est un point $\iff I_V$ est maximal, i.e. $K[V]$ est un corps.

▷ On peut le voir dans la version faible du Nullstellensatz. ■

Lemme. (*Correspondance entre idéaux premiers et variétés*)

V est irréductible $\iff I_V$ est premier, i.e. $K[V]$ est intègre.

▷ Si I_V est non premier, il existe $P_1, P_2 \notin I_V$ tels que $P_1 P_2 \in I_V$. Ainsi V_1 le lieu d'annulation de $P_1 \subsetneq V$ et V_2 de $P_2 \subsetneq V$. Il suit que $V_1 \cup V_2 = \{x \in V, P_1 P_2(x) = 0\} = V$. Réciproquement, si V est réductible, écrivons $V = V_1 \cup V_2$, avec $V_1, V_2 \neq V$, d'où $I_V \subsetneq I_{V_1}$ et $I_V \subsetneq I_{V_2}$, car V, V_1, V_2 sont algébriques. Donc il existe $P_1 \in I_{V_1} \setminus I_V$, $P_2 \in I_{V_2} \setminus I_V$. $P_1 P_2$ s'annule sur V , car il s'annule sur V_1 et V_2 , donc I_V n'est pas premier. ■

On tente de varier le point de vue.

Définition. (*Application polynomiale entre variétés affines*)

Soient V, W deux variétés algébriques affines. On appelle *application polynomiale* de V à W toute fonction f de $V \subseteq \mathbb{A}^n$ dans $W \subseteq \mathbb{A}^m$, n, m entiers naturels, telle qu'il existe $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ tels que $\forall x \in V \quad f(x) = (f_1(x), \dots, f_m(x))$, avec $(f_1(x), \dots, f_m(x)) \in W$. On parle égale de *morphisme de variétés algébriques*.

Définition. (*Isomorphisme entre variétés affines*)

Soient V, W deux variétés algébriques affines. Un *isomorphisme* entre variétés affines est une application polynomiale de $f : V \longrightarrow W$ telle qu'il existe $g : W \longrightarrow V$ polynomiale avec $g \circ f = id_V$ et $f \circ g = id_W$.



Ce n'est pas « un morphisme bijectif » ! (Prendre la fonction cube.)

Définition-propriété. (Transposée d'un morphisme de variétés algébriques)

Soient V, W deux variétés algébriques affines. Soit $f : V \longrightarrow W$ polynomiale. L'application :

$$\begin{aligned} f^* : K[W] &\longrightarrow K[V] \\ h &\longmapsto h \circ f \end{aligned}$$

est un homomorphisme de K -algèbres. (On rappelle qu'un homomorphisme de K -algèbre fixe les éléments de K .)

▷ Soit $f = (f_1, \dots, f_m)$ par définition. Si $P \in K[Y_1, \dots, Y_m]$, $h \in K[W]$ la classe de P modulo I_W , $f^*(h) = (P \circ (f_1, \dots, f_m))(X_1, \dots, X_n)$ modulo I_W est bien définie car vient d'un morphisme nul sur I_W . Il est immédiat qu'elle définit un homomorphisme de K -algèbres. ■

Remarque. $x \in V$ si et seulement si pour tout $Q \in I_V$, $Q(x) = 0$. Si $x \in V$, $(f_1(x), \dots, f_n(x)) \in W \iff \forall P \in I_W \quad P(f_1(x), \dots, f_m(x)) = 0$.

On énonce maintenant le théorème central de la théorie des variétés affines.

Théorème. (Théorème de correspondance des variétés affines)

Soit K un corps. On a une équivalence de catégories entre la catégorie dont les objets sont les variétés affines et les morphismes les applications polynomiales, avec la catégorie des K -algèbres de type fini intègres dont les morphismes sont les homomorphismes de K -algèbres. Explicitement,

1. toute K -algèbre de type fini intègre est l'algèbre de coordonnées d'une variété affine et V est isomorphe à W si et seulement si $K[V]$ est isomorphe à $K[W]$ en tant que K -algèbres.
2. Soit $\phi : K[W] \longrightarrow K[V]$ un homomorphisme de K -algèbre. Il existe une unique application polynomiale $f : V \longrightarrow W$ telle que $\phi = f^*$. De plus, si $V \xrightarrow{f} W \xrightarrow{g} X$, $(g \circ f)^* = f^* \circ g^*$.

Cette équivalence préserve le type et la dimension, de sorte qu'on aurait pu dire : on a une équivalence de catégories entre la catégorie dont les objets sont les variétés affines de dimension n et les morphismes les applications polynomiales, avec la catégorie des K -algèbres de type fini n intègres dont les morphismes sont les homomorphismes de K -algèbres.

▷ Si A est une K -algèbre de type fini intègre, il existe $t_1, \dots, t_n \in A$ tels que $A = K[t_1, \dots, t_n]$, donc il existe $K[X_1, \dots, X_n] \hookrightarrow A$ une surjection ψ qui à $X_i \mapsto t_i$, si $I = \text{Ker}(\psi)$, on a $A \simeq K[X_1, \dots, X_n]/I$. Comme A est intègre, I est premier, donc réduit. Si on pose $V = \mathcal{V}(I) \subseteq \mathbb{A}^n$, on a $K[V] \simeq A$. Si $g : V \longrightarrow W$, $g : W \longrightarrow V$ sont polynomiales et inverses l'une de l'autre, alors en passant aux transposées, $f^* : K[W] \longrightarrow K[V]$ et $g^* : K[V] \longrightarrow K[W]$ sont clairement inverses l'une de l'autre en utilisant la contravariance que l'on vérifiera indépendamment dans le second point. Si maintenant $\phi : K[W] \longrightarrow K[V]$ et $\psi : K[V] \longrightarrow K[W]$ sont des homomorphismes réciproques de K -algèbre, on

sait encore par le deuxième point qu'il existe $f : V \longrightarrow W$, $g : W \longrightarrow V$ tels que $\phi = f^*$ et $\psi = g^*$. On obtient $(f \circ g)^* = id_W^*$ et $(g \circ f)^* = id_V^*$ d'où $f \circ g = id_W$ et $g \circ f = id_V$.

On rappelle : $K[V] = K[X_1, \dots, X_n]/I_V$ et $K[W] = K[Y_1, \dots, Y_m]/I_W$. Soit donnée $\phi : K[W] \longrightarrow K[V]$. Posons $y_i = Y_i$ modulo I_W puis $g_i = \phi(y_i) \in K[V]$ la classe de $f_i \in K[X_1, \dots, X_n]$ modulo I_V . Posons $f_i : \mathbb{A}^n \longrightarrow \mathbb{A}^m$ qui à $x \mapsto (f_1(x), \dots, f_m(x))$. Montrons que $f : V \longrightarrow W$ et que $f^*(y_i) = y_i \circ f = f_i \text{ mod } I_V = g_i = \phi(y_i)$. On a $\phi, f^* : K[W] \longrightarrow K[V]$. Or $K[W]$ est engendrée comme K -algèbre par les y_i . Or $f^*(y_i) = \phi(y_i)$, donc $\phi = f^*$. Or $x \in V$ si et seulement si $\forall P \in I_V \quad P(x) = 0$. Soit $Q \in I_W$. Alors $Q(f_1(X), \dots, f_m(X)) = Q(\phi(y_1), \dots, \phi(y_m)) = \phi(Q(y_1, \dots, y_m)) = \phi(Q(Y_1, \dots, Y_m) \text{ mod } I_W) = 0$, car ϕ est un homomorphisme de K -algèbres. ■

2.1.7.2 Corps de fonctions d'une variété

On aimerait inclure les fractions rationnelles, également foncièrement définies par des polynômes, dans ces définitions.

Définition. (Corps des fonctions d'une variété affine)

Soit V une variété affine. Son *corps des fonctions* est $K(V) = \text{Frac}(K[V])$, qui est bien défini, car $K[V]$ est intègre.

Remarque. Soit $f \in K(V)$. Elle induit une fonction $V \longrightarrow K = \mathbb{A}^1$ définie au moins, si $f = \frac{f_1}{f_2}$, sur $V \setminus \mathcal{V}(f_2)$.

Définition. (Fonction régulière, domaine)

Soit $f \in K(V)$. On dit que f est *régulière en x* si l'on peut écrire $f = f_1/f_2$ avec $f_1, f_2 \in K[V]$ et $f_2(x) \neq 0$.

On note $\text{dom}(f)$ le *domaine* de f , qui est l'ensemble des $x \in V$ tels que f soit régulière en x .

Proposition. (Ouverture des domaines)

Le domaine d'une fonction est un ouvert de V , non vide si K est algébriquement clos, donc dense.

▷ On note $D_f = \{h \in K[V] \mid fh \in K[V]\}$ l'idéal des dénominateurs dans $K[V]$. Montrons que $\text{dom}(f) = V \setminus \mathcal{V}(D_f)$ et cela suffira. Soit $x \in \text{dom}(f)$. Alors $f = f_1/f_2$ avec $f_1 \in K[V]$ et $f_2(x) \neq 0$. On a $f_2 \in D_f$, donc $x \notin \mathcal{V}(D_f)$. Soit maintenant $x \notin \text{dom}(f)$. Pour tous $f_1, f_2 \in K[V]$ tels que $f = f_1/f_2$, $f_2(x) = 0$. Donc pour tout $h \in D_f$, on trouve $h(x) = 0$, donc $x \in \mathcal{V}(D_f)$. Le domaine est non vide : il existe une écriture $f = f_1/f_2$ avec $f_2 \in K[V] \setminus \{0\}$, donc $V \setminus \mathcal{V}(f_2) \subseteq \text{dom}(f)$ où $V \setminus \mathcal{V}(f_2) \neq \emptyset$ par le Nullstellensatz. ■

Définition. (Anneau local d'une variété en un point)

Soit V une variété algébrique et $x \in V$. L'*anneau local de V en x* est l'ensemble des fonctions régulières au point x : $\mathcal{O}_{V,x} = \{f \in K(V), f \text{ régulière en } x\}$. Son unique idéal maximal est l'ensemble des fonctions régulières en x qui s'annulent en x : $\mathfrak{M}_{V,x} = \{f \in \mathcal{O}_{V,x} \mid f(x) = 0\}$, appelé *idéal maximal en x* .

Remarques.

1. C'est bien un anneau local, soit $\mathcal{O}_{V,x}^\times = \mathcal{O}_{V,x} \setminus \mathfrak{M}_{V,x}$.

▷ En effet, l'évaluation $f \mapsto f(x)$ induit un isomorphisme $\mathcal{O}_{V,x}/\mathfrak{M}_{V,x} \rightarrow K$, d'où la maximalité. Par ailleurs, si $f \in \mathcal{O}_{V,x}$ ne s'annule pas en x , alors $\frac{1}{f} \in \mathcal{O}_{V,x}$, d'où la localité : les éléments inversibles sont bien les éléments qui n'appartiennent pas à $\mathfrak{M}_{V,x}$. ■

2. Il y a aussi, sans mauvais jeu de mots, localisation du point de vue topologique, car la définition ne dépend que d'un ouvert autour de x (*voir ci-dessous*). Si U est un ouvert affine de V , si $x \in U \subseteq V$, on peut définir $\mathfrak{M}_{U,x} \subseteq \mathcal{O}_{U,x} \subseteq K(U)$. On en déduit :

Proposition

Le corps de fractions d'une variété (affine) V est identique au corps de fractions d'un ouvert de V .

▷ Ainsi, si U est un ouvert affine de V , si $x \in U \subseteq V$, on peut définir $\mathfrak{M}_{U,x} \subseteq \mathcal{O}_{U,x} \subseteq K(U)$. Si $f \in K[V]$, on note $V_f = V \setminus \{x \in V \mid f(x) = 0\}$. Alors l'ouvert $V'_f = \{(x,t) \in \mathbb{A}^n \times \mathbb{A}^1, x \in V, 1 - tf(x) = 0\}$ est une variété affine de \mathbb{A}^{n+1} . De plus, V'_f est isomorphe à V_f par la projection de \mathbb{A}^{n+1} sur \mathbb{A}^n , de réciproque $x \mapsto (x, \frac{1}{f(x)})$; ainsi $K[V_f] = K[V][\frac{1}{f}]$ donc $K(V_f) = K(V)$. ■

Inversement, on voit que l'opération algébrique de localisation correspond géométriquement à se restreindre à un ouvert (comment ?).

Ceci permet de définir $K(V)$ dans deux cas :

- si V est un ouvert non vide d'une variété affine,
- si V est projective (*voir section suivante*). En effet, si $V \subseteq \mathbb{P}^n$, $K(V) = K(V_i)$ où $V_i = V \cap U_i$ avec $U_i = \{x_i \neq 0\} \subseteq \mathbb{P}^n$. On peut alors définir $\mathfrak{M}_{V,x} \subseteq \mathcal{O}_{V,x} \subseteq K(V)$ dans ce cas.

Théorème

1. Soit V une variété affine. Alors

$$\{f \in K(V) \mid f \text{ régulière en tout } x \in V\} = \bigcap_{x \in V} \mathcal{O}_{V,x} = K[V].$$

2. Soit V une variété projective. Alors

$$\{f \in K(V) \mid f \text{ régulière en tout } x \in V\} = \bigcap_{x \in V} \mathcal{O}_{V,x} = K.$$

▷ Par définition, f est régulière si et seulement si $\text{dom}(f) := V \setminus \mathcal{V}(D_f) = V$, avec $D_f = \{h \in K[V] \mid hf \in K[V]\}$, qui équivaut à $\mathcal{V}(D_f) = \emptyset$. D'après le Nullstellensatz, ceci équivaut à $1 \in D_f$, et cette condition implique que $f = 1.f \in K[V]$.

Dans le cas projectif, on traite le cas $V = \mathbb{P}^n$ pour simplifier des notations trop lourdes qui cacheraient les idées de la preuve. Soit $f \in K(\mathbb{P}^n)$ régulière pour tout $x \in \mathbb{P}^n$. Montrons que f est constante. On pose $U_i = \{[x_0, \dots, x_n] \in \mathbb{P}^n, x_i \neq 0\} \simeq \mathbb{A}^n$ par $[x_0, \dots, x_n] \mapsto (\frac{x_0}{x_i}, \dots, \hat{1}, \dots, \frac{x_n}{x_i})$ de réciproque $(y_1, \dots, y_n) \mapsto [y_1, \dots, \frac{1}{y_i}, \dots, y_n]$. L'application $f_i = f|_{U_i}$ est un polynôme en (y_1, \dots, y_n) de sorte que $f_i(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}) = x_i^{-d_i} F_i(x_0, \dots, x_n)$ est un polynôme homogène de degré d_i avec X_i ne divisant pas F_i . En regardant sur $U_i \cap U_j$, $x_i^{-d_i} F_i = x_j^{-d_j} F_j \iff x_j^{d_j} F_i = x_i^{d_i} F_j$, donc $x_d^{d_j} \mid F_j \implies d_j = 0$, donc tous les polynômes F_i sont constants. Ceci termine la preuve. ■

2.1.7.3 Applications rationnelles, applications birationnelles

Définition. (*Application rationnelle*)

Une *application rationnelle* notée $f : V \cdots \rightarrow W$, V, W deux variétés algébriques affines incluses respectivement dans \mathbb{A}^n et dans \mathbb{A}^m , s'il existe $f_1, \dots, f_m \in K(V)$ telles que $f = (f_1, \dots, f_m)$ et si $x \in \text{dom}(f) = \bigcap_{i=1}^m \text{dom}(f_i) \implies (f_1(x), \dots, f_m(x)) \in W$.

Sous cette définition, les applications rationnelles ne se composent pas naturellement : pour $f : V \cdots \rightarrow W$ et $g : W \cdots \rightarrow X$ deux applications rationnelles, on ne peut définir $g \circ f$ nulle part ! si $f(\text{dom}(f)) \subseteq W \setminus \text{dom}(g)$.

Définition. (*Application dominante*)

Une application rationnelle $f : V \cdots \rightarrow W$ entre deux variétés V, W affines est dite *dominante* si $f(\text{dom}(f))$ est dense dans W .

L'intérêt direct de cette notion est que **l'on peut alors définir la composition avec l'application rationnelle dominante f pour toute application rationnelle.**

En particulier, la transposée $f^* : K(W) \longrightarrow K(V)$, $h \mapsto h \circ f$ est bien définie.

Définition. (*Isomorphisme birationnel*)

Un *isomorphisme birationnel* est une application rationnelle $f : V \cdots \rightarrow W$ telle qu'il existe $g : W \cdots \rightarrow V$ telles que $f \circ g = \text{id}_W$ et $g \circ f = \text{id}_V$ en identifiant deux applications égales sur un ouvert dense ; ces deux applications sont automatiquement dominantes.



Ce n'est pas un isomorphisme au sens déjà connu. En revanche, un isomorphisme algébrique est un isomorphisme birationnel.

Théorème. (Isomorphie birationnelle par les corps de fonctions)

Soient V, W deux variétés algébriques affines.

1. Les variétés V, W sont birationnellement isomorphes si et seulement si $K(V) \simeq K(W)$ sont isomorphes par des K -isomorphismes de corps.
2. Tout K -homomorphisme $K(W) \xrightarrow{\phi} K(V)$ correspond à une application rationnelle dominante $f \cdots \rightarrow W$ telle que $\phi = f^*$. De plus, $(g \circ f)^* = f^* \circ g^*$. De plus, si $V \xrightarrow{f} W \xrightarrow{g} X$.

▷ $g^* \circ f^* = id_W^*$, $f^* \circ g^* = id_V^*$ et $g^* : K(V) \rightarrow K(W)$, $f^* : K(W) \rightarrow K(V)$. Si $\phi : K(W) \simeq K(V)$, $\phi = f^*$ puis $\phi^{-1} = g^*$ conviennent, en admettant la suite du théorème. Montrons-le indépendamment. On observe que $K(V)$ est une extension de corps de $K(W) \simeq \phi(K(W))$, avec $K[V] \subseteq K(V)$ et $K[W] \subseteq K(W)$. Si $K[W] \subseteq K[V]$, l'inclusion correspond à $f : V \rightarrow W$ et l'on se ramène au théorème dans le cas des variétés affines. Vérifions que l'on peut toujours se ramener à ce cas. $K[W] = K[t_1, \dots, t_m] \subseteq K[V_g]$ donc $K[W] \subseteq K[V][t_1, \dots, t_m] \subseteq K(V)$. ■

Corollaire. (Isomorphie birationnelle par les ouverts)

Sont équivalents :

1. V et W sont birationnellement isomorphes,
2. $K(V) \simeq K(W)$,
3. il existe un ouvert $V_0 \subseteq V$, $W_0 \subseteq W$ et $V_0 \simeq W_0$ par des fonctions régulières.

▷ On a montré que les deux premiers points étaient équivalents ; il est clair que le troisième point implique le premier, car on a vu que l'algèbre de coordonnées ne dépend que d'un ouvert. Montrons que le premier point implique le troisième. Le point délicat est de montrer que deux variétés birationnelles contiennent des ouverts isomorphes. Si $f : V \cdots \rightarrow W$ et $g : W \cdots \rightarrow V$ sont des applications rationnelles et inverses, notons \tilde{f} la restriction de f à son domaine de \tilde{g} la restriction de g à $\text{dom}(g)$. Posons $V_0 = \tilde{f}^{-1}\tilde{g}^{-1}\text{dom}(f)$ et $W_0 = \tilde{g}^{-1}\tilde{f}^{-1}\text{dom}(g)$. On vérifie par simple calcul que $f(V_0) \subseteq W_0$ et $g(W_0) \subseteq V_0$, ce qui donne l'énoncé voulu puisqu'alors dès que les fonctions sont définies, $f \circ g(y) = y$ et $g \circ f(x) = x$. ■

Exemple. (Isomorphie birationnelle)

On reprend la paramétrisation d'une conique simple. Prenons $V = \mathbb{A}^1$ et $W = \{(x, y) \in \mathbb{A}^2 \mid x^3 = y^2\}$. Exhibons $f : V \rightarrow W$ qui à $t \mapsto (t^2, t^3)$ de réciproque $g : (x, y) \cdots \rightarrow \frac{y}{x}$. C'est un isomorphisme birationnel et ici explicitement $V_0 = \mathbb{A}^1 \setminus \{0\}$, $W_0 = W \setminus \{(0, 0)\}$.

C'est un exemple où l'on peut exhiber un isomorphisme birationnel entre des ouverts stricts.

On mentionne :

Théorème

Toute variété est birationnelle à une hypersurface.

▷ Montrons qu'une variété de dimension d est birationnelle à une hypersurface de \mathbb{A}^{d+1} . Dans $K(V)$, on choisit x_1, \dots, x_d algébriquement indépendants tels que $K(V)/K(x_1, \dots, x_d)$ soit algébrique de degré fini. Par le théorème de l'élément primitif, $K(V) = K(x_1, \dots, x_d)(y)$. En particulier, y est racine d'un certain $y^n + f_{n-1}(x_1, \dots, x_d)y^{n-1} + \dots + f_0(x_1, \dots, x_d) = 0$. Il existe $g \in K[x_1, \dots, x_d]$ tel que $gf_j \in K[x_1, \dots, x_d]$ en remplaçant g par gy , on peut supposer $f_j \in K[x_1, \dots, x_d]$. Posons $F(X_1, \dots, X_d, Y) = Y^n + f_{n-1}Y^{n-1} + \dots + f_0(X) = 0$ et $W = \{(x_1, \dots, x_d, y) \in \mathbb{A}^{d+1} \mid F(x, y) = 0\}$. Alors $K[W] = K[x_1, \dots, x_d, Y]/(F) = K[x_1, \dots, x_d, y]$, y vérifiant la condition ci-dessus. D'où $\text{Frac}(K[W]) = K(x_1, \dots, x_d)(y) \simeq K(V)$, d'où le résultat. ■

2.1.7.4 Image d'une variété affine

Contre-exemple. (Image d'une variété par une application rationnelle)

Soit $f : \mathbb{A}^2 \rightarrow \mathbb{A}^2$ qui à $(x, y) \mapsto (x, xy)$. C'est une application polynomiale, régulière, et même birationnelle, mais son image n'est pas une variété

Calculons son image. $f(\mathbb{A}^1 \setminus \{0\} \times \mathbb{A}^1) = \mathbb{A}^1 \setminus \{0\} \times \mathbb{A}^1$ et $f(0 \times \mathbb{A}^1) = \{(0, 0)\}$. Son image est donc $\mathbb{A}^2 \setminus \{(0, y) \mid y \in \mathbb{A}^1 \setminus \{0\}\}$. Ce n'est clairement pas une variété. □

2.1.7.5 Définitions

Le but est d'étudier les ensembles algébriques indépendamment d'un plongement $V \subseteq k^n$. On a déjà défini l'invariant $\mathcal{O}(V)$, qui ne dépend pas du plongement.

Définition. (Application polynomiale entre variétés affines)

Soit $V \subseteq k^n, W \subseteq k^n$ deux ensembles algébriques. Une application $P : V \rightarrow W$ est dite *polynomiale* si c'est la restriction à V d'une application polynomiale $k^n \xrightarrow{\tilde{P}} k^n$, donnée par $x = (x_1, \dots, x_n) \rightarrow (P_1(x), \dots, P_m(x))$ avec $P_1, \dots, P_m \in k[X_1, \dots, X_n]$.

$$\begin{array}{ccc} k^n & \xrightarrow{\tilde{P}} & k^n \\ \uparrow & & \uparrow \\ V & \xrightarrow{P} & W \end{array}$$

Fait

Les fonctions polynomiales (régulières) sur V sont les morphismes de cette variété vers une droite (*i.e.* k) : $f \in \mathcal{O}(V) = \mathcal{O}(k^n)/I_V \iff f : V \rightarrow k$ polynomiale.

Propriété

$$\mathcal{O}_V(U_f) = \mathcal{O}(V)[f^{-1}].$$

▷ On pose $V = V_I$, $I \subseteq k[X_1, \dots, X_n]$ et $J = \langle I, Yf(X_1, \dots, X_n) - 1 \rangle \subseteq K[X_1, \dots, X_n, Y]$. $U_K = \{(x, y), x \in V_I, yf(x) = 1\}$ en bijection avec $U_f = \{x \in V_I, f(x) \neq 0\}$ par $x, y \mapsto x$ ($x \in U_f$!) et $x \mapsto (x, \frac{1}{f(x)})$. ■

Heuristique

Ici, U_f est un ouvert de V défini par $f(V) \neq 0$, et U_f est aussi un fermé de $V \times k$ définie par (u, x) où $f(u)x = 1$.

Cette façon de voir les choses de deux manières duales est fondamentale, et souvent, le côté fermé est le meilleur. Par exemple plus pratique, $GL_n \subseteq \mathfrak{M}_n$ est un ouvert avec $\det(M) \neq 0$, mais c'est un fermé de $\mathfrak{M}_n \times \mathfrak{M}_n$ par $\{(M, N) \mid MN = 1\}$.

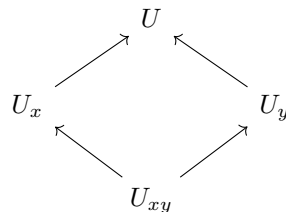
Là, c'est une question de point central d'une droite et hyperbole (?).

Exercice 4

Soit $U = A^2 \setminus \{(0, 0)\}$. Montrer que $\mathcal{O}_V(U) = \mathcal{O}(U)$.

▷ **Éléments de réponse.**

Signalons : on est dans un anneau intègre, donc les fonctions régulières se plongent dans le corps des fractions.



On identifie $f : f|_{U_x} \times f|_{U_y}$ et $f|_{U_{xy}} \in K[x, y]$. $f|_{U_x} \in k[X, Y, \frac{1}{X}] = \frac{a}{X^n}$, $X \nmid a$ et $f|_{U_y} \in k[X, Y, \frac{1}{Y}] = \frac{a}{Y^n}$, $Y \nmid a$; on utilise la factoriabilité de $k[X, Y]$. D'où $aY^n = bX^n$ puis $Y \mid b$, donc $m = 0$. D'où $\mathcal{O}_V(U) = \mathcal{O}(V)$.

2.1.7.6 Considérations fonctorielles

VOC On note $\text{App.Poly}(V, W)$ les applications polynomiales de V vers W .

Définition. ()

Soit $\varphi : V \rightarrow W$ polynomiale. On lui associe $\varphi^* : \mathcal{O}(W) \rightarrow \mathcal{O}(V)$ la *précomposition par* φ^* via $(f : W \xrightarrow{\text{POLY}} k) \mapsto (V \xrightarrow{\varphi} W \xrightarrow{f} k)$.

À partir de là, $k = \bar{k}$.

Propriété

L'application $\varphi \rightarrow \varphi^*$ est une bijection $\text{App.Poly}(V, W) \rightarrow \text{Hom}_{k\text{-alg.}}(\mathcal{O}(W), \mathcal{O}(V))$.

▷ Cela repose sur la formule. Si $x \in V, y \in W$, soit $\mathcal{M}_x \subseteq \mathcal{O}(V)$ et $\mathcal{M}_y \subseteq \mathcal{O}(W)$ les idéaux maximaux correspondant. Alors $\mathcal{M}_{\varphi(x)} = (\varphi^*)^{-1}(\mathcal{M}_x)$. On a $f : \mathcal{O}(W) \rightarrow \mathcal{O}(V) \rightarrow (\varphi : V \rightarrow W)$ et $\mathcal{M}_{\varphi(x)} = f^{-1}(\mathcal{M}_x)$.

$$\begin{array}{ccc}
 k^n & \xrightarrow{\Phi} & k^m \\
 \uparrow & & \uparrow \\
 V & \xrightarrow{\varphi} & W
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathcal{O}(k^n) = k[x_1, \dots, x_n] & \xrightarrow{\exists F} & \mathcal{O}(k^n) \\
 \Downarrow & & \Downarrow \\
 \mathcal{O}(W) & \longrightarrow & \mathcal{O}(V) \\
 \downarrow & & \downarrow \\
 V \ni x_1 & \xrightarrow{f} & f(x_1) \in V
 \end{array}$$

■

Théorème

L'association de l'ensemble des ensembles algébriques vers les k -algèbres de type fini réduites qui à $V \subseteq k^n \rightarrow \mathcal{O}(V)$ est un foncteur contravariant, pour les morphismes $\text{Poly}(\cdot, \cdot)$ à la source et $\text{Hom}_{k\text{-alg.}}(\cdot, \cdot)$ à l'arrivée et c'est une (anti-)équivalence.

▷ Le foncteur est pleinement fidèle. C'est déjà fait : $\text{App.Poly}(V, W) \xrightarrow{\sim} \text{Hom}_{k\text{-alg.}}(\mathcal{O}(W), \mathcal{O}(V))$.

Il est essentiellement surjectif. Soit A une k -algèbre de type fini réduite. On peut écrire $A \simeq k[X_1, \dots, X_n]/I$ où $I = \sqrt{I}$. On pose $V = V_I \subseteq k^n$ d'où par le théorème des zéros $\psi(V \subseteq k^n) = k[X_1, \dots, X_n]/I \simeq A$ ■

Lemme. (Foncteur des points)

Soit k un corps quelconque et \bar{k} sa clôture algébrique. Soit A une k -algèbre de type finie. L'application

$$\text{Hom}_k(A, \bar{k}) \longrightarrow \text{SpMax}(A)$$

qui à φ donne $\text{Ker}(\varphi)$, est surjective (par le THO) et à fibres finies.

Il n'est pas tout à fait clair que l'image de φ est une extension algébrique finie de k : $\varphi(A)$ est une k -algèbre de type fini et algébrique sur \bar{k} .

Heuristique

$\text{Hom}_k(A, \bar{k})$ se comporte bien si $A = \text{Hom}_{k\text{-alg.}}(A, l)$ est l'ensemble des solutions du système à coefficients dans \bar{k} .

On peut l'identifier à $\{(M, i)\}$ où $M \in \text{SpMax}(A)$ et i est un plongement du corps résiduel de M $A/M \hookrightarrow \bar{k}$.

2.1.7.7 Applications sur le produit de variétés

Lemme

Soit k algébriquement clos et A, B deux k -algèbres intègres. Alors $A \otimes_k B$ est intègre.

▷ D'abord, on peut se ramener au cas du type fini : si $x = \sum_{i=1}^n a_i \otimes b_i \in A \otimes_k B$ et de même $y = \sum_{i=1}^n c_i \otimes d_i$, avec $xy = 0$, qui est l'hypothèse de notre démonstration ; on veut montrer que $x = 0$ ou $y = 0$, alors en posant $A' = k[a_i, c_i, i \in \llbracket 1, n \rrbracket]$ et $B' = k[b_i, d_i, i \in \llbracket 1, n \rrbracket]$, alors $A' \subseteq A$ et $B' \subseteq B$ sont intègres et de type fini.

Sous ces hypothèses, soit $\varphi : A \rightarrow k$ un morphisme, $M = \text{Ker}(\varphi)$ idéal maximal de A . On définit $\varphi \otimes \text{id}_B : A \otimes_k B \rightarrow k \otimes_k B = B$, notée encore φ , de sorte que $\text{Ker}(\varphi \otimes \text{id}_B) = \text{Ker}(\varphi) \otimes_k B$. Or

$$a \otimes b \mapsto \varphi(a)b$$

$\varphi(x)\varphi(y) = 0 \in B$, donc par intégrité de B , $\varphi(x) = 0$ ou $\varphi(y) = 0$. Or, $\varphi(x) = 0 \iff x \in M_\varphi \otimes_k B \subseteq A \otimes_k B$; si c'est le cas, on dira que φ est de premier type. De même, $\varphi(y) = 0 \iff y \in M_\varphi \otimes_k B$ et l'on dira là que φ est de second type. Dans le premier cas, $x \in \left(\bigcap_{\varphi \text{ de premier type}} M_\varphi \right) \otimes B$ et dans le second

cas, $y \in \left(\bigcap_{\varphi \text{ de second type}} M_\varphi \right) \otimes B$. Notons I et J ces deux idéaux de A . Alors $V(I) \cup V(J) = \text{SpMax}(A)$,

mais comme A est intègre, cet espace est irréductible au sens topologique, donc $V(I)$ ou $V(J)$ est égal à $\text{SpMax}(A)$. Ceci signifie que $\forall \varphi \quad \varphi(x) = 0$, soit $x = 0$ dans le premier cas, ou semblablement $y = 0$ dans le second cas. ■

Lemme

Soit k algébriquement clos et A, B deux k -algèbres réduites de type fini. Alors $A \otimes_k B$ est réduit.

▷ La preuve n'est pas si évidente. Soit $x \in A \otimes_k B$ nilpotent, avec $x = \sum_{i=1}^n a_i \otimes b_i$. Soit $\varphi : B \rightarrow k$ morphisme de k -algèbres, autrement dit un point de l'ensemble algébrique associé à B

par le théorème de zéros. Posons $\tilde{\varphi}(x) = \sum_{i=1}^n a_i \varphi(b_i) \in A$ par bifonctorialité du produit tensoriel : $\tilde{\varphi} : id_A \otimes_k \varphi : A \otimes_k B \rightarrow A$. Puisque x est nilpotent, $\varphi(x)$ aussi, et par réduction de A , $\varphi(x) = 0$. Alors $\text{Ker}(\tilde{\varphi}) = A \otimes_k \text{Ker}(\varphi) \subseteq A \otimes_k B$. Or ceci vaut pour tout $\varphi : B \rightarrow k$, donc pour tout idéal maximal M de B , on a $x \in A \otimes_k M \subseteq A \otimes_k B$, d'où $x \in \bigcap_{M \subseteq B, M \text{ maximal}} A \otimes_k M = A \otimes_k \bigcap_{M \subseteq B, M \text{ maximal}} M = \{0\}$ par réduction de B . Donc $x = 0$. ■

Remarque. On peut remplacer k algébriquement clos par k parfait.

Exercice 5

Donner un contre-exemple où k n'est pas clos.

▷ **Éléments de réponse.**

On tensorise une extension algébrique avec elle-même : $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, qui vaut un produit de deux copies de \mathbb{C} , qui n'est donc pas intègre.

On aurait aussi pu choisir une extension purement inséparable.

Corollaire

La catégorie des ensembles algébriques admet des produits finis et $\mathcal{O}(V \times W) = \mathcal{O}(V) \otimes_k \mathcal{O}(W)$.

Remarque. Ceci est cohérent avec la preuve de ce que le produit de deux variétés affines est une variété. En effet, si $V = V_I$ où $I \subseteq k[X_1, \dots, X_n]$ et $W = V_J$ où $J \subseteq k[Y_1, \dots, Y_m]$, alors $V \times W = V_S$ où $S = \langle I, J \rangle \subseteq k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ et $k[X_1, \dots, X_n]/I \otimes_k k[Y_1, \dots, Y_m]/J = k[X_1, \dots, X_n, Y_1, \dots, Y_m]/S$.

2.1.7.8 Caractérisations classiques

Exercice 6

Soit $\varphi : V \rightarrow W$ une application polynomiale. Alors $\overline{\varphi(V)} = V_{\text{Ker}(\varphi^*)}$ où $\varphi^* : \mathcal{O}(W) \rightarrow \mathcal{O}(V)$. Donc φ^* injective $\iff \varphi(V)$ dense dans W .

▷ **Éléments de réponse.**

On se ramène au deuxième cas par la manipulation suivante : on peut supposer $W = \overline{\varphi(V)}$.

$$\begin{array}{ccc} \mathcal{O}(\overline{\varphi(V)}) & \hookrightarrow & \mathcal{O}(V) \\ \uparrow & \nearrow \varphi^* & \\ \mathcal{O}(W) & & \end{array}$$

est injective (la factorisation canonique de φ^*). Ainsi $\mathcal{O}(\overline{\varphi(V)}) = \text{Ker}(\varphi^*)$.

2.1.7.9 Morphismes finis

Définition. (*Morphisme fini*)

Soit $\varphi : V \rightarrow W$. On dit que φ est un *morphisme fini* si $\varphi^* : \mathcal{O}(W) \rightarrow \mathcal{O}(V)$ est un morphisme fini d'anneaux, i.e. $\mathcal{O}(V)$ est un $\mathcal{O}(W)$ module de type fini.

Remarque. Morphisme fini = de type fini et entier.

On peut alors énoncer une des rares propriétés pour montrer qu'un morphisme est surjectif.

Propriété

Soit $\varphi : V \rightarrow W$ un morphisme fini. Alors φ est fermé (i.e. pour tout $F \subseteq V$ fermé, $\varphi(F)$ est fermé dans W).

▷ φ factorise $V \rightarrow \overline{\varphi(V)} \rightarrow W$. Quitte à remplacer W par $\overline{\varphi(V)}$, on se ramène à $\overline{\varphi(V)} = W$. qui signifie que $\varphi^* : \mathcal{O}(W) \rightarrow \mathcal{O}(V)$ est injective (et fini par hypothèse) par $\mathcal{O}(W)/\text{Ker}(\varphi) = \mathcal{O}(\overline{\varphi(V)})$. On se ramène à un énoncé d'algèbre commutative : si $f : A \rightarrow B$ est un morphisme fini et injectif entre k -algèbres de type fini, alors $\text{SpMax}(B) \rightarrow \text{SpMax}(A)$ est surjective.

$$N \mapsto f^{-1}(N)$$

Soit $M \subseteq A$ idéal maximal. Si $\langle f(M) \rangle \neq B$, soit $N \subseteq B$ un idéal maximal, avec $f(M) \subseteq N$, alors $f^{-1}(N) = M$. Posons $I = \langle f(M) \rangle \subseteq B$. Supposons $I = B$, soit $MB = B$ où B est considéré comme un A -module fini. $\sum f(m_i)b_i \in MB$. Par le lemme de Nakayama, il existe $a \in A$ tel que $a \equiv 1 \pmod{M}$ et $aB = 0$. Donc $a \neq 0$ et $f(a) = 0$ ce qui contredit l'injectivité de f . ■

2.1.8 Faisceaux de fonctions régulières

Le but est d'aller définir les variétés algébriques et pas seulement les ensembles algébriques.

Définition. (*Faisceau de fonctions*)

Soit X un espace topologique. Un *faisceau de fonctions* sur X à valeurs dans k est la donnée pour tout U de X , d'un sous-ensemble $\mathcal{A}(U) \subseteq k^U$ l'ensemble des fonctions de $U \rightarrow k$ tel que pour tous ouverts $V \subseteq U$, $f \in \mathcal{A}(U) \implies f|_V \in \mathcal{A}(V)$ et des axiomes de recollement : si $U = \bigcup_{i \in I} V_i$ et pour tout $i \in I$, $f_i \in \mathcal{A}(V_i)$ tel que $f_i|_{V_i \cap V_j} = f_j|_{V_i \cap V_j} \in \mathcal{A}(V_i \cap V_j)$, alors les f_i se recollent (forcément) en $f \in \mathcal{A}(U)$!

Remarque. Les axiomes de séparation sont immédiats.

→ *Notation.* On note $\mathcal{A}(U) = H^0(U, \mathcal{A}) = \Gamma(U, \mathcal{A})$.

Définition. ()

Soit V un ensemble algébrique et $U \subseteq V$ un ouvert, $f : U \rightarrow k$ une fonction. On dit que f est *régulière* si pour tout $x \in U$, il existe $g, h \in \mathcal{O}(V)$ tel que $h(x_0) \neq 0$ et $f(x) = \frac{g(x)}{h(x)}$ pour tout $x \in U'$, avec h ne s'annulant pas sur U .

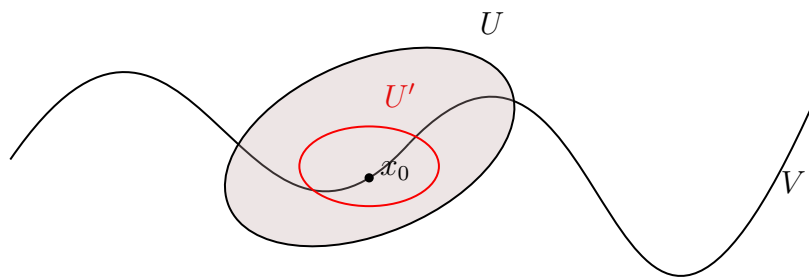


FIGURE 2.1.1 : Fonction régulière en un point : définition. —

Heuristique

On présente ces fonctions comme étant localement des fractions rationnelles.

→ *Notation.* On pose $\mathcal{O}_V(U)$ l'ensemble des fonctions régulières $U \rightarrow k$.

Fait

$U \rightarrow \mathcal{O}_V(U) \subseteq k^U$ est un faisceau.

C'est automatique, car la définition de la régularité est locale.

Proposition

$\mathcal{O}_V(V) = \mathcal{O}(V)$.

En conséquence, $\mathcal{O}_V(U_j) = \mathcal{O}_{U_h}(U_h) = \mathcal{O}(U_h) = \mathcal{O}(V)_h = \mathcal{O}(V)[h^{-1}] = \mathcal{O}(V)[X] / \langle Xh - 1 \rangle$.

▷ On a un morphisme $\psi: \mathcal{O}(V) \longrightarrow \mathcal{O}_V(V)$ en prenant $g = f$, $h = 1$ et $U' = V$ dans la

$$f \longmapsto f$$

définition.

Montrons l'injectivité de ψ . Elle est clair, car $\mathcal{O}(V) \subseteq k^{(V)}$ et $\mathcal{O}_V(V) \subseteq k^{(V)}$.

Montrons la surjectivité. Soit $f \in \mathcal{O}_V(V)$. Pour tout $x \in V$, il existe un ouvert U_x dans V et $g, h \in \mathcal{O}(V)$ avec h ne s'annulant pas sur U et telle que sur U_x , $f = \frac{g}{h}$. Or V est quasi-compact et les ouverts principaux forment une base de la topologie, donc on a un recouvrement $V = \bigcup_{i=1}^n NU_{h_i}$, avec $h_i \in \mathcal{O}(V)$ et, sur U_{h_i} , $f = \frac{g_i}{h_i}$. Sur $U_{h_i} \cap U_{h_j} = U_{h_i h_j}$, $f = \frac{g_i}{h_i} = \frac{g_j}{h_j}$ d'où $g_i h_j - g_j h_i = 0$ sur $U_{h_i h_j} \in \mathcal{O}(U_{h_i h_j}) = \mathcal{O}(V)_{h_i h_j}$ qui arrive si et seulement si $\exists n \in \mathbb{N} \quad (h_i h_j)^n (g_i h_j - g_j h_i) = 0 \in \mathcal{O}(V)$ sur V où l'on a utilisé une propriété de base de la localisation. Ici, l'anneau $\mathcal{O}(V)$ est réduit, donc on peut prendre $n = 1$. Ainsi $h_i^n h_j^{n+1} g_i = h_i^{n+1} h_j^n g_j$ d'où $\frac{g_i h_i^n}{h_i^{n+1}} = \frac{g_j h_j^n}{h_j^{n+1}}$. On peut supposer que n est le même pour toutes les paires (i, j) , quitte à la prendre maximal. On pose pour tout $i = 1, \dots, n$, $g'_i = h_i^n g_i$ et $h'_i = h_i^{n+1}$. Alors $U_{h'_i} = U_{h_i}$, $f = \frac{g'_i}{h'_i}$ sur U_{h_i} et $g'_i h'_j = g'_j h'_i$. On suppose donc $n = 0$. Pour définir l'antécédant de f par ψ , on fait une sorte de partition de l'unité : $V = \bigcup_{i=1}^n U_{h_i}$ d'où $\langle h_1, \dots, h_n \rangle = \mathcal{O}(V)$ et $\emptyset = \bigcap_i V_{h_i}$ d'où $a_1, \dots, a_n \in \mathcal{O}(V)$ telles que $1 = a_1 h_1 + a_2 h_2 + \dots + a_n h_n$. On pose $g = \sum_{i=1}^n a_i g_i \in \mathcal{O}(V)$. Vérifions que $g = f$. Il suffit de le faire sur tous les U_{h_i} . Sur U_{h_1} donc, $h_1 g = \sum a_i h_1 g_i = \sum a_i h_i g_1$ d'où $h_1 g = g_1$, d'où $g = \frac{g_1}{h_1} = f$ sur U_{h_1} . ■

Exercice 7

On prend $V = k^2$ et $U = V \setminus \{(0,0)\}$. montrer que $\mathcal{O}_V(U) = \mathcal{O}(V)$.

Rappel. Soit \mathcal{C} une catégorie, I un ensemble ordonné filtrant, par exemple \mathbb{N} . Si on a système inductif $i \in I, X_i \in \mathcal{C}$, $i \leq j$ implique $X_i \xrightarrow{f_{ij}} X_j \xrightarrow{\varphi_{jk}} X_k$. La limite inductive X est caractérisée par la propriété universelle $\text{Hom}(X, Y) = \lim \text{Hom}(X_i, Y)$ limite ensemble.

→ *Notation.* Soit X un espace topologique, \mathcal{O}_X un faisceau de fonctions. Pour $x \in X$, on pose

$$\mathcal{O}_{X,x} = \varinjlim_{U \text{ ouvert } \ni x} \mathcal{O}_X(U).$$

Si $a \in \mathcal{O}_{X,x}$, $a = (U, f)$ où $U \subseteq X$ ouvert contenant x , $f \in \mathcal{O}_X(U)$. On décrète la relation d'équivalence suivante, que $(U, f) = (U', f')$ s'il existe un ouvert $x \in V \subseteq U \cap U'$ avec $f|_V = f'|_V \in \mathcal{O}_X(V)$.

Proposition

Soit $V \subseteq k^n$ un ensemble algébrique, $x \in V$, correspondant à l'idéal maximal $\mathcal{M}_x \subseteq \mathcal{O}(V)$. Alors $\mathcal{O}_{V,w} = \mathcal{O}(V)_{\mathcal{M}_x}$ le localisé de $\mathcal{O}(V)$ en l'idéal premier \mathcal{M}_x . C'est A où $S = \mathcal{O}(V) \setminus \mathcal{M}_x$.

Proposition

Soit $x \in V$, $\mathcal{M}_x \subseteq \mathcal{O}(V)$. Alors on a un isomorphisme naturel du localisé de \mathcal{O}_V en \mathcal{M}_x : $\psi : \mathcal{O}(V)_{\mathcal{M}_x} \xrightarrow{\sim} \mathcal{O}_{V,x}$ l'anneau des germes de fonctions en x sur l'espace annelé (V, \mathcal{O}_V) .

▷ On a un morphisme $F: \mathcal{O}(V) \longrightarrow \mathcal{O}_{V,x} = \varphi_x$. Or $\varphi \in \mathcal{M}_x$ donc $\varphi(x) \neq 0$, donc $\varphi \mapsto \overline{(V, \varphi)}$

$\varphi_x = \overline{(U_\varphi, \varphi)}$ où $x \in U_\varphi$ et φ est inversible sur U_φ . On rappelle que l'ensemble des fonctions régulières sur U_φ est $\mathcal{O}(U_\varphi) = \mathcal{O}(V)[\varphi^{-1}] = \mathcal{O}(V)[X]/\langle X\varphi - 1 \rangle$. Donc $F(\mathcal{M}_x^c) \subseteq \mathcal{O}_{V,x}^\times$. Par propriété universelle de la localisation, on obtient

$$\begin{array}{ccc} \mathcal{O}(V) & \xrightarrow{F} & \mathcal{O}_{V,x} \\ & \searrow x \mapsto \frac{x}{1} & \nearrow \psi \\ & \mathcal{O}_{\mathcal{M}_x} & \end{array}$$

Montrons que ψ est surjective. Soit (U, f) , $U \ni x$ ouvert, un germe de fonction régulière en x . On remplace U par un ouvert principal U_h , où $h \in \mathcal{O}(V)$, $h(x) \neq 0$, ce qui est possible, car les ouverts principaux forment une base de la topologie de Zariski.

Soit $f \in \mathcal{O}_V(U_h) = \mathcal{O}_{U_h}(U_h) = \mathcal{O}(U_h) = \mathcal{O}[V][h^{-1}]$ qui donne $f = \frac{a}{h^r}$ (voyons bien que $x \in U_h \subseteq U \subseteq V$). On a $h \notin \mathcal{M}_x$. Ainsi, $\psi(\frac{a}{h^r}) = f$ où $\frac{a}{h^r} \in \mathcal{O}[V]_{\mathcal{M}_x}$. Or ψ est injective. Supposons $h \notin \mathcal{M}_x$, et $\psi(\frac{a}{h}) = 0$, $a \in \mathcal{O}(V)$, qui implique $\psi(a) = 0$. Montrons que $a = 0 \in \mathcal{O}(V)_{\mathcal{M}_x}$. Or $\psi(a) = 0$ signifie qu'il existe $x \in U \subseteq V$ ouvert, avec $a = 0$ sur U . On peut supposer $U = U_h$ principal avec $h(x) \neq 0$. Or $a = 0$ sur U_h équivaut à $a = 0 \in \mathcal{O}(U_h) = \mathcal{O}(V)[h^{-1}]$. Donc il existe $r \in \mathbb{N}$ tel que $h^r a = 0 \in \mathcal{O}(V) \Leftrightarrow a = 0 \in \mathcal{O}(V)_{\mathcal{M}_x}$. ■

On peut résumer cela avec le diagramme suivant :

$$\begin{array}{ccc} a \in \mathcal{O}(V) & \longrightarrow & \mathcal{O}_{V,x} \ni 0 \\ h \in \mathcal{M}_x \downarrow & & \nearrow \\ \mathcal{O}(V)[h^{-1}] & & \\ \downarrow & & \\ \mathcal{O}(V)_{\mathcal{M}_x} & & \end{array}$$

Exercice 8

Soit X une variété k -algébrique. Montrer que la k -algèbre $H^0(X, \mathcal{O}_X) = \mathcal{O}_X(X)$ est réduite. Supposons de plus qu'elle est finiment engendrée. Soit Y la variété telle que $\mathcal{O}(V) = H^0(X, \mathcal{O}_X)$. Construire un morphisme naturel $X \rightarrow Y$.

2.1.9 Variétés algébriques affines

On suppose ici $k = \bar{k}$.

Définition. (*Espace k -annelé*)

Un k -espace annelé est un couple formé d'un espace topologique X et des faisceaux d'anneaux de fonctions \mathcal{O}_X ($\mathcal{O}_X(U) \subseteq k^U$ des sous- k -algèbres).

Définition. ()

Un morphisme $(X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$ est : $\varphi : X \rightarrow Y$ continue, et $\forall U \subseteq Y$ ouvert, $\varphi_U^* : \mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(\varphi^{-1}(U))$ qui à $f \mapsto (f \circ \varphi) : \varphi^{-1}(U) \rightarrow k$ (i.e. pour tout $f \in \mathcal{O}_Y(U)$, on a $(f \circ \varphi) \in \mathcal{O}_X(\varphi^{-1}(U))$).

Par passage à la limite, on en déduit pour tout $x \in X$: $\varphi_x^* : \mathcal{O}_{Y, \varphi(x)} \rightarrow \mathcal{O}_{X, x}$. Ce dernier peut ne pas être un anneau local, mais c'est le cas si X est une variété algébrique.

Lemme

Soit $V \subseteq k^n$, soit $W \subseteq k^m$ des ensembles algébriques. On a une bijection $\text{App.Poly}(V, W) \rightarrow (\text{Hom}_{k\text{-esp.-ann.}}((V, \mathcal{O}_V), (W, \mathcal{O}_W)))$ qui vérifie bien la propriété des $F \mapsto f = F : V \rightarrow W$ morphismes. Dans l'autre sens, $f : V \rightarrow W$ qui satisfait la propriété des morphismes donne $f : V \rightarrow W$ polynomiale par factorisation.

Définition. (*Variété affine*)

Une variété sur k affine est un k -espace annelé isomorphe à (V, \mathcal{O}_V) pour un ensemble algébrique $V \in k^n$.

Fait

Les catégories suivantes sont équivalentes :

- ★ les k -variétés affines munis des morphismes d'espaces annelés ;
- ★ les k -ensembles algébriques avec App.Poly ;
- ★ la catégorie opposée des k -algèbres de type fini réduites munies des morphismes de k -algèbres.

La clôture de k intervient pour l'équivalence des deux dernières.

Remarque. Sans l'hypothèse $k = \bar{k}$, on peut définir une k -variété affine l'aide du spectre maximal de A . On pose $X = \text{SpMax}(A)$ où A est une k -algèbre de type fini réduite. On définit un faisceau \mathcal{O}_X de k -algèbres, de telle sorte que $\mathcal{O}_X(U_f) = A[f^{-1}]$ pour tout $f \in A$. Attention ! Si k n'est pas clos, $\mathcal{O}_X(U) \not\subseteq k^U$, car $f(x) \in A/\mathcal{M}_x$.

Fait

Une variété algébrique est un espace noethérien.

2.1.10 Sous-variétés, immersions**Définition. (*Sous-variété algébrique*)**

Soit (X, \mathcal{O}_X) un espace k -annelé. Soit $Y \subseteq X$ un sous-ensemble. On munit Y de la topologie induite et du faisceau. On dispose de $Y \hookrightarrow X$. On pose pour tout $V \subseteq Y$ ouvert : $\mathcal{O}_{X|Y}(V) = \{f : V \rightarrow k \mid \forall x \in V \exists U \subseteq X \text{ ouvert}, U \ni x \exists g \in \mathcal{O}_X(U) \mid f = g \text{ sur } V \cap U\}$.

Définition. (*Immersion*)

Un morphisme $(Z, \mathcal{O}_Z) \xrightarrow{\varphi} (X, \mathcal{O}_X)$ est une *immersion* si le morphisme induit φ_1 est un isomorphisme, dans le diagramme :

$$(Z, \mathcal{O}_Z) \xrightarrow[\varphi_1]{\sim} (\varphi(Z), \mathcal{O}_{X|\varphi(Z)}) \xrightarrow[\varphi_2]{\rightarrow} (X, \mathcal{O}_X).$$

Si $\varphi(Z) \subseteq X$ est fermé (resp. ouvert, resp. localement fermé), on dit que φ est une *immersion fermée* (resp. *ouverte*, resp. *localement fermée*).

2.1.11 Variétés algébriques abstraites**Définition. (*Variété algébrique*)**

Une *k-variété algébrique* (ou variété algébrique sur k) est un k -espace annelé (X, \mathcal{O}_X) tel qu'il existe un recouvrement fini par des ouverts $\bigcup_{i=1}^n X_i = X$ et $(X_i, \mathcal{O}_{X|X_i})$ est une k -variété affine pour chaque i . Un morphisme est un morphisme de k -espace annelé.

Théorème

Soit (X, \mathcal{O}_X) une k -variété. Soit (V, \mathcal{O}_V) une k -variété affine. Alors le morphisme naturel de $\text{Hom}_{k\text{-var}}(X, \mathcal{O}_X), (V, \mathcal{O}_V)$ vers $\text{Hom}_{k\text{-alg.}}(A = \mathcal{O}_V(V), \mathcal{O}_X(X) = \Gamma(X, \mathcal{O}_X))$ qui à $f : X \rightarrow Y$ donne $(\varphi : (\varphi \circ f))$ est un isomorphisme.

▷ Écrivons :

$$\begin{array}{ccc}
 \text{Hom}_{k\text{-alg.}}(A = \mathcal{O}_V(V), \mathcal{O}_X(X)) & \xleftarrow{\text{existe toujours}} & \text{Hom}_{k\text{-Var}}((X, \mathcal{O}_X)(V, \mathcal{O}_V)) \\
 \downarrow \text{restriction} & \xrightarrow{\quad} & \downarrow \varphi \mapsto (\varphi|_{X_i})_{i=1, \dots, n} \\
 \prod_{i=1}^n \text{Hom}_{k\text{-alg.}}(A, \mathcal{O}_X(X_i)) & \xleftarrow{\text{bijection dans le cas affine}} & \prod_{i=1}^n \text{Hom}_{k\text{-Var}}((X_i, \mathcal{O}_{X_i})(V, \mathcal{O}_V)) \\
 \downarrow \quad \downarrow & \xrightarrow{(f_1, \dots, f_n) \mapsto (f_j|_{X_i \cap X_j})} & \downarrow (f_1, \dots, f_n) \mapsto (f_i|_{X_i \cap X_j})_{i \neq j} \\
 \prod_{i=1}^n \text{Hom}_{k\text{-alg.}}(A, \mathcal{O}_X(X_i \cap X_j)) & \xleftarrow{\quad} & \prod_{i \neq j} \text{Hom}_{k\text{-alg.}}(X_i \cap X_j, V)
 \end{array}$$

et si $X_i \cap X_j$ est affine pour tous i, j (cette hypothèse est souvent vérifiée) alors on a construit la flèche verte par une chasse dans le diagramme. Dans le cas général, on écrit $X_i \cap X_j = \bigcup_{k=1}^N X_{i,j,k}$ avec $X_{i,j,k}$ affine et on se restreint aux $X_{i,j,k}$. (C'est un exemple d'égaliseur.) ■

Exemple

Soit k un corps algébriquement clos, et A une k -algèbre réduite et de type fini. Alors on peut désigner par $\text{Spm}(A)$ (ou $\text{SpecMax}(A)$, c'est pareil) deux choses. Soit c'est simplement l'ensemble des idéaux maximaux (autrement dit ici, les morphismes de k -algèbres $A \rightarrow k$, muni de la topologie de Zariski. Ou bien, c'est la k -variété associée : cela revient à munir l'espace topologique $\text{Spm}(A)$ de son faisceau de fonctions régulières défini en cours. Si $A = k[X_1, \dots, X_n]/I$, et si V est l'ensemble algébrique défini par I , c'est le k -espace annelé (V, \mathcal{O}_V) .

Exercice 9 (Critère d'affinité)

Remarque. $V = \text{SpMax}(A)$ est la variété affine associée à un k -algèbre A .

2.1.12 Construction des variétés par patching

Définition. (Condition de cocycles, recollement)

Pour $n \in \mathbb{N}$ et $i \in \llbracket 1, n \rrbracket$, on se donne (X_i, \mathcal{O}_{X_i}) des k -variétés et pour $i \neq j$, on se donne un ouvert $X_{i,j} \subseteq X_i$ et des isomorphismes de k -variétés $X_{i,j} \xrightarrow{\varphi_{i,j}} X_{j,i}$ avec une condition de compatibilité, dite de *cocycle* (condition inexistante de $n = 2$) : pour i, j, k trois unités distinctes notées ici 1, 2, 3,

$$X_{1,2} \cap X_{1,3} \xrightarrow{\varphi_{1,2}} X_{2,1} \cap X_{2,3} \xrightarrow{\varphi_{2,3}} X_{3,1} \cap X_{3,2}$$

qui se factorise en $\varphi_{1,3}$. On note ces intersections, dans l'ordre, cX_1, cX_2, cX_3 ,

Alors les X_i se recollent, *i.e.* il existe une k -variété X avec des ouverts $U_1, \dots, U_n \subseteq X$ et des sous-variétés $U_i \xrightarrow{f_i} X_i$ isomorphique compactibles aux φ_i :

$$\begin{array}{ccc} U_j \cap U_i & \xrightarrow{f_i} & X_{ij} \subseteq X_i \\ f_j \downarrow & \swarrow \varphi_{i,j} & \\ X_{ji} \subseteq X_j & & \end{array}$$

en notant $\varphi_{i,j} = f_j \circ f_i^{-1}$.

Lemme

Si $\iota_V : U_V \hookrightarrow V$ et $\iota_W : U_W \hookrightarrow W$ sont deux immersions ouvertes de variétés affines, alors $U_V \times U_W \rightarrow V \times W$ est une immersion ouverte.

▷ Décomposons : $U_V \times U_W \rightarrow U_V \times W \rightarrow V \times W$. On peut donc supposer $U_W = W$. On écrit $U_V = \bigcup_{i=1}^n U_{f_i}$ où les $f_i \in H^0(U, \mathcal{O}_V) = \mathcal{O}(V)$. Il suffit de traiter donc le cas où $U_V = U_f$ est principal. On écrit $U_V \times W = \bigcup_{i=1}^n (U_{f_i} \times W)$ avec les $U_{f_i} \times W$ ouverts. Or $\text{SpMax}(A[f_i^{-1}] \otimes_k B) = (A \otimes_k B)[(f_i \otimes 2)^{-1}]$, d'où $U_{f_i} \times W$ est un ouvert principal de $U_V \times W$. Pour conclure, remarquons que l'on peut recouvrir U par des ouverts qui sont principaux dans V et dans U . En effet, on peut plonger $H^0(V, \mathcal{O}(V)) \rightarrow H^0(U, \mathcal{O}_U)$ et $U_{f_i} \subseteq V$ égale $U_{\rho(f_i)} \subseteq U$. Ainsi, $U_{f_i} \times W \subseteq U_V \times W \subseteq V \times W$ est un recouvrement ouvert dans chacun des deux derniers termes. La nature locale des faisceaux fait vérifier leur condition automatiquement. ■

Propriété. (Produit de variétés algébriques)

Soit k un corps algébriquement clos. La catégorie des k -variétés algébriques admet des produits finis.

▷ Soient V, W deux k -variétés algébriques. Nous allons munir $V \times W$ d'une topologie qui en fait un k -espace annelé, qui en fait une k -variété.

Supposons $V = \text{SpMax}(A)$, $W = \text{SpMax}(B)$ affine avec A, B deux k -algèbres réduites de type fini. On a alors $V \times W = \text{SpMax}(A \otimes_k B)$. On a vu que c'est vrai ensemblistement. Rappelons que la catégorie des k -variétés affines est équivalente à la catégorie opposée des k -algèbres réduites de type fini et que $(A, B) \mapsto A \otimes_k B$ est un co-produit dans la catégorie des k -algèbres.

Prenons $W = \text{Spec}(B)$ et V quelconque. On écrit $V = \bigcup_{i=1}^n V_i$ où V_i est un ouvert affine. Alors

$V_i \times W$ existe par ce qui précède. On recolle les $V_i \times W$. Ensemblistement, $V \times W = \bigcup_{i=1}^n (V_i \times W)$. On

a que $(V_i \cap V_j) \times W$ est ouvert dans $V_i \times W$; pour le voir, écrire $V_i \cap V_j = \bigcup_{k=1}^N U_k$ avec U_k ouvert affine de $V_i \cap V_j$. Il suffit donc de montrer que les $U_k \times W$ sont ouverts affines dans $V_i \times W$.

En utilisant le lemme précédent, si W est affine, les k -variétés affines $V_i \times W$ se recollent en une k -variété, qui est $V \times W$. Récapitulons : $V_i \times W$ et $V_j \times W$ ont pour intersection $(V_i \cap V_j) \times W$ qui est recouverte par les $U_k \times W$ qui sont des ouverts de $V_i \times W$ et $V_j \times W$.

Reste le cas général. On écrit $W = \bigcup_{i=1}^n W_i$ avec les W_i affines. Alors $W \times W = \bigcup_{i=1}^n V \times W_i$ avec les $V \times W_i$ des k -variétés. Comme précédemment, on vérifie que les $(V \times W_i)$ se recollent.

Vérifions la propriété universelle du produit. Montrons que pour toute X k -variété, on a $\text{Hom}_{k\text{-Var}}(X, V \times W) = \text{Hom}_{k\text{-Var}}(X, V) \times \text{Hom}_{k\text{-Var}}(X, W)$. Si $X = \text{SpMax}(C)$, $V = \text{SpMax}(A)$, $W = \text{SpMax}(B)$, on retrouve une propriété connue pour le produit tensoriel de k -algèbres. Dans le cas général, on définit $\text{Hom}(X, V \times W) \xrightarrow{\varphi} \text{Hom}(X, V) \times \text{Hom}(X, W)$ comme suit : soit $h : X \rightarrow V \times W$. On écrit $V = \bigcup_{i=1}^n V_i$ et $W = \bigcup_{j=1}^n W_j$ affines. Alors on sait que $V_i \times W_j$ affine est un recouvrement ouvert de $V \times W$. Posons $X_{ij} = h^{-1}(V_i \times W_j) \subseteq X$ ouvert. On prend un recouvrement par des ouverts affines $X_{ijk} = \bigcup_{k=1}^N X_{ijk}$ avec les X_{ijk} affines. On a entre variétés affines $h|_{X_{ijk}} : X_{ijk} \rightarrow V_i \times W_j$. Par la propriété dans le cas affine, on récupère $f_{ijk} : X_{ijk} \rightarrow V_i$ et $g_{ijk} : X_{ijk} \rightarrow W_j$. Les (X_{ijk}) forment un recouvrement ouvert de X et les V_i un recouvrement de V . Ainsi, les f_{ijk} se recollent par nature locale des morphismes entre faisceaux : $f_{ijk} = f_{i'j'k'}$ sur $X_{ijk} \cap X_{i'j'k'}$. On obtient $f : X \rightarrow V$ et $g : X \rightarrow W$. On a donc construit $\Phi(h) = (f, g)$. Remarque : f et g sont indépendantes du choix de recouvrement. ■

Remarque. Cette preuve catégorique qui fonctionnerait en théorie des schémas est cependant plus complexe que le constat suivant : on peut définir ensemblistement $(f, g) \mapsto (x \mapsto (f(x), g(x)))$ de $\text{Hom}(X, V) \times \text{Hom}(X, W) \rightarrow \text{Hom}(X, V \times W)$, car dans la catégorie des k -variétés, l'application sous-jacente à un morphisme le détermine (ce qui n'est pas le cas pour des schémas).

Remarque. On a les projections $\pi_V : V \times W \rightarrow V$ et $\pi_W : V \times W \rightarrow W$ qui sont des morphismes et $\Phi(h) = (\pi_V \circ h, \pi_W \circ h)$.

2.1.13 Fonctions rationnelles

Propriété. (*Corps des fractions isomorphes*)

Soit k un corps et soient A, B deux k -algèbres de type fini intègres, telles que $\text{Frac}(A)$ et $\text{Frac}(B)$ sont isomorphes comme extensions de corps de k . Alors il existe $a \in A$ et $b \in B$ non nuls tels que $A[\frac{1}{a}]$ et $B[\frac{1}{b}]$ soient isomorphes.

Elles sont un peu l'analogue des fonctions méromorphes.

Définition. (*Fonctions rationnelles*)

Soit V une k -variété algébrique, très souvent supposée irréductible. On pose $\mathcal{M}(V) = k(V) = \{(U, f) \mid U \subseteq V \text{ ouvert dense i.e. non vide car } V \text{ est irréductible}\} / (U, f) \sim (U', f') \text{ si } f = f' \text{ sur } U \cap U'$.

C'est le *corps des fractions rationnelles* sur X .

Fait

Si $U \subseteq V$ est un ouvert affine, $U = \text{SpMax}(A)$ où A est une k -algèbre de type fini (intègre, car V est irréductible), alors il y a un isomorphisme naturel $\text{Frac}(A) \simeq k(V)$.

En exercice.

Remarque. Si l'on suppose toutes les variétés irréductibles, alors dans la définition d'application rationnelle, si $\varphi = \varphi'$, alors $\varphi = \varphi'$ sur $U \cap U'$, en fait sans autre hypothèse (pas besoin de séparation, surtout qu'on en sait pas ce que cela signifie!).

Propriété

Soient V et W des k -variétés irréductibles. Les propositions suivantes sont équivalentes :

- (i) V et W sont birationnelles ;
- (ii) les corps de fonctions $\mathcal{M}(V)$ et $\mathcal{M}(W)$ sont isomorphes en tant qu'extensions de k ;
- (iii) il existe deux ouverts affines $U_V \subseteq V$ et $U_W \subseteq W$ tels que U_V et U_W sont isomorphes comme k -variétés.

Exemple fondamental. (L'espace projectif \mathbb{P}^n)

On travaille dans la k -algèbre $R = k[\frac{X_i}{X_j}, i, j \in \llbracket 0, n \rrbracket] \subseteq k[X_0, \dots, X_n] \simeq k[T_i^{\pm 1}, i \in \llbracket 1, n \rrbracket]$. On pose $R_i = k[\frac{X_j}{X_i}, j \in \llbracket 0, n \rrbracket, j \neq i] \simeq k[T_1, \dots, T_n]$. Ainsi $R_{ij} = \langle R_i, R_j \rangle = k[\frac{X_k}{X_i}, \frac{X_k}{X_j}, k \in \llbracket 0, n \rrbracket] \simeq k[T_1, \dots, T_{n-1}, T_n, T_n^{-1}]$, sous-anneaux de R . Posons $X_i = \text{SpMax}(R_i) \simeq \mathbb{A}^n$ l'espace affine k^n . D'autre part $X_{ij} = \text{SpMax}(R_{ij}) \simeq \mathbb{A}^{n-1} \times \mathbb{G}_m = k^{n-1} \times k^*$, où $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$. Alors les X_i se recollent, le long des ouverts $X_{ij} \subseteq X_i$ principaux. Les conditions de cocycles sont automatiquement vérifiées, car au niveau des corps de fonctions $k(X_i) = \mathcal{M}(X_i) = k(\frac{X_j}{X_i}, i, j \in \llbracket 0, n \rrbracket) = R$. Les $\varphi_{i,j}$ sont l'identité.

On a $\mathbb{P}^n(k) = (k^{n+1} \setminus \{0\})/k^\times = \text{Hom}_{k\text{-var}}(\star, \mathbb{P}^n) = (\mathbb{A}^{n+1} \setminus \{0\})/\mathbb{G}_m$. Il y a une flèche facile $F : (k^{n+1} \setminus \{0\})/k^\times \rightarrow \mathbb{P}^n$. Soit $(\lambda_0, \dots, \lambda_n)$. Soit $i \in \{0, \dots, n\}$ avec $\lambda_i \neq 0$. On peut supposer $\lambda_i = 1$. On pose $F(\lambda_0, \dots, 1, \dots, \lambda_{i-1}, \lambda_n) = X_i$. On vérifie que c'est indépendant du choix de i (cela découle du choix des $\varphi_{i,j}$) : en remplaçant $X_{i,j} \rightarrow X_{j,i}$, $k[\frac{X_j}{X_i}][(\frac{X_j}{X_i})^{-1}] = k\frac{X_i}{X_j}^{-1}$.

Exercice 10

Soit $V = \text{SpMax}(A)$ une variété affine. Trouver une condition sur A pour avoir $\text{Hom}_k(V, \mathbb{P}^n) = \{(a_0, \dots, a_n) \mid \text{l'un des } a_i \in A^\times\}/A^\times$.

Lemme

Soient V, W deux variétés algébriques irréductibles. Alors $\Phi \rightarrow \Phi^*$ induit une bijection

$$\text{Rat.Dot}(V, W) \xrightarrow{\sim} \text{Hom}_{k\text{-alg.}}(k(W), k(V))$$

avec $\mathcal{M}(W) = k(W)$ et $\mathcal{M}(V) = k(V)$ et $\varphi : k(W) \rightarrow k(V)$ où $k(V) = \text{Frac}(\mathcal{O}_V(U_V)) \supseteq \mathcal{O}_V(U_V)$, $U_V \subseteq V$ ouvert affine de V et $k(W) = \text{Frac}(\mathcal{O}_W(U_W)) \supseteq \mathcal{O}_W(U_W)$ où U_W est un ouvert affine de W .

▷ Comme $\mathcal{O}_W(U_W)$ est de type fini sur k , il existe $a \in \mathcal{O}_V(U_V)$ tel que $\varphi(\mathcal{O}_W(U_W)) \subseteq \mathcal{O}_V(U_V)[a^{-1}]$ par le lemme précédent, en prenant un dénominateur commun. On peut donc remplacer V par $U_a = D(a) \subseteq V$ et W par U_W . On se ramène au cas $\varphi(\mathcal{O}_W(W)) \subseteq \mathcal{O}_V(V)$, V, W affines, qui donne φ correspondant à $\Phi : V \rightarrow W$. ■

2.1.13.1 Applications birationnelles**Théorème**

On suppose k séparablement clos. Soit V une k -variété irréductible de dimension d . Alors V est k -birationnelle à une hypersurface $H \subseteq \mathbb{A}^{d+1}$, i.e. $H = V(f)$ où $f \in k[X_1, \dots, X_{d+1}]$.

▷ Comme k est séparablement clos, on peut écrire $k(V) \supseteq k(x_1, \dots, x_d) \supseteq k$ où la première extension est algébrique, finie et séparable et la deuxième transcendantale pure. Par le théorème de l'élément primitif, $k(V) = k(x_1, \dots, x_d)[T]/\langle P \rangle$ où $P \in k[x_1, \dots, x_d][T]$. Ainsi $f(x_1, \dots, x_{d+1}) = P(x_{d+1})$. ■



Ceci ne trivialise pas du tout la géométrie algébrique en la ramenant aux études des hypersurfaces, car la birationalité n'est pas géniale. Par exemple, un espace projectif est birationnel à l'espace affine correspondant, pourtant, géométriquement, ils sont très différents.

2.1.13.2 Théorème de constructibilité de Chevalley

Des nombreux théorèmes de constructibilité, voici le plus simple.

Propriété. (Caractère localement fermé)

Un sous-ensemble d'un espace topologiquement est localement fermé si et seulement si c'est l'intersection d'un ouvert et d'un fermé.

Définition. (Sous-ensemble constructible)

Soit X un espace topologique. Un sous-ensemble C de X est *constructible* si C est une réunion finie d'ensembles localement fermés.

Remarque. Un constructible d'un fermé est constructible.

Contre-exemple. (*Constructible non localement fermé*)

Soit k^2 un corps, par exemple $k = \mathbb{C}$, muni de la topologie de Zariski. Alors $(k^* \times k) \cup \{(0,0)\}$ est constructible, mais n'est pas localement fermé. \square

Lemme. (*Constructibilité par un recouvrement*)

Soient X un espace topologique, C une partie de X et $(W_i)_{i \in I}$ un recouvrement ouvert fini de C . Alors C est constructible si et seulement si $C \cap W_i$ est constructible dans W_i pour tout $i \in \llbracket 1, n \rrbracket$.

L'image d'un morphisme n'est pas forcément une variété (garder en tête l'exemple $(x, y) \mapsto (x, xy)$, mais il n'est pas trop méchant non plus comme le montre le

Théorème. (*Théorème de constructibilité de Chevalley*)

Soit $\varphi : V \rightarrow W$ un morphisme de variétés. Alors si C est constructible dans V , $\varphi(C)$ est constructible dans W .

▷ On se ramène à $C = V$, à W affine et à V affine par un lemme de recouvrement sur la constructibilité. Enfin, on peut supposer V irréductible et φ dominant. Montrons :

Lemme

Soit φ un morphisme dominant de $V \rightarrow W$ des variétés irréductibles. Alors l'image de V par φ contient un ouvert de W .

▷ On écrit $V = \text{SpMax}(B)$ et $W = \text{SpMax}(A)$ où A, B sont des k -algèbres intègres de type fini. φ est donné par $\varphi^* : A \hookrightarrow B$ de k -algèbres injectif. On a donc le diagramme

$$\begin{array}{ccccc} A & \longrightarrow & A[x_1, \dots, x_d] & \longrightarrow & B \\ \downarrow & & & & \downarrow \\ K = \text{Frac}(A) & \longrightarrow & K' = K(x_1, \dots, x_d) & \longrightarrow & L = \text{Frac}(B) \end{array}$$

commutatif, où $B = k[y_1, \dots, y_N]$. On peut trouver des équations $0 = y_i^{M_i} + \lambda_{i, M-1} y_i^{M-1} + \lambda_{i, M-2} y_i^{M-2} + \dots + \lambda_{i, 0}$ pour i allant de 1 à N , avec les $\lambda_{i, j} \in K'$. On peut exhiber un dénominateur commun $\lambda_{i, j} = \frac{a_{i, j}}{a}$ où $a_{i, j}$ et a sont dans A' . Ainsi $A \rightarrow A[X_1, \dots, X_d][\frac{1}{a'}] \rightarrow B[\frac{1}{a'}]$ où le dernier morphisme est fini, donc injectif. On en déduit que l'ouvert principal $V \supseteq \tilde{U} \twoheadrightarrow U \subseteq_{\text{ouvert principal}} W \times \mathbb{A}^d \xrightarrow{\pi_W} W = \text{SpMax}(A)$. Ainsi, $\text{Im}(\varphi) \supseteq \varphi(\tilde{U}) = \pi_W(U)$. Maintenant que l'on s'est ramené à une projectif, reste à constater que $\pi_W(U)$ est un ouvert non vide de W . On peut le calculer explicitement, car $\pi_W(U) = \bigcup_{i \in I} D(a_i)$ où

$$a' = \sum_{i \in I \subseteq \mathbb{N}^d} a_i X^i \text{ où } a_i \neq 0. \blacksquare$$

On raisonne par récurrence sur la dimension. ■

2.1.14 Le cas $k \neq \bar{k}$: comment se ramener à un corps algébriquement clos avec un peu de théorie de Galois

2.1.14.1 Variétés sur un corps parfait

C'est très pratique : pour étudier des courbes elliptiques sur \mathbb{Q} , ou sur \mathbb{F}_p , on a affaire à un corps parfait mais pas algébriquement clos. On utilise donc le principe de la *descente galoisienne* exposé ci-dessous. On rappelle qu'un corps k est parfait si sa clôture algébrique \bar{k} est égale à sa clôture séparable k_s qui est la réunion de ses sous-extensions finies

En toute généralité, k admet une clôture séparable k_s définie à isomorphisme près, mais à isomorphisme non unique près. Cette non-canonicité est encodée par le groupe de Galois : $G = \text{Gal}(k_s/k) = \{\sigma \in \text{Aut}(k_s) \mid \sigma|_k = \text{id}_k\}$. De plus, on peut pour beaucoup de questions se ramener à une extension galoisienne finie l/k , cas que nous traitons donc d'abord. On prend $G = \text{Gal}(l/k)$.

Fait

$k = H^0(G, l) = \{x \in l \mid \forall \sigma \in G \mid \sigma x = x\}$ l'ensemble des points fixes sous l'action de G .

Le but est d'étendre cela aux espaces vectoriels, et le gros du travail sera fait.

Définition. ()

Un (G, l) -module, *i.e.* un l -espace vectoriel avec une action semi-linéaire de G , est un l -ev W avec une action de G par automorphismes de groupes abéliens tel que pour tous $\sigma \in G$, $\sigma(x.w) = \sigma(x)\sigma(w)$ pour tous $w \in W, x \in l$.

Un morphisme de (G, l) -modules est une application linéaire compatible avec l'action de groupe.

Théorème. (Lemme de Speiser)

On a un foncteur

$$\begin{aligned} k\text{-Vect} &\longrightarrow (G, l)\text{-Mod} \\ V &\longmapsto l \otimes_k V \end{aligned}$$

avec l'action de G définie sur un tenseur pur par $\sigma(x \otimes w) = \sigma(x) \otimes w$.

C'est une équivalence de catégories. De plus, son quasi-inverse est donnée par $W \mapsto H^0(G, W)$.

Vérifions-le. On a l'isomorphisme de (l, G) -modules $l \otimes_k H^0(G, W) \rightarrow W, x \otimes w \mapsto x.w$. On peut d'abord se ramener au cas des dimensions finies puis le reste viendra.

On détaille la démonstration dans le cas \mathbb{C}/\mathbb{R} qui permet donc de faire de la géométrie algébrique réelle à partir de la géométrie algébrique complexe. Notons C_2 son groupe de Galois. Un (\mathbb{C}, C_2) -module W est un \mathbb{C} -espace vectoriel et une involution anti-linéaire $J : W \rightarrow W$ vérifiant $J(ix) = -iJ(x)$ et \mathbb{R} -linéaire, avec $J^2 = id$. Puisque J annule $X^2 - 1$, $W = W_+ \oplus W_-$ les sous-espaces propres associés respectivement aux valeurs 1 et -1. On a $W_+ = H^0(G, W)$. Remarquons que $W_- = iW_+$. Par suite, $H^0(G, W)$ engendre W comme l -espace vectoriel.

Tout cela s'adapte aux extensions galoisiennes infinies très facilement, en particulier à k_s/k , $\Gamma = \text{Gal}(k_s/k)$ groupe de Galois absolu. Un (Γ, k_s) -module est la même chose plus une condition de continuité : pour tout $w \in W$, le sous-groupe $\Gamma_w = \{\sigma \in \Gamma \mid \sigma w = w\}$ est ouvert pour la topologie (discrète) de Krull. On montre que cette condition est équivalente à ce qu'il existe l/k une sous-extension finie avec $\Gamma_w = \text{Aut}_l(k_s) \subseteq \Gamma$.

Ainsi, dans l'idée, une k -variété sur un corp parfait est une k_s -variété munie d'une adction semi-linéaire de Γ .

Fait

Le lemme de Speiser induit une équivalence entre les k -algèbres de type fini réduites et les k_s -algèbres de type fini réduites munies d'une action semi-linéaire continue du groupe de Galois par automorphismes de k -algèbres.

Exercice 11

Justifions : $k_s \otimes_k A$ est réduite dès que A est réduite. De même, $H^0(G, B)$ est de type fini dès que B est de type fini.

Définition. (Variété sur un corps parfait)

Voici un complément concernant les variétés sur un corps parfait k . [Rappel : comme k est parfait, une clôture séparable de k en est aussi une clôture algébrique : $\bar{k} = k_s$] Soit $\Gamma := \text{Gal}(\bar{k}/k)$. Soit X une \bar{k} -variété. Une **donnée de descente** (galoisienne) sur X est définie comme suit. Pour chaque $\sigma \in \Gamma$, on se donne un isomorphisme de \bar{k} -variétés

$$\sigma X \xrightarrow{\varphi_\sigma} X,$$

tel que, pour tous $\sigma, \tau \in \Gamma$, la composition

$$\sigma\tau X \xrightarrow{\sigma\varphi_\tau} X \xrightarrow{\varphi_\sigma} X$$

est égale à $\varphi\sigma\tau$. Cette relation

$$\varphi\sigma\tau = \varphi\sigma \circ {}^\sigma\varphi\tau$$

est appelée "condition de cocycle". Souvenez-vous que ${}^\sigma X = X$ en tant qu'espace topologique. La condition de cocycle implique donc qu'on a une **action de groupe** de Γ sur l'espace topologique X , par homéomorphismes. [Dans notre contexte, cette action détermine la donnée de descente, mais cela n'est plus vrai dans le contexte des schémas].

On demande en plus une "condition de continuité", sous la forme qui suit. Pour tout ouvert affine $U \subset X$, le sous-groupe $\text{Stab}(U) \subset \Gamma$, formé des σ tels que $\sigma(U) = U$, doit être ouvert (pour la topologie de Krull du groupe profini Γ). Cela signifie simplement qu'il existe une sous-extension $k \subset l \subset \bar{k}$, avec l/k finie, telle que $\text{Stab}(U) = \text{Gal}(\bar{k}/l)$. [Notez que l/k dépend de l'ouvert affine U . Mais on peut prendre une même extension fine l/k qui marche pour tous les ouverts d'un recouvrement **fini** donné de X , par des ouverts affines.] On obtient en conséquence une action semi-linéaire de $\text{Gal}(\bar{k}/l)$ sur la \bar{k} -algèbre $A := \mathcal{O}_V(U)$. Comme dans l'énoncé général du Lemme de Speiser, on demande encore une condition de continuité : pour tout $a \in A$, $\text{Stab}(a) \subset \text{Gal}(\bar{k}/l)$ doit être un sous-groupe ouvert. Plus simplement : on peut demander que A soit isomorphe, avec l'action semi-linéaire de $\text{Gal}(\bar{k}/l)$, à une \bar{k} -algèbre de la forme $\bar{k} \otimes_l B$, où B est une l -algèbre.

Enfin, on demande une condition topologique sur X , pour assurer que la notion de k -variété algébrique qu'on aura ainsi définie, coïncide avec la notion de " k -schéma séparé, réduit et de type fini". Cette condition est : X est séparée (en tant que \bar{k} -variété), et il existe un recouvrement de X par des ouverts affines, et chacun stable par l'action de Γ . Cette condition est automatiquement vérifiée, si X est une variété quasi-projective (=localement fermée dans un espace projectif \mathbb{P}^n .) Voilà donc la définition générale d'une "donnée de descente" (φ_σ), sur une \bar{k} -variété X . On dit que X , munie de cette donnée de descente, est une k -variété. Un morphisme entre deux k -variétés, est un morphisme de \bar{k} -variétés qui est compatible aux données de descentes. [Ecrivez le diagramme commutatif qui exprime cela, si ce n'est pas clair pour vous]

Retour à ce qui est au programme de l'examen, quand $k = \mathbb{R}$. Une donnée de descente comme ci-dessus n'est rien d'autre qu'une "anti-involution" $X \xrightarrow{\varphi} \bar{X}$, où \bar{X} est la variété conjuguée de X , telle que définie en cours. Rappel : "anti-involution" signifie que $\bar{\varphi} = \varphi^{-1}$. Ceci est l'analogue algébrique de la notion de "fonction anti-holomorphe" (vs "fonction holomorphe"). Si (X, φ) est une \mathbb{R} -variété, un \mathbb{R} -point de X est un point fixe de φ . [Plus généralement mais pas au programme : si $(X, (\varphi_\sigma))$ est une k -variété, un k -point de X est un élément de $H^0(\Gamma, X)$, un point fixe de Γ agissant sur l'espace topologique X].

Exercice 12

Soit $a, b \in \mathbb{R}$. Définir rigoureusement la \mathbb{R} -variété affine $C(a)$, donnée par l'équation $X^2 + Y^2 = a$, comme sous-variété fermée de \mathbb{R}^2 . ("cercle de rayon a "). A quelle condition

$C(a)$ et $C(b)$ sont-elle isomorphes comme \mathbb{C} -variétés ? Et comme \mathbb{R} -variétés ?

2.2 Géométrie des variétés algébriques

2.2.1 Dimension des variétés algébriques

2.2.1.1 Rappels sur les degrés de transcendance

Définition. (*Base de transcendance*)

Pour toute extension de corps L de K , une famille d'éléments de L est une *base de transcendance* si elle est algébriquement indépendante sur K et si elle n'est strictement contenue dans aucune famille algébriquement indépendante de L . (Une famille \mathcal{F} d'éléments de L est dite *algébriquement indépendante* sur K si pour tous $x_1, \dots, x_n \in L$, il n'existe pas de polynôme non nul $P \in K[X_1, \dots, X_n]$ tel que $P(x_1, \dots, x_n) = 0$.)

Théorème. (*Existence de bases de transcendance*)

Pour tout corps K , pour toute extension transcendante L de K (c'est-à-dire, qui n'est pas algébrique (c'est-à-dire qu'il existe un élément non algébrique)), il existe des bases de transcendance de L sur K .

▷ Il s'agit encore une fois d'appliquer le lemme de Zorn. On considère l'ensemble \mathcal{F} des familles d'éléments de L algébriquement indépendantes sur K . Cet ensemble est inductif. En effet, il est non vide par définition d'une extension transcendante : il existe un élément α de L non algébrique sur K , et sa famille $\{\alpha\}$ est algébriquement indépendante sur K . Soit maintenant C une chaîne de \mathcal{F} , c'est-à-dire un ensemble de familles algébriquement indépendantes sur K totalement ordonnées pour l'inclusion. Leur réunion est encore algébriquement indépendante sur K , et c'en est trivialement un majorant. Montrons-le. Cette chaîne, on peut l'écrire $C = \{\mathcal{A}_i \mid i \in I\}$ où I est totalement ordonné, avec donc pour tous $i, j \in I$, $i \leq j \implies \mathcal{A}_i \subseteq \mathcal{A}_j$. Notons $\mathcal{A} = \bigcup_{i \in I} \mathcal{A}_i$. Pour tous $x_1, \dots, x_n \in \mathcal{A}$, pour tout $j \in \llbracket 1, n \rrbracket$, il existe $i_j \in I$ tel que $x_j \in \mathcal{A}_{i_j}$. Soit $i_0 = \max_{1 \leq j \leq n} i_j$. Puisque la famille $(\mathcal{A}_i)_{i \in I}$ est totalement ordonnée, on a $x_1, \dots, x_n \in \mathcal{A}_{i_0}$. La famille \mathcal{A}_{i_0} étant algébriquement indépendante, on en déduit qu'il n'existe pas de polynôme non nul $P \in K[X_1, \dots, X_n]$ tel que $P(x_1, \dots, x_n) = 0$. Ainsi \mathcal{A} est algébriquement indépendante.

Ainsi, il existe un élément maximal de \mathcal{F} . Par définition, c'est une base de transcendance de L sur K . ■

Remarque. Dans le cas fini, l'existence est donnée par le lemme de normalisation de Noether.

Théorème. (Caractérisation des bases de transcendance)

Pour tout corps K , pour tout extension transcendante L de K , $(\xi_i)_{i \in I}$ est une base de transcendance de L sur K si et seulement si les ξ_i sont algébriquement indépendants et L est algébrique sur $K(\xi_i)_{i \in I}$.

▷ C'est immédiat : si l'extension n'était pas algébrique, il y aurait un $\eta \in L$ transcendant sur $K(\xi_i)_{i \in I}$; mais alors la famille obtenue en rajoutant η aux $(\xi_i)_{i \in I}$ est encore algébriquement indépendante, contredisant la maximalité de la famille $(\xi_i)_{i \in I}$. ■

On peut vérifier le théorème suivant :

Théorème. (Définition du degré de transcendance)

Toutes les bases de transcendance d'une extension de corps ont le même cardinal.

Définition. (Degré de transcendance)

On appelle *degré de transcendance* de l'extension L/K , le cardinal commun à toutes les bases de transcendance de L/K .

C'est la cardinalité maximale des sous-ensembles algébriquement indépendants de L/K .

2.2.1.2 Théorie de la dimension algébrique**Définition. (Dimension d'une variété algébrique)**

Soit V une variété algébrique irréductible. On définit sa *dimension* en tant que variété, comme le degré de transcendance $\deg \operatorname{tr}(K(V)/K) := \dim(V)$.

Remarque. Il est illusoire de considérer un sous-ensemble algébrique quelconque : un point et une droite réunis, forment un sous-ensemble algébrique (une variété au sens large), mais « toutes les parts n'ont pas la même dimension ».

Exemples. (Dimension des variétés algébriques)

1. $\dim(\mathbb{A}^n) = \dim(\mathbb{P}^n) = \deg \operatorname{tr} K(X_1, \dots, X_n)/K = n$. (En effet, ils ont le même corps des fonctions.)
2. La dimension coïncide dans le cas des espaces vectoriels en particulier.
3. Si U est un ouvert non vide de V , $\dim(U) = \dim(V)$.
4. (*Cas des hypersurfaces*) Soit $f \in K[X_1, \dots, X_n] \setminus K$ irréductible. Alors si $V = \{x \in \mathbb{A}^n \mid f(x) = 0\}$, $\dim(V) = n - 1$.

On a $K[V] = K[X_1, \dots, X_n]/(f) = K[x_1, \dots, x_n]$. Disons que X_n apparaît dans f : $f = X_n^d f_0(X_1, \dots, X_{n-1}) + \dots + f_d(X_1, \dots, X_{n-1})$ où $f_0 \neq 0$. Or X_n est algébrique sur $K(x_1, \dots, x_{n-1})$, car $x_n^d f_0(x_1, \dots, x_{n-1}) + \dots + f_d(x_1, \dots, x_{n-1}) = 0$. Ainsi $\deg \operatorname{tr}(K(V)/K) \leq n - 1$, car les x_1, \dots, x_{n-1}

sont algébriquement indépendants. Sinon, il existerait $g(x_1, \dots, x_{n-1}) = 0$, $g \in K[X_1, \dots, X_{n-1}]$, et l'on en déduirait $g(X_1, \dots, X_{n-1}) \in (f)$, donc $f \mid g$ dans $K[X_1, \dots, X_n]$, contradiction. Ainsi $\deg \text{tr}(\text{Frac}(K[V])) = n - 1$.

5. On peut démontrer (en exercice) que $\dim(V \times W) = \dim(V) + \dim(W)$.

Proposition. (*Dimension d'une sous-variété algébrique*)

Soient $Y \subseteq V$ deux variétés affines, avec Y fermée dans V . Alors $\dim(Y) \leq \dim(V)$, avec égalité, si et seulement si, $Y = V$.

▷ On a un morphisme injectif $j : Y \hookrightarrow V \subseteq \mathbb{A}^n$. Aussi $I_V \subseteq I_Y$ et $j^* : K[V] = K[X_1, \dots, X_n]/I_V \rightarrow K[Y] = K[X_1, \dots, X_n]/I_Y$ résulte de la factorisation de la flèche canonique $K[X_1, \dots, X_n] \rightarrow K[X_1, \dots, X_n]/I_Y$ surjective, donc est surjective. Son noyau est I_Y/I_V . On peut choisir $y_1, \dots, y_r \in K[Y]$ qui forment une base de transcendance de $K(Y)/K$, avec $r = \dim(Y)$, quitte à éliminer les dénominateurs, car $r < \infty$. Il existe $x_1, \dots, x_r \in K[V]$ tels que $j^*x_i = y_i$ pour chaque i et les x_1, \dots, x_r sont algébriquement indépendants. En effet, si $F(x_1, \dots, x_r) = 0$ pour $F \in K[X_1, \dots, X_r]$. On en déduirait $j^*(F(x_1, \dots, x_r)) = F(y_1, \dots, y_r) = 0$, donc $F = 0$, donc $\deg \text{tr} K(V) = \dim(V) \geq r$.

$\dim(V) = \dim(Y)$ si et seulement si x_1, \dots, x_r est une base de transcendance de $K(V)/K$. Par le lemme de Noether, quitte à remplacer x_1, \dots, x_r par $x'_i = \sum a_{ij}x_j$, on peut supposer $K[V]/K[x_1, \dots, x_r]$ extension entière d'anneaux (qui sont des K -algèbres). On veut montrer que, dans ce nouveau cas, elle est en fait injective, soit $\text{Ker}(j^*) = \{0\}$. Alors on aurait j^* un isomorphisme (de K -algèbres) donc $j : Y \hookrightarrow X$ un isomorphisme, d'où $Y = V$. Soit donc $u \in \text{Ker}(j^*) \subseteq K[V]$. u est entier sur $K[x_1, \dots, x_r]$, donc racine de $T^d + p_{d-1}(x_1, \dots, x_r)T^{d-1} + \dots + p_0(x_1, \dots, x_r) = 0$, supposée irréductible tant qu'à faire, avec les $p_i \in K[x_1, \dots, x_r]$. On y applique $j^* : j^*(u)^d + p_{d-1}(y_1, \dots, y_r)j^*(u)^{d-1} + \dots + p_0(y_1, \dots, y_r) = 0$ où $p_0(y_1, \dots, y_r) = 0$ donc le reste des termes s'annule, donc l'équation est $T = 0$, donc $u = 0$. ■

On généralise ce que l'on a vu pour \mathbb{A}^n grâce à un théorème dû à Krull :

Théorème. (*Théorème des idéaux principaux de Kull, Hauptidealsatz*)

Soit V une variété affine et $f \in K[V] \setminus \{0\}$. Alors toutes les composantes irréductibles de $V(f) = \{x \in V, f(x) = 0\}$, si $V(f) \neq \emptyset$, sont de dimension $\dim(V) - 1$.

⊗ (*Idée de la preuve.*) Le théorème étant particulièrement intuitif, on ne propose que le principe de la preuve.

- **Étape 1.** $V(f) = W_1 \cup \dots \cup W_s$ avec les W_i irréductibles. En localisant, on se ramène à supposer $V \cap \{f = 0\} = W$ irréductible. On choisit $g_i \in K[V]$, nulle sur W_i , $i \geq 2$, pas sur W_1 . Ainsi V se ramène à $V \setminus \{g_2 \dots g_s = 0\}$ et $K[V]$ à $K[V][\frac{1}{g_2}, \dots, \frac{1}{g_s}]$.
- **Étape 2.** $V \cap (f = 0) = W$ irréductible, $I_W = \sqrt{(f)}$. Le lemme de Noether ($n = \dim(V)$) donne $K[x_1, \dots, x_r] \xrightarrow{j} K[V]$ avec les x_1, \dots, x_r algébriquement indépendants, extension entière. Ce morphisme correspond à $\pi : V \rightarrow \mathbb{A}^n$ tel que $\pi^* = j$. Si $L = K(V)$, $F = K(\mathbb{A}^n)$, $f_0 = N_{L/F}(f)$, on montre en tant que lemme que $\sqrt{(f)} \cap K[\mathbb{A}^n] = \sqrt{(f_0)}$.

- **Étape 3.** $K[W]$ est entier sur $K[X_1, \dots, X_n]/\sqrt{(f_j)}$ de degré de transcendance $n - 1$ donc $\deg \text{tr} = n - 1$, un de moins.

Le résultat est alors démontré. ■

Corollaire. (Théorème de Bézout pour les variétés projectives, version faible)

Soit V une variété projective de $\dim(V) = n \geq 1$ de \mathbb{P}^N . Soit F homogène de degré $d \geq 1$ avec $F \notin I_V$. Alors $V \cap Z(F) \neq \emptyset$ et $V \cap Z(F) = W_1 \cup \dots \cup W_s$, avec $\dim(W_i) = n - 1$.

▷ Notons $Z = Z(F)$. Alors $(V \cap Z)^{aff} = V^{aff} \cap Z^{aff}$, d'où $\dim(V^{aff}) = n + 1$. Par le théorème de Krull, $V^{aff} \cap Z^{aff}$ est soit vide, soit réunion de composantes de dimension $(n + 1) - 1$. Mais $0 \in V^{aff} \cap Z^{aff}$, donc $V^{aff} \cap Z^{aff} = W_1^{aff} \cup \dots \cup W_t^{aff}$, avec $\dim(W_i^{aff}) = n$. Ainsi $\dim(V \cap Z) = W_1 \cup \dots \cup W_t$, avec $\dim(W_i) = \dim(W_i^{aff}) - 1$. ■

Corollaire. (Théorème de Krull itéré)

Soit V une variété affine dans \mathbb{A}^N , respectivement projective dans \mathbb{P}^N . Soient $f_1, \dots, f_r \in K[X_1, \dots, X_n]$ quelconques, respectivement homogènes non constants. Alors toute composante irréductible de $V \cap \{f_1(x) = \dots = f_r(x) = 0\}$ est de dimension $\geq \dim(V) - r$, en particulier, non vide si $\dim(V) \geq r$.

▷ On applique le théorème de Krull par induction. Dans le cas $r = 1$, c'est exactement le théorème. Pour passer du rang $r - 1$ au rang r , $V \cap \{f_1 = \dots = f_{r-1} = 0\} = W_1 \cup \dots \cup W_s$ avec $\dim(W_i) \geq \dim(V) - r + 1$, d'où $V \cap \{f_1 = \dots = f_r = 0\} = \bigcup_{i=1}^s W_i \cap \{f_r = 0\}$ et dans cette réunion, toutes les composantes irréductibles de dimension $\geq \dim(W_i) - 1 \geq \dim(V) - r$. ■

Corollaire. (Dimension d'une intersection)

1. Soient V, W deux variétés affines de \mathbb{A}^n . Alors $\dim(U_j) \geq \dim(V) + \dim(W) - n$ pour chaque composante irréductible de $V \cap W = U_1 \cup \dots \cup U_s$, éventuellement $V \cap W = \emptyset$.
2. Soient V, W deux variétés algébriques de \mathbb{P}^n . Si $\dim(V) + \dim(W) \geq n$, alors $V \cap W \neq \emptyset$ et toute composante est de dimension $\geq \dim(V) + \dim(W) - n$.

▷ On utilise un procédé diagonal. Soit $\Delta = \{(x, y) \in \mathbb{A}^n \times \mathbb{A}^n = \mathbb{A}^{2n}, x = y\}$. C'est une variété : c'est $\{x_1 - y_1 = \dots = x_n - y_n = 0\}$. Soit $\delta : \mathbb{A}^n \rightarrow \mathbb{A}^{2n}$ qui à $x \mapsto (x, x)$. Cette application fournit un isomorphisme entre \mathbb{A}^n et Δ . De plus, si $V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^n$, $V \times W \cap \Delta = \delta(W \cap W) = \{(x, y) \in \mathbb{A}^{2n}, x \in V, y \in W, x = y\} = \{(x, x) \in \mathbb{A}^n \times \mathbb{A}^n \mid x \in V \cap W\}$. Si U_i est une composante irréductible de $V \cap W$, alors $\delta(U_i)$ aussi de $V \times W \cap \Delta$. Or $\dim(V \times W) = \dim(V) + \dim(W)$ donc $\dim(U_i) \geq \dim(V) + \dim(W) - n$.

On traite maintenant le cas projectif en se ramenant au premier cas. Avec les notations usuelles, $V^{aff}, W^{aff} \subseteq \mathbb{A}^{n+1}$. Si $V \cap W = U_1 \cup \dots \cup U_s$, $V^{aff} \cap W^{aff} = U_1^{aff} \cup \dots \cup U_s^{aff}$ et $0 \in U_i^{aff}$. On a vu

que $\dim(U_i^{aff}) \geq \dim(V^{aff}) + \dim(W^{aff}) - (n+1) = (\dim(V) + 1) + (\dim(W) + 1) - (n+1) = (\dim(V) + \dim(W) - n) + 1$, mais par hypothèse $\dim(V) + \dim(W) - n \geq 0$. Donc $U_i \neq \emptyset$ et $\dim(U_i) \geq \dim(V) + \dim(W) - n$. ■

Ceci permet une description inductive de la dimension. Soit V une variété de la dimension n . Soit $f \notin I_V$ non constant (soit non inversible dans $K[V]$). Alors $V \cap \{f = 0\} = W_1 \cup \dots \cup W_s$ avec $\dim(W_i) = n - 1$. Posons $V_{n-1} = W_1$. Alors :

$$V = V_n \supseteq V_{n-1} \supseteq \dots \supseteq V_0$$

avec les V_i irréductibles et $\dim(V_i) = i$. On peut en fait énoncer :

Proposition. (*Description inductive de la dimension*)

1. Soit V une variété de dimension n . Il existe une suite de sous-variétés fermées dans V telles que $V = V_n \supseteq V_{n-1} \supseteq \dots \supseteq V_0$, avec $\dim(V_i) = i$.
2. Inversement, si l'on a une suite $V'_0 \subsetneq V'_1 \subsetneq \dots \subsetneq V'_n = V$, avec les V'_i irréductibles et la suite maximale (si $V'_i \subseteq W_i \subseteq V'_{i+1}$ alors $W_i = V'_i$ ou V'_{i+1}), alors $\dim(V) = n$.

Par suite, la dimension d'une variété V affine (ou projective, car en travaillant un peu plus, on obtient le même résultat), est la longueur maximale des chaînes de sous-variétés fermés incluses dans V .

▷ L'existence est donné par propriété noethérienne. Ensuite, il faut montrer que $\dim(V'_i) = i$. Pour cela, on applique Krull de façon récurrente. $\dim(V'_0) = 0$, sinon un point serait contenu dans V'_0 ce qui contredit la maximalité. Ensuite, $\dim(V'_{i+1}) = \dim(V'_i) + 1$. En effet, $V'_i \subsetneq V'_{i+1}$, donc $\dim(V'_i) < \dim(V'_{i+1})$. Si on avait $\dim(V'_{i+1}) \geq \dim(V'_i) + 2$, choisissons $f \in I_{V'_i}$, $f \notin I_{V'_{i+1}}$, de sorte que $V'_i \subseteq V'_{i+1} \cap \{f = 0\} \subseteq V'_{i+1}$ où chaque composante du terme intermédiaire vérifie $\dim(W_i) = \dim(V'_{i+1}) - 1 > \dim(V'_i)$. Ainsi, il existe j tel que $V'_i \subseteq W_j$. ■

Fait. (*Une troisième définition de la dimension*)

Une variété affine V est de dimension n si et seulement si elle se plonge dans \mathbb{A}^n par une application à fibres finies non vides. Soit V une variétés affines et $f : V \rightarrow \mathbb{A}^n$ à fibres finies non vides. Soit $\phi : K[\mathbb{A}^n] = K[X_1, \dots, X_n] \rightarrow K[V]$ extension algébrique entière, donnée par le lemme de normalisation de Noether si $\phi = f^*$ avec f polynomiale, si $a = (a_1, \dots, a_n) \in \mathbb{A}^n$, montrons que $f^{-1}(\{a\})$ fini non vide, $\phi(P(x)) = f^*P = P \circ f$. Réciproquement, si on a $V \subseteq \mathbb{A}^N$, $K[V] = K[t_1, \dots, t_N]$. Soit $t = t_i$, t entier sur $\phi(K[x_1, \dots, x_n])$, alors $t^d + b_{d-1}t^{d-1} + \dots + b_0 = 0$ avec $b_j \in \phi(K[X_1, \dots, X_n])$. Ainsi $(t_1, \dots, t_N) \in f^{-1}(a) \iff$ pour chaque $t = t_i$, $t(a)$ vérifie $t(a)^d + b_0 \circ f(a)t(a)^{d-1} + \dots + b_0 \circ f(a) = 0$, donc appartient à un ensemble vide non vide.

Cette description, quoiqu'un peu abstraite, et la plus concrète des définitions de la dimension.

On peut en donner une autre grâce à l'espace tangent, ce que l'on fera après le théorème suivant.

Soit $f : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ donnée par $(x,y) \mapsto (x,yx)$. Elle est dominante, c'est-à-dire d'image dense, mais $(0,a)$ avec $a \neq 0$ n'est pas dans l'image. En général, $f^{-1}(a,b)$ est fini réduit à un point, mais $f^{-1}(0,b) = \emptyset$ si $b \neq 0$ et $= \{0\} \times \mathbb{A}^1$ si $b = 0$. Si $(a,b) \in \mathbb{A}^2 \setminus \{a = 0\}$, alors $f^{-1}(a,b)$ est non vide et fini.

Théorème. (Théorème de la dimension des fibres)

Soient V, W deux variétés affines ou projectives. Si $f : V \longrightarrow W$ est une application dominante (régulière, polynomiale). Alors :

1. $\dim(V) \geq \dim(W)$ et la dimension de toutes les fibres non vides $f^{-1}(y)$ excède $\dim(V) - \dim(W)$; dans le cas projectif, le cas des fibres vides n'apparaît pas;
2. s'il existe $w_0 \in W$, $f^{-1}(w_0)$ est fini non vide, alors $\dim(V) = \dim(W)$;
3. il existe un ouvert W_0 de W tel que pour tout $w \in W_0$, les composantes $f^{-1}(w)$ sont toutes de dimension $\dim(V) - \dim(W)$.

▷ L'application dominante $f : V \longrightarrow W$ donne un morphisme de corps $f^* : K(W) \longrightarrow K(V)$ donc injectif. Ainsi, une base de transcendance de $K(W)$ donne une partie algébriquement indépendante de $K(V)$. Alors $m = \dim(W) = \deg \operatorname{tr}(K(W)) \leq \deg \operatorname{tr}(K(V)) = \dim(V) = n$.

Dès maintenant, on suppose V, W affines, car il est clair que le reste de la proposition suffit d'être démontré dans le cas affine. Soit $y = f(x) \in W$. Il existe $g_1, \dots, g_m \in K[W]$ telles que $W \cap \{g_1(w) = \dots = g_m(w) = 0\} = \{y_1, \dots, y_s\}$ où $y_1 = y$. On choisit $g_1 \in K[W] \setminus \{0\}$ nulle en y . Par le théorème de Krull, la dimension de chaque composante de $W \cap \{g_1 = 0\}$ est $\dim(W) - 1$, avec $W \cap \{g_1 = 0\} = W_1 \cup \dots \cup W_s$ où $y \in W_1$. Par induction, on trouve g_1, \dots, g_j . La dimension des composantes de $W \cap \{g_1 = \dots = g_j = 0\}$ est $\dim(W) - j$ avec y dedans. Ainsi $\dim(W \cap \{g_1 = \dots = g_m = 0\}) = 0$ avec y dedans. Il existe élémentairement une fraction $g \in K[W]$ telle que $y \in W \setminus \{g = 0\}$, y_2, \dots, y_s n'y étant pas. On remplace W par $W_0 = W \setminus \{g = 0\}$. On peut supposer $W \cap \{g_1 = \dots = g_n = 0\} = \{y\}$. Alors $f^{-1}(y) = \{x \in V, g_1 \circ f(x) = \dots = g_m \circ f(x) = 0\}$. Par corollaire du théorème de Krull, toutes les composantes sont de dimension $\geq n - m$, ce qu'il fallait démontrer.

Ensuite, on a alors $0 = \dim(f^{-1}(w_0)) \geq n - m$. Mais $n \geq m$, donc $n = m$.

Enfin, si $f^* : K(W) \longrightarrow K(V)$, $K(W)$ et $K[V]$ s'identifient à des sous-corps et sous-algèbres de $K(V)$. Définissons A la $K(W)$ -algèbre engendrée par $K[V]$ dans $K(V)$. Alors A est de type fini sur $K(W)$. Par le lemme de normalisation de Noether, il existe x_1, \dots, x_t algébriquement indépendant sur $K(W)$ telle que A soit entière sur $K(W)[x_1, \dots, x_t]$. Alors $\operatorname{Frac}(A) = K(V)$ et $\deg \operatorname{tr}(A) = n$. De plus, $\deg \operatorname{tr}(K(W)) = m$, d'où $\deg \operatorname{tr}(K(V)/K(W)) = n - m$: combien d'éléments transcendents faut-il rajouter... (Le degré de transcendance d'une algèbre est celui de son corps des fractions; il faut qu'elle soit intègre pour que cela ait un sens.) Or $K[V] = K[t_1, \dots, t_N]$ et pour $t = t_i$, il est entier sur $K(W)[x_1, \dots, x_t] \ni f_j$, vérifiant $t^d + f_{d-1}t^{d-1} + \dots + f_0 = 0$. Or $K(W) = \operatorname{Frac}(K[V])$. Il existe $g \in K[W] \setminus \{0\}$ avec tous les $f_j g \in K[W]$. Donc t_1, \dots, t_N est entier sur $K[W][\frac{1}{g}][x_1, \dots, x_t]$ où $K[W][\frac{1}{g}] = K[W_0]$ où $W_0 = W \setminus \{g = 0\}$ et $V_0 = V \setminus \{g \circ f = 0\}$. On a donc une flèche f^* composée de $K[W_0] \hookrightarrow K[W_0][x_1, \dots, x_t] \hookrightarrow K[V_0]$, des inclusions respectivement i, j qui correspondent à $f : V_0 \longrightarrow W_0 \times \mathbb{A}^t$ donnée par f_1 à fibres discrètes non vides (car j définit une extension entière et on renvoie au fait précédent) et $W_0 \times \mathbb{A}^t \longrightarrow W_0$ donnée par W_2 , qui se composent en f . Alors $f_2^{-1}(w_0) = w_0 \times \mathbb{A}^t$, $w_0 \in W_0$, et $f^{-1}(w_0) = f_1^{-1}(w_0 \times \mathbb{A}^t)$ union finie de composantes de dimension

$$t = n - m.$$

Enfin, remarquons qu'il n'y a pas de fibres vides dans le cas des variétés projectives. En effet, par théorème de l'élimination, l'image de f dominante est dense et fermée, donc f est surjective. ■

Exemple. (Éclatement d'un point)

On illustre un exemple de saut de dimension des fibres dans le cas des variétés affines.

Soit $P = [0, \dots, 0, 1] \in \mathbb{P}^n$. Soit $\phi : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$ qui à $[x_0, \dots, x_n] \mapsto [x_0, \dots, x_{n-1}]$. Alors $\text{dom}(\phi) = \mathbb{P}^n \setminus \{P_0\}$.

On a $V = \overline{\text{Graphe}(\phi)}^{\text{Zariski}} \subseteq \mathbb{P}^n \times \mathbb{P}^{n-1}$. f envoie V dans \mathbb{P}^n et g l'envoie dans \mathbb{P}^{n-1} . Posons $G_\phi = \{([x_0, \dots, x_n] \neq P_0, [y_0, \dots, y_{n-1}]) \in \mathbb{P}^n \times \mathbb{P}^{n-1} \mid [x_0, \dots, x_{n-1}] = [y_0, \dots, y_{n-1}]\}$ (soit $x_i y_j - x_j y_i = 0$ pour $0 \leq i, j \leq n-1$). Alors $V = \{([x_0, \dots, x_n], [y_0, \dots, y_{n-1}]) \in \mathbb{P}^n \times \mathbb{P}^{n-1}\}$. On a $f^{-1}(P_0) = \{P_0\} \times \mathbb{P}^{n-1}$. Si $P = [x_0, \dots, x_n] \neq P_0$, alors $f^{-1}(P) = \{([x_0, \dots, x_n], [x_0, \dots, x_{n-1}])\}$. D'où $\dim(V) = n$.

Exercice 13

Commenter l'affirmation suivante : « Deux variétés affines ont même dimension si et seulement si elles sont birationnellement isomorphes. »

▷ **Éléments de réponse.**

Impossible, toute variété étant birationnellement isomorphe à une hypersurface. L'identité des dimensions est donc toute autre.

Exercice 14

Montrer que $\{(t, e^t), t \in \mathbb{R}\}$ n'est pas une variété affine.

2.2.1.3 Application : existence de droites dans une surface cubique

Voici une application des théorèmes de la dimension.

Théorème. (Toute surface cubique contient une droite)

Soit V une surface cubique dans \mathbb{P}^3 . Alors V contient une droite projective.

▷ On note G l'ensemble des droites de \mathbb{P}^3 , variété projective de dimension 4. Soit $V \in \mathbb{P}^N$. L'espace des polynômes homogènes de degré 3 en X, Y, Z, T est de dimension 20. Notons $Z = \{(V, D) \in \mathbb{P}^N \times G, D \subseteq V\}$, fermé donc variété projective. Les projections p, q l'envoient respectivement dans \mathbb{P}^N et dans G . Alors $q^{-1}(D) \simeq \mathbb{P}^{N-4}$. On peut choisir les coordonnées de \mathbb{P}^3 de sorte que $D = \{[X, Y, Z, T] \in \mathbb{P}^3, X = Y = 0\}$. $V = \{[X, Y, Z, T] \in \mathbb{P}^3, F(X, Y, Z, T) = 0\}$. De plus, $D \subseteq V \iff F(0, 0, Z, T) \equiv 0$. Ceci équivaut à ce que les coefficients de $Z^3, Z^2 T, Z T^2, T^3$ sont nuls. Donc $\dim(Z) = (N - 4) + \dim(G) = N$. Trouvons $V_0 \in \mathbb{P}^N$ telle que $p^{-1}(V_0)$ soit fini non vide. V_0 est d'équation $XYZ - T^3 = 0$. Notons

$D_1 = \{T = X = 0\}$, $D_2 = \{T = Y = 0\}$, $D_3 = \{T = Z = 0\}$. On note aussi $\Pi = \{T = 0\}$, de sorte que $\Pi \cap V_0 = D_1 \cup D_2 \cup D_3$. Plaçons-nous dans $U_T = \{[X, Y, Z, T] \mid T \neq 0\}$. S'il y avait une droite $D \subseteq V_0$ mais pas incluse dans Π , $D \cap U = \{(a_1 t + b_1, a_2 t + b_2, a_3 t + b_3, 1), t \in \mathbb{A}^1\}$. Ainsi, pour tout t , $(a_1 t + b_1)(a_2 t + b_2)(a_3 t + b_3) = 1$. En développant, on obtient un polynôme en t^3 d'où l'on tire par le calcul $a_1 = a_2 = a_3 = 0$ par identification des coefficients.

On a donc $p : Z \longrightarrow p(Z) \subseteq \mathbb{P}^N$. De plus $\dim(p^{-1}(V_0)) = 0$, donc $\dim(p(Z)) = \dim(Z) = N$. Le théorème de l'élimination dit que $p(Z)$ est fermée, donc $p(Z) = \mathbb{P}^N$. Donc $\dim(Z) = (N - 4) + \dim(G) = N$. Or $p(Z)$ est l'ensemble des $V \in \mathbb{P}^N$ qui contiennent une droite. ■

En regardant plus près le théorème de la dimension, on obtient que presque toute ne contiennent qu'un nombre fini de droites.

2.2.2 Espace tangent, points singuliers en géométrie algébrique

La notion d'espace tangent coïncide avec celle du calcul différentiel, à ceci près que la géométrie algébrique sait le définir en tout point d'une variété algébrique, même non lisse.

Intuitivement, dans le cas d'une courbe, on retrouve la notion de tangente (d'ailleurs, on en a déjà parlé dans les PROLÉGOMÈNES) ; dans le cas d'une surface, on trouve la notion de plan tangent. On généralise cette définition.

Définition. (Espace tangent à une hypersurface)

Soit $f \in K[X_1, \dots, X_n]$ irréductible et $V = \{x \in \mathbb{A}^n \mid f(x) = 0\}$. On appelle *espace tangent*, l'ensemble

$$T_a(V) = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid \sum_{j=1}^n \frac{\partial f}{\partial x_j}(a)(x_j - a_j) = 0\}.$$

Autrement dit, $T_a(V) = \mathcal{V}(f_a^{(1)})$ où $f_a^{(1)}$ la composante homogène de degré 1 (= partie linéaire) de f en a .

C'est un sous-espace affine passant par le point a dirigé par l'espace tangent au gradient de f en a . Il passe de plus par le point $\sum_{j=1}^n \frac{\partial f}{\partial x_j}(a)a_j$ et donc, s'il est nul, c'est un espace vectoriel.

Remarque. En général, $\dim T_a(V) = n - 1 = \dim(V)$. Cependant, si $\frac{\partial f}{\partial x_1}(a) = \dots = \frac{\partial f}{\partial x_n}(a) = 0$, c'est-à-dire si a est un point singulier, ce n'est pas évident.

Lemme

$\{a \in V \mid \dim T_a(V) = n - 1\}$ est un ouvert non vide (donc dense) dans V .

▷ Notons $V^{sing} = \{a \in V \mid \frac{\partial f}{\partial x_i}(a) = 0 \quad \forall i\}$ qui est un fermé distinct de V . Si $\frac{\partial f}{\partial x_1}$ est nulle sur V , alors f divise $\frac{\partial f}{\partial x_1}$ dans $K[X_1, \dots, X_n]$, mais cela implique $\frac{\partial f}{\partial x_1} = 0$: en effet, ou bien $\deg_{x_1}(f) = 0$ et $\frac{\partial f}{\partial x_1} = 0$, ou bien $\deg_{x_1}(f) = d_1 \geq 1$, d'où $\deg_{x_1} \frac{\partial f}{\partial x_1} = d_1 - 1$. Si la caractéristique de K est

nulle, $\frac{\partial f}{\partial x_1} = \dots = \frac{\partial f}{\partial x_n} = 0$, d'où f constante; si la caractéristique de K est un nombre premier p , $\frac{\partial f}{\partial x_1} = \dots = \frac{\partial f}{\partial x_n} = 0$, $f(X_1, \dots, X_n) = \sum a_{i_1, \dots, i_n} X_1^{i_1 p} \dots X_n^{i_n p}$; comme $a_{i_1, \dots, i_n} = (b_{i_1, \dots, i_n})^p$ d'où $f = g^p$. D'où le résultat. ■

Suite à ce toy model, on peut donner une définition générale.

Définition. (Espace tangent à une variété affine)

Soit $V \subseteq \mathbb{A}^n$ une variété affine. Alors :

$$T_a(V) = \bigcap_{f \in I_V} \{x \in \mathbb{A}^n \mid f_a^{(1)} = 0\},$$

i.e.

$$\sum_{j=1}^n \frac{\partial f}{\partial x_j}(a)(x_j - a_j) = 0.$$

Autrement dit, c'est l'intersection de tous les espaces tangents des hypersurfaces définies par des polynômes de l'idéal annulateur de la variété. Les connaisseurs de la notion de transversalité ne seront pas surpris.

Remarque. Si f_1, \dots, f_m sont des générateurs de I_V , $T_a(V) = \bigcap_{i=1}^m \{x \in \mathbb{A}^n \mid (f_i)_a^{(1)}(x) = 0\}$.

Théorème

1. $\forall a \in V \quad \dim(T_a(V)) \geq \dim(V)$.
2. $\{a \in V \mid \dim(T_a(V)) = \dim(V)\}$ est un ouvert dense de V .

▷ Soient f_1, \dots, f_m générateurs de I_V . Alors $T_a(V) = \{x \in \mathbb{A}^n \mid \forall j \in \llbracket 1, m \rrbracket \quad \sum_{i=1}^n \frac{\partial f_j}{\partial x_i}(a)x_i = 0\}$.

On a m équations, n indéterminées, d'où une matrice $J(a) = \left(\frac{\partial f_j}{\partial x_i}(a)\right)$. Alors $\dim(T_a(V)) = n - \text{rg}(J(a))$. Notons $r_0 = \max_{a \in V} \text{rg}(J(a))$ et $d_0 = n - r_0$. Pour tout $a \in V$, $\dim(T_a(V)) \geq d_0$. Il existe un mineur $r_0 \times r_0$, de $J(a) \neq 0$ et tous les mineurs $(r_0 + 1) \times (r_0 + 1)$ sont nuls. Ainsi $\{a \in V \mid \dim(T_a(V)) > d_0\} = \{a \in V \mid \text{tous les mineurs } r_0 \times r_0 \text{ de } J(a) \text{ sont nuls}\} \iff \text{rg}(J(a)) < r_0$. En particulier, $\{a \in V \mid \dim(T_a(V)) = d_0\}$ est un ouvert non vide. Il faut montrer que $d_0 = \dim(V)$ où $d_0 = \min_{a \in V} \dim(T_a(V))$. Si V est une hypersurface de \mathbb{A}^n , c'est déjà vu, or toute variété est birationnelle à une hypersurface. Il suffit enfin de vérifier que si $\phi : V \simeq W$ et $b = \phi(a)$, alors $T_a(V) \simeq T_b(W)$, ce que l'on fera avec une autre définition de l'espace tangent indépendante. En effet, ϕ est définie entre ouverts V_0, W_0 de V, W , mais $T_a(V) = T_a(V_0) \simeq T_b(W_0) = T_b(W)$, donc sur un ouvert $\dim T_b(W) = \dim(W) = d$, donc sur un ouvert $\dim(T_a(V)) = \dim(V)$. ■

Retour vers le passé. On obtient la quatrième définition de la dimension annoncée : $\dim(V) = \min_{a \in V} \dim(T_a(V))$.

Définition. (Point singulier, point lisse)

Un point $a \in V$ tel que $\dim(T_a(V)) > \dim(V)$ est *singulier*. Le cas contraire, on dit que a est *lisse*.

Exemple. (Trouver des points singuliers)

Il s'agit, connaissant la dimension, d'écrire la matrice des dérivées partielles et d'en calculer le rang.

On donne une deuxième définition, quelque peu meilleure, car extrinsèque, de l'espace tangent :

Définition-propriété. (Espace tangent à une variété affine, 2v)

Soit V une variété affine et $a \in V$. Alors $\mathfrak{M}_{V,a}/\mathfrak{M}_{V,a}^2$ est un K -espace vectoriel et son dual est naturellement isomorphe à $T_a(V)$.

▷ On rappelle que $\mathfrak{M}_{V,a} = \{f \in \mathcal{O}_{V,a} \mid f(a) = 0\}$ est l'unique idéal maximal de l'anneau local $\mathcal{O}_{V,a}$ des fonctions de $K(V)$ régulières en a . Notons $M_a = (X_1 - a_1, \dots, X_n - a_n)$ l'idéal de a dans $K[X_1, \dots, X_n]$. Alors M_a/M_a^2 est l'ensemble des formes linéaires en $X_1 - a_1, \dots, X_n - a_n$: en effet, de $l = \sum_{i=1}^n b_i(X_i - a_i) \mapsto l \longrightarrow l \bmod M_a^2$, d'où $(\mathbb{A}^n)^{\text{dual}} \longrightarrow M_a \longrightarrow M_a/M_a^2$. L'idéal M_a^2 est engendré par $(X_i - a_i)(X_j - a_j)$: en effet, si $f \in M_a$, $f = f^{(1)} + f^{(2)} + \dots + f^{(n)}$ où $f^{(2)} + \dots + f^{(n)} \in M_a^2$. De plus, $\mathcal{O}_{\mathbb{A}^n,a} = K[\mathbb{A}^n]$ localisé par rapport à l'idéal premier M_a , soit $\{f = \frac{P}{Q} \text{ avec } P, Q \text{ polynomiaux, } Q(a) \neq 0, Q \notin M_a\}$ et $\mathfrak{M}_{\mathbb{A}^n,a} = \{f \in \mathcal{O}_{\mathbb{A}^n,a} \mid f(a) = 0\}$. Alors $\mathfrak{M}_{\mathbb{A}^n,a}/\mathfrak{M}_{\mathbb{A}^n,a}^2 = M_a/M_a^2$. En effet, $M_a/M_a^2 \hookleftarrow M_a \rightarrow \mathfrak{M}_{\mathbb{A}^n,a} \longrightarrow \mathfrak{M}_{\mathbb{A}^n,a}/\mathfrak{M}_{\mathbb{A}^n,a}^2$ fournit une injection de $M_a/M_a^2 \hookrightarrow \mathfrak{M}_{\mathbb{A}^n,a}$. Pour $a \in V \subseteq \mathbb{A}^n$, $T_a(V) = \{x \in \mathbb{A}^n \mid f^{(1)}(x) = 0 \quad \forall f \in I_V\}$. On a donc $\psi : M_a \longrightarrow (\mathbb{A}^n)^* \longrightarrow T_a(V)^*$ qui à $f \mapsto f^{(1)} \mapsto f_{T_a(V)}^{(1)}$. Il est clair que $\text{Ker}(\psi) \supseteq M_a^2 + I_V$. D'autre part, si $f \in \text{Ker}(\psi)$, $f^{(1)}$ est nulle sur $T_a(V)$. Si g_1, \dots, g_n sont générateurs de I_V , $g_1^{(1)}, \dots, g_m^{(1)}$ formes linéaires sur \mathbb{A}^n qui engendrent comme espace vectoriel les formes linéaires nulles sur $T_a(V)$, donc $f^{(1)} = \sum_{j=1}^m a_j g_j^{(1)}$, donc $f - \sum a_j g_j \in M_a^2$, $\sum a_j g_j \in I_V$. Ainsi $\mathfrak{M}_{\mathbb{A}^n,a}/\mathfrak{M}_{\mathbb{A}^n,a}^2 = M_a/(M_a^2 + I_V) \simeq T_a(V)^*$, d'où $T_a(V) \simeq (\mathfrak{M}_{\mathbb{A}^n,a}/\mathfrak{M}_{\mathbb{A}^n,a}^2)^*$. ■

Corollaire. (Structure de l'espace tangent)

L'espace tangent à une variété affine en un point est un espace vectoriel.

Corollaire. (Transport de l'espace tangent par isomorphisme)

Si $\phi : V \simeq W$ et $b = \phi(a)$, $d\phi(a) : T_a(V) \simeq T_b(W)$.

Définition. (Différentielle, application linéaire tangente)

Soit $\phi : V \longrightarrow W$ régulière avec $\phi(a) = b$. $\phi^* : \mathcal{O}_{W,b} \longrightarrow \mathcal{O}_{V,a}$ avec $h \mapsto h \circ \phi$ permet de définir :

$$\begin{array}{ccc} \mathfrak{M}_{W,b} & \xrightarrow{\phi^*} & \mathfrak{M}_{V,a} \\ \downarrow & & \downarrow \\ \mathfrak{M}_{W,b}/\mathfrak{M}_{W,b}^2 & \xrightarrow[\phi^\#]{} & \mathfrak{M}_{V,a}/\mathfrak{M}_{V,a}^2 \end{array}$$

d'où $(\mathfrak{M}_{V,a}/\mathfrak{M}_{V,a}^2)^* \xrightarrow{d\phi(a)} (\mathfrak{M}_{W,b}/\mathfrak{M}_{W,b}^2)^*$ donnée par $(\phi^\#)^t$.

On dispose d'une règle de la chaîne :

Proposition. (Chain rule en géométrie algébrique)

Si $V \xrightarrow{\phi} W \xrightarrow{\psi} U$ avec $a \mapsto b \mapsto c$, donnée par $d(\psi \circ \phi)(a) = d\psi(b) \circ d\phi(a)$.

▷ Avec la définition fonctorielle de la différentielle, la preuve est quasi immédiate :

$$\begin{array}{ccccc} \mathfrak{M}_{U,c} & \xrightarrow{\psi^*} & \mathfrak{M}_{W,b} & \xrightarrow{\phi^*} & \mathfrak{M}_{V,a} \\ \downarrow & & \downarrow & & \downarrow \\ \mathfrak{M}_{U,c}/\mathfrak{M}_{U,c}^2 & \xrightarrow{\psi^\#} & \mathfrak{M}_{W,b}/\mathfrak{M}_{W,b}^2 & \xrightarrow{\phi^\#} & \mathfrak{M}_{V,a}/\mathfrak{M}_{V,a}^2 \end{array}$$

d'où le résultat. ■

Exercice 15

Soit A une k -algèbre réduite et de type fini. Soit $P \in A[X]$ un polynôme unitaire, tel qu'il existe $Q, R \in A[X]$ vérifiant $QP + RP' = 1 \in A[X]$. Soit $f : Y \rightarrow X$ le morphisme de k -variétés affines, associé à l'inclusion de k -algèbres $A \hookrightarrow A[X]/P$. Montrer que, pour tout $p \in X$, le morphisme $TPY \longrightarrow Tf(p)X$ induite sur les espaces tangents, est un isomorphisme. On dit que f est un morphisme *étale standard*.

2.2.3 Compléments en vrac

Voici une précision concernant la démonstration de la proposition 2.4.6. On a utilisé de manière cruciale le résultat suivant. Soit $B \hookrightarrow A$ une injection entre k -algèbres intègres de type fini. [Dans le cours, $B = k[a_1, \dots, a_d]$ est une algèbre de polynômes sur k]. Supposons que l'extension induite sur les corps de fractions, $K := \text{Frac}(A) \hookrightarrow L := \text{Frac}(B)$, est finie séparable. Alors, il existe $f \in B$, et $y \in A_f$, tel que

$$A_f = B_f[y] \simeq B_f[X]/P,$$

où $P \in B_f(X)$ est un polynôme unitaire, et vérifiant une relation de Bézout avec sa dérivée ($QP + RP' = 1$) dans l'anneau $B_f[X]$.

▷ Démonstration : on peut d'abord remarquer que le morphisme naturel

$$F : A \otimes_B K \longrightarrow L,$$

$$a \otimes x \mapsto ax$$

est un isomorphisme. [Plus concrètement : cela signifie ici que L est engendré, comme anneau, par ses deux sous-anneaux K et A]. En effet, $Im(F)$ est une K -algèbre intègre et finie (comme K -ev), donc est un corps. Comme le corps des fractions de $Im(F)$ est égal à L , on conclut $Im(F) = L$. Puis, L/K est finie séparable, elle est monogène par le th. de l'élément primitif. Soit donc $y \in L$ tel que $L = K[y]$, et soit $P \in K[X]$ le polynôme minimal (unitaire) de y . Il est séparable, donc on a une relation de Bézout $QP + RP' = 1$ dans $K[X]$. Soit y_1, \dots, y_n un système de générateurs de la k -algèbre de type fini A . Par hypothèse, il existe des polynômes $P_1, \dots, P_n \in K[X]$, tels que $y_i = P_i(y)$ pour tout i . On prend maintenant un "dénominateur commun f " à toutes ces données. Soit donc $f \in B$, tel que P, Q, R et les P_i sont dans $B_f[X]$, et tel que $y \in A_f = A \otimes_B B_f$. Soit On vérifie que ce f convient. Ceci est un exemple d'un phénomène de "spreading out". [Attention, petite subtilité dans cette démo : il ne suffit pas de demander seulement que P, Q, R sont dans $B_f[X]$, et que $y \in A_f$: la condition sur les P_i est nécessaire. En effet, le résultat est faux si A n'est pas de type fini sur k .] ■

Bonjour, suite aux remarques inspirées de deux d'entre vous, voici un rectificatif concernant deux assertions que j'ai énoncées de manière incorrecte. 1) Soit R une k -algèbre et X une k -variété ($k = \bar{k}$). On a défini le foncteur des points $X(R)$, à l'aide d'une pirouette avec le lemme de Yoneda. J'ai dit que, lorsque R est local, alors $X(R)$ consiste en les couples (x, f) , où $x \in X$ et $f : \mathcal{O}_{X,x} \longrightarrow R$ est un morphisme de k -algèbres. Cet énoncé est **faux**, sauf si R est local et **artinien**. Concrètement, une k -algèbre de type fini et artinienne c'est une k -algèbre de dimension finie sur k . [Si elle est locale, son idéal maximal M est alors nilpotent]. Exemple typique : $R = k[\epsilon]$. Remarque hors programme : dans le contexte des schémas (où l'on a plus de points dans l'espace topologique sous-jacent), l'énoncé initial est vrai.

2) J'ai affirmé que, si I est un idéal d'un anneau noethérien, alors le morphisme naturel $A \longrightarrow \hat{A}$ est injectif. Cela est **faux**. Par contre, et c'est ce qu'on utilise en pratique, c'est vrai si on ajoute l'hypothèse que A est local et que $I = M$ est son idéal maximal.

Le contre-exemple à 2), présenté par votre camarade est : $A = k \times k$, et $I = 0 \times k$. Alors $\hat{A} = k$ et le morphisme $A \longrightarrow \hat{A}$ est surjectif, non injectif. Le point clé est ici que $I = I^2$. [Remarquez que, par le lemme de Nakayama, si $I \subset A$ est un idéal d'un anneau vérifiant $I = I^2$, et si I est de type fini comme A -module, alors $I = eA$ avec $e \in A$ idempotent, i.e. $e^2 = e$.]

2.2.3.1 14 octobre 2024

Soit A une k -algèbre réduite et de type fini. Soit $P \in A[X]$ un polynôme unitaire, vérifiant une relation de Bézout avec sa dérivée : $QP + RP' = 1$, dans l'anneau $A[X]$. Posons

$B := A[X]/P$. On a vu en cours que B est réduite. Soit $f : V = \text{Spm}(B) \longrightarrow W = \text{Spm}(A)$ le morphisme (fini) de variétés affines correspondant à l'inclusion $A \hookrightarrow B$. Alors, pour tout $v \in V$, l'application k -linéaire $[Df_v : T_v V \longrightarrow Tf(v)W]$ (différentielle de f en v) est un isomorphisme.

Démonstration : pour tout $w \in W$, on peut évaluer les coefficients de P (qui sont des éléments de $\mathcal{O}_W(W)$) en w . On note $\text{ev}_w(P) \in k[X]$ le polynôme correspondant, il est à coeffs dans k . De la même manière, pour toute k -algèbre R , on peut évaluer P en un R -point $w \in W(R)$, le résultat est noté $\text{ev}_w(P) \in R[X]$. Maintenant, rappelons la description du cours de l'espace tangent : $[T_v V = \rho^{-1}(v) = x \in V(k[\epsilon]), \text{ tels que } \rho(x) = v,]$ où $\rho : V(k[\epsilon]) \longrightarrow V(= V(k))$ est associé à la réduction $k[\epsilon] \xrightarrow{\epsilon \mapsto 0} k$. De même pour $Tf(v)W$.

Ensuite, je vous laisse vous convaincre que, pour toute k -algèbre R , $V(R)$ consiste en les couples $v = (w, u)$, où $w \in W(R)$, et $u \in R$ est une racine du polynôme $\text{ev}_w(P) \in R[T]$. Lorsque $R = k$, on obtient une description du morphisme f par la formule simple $[f(w, u) = w.]$ Soit $v = (w, u) \in V(k)$, et soit $t \in Tf(v)W = \rho^{-1}(w)$. En utilisant la description précédente, on voit que la préimage $(Df_v)^{-1}(t)$ est formée par les $U \in k[\epsilon]$, qui sont racine du polynôme $\text{ev}_t(P) \in k[\epsilon][T]$, et tels que $\rho(U) = u$.

Autrement dit : $(Df_v)^{-1}(t)$ consiste en les relèvements de u (qui est une racine de $\text{ev}_w(P) = \rho(\text{ev}_t(P)) \in k[T]$), en une racine de $\text{ev}_t(P) \in k[\epsilon][T]$.

Si l'on parvient à justifier l'existence et l'unicité d'un tel relèvement, on a gagné. Or ceci est une conséquence du lemme de Hensel, dont voici l'énoncé. (On réinitialise les notations!) Soit A un anneau. Soit $I \subset A$ un idéal formé d'éléments nilpotents. [Pour l'application, prendre $A = k[\epsilon]$, et $I = k\epsilon$]. Soit $P \in A[T]$ un polynôme, tel que P' dans l'anneau quotient $A[T]/I$ est inversible. Soit $u \in A/I$ une racine de P modulo I , c'est-à-dire une racine de $\bar{P} \in (A/I)[T]$. On suppose que $P'(u) \in A/I$ est inversible. [Ceci est automatiquement le cas s'il existe une relation de Bézout $QP + RP' = 1 \in A[T]$; le vérifier!] Alors u se relève de manière unique en un $U \in A$, qui est racine de P .

Pour la démo : soit $U \in A$ n'importe quel relevé de u . Alors $P(U) = i \in I$, et $P'U$ est inversible dans A (car inversible modulo I , et I est formé de nilpotents...). On modifie U , en utilisant la formule $[P(U + ai) = P(U) + aiP'(U); \text{ modulo } i^2]$ Puisque $P'(U)$ est inversible, on peut choisir $a = \frac{-1}{P'(U)}$, qui est tel que $P(U + ai) = 0$ modulo i^2 . En particulier, l'indice de nilpotence de $P(U + ai)$ est strictement plus petit que celui de $P(U)$. On conclut par récurrence.

Pour la terminologie : un morphisme $f : V \rightarrow W$ comme ci-dessus est un morphisme fini **étale standard**. Notez qu'une définition possible pour un morphisme étale entre k -variétés (qui est une notion hors-programme!), est que sa différentielle soit un isomorphisme en tout

point. Comme vu en cours, un tel morphisme est très rarement un iso local, contrairement à la situation analogue en géométrie différentielle.

2.3 Variétés projectives

Propriété. (Base de la topologie de Zariski sur une variété projective)

Les $D(f) = V(f)^c$ dans $\mathbb{P}^n(k)$ forment une base de sa topologie

Définition. (Sous-ensemble algébrique de l'espace projectif)

Les sous-ensembles algébriques de \mathbb{P}^n sont les $\{[x_0, \dots, x_n] \in \mathbb{P}^n \mid \forall i \in I \quad F_i(x_0, \dots, x_n) = 0\}$ avec les F_i homogènes.

Définition-propriété. (Idéal homogène)

Si I est l'idéal engendré par les F_i dans $K[X_0, \dots, X_n]$, on dit que c'est un *idéal homogène*. Il est équivalent de dire que I est un idéal de $K[X_0, \dots, X_n]$ et si $I \ni F = F_0 + \dots + F_d$ sa décomposition homogène, alors tous les $F_j \in I$.

Le sous-ensemble algébrique précédent est alors $\{[x_0, \dots, x_n] \in \mathbb{P}^n \mid \forall F \text{ homogène} \in I \quad F(x_0, \dots, x_n) = 0\}$.

▷ Supposons que l'idéal I aient un ensemble $\{f_\lambda\}_{\lambda \in \Lambda}$ de générateurs homogènes. Soit $g \in I$ et soit $g = \sum_i g_i$ sa décomposition homogène. Alors $g = \sum_{j=1}^m h_j f_{\lambda_j}$ pour un $m \in \mathbb{N}$ et $h_j \in k[X_0, \dots, X_n]$. Maintenant, décomposons $\sum h_j f_{\lambda_j}$ en composantes homogènes. Puisque f_{λ_j} est homogène, on peut voir que toute composante homogène de $\sum h_j f_{\lambda_j}$ sera de la forme $\sum_{k \in K} h'_k f_{\lambda_k}$ pour $K \subseteq \{1, \dots, m\}$. Puisque cette décomposition est unique, cela signifie que chaque g_i doit coïncider avec une expression du type $\sum_{k \in K} h'_k f_{\lambda_k}$, qui implique les $g_i \in I$.

Réciproquement, supposons que $f = \sum_i f_i$ implique $f_i \in I$ pour tout i . Soit $\{g_1, \dots, g_m\}$ un système de générateurs de I , fini par noethérianité. Alors l'ensemble des $h \in K[X_0, \dots, X_n]$ tels que h soit une composante homogène de l'un des g_i est évidemment un système de générateurs de I . D'où le résultat. Remarquons que la finitude est inutile, mais elle permet la remarque suivante. ■



On remarque que ce dernier ensemble est fini ! On a donc montré que **si I est un idéal homogène, il a un système fini de générateurs homogènes.**

Propriétés

L'intersection, la somme, le produit et le radical d'idéaux homogènes sont homogènes. De plus, un idéal homogène est premier si et seulement si il vérifie la condition de primalité sur les éléments homogènes.

Exercice 16

Soit $a \subseteq k[X_0, \dots, X_n]$ un idéal homogène et $V_+(a) = \{x \in \mathbb{P}^n(k) \mid f(x) = 0 \quad \forall f \in a \text{ homogène}\}$. Montrer que les fonctions $a \mapsto V_+(a)$ et $Z \mapsto C(Z)$ définissent des bijections entre l'ensemble des idéaux radiciels homogènes non exceptionnels, les sous-espaces fermés de $\mathbb{P}^n(k)$ et les cônes affines fermés $C \subseteq \mathbb{A}^{n+1}(k)$ non nuls.

Si $Z \subseteq \mathbb{P}^n(k)$ est fermé, on note $I_+(Z)$ l'idéal homogène correspondant. Montrer que $I_+(Z) = I(C(Z))$ et en déduire que Z est irréductible si et seulement si $I_+(Z)$ est premier si et seulement si $C(Z)$ est irréductible.

2.3.1 Propriétés générales des variétés projectives

On conseille vivement au lecteur de revoir les propriétés du prolégomène quant aux idéaux homogènes de polynômes.

Définition. (*Variété (algébrique) projective*)

Soit V un sous-ensemble de \mathbb{P}^n . On parle de *variété (algébrique) projective* de \mathbb{P}^n si V est l'ensemble des zéros communs à une famille de polynômes homogènes de $K[X_1, \dots, X_{n+1}]$, ou, ce qui revient au même, les zéros communs d'un idéal homogène de $K[X_1, \dots, X_{n+1}] \simeq K[X_0, \dots, X_n]$ ET (mais encore, cela varie selon les auteurs) si V est irréductible avec une définition semblable au cas affine.

On peut transposer le théorème des zéros de Hilbert en une correspondance entre sous-ensembles algébriques de \mathbb{P}^n et idéaux homogènes réduits de $K[X_0, \dots, X_n]$.

▷ Le radical d'un idéal homogène est homogène. Soit I un idéal homogène de $K[X_1, \dots, X_n]$ et J son radical. Soit $x^n \in I$. Soit x_k le monôme de plus haut degré apparaissant dans x . Il est clair en voyant les degrés que $x_k^n \in I$, soit $x_k \in J$. Alors $x - x_k$ est encore dans J . En recommençant jusqu'à plus soif, on obtient que toutes les composantes de x de chaque degré sont dans J . ■

Mais il faut faire attention à l'idéal (X_0, \dots, X_n) , dit *irrelevant* en anglais, homogène maximal mais qui définit l'ensemble vide dans l'espace projectif. Une version correcte de l'énoncé projectif est donc le suivant.

Théorème. (*Théorème des zéros de Hilbert adapté au cas projectif*)

Soit K un corps algébriquement clos. à tout idéal homogène I , on associe $\mathcal{V}(I)$ l'ensemble de ses zéros communs dans \mathbb{P}^n ; à tout ensemble algébrique $V \subseteq \mathbb{P}^n$, on associe l'idéal $\mathcal{I}(V)$ engendré par les polynômes homogènes s'annulant en V . On obtient une bijection entre idéaux réduits homogènes distincts de $K[X_0, \dots, X_n]$, c'est-à-dire en excluant l'idéal *exceptionnel* $I_1 = (X_0, \dots, X_n)$, et sous-ensembles algébriques.

De plus, les sous-variétés correspondent aux idéaux premiers homogènes.

Remarque. (Comment passer des variétés projectives aux cônes affines ?) Soit une variété affine $V = \{x \in \mathbb{P}^N \mid F_1(x) = \dots = F_t(x) = 0\}$. On note $V^{aff} = \{x \in \mathbb{A}^{N+1} \mid F_1(x) = \dots = F_t(x) = 0\}$ la variété affine canoniquement associée et $\pi : \mathbb{A}^{N+1} \setminus \{0\} \longrightarrow \mathbb{P}^N$ la projection canonique de sorte que $\dim(V^{aff}) = \dim(V) + 1$ (voir plus tard). Alors :

$$V^{aff} = \pi^{-1}(V) \cup \{0\}.$$

Remarquons $K(\mathbb{A}^n) = K(X_0, \dots, X_N)$ et $K(\mathbb{P}^N) = K(\frac{X_1}{X_0}, \dots, \frac{X_N}{X_0})$. De plus, $\overline{V^{aff} \cap W^{aff}} = (V \cap W)^{aff}$.

2.3.2 Plongement de Segre

Définition. (Plongement de Segre)

Soient m, n deux entiers naturels. Le *plongement de Segre* $S = S_{m,n} : \mathbb{P}^m \times \mathbb{P}^n \rightarrow \mathbb{P}^N$ avec $N = mn + m + n = (n+1)(m+1) - 1$, est l'application définie par

$$S((x_0, \dots, x_m), (y_0, \dots, y_n)) = (x_i y_j)_{0 \leq i \leq m, 0 \leq j \leq n}.$$

Propriété. (Propriété fondamentale du plongement de Segre)

Le plongement de Segre S identifie $\mathbb{P}^m \times \mathbb{P}^n$ à une sous-variété projective de \mathbb{P}^{mn+n+m} .

▷ Observons tout d'abord que S est bien définie puisque $x_i y_j$ est homogène par rapport aux variables x et aux variables y et, de plus, comme il existe une coordonnée x_{i_0} non nulle et une coordonnée y_{j_0} non nulle, il y a une coordonnée $x_{i_0} y_{j_0}$ non nulle. Ensuite si le point de \mathbb{P}^{mn+n+m} de coordonnées $z_{i,j}$ est égal au point de coordonnées $x_i y_j$ et au point de coordonnées $x_{i_0} y_{j_0}$. On voit aisément que $[x_0; \dots; x_m] = [x'_0; \dots; x'_m]$ dans \mathbb{P}^m et $[y_0; \dots; y_n] = [y'_0; \dots; y'_n]$ dans \mathbb{P}^n ; ainsi S est injective (ce qui justifie appellation plongement). Montrons maintenant que l'image de S est un fermé. Il est immédiat que les points de $(z_{i,j}) \in S(\mathbb{P}^m \times \mathbb{P}^n)$ vérifie les équations : $\forall 0 \leq i, k \leq m, 0 \leq j, h \leq n \quad z_{i,j} z_{k,h} - z_{i,h} z_{k,j} = 0$, puisque $(x_i y_j)(x_k y_h) - (x_i y_h)(x_k y_j) = 0$. Montrons qu'un point $(z_{i,j})$ de \mathbb{P}^{mn+n+m} vérifiant les équations ci-dessus est dans l'image de S . L'une des coordonnées $(z_{i,j})$ est non nulle, pour simplifier les notations on peut supposer que $z_{0,0} = 1$, on peut alors récrire les équations comme $z_{k,h} = z_{0,h} z_{k,0}$. Choisissons donc $P = (1, z_{1,0}, \dots, z_{m,0})$ et $Q = (1, z_{0,1}, \dots, z_{0,n})$, on obtient $S(P, Q) = (z_{i,j})$. ■

Il est clair que le produit de deux variétés affines est une variété affine. C'est moins évident dans le cas projectif.

Corollaire. (Produit de variétés projectives)

Le produit de deux variétés projectives est une variété projective.

Exemple

Le plongement de Segre pour $n = 1$ et $m = 2$ nous donne l'isomorphisme de la quadrique $S : z_{00}z_{11} - z_{01}z_{10} = 0$ à $\mathbb{P}^1 \times \mathbb{P}^1$.

2.3.3 Théorème de l'élimination**Théorème. (Théorème de l'élimination)**

Soit X une variété projective, Y une variété affine ou projective.

1. (*Forme géométrique*) Soit X une variété projective. Alors la projection $p : X \times Y \longrightarrow Y$ est une application fermée.
2. (*Forme algébrique*) (Penser à $X = \mathbb{P}^n$, $Y = \mathbb{A}^n$.) Soient des polynômes $f_j(x, y)$ homogènes en x ; il existe des polynômes $g_i \in K[y]$ tels que :

$$\exists x \neq (0, \dots, 0) \forall i \quad f_j(x, y) = 0 \iff \forall i \quad g_i(y) = 0.$$

▷ Soit $K[X]_s$ l'ensemble des polynômes homogènes de degré s , I_s l'idéal de $K[X]$ engendré par les monômes de degré s et $\mathcal{J}(y)$ l'idéal engendré par les $f_j(x, y)$. Alors, par le Nullstellensatz, $(\forall j \quad f_j(x, y) = 0 \implies x = (0, \dots, 0)) \iff \exists s \geq 1 \quad I_s \subseteq \mathcal{J}(y)$. Posons $W_s = \{y \mid I_s \subseteq \mathcal{J}(y)\}$. Alors $y \in \bigcap_{s \geq 1} W_s \iff \exists w \neq (0, \dots, 0) \forall j \quad f_j(x, y) = 0$. Montrons que W_s est fermé. Pour chaque $M_\alpha(X)$ monôme de degré s , $M_\alpha(X) \in \mathcal{J}(y) \iff M_\alpha(X) = \sum_j A_{j,\alpha}(X) f_j(x, y)$ où le degré du premier terme est $s - d_j$ et $\deg(f_j) = d_j$. Tout polynôme (homogène) $A_{j,\alpha}$ est combinaison linéaire des monômes $N_{\beta,j}$ de degré $s - d_j$. Les polynômes $N_{\beta,j} f_j$ sont dans $K[X]_s$ et leurs coefficients forment une matrice de rang $\leq \dim(K[X]_s) = N$. Ils n'engendrent pas l'espace, si et seulement si, tous les mineurs $N \times N$ sont nuls. ■

Corollaire. (Image d'une variété projective par une application régulière)

Soit $f : X \longrightarrow Y$ régulière et X projective. Alors $f(X)$ est fermé dans Y .

▷ On pose $\Gamma_f = \{(x, y) \in X \times Y \mid y = f(x)\}$. La projection de Γ_f sur Y est $f(X)$. ■

Ceci permet de dire que l'image d'une variété par une application régulière reste une variété.

2.3.4 Grassmannienne

De même que l'ensemble des droites vectorielles de l'espace vectoriel de V est un espace, dit projectif, on peut imaginer définir le même objet pour d'autres types de sous-espaces que les droites. Par exemple, l'ensemble des hyperplans projectifs de V forme un espace dont on voit immédiatement qu'il est le projectif du dual de V . Dans les espaces projectifs, l'ensemble des droites projectives dans \mathbb{P}^2 est isomorphe à \mathbb{P}^2 .

Plus généralement, on peut définir la grassmannienne de V comme l'ensemble des sous-espaces de V de dimension k , si V est de dimension n , et l'on note $Gr(k, n)$.

Voici un exemple.

Théorème

$Gr(1, 3)$ l'ensemble des droites projectives de \mathbb{P}^3 , soit l'ensemble des plans de \mathbb{A}^n , s'identifie naturellement à une variété projective : une quadrique dans \mathbb{P}^5 ; en particulier, $\dim Gr(1, 3) = 4$.



Certains ouvrages utilisent la convention $Gr(2, 4)$ pour noter ce que nous appelons $Gr(1, 3)$, en prenant la dimension affine au lieu de la dimension projective comme nous faisons.

Remarque. $\dim G(k, n) = (k + 1)(n - k)$.

Preuve.

▷ Soit $W \subseteq \mathbb{A}^4$ un sous-espace vectoriel avec $\dim W = 2$. Soit e_1, e_2 une base de W . Notons

$$e_1 = (x_0, \dots, x_3) \text{ et } e_2 = (y_0, \dots, y_3). \text{ On introduit (le produit extérieur) } \phi(e_1, e_2) = \begin{pmatrix} x_0 y_1 - x_1 y_0 \\ x_0 y_2 - x_2 y_0 \\ x_0 y_3 - x_3 y_0 \\ x_1 y_2 - x_2 y_1 \\ x_1 y_3 - x_3 y_1 \\ x_2 y_3 - x_3 y_2 \end{pmatrix}.$$

Le vecteur $\phi(e_1, e_2) \in \mathbb{A}^6 \setminus \{0\}$, donc on peut regarder ϕ à valeurs dans \mathbb{P}^5 . Si e'_1, e'_2 est une autre base, alors $\phi(e_1, e_2) = \phi(e'_1, e'_2)$ dans \mathbb{P}^5 . En effet, si $e'_1 = ae_1 + be_2$, $e'_2 = ce_1 + de_2$, alors $\phi(e'_1, e'_2) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \phi(e_1, e_2)$ dans \mathbb{A}^6 , ce qui se vérifie par un simple, est-ce le mot, calcul. Ceci permet de définir l'application $\phi : Gr(1, 3) \rightarrow \mathbb{P}^5$ qui à $W \mapsto \phi(e_1, e_2)$. Il s'agit de montrer que ϕ est injective et que son image est un sous-ensemble algébrique de \mathbb{P}^5 , en fait même, une quadrique.

Montrons l'injectivité. Supposons $\phi(e_1, e_2) = \phi(e'_1, e'_2) = [z_{ij}] \in \mathbb{P}^5$ pour $0 \leq i < j \leq 3$. On peut supposer $z_{0,1} \neq 0$ et même $x_0 y_1 - x_1 y_0 = 1 = x'_0 y'_1 - x'_1 y'_0$ quitte à remplacer e_1 et e_2 par une autre base de W . On a donc $e_1 = (1, 0, x_2, x_3)$, $e_2 = (0, 1, y_2, y_3)$, $e'_1 = (1, 0, x'_2, x'_3)$, $e'_2 = (1, 0, y'_2, y'_3)$. Alors

$$\phi(W) = \phi(e_1, e_2) = \begin{pmatrix} 1 \\ y_2 \\ y_3 \\ -x_2 \\ -x_3 \\ x_2 y_3 - x_3 y_2 \end{pmatrix} = \begin{pmatrix} 1 \\ y'_2 \\ y'_3 \\ -x'_2 \\ -x'_3 \\ x'_2 y'_3 - x'_3 y'_2 \end{pmatrix} = \phi(W') = (z_{01}, z_{02}, z_{03}, z_{12}, z_{13}, z_{23}).$$

Quand $z_{01} \neq 0$, et l'on peut supposer qu'il égale 1, si $[z_{ij}] \in \phi(Gr(1, 3))$, $z_{23} = (-z_{12})(z_{03}) - (-z_{13})(z_{02})$, puis $\boxed{z_{01} z_{23} + z_{12} z_{03} - z_{13} z_{02} = 0}$ qui définit une forme quadratique. Soit Z l'ensemble des zéros de cette forme quadratique dans \mathbb{P}^5 . Alors $\phi(Gr(1, 3)) \subseteq Z$. Si $P = [z_{ij}] \in Z$, on peut

supposer $z_{01} = 1$, donc les z_{ij} vérifient la première équation ; alors, si l'on pose $e_1 = (1, 0, -z_{12}, -z_{13})$ et $e_2 = (0, 1, z_{02}, z_{03})$ et $W = \text{Vect}(e_1, e_2)$, alors $\phi(W) = \phi(e_1, e_2) = P$. ■

Remarque. $\mathbb{P}^n = \bigcup_{i=0}^n U_i$ avec $U_1 \simeq \mathbb{A}^n$. De plus, $Gr(1, 3) \setminus \{z_{01} = 0\} \simeq \mathbb{A}^4$. Ainsi, $[z_{01}, \dots, z_{23}] = [1, z_{02}, \dots, z_{23}] \rightsquigarrow (z_{02}, \dots, z_{13})$.

2.3.4.1 Grassmannienne de droites

2.3.4.2 Existence de droites contenues dans une hypersurface

2.3.4.3 Une autre application : coordonnées de Chow

2.3.4.4 Le grand théorème de Bézout

Appendice

