Cours de mathématiques

TOME XI

GÉOMÉTRIE

Mathématiques générales

France $\sim$ 2024

Écrit et réalisé par Louis Lascaud

Chapitre 1

Géométrie dans l'espace

Résumé

On s'intéresse d'abord à la géométrie élémentaire euclidienne du plan et de l'espace : incidence, parallélisme, distances, angles. La structure de groupe, notamment grâce aux isométries laissant invariant le polyèdre, est revue en détail.

1.1 Géométrie du plan

1.1.1 Classification des isométries du plan

1.1.1.1 Isométries vectorielles du plan

Définition. ***(Matrice de rotation du plan)***

On appelle *matrice de rotation du plan*, et l'on note de la façon suivante, toute matrice qui s'écrive sous la forme :

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Définition. ***(Matrice de symétrie du plan)***

On appelle *matrice de symétrie du plan*, et l'on note de la façon suivante, toute matrice qui s'écrive sous la forme :

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Proposition. ***(Propriétés opératoires de $\mathcal{O}_2(\mathbb{R})$)***

Soient θ, θ' deux réels. Alors :

(i) $R_\theta R_{\theta'} = R_{\theta+\theta'}$;

(ii) $S_\theta S_{\theta'} = R_{\theta-\theta'}$;

(iii) $R_\theta S_{\theta'} = S_{\theta+\theta'}$;

(iv) $S_\theta R_{\theta'} = S_{\theta-\theta'}$.

Conséquence. ***(Commutativité de*** $SO_2(\mathbb{R})$***)***

Deux matrices de rotation du plan commutent toujours.

Chapitre 2

Géométrie affine ou euclidienne

Résumé

L'objectif principal de ce cours est l'initiation à la géométrie affine et euclidienne. Le lien avec les groupes, en particulier, sera très fort. Le cours donne les bases ou les fondements pour construire les notions dites géométriques de point, de plan, d'espace, d'hyperplan, d'angle, de distance... La géométrie affine, quant à elle, est la géométrie d'Euclide sans les angles ni les distances (plus précisément, sans mesure). Ses objets sont les points, les droites, etc. Les fondements de la géométrie affine permettent de donner un sens nouveau aux théorèmes de la géométrie anciens, comme par exemple, le postulat d'Euclide. On dispose aussi de beaux théorèmes : Thalès, Céva, Ménélaüs. C'est aussi un paradigme de mathématiques déductives.

2.1 Motivations. Qu'il faut savoir de quoi l'on parle

Exercice 1

Qu'est-ce qu'un point ? Un triangle ? Une droite ? Un plan ? Un angle ?

▷ **Éléments de réponse.**

On peut s'appuyer, au choix, sur les axiomes d'Euclide ou sur la formulation cartésienne de la géométrie.

Pour sentir ce qu'est la géométrie axiomatique, on propose l'activité suivant. On admet le cinquième postulat d'Euclide, qui s'énonce de la manière suivante :

Axiome. ***(Euclide)***

Étant donné dans un plan une droite et un point n'appartenant pas à cette droite, il existe une unique droite passant par ce point parallèle à cette droite.

Mais il faut d'abord définir ce qu'est le parallélisme ! L'élève peut aisément deviner ce qu'elle est dans le plan :

Définition. ***(Parallélisme)***

Deux droites d et d' du plan sont *parallèles*, si et seulement si, $(d = d' \text{ ou } d \cap d' = \emptyset)$.

Tout l'intérêt de l'activité repose dans l'exercice par le lecteur de la démonstration suivante :

Exercice 2

Montrer que la relation de parallélisme est une relation d'équivalence.

▷ **Éléments de réponse.**

Seule la transitivité est intéressante, et requiert bel et bien le cinquième postulat d'Euclide (en particulier, dans les géométries non euclidiennes, la relation de parallélisme n'est pas transitive !). Ensuite, montrer le parallélisme de deux droites revient à montrer logiquement une disjonction, méthode de raisonnement classique.

Méthode. ***(Étudier une figure ou un lieu géométrique)***

1. Cas de dégénérescence
2. Relations entre les mesures : liens longueurs des arêtes, angles, etc.
3. Caractérisations parmi d'autres
4. Passage en dimensions supérieures

2.2 Application affine

Théorème. ***(Envoi de points)***

Soit $(a_0,...,a_n)$ un repère affine de $\mathcal{E}$ et soient $b_0,...,b_n$ des points quelconques de $\mathcal{F}$. Il existe alors une unique application affine f telle que pour $i = 0,...,n$, $f(a_i) = b_i$.

▷ Par hypothèse, $a_0a_1,...,a_0a_n$ forment une base de la direction E de $\mathcal{E}$. Posons, pour tout i, $\varphi(a_0a_i) = a_0b_i$. L'application linéaire φ est entièrement déterminée par ces données (voir le cours d'algèbre linéaire). Par suite, on peut définir une application affine sur $\mathcal{E}$ par $f(M) = a_0 + \varphi(a_0M)$. Alors il est clair que $f(a_i) = a_0 + \varphi(a_0a_i) = a_0 + a_0b_i = b_i$. Pour l'unicité, elle vient de ce qu'une application affine préserve les barycentres, et que tout point d'un espace affine s'écrit comme barycentre des points d'un repère. ■

On remarque que : **f est une transformation si et seulement si les points $(a_0,b_1,...,b_n)$ sont affinement indépendants.**

2.2.1 Groupe affine

Propriété

En dimension finie, l'action du groupe affine sur les simplexes est transitive.

▷ C'est la propriété précédente sous la bonne définition des simplexes. ■

Chapitre 3

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. L'aspect pratique de cette introduction est sous-tendu par un pré-requis d'algèbre commutative à confirmer.

3.1 Prolégomènes

3.1.1 Sous-ensembles algébriques d'un espace vectoriel

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

Soit K un corps et l'on note $\mathbb{A}^n_K = K^n$ un K-espace vectoriel. Un *sous-ensemble algébrique* est un ensemble de la forme $V = \{x \in K^n \mid \forall i \in I \quad P_i(x) = 0\}$ où $(P_i)_{i\in I} \in K[X_1,...,X_n]^I$, I un ensemble. On parle également de *variété algébrique*[a] de K^n.
On observe immédiatement que si I est l'idéal engendré par les P_i, alors I est l'ensemble des zéros d'éléments de I. Par suite, à un idéal I de $K[X_1,...,X_n]$, on peut lui associer $\mathcal{V}(I) = \{x \in K^n \mid \forall P \in I \quad P(x) = 0\}$ son *lieu commun d'annulation*. Réciproquement, pour $S \subseteq K^n$, on peut lui associer $\mathcal{J}(S) = \mathcal{I}(S) = \{P \in K[X_1,...,X_n] \mid \forall x \in S \quad P(x) = 0\}$ son *idéal annulateur (multiple)*.

[a] Convention non universelle. Dans ce cours, on réserve cette appellation aux sous-ensembles algébriques irréductibles, voir la section Variétés affines et projectives.

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.

Propriété

L'anneau $K[X_1,...,X_n]$ est principal $\iff$ $n = 1$. Il est toujours factoriel et noethérien.

Heuristique

Prenons V l'ensemble des zéros de $P \in K[X_1,...,X_n]$ où $P = X_1^2 + ... + X_n^2 + 1$. 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 $\mathcal{J}(S_2) \subseteq \mathcal{J}(S_1)$.

3.1.2 Espaces affines et espaces projectifs

3.1.2.1 Généralités de géométrie projective

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 $V_1 \cap V_2 \geqslant \dim V_1 + \dim V_2 - n$ (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 $P = [x_0,...,x_n] = [\lambda x_0,..., \lambda x_n] \in \mathbb{P}^n$. Si $F \in K[x_0,...,x_n]$, $F(P)$ n'a aucun sens. Si F est homogène de degré d, par définition $F(\lambda x_0,...,\lambda x_n) = \lambda^d F(x_0,...,x_n)$, 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 $\{[x_0,...,x_n] \in \mathbb{P}^n \mid \forall i \in I \quad F_i(x_0,...,x_n) = 0\}$ avec les F_i homogènes.

Définition-propriété. ***(Idéal homogène)***

Si I est l'idéal engendré par les F_i dans $K[X_0,...,X_n]$, on dit que c'est un *idéal homogène*. Il est équivalent de dire que I est un idéal de $K[X_0,...,X_n]$ et si $I \ni F = F_0 + ... + F_d$ sa décomposition homogène, alors tous les $F_j \in I$.
Le sous-ensemble algébrique précédent est alors $\{[x_0,...,x_n] \in \mathbb{P}^n \mid \forall F \text{ homogène } \in I \quad F(x_0,...,x_n) = 0\}$.

▷ 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 $h_j \in k[X_0,...,X_n]$. 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 $K \subseteq \{1,...,m\}$. 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 $\{g_1,...,g_m\}$ un système de générateurs de I, fini par noethérianité. Alors l'ensemble des $h \in K[X_0,...,X_n]$ 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 $\mathbb{P}(V)$ d'un sous-espace vectoriel de $\mathbb{A}^{n+1}$.
On définit : $\dim(\mathbb{P}(W)) = \dim(W) - 1$.

▷ Prenons $V = \{[x_0,...,x_n] \in \mathbb{P}^n \mid L_1(x) = ... = L_r(x) = 0\}$ 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 $\{(x_0,...,x_n) \in \mathbb{A}^{n+1} \mid L_1 = ... = L_r = 0\}$, 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 $rg(S)$ 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 une 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 $\dim(V_1) + \dim(V_2) \geqslant n$, alors $V_1 \cap V_2 \neq \emptyset$ et $\dim(V_1 \cap V_2) \geqslant \dim(V_1) + \dim(V_2) - n$.

▷ $\tilde{V_1}$ 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 $\dim \tilde{V_1} \cap \tilde{V_2} \geqslant (\dim V_1+1)+(\dim V_2+1)-(n+1) = (\dim V_1+\dim V_2-n)+1 \geqslant 1$ donc $\mathbb{P}(\tilde{V_1} \cap \tilde{V_2}) \neq \emptyset$. Or $\dim(V_1 \cap V_2) = \dim \mathbb{P}(\tilde{V_1} \cap \tilde{V_2}) = \dim(\tilde{V_1} \cap \tilde{V_2}) - 1 \geqslant \dim V_1 + \dim V_2 - n$. 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* $H_i = \{[x_0,...,x_n] \in \mathbb{P}^n \mid x_i = 0\}$ 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, $\mathbb{P}^n = U_0 \bigcup H_0 \simeq \mathbb{A}^n \bigsqcup \mathbb{P}^{n-1}$. 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 $i = 0$, $P = [x_0,...,x_n] \in U_0$ donc $x_0 \neq 0 = [1, \frac{x_1}{x_0},..., \frac{x_n}{x_0}]$. 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 $U_0 \longrightarrow \mathbb{A}^n$, définie par $[x_0,...,x_n] \longmapsto (\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})$, de réciproque $\psi : (y_1,...,y_n) \longmapsto [1, y_1,...,y_n]$. Elle est bien définie par des polynômes. ■

Observation

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

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 $[x_0,x_1,x_2] \longrightarrow (\frac{x_1}{x_0}, \frac{x_2}{x_0})$ de réciproque $(x,y) \longmapsto [1,x,y]$. 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 $\overline{V} = \{[x_0,...,x_n] \in \mathbb{P}^n \mid F(x_0,...,x_n) = 0\}$. 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 $\overline{V} \cap U_0 = \{[1,y_1,...,y_n] \in \mathbb{P}^n \mid F(1, y_1,..., y_n) = 0\}$ dans U_0 hypersurface de $\mathbb{A}^n$ définie par $F(1,y_1,...,y_n) = 0$ polynôme de degré $\leqslant d$. On la note V. Alors $\overline{V} = (\overline{V} \cap U_0) \sqcup (\overline{V} \cap H_0)$. Or $\overline{V} \cap H_0 = \{[0,x_1,...,x_n] \in \mathbb{P}^n \mid F(0,x_1,...,x_n) = 0\}$ polynôme homogène de degré d. Remarque : si $F = x_0F_1$, alors $F(0,x_1,...,x_n) \equiv 0$. Supposons que X_0 ne divise pas F. Alors $F(0,x_1,...,x_n) \not\equiv 0$. $\overline{V} \cap H_0$ est une hypersurface de $H_0 = \mathbb{P}^{n-1}$ de degré d. Alors $\overline{V} = \psi(V) \sqcup (\overline{V} \cap H_0)$ réunion d'une hypersurface affine dans $\mathbb{A}^n$ et d'une hypersurface projective de $\mathbb{P}^{n-1}$. Si maintenant $F = X_0F_1$, Alors $\overline{V} = (\overline{V} \cap U_0) \sqcup H_0$. Pour $F(x_0,...,x_n)$ donné (homogène), l'hypersurface affine associée est définie par $f(y_1,...,y_n) = F(1,y_1,...,y_n)$. Si $f(y_1,...,y_n) = 0$ définit $V \subseteq \mathbb{A}^n$, on veut $\overline{V} \subseteq \mathbb{P}^n$ telle que $\overline{V} \cap U_0 = \psi(V)$. On prend $F(x_0,...,x_n) = x_0^d f(\frac{x_1}{x_0},..., \frac{x_n}{x_0})$ avec $d = \deg_{\text{total}}(f)$. Rappelons l'essence de ce procédé : d'une part $F(\lambda x_0,..., \lambda x_n) = \lambda^d F(x_0,...,x_n)$ et $F \in K[X_0,...,X_n]$ et x_0 ne divisant par F, il existe un monôme $X_1^{i_0}...X_n^{i_n}$ de degré d avec son coefficient non nul ; d'autre part, $F(1,x_1,...,x_n) = f(x_1,...,x_n)$. Ces deux constructions ne sont pas rigoureusement identiques, mais presque, en ce sens qu'elles sont bijectives. On a bien finalement $\overline{V} \cap U_0 = Q(V)$.

3.1.2.2 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 $X = [X_0,...,X_n]$, $Y_j = \sum_{i=0}^{n} a_{ji}X_i$ ce qui fournit une application :

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

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. ■

3.1.2.3 Paramétrage des sous-espaces linéaires

On voit comment ça marche sur une exemple.

Exemple. ***(Paramétrer un s.e.l)***

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

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

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.

3.1.3 Courbes affines, courbes projectives

3.1.3.1 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)*

Une *courbe de degré d* est un polynôme homogène non nul de degré d en (X,Y,Z) modulo la relation $F_1 \sim F_2 \iff \exists \lambda \in K^\times \quad F_2 = \lambda F_1$.
Remarquons que si $V = K[X,Y,Z]_d$, l'ensemble des courbes de degré d est $\mathbb{P}(V)$.

Reformulation pratique. *(Courbe et ensembles algébriques)*

Les ensembles algébriques sont les intersections quelconques de courbes.

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 $D \subseteq C$.

---

[1] En effet, si $H(U,V)$ est un polynôme homogène de degré d non nul, alors $H(u,1) = a_0 \prod_{j=1}^{d_1}(u - \alpha_i)$ car c'est un polynôme à une variable de degré $d_1 \leqslant d$. 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 $n \geqslant 2$; 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).

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

L'espace des polynômes homogènes de degré d en $X_0,...,X_n$ 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.

3.1.3.2 Application : le théorème des 5 points

De la propriété précédente, on déduit :

Proposition. ***(Théorème des cinq points projectif)***

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

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

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 $P_1,...,P_5$ 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 $\{P_1,...,P_n\}$ 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 point et d'une droite passant par l'autre est une conique ; il n'y a pas unicité.

Réciproquement, supposons que $P_1,...,P_3 \in D$. Soit C une conique passant par $P_1,...,P_5$. 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 $\dim(S_2(P_1,...,P_5)) \geqslant 2$. Alors pour tout P_6, $\dim(S_2(P_1,...,P_6)) \geqslant 1$. 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 $P_1,...,P_6$. 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 $\dim(S_2(P_1,...,P_5)) = 1$ 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 3

(Et dans $\mathbb{A}^2$?) Soient $P_1,...,P_5 \in \mathbb{A}^2$. 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 $(a,c,d,e,f) \neq (0,...,0)$. 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 neufs points)*

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

Plus généralement encore :

Proposition. *(Théorème des quelques points)*

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

On retiendra l'inégalité fondamentale :

Formule

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

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...)

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

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 $\geqslant 2$.

Lemme

Soit $f = 0$ l'équation de $C \ni P = (x_0,y_0)$ et $f = f_0 + ... + f_d$ la décomposition homogène de f en $(x - x_0,y - y_0)$ avec les notations évidentes, soit $f = f(x_0,y_0)(= 0) + a(x - x_0) + b(y - y_0) + f_2(x - x_0,y - y_0) + ...$ 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 $(\frac{\partial f}{\partial x}(x_0,y_0), \frac{\partial f}{\partial y}(x_0,y_0)) \neq (0,0)$.

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.

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.

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 $\frac{\partial}{\partial X}(FG) = \frac{\partial}{\partial X}F.G + F\frac{\partial}{\partial X}G$ vaut 0 en $(x_0,...,z_0)$. ■

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 $\geqslant 2$; par le théorème de Bézout, $D \subseteq C$. ■

Exercice 4

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

3.1.3.4 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 $(U_0,U_1) \mapsto (U_0^2, U_1^2, U_0U_1)$, 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 $\mathbb{P}^1 \dashrightarrow C$ 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 $\mathrm{car}(K) \neq 2$. 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 $[U_0^2,U_1^2,U_0U_1] = [V_0^2, V_1^2, V_0V_1]$. 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 $XY - Z^2$. 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 $\mapsto \pi^{-1}(droite)$, 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 $\mathcal{D}_{P_0} = \{[a,b] \mid [a,b] \in \mathbb{P}^1\}$. 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 $(A\frac{b^2}{a^2} - B\frac{b}{a} + c)Y + (-D\frac{b}{a} + E)Z = 0$. ■

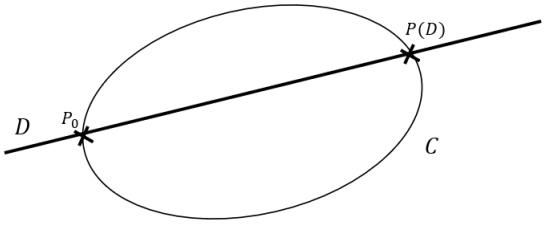

FIGURE 3.1.1 : *Description des coniques projectives.* —
Illustration du cas non algébriquement clos, par exemple $\mathbb{P}^2(\mathbb{R})$.

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

3.1.3.5 Cubiques et courbes elliptiques

Nous allons voir qu'avec une petit 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 suivant : 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,

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

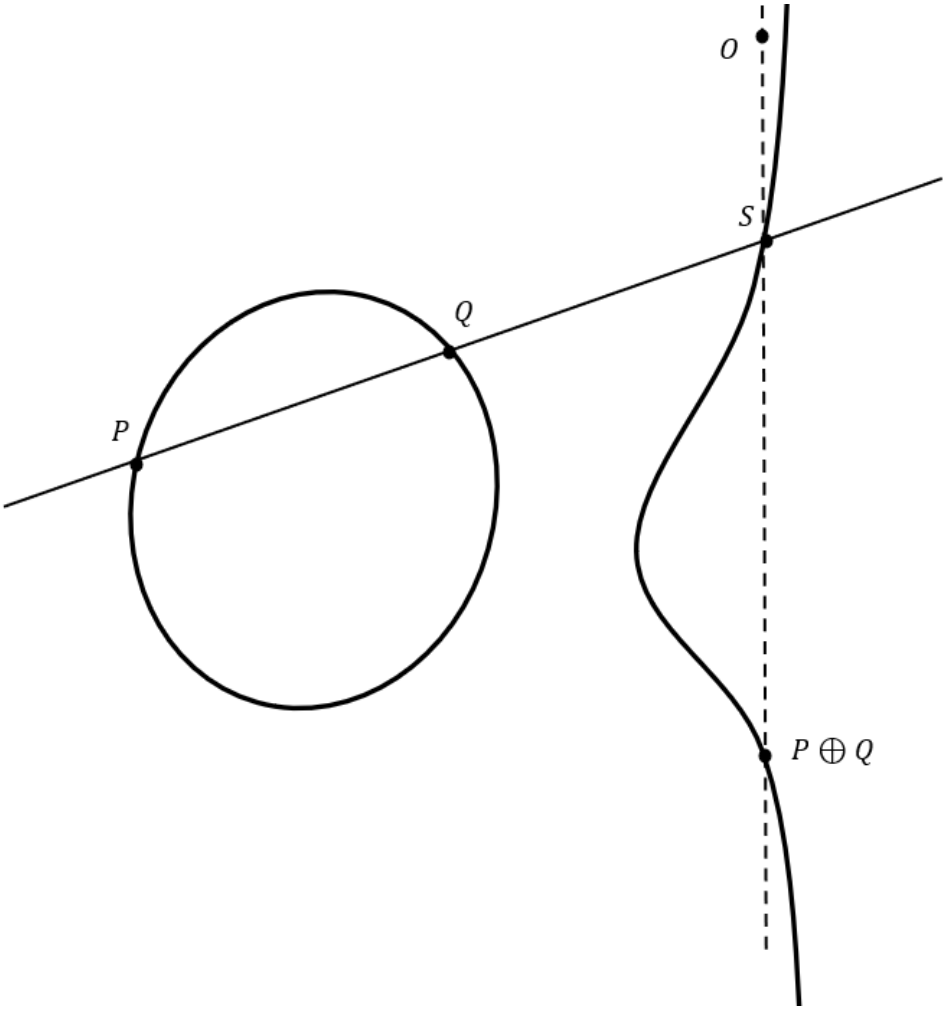

FIGURE 3.1.2 : *Addition de deux points d'une cubique.* —
Définition d'une loi de groupe sur une cubique à deux composantes connexes. Notons que le point O est égal en projectives au point à l'infini de l'autre branche.

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

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

on pose $T' = (P \oplus Q) \oplus R$ et $W' = P \oplus (Q \oplus R)$. On veut montrer $W' = T'$, c'est-à-dire, $W = T$ *(voir le dessin sur tableau reproduit ci-dessous)*.

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 $K[X_1,...,X_n]$. 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 huits points)***

Soient $P_1,...,P_8$ 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 $\dim(S_3(P_1,...,P_8)) = 2$.

▷ Remarquons que $\geqslant 2$ est immédiat.

Dans le premier cas, P_1,P_2 et P_3 sont alignés. On choisit $Q \in D_{P_1P_2}$ distinct d'eux trois, de sorte que $\dim(S_3(P_1,...,P_8,Q) \geqslant 1$, donc il existe une cubique C passant par $P_1,...,P_8$ 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 $\dim(S_3(....,Q) = 1$, donc $\dim(S_3(P_1,...,P_8) \leqslant 2$, donc elle est égale à 2.

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

Enfin, supposons qu'il n'y a aucun triplet aligné, aucun sextuplet conconique. Supposons que $\dim(S_3(P_1,...,P_8)) \geqslant 3$. On choisit $Q,R \in D_{P_1P_2}$ distincts. Alors $\dim(S_3(P_1,...,P_8,Q,R) \geqslant 3-2 = 1$; il existe donc une cubique C passant par ces 10 points. Alors $\{P_1,P_2,Q,R\} \subseteq C \cap D_{P_1P_2}$, donc $C = D_{P_1P_2} \cup C_0$ conique. Ainsi $P_3,...,P_8 \in C_0$, 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 $\{P_1,...,P_9\} = C \cap C_1$ avec $P_1,...,P_8$ distincts, alors si un troisième conique C_2 passe par $P_1,...,P_8$, elle passe par P_9.

▷ Si $P_1,...,P_4$ étaient alignés sur D, on aurait $\{P_1,...,P_4\} \subseteq C \cap D$, donc $C = D \cup C_0$, absurde. Si $P_1,...,P_7$ étaient conconiques dans C_0, $\{P_1,...,P_7\} \subseteq C \cap C_0$, donc C est non irréductible ; absurde. Soit F l'équation de C, F_1 celle de C_1. Ainsi $S_3(P_1,...,P_8) = vec(F,F_1)$ de dimension 2. Soit F_2 l'équation définissant C_2. On obtient $F_2 \in S_3(P_1,...,P_8)$, 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 a 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 $\lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + A}{y_1 + y_2}$ 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 $x^3 + Ax + B - (\lambda x + \mu)^2 = (x - x_1)...(x - x_3) = 0$, 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. ■

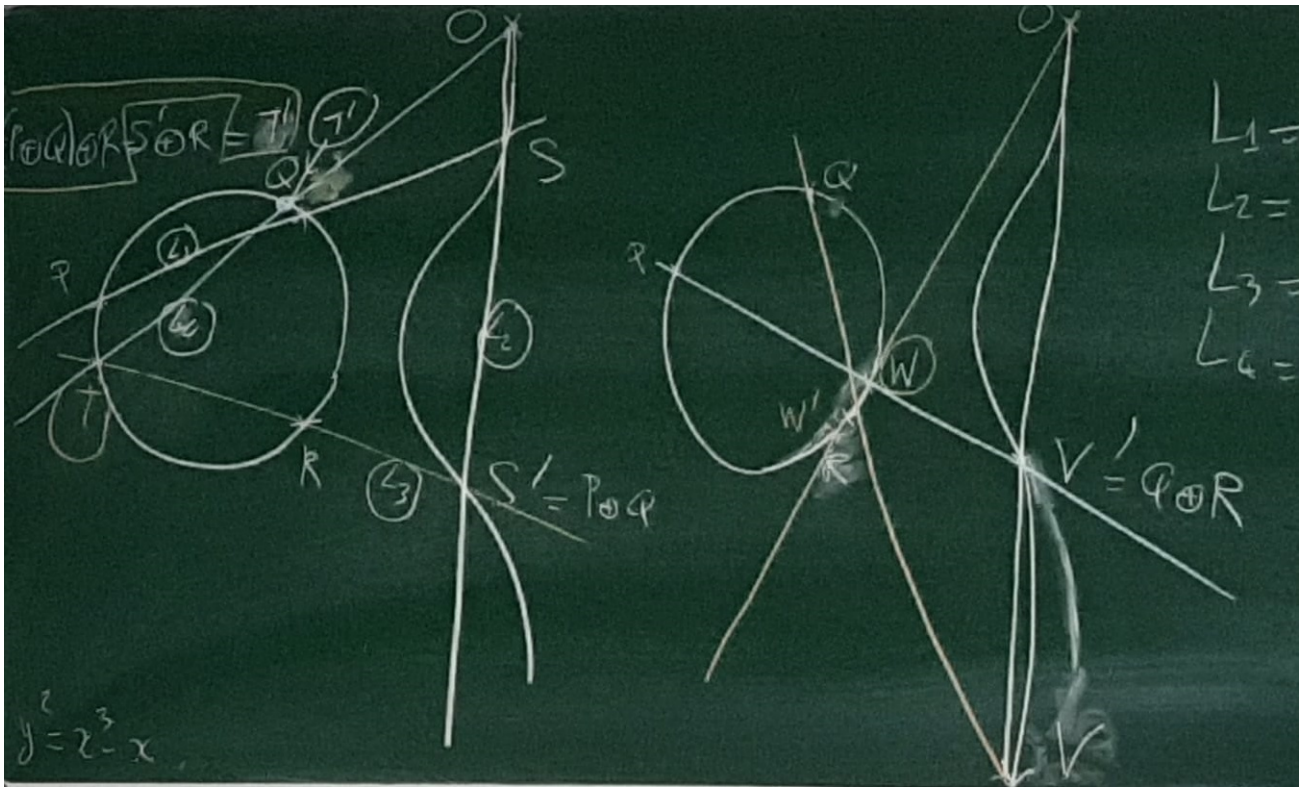

FIGURE 3.1.3 : *Associativité de la loi sur une cubique.* —
Les notations sont celles de la preuve.

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 $\mathbb{P}^1 \longrightarrow C$ 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. □

3.2 Variétés affines et projectives

3.2.1 Introduction

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 $\{\mathcal{V}(I), I \text{ idéal de } K[X_1,...,X_n]\}$. Ainsi, les sous-ensembles algébriques sont les fermés d'une topologie (dite *de Zariski*).

▷ On a $\mathcal{V}(K[X_1,...,X_n]) = \emptyset$ et $\mathcal{V}(\{0\}) = K^n$, $\bigcap_{j\in J} \mathcal{V}(I_j) = \mathcal{V}(\sum_{j\in J} I_j)$, 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. $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$.
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 $\mathcal{J}(\mathcal{V}(I)) = \sqrt{I}$).

▷ Les inclusions proposées sont tautologiques. Soit S un sous-ensemble algébrique, soit $S = \mathcal{V}(I)$ pour un certain idéal I de $K[X_1,...,X_n]$. 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 $P = X$. □

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. □

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 $K[X_1,...,X_n]$ 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 :

3.2.2 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 $K[X_1,...,X_n]$ qui à un ensemble algébrique $S \longmapsto \mathcal{J}(S)$ et de réciproque qui à $I \longmapsto \mathcal{V}(I)$. En particulier, on peut identifier les deux.
3. *(Troisième forme)* (Un peu pompeusement, car c'est la réécriture de la première

forme.) Pour $I = (P_1,...,P_r), Q \in K[X_1,...,X_n]$, si $(P_1(x) = ... = P_r(x) = 0 \implies Q(x) = 0)$, alors il existe $M \geqslant 1$, $A_1,...,A_r \in K[X_1,...,X_n]$ 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 $A_i \in K_0[X_1,...,X_n]$.

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

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

Soit $L = K[t_1,...,t_n]$ 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 $t_1,...,t_n$ 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 $L = K[x_1,...,x_n]$ une algèbre de type fini. Il existe $y_1,...,y_r \in L$ algébriquement indépendants sur K tels que $L/K[y_1,...,y_r]$ soit entière (algébrique).

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

Montrons donc cela. On a que x_{n+1} est algébrique sur $K(x_1,...,x_r)$, donc en prenant la décomposition homogène $F_d(x_1,...,x_{n+1}) + F_{d-1}(x_1,...,x_{n+1}) + ... + F_1 = 0$. Alors $x_i = y_i + a_i x_{r+1}$ pour $1 \leqslant i \leqslant r$ et $a_i \in K$, $F_d \not\equiv 0$. Par suite, $F_d(a_1,...,a_r,1)x_{r+1}^d +$ termes de degré $\leqslant d-1$ en $x_{n+1} = 0$. Comme le corps est infini, il existe $a_1,...,a_r \in K, F_d(a_1,...,a_n,1) \neq 0$. Donc x_{n+1} est un entier algébrique sur $K[y_1,...,y_r]$.

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

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

Posons $L = K[x_1,...,x_n]$ un corps. Alors par le lemme, L est entier sur $K[y_1,...,y_r]$ où les y_i sont algébriquement indépendants. Par une propriété classique de théorie des nombres, $K[y_1,...,y_r]$ 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 $I \subsetneq K[X_1,...,X_n]$, alors $\mathcal{V}(I) \neq \emptyset$.

▷ D'après le théorème de Krull, il existe $I \subseteq \mathfrak{M} \subsetneq K[X_1,...,X_n]$ où $\mathfrak{M}$ est un idéal maximal. Introduisons $L = K[X_1,...,X_n]/\mathfrak{M}$. C'est un corps. Posons $x_i = X_i \bmod \mathfrak{M}$; on a $L = K[x_1,...,x_n]$. Par la proposition-clef, L/K est algébriquement, donc $L = K$, car K est algébriquement clos, donc $x_i \in K$ et pour tout $P \in \mathfrak{M}$, $P(x_1,...,x_n) = P(X_1 \bmod \mathfrak{M},..., X_n \bmod \mathfrak{M}) = P(X_1,...,X_n) \bmod \mathfrak{M} = 0$. Ainsi $(x_1,...,x_n) \in \mathcal{V}(\mathfrak{M}) \subseteq \mathcal{V}(I)$, d'où $\boxed{\mathfrak{M} = (X_1 - x_1,...,X_n - x_n)}$. En effet : notons $\mathfrak{M}' = (X - x_1,...,X - x_n)$. Si $P(x_1,...,x_n) = 0$, alors $P \in \mathfrak{M}'$. En effet, il suffit de diviser euclidiennement dans $K[X_1,...,X_{n-1}][X_n]$ 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 $P(x_1,...,x_n) = 0$ 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 $K[X_1,...,X_n,T]$. Alors $P_1(X),...,P_r(X), 1 - TQ(X)$ n'ont aucun zéro commun. En effet, si $P_1(x) = ... = P_r(x) = 0$, alors $1 - tQ(x) = 1 \neq 0$. D'après le théorème faible, l'idéal engendré par $P_1,...,P_r,1 - TQ$ est égal à $K[X_1,...,X_n,T]$, c'est-à-dire qu'il existe $A_i(X,T) \in K[X_1,...,X_n,T)$ tels que $1 = A_1(X,T)P_1(X) + ... + A_r(X,T)P_r(X) + B(X,T)(1 - TQ(X))$. Or $K[X_1,...,X_n,T] \subseteq K(X_1,...,X_n)[T]$. On pose $T = 1/Q(X)$. Ainsi $1 = \sum_{i=1}^{r} A_i(X, \frac{1}{Q(X)})P_i(X)$ dans $K(X_1,...,X_n)$. Posons $M = \max(\deg_T(A(X,T)))$, d'où $Q^M = \sum_{i=1}^{r} Q^M A_i(X, \frac{1}{Q})P_i(X)$ à coefficients dans $K[X_1,...,X_n]$, et le théorème est démontré. ■

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

3.2.2.1 Conséquences du Nullstellensatz de Hilbert

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

Supposons K algébriquement clos. Tout idéal strict I de $K[X_1,...,X_n]$ 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 $K[X_1,...,X_n]$.

Corollaire. *(Théorème de d'Alembert-Gauss)*

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

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

Supposons K algébriquement clos. Tout idéal maximal de $K[X_1,...,X_n]$ est de type fini engendré par n élements. Explicitement, $\mathfrak{M} = \langle f_1,...,f_r \rangle$ 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 $K[X_1,...,X_n]$ est engendré par $\leqslant n$ polynômes ! Tout idéal de $K[X_1,...,X_n]$ 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 $K[X_1,...,X_n]$ n'étant pas principal pour $n \geqslant 2$, 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 $K[X_1,...,X_n]$ 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.

3.2.3 La 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 $K[X_1,...,X_n]$.
En particulier, tout idéal maximal de $K[X_1,...,X_n]$ 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 $K[X_1,...,X_n]$ 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 W qui ne peut contenir de branches infinis. Cette construction donne $V = W_1 \cup ... \cup W_r$ avec les W_i irréductibles qui sont les racines de cet arbre. ■

Remarque importante. Si on impose que pour tout $i \neq j$, $W_i \subsetneq W_j$ et $W_j \subsetneq W_i$, 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 $\mathcal{V}(I_1) \cup \mathcal{V}(I_1) = \mathcal{V}(I_1 I_2)$. 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.

3.2.4 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.

3.2.4.1 L'algèbre de coordonnées d'une variété affine

Définition. ***(Algèbre des coordonnées)***

Soit V une variété algébrique affine. On note $K[V] = K[X_1,...,X_n]/I_V$, 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 $P : V \to \mathbb{A}^1$, et $\overline{f} = \overline{g}$ 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 $P_1P_2 \in V$. Ainsi V_1 le lieu d'annulation de $P_1 \subsetneq V$ et V_2 de $P_2, \subsetneq V$. Il suit que $V_1 \cup V_2 = \{x \in V, P_1P_2(x) = 0\} = V$. 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_1P_2 s'annule sur V, car il s'annule sur V_1 et V_2, donc I_V n'est pas 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 $f_1,...,f_m \in K[X_1,...,X_n]$ tels que $\forall x \in V \quad f(x) = (f_1(x),...,f_m(x))$, avec $(f_1(x),...,f_m(x)) \in W$. 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 :

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

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

▷ Soit $f = (f_1,...,f_m)$ par définition. Si $P \in K[Y_1,...,Y_m]$, $h \in K[W]$ la classe de P modulo I_W, $f^\star(h) = (P \circ (f_1,...,f_m)(X_1,...,X_n))$ 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 $x \in V$, $(f_1(x),...,f_n(x)) \in W \iff \forall P \in I_W \quad P(f_1(x),...,f_m(x)) = 0$.

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 $\phi = f^\star$. De plus, si $V \xrightarrow{f} W \xrightarrow{g} X$, $(g \circ f)^\star = f^\star \circ g^\star$.

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 $t_1,...,t_n \in A$ tels que $A = K[t_1,...,t_n]$, donc il existe $K[X_1,...,X_n] \hookrightarrow A$ une surjection ψ qui à $X_i \mapsto t_i$, si $I = \mathrm{Ker}(\psi)$, on a $A \simeq K[X_1,...,X_n]/I$. 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, $f^\star : K[W] \longrightarrow K[V]$ et $g^\star : K[V] \longrightarrow K[W]$ 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 $\phi = f^\star$ et $\psi = g^\star$. On obtient $(f \circ g)^\star = id_W^\star$ et $(g \circ f)^\star = id_V^\star$ d'où $f \circ g = id_W$ et $g \circ f = id_V$.

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

3.2.4.2 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 $K(V) = Frac(K[V])$, 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 $\mathrm{dom}(f)$ 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 $\mathrm{dom}(f) = V \setminus \mathcal{V}(D_f)$ et cela suffira. Soit $x \in \mathrm{dom}(f)$. 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 $x \notin \mathrm{dom}(f)$. 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 $V \setminus \mathcal{V}(f_2) \subseteq \mathrm{dom}(f)$ 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 $\mathcal{O}_{V,x}/\mathfrak{M}_{V,x} \to K$, 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'appartient 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 $\mathfrak{M}_{U,x} \subseteq O_{U,x} \subseteq K(U)$. 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 $\mathfrak{M}_{U,x} \subseteq O_{U,x} \subseteq K(U)$. 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 $\mathrm{dom}(f) := V \setminus \mathcal{V}(D_f) = V$, 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 $U_i = \{[x_0,...,x_n] \in \mathbb{P}^n, x_i \neq 0\} \simeq \mathbb{A}^n$ par $[x_0,...,x_n] \mapsto (\frac{x_0}{x_i},...,\hat{1},..., \frac{x_n}{x_i})$ de réciproque $(y_1,...,y_n) \mapsto [y_1,...,\frac{1}{i},..., y_n]$. L'application $f_i = f_{|U_i}$ est un polynôme en $(y_1,...,y_n)$ de sorte que $f_i(\frac{x_0}{x_i},..., \frac{x_n}{x_i}) = x_i^{-d_i} F_i(x_0,...,x_n)$ est un polynôme homogène de degré d_i avec X_i ne divisant par 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. ■

3.2.4.3 Applications rationnelles, applications birationnelles

Définition. ***(Application rationnelle)***

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

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

Définition. ***(Application dominante)***

Une application rationnelle $f : V \cdots \to W$ entre deux variétés V,W affines est dite *dominante* si $f(\mathrm{dom}(f))$ 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 $f^\star : K(W) \longrightarrow K(V)$, $h \mapsto h \circ f$ est bien définie.

Définition. ***(Isomorphisme birationnel)***

Un *isomorphisme birationnel* est une application rationnelle $f : V \cdots \to W$ telle qu'il existe $g : W \cdots \to V$ telles que $f \circ g = id_W$ et $g \circ f = id_V$ 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 $f \cdots \to W$ telle que $\phi = f^\star$. De plus, $(g \circ f)^\star = f^\star \circ g^\star$. De plus, si $V \xrightarrow{f} W \xrightarrow{g} X$.

$\triangleright$ $g^\star \circ f^\star = id_W^\star$, $f^\star \circ g^\star = id_V^\star$ et $g^\star : K(V) \longrightarrow K(W)$, $f^\star : K(W) \longrightarrow K(V)$. Si $\phi : K(W) \simeq K(V)$, $\phi = f^\star$ puis $\phi^{-1} = g^\star$ 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 $f : V \longrightarrow W$ et l'on se

ramène au théorème dans le cas des variétés affines. Vérifions que l'on peut toujours se ramener à ce cas. $K[W] = K[t_1,...,t_m] \subseteq K[V_g]$ donc $K[W] \subseteq K[V][t_1,...,t_m] \subseteq K(V)$. ■

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 $f : V \cdots \to W$ et $g : W \cdots \to V$ sont des applications rationnelles et inverses, notons $\tilde{f}$ la restriction de f à son domaine de $\tilde{g}$ la restriction de fg à $\mathrm{dom}(g)$. Posons $V_0 = \tilde{f}^{-1}\tilde{g}^{-1}\mathrm{dom}(f)$ et $W_0 = \tilde{g}^{-1}\tilde{f}^{-1}\mathrm{dom}(g)$. 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 $f : V \longrightarrow W$ qui à $t \mapsto (t^2,t^3)$ de réciproque $g : (x,y) \cdots \to \frac{y}{x}$. C'est un isomorphisme birationnel et ici explicitement $V_0 = \mathbb{A}^1 \setminus \{0\}$, $W_0 = W \setminus \{(0,0)\}$. C'est une exemple où l'on peut exhiber un isomorphisme birationnelle 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 $x_1,...,x_d$ algébriquement indépendants tels que $K(V)/K(x_1,...,x_d)$ soit algébrique de degré fini. Par le théorème de l'élément primitif, $K(V) = K(x_1,...,x_d)(y)$. En particulier, y est racine d'un certain $y^n + f_{n-1}(x_1,...,x_d)y^{n-1} + ... + f_0(x_1,...,x_d) = 0$. Il existe $g \in K[X_1,...,X_d]$ tel que $gf_j \in K[X_1,...,X_d]$ en remplaçant g par gy, on peut supposer $f_j \in K[X_1,...,X_d]$. Posons $F(X_1,...,X_d,Y) = Y^n + f_{d-1}Y^{n-1} + ... + f_0(X) = 0$ et $W = \{(x_1,...,x_d,y) \in \mathbb{A}^{d+1} \mid F(x,y) = 0\}$. Alors $K[W] = K[x_1,...,x_d,Y]/(F) = K[x_1,...,x_d,y]$, y vérifiant la condition ci-dessus. D'où $Frac(K[W]) = K(x_1,...,x_d)(y) \simeq K(V)$, d'où le résultat. ■

3.2.4.4 Image d'une variété affine

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

Soit $f : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ qui à $(x,y) \mapsto (x,xy)$. C'est une application polynomiale, régulière, et même birationnelle.
Cherchons 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. □

3.2.5 Variétés projectives

3.2.5.1 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 $K[X_1,...,X_{n+1}]$, ou, ce qui revient au même, les zéros communs d'un idéal homogène de $K[X_1,...,X_{n+1}] \simeq K[X_0,...,X_n]$ 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 $K[X_0,...,X_n]$.

▷ Le radical d'un idéal homogène est homogène. Soit I un idéal homogène de $K[X_1,...,X_n]$ 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 $(X_0,...,X_n)$, 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 $K[X_0,...,X_n]$, c'est-à-dire en excluant l'*idéal exceptionnel* $I_1 = (X_0,...,X_n)$, et sous-ensembles algébriques.
De plus, les sous-variétés correspondent aux idéaux premiers homogènes.

Comment passer des variétés projectives aux cônes affines ? Soit une variété affine $V = \{x \in \mathbb{P}^N \mid F_1(x) = ... = F_t(x) = 0\}$. On note $V^{aff} = \{x \in \mathbb{A}^{N+1} \mid F_1(x) = ... = F_t(x) = 0\}$ 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 $K(\mathbb{A}^n) = K(X_0,...,X_N)$ et $K(\mathbb{P}^N) = K(\frac{X_1}{X_0},..., \frac{X_N}{X_0})$. De plus, $\boxed{V^{aff} \cap W^{aff} = (V \cap W)^{aff}}$.

3.2.5.2 Plongement de Segre

Définition. ***(Plongement de Segre)***

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

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

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 $[x_0; ...; x_m] = [x'_0; ...; x'_m]$ dans $\mathbb{P}^m$ et $[y_0; ...; y_m] = [y'_0; ...; y'_m]$ dans $\mathbb{P}^m$; 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 : $\forall 0 \leqslant i,k \leqslant m, 0 \leqslant j,h \leqslant n \quad z_{i,j} z_{k,h} - z_{i,h} z_{k,j} = 0$, puisque $(x_i y_j)(x_k y_h) - (x_i y_j)(x_k y_j) = 0$. 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 $P = (1, z_{1,0},..., z_{m,0})$ et $Q = (1, z_{0,1},...,z_{0,n})$, 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 $\mathbb{P}^1 \times \mathbb{P}^1$.

3.2.5.3 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 :

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

▷ 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, $(\forall j \quad f_j(x,y) = 0 \implies x = (0,...,0)) \iff \exists s \geqslant 1 \quad I_s \subseteq \mathcal{J}(y)$. Posons $W_s = \{y \mid I_s \subseteq \mathcal{J}(y)\}$. Alors $y \in \bigcap_{s \geqslant 1} W_s \iff \exists w \neq (0,...,0)\ \forall j \quad f_j(x,y) = 0$. 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 $\leqslant \dim(K[X]_s) = N$. 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.

3.2.6 Dimension et espace tangent

3.2.6.1 Rappels sur les degrés de transcendance

Définition. ***(Base de transcendance)***

Pour tout extension de corps L de K, une famille d'élements 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 $x_1,...,x_n \in L$, il n'existe pas de polynôme non nul $P \in K[X_1,...,X_n]$ tel que $P(x_1,...,x_n) = 0$.)

Théorème. ***(Existence de bases de transcendance)***

Pour tout corps K, pour tout 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 $i,j \in I$, $i \leqslant j \implies \mathcal{A}_i \subseteq \mathcal{A}_j$. Notons $\mathcal{A} = \bigcup_{i\in I} \mathcal{A}_i$. Pour tous $x_1,...,x_n \in \mathcal{A}$, pour tout $j \in [\![1,n]\!]$, il existe $i_j \in I$ tel que $x_j \in \mathcal{A}_{i_j}$. Soit $i_0 = \max_{1\leqslant j\leqslant n} i_j$. Puisque la famille $(\mathcal{A}_i)_{i\in I}$ est totalement ordonnée, on a $x_1,...,x_n \in \mathcal{A}_{i_0}$. La famille $\mathcal{A}_{i_0}$ étant algébriquement indépendante, on en déduit qu'il n'existe pas de polynôme non nul $P \in K[X_1,...,X_n]$ tel que $P(x_1,...,x_n) = 0$. 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.

3.2.6.2 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 $\deg \mathrm{tr}(K(V)/K) := \dim(V)$.

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. $\dim(\mathbb{A}^n) = \dim(\mathbb{P}^n) = \deg \mathrm{tr} K(X_1,...,X_n)/K = n$. (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 $f \in K[X_1,...,X_n] \setminus K$ irréductible. Alors si $V = \{x \in \mathbb{A}^n \mid f(x) = 0\}$, $\dim(V) = n - 1$.

   ▷ On a $K[V] = K[X_1,...,X_n]/(f) = K[x_1,...,x_n]$. Disons que X_n apparaît dans f : $f = X_n^d f_0(X_1,...,X_{n-1}) + ... + f_d(X_1,...,X_{n-1})$ où $f_0 \neq 0$. Or Xx_n est algébrique sur $K(x_1,...,x_{n-1})$, car $x_n^d f_0(x_1,...,x_{n-1}) + ... + f_d(x_1,...,x_{n-1}) = 0$. Ainsi $\deg \mathrm{tr}(K(V)/K) \leqslant n-1$, car les $x_1,...,x_{n-1}$ sont algébriquement indépendants. Sinon, il existerait $g(x_1,...,x_{n-1}) = 0$, $g \in K[X_1,...,X_{n-1}]$, et l'on en déduirait $g(X_1,...,X_{n-1}) \in (f)$, donc $f \mid g$ dans $K[X_1,...,X_n]$, contradiction. Ainsi $\deg \mathrm{tr}(Frac(K[V]) = n-1$. ■

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 $\dim(Y) \leqslant \dim(V)$, 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 $j^\star : K[V] = K[X_1,...,X_n]/I_V \longrightarrow K[Y] = K[X_1,...,X_n]/I_Y$ résulte de la factorisation de la flèche canonique $K[X_1,...,X_n] \longrightarrow K[X_1,...,X_n]/I_Y$ surjective, donc est surjective. Son noyau est I_Y/I_V. On peut choisir $y_1,...,y_r \in K[Y]$ qui forment une base de transcendance de $K(Y)/K$, avec $r = \dim(Y)$, quitte à éliminer les dénominateurs, car $r < \infty$. Il existe $x_1,...,x_r \in K[V]$ tels que $j^\star x_i = y_i$ pour chaque i et les $x_1,...,x_r$ sont algébriquement indépendants. En effet, si $F(x_1,...,x_r) = 0$ pour $F \in K[X_1,...,X_r$. On en déduirait $j^\star(F(x_1,...,x_r)) = F(y_1,...,y_r) = 0$, donc $F = 0$, donc $\deg \mathrm{tr} K(V) = \dim(V) \geqslant r$.

$\dim(V) = \dim(Y)$ si et seulement si $x_1,...,x_r$ est une base de transcendance de $K(V)/K$. Par le lemme de Noether, quitte à remplacer $x_1,...,x_r$ par $x_i' = \sum a_{ij}x_j$, on peut supposer $K[V]/K[x_1,...,x_r]$ extension entière d'anneaux (qui sont des K-algèbres). On veut montrer que, dans ce nouveau cas, elle est en fait injective, soit $\mathrm{Ker}(j^\star) = \{0\}$. Alors on aurait $j^\star$ un isomorphisme (de K-algèbres) donc $j : Y \hookrightarrow X$ un isomorphisme, d'où $Y = V$. Soit donc $u \in \mathrm{Ker}(j^\star) \subseteq K[V]$. u est entier sur $K[x_1,...,x_r]$, donc racine de $T^d + p_{d-1}(x_1,...,x_r)T^{d-1} + ... + p_0(x_1,..,x_r) = 0$, supposée irréductible tant qu'à faire, avec les $p_i \in K[X_1,...,X_r]$. On y applique $j^\star$. : $j^\star(u)^d + p_{d-1}(y_1,...,y_r)j^\star(u)^{d-1} + ... + p_0(y_1,...,y_r) = 0$ où $p_0(y_1,...,y_r) = 0$ 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.** $V(f) = W_1 \cup ... \cup W_s$ avec les W_i irréductibles. En localisant, on se ramène à suppose $V \cap \{f = 0\} = W$ irréductible. On choisit $g_i \in K[V]$, nulle sur W_i, $i \geqslant 2$, pas sur W_1. Ainsi V se ramène à $V \setminus \{g_2...g_s = 0\}$ et $K[V]$ à $K[V][\frac{1}{g_2},..., \frac{1}{g_s}]$.
- **Étape 2.** $V \cap (f = 0) = W$ irréductible, $I_W = \sqrt{(f)}$. Le lemme de Noether ($n = \dim(V)$) donne $K[x_1,...,x_r] \overset{j}{\hookrightarrow} K[V]$ avec les $x_1,...,x_r$ algébriquement indépendants, extension entière. Ce morphisme correspond à $\pi : V \longrightarrow \mathbb{A}^n$ tel que $\pi^\star = j$. 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 $K[X_1,...,X_n]/\sqrt{(f_j)}$ de degré de transcendance $n - 1$ donc $\deg \mathrm{tr} = n - 1$, un de moins.

Le résultat est alors démontré. ■

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

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

Corollaire. *(Théorème de Kull itéré)*

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

▷ 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, $V \cap \{f_1 = ... = f_{-1} = 0\} = W_1 \cup ... \cup W_s$ avec $\dim(W_i) \geqslant \dim(V) - r + 1$, d'où $V \cap \{f_1 = ... = f_r = 0\} = \bigcup_{i=1}^{s} W_i \cap \{f_r = 0\}$ et dans cette réunion, toutes les composantes irréductibles de dimension $\geqslant \dim(W_i) - 1 \geqslant \dim(V) - r$. ■

Corollaire. *(Dimension d'une intersection)*

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

▷ 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 $\{x_1 - y_1 = ... = x_n - y_n = 0\}$. Soit $\delta : \mathbb{A}^n \longrightarrow \mathbb{A}^{2n}$ 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 $\dim(U_i) \geqslant \dim(V) + \dim(W) - n$.

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 $V \cap W = U_1 \cup ... \cup U_s$, $V^{aff} \cap W^{aff} = U_1^{aff} \cup ... U_s^{aff}$ et $0 \in U_i^{aff}$. On a vu que $\dim(U_i^{aff}) \geqslant \dim(V^{aff}) + \dim(W^{aff}) - (n+1) = (\dim(V) + 1) + (\dim(W) + 1) - (n+1) = (\dim(V) + \dim(W) - n) + 1$, mais par hypothèse $\dim(V) + \dim(W) - n \geqslant 0$. Donc $U_i \neq \emptyset$ et $\dim(U_i) \geqslant \dim(V) + \dim(W) - n$. ■

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 $V \cap \{f = 0\} = W_1 \cup ... \cup W_s$ avec $\dim(W_i) = n - 1$. Posons $V_{n-1} = W_1$. Alors :

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

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 $V = V_n \supseteq V_{n-1} \supseteq ... \supseteq V_0$, avec $\dim(V_i) = i$.
2. Inversement, si l'on a une suite $V'_0 \subsetneq V'_1 \subsetneq ... \subsetneq V'_n = V$, 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 $\dim(V'_{i+1}) \geqslant \dim(V'_i) + 2$, 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 $f : V \longrightarrow \mathbb{A}^n$ à fibres finies non vides. Soit $\phi : K[\mathbb{A}^n] = K[X_1,...,X_n] \longrightarrow K[V]$ extension algébrique entière, donnée par le lemme de normalisation de Noether si $\phi = f^\star$ avec f polynomiale, si $a = (a_1, ..., a_n) \in \mathbb{A}^n$, montrons que $f^{-1}(\{a\})$ fini non vide, $\phi(P(x)) = f^\star P = P \circ f$. Réciproquement, si on a $V \subseteq \mathbb{A}^N$, $K[V] = K[t_1,...,t_N]$. Soit $t = t_i$, t entier sur $\phi(K[x_1,...,x_n])$, alors $t^d + b_{d-1}t^{d-1} + ... + b_0 = 0$ avec $b_j \in \phi(K[X_1,...,X_n])$. Ainsi $(t_1,...,t_N) \in f^{-1}(a) \iff$ pour chaque $t = t_i$, $t(a)$ vérifie $t(a)^d + b_0 \circ f(a)t(a)^{d-1} + ... + b_0 \circ f(a) = 0$, 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 $f^{-1}(0,b) = \emptyset$s i $b \neq 0$ 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. $\dim(V) \geqslant \dim(W)$ 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 $f^\star : K(W) \longrightarrow K(V)$ donc injectif. Ainsi, une base de transcendance de $K(W)$ donne une partie algébriquement indépendante de $K(V)$. Alors $m = \dim(W) = \deg \mathrm{tr}(K(W)) \leqslant \deg \mathrm{tr}(K(V)) = \dim(V) = n$.

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 $g_1,...,g_m \in K[W]$ telles que $W \cap \{g_1(w) = ... = g_n(w) = 0\} = \{y_1,...,y_s\}$ 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 $W \cap \{g_1 = 0\} = W_1 \cup ... \cup W_s$ où $y \in W_1$. Par induction, on trouve $g_1,...,g_j$. La dimension des composantes de $W \cap \{g_1 = ... = g_j = 0\} = \dim(W) - j$ avec y dedans. Ainsi $\dim(W \cap \{g_1 = ... = g_m = 0\}) = 0$ avec y dedans. Il existe élémentairement une fraction $g \in K[W]$ telle que $y \in W \setminus \{g = 0\}$, $y_2,...,y_s$ n'y étant pas. On remplace W par $W_0 = W \setminus \{g = 0\}$. On peut supposer $W \cap \{g_1 = ... = g_n = 0\} = \{y\}$. Alors $f^{-1}(y) = \{x \in V, g_1 \circ f(x) = ... = g_m \circ f(x) = 0\}$. Par corollaire du théorème de Krull, toutes les composantes sont de dimension $\geqslant n - m$, ce qu'il fallait démontrer.

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

Enfin, si $f^\star : K(W) \longrightarrow K(V)$, $K(W)$ 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 $x_1,...,x_t$ algébriquement indépendant sur $K(W)$ telle que A soit entière sur $K(W\check{r}[x_1,...,x_t]$. Alors $Frac(A) = K(V)$ et $\deg \mathrm{tr}(A) = n$. De plus, $\deg \mathrm{tr}(K(W)) = m$, d'où $\deg \mathrm{tr}(K(V)/K(W)) = n - m$: combien d'éléments transcendants 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 $K[V] = K[t_1,...,t_N]$ et pour $t = t_i$, il est entier sur $K(W)[x_1,...,x_t] \ni f_j$, vérifiant $t^d + f_{d-1}t^{d-1} + ... + f_0 = 0$. Or $K(W) = Frac(K[V])$. Il existe $g \in K[W] \setminus \{0\}$ avec tous les $f_j g \in K[W]$. Donc $t_1,...,t_N$ est entier sur $K[W][\frac{1}{g}][x_1,...,x_t]$ 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 $f^\star$ composée de $K[W_0] \hookrightarrow K[W_0][x_1,...,x_t] \hookrightarrow K[V_0]$, 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 $P = [0,...,0,1] \in \mathbb{P}^n$. Soit $\phi : \mathbb{P}^n \cdots \to \mathbb{P}^{n-1}$ qui à $[x_0,...,x_n] \mapsto [x_0,...,x_{n-1}]$. Alors $\mathrm{dom}(\phi) = \mathbb{P}^n \setminus \{P_0\}$. On a $V = \overline{\text{Graphe de } \phi}^{\text{Zariski}} \subseteq \mathbb{P}^n \times \mathbb{P}^{n-1}$. f envoie V dans $\mathbb{P}^n$ et g l'envoie dans $\mathbb{P}^{n-1}$. Posons $G_\phi = \{([x_0,...,x_n] \neq P_0, [y_0,...,y_{n-1}]) \in \mathbb{P}^n \times \mathbb{P}^{n-1} \mid [x_0,...,x_{n-1}] = [y_0,...,y_{n-1}]\}$ (soit $x_i y_j - x_j y_i = 0$ pour $0 \leqslant i,j \leqslant n-1$. Alors $V = \{([x_0,...,x_n],[y_0,...,y_{n-1}]) \in \mathbb{P}^n \times \mathbb{P}^{n-1}\}$. On a $f^{-1}(P_0) = \{P_0\} \times \mathbb{P}^{n-1}$. Si $P = [x_0,...,x_n] \neq P_0$, alors $f^{-1}(P) = \{([x_0,...,x_n],[x_0,...,x_{n-1}])\}$. D'où $\dim(V) = n$.

Exercice 5

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.

3.2.6.3 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, $D \subseteq V \Leftrightarrow F(0,0,Z,T) \equiv 0$. Ceci équivaut à ce que les coefficients de Z^3,Z^2T,ZT^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.

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

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

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 $\frac{\partial f}{\partial x_1}(a) = ... = \frac{\partial f}{\partial x_n}(a) = 0$, 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 $K[X_1,...,X_n]$, mais cela implique $\frac{\partial f}{\partial x_1}$: en effet, ou bien $\deg_{x_1}(f) = 0$ et $\frac{\partial f}{\partial x_1} = 0$, ou bien $\deg_{x_1}(f) = d_1 \geqslant 1$, d'où $\deg_{x_1} \frac{\partial f}{\partial x_1} = d_1 - 1$. Si la caractéristique de K est nulle, $\frac{\partial f}{\partial x_1} = ... = \frac{\partial f}{\partial x_n} = 0$, d'où f constante ; si la caractéristique de K est un nombre premier p, $\frac{\partial f}{\partial x_1} = ... = \frac{\partial f}{\partial x_n} = 0$, $f(X_1,...,X_n) = \sum a_{i_1,...,i_n} X_1^{i_1 p}...X_n^{i_n p}$; comme $a_{i_1,...,i_n} = (b_{i_1,...,i_n})^p$ 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 $f_1,...,f_m$ 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. $\forall a \in V \quad \dim(T_a(V)) \geqslant \dim(V)$.
2. $\{a \in V \mid \dim(T_a(V)) = \dim(V)\}$ est un ouvert dense de V.

▷ Soient $f_1,...,f_m$ générateurs de I_V. Alors $T_a(V) = \{x \in \mathbb{A}^n \mid \forall j \in [\![1,m]\!] \quad \sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}(a) x_i = 0\}$. On a m équations, n indéterminées, d'où une matrice $J(a) = \left(\frac{\partial f_j}{\partial x_i}(a)\right)$. Alors $\dim(T_a(V)) = n - \mathrm{rg}(J(a))$. Notons $r_0 = \max_{a \in V} \mathrm{rg}(J(a))$ et $d_0 = n - r_0$. Pour tout $a \in V$, $\dim(T_a(V)) \geqslant d_0$. 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 $\{a \in V \mid dim(T_a(V)) > d_0\} = \{a \in V \mid$ tous les mineurs $r_0 \times r_0$ de $J(a)$ sont nuls$\} \iff \mathrm{rg}(J(a)) < r_0$. 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 $M_a = (X_1 - a_1,...,X_n - a_n)$ l'idéal de a dans $K[X_1,...,X_n]$. Alors M_a/M_a^2 est l'ensemble des formes linéaires en $X_1 - a_1,...,X_n - a_n$: 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 $f \in M_a$, $f = f^{(1)} + f^{(2)} + ... + f^{(n)}$ où $f^{(2)} + ... + f^{(n)} \in M_a^2$. De plus, $\mathcal{O}_{\mathbb{A}^n,a} = K[\mathbb{A}^n]$ localisé par rapport à l'idéal premier M_a, soit $\{f = \frac{P}{Q}$ avec P,Q 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, $M_a/M_a^2 \leftarrow M_a \rightarrow \mathfrak{M}_{\mathbb{A}^n,a} \longrightarrow \mathfrak{M}_{\mathbb{A}^n,a}/\mathfrak{M}_{\mathbb{A}^n,a}^2$ 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 $\psi : M_a \longrightarrow (\mathbb{A}^n)^* \longrightarrow T_a(V)^\star$ qui à $f \mapsto f^{(1)} \mapsto f^{(1)}_{T_a(V)}$. 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 $g_1,...,g_n$ sont générateurs de IV, $g_1^{(1)},...,g_m^{(1)}$ 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 $f - \sum a_j g_j \in M_a^2$, $\sum a_j g_j I_V$. 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 $\phi(a) = b$. $\phi^\star : \mathcal{O}_{W,b} \longrightarrow \mathcal{O}_{V,a}$ 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. ■

3.2.7 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 $e_1 = (x_0,...,x_3)$ et $e_2 = (y_0,...,y_3)$. On introduit (le produit extérieur) $\phi(e_1,e_2) = \begin{pmatrix} x_0y_1 - x_1y_0 \\ x_0y_2 - x_2y_0 \\ x_0y_3 - x_3y_0 \\ x_1y_2 - x_2y_1 \\ x_1y_3 - x_3y_1 \\ x_2y3 - x_3y_2 \end{pmatrix}$.
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 $\phi : Gr(1,3) \longrightarrow \mathbb{P}^5$ qui à $W \longmapsto \phi(e_1,e_2)$. 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 $0 \leqslant i < j \leqslant 3$. On peut supposer $z_{0,1} \neq 0$ et même $x_0y_1 - x_1y_0 = 1 = x_0'y_1' - x_1'y_0'$ 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
$$\phi(W) = \phi(e_1,e_2) = \begin{pmatrix} 1 \\ y_2 \\ y_3 \\ -x_2 \\ -x_3 \\ x_2y_3 - x_3y_2 \end{pmatrix} = \begin{pmatrix} 1 \\ y_2' \\ y_3' \\ -x_2' \\ -x_3' \\ x_2'y_3' - x_3'y_2' \end{pmatrix} = \phi(W') = (z_{01},z_{02},z_{03},z_{12},z_{13},z_{23}).$$
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 $z_{01}z_{23} + z_{12}z_{03} - z_{13}z_{02} = 0$, 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 $W = \mathrm{Vect}(e_1,e_2)$, 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, $[z_{01},...,z_{23}] = [1,z_{02},...,z_{23}] \rightsquigarrow (z_{02},...,z_{13})$.

3.2.7.1 Grassmannienne de droites

3.2.7.2 Existence de droites contenues dans une hypersurface

3.2.7.3 Une autre application : coordonnées de Chow

3.2.7.4 Le grand théorème de Bézout

3.3 Surfaces

3.3.1 Quadriques

3.3.1.1 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 $\mathrm{car}(K) \neq 2$.

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 $\mathrm{rg}(Q)$ 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 $r = \mathrm{rg}(Q)$.

- 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.

3.3.1.2 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 $\leqslant 9$. Puisque $10-9\geqslant 1$, 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 $\#(L\cap S)\leqslant d$ 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,...,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,...,L_4 appartiennent à une des deux familles donc les droites appartenant à l'autre famille rencontrent L_1,...,L_4 et ce sont les seules, d'où l'infinité. Ainsi, $\mathcal{L}$ est en bijection ensembliste avec $\mathbb{P}^1$. Si maintenant $L_4 \subsetneq S$, $S \cap L_4 = \{P_1, P_3\}$, 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 $\{P_2\}$. ■

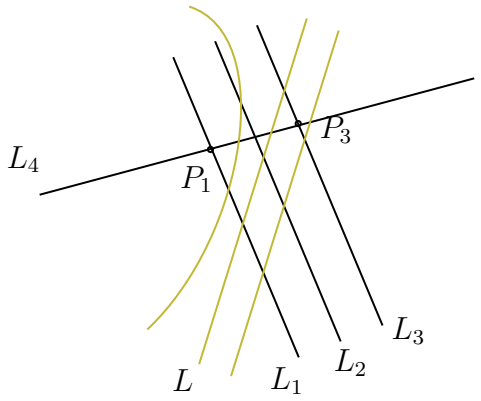

FIGURE 3.3.1 : *Droites sur une quadrique.* —

3.3.2 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.

3.3.2.1 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 doit 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, $\frac{\partial G}{\partial X} = Z\frac{\partial Q}{\partial X} + 2L_1\frac{\partial L_1}{\partial X} + L_1^2\frac{\partial L_2}{\partial X}$, ..., $\frac{\partial G}{\partial Z} = Q + Z\frac{\partial Q}{\partial Z}$. Toutes les dérivées partielles sont nulles en P_0. ■

Remarque préliminaire. Soient M_1,...,M_3 distinctes dans $\mathbb{P}^2$. Alors, premier cas, elles forment un triangle non dégénéré ou, second cas, elles sont concourante, 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, $\mathrm{rg}(m_1,m_2,m_3) = 2$, 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 $\Pi_1,...,\Pi_5$ contenant L tels que pour tout $i \in [\![1,5]\!]$, $\Pi_i \cap S = L \cup L_i \cup L_i'$ 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 récrit 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 $D(\alpha T,T) = T^2D(\alpha,1)$, 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 $F = Z(f_0T^2 + f_1ZT + f_2Z^2)$. On obtient directement que modulo Z^2, $\Delta(Z,T) = -B^2F = -(T+bZ)^2Z(f_0T^2 + ...) \equiv f_0T^4Z$. Montrons que $f_0 \neq 0$. Il n'y a aucun point singulier : pour $P = (0,0,0,1)$, $G = ZQ + XYT$, $\overrightarrow{\mathrm{grad}}\, G(P) = (0,0,Q(0,0,0,1),0) \neq (0,0,0,0)$, 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 $C(Z,T) = c_1Z$, $D(Z,T) = T^2 + d_1ZT + d_2Z^2$. Ainsi $\Delta(Z,T) \equiv -CD^2 \equiv c_1ZT^4$ modulo Z^2, et $c_1 \neq 0$ grâce à la lissité en $P = (0,1,0,0)$ et $\overrightarrow{\mathrm{grad}}\, G(P) = (0,c_1,0,0)$. ■

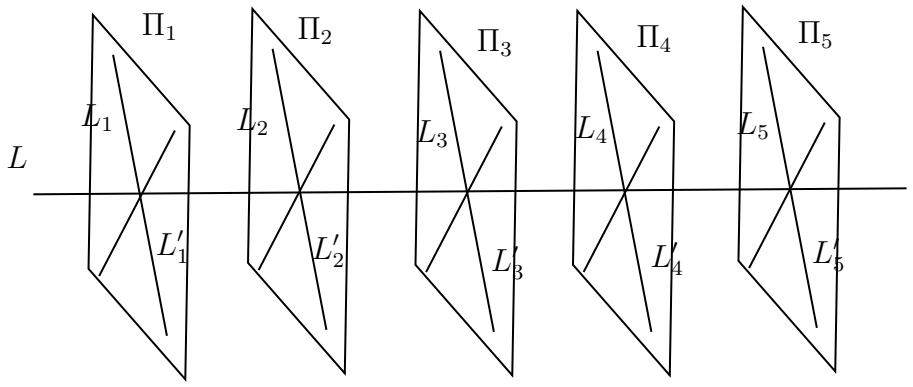

FIGURE 3.3.2 : *Voici dix droites.* — C'est déjà ça.

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 numéroter ces droites L_i, L'_i, L''_i pour $1 \leqslant i \leqslant 5$ 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 $\Pi_i \cap M =$ 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 $L'_i \cap L''_j =$ un point. Si Π_i est un plan contenant L, L'_i, L_i, $\Pi_i \cap L''_j =$ un point et L''_j ne rencontre pas L, pas L_i, donc rencontre L'_i. ■

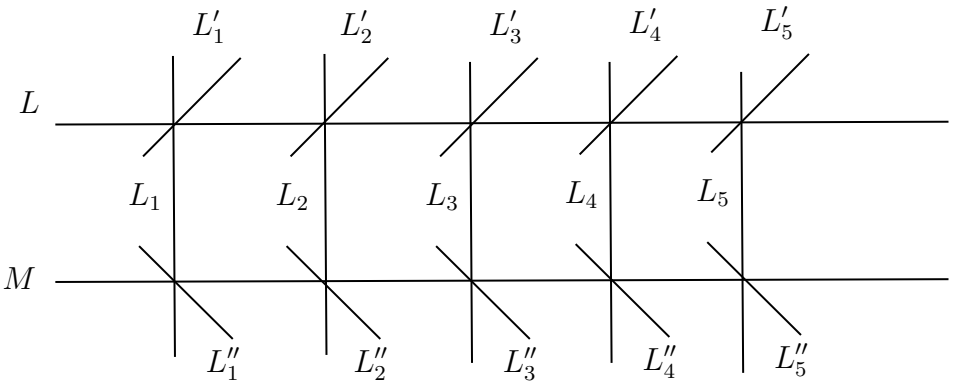

FIGURE 3.3.3 : *En voilà dix-sept autres.* — Et le compte est bon.

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_j.

Preuve.

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

Chapitre 4

Exercices

Difficulté des exercices :

- ● ○ ○ ○ ○ Question de cours, application directe, exercice purement calculatoire sans réelle difficulté technique
- ● ● ○ ○ ○ Exercice faisable, soit intuitivement, soit en employant des moyens rudimentaires ou des techniques déjà vues
- ● ● ● ○ ○ Exercice relativement difficile et dont la résolution appelle à une réflexion plus importante à cause d'obstacles techniques ou conceptuels, qui cependant devraient être à la portée de la plupart des étudiants bien entraînés
- ● ● ● ● ○ Exercice très exigeant, destiné aux élèves prétendant aux concours les plus difficiles, exercice « classique ».
- ● ● ● ● ● La résolution de l'exercice requiert un raisonnement et des connaissances extrêmement avancés, dépassant les attentes du prérequis. Il est presque impossible de le mener à terme sans indication. Bien qu'exigibles à très peu d'endroits, ces exercices sont très intéressants et présentent souvent des résultats forts.

Appendice

Table des matières

Bibliographie

[1] *Titre du livre*, Auteur du livre, date, maison d'édition

Table des figures

Liste des tableaux