

---

---

*Cours accéléré de 3<sup>e</sup> cycle — Automne 1999*

---

---

# **ALGÈBRE COMMUTATIVE**

*ET INTRODUCTION À LA*

# **GÉOMÉTRIE ALGÈBRIQUE**

**Antoine CHAMBERT-LOIR**

---

---

*Université Pierre et Marie Curie – Paris VI*

---

---

*Antoine Chambert-Loir*

Institut de mathématiques de Jussieu, Boite 247, 4, place Jussieu,  
F-75252 Paris Cedex 05.

*E-mail* : `chambert@math.jussieu.fr`

Ce livre est disponible à l'adresse Internet [http://www.math.jussieu.fr/~chambert/  
publications.html#acl98d](http://www.math.jussieu.fr/~chambert/publications.html#acl98d)

Copyright © 1998–99, Antoine Chambert-Loir

# ALGÈBRE COMMUTATIVE ET INTRODUCTION À LA GÉOMÉTRIE ALGÈBRIQUE

**Antoine Chambert-Loir**

*Résumé.* — Ce cours de 3<sup>e</sup> cycle a deux visages, l’algèbre et la géométrie : d’une part des parties définies par des équations polynômiales, d’autre part des algèbres de type fini sur un corps. On montrera sur quelques exemples (théorème des zéros de Hilbert, dimension, régularité) comment ce sont deux faces d’une même tête et comment les aspects géométriques et algébriques s’éclairent mutuellement.

*Abstract.* — This graduate course has two faces : algebra and geometry. Indeed, we study simultaneously loci of points defined by polynomial equations and algebras of finite type over a field. We shall show on examples (Hilbert’s Nullstellensatz, dimension theory, regularity) how these are two faces of a single head and how both geometric and algebraic aspects enlight the one the other.



# TABLE DES MATIÈRES

<b>1. Préliminaires d'algèbre commutative</b> .....	1
1.1. Anneaux, idéaux .....	1
1.2. Localisation .....	3
1.3. Chaînes, anneaux noethériens .....	4
1.4. Anneaux artiniens .....	7
1.5. Éléments entiers .....	9
1.6. Produit tensoriel .....	11
1.7. Limites inductives .....	12
<b>2. Préliminaires de topologie</b> .....	15
2.1. Faisceaux .....	15
2.2. Espaces annelés .....	17
2.3. Espaces annelés modelés .....	17
<b>3. Variétés algébriques</b> .....	21
3.1. Ensembles algébriques .....	21
3.2. Topologie de Zariski .....	25
3.3. Variétés algébriques affines .....	29
3.4. Variétés algébriques .....	32
3.5. Localisation .....	35
<b>4. Exemples</b> .....	39
4.1. Espaces projectifs .....	39
4.1.1. Droite projective .....	39
4.1.2. Espace projectif .....	39
4.2. Produits .....	43
4.3. Grassmanniennes .....	47
4.3.1. Construction .....	47
4.3.2. Le plongement de Plücker .....	48

4.3.3. Relations de Grassmann.....	49
4.3.7. Exemple.....	51
4.4. Quotients.....	52
<b>5. Théorie locale des variétés algébriques.....</b>	<b>57</b>
5.1. Dimension.....	57
5.2. Codimension.....	62
5.3. Systèmes de paramètres.....	65
5.4. Espace tangent.....	68

Au lecteur

Avant que tu n'entames la lecture de ces pages,  
L'auteur un peu coupable de leur aridité  
Voudrait par ce sonnet te donner du courage  
Afin que par l'étude tu ne sois rebuté.

L'algèbre commutative est certes un peu austère  
Mais en en dénouant les belles subtilités,  
Tu entendras souvent le nom d'Emmy Noether  
Dont les anneaux jouissent de grandes propriétés.

À la géométrie, elle offre des méthodes  
Dont je ne puis, hélas, dans cette petite ode  
Louer comme il se doit la force inégalée

Et j'espère dans ce cours par trop accéléré  
Te guider sûrement parmi ces équations  
Qui par l'algèbre trouvent une démonstration.



# CHAPITRE 1

## PRÉLIMINAIRES D'ALGÈBRE COMMUTATIVE

### 1.1. Anneaux, idéaux

Nous supposons connues les notions de *groupe*, d'*anneau*, de *corps*, de *module*, ainsi que celles d'homomorphismes de groupes, d'anneaux, de corps, de modules, etc.

Par convention, un anneau possède toujours un élément unité, noté en général 1. On notera  $A^*$  ou  $A^\times$  le groupe multiplicatif des éléments inversibles de  $A$ .

Si  $k$  est un anneau, une *k*-algèbre est un anneau  $A$  muni d'un homomorphisme d'anneaux  $f : k \rightarrow A$ . Lorsque cet homomorphisme est injectif, on considère souvent  $A$  comme un sur-anneau de  $k$ . Si  $(A, f : k \rightarrow A)$  et  $(B, g : k \rightarrow B)$  sont deux *k*-algèbres, un homomorphisme de *k*-algèbres est un morphisme d'anneaux  $\varphi : A \rightarrow B$  tel que  $g = \varphi \circ f$ .

Si  $(X_i)_{i \in I}$  est une famille d'indéterminées, on définit une *k*-algèbre  $k[X_i]$  des *polynômes* en les  $X_i$ . Cette algèbre vérifie la propriété universelle suivante : pour toute *k*-algèbre  $A$ , l'application canonique

$$\text{Hom}_{k\text{-Alg}}(k[X_i], A) \rightarrow \text{Hom}_{\text{Ens}}(I, A), \quad f \mapsto (i \mapsto f(X_i))$$

est une bijection.

On ne détaille pas la notion de *degré* en une des indéterminées, voire de degré tout court si  $I$  est un singleton. On a une *division euclidienne* dans les anneaux de polynômes : soient  $f$  et  $g \in A[X]$ , le coefficient dominant de  $g$  étant inversible dans  $A$ . Il existe alors  $q$  et  $r \in A[X]$  uniques tels que  $f = gq + r$  et  $\text{degr } r < \text{degr } g$ .

Un *idéal* d'un anneau  $A$  est un sous- $A$ -module de  $A$ . L'intersection de deux idéaux de  $A$  est un idéal de  $A$ . L'image réciproque d'un idéal par un homomorphisme d'anneaux est un idéal ; en particulier, le noyau d'un homomorphisme d'anneaux est un idéal. L'*idéal engendré* par une partie de  $A$  est par définition le plus petit idéal de  $A$  contenant cette partie. Si  $I$  et  $J$  sont deux idéaux de  $A$ , les idéaux  $I + J$  et  $I \cdot J$  (noté aussi  $IJ$ ) sont les idéaux engendrés par les sommes  $a + b$  (resp. les produits  $ab$ ) pour  $a \in I$  et  $b \in J$ .

Si  $I$  est un idéal de  $A$ , la relation  $x \sim y$  si et seulement si  $x - y \in I$  est une relation d'équivalence. L'ensemble quotient  $A/\sim$ , noté  $A/I$ , possède alors une unique structure

d'anneau telle que la surjection canonique  $\pi : A \rightarrow A/I$  soit un homomorphisme d'anneaux. L'anneau quotient  $A/I$  vérifie la propriété universelle suivante : pour tout anneau  $B$  et tout homomorphisme  $f : A \rightarrow B$  tel que  $f(I) = (0)$ , il existe un unique homomorphisme d'anneaux  $\varphi : A/I \rightarrow B$  tel que  $f = \varphi \circ \pi$ .

L'application qui à un idéal  $J$  de  $A/I$  associe  $\pi^{-1}(J) \subset A$  est une bijection entre l'ensemble des idéaux de  $A/I$  et les idéaux de  $A$  qui contiennent  $I$ .

On dit qu'un élément  $a \in A$  est un *diviseur de zéro* s'il existe  $b \in A, b \neq 0$  tel que  $ab = 0$ . On dit que  $A$  est *intègre* s'il est non nul et s'il n'admet pas d'autre diviseur de zéro que 0. On dit qu'un idéal  $I$  de  $A$  est *premier* si l'anneau quotient  $A/I$  est intègre. Cela revient à la proposition suivante : si  $fg \in I$ , alors  $f \in I$  ou  $g \in I$ . On dit qu'un idéal  $I$  est *maximal* si  $A/I$  est un corps ; cela équivaut à dire que  $I$  est un élément maximal pour l'inclusion parmi les idéaux de  $A$  distincts de  $A$ . On prouve à l'aide du lemme de Zorn que tout idéal est contenu dans un idéal maximal ; en particulier, il existe des idéaux maximaux, et *a fortiori* des idéaux premiers. Un anneau qui ne contient qu'un seul idéal maximal est dit *local*. On démontre qu'un anneau  $A$  est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal (*exercice !*).

LEMME 1.1.1 (Lemme d'évitement). — Soient  $I, J$  et  $\mathfrak{p}$  des idéaux de  $A$ . Si  $\mathfrak{p}$  est premier et si  $IJ \subset \mathfrak{p}$ , alors  $I \subset \mathfrak{p}$  ou  $J \subset \mathfrak{p}$ .

*Démonstration.* — Si  $I \not\subset \mathfrak{p}$ , il existe  $x \in I$  tel que  $x \notin \mathfrak{p}$ . De même, si  $J \not\subset \mathfrak{p}$ , soit  $y \in J$  n'appartenant pas à  $\mathfrak{p}$ . Alors,  $xy \in IJ$  mais,  $\mathfrak{p}$  étant premier,  $xy$  n'appartient pas à  $\mathfrak{p}$ . Autrement dit,  $IJ \not\subset \mathfrak{p}$ .  $\square$

LEMME 1.1.2 (Un autre lemme d'évitement). — Soient  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  et  $I$  des idéaux de  $A$  tels que  $I \subset \bigcup_i \mathfrak{p}_i$ . Si  $A$  contient un corps infini, ou si au plus deux des  $\mathfrak{p}_i$  ne sont pas premiers, il existe  $i$  tel que  $I \subset \mathfrak{p}_i$ .

*Preuve* (cf. [?], p. 91). — Aucun espace vectoriel sur un corps infini n'est réunion finie de sous-espaces vectoriels stricts. Si  $A$  contient un corps infini  $k$ , ce fait appliqué aux  $k$ -espaces vectoriels  $\mathfrak{p}_i \cap I$  implique que l'un des  $\mathfrak{p}_i \cap I = I$ .

L'autre cas se montre par récurrence sur  $n$ , le résultat étant clair pour  $n = 1$ . Supposons que  $I$  n'est contenu dans aucun des  $\mathfrak{p}_i$ . Par récurrence, pour tout  $i$ ,  $I \not\subset \bigcup_{j \neq i} \mathfrak{p}_j$ , si bien qu'il existe  $x_i \in I$  tel que  $x_i \notin \mathfrak{p}_j$  pour  $i \neq j$ . En particulier,  $x_i \in \mathfrak{p}_i$ .

Si  $n = 2$ ,  $x_1 + x_2$  appartient à  $I$ , mais il est facile de voir qu'il n'appartient ni à  $\mathfrak{p}_1$  ni à  $\mathfrak{p}_2$ , d'où une contradiction. Si  $n > 2$ , on peut supposer que  $\mathfrak{p}_1$  est premier. Alors,  $a = x_1 + x_2 \dots x_n$  appartient à  $I$ . Cependant, pour  $i \neq 1$ ,  $x_2 \dots x_n \in \mathfrak{p}_i$  donc  $a \notin \mathfrak{p}_i$ . De même, comme  $\mathfrak{p}_1$  est premier et que pour  $i \geq 2$ ,  $x_i \notin \mathfrak{p}_1$ , leur produit  $x_2 \dots x_n \notin \mathfrak{p}_1$ . Par suite,  $a \notin \mathfrak{p}_1$ . On a encore une contradiction.  $\square$

On note  $\text{Spec}A$  le *spectre premier*, ou *spectre* de  $A$  : c'est l'ensemble des idéaux premiers de  $A$ . Soit  $f : A \rightarrow B$  est un homomorphisme d'anneaux. Pour tout idéal premier  $\mathfrak{q}$

de  $B$ ,  $f^{-1}(\mathfrak{q})$  est un idéal premier de  $A$ , d'où une application  $\text{Spec } B \rightarrow \text{Spec } A$ . Le *spectre maximal* de  $A$ , noté  $\text{Spm } A$  est l'ensemble des idéaux maximaux de  $A$ . On prendra garde qu'un homomorphisme d'anneaux  $f : A \rightarrow B$  n'induit pas d'application  $\text{Spm } B \rightarrow \text{Spm } A$  car l'image réciproque d'un idéal maximal n'est pas forcément un idéal maximal. (*Exercice : trouver un contre-exemple.*)

## 1.2. Localisation

On dit qu'un élément  $a \in A$  est *nilpotent* s'il existe  $n \geq 1$  tel que  $a^n = 0$ . L'ensemble des éléments nilpotents de  $A$  est un idéal de  $A$  appelé *nilradical*. Si cet idéal est égal à  $(0)$ , on dit que  $A$  est *réduit*. Plus généralement, si  $I$  est un idéal de  $A$ , on appelle *radical* de  $I$  l'ensemble noté  $\sqrt{I}$  des éléments  $a \in A$  tels qu'il existe  $n \geq 1$  de sorte que  $a^n \in I$ . C'est un idéal de  $A$  qui contient  $I$ . Un idéal égal à son radical est dit *radiciel*.

LEMME 1.2.1. — *Le radical d'un idéal est l'intersection des idéaux premiers qui le contiennent. En particulier, le nilradical d'un anneau est l'intersection de ses idéaux premiers.*

Une *partie multiplicative* de  $A$  est une partie  $S \subset A$  contenant 1 et telle que si  $a, b \in S$ , alors  $ab \in S$ . L'*anneau de fractions*  $S^{-1}A$  est le quotient de l'ensemble  $A \times S$  par la relation d'équivalence  $(a, s) \sim (a', s')$  si et seulement s'il existe  $t \in S$  tel que  $t(a's - as') = 0$ . Notant  $a/s$  la classe du couple  $(a, s)$ ,  $S^{-1}A$  est muni des lois

$$(a/s) + (a'/s') = (as' + a's)/ss', \quad (a/s) \cdot (a'/s') = aa'/ss'$$

qui en font un anneau. L'application  $i : A \rightarrow S^{-1}A$  donnée par  $a \mapsto a/1$  est un homomorphisme d'anneaux. Il vérifie la propriété universelle suivante : pour tout homomorphisme d'anneaux  $f : A \rightarrow B$  tel que  $\varphi(S) \subset B^*$ , il existe un unique homomorphisme d'anneaux  $g : S^{-1}A \rightarrow B$  tel que  $f = g \circ i$ . L'anneau  $S^{-1}A$  est nul si et seulement si  $0 \in S$ . L'anneau  $S^{-1}A$  est appelé *anneau localisé* de  $A$  en la partie multiplicative  $S$ .

Donnons des exemples de parties multiplicatives :

- si  $f \in A$  n'est pas nilpotent, la partie  $S = \{1, f, f^2, \dots\}$  est multiplicative et ne contient pas 0 ; on note  $A_f$  l'anneau  $S^{-1}A$ .
- si  $\mathfrak{p}$  est un idéal premier de  $A$ ,  $S = A \setminus \mathfrak{p}$  est une partie multiplicative ; on note  $A_{\mathfrak{p}} = S^{-1}A$ .
- si  $I$  est un idéal de  $A$ ,  $S = 1 + I = \{a \in A ; a - 1 \in I\}$  est une partie multiplicative.
- Si  $A$  est intègre,  $S = A \setminus \{0\}$  est une partie multiplicative. L'anneau  $S^{-1}A$  est alors un corps, appelé *corps des fractions* de  $A$ .
- L'image réciproque d'une partie multiplicative par un homomorphisme d'anneaux est une partie multiplicative.

Emmy NOETHER (1882–1935)

*Fille d'un mathématicien réputé, les travaux d'Emmy Noether en algèbre furent fondamentaux : introduction des anneaux noethériens, théorème de décomposition primaire, étude des extensions entières et le lemme de normalisation, etc.*



Si  $I$  est un idéal de  $A$ , on note  $S^{-1}I$  l'idéal  $i(I)(S^{-1}A)$  engendré par l'image de  $I$  dans  $S^{-1}A$ . C'est un idéal de  $S^{-1}A$ , égal à  $A$  si et seulement si  $S \cap I \neq \emptyset$ . De plus, tout idéal de  $S^{-1}A$  est de cette forme. Enfin, l'application  $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$  définit une bijection de l'ensemble des idéaux premiers de  $A$  qui ne rencontrent pas  $S$  vers l'ensemble des idéaux premiers de  $S^{-1}A$ . En particulier, l'anneau  $A_{\mathfrak{p}}$  est local, d'idéal maximal  $\mathfrak{p}A_{\mathfrak{p}}$  ; on l'appelle *localisé de  $A$  en  $\mathfrak{p}$* .

On déduit aussi de ce qui précède que *pour tout idéal  $I$  disjoint de  $S$ , il existe un idéal premier contenant  $I$  disjoint de  $S$*  (considérer un idéal maximal de  $S^{-1}A$  contenant  $S^{-1}I$ ).

*Preuve du lemme.* — Si  $f \in A$  n'est pas nilpotent, il faut prouver qu'il existe un idéal premier de  $A$  qui ne contient pas  $f$ . L'anneau  $A_f$  n'étant pas nul (si  $1/f = 0$ , il existe  $n$  tel que  $f^n = 0$  alors que  $f$  est supposé n'être pas nilpotent), il contient un idéal premier qui est de la forme  $\mathfrak{p}A_f$  pour un idéal premier  $\mathfrak{p}$  de  $A$  qui ne contient pas  $f$ .  $\square$

### 1.3. Chaînes, anneaux noethériens

De manière générale, une *chaîne* dans un ensemble ordonné est une famille finie strictement croissante  $x_0 < x_1 < \dots < x_n$ . Sa *longueur* est  $n$ .

On dit qu'un anneau est *noethérien* si toute suite croissante d'idéaux de  $A$  est stationnaire. Cela équivaut à dire que tout idéal de  $A$  est engendré par un nombre fini d'éléments. Tout quotient d'un anneau noethérien est noethérien. Enfin, on a le *théorème de Hilbert* : si  $A$  est noethérien,  $A[X]$  est noethérien. En particulier, pour tout corps  $k$ ,  $k[X_1, \dots, X_n]$  est noethérien.

LEMME 1.3.1. — *Un anneau noethérien est intègre si et seulement s'il est réduit et n'a qu'un seul idéal premier minimal.*

*Démonstration.* — Si  $A$  est intègre,  $(0)$  est l'unique idéal premier minimal de  $A$ . Réciproquement, si  $A$  n'a qu'un seul idéal premier minimal  $\mathfrak{p}$ , on a en vertu du lemme 1.2.1 l'égalité  $\mathfrak{p} = \sqrt{(0)}$ . Comme  $A$  est réduit,  $\mathfrak{p} = (0)$  et  $A$  est intègre.  $\square$

Je renvoie par exemple à [?], § 6 pour l'énoncé général du théorème de décomposition primaire. J'en extrais le résultat suivant qui précise quelque peu le lemme précédent.

PROPOSITION 1.3.2. — *Soit  $A$  un anneau noethérien réduit. Alors,  $A$  n'a qu'un nombre fini d'idéaux premiers minimaux. Leur intersection est égale à  $(0)$  et leur réunion est l'ensemble des diviseurs de zéro dans  $A$ .*

*Démonstration.* — La description du radical d'un idéal montre que tout idéal radiciel est intersection d'idéaux premiers. Soit  $\mathfrak{C}$  l'ensemble des idéaux radiciels qui ne sont pas intersection finie d'idéaux premiers et montrons que  $\mathfrak{C}$  est vide. Comme  $A$  est noethérien, on pourrait sinon trouver un élément maximal  $I$  dans  $\mathfrak{C}$ . En écrivant  $I$  comme intersection d'idéaux premiers, on voit que l'on peut trouver des idéaux radiciels  $I_1$  et  $I_2$  tels que  $I = I_1 \cap I_2$ , mais  $I \neq I_1$  et  $I \neq I_2$ . Comme  $I$  est supposé maximal dans  $\mathfrak{C}$ ,  $I_1$  et  $I_2$  sont intersections finies d'idéaux premiers et par conséquent,  $I$  aussi.

Écrivons alors

$$\sqrt{(0)} = (0) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r.$$

Il n'est pas restrictif de supposer que les  $\mathfrak{p}_i$  sont des idéaux premiers minimaux distincts de  $A$  et que la décomposition est minimale. Si alors  $\mathfrak{p}$  est un idéal premier, on a  $(0) = \bigcap \mathfrak{p}_i \subset \mathfrak{p}$ . D'après le lemme d'évitement 1.1.1, cela implique que  $\mathfrak{p}$  contient l'un des  $\mathfrak{p}_i$  et tous les idéaux premiers minimaux de  $A$  sont parmi les  $\mathfrak{p}_i$ .

Il reste à montrer qu'un élément  $a \in A$  est un diviseur de zéro si et seulement s'il appartient à l'un des  $\mathfrak{p}_i$ . Si  $a \in \mathfrak{p}_i$ , comme  $\bigcap_{j \neq i} \mathfrak{p}_j \neq (0)$ , il existe un élément non nul  $x$  de cette intersection. Alors,  $ax \in \bigcap_j \mathfrak{p}_j = (0)$  et  $a$  est un diviseur de zéro. Réciproquement, si  $a \in A$  est un diviseur de zéro, soit  $x \in A \setminus \{0\}$  tel que  $ax = 0$ . Comme  $x \neq 0$ , il existe  $i$  tel que  $x \notin \mathfrak{p}_i$ . L'égalité  $ax = 0$  implique que  $a \in \mathfrak{p}_i$ .  $\square$

Soit  $A$  un anneau intègre. On dit qu'un élément  $a \in A$  non inversible est *irréductible* si l'égalité  $a = bc$  implique que  $b$  ou  $c$  est inversible. Un élément  $a \in A$  est dit *premier* si l'idéal  $(a)$  est premier; cela implique que  $a$  est irréductible mais la réciproque est fautive. On dit que  $A$  est *factoriel* si tout élément de  $A$  qui n'est ni nul ni inversible peut s'écrire comme produit d'éléments premiers de  $A$  (unique décomposition en facteurs irréductibles).

On a le lemme de Gauß : si l'anneau  $A$  est factoriel, alors pour tout élément irréductible  $a \in A$ ,  $a|bc$  implique  $a|b$  ou  $a|c$ , autrement dit  $a$  est premier. La réciproque est vraie si  $A$  est noethérien. Enfin, si  $A$  est factoriel,  $A[X]$  est factoriel (résultat que Gauß avait démontré lorsque  $A = \mathbf{Z}$ ). En particulier, pour tout corps  $k$ , l'anneau  $k[X_1, \dots, X_n]$  est factoriel.

On dit qu'un  $A$ -module  $M$  est de type fini s'il est engendré comme  $A$ -module par un nombre fini d'éléments. Cela équivaut à dire qu'il existe  $n \geq 1$  et un homomorphisme

Carl Friedrich Gauß (1777–1855)

*Peut-être l'un des scientifiques les plus universels, son œuvre a eu une influence majeure sur un grand nombre de domaines des mathématiques (théorie des nombres, analyse, géométrie différentielle) et de la physique (magnétisme, astronomie, optique).*



surjectif de  $A$ -modules  $f : A^n \rightarrow M$ . On dit qu'un  $A$ -module  $M$  est *noethérien* si toute suite croissante de sous- $A$ -modules de  $M$  est stationnaire. Cela équivaut à dire que tout sous- $A$ -module de  $M$  est de type fini. Quotients et sous-modules d'un module noethérien sont noethériens, de même que les produits finis de modules noethériens. Si  $A$  est noethérien, un  $A$ -module est noethérien si et seulement s'il est de type fini.

**THÉORÈME 1.3.3 (Lemme de Nakayama).** — *Soient  $A$  un anneau,  $\mathfrak{a}$  un idéal de  $A$  et  $M$  un  $A$ -module de type fini tel que  $M = \mathfrak{a}M$ . Alors, il existe  $a \in 1 + \mathfrak{a}$  tel que  $aM = 0$ .*

*En particulier, si  $A$  est local et  $\mathfrak{a}$  son idéal maximal, on a  $M = 0$ .*

*Démonstration.* — Soient  $m_1, \dots, m_n$  des générateurs de  $M$ . Comme  $M = \mathfrak{a}M$ , il existe des éléments  $a_{ij} \in \mathfrak{a}$  tels que pour tout  $i \in \{1, \dots, n\}$ ,

$$m_i = \sum_{j=1}^n a_{ij} m_j.$$

Soient  $A$  la matrice des  $a_{ij}$  et  $I$  la matrice identité  $n \times n$ ; ainsi,  $I - A$  annule le vecteur colonne  $(m_1, \dots, m_n)$ . La matrice  $B$  transposée de la matrice des cofacteurs de  $I - A$  vérifie  $B(I - A) = \det(I - A)I$ . Ainsi,  $\det(I - A)I$  annule le vecteur colonne  $(m_1, \dots, m_n)$ , ce qui signifie que  $\det(I - A)$  annule tous les  $m_i$  et donc  $M$ . Posons  $a = \det(I - A)$ ; en développant le déterminant, on voit que  $a \in 1 + \mathfrak{a}$ , ainsi qu'il fallait démontrer.

Si  $A$  est local d'idéal maximal  $\mathfrak{m}$ , on a  $a \in A^\times$ , ce qui implique  $M = 0$ . □

*Exercice 1.3.4.* — Donner une autre démonstration du lemme de Nakayama suivant la méthode suivante. Le prouver d'abord pour un anneau local en raisonnant par récurrence sur le nombre minimal de générateurs de  $M$ . En introduisant la partie multiplicative  $1 + \mathfrak{a}$ , déduire par un argument de localisation le cas général du cas local.

### 1.4. Anneaux artiniens

On dit qu'un anneau  $A$  est *artinien* si toute suite décroissante d'idéaux de  $A$  est stationnaire. Un *module artinien* est un module tel que toute suite décroissante de sous-modules est stationnaire. Produits finis, quotients et sous-modules de modules artiniens sont artiniens.

Un  $A$ -module non nul  $M$  est dit *simple* s'il n'admet que  $(0)$  et  $M$  comme sous- $A$ -module ; il existe alors un idéal maximal  $\mathfrak{m}$  de  $A$  tel que  $M \simeq A/\mathfrak{m}$ . La *longueur* d'un  $A$ -module  $M$  est la borne supérieure des longueurs de chaînes de sous- $A$ -modules de  $M$ . On la note  $\ell_A(M)$  ou  $\ell(M)$ .

PROPOSITION 1.4.1. — *Soient  $M$  un  $A$ -module et  $N$  est un sous- $A$ -module de  $M$ . Si deux des modules  $M$ ,  $N$  et  $M/N$  sont de longueur finie, le troisième l'est aussi et on a l'égalité*

$$\ell(M) = \ell(N) + \ell(M/N).$$

*Démonstration.* — Si  $N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_a$  et  $M_0/N \subsetneq \dots \subsetneq M_b/N$  sont des chaînes de sous-modules de  $N$  et  $M/N$  respectivement,

$$N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_a \subset M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_b$$

est une chaîne de sous-modules de  $M$  de longueur  $a + b$ , d'où l'inégalité  $\ell(M) \geq \ell(N) + \ell(M/N)$ .

En particulier, si  $M$  est de longueur finie,  $N$  et  $M/N$  aussi. Réciproquement, on suppose que  $N$  et  $M/N$  sont de longueur finie et on veut prouver que  $M$  est de longueur finie égale à  $\ell(N) + \ell(M/N)$ . Soit donc  $M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_a$  une chaîne de sous- $A$ -modules de  $M$ . On remarque que si  $M' \subset M''$  sont deux sous- $A$ -modules de  $M$  tels que  $M' \cap N = M'' \cap N$  et  $M' + N = M'' + N$ , alors  $M' = M''$ . Par suite, pour tout  $i$ , au moins une des deux inclusions

$$M_i \cap N \subset M_{i+1} \cap N \quad \text{et} \quad M_i + N \subset M_{i+1} + N$$

est stricte, ce qui implique que  $\ell(N) + \ell(M/N) \geq a$ . Autrement dit,  $\ell(N) + \ell(M/N) \geq \ell(M)$  et la proposition est démontrée.  $\square$

Un  $A$ -module est de longueur finie est artinien ; réciproquement, un  $A$ -module noethérien et artinien est de longueur finie. Enfin, si  $M$  est un  $A$ -module de longueur finie, toute chaîne maximale de sous-modules est de longueur  $\ell(M)$ .

LEMME 1.4.2. — 1) *Un anneau artinien intègre est un corps.*

2) *Un anneau artinien n'a qu'un nombre fini d'idéaux premiers, tous maximaux.*

*Démonstration.* — Soit  $A$  un anneau artinien.

1) Supposons  $A$  intègre. Si  $x \in A \setminus \{0\}$ , la suite d'idéaux  $(x) \supset (x^2) \supset \dots$  est stationnaire. Il existe ainsi  $n$  tel que  $(x^n) = (x^{n+1})$ , d'où un élément  $a \in A$  tel que  $ax^{n+1} = x^n$ . Puisque  $A$  est intègre et  $x \neq 0$ , on peut simplifier par  $x^n$  et  $ax = 1$  ;  $x$  est donc inversible.

2) Supposons par l'absurde que  $A$  possède une infinité d'idéaux maximaux distincts  $\mathfrak{m}_1, \mathfrak{m}_2, \dots$ . La suite décroissante d'idéaux

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \mathfrak{m}_2 \supset \mathfrak{m}_1 \mathfrak{m}_2 \mathfrak{m}_3 \supset \dots$$

est alors stationnaire, d'où une égalité  $\mathfrak{m}_1 \dots \mathfrak{m}_{n-1} = \mathfrak{m}_1 \dots \mathfrak{m}_n$  qui implique évidemment l'inclusion  $\mathfrak{m}_1 \dots \mathfrak{m}_{n-1} \subset \mathfrak{m}_n$ . D'après le lemme d'évitement 1.1.1, l'un des  $\mathfrak{m}_i$  pour  $i < n$  est contenu dans  $\mathfrak{m}_n$ , ce qui contredit le fait que  $\mathfrak{m}_i$  est maximal. Ainsi,  $A$  n'a qu'un nombre fini d'idéaux maximaux.

Enfin, si  $\mathfrak{p}$  est un idéal premier de  $A$ ,  $A/\mathfrak{p}$  est un anneau artinien intègre, donc un corps d'après le 1). Ainsi,  $\mathfrak{p}$  est maximal.  $\square$

THÉORÈME 1.4.3 (Akizuki). — *Soit  $A$  un anneau. Les conditions suivantes sont équivalentes :*

- a)  $A$  est artinien ;
- b)  $A$  est de longueur finie comme  $A$ -module ;
- c)  $A$  est noethérien et tout idéal premier de  $A$  est maximal.

*Démonstration.* — La condition b) implique que toute suite monotone d'idéaux de  $A$  est stationnaire, d'où a) et la première partie du c).

D'autre part, supposant b), si  $\mathfrak{p}$  est un idéal premier de  $A$ ,  $A/\mathfrak{p}$  est un anneau artinien intègre, donc un corps d'après le 2) du lemme. Par suite  $\mathfrak{p}$  est maximal.

Supposons c). Comme  $A$  est noethérien, il existe une suite de composition

$$0 \subset I_n \subset I_{n-1} \subset \dots \subset I_1 \subset I_0 = A$$

où  $I_k/I_{k+1} = A/\mathfrak{p}_k$  pour un certain idéal premier  $\mathfrak{p}_k$ . La condition c) implique que  $\mathfrak{p}_k$  est un idéal maximal. Par suite,  $A$  est de longueur finie comme  $A$ -module, d'où b).

Il reste à montrer qu'un anneau artinien est de longueur finie comme  $A$ -module. Soient  $\mathfrak{m}_1, \dots, \mathfrak{m}_n$  les idéaux maximaux de  $A$ , en nombre fini d'après le lemme précédent. Introduisons l'idéal

$$I = \mathfrak{m}_1 \dots \mathfrak{m}_n = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n.$$

La suite  $I \supset I^2 \supset \dots$  étant stationnaire, il existe un entier  $s$  tel que  $I^s = I^{s+1}$ . On va montrer que  $I^s = 0$ .

Soit donc  $J = (0 : I^s)$  l'ensemble des  $a \in A$  tels que  $aI^s = 0$ . Si  $J \neq A$ , comme  $A$  est artinien, il existe un plus petit idéal  $J' \subset A$  contenant strictement  $J$ . Soit  $a \in J'$  un élément non nul. On a  $aI + J \neq aA + J$ . Sinon, posant  $M = (A/J)a$ , on aurait  $IM = M$  et d'après le lemme de Nakayama, il existerait  $x \in 1 + I$  tel que  $xM = 0$ . Un tel  $x$  est inversible, d'où  $M = 0$ , contrairement au fait que  $a \neq 0$ . L'inclusion  $J \subset aI + J \subset J'$  montre alors que  $J = aI + J$ , soit  $aI \subset J$ . Pour tout  $b \in I$ , on a  $ab \in J$ , c'est-à-dire  $abI^s = 0$  et donc  $aI^{s+1} = 0$ . Comme  $I^s = I^{s+1}$ ,  $aI^s = 0$  et  $a \in J$ . Ainsi,  $J' = J$ , ce qui est absurde ; nous avons donc prouvé que  $J = A$ , c'est-à-dire  $I^s = 0$ .

Emil ARTIN (1898–1962)

*Les travaux d'E. Artin portèrent sur l'algèbre (groupe de tresses, algèbres semi-simples, groupes finis...) et la théorie des nombres (théorie algébrique et analytique des corps quadratiques, théorie du corps de classes...)*



Dans la suite décroissante d'idéaux

$$A \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_1 \dots \mathfrak{m}_n = I \supset I\mathfrak{m}_1 \supset I\mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset I^2 \supset I^2\mathfrak{m}_1 \supset \cdots \supset I^s = 0$$

chaque quotient successif est un  $A$ -module artinien de la forme  $M/\mathfrak{m}M$ . C'est ainsi un espace vectoriel sur le corps  $A/\mathfrak{m}$ , nécessairement de dimension finie. Par suite, la longueur de chaque quotient successif est finie et  $A$  est de longueur finie comme  $A$ -module.  $\square$

### 1.5. Éléments entiers

Soit  $f : A \rightarrow B$  un homomorphisme d'anneaux. Un élément  $x \in B$  est *entier* sur  $A$  si et seulement s'il existe  $n \geq 1$  et des éléments  $a_1, \dots, a_n \in A$  tels que

$$x^n + f(a_1)x^{n-1} + \cdots + f(a_{n-1})x + f(a_n) = 0.$$

Une telle équation s'appelle *relation de dépendance intégrale*.

PROPOSITION 1.5.1. — *Un élément  $x \in B$  est entier sur  $A$  si et seulement s'il existe un sous-anneau  $R$  de  $B$  contenant  $A[x]$  et qui est de type fini comme  $A$ -module.*

*Démonstration.* — Si  $x$  admet une relation de dépendance intégrale comme ci-dessus, on voit que l'algèbre  $A[x]$  engendrée par  $x$  dans  $B$  est engendrée comme  $A$ -module par  $1, x, \dots, x^{n-1}$ . Il suffit donc de poser  $R = A[x]$ .

Réciproquement, soit  $R$  une sous- $A$ -algèbre contenue dans  $B$  et de type fini comme  $A$ -module. Soient  $m_1, \dots, m_n$  des générateurs de  $M$  comme  $A$ -module. Puisque  $xR \subset R$ , il existe des éléments  $a_{ij} \in A$  tels que  $xm_i = \sum_j a_{ij}m_j$ . La matrice  $xI_n - (a_{ij})$  annule tous les  $m_i$  donc  $R$ . Les formules de Cramer impliquent que son déterminant annule aussi  $R$

et comme  $1 \in R$ , ce déterminant est nul. En le développant, on trouve une relation de dépendance intégrale pour  $x$ .  $\square$

On dit que  $f$  est *entier*, ou bien que  $B$  est entier sur  $A$ , ou encore que  $B$  est une algèbre entière sur  $A$ , ou bien encore que  $B$  est une *extension entière* de  $A$  si tout élément de  $B$  est entier sur  $A$ . Si  $B$  est une  $A$ -algèbre de type fini,  $B$  est entière sur  $A$  si et seulement si  $B$  est un  $A$ -module de type fini. On dit alors que  $B$  est finie sur  $A$ .

L'ensemble des éléments  $x \in B$  entiers sur  $A$  est une sous- $A$ -algèbre de  $B$ , appelée *clôture intégrale* de  $A$  dans  $B$ .

LEMME 1.5.2. — *Si  $A \subset B$  sont deux anneaux intègres avec  $B$  entier sur  $A$ , alors  $A$  est un corps si et seulement si  $B$  est un corps.*

Soient  $k \subset K$  deux corps. Les éléments de  $K$  entiers sur  $k$  sont dits *algébriques*, les autres sont dits *transcendants*. Si tout élément de  $K$  est algébrique sur  $k$ , on dit que  $K$  est algébrique sur  $k$  et on parle d'*extension algébrique*. La clôture intégrale de  $k$  dans  $K$  s'appelle *clôture algébrique* de  $k$  dans  $K$ . Un corps  $k$  est dit *corps — algébriquement clos* s'il est algébriquement clos dans tout corps  $K$  contenant  $k$ . Si  $k$  est un corps, il existe une clôture algébrique de  $k$  : c'est une extension  $k \subset K$  algébrique et algébriquement close. Deux clôtures algébriques de  $k$  sont isomorphes (comme  $k$ -algèbres).

On dit aussi qu'un élément de  $K$  algébrique sur  $k$  est *séparable* sur  $k$  si son polynôme minimal a ses racines distinctes dans une clôture algébrique de  $K$ , ou, de manière équivalente, si la dérivée de ce polynôme minimal est non nulle. Si  $k$  est de caractéristique nulle, cette condition est automatique. On dit qu'une extension algébrique est séparable si tous ses éléments sont séparables.

THÉORÈME 1.5.3 (Théorème de l'élément primitif). — *Soit  $K = k[x, y]$  une extension algébrique finie de corps. On suppose que  $y$  est séparable sur  $k$ . Alors, il existe  $z \in K$  tel que  $K = k[z]$ .*

*Si de plus  $k$  est infini, tout élément de  $K$  de la forme  $x + cy$  pour  $c \in k$  convient, sauf peut-être un nombre fini d'entre eux.*

*Démonstration.* — On ne fait la démonstration que dans le cas où  $k$  est infini. L'autre cas est en un sens plus élémentaire et ne nous servira pas.

Soient  $P$  et  $Q \in k[X]$  les polynômes minimaux de  $x$  et  $y$  respectivement et soit  $F$  une extension finie de  $K$  dans laquelle  $P$  et  $Q$  sont scindés. On notera  $x = x_1, \dots, x_p$  et  $y = y_1, \dots, y_q$  leurs racines. L'hypothèse que  $y$  est séparable implique que les  $y_j$  sont tous distincts. Ainsi, si  $i \in \{1, \dots, p\}$  et  $j \in \{2, \dots, q\}$ , l'équation  $x_i + cy_j = x_1 + cy_1$  n'a qu'une solution et comme  $k$  est infini, on peut choisir  $c$  tel que pour tous  $i$  et  $j$ ,  $j \neq 1$ ,  $x_i + cy_j \neq x_1 + cy_1 = x + cy$ .

Posons  $z = x + cy$  et montrons que  $K = k[z]$ . Le polynôme  $R(X) = P(z - cX) \in k[z][X]$  s'annule pour  $X = y$  puisque  $P(z - cy) = P(x) = 0$ , de même que le polynôme  $Q$  dont  $y$  est

même racine simple. De plus, ils n'ont pas d'autre racine commune : d'après le choix fait pour  $c$ , si  $j \neq 1$ ,  $z - cy_j = x_1 + cy_1 - cy_j$  n'est pas un des  $x_i$  dont  $P(z - cy_j) \neq 0$ . Autrement dit, leur pgcd est égal à  $X - y$ . Or, le théorème de Bézout <sup>(1)</sup> implique que ce pgcd est un polynôme dont les coefficients appartiennent au corps engendré par les coefficients de  $R$  et  $Q$ , c'est-à-dire à  $k[z]$ .

Ainsi,  $y \in k[z]$ , puis  $x = z - cy \in k[z]$ . Par conséquent,  $k[x, y] = k[z]$ .  $\square$

On dit qu'une famille  $(x_i)_{i \in I}$  d'éléments de  $K$  est *algébriquement indépendante* s'il n'existe pas de polynôme non nul  $P \in k[X_i]$  tel que  $P(x_i) = 0$ , autrement dit si l'homomorphisme canonique de  $k$ -algèbres  $k[X_i] \rightarrow K$  tel que  $X_i \mapsto x_i$  est injectif. Une *base de transcendance* de  $K$  sur  $k$  est une famille  $(x_i)$  algébriquement indépendante d'éléments de  $K$  telle que  $K$  est algébrique sur la sous-extension de  $K$  engendrée par les  $x_i$ .

Il existe des bases de transcendance. On a en effet l'analogue suivant du théorème de la base incomplète : si  $L \subset G$  sont deux parties de  $K$ , avec  $L$  algébriquement indépendante sur  $k$  et  $G$  telle que  $K$  est algébrique sur l'extension engendrée par  $G$ , il existe une base de transcendance  $B$  avec  $L \subset B \subset G$ . Le cardinal d'une telle base ne dépend que de l'extension  $k \subset K$  et est appelé *degré de transcendance* de  $K$  sur  $k$ , noté  $\deg \operatorname{tr}_k K$ , voire  $\deg \operatorname{tr} K$  s'il n'y a pas de confusion possible sur  $k$ . Enfin, si  $k \subset K \subset K'$  sont trois corps, on a la relation

$$\deg \operatorname{tr}_k K + \deg \operatorname{tr}_K K' = \deg \operatorname{tr}_k K'.$$

Par abus de langage, on emploiera les mots algébriques, algébriquement indépendants, degré de transcendance pour une  $k$ -algèbre intègre  $A$ . Il s'agira alors des notions correspondantes dans le corps des fractions de  $A$ .

## 1.6. Produit tensoriel

Soient  $k$  un anneau,  $M$  et  $N$  deux  $k$ -modules. Le *produit tensoriel*  $M \otimes_k N$  est un  $k$ -module muni d'une application  $k$ -bilinéaire  $\varphi : M \times N \rightarrow M \otimes_k N$  qui vérifie la propriété universelle suivante : pour tout  $k$ -module  $P$  et toute application  $k$ -bilinéaire  $f : M \times N \rightarrow P$ , il existe une unique application  $k$ -linéaire  $\tilde{f} : M \otimes_k N \rightarrow P$  telle que  $f = \tilde{f} \circ \varphi$ .

On peut le construire en prenant le quotient du  $k$ -module  $k^{(M \times N)}$  dont les éléments sont les sommes finies  $\sum c_{a,b}(a,b)$  par le sous-module engendré par les éléments

$$\lambda(a,b) - (\lambda a, b), \quad \lambda(a,b) - (a, \lambda b), \quad (a+b, c) - (a, c) - (b, c).$$

La classe du couple  $(a, b)$  dans  $M \otimes_k N$  est notée  $a \otimes b$ .

1. Étienne BÉZOUT (1730–1783). — Ses travaux portèrent notamment sur l'utilisation des déterminants pour résoudre les équations linéaires, ainsi que sur le nombre de points intersection de deux courbes algébriques planes. Il publia en 1779 une *Théorie générale des équation algébriques*.

Si  $A$  et  $B$  sont deux  $k$ -algèbres,  $A \otimes_k B$  hérite d'une structure naturelle de  $k$ -algèbre telle que  $(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb')$ . L'application  $A \rightarrow A \otimes_k B$  définie par  $a \mapsto a \otimes 1$  est alors un homomorphisme d'algèbres ; de même, on a un homomorphisme d'algèbres  $B \rightarrow A \otimes_k B$ .

Par exemple, si  $(X_i)$  et  $(Y_j)$  sont des indéterminées, on a

$$k[X_i] \otimes_k k[Y_j] \simeq k[X_i, Y_j]$$

l'isomorphisme étant induit par l'application bilinéaire

$$k[X_i] \times k[Y_j] \rightarrow k[X_i, Y_j], \quad (P(X_i), Q(Y_j)) \mapsto P(X_i)Q(Y_j).$$

On laisse au lecteur le lemme suivant.

LEMME 1.6.1. — Soient  $I$  un idéal de  $A$  et  $J$  un idéal de  $B$ , ils engendrent un idéal  $(I, J)$  dans  $A \otimes_k B$  et l'on a un isomorphisme canonique

$$(A \otimes_k B)/(I, J) \simeq (A/I) \otimes_k (B/J)$$

qui envoie la classe de  $a \otimes b$  vers le produit tensoriel des classes de  $a$  et de  $b$ .

## 1.7. Limites inductives

Soit  $I$  un ensemble ordonné. On suppose que  $I$  est filtrant, c'est-à-dire que si  $i$  et  $j$  sont deux éléments de  $I$ , il existe  $k \in I$  tel que  $k \geq i$  et  $k \geq j$ .

Soit  $\mathfrak{C}$  une catégorie. Un système inductif dans  $\mathfrak{C}$  est la donnée pour tout  $i$  dans  $I$  d'un objet  $A_i$  de  $\mathfrak{C}$  et pour tous  $i \leq j$  dans  $I$  d'un morphisme  $\varphi_{ij} : A_i \rightarrow A_j$  tels que :

– si  $i \leq j \leq k$ ,  $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$  ;

– pour tout  $i$ ,  $\varphi_{ii} = \text{id}_{A_i}$ .

Soit  $\mathcal{A} = ((A_i)_i, (\varphi_{ij}))$  un tel système inductif. Soit  $A$  un objet de  $\mathfrak{C}$  et pour tout  $i \in I$  un morphisme  $\theta_i : A_i \rightarrow A$  tels que pour tous  $i \leq j$ ,  $\theta_i = \theta_j \circ \varphi_{ij}$ . On dit que  $(A, (\theta)_i)$  est une limite inductive du système inductif  $\mathcal{A}$  si pour tout objet  $B$  de  $\mathfrak{C}$  muni de morphismes  $\psi_i : A_i \rightarrow B$  vérifiant  $\psi_i = \psi_j \circ \varphi_{ij}$ , il existe un unique morphisme  $\alpha : A \rightarrow B$  tel que  $\psi_i = \alpha \circ \theta_i$  pour tout  $i \in I$ .

Si un système inductif admet une limite, celle-ci est unique à isomorphisme unique près. On la note  $\varinjlim A_i$ .

Dans les catégories des ensembles, des groupes, des anneaux, des modules, des  $k$ -algèbres, tout système inductif  $(a_i)$  admet une limite inductive. On la construit comme suit. Soit  $X$  la réunion disjointe des  $A_i$  et soit  $\sim$  la relation d'équivalence suivante dans  $X$  définie ainsi : si  $a \in A_i$  et  $b \in A_j$ ,  $a \sim b$  si et seulement si il existe  $k \in I$  tel que  $k \geq i$  et  $k \geq j$

tels que  $c = \varphi_{ik}(a) = \varphi_{jk}(b)$ . L'ensemble quotient  $X/\sim$  est alors une limite inductive du système  $(A_i)$ .

Si  $J$  est une partie de  $I$  et  $(A_i)$  un système inductif indexé par  $I$ , on a un morphisme naturel

$$\lim_{\substack{\longrightarrow \\ j \in J}} A_j \rightarrow \lim_{\substack{\longrightarrow \\ i \in I}} A_i.$$

Si pour tout  $i \in I$ , il existe  $j \in J$  tel que  $j \geq i$  (on dit que  $J$  est cofinal dans  $I$ ), ce morphisme est un isomorphisme.

*Exercice 1.7.1.* — Soit  $A$  un anneau et  $S$  une partie multiplicative de  $A$ . On munit  $S$  de la relation de divisibilité :  $s \leq s'$  si et seulement si il existe  $t \in S$  tel que  $s' = ts$ .

Soit  $M$  un  $A$ -module. Pour tout  $s \in S$ , on pose  $M_s = M$  et pour  $s \leq st$ , on définit  $\varphi_{s,st} : M_s \rightarrow M_{st}$  comme la multiplication par  $t$  dans  $M$ . Montrer que cela définit un système inductif et que  $\lim_{\substack{\longrightarrow \\ s \in S}} (M_s) = S^{-1}M$ .



# CHAPITRE 2

## PRÉLIMINAIRES DE TOPOLOGIE

### 2.1. Faisceaux

Dans son article fondamental [?], Jean-Pierre Serre a montré que la théorie des faisceaux inventée un peu plus de 20 ans auparavant par Jean Leray <sup>(1)</sup> pouvait s'appliquer avec succès en géométrie algébrique. Désormais, c'est l'un des outils inévitables de tout géomètre algébriste.

Rappelons en brièvement la définition.

**DÉFINITION 2.1.1.** — *Soit  $X$  un espace topologique. Un préfaisceau  $\mathcal{F}$  sur  $X$  est la donnée pour tout ouvert  $U$  de  $X$  un ensemble  $\mathcal{F}(U)$  et pour tout couple d'ouverts  $V \subset U$  d'une application  $r_{UV} : \mathcal{F}(U) \rightarrow \mathcal{F}(V)$  telles que  $r_{UU} = \text{id}$  et si  $W \subset V \subset U$  sont trois ouverts,  $r_{UW} = r_{VW} \circ r_{UV}$ .*

*On dit que  $\mathcal{F}$  est un faisceau si pour tout ouvert  $U$  de  $X$  et toute famille d'ouverts  $(U_i)_i$  telle que  $U = \bigcup_i U_i$ , l'application naturelle*

$$(r_{UU_i}) : \mathcal{F}(U) \rightarrow \prod_i \mathcal{F}(U_i)$$

*est injective et a pour image l'ensemble des  $(f_i)_i \in \prod \mathcal{F}(U_i)$  tels que pour tout couple  $(i, j)$ ,*

$$r_{U_i, U_i \cap U_j}(f_i) = r_{U_j, U_i \cap U_j}(f_j).$$

**Exemple 2.1.2** (Faisceau des fonctions). — Notons  $\mathcal{F}(U)$  l'ensemble des fonctions de  $U$  dans  $\mathbf{R}$  et soit  $r_{UV}$  l'application de restriction. Alors,  $\mathcal{F}$  est un faisceau.

Par analogie avec cet exemple, les  $r_{UV}$  sont appelées applications de restriction et  $r_{UV}(f)$  est souvent noté  $f|_V$ . Des raisons historiques font que  $\mathcal{F}(U)$  est aussi noté  $\Gamma(U, \mathcal{F})$ .

---

1. Jean LERAY. — Inventa aussi bien la théorie des faisceaux en topologie algébrique que la notion de « solution faible » en théorie des équations aux dérivées partielles qu'il appliqua à l'étude de l'équation d'Euler en hydrodynamique.

*Exemple 2.1.3* (Faisceau des fonctions continues). — Notons  $\mathcal{C}(U)$  l'ensemble des fonctions continues  $U \rightarrow \mathbf{R}$  et soit  $r_{UV}$  l'application qui associe à une fonction continue sur  $U$  sa restriction à l'ouvert  $V$ . Alors,  $\mathcal{C}$  est un faisceau ; pour la surjectivité, il faut se rappeler qu'une fonction est continue si et seulement si elle est continue en tout point, et ceci équivaut à ce que sa restriction à un voisinage de ce point y soit continue.

On définit aussi des faisceaux en groupes, en anneaux,... Par exemple, pour un faisceau en groupes, on suppose que chaque  $\mathcal{F}(U)$  est un groupe et que les applications de restriction sont des morphismes de groupes. Le faisceau des fonctions continues sur un espace topologique est ainsi un faisceau en  $\mathbf{R}$ -algèbres.

**DÉFINITION 2.1.4.** — Si  $\mathcal{F}$  et  $\mathcal{G}$  sont deux (pré)-faisceaux sur  $X$ , un morphisme de (pré)-faisceaux  $\varphi : \mathcal{F} \rightarrow \mathcal{G}$  est la donnée pour tout ouvert  $U$  de  $X$  d'une application  $\varphi(U) : \mathcal{F}(U) \rightarrow \mathcal{G}(U)$  telles que  $\varphi(V) \circ r_{UV} = r_{UV} \circ \varphi(U)$ .

Si  $\mathcal{F}$  et  $\mathcal{G}$  sont des faisceaux en groupes, on ajoutera à la définition d'un morphisme de faisceaux en groupes la condition que les applications  $\varphi(U)$  sont des morphismes de groupes. De même pour les faisceaux en anneaux,...

*Exemple 2.1.5.* — Les injections naturelles  $\mathcal{C}(U) \rightarrow \mathcal{F}(U)$  définissent un morphisme de faisceaux  $\mathcal{C} \rightarrow \mathcal{F}$ .

Si  $\mathcal{F}$  et  $\mathcal{G}$  sont deux (pré)-faisceaux sur  $X$  tels que pour tout ouvert  $U$ ,  $\mathcal{F}(U) \subset \mathcal{G}(U)$ , on dit que  $\mathcal{F}$  est un sous-(pré)-faisceau de  $\mathcal{G}$ . Par exemple, le faisceau des fonctions continues est un sous-faisceau du faisceau des fonctions.

On ne détaille pas la construction du faisceau  $\mathcal{F}^\dagger$  associé à un préfaisceau  $\mathcal{F}$  : c'est un faisceau muni d'un morphisme  $\mathcal{F} \rightarrow \mathcal{F}^\dagger$  universel pour les morphismes de  $\mathcal{F}$  dans un faisceau. Dans le cas fréquent où  $\mathcal{F}$  est un sous-préfaisceau d'un faisceau  $\mathcal{G}$ ,  $\mathcal{F}^\dagger$  est un sous-faisceau de  $\mathcal{G}$  que l'on peut définir ainsi : un élément  $f \in \mathcal{G}(U)$  appartient à  $\mathcal{F}^\dagger(U)$  si et seulement s'il existe un recouvrement ouvert  $(U_i)_i$  de  $U$  tel que pour tout  $i$ ,  $r_{UU_i}(f) \in \mathcal{F}(U_i)$ .

**DÉFINITION 2.1.6.** — Soit  $f : X \rightarrow Y$  une application continue entre espaces topologiques. Si  $\mathcal{F}$  est un faisceau sur  $X$ , on définit un faisceau  $f_*\mathcal{F}$  sur  $Y$  en posant  $f_*\mathcal{F}(U) = \mathcal{F}(f^{-1}(U))$  pour tout ouvert  $U$  de  $Y$ .

Si  $\mathcal{G}$  est un faisceau sur  $Y$ , le faisceau  $f^{-1}\mathcal{G}$  est le faisceau associé au préfaisceau dont l'ensemble des sections sur un ouvert  $U$  de  $X$  est la limite inductive des  $\mathcal{G}(V)$  lorsque  $V$  parcourt les ouverts de  $Y$  qui contiennent  $f(U)$ .

*Exemple 2.1.7.* — Si  $f : X \rightarrow Y$  est une application continue, on a un morphisme de faisceaux  $f^* : f^{-1}\mathcal{C}_Y \rightarrow \mathcal{C}_X$  : si  $V$  est un ouvert de  $X$ , un élément de  $f^{-1}\mathcal{C}_Y(V)$  est une fonction continue  $\varphi$  sur un voisinage de  $f(V)$ . On lui associe la fonction  $\varphi \circ f$  qui est continue sur  $V$ .

On a aussi un morphisme de faisceaux  $\mathcal{C}_Y \rightarrow f_*\mathcal{C}_X$  : si  $V$  est un ouvert de  $Y$ , un élément de  $f_*\mathcal{C}_X(V)$  est une fonction continue sur  $f^{-1}(V)$ . Ainsi, à la fonction  $\varphi \in \mathcal{C}_Y(V)$ , on associe la fonction  $\varphi \circ f \in \mathcal{C}_X(f^{-1}(V))$ .

*Exercice 2.1.8* (cf. [?], Ex. II.1.18). — Soient  $f : X \rightarrow Y$  une application continue,  $\mathcal{F}$  un faisceau sur  $X$  et  $\mathcal{G}$  un faisceau sur  $Y$ . Définir des applications « naturelles »  $f^{-1}f_*\mathcal{F} \rightarrow \mathcal{F}$  et  $\mathcal{G} \rightarrow g_*g^{-1}\mathcal{G}$  et en déduire une bijection

$$\mathrm{Hom}(f^{-1}\mathcal{G}, \mathcal{F}) \simeq \mathrm{Hom}(\mathcal{G}, f_*\mathcal{F}).$$

## 2.2. Espaces annelés

La « vraie » définition d'un espace annelé dont a besoin la théorie des schémas est courte : c'est un espace topologique muni d'un faisceau d'anneau. Cependant, comme notre introduction à la géométrie algébrique se limite aux variétés algébriques, nous pourrions nous contenter d'une définition plus restrictive et supposer que le faisceau d'anneaux est un sous-faisceau du faisceau des fonctions.

**DÉFINITION 2.2.1.** — *On appelle espace annelé la donnée d'un espace topologique  $X$  et d'un sous-faisceau  $\mathcal{O}_X$  du faisceau des fonctions sur  $X$ .*

*Un morphisme d'espaces annelés est une application continue  $f : X \rightarrow Y$  telle que pour tout ouvert  $U$  de  $Y$  et toute fonction  $\varphi \in \mathcal{O}_Y(U)$ , la fonction  $\varphi \circ f$  sur  $f^{-1}(U)$  appartient à  $\mathcal{O}_X(f^{-1}(U))$ .*

(Autrement dit, on a  $\mathcal{O}_Y \subset f_*\mathcal{O}_X$ .)

**DÉFINITION 2.2.2.** — *Si  $(X, \mathcal{O}_X)$  est un espace annelé et  $U$  un ouvert de  $X$ , le couple  $(U, \mathcal{O}_X|_U)$  est un espace annelé, appelé espace annelé induit par  $X$  sur  $U$ .*

*Plus généralement, si  $i : A \hookrightarrow X$  est l'inclusion d'une partie de  $A$  dans  $X$ , soit  $\mathcal{I}_A$  le sous-faisceau de  $\mathcal{O}_X$  tel que pour tout ouvert  $U \subset X$ ,  $f \in \mathcal{I}_A(U)$  si et seulement si  $f(x) = 0$  pour tout  $x \in A \cap U$ . L'espace annelé  $(A, i^{-1}(\mathcal{O}_X/\mathcal{I}_A))$  est appelé espace annelé induit par  $X$  sur  $A$ .*

## 2.3. Espaces annelés modelés

En géométrie différentielle, on définit une variété comme un espace topologique plus une structure supplémentaire (appelée en général *atlas*) une famille de paramétrisations, qui permet d'identifier un voisinage de tout point à un ouvert de  $\mathbf{R}^n$ . Ces paramétrisations

sont « compatibles » en ce sens que sur l'intersection de deux voisinages, on passe d'une identification à une autre par un difféomorphisme d'ouverts de  $\mathbf{R}^n$ .

Les paramétrisations permettent alors de définir la notion de fonction différentiable sur une variété différentielle ; le fait que la notion soit bien définie provient de ce que la composition d'une fonction différentiable et d'un difféomorphisme est différentiable. Et si, par hasard, on n'avait imposé aux difféomorphismes qui identifient deux paramétrisations de n'être que des homéomorphismes, ou bien, de n'être que de classe  $\mathcal{C}^p$ , on n'aurait pu définir que des fonctions continues, ou que des fonctions de classe  $\mathcal{C}^k$  pour  $k \leq p$ .

Mieux, on peut même définir maintenant intrinsèquement, c'est-à-dire sans référence à l'atlas, la notion de  $\mathcal{C}^p$ -difféomorphisme de variétés : une application continue  $f : X \rightarrow Y$  est de classe  $\mathcal{C}^p$  si et seulement si pour toute fonction  $\varphi$  de classe  $\mathcal{C}^p$  sur  $Y$ , la fonction  $\varphi \circ f$  est de classe  $\mathcal{C}^p$  sur  $X$ . Inversement, on peut retrouver les paramétrisations dont on est parti : ce sont des  $\mathcal{C}^\infty$ -difféomorphismes d'un ouvert de  $X$  sur un ouvert de  $\mathbf{R}^n$ .

Autrement dit, la structure intéressante n'est pas tant l'atlas — qui pour être intrinsèque nécessite l'artifice lourd consistant à considérer des atlas maximaux — que le couple formé de  $X$  et du faisceau des fonctions  $\mathcal{C}^\infty$  sur  $X$  : un espace annelé ! Le fait que  $X$  soit une variété différentiable de dimension  $n$  se traduit en disant que tout point de  $X$  possède un voisinage  $U$  tel que  $(U, \mathcal{C}^\infty|_U)$  soit isomorphe en tant qu'espace annelé à l'espace annelé défini par un ouvert de  $\mathbf{R}^n$ .

On veut généraliser un peu ces considérations. Donnons nous une sous-catégorie pleine  $\mathcal{L}$  (pour *locale*) de la catégorie des espaces annelés. Ce seront les modèles locaux. On dira qu'un espace annelé  $X$  est modelé sur  $\mathcal{L}$  si tout point de  $X$  possède un voisinage ouvert isomorphe à un objet de  $\mathcal{L}$ . Cela définit les objets d'une catégorie  $\mathcal{G}$  (pour *globale*) dont les morphismes sont les morphismes d'espaces annelés.

Pour construire des exemples non triviaux, la méthode suivante, dite de recollement, est fondamentale.

### THÉORÈME 2.3.1 (Construction d'espaces annelés par recollement)

Soient  $(X_i, \mathcal{O}_{X_i})_i$  une famille finie d'espaces annelés et, pour tout couple  $(i, j)$  un ouvert  $X_{ij}$  de  $X_j$ , un isomorphisme d'espaces annelés  $\varphi_{ij} : X_{ij} \rightarrow X_{ji}$ , tels que

- si  $i = j$ ,  $X_{ii} = X_i$  et  $\varphi_{ii} = \text{id}_{X_i}$  ;
- pour tous  $i$  et  $j$ ,  $\varphi_{ji} = \varphi_{ij}^{-1}$  ;
- pour tous  $i, j, k$ ,  $\varphi_{ij}(X_{ij} \cap X_{jk}) = X_{ji} \cap X_{jk}$  et on a la relation  $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$  sur l'ouvert  $X_{ij} \cap X_{jk}$  de  $X_i$ .

Alors, il existe une (à isomorphisme unique près) unique espace annelé  $(X, \mathcal{O}_X)$  muni d'une famille d'ouverts  $U_i$ , et pour tout  $i$  un isomorphisme d'espaces annelés

$$\varphi_i : (U_i, \mathcal{O}_X|_{U_i}) \rightarrow (X_i, \mathcal{O}_{X_i})$$

tels que pour tous  $i$  et  $j$ ,  $X_{ij} = \varphi_i(U_i \cap U_j)$  et  $\varphi_{ij} = \varphi_j \circ \varphi_i^{-1}$ .

*Démonstration.* — L'unicité est à peu près tautologique : si on a deux tels espaces annelés  $(X, \mathcal{O}_X)$  et  $(X', \mathcal{O}_{X'})$ , on constate que  $\theta_i = (\varphi'_i)^{-1} \circ \varphi_i$  est un isomorphisme  $U_i \rightarrow U'_i$  et que sur  $U_i \cap U_j$ ,  $\theta_i = \theta_j$ , d'où un isomorphisme canonique  $\theta : X \rightarrow X'$ .

Il nous faut donc maintenant construire un tel  $X$ . Soit d'abord  $X_* = X_i$  l'espace annelé réunion disjointe des  $X_i$  ; un point de  $X_*$  est ainsi un couple  $(i, x)$  où  $x \in X_i$ . On définit une relation sur  $X_*$  en posant  $(i, x) \sim (j, y)$  si et seulement si  $x \in X_{ij}$  et  $y = \varphi_{ij}(x)$ . C'est une relation d'équivalence et on définit l'espace topologique sous-jacent à  $X$  comme le quotient de  $X_*$  par cette relation d'équivalence. (Autrement dit,  $X$  est l'ensemble des classes d'équivalences de points de  $X_*$  muni de la topologie quotient pour laquelle une partie  $\Omega \subset X$  est ouverte si et seulement si son image réciproque dans  $X_*$  est ouverte.) On note  $\pi$  l'application continue canonique  $X_* \rightarrow X$ .

On définit  $U_j = \pi(X_j)$  et il est facile de vérifier que  $\pi : X_j \rightarrow U_j$  est un homéomorphisme. L'image réciproque dans  $X_*$  de  $U_j$  est l'ouvert  ${}_i X_{ij}$  ; par suite,  $X_j$  est ouvert dans  $X$ . Les  $U_j$  forment donc un recouvrement ouvert de  $X$ .

Pour définir le faisceau  $\mathcal{O}_X$ , on doit donner ses sections sur un ouvert  $V$  arbitraire :  $\mathcal{O}_X(V)$  est l'ensemble des fonctions  $f$  sur  $V$  telles que  $f \circ \pi \in \mathcal{O}_{X_*}(\pi^{-1}(V))$ . Il est facile de voir que cela définit bien un faisceau. Par construction même, l'image réciproque du faisceau  $\mathcal{O}_X|_{U_j}$  sur  $X_j$  est canoniquement isomorphe à  $\mathcal{O}_{X_j}$ .  $\square$

Il nous reste à énoncer deux lemmes faciles et néanmoins utiles.

LEMME 2.3.2. — *Soient  $X$  un espace topologique et  $(U_i)_i$  un recouvrement ouvert de  $X$ . Une partie  $Z$  de  $X$  est ouverte (resp. fermée) si et seulement si pour tout  $i$ ,  $Z \cap U_i$  est ouvert (resp. fermé) dans  $U_i$ .*

*Démonstration.* — Démontrons le pour ouvert, l'assertion correspondante pour les fermés s'en déduit par passage aux complémentaires. Si  $Z$  est ouvert, il est clair que  $Z \cap U_i$  est ouvert dans  $U_i$  pour tout  $i$ . Réciproquement, soit  $z \in Z$ . Il existe  $i$  tel que  $z \in U_i$ . Comme  $Z \cap U_i$  est ouvert dans  $U_i$ , il contient un voisinage ouvert de  $z$  dans  $U_i$ , qui est donc de la forme  $\Omega \cap U_i$  pour un ouvert  $\Omega$  de  $X$ . Puisque  $U_i$  est ouvert,  $Z \cap U_i$  est un voisinage ouvert de  $z$  contenu dans  $Z$ , si bien que  $Z$  est ouvert.  $\square$

LEMME 2.3.3 (Description locale des morphismes). — *Si  $f : X \rightarrow Y$  est un morphisme d'espaces annelés et si  $U \subset X$ ,  $V \subset f(U) \subset Y$ , alors  $f : U \rightarrow V$  est un morphisme d'espaces annelés.*

*Réciproquement, une application  $f : X \rightarrow Y$  est un morphisme d'espaces annelés s'il existe des recouvrements ouverts  $(U_i)$  de  $X$  et  $(V_i)$  de  $Y$  tels que pour tout  $i$ ,  $f(U_i) \subset V_i$  et  $f|_{U_i} : U_i \rightarrow V_i$  soit un morphisme d'espaces annelés.*



# CHAPITRE 3

## VARIÉTÉS ALGÈBRIQUES

### 3.1. Ensembles algébriques

Soit  $k$  un corps (commutatif, bien entendu !). On note  $\mathbf{A}^n = k^n$  l'espace affine sur  $k$ . La géométrie algébrique s'intéresse aux ensembles définis par des équations polynomiales, c'est-à-dire aux parties  $Z$  de  $\mathbf{A}^n$  définies par l'annulation d'une famille de polynômes de  $k[X_1, \dots, X_n]$ . Par exemple :

$$\begin{aligned}(3.1.1) \quad & Z_1 = \{(x, y) \in \mathbf{C}^2; x^2 + y^2 + 1 = 0\} \\(3.1.2) \quad & Z_2 = \{(x, y) \in \mathbf{R}^2; x^2 + y^2 + 1 = 0\}, \\(3.1.3) \quad & Z_3 = \{(x, y) \in \mathbf{C}^2; y^2 = x^3 - x\}, \\(3.1.4) \quad & Z_4 = \{(x, y, z) \in \mathbf{Q}^n; x^n + y^n = z^n\} \quad (n \geq 1).\end{aligned}$$

Mais si  $Z$  est une telle partie, et si deux polynômes  $P_1$  et  $P_2$  s'annulent sur  $Z$ ,  $P_1 + P_2$  s'annulera sur  $Z$ , de même que  $\lambda P_1$  pour tout  $\lambda \in k$ . Ainsi, au lieu d'une famille quelconque de polynômes, on s'intéresse directement aux *idéaux* de  $k[X_1, \dots, X_n]$ .

**DÉFINITION 3.1.5.** — Soit  $I$  un idéal de  $k[X_1, \dots, X_n]$ . On appelle ensemble algébrique défini par  $I$  l'ensemble

$$\mathcal{V}(I) = \{(x_1, \dots, x_n) \in \mathbf{A}^n; \forall P \in I, P(x_1, \dots, x_n) = 0\}.$$

Réciproquement, si  $Z$  est une partie de  $\mathbf{A}^n$ , on définit l'idéal de  $Z$  comme

$$\mathcal{I}(Z) = \{P \in k[X_1, \dots, X_n]; \forall (x_1, \dots, x_n) \in Z, P(x_1, \dots, x_n) = 0\}.$$

Comme l'anneau  $k[X_1, \dots, X_n]$  est noethérien, un ensemble algébrique est en fait défini par un ensemble fini de polynômes. Si  $f_1, \dots, f_r$  sont des polynômes, on notera  $\mathcal{V}(f_1, \dots, f_r)$  l'ensemble algébrique  $\mathcal{V}((f_1, \dots, f_r))$  défini par l'idéal engendré par les  $f_i$ .

D'autre part, les propriétés suivantes sont élémentaires :

PROPOSITION 3.1.6

1. Si  $I_1 \subset I_2$ ,  $\mathcal{V}(I_1) \supset \mathcal{V}(I_2)$ .
2. Si  $Z_1 \subset Z_2$ ,  $\mathcal{I}(Z_1) \supset \mathcal{I}(Z_2)$ .
3. Si  $Z_1$  et  $Z_2$  sont deux parties de  $\mathbf{A}^n$ ,  $\mathcal{I}(Z_1 \cup Z_2) = \mathcal{I}(Z_1) \cap \mathcal{I}(Z_2)$ .
4. Pour tout idéal  $I$ ,  $I \subset \mathcal{I}(\mathcal{V}(I))$ .
5. Pour toute partie  $Z \subset \mathbf{A}^n$ ,  $Z \subset \mathcal{V}(\mathcal{I}(Z))$ , avec égalité si et seulement si  $Z$  est un ensemble algébrique.

*Exercice 3.1.7.* — Les démontrer (voir [?], I.1.2, pour une démonstration).

COROLLAIRE 3.1.8. — Les applications  $\mathcal{I}$  et  $\mathcal{V}$  définissent des bijections réciproques l'une de l'autre entre ensembles algébriques de  $\mathbf{A}^n$  et idéaux de  $k[X_1, \dots, X_n]$  de la forme  $\mathcal{I}(Z)$ .

PROPOSITION 3.1.9. — L'ensemble vide et  $\mathbf{A}^n$  sont des ensembles algébriques.

*La réunion de deux ensembles algébriques est un ensemble algébrique.*

*L'intersection d'une famille quelconque d'ensembles algébriques est un ensemble algébrique.*

*Démonstration.* — L'ensemble vide et  $\mathbf{A}^n$  sont définis par les idéaux  $k[X_1, \dots, X_n]$  et  $(0)$  respectivement.

Si  $Z_1$  et  $Z_2$  sont deux parties de  $\mathbf{A}^n$  définies par des idéaux  $I_1$  et  $I_2$ , montrons que  $Z_1 \cup Z_2 = \mathcal{V}(I_1 \cdot I_2)$ . (Rappelons que  $I_1 \cdot I_2$  est l'idéal de  $k[X_1, \dots, X_n]$  engendré par les produits  $f_1 f_2$ , où  $f_1 \in I_1$  et  $f_2 \in I_2$ .) En effet, comme  $I_1 I_2 \subset I_1$ , on a  $Z_1 \subset \mathcal{V}(I_1 \cdot I_2)$ , et de même pour  $Z_2$ , d'où une inclusion. Dans l'autre sens, si  $x = (x_1, \dots, x_n) \notin Z_1 \cup Z_2$ , il existe  $f_1 \in I_1$  et  $f_2 \in I_2$  tels que  $f_1(x) \neq 0$  et  $f_2(x) \neq 0$ . Il en résulte  $f_1 f_2(x) \neq 0$ , d'où  $x \notin \mathcal{V}(I_1 \cdot I_2)$ .

Enfin soit  $(Z_\alpha)_{\alpha \in A}$  une famille d'ensembles algébriques de  $\mathbf{A}^n$ ,  $Z_\alpha$  étant défini par un idéal  $I_\alpha$ . Montrons que  $\bigcap_\alpha Z_\alpha$  est défini par l'idéal  $I = \sum_\alpha I_\alpha$  engendré par les  $I_\alpha$ . Comme pour tout  $\alpha$ , on a  $I_\alpha \subset I$ , il vient  $\mathcal{V}(I) \subset Z_\alpha$ , et donc  $\mathcal{V}(I) \subset \bigcap_\alpha Z_\alpha$ . Réciproquement, considérons  $x \in \bigcap_\alpha Z_\alpha$  et  $f \in I$ . On peut écrire  $f$  comme une somme finie  $\sum_\alpha f_\alpha$ , où pour tout  $\alpha$ ,  $f_\alpha \in I_\alpha$ . Comme  $x \in Z_\alpha$ , on a  $f_\alpha(x) = 0$  et finalement,  $f(x) = 0$ , ce qui prouve que  $x \in \mathcal{V}(I)$ .  $\square$

*Exercice 3.1.10.* — Un ensemble algébrique peut être défini par plusieurs idéaux. Par exemple, les idéaux  $I_1 = (X^2 + Y^2, XY^3)$  et  $I_2 = (X^2, Y^3)$  de  $\mathbf{C}[X, Y]$  définissent tous deux  $(0, 0)$  dans  $\mathbf{C}^2$ . Prouver qu'ils sont effectivement distincts.

Montrer cependant que l'idéal  $I_3 = (X, Y) = \mathcal{I}((0, 0))$  les contient tous deux et que c'est le plus grand idéal de définition de  $(0, 0)$ .

David HILBERT (1862–1943)

*Hilbert a contribué à un grand nombre de branches des mathématiques : théorie des invariants, nombres algébriques, analyse fonctionnelle, physique mathématique (relativité générale), calcul des variations... Les 23 problèmes qu'il a soulevés lors du congrès international de Paris en 1900 ont servi de fil conducteur à des pans entiers des mathématiques du XX<sup>e</sup> siècle.*



Lorsque le corps  $k$  est algébriquement clos, le théorème des zéros de Hilbert, auquel un snobisme atavique nous fait préférer son nom allemand *Nullstellensatz*, décrit le plus grand idéal de définition d'un ensemble algébrique en terme d'un idéal de définition quelconque. Ce théorème possède (au moins) quatre incarnations, toutes intéressantes. Les voici.

**THÉORÈME 3.1.11 (Nullstellensatz, 1).** — Soient  $k$  un corps et  $A$  une  $k$ -algèbre de type fini. Si  $A$  est un corps, alors  $A$  est une extension algébrique finie de  $k$ .

*Preuve* (Zariski, cf. [?], ex. 18, p. 70). — Soient  $x_1, \dots, x_n \in A$  des générateurs de  $A$  comme  $k$ -algèbre. On raisonne par récurrence sur  $n$ . Si  $n = 1$ , c'est-à-dire  $A = k[x_1]$ , alors  $x_1$  est nécessairement algébrique sur  $k$  car, s'il était transcendant,  $A$  serait isomorphe à  $k[X]$  qui n'est pas un corps. Supposons  $n > 1$  et le résultat vrai pour  $n - 1$ . Soit  $K \subset A$  le corps des fractions de  $k[x_1]$ ; on voit que  $A = K[x_2, \dots, x_n]$  et par récurrence,  $A$  est algébrique sur  $K$ . Il existe ainsi des polynômes unitaires  $P_2, \dots, P_n$  dans  $K[X]$  tels que  $P_j(x_j) = 0$ . Soit  $f \in K^*$  le produit des dénominateurs des  $P_j$ , de sorte que les coefficients de  $P_j$  appartiennent à  $A' = k[x_1][1/f]$ . Autrement dit,  $A$  est entière sur  $A'$ . Comme  $A$  est un corps,  $A'$  aussi d'après 1.5.2.

Si  $x_1$  était transcendant sur  $k$ , on aurait  $A' \simeq k[X][1/P]$  pour  $P$  un polynôme non nul de  $k[X]$ . Il est alors facile de voir que  $A'$  n'est pas un corps, par exemple parce que  $1 + XP$  n'est pas nul, mais n'est pas non plus inversible. Autrement dit,  $x_1$  est algébrique sur  $k$ , les  $x_j$  pour  $j \geq 2$  sont algébriques sur  $k[x_1]$  donc sur  $k$ , et  $A$  est la composée d'un nombre fini d'extensions algébriques finies de  $k$ , donc une extension algébrique finie de  $k$ .  $\square$

**COROLLAIRE 3.1.12 (Nullstellensatz, 2).** — Si  $k$  est un corps algébriquement clos, les idéaux maximaux de  $k[X_1, \dots, X_n]$  sont de la forme  $(X_1 - a_1, \dots, X_n - a_n)$  pour  $(a_1, \dots, a_n) \in \mathbf{A}^n$ .

*Démonstration.* — Soit  $\mathfrak{m}$  un idéal maximal de  $k[X_1, \dots, X_n]$  et  $A$  l'anneau quotient  $k[X_1, \dots, X_n]/\mathfrak{m}$  qui est une  $k$ -algèbre de type fini, engendrée par les images des  $X_j$ . Comme  $\mathfrak{m}$  est supposé maximal,  $A$  est un corps et donc, d'après le théorème 3.1.11, une extension algébrique finie de  $k$ . Le corps  $k$  étant algébriquement clos, l'inclusion  $k \hookrightarrow A$  est un isomorphisme. Il existe donc des éléments  $a_1, \dots, a_n \in k$  tels que  $X_j - a_j \in \mathfrak{m}$ , d'où

$$\mathfrak{m} \supset (X_1 - a_1, \dots, X_n - a_n).$$

Réciproquement, soit  $P \in \mathfrak{m}$ . Par des divisions euclidiennes, on peut écrire

$$P = (X_1 - a_1)Q_1(X_1, \dots, X_n) + (X_2 - a_2)Q_2(X_2, \dots, X_n) \\ + \dots + (X_n - a_n)Q_n(X_n) + P(a_1, \dots, a_n).$$

La constante  $P(a_1, \dots, a_n)$  appartient donc à  $\mathfrak{m}$  et est nécessairement nulle, ce qui implique  $P \in (X_1 - a_1, \dots, X_n - a_n)$ .  $\square$

**COROLLAIRE 3.1.13** (Nullstellensatz, 3). — *Soient  $k$  un corps algébriquement clos et  $I$  un idéal de  $k[X_1, \dots, X_n]$  distinct de  $(1)$ . Alors,  $\mathcal{V}(I) \neq \emptyset$ .*

*Démonstration.* — Soit  $\mathfrak{m}$  un idéal maximal de  $k[X_1, \dots, X_n]$  contenant  $I$ . D'après le corollaire 3.1.12, il existe  $(a_1, \dots, a_n) \in \mathbf{A}^n$  tel que  $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ . On en déduit que pour tout  $P \in \mathfrak{m}$ , et a fortiori pour tout  $P \in I$ , on a  $P(a_1, \dots, a_n) = 0$ . Autrement dit,  $(a_1, \dots, a_n) \in \mathcal{V}(I)$  qui est ainsi non vide.  $\square$

**COROLLAIRE 3.1.14** (Nullstellensatz, 4). — *Supposons que  $k$  est algébriquement clos et soit  $Z$  un ensemble algébrique de  $\mathbf{A}^n$  défini par un idéal  $I$ . Alors,  $\mathcal{I}(Z) = \sqrt{I}$ , le radical de  $I$ .*

*Démonstration.* — Rappelons que  $\sqrt{I}$  est l'ensemble des  $P \in k[X_1, \dots, X_n]$  tels qu'il existe  $r \geq 1$  de sorte que  $P^r \in I$ . Si  $P \in \sqrt{I}$ , soit  $r \geq 1$  tel que  $P^r \in I$ . Ainsi, pour tout  $x \in Z$ ,  $P^r(x) = 0$ , et donc  $P(x) = 0$ . Autrement dit  $P \in \mathcal{I}(Z)$ .

Réciproquement, soit  $P \in \mathcal{I}(Z)$  et montrons qu'il existe  $r \geq 1$  tel que  $P^r \in I$ . Comme  $k[X_1, \dots, X_n]$  est noethérien, il existe des polynômes

$$P_1, \dots, P_m \in k[X_1, \dots, X_n]$$

tels que  $I = (P_1, \dots, P_m)$ . Soit  $P \in \mathcal{I}(Z)$ . On constate que l'ensemble algébrique de  $k^{n+1}$  défini par l'idéal  $(P_1, \dots, P_m, 1 - TP)$  de  $k[X_1, \dots, X_n, T]$  est vide. D'après le théorème 3.1.13, cet idéal est égal à  $k[X_1, \dots, X_n, T]$ , si bien qu'il existe des polynômes  $Q_j \in k[X_1, \dots, X_n, T]$  pour  $0 \leq j \leq m$  tels que

$$\sum_{j=1}^m P_j Q_j + (1 - TP)Q_0 = 1.$$

Posons  $T = 1/P$  dans cette égalité, on en déduit une égalité de fractions rationnelles

$$\sum_{j=1}^m P_j(X_1, \dots, X_m) Q_j(X_1, \dots, X_m, 1/P) = 1.$$

Soit  $r \geq 1$  un entier tel que pour tout  $j$ ,  $r$  est plus grand que le degré en  $T$  de  $Q_j$ . Alors,  $P^r Q_j(X_1, \dots, X_m, 1/P)$  appartient à  $k[X_1, \dots, X_n]$ , si bien que l'on a

$$P^r = \sum_{j=1}^m P_j(X_1, \dots, X_m) P^r Q_j(X_1, \dots, X_m, 1/P)$$

et donc  $P^r \in I$ . □

*Exercice 3.1.15.* — Dans l'exercice 3.1.10, vérifier que  $I_3$  est bien égal aux radicaux de  $I_1$  et  $I_2$ .

*Exercice 3.1.16.* — Donner des exemples montrant que les corollaires 3.1.12, 3.1.13 et 3.1.14 sont mis en défaut si  $k$  n'est pas algébriquement clos.

**DÉFINITION 3.1.17.** — Si  $Z$  est un ensemble algébrique, on note  $\mathcal{A}(Z)$  l'anneau quotient  $k[X_1, \dots, X_n]/\mathcal{I}(Z)$ . Il est réduit.

*Exercice 3.1.18.* — (On suppose que  $k$  est algébriquement clos.) Soit  $Z \subset \mathbf{A}^n$  un ensemble algébrique. Montrer l'équivalence des propriétés suivantes :

1.  $Z$  est fini ;
2.  $\mathcal{A}(Z)$  est un  $k$ -espace vectoriel de dimension finie ;
3. tout idéal premier de  $\mathcal{A}(Z)$  est maximal.

(Utiliser les différentes caractérisations des anneaux artiniens fournies par le théorème d'Akizuki.)

*Désormais, et sauf mention explicite du contraire,  $k$  est un corps algébriquement clos.*

### 3.2. Topologie de Zariski

On peut reformuler la proposition 3.1.9 de la façon suivante :

**DÉFINITION 3.2.1.** — Les ensembles algébriques de  $\mathbf{A}^n$  sont les fermés d'une topologie sur  $\mathbf{A}^n$ , dite topologie de Zariski. Toute partie de  $\mathbf{A}^n$  sera munie de la topologie induite. En particulier, si  $Z$  est un ensemble algébrique, les fermés de  $Z$  sont les ensembles algébriques contenus dans  $Z$ .

Le théorème des zéros de Hilbert se reformule en :

Oscar ZARISKI (1899–1986)

*Zariski est l'un des premiers mathématiciens à avoir développé la géométrie algébrique à l'aide de méthodes algébriques. Il est notamment connu pour avoir étudié la « résolution des singularités » des surfaces. Son livre Commutative algebra, écrit en collaboration avec P. Samuel est devenu un grand classique.*



PROPOSITION 3.2.2. — Soit  $Z$  un ensemble algébrique. L'application  $X \mapsto \mathcal{I}(X)$  induit une bijection entre fermés de  $Z$  et idéaux de  $\mathcal{A}(Z)$  égaux à leur radical ; par cette bijection, les points de  $Z$  correspondent aux idéaux maximaux de  $\mathcal{A}(Z)$ .

Exercice 3.2.3. — Soit  $X$  un espace topologique compact et notons  $\mathcal{C}$  l'anneau des fonctions continues  $X \rightarrow \mathbf{R}$ . Montrer que les idéaux maximaux de  $\mathcal{C}$  sont de la forme  $\{f; f(x) = 0\}$  pour un unique  $x \in X$ . (Question subsidiaire : le résultat reste-t-il vrai si  $X$  n'est plus supposé compact ?)

PROPOSITION 3.2.4. — Si  $Z$  est une partie de  $\mathbf{A}^n$ ,  $\mathcal{V}(\mathcal{I}(Z))$  est l'adhérence de  $Z$  dans  $\mathbf{A}^n$  pour la topologie de Zariski.

Démonstration. — Si  $I$  est un idéal de  $k[X_1, \dots, X_n]$ , on a  $Z \subset \mathcal{V}(I)$  si et seulement si pour tout  $P \in I$  et tout  $x \in Z$ ,  $P(x) = 0$ , autrement dit, si et seulement si pour tout  $P \in I$ ,  $P \in \mathcal{I}(Z)$ , c'est-à-dire  $I \subset \mathcal{I}(Z)$ . La proposition en résulte.  $\square$

PROPOSITION 3.2.5. — Toute intersection décroissante de fermés de  $\mathbf{A}^n$  est stationnaire. (On dit que  $\mathbf{A}^n$  est un espace noethérien.)

Démonstration. — Cela revient à dire que toute réunion croissante d'idéaux (radiciels) de  $k[X_1, \dots, X_n]$  est stationnaire, ce qui est vrai puisque  $k[X_1, \dots, X_n]$  est noethérien.  $\square$

Remarquons que par l'évaluation des polynômes, tout élément de  $\mathcal{A}(Z)$  définit une fonction  $Z \rightarrow k$ .

DÉFINITION 3.2.6. — Si  $Z$  est un ensemble algébrique, on appelle ouvert affine de  $Z$  tout ouvert de la forme  $D(f) = \{x \in Z; f(x) \neq 0\}$ .

C'est l'ouvert complémentaire dans  $Z$  du fermé  $\mathcal{V}(f) \cap Z$ .

PROPOSITION 3.2.7. — Soit  $Z$  un ensemble algébrique de  $\mathbf{A}^n$ .

1. Tout ouvert de  $Z$  est réunion finie d'ouverts affines de  $Z$ .

2. On peut extraire de tout recouvrement ouvert de  $Z$  un sous-recouvrement fini.

En d'autres termes, la topologie de Zariski d'un ensemble algébrique est *quasi-compacte* et les ouverts affines en forment une base d'ouvert.

*Démonstration.* — Soit  $U$  un ouvert de  $Z$ ,  $F$  son fermé complémentaire dont on note  $I \subset \mathcal{A}(Z)$  l'idéal. Soit  $(f_i)$  une famille de générateurs de l'idéal  $I$ . Alors,  $x \in U$  si et seulement s'il existe  $i$  tel que  $f_i(x) \neq 0$ , c'est-à-dire  $U = \bigcap_i D(f_i)$ .

Pour la seconde partie, il suffit de prouver que l'on peut extraire un recouvrement fini de  $Z$  d'un recouvrement ouvert par des ouverts affines. Soit  $Z = \bigcup_i D(f_i)$  un tel recouvrement. Alors, l'idéal engendré par les  $f_i$  dans  $\mathcal{A}(Z)$  n'est contenu dans aucun idéal maximal de  $\mathcal{A}(Z)$  : un tel idéal maximal correspond à un point  $x \in Z$  tel que pour tout  $i$ ,  $f_i(x) = 0$  ce qui contredit le fait que les  $D(f_i)$  recouvrent  $Z$ . Cet idéal est donc égal à  $\mathcal{A}(Z)$  et il existe une combinaison linéaire  $\sum_i a_i f_i = 1$ . La somme précédente est bien sûr finie et la réunion des  $D(f_i)$  pour lesquels  $a_i \neq 0$  est égale à  $Z$ .  $\square$

*Exercice 3.2.8.* — Soit  $Z$  un ensemble algébrique de  $\mathbf{A}^n$ . Montrer que l'application qui associe à un idempotent  $e \in \mathcal{A}(Z)$  (c'est-à-dire vérifiant  $e^2 = e$ ) le fermé  $\mathcal{V}(e)$  définit une bijection sur l'ensemble des parties de  $Z$  à la fois ouvertes et fermées.

En particulier,  $Z$  est connexe si et seulement si  $\mathcal{A}(Z)$  n'a pas d'autre idempotents que 0 et 1.

**DÉFINITION 3.2.9.** — On dit qu'une partie non vide  $Z \subset \mathbf{A}^n$  est irréductible si pour tous fermés  $Z_1$  et  $Z_2$  de  $\mathbf{A}^n$  tels que  $Z \subset Z_1 \cup Z_2$ , on a  $Z \subset Z_1$  ou  $Z \subset Z_2$ .

**LEMME 3.2.10.** — Une partie non vide  $Z$  est irréductible si et seulement si elle n'est pas réunion de deux fermés (pour la topologie induite) strictement contenus dans  $Z$ .

Si  $Z$  est irréductible, tout ouvert non vide de  $Z$  est dense dans  $Z$ .

*Démonstration.* — La première partie du lemme est une reformulation de la définition puisqu'un fermé de  $Z$  est de la forme  $Z \cap Z_1$  pour un ensemble algébrique  $Z_1 \subset \mathbf{A}^n$ .

L'autre assertion en résulte : par passage aux complémentaires, on voit que l'intersection de deux ouverts non vides d'une partie irréductible est non vide. Par suite, tout ouvert non vide d'une partie irréductible est dense.  $\square$

**PROPOSITION 3.2.11.** — Un ensemble algébrique  $Z$  est irréductible si et seulement si son idéal  $\mathcal{I}(Z)$  est un idéal premier de  $k[X_1, \dots, X_n]$ .

Remarquons que cela revient à dire que  $\mathcal{A}(Z)$  est intègre.

*Démonstration.* — Supposons que  $Z$  est irréductible et soient  $f, g \in k[X_1, \dots, X_n]$  tels que  $fg \in \mathcal{I}(Z)$ . On a ainsi

$$Z \subset \mathcal{V}(fg) = \mathcal{V}(f) \cup \mathcal{V}(g).$$

Quitte à échanger  $f$  et  $g$ , on peut ainsi supposer que  $Z \subset \mathcal{V}(f)$ . Autrement dit,  $f \in \mathcal{I}(Z)$ , et  $\mathcal{I}(Z)$  est un idéal premier.

Réciproquement, supposons que  $\mathcal{I}(Z)$  est un idéal premier. Si  $Z = Z_1 \cup Z_2$ , on a  $\mathcal{I}(Z) = \mathcal{I}(Z_1) \cap \mathcal{I}(Z_2)$ . D'après le lemme d'évitement des idéaux premiers 1.1.1, on a  $\mathcal{I}(Z_1) = \mathcal{I}(Z)$  ou  $\mathcal{I}(Z_2) = \mathcal{I}(Z)$ . Ainsi,  $Z = Z_1$  ou  $Z = Z_2$ .  $\square$

*Exercice 3.2.12* (Fermés de la droite affine). — Montrer que les fermés de  $\mathbf{A}^1$  sont les parties finies de  $\mathbf{A}^1$  ainsi que  $\mathbf{A}^1$ . En particulier,  $\mathbf{A}^1$  est irréductible. Remarquer aussi que tout ouvert non vide est dense et que la topologie de Zariski sur  $\mathbf{A}^1$  n'est pas séparée.

Montrer enfin que la topologie de Zariski sur  $\mathbf{A}^2 = \mathbf{A}^1 \times \mathbf{A}^1$  est strictement plus fine que la topologie produit.

*Exercice 3.2.13*. — Traduire géométriquement le lemme d'évitement 1.1.2.

PROPOSITION 3.2.14. — *Tout ensemble algébrique non vide  $Z$  de  $\mathbf{A}^n$  s'écrit de manière unique comme la réunion d'un nombre fini de parties irréductibles  $Z = Z_1 \cup \dots \cup Z_m$  telles que  $Z_i \not\subset Z_j$  pour  $i \neq j$ .*

*Démonstration*. — Transcrite en termes d'idéaux, c'est un cas particulier de la décomposition primaire qui implique qu'un anneau noethérien réduit n'a qu'un nombre fini d'idéaux premiers minimaux dont l'intersection est réduite à  $(0)$ , voir la proposition 1.3.2.

On peut aussi le démontrer en n'utilisant que le fait (proposition 3.2.5) que  $Z$  est un espace noethérien. L'argument est de toutes façons analogue à celui fait dans la proposition 1.3.2.

Montrons maintenant que tout fermé est réunion finie de fermés irréductibles. Pour obtenir la proposition, il suffira de considérer une expression de  $Z$  comme réunion finie de fermés irréductibles et de n'en retenir que les parties maximales.

Considérons donc l'ensemble  $\mathcal{C}$  des parties fermées de  $Z$  qui ne sont pas réunion finie de parties irréductibles. Si par l'absurde  $\mathcal{C}$  est non vide, le fait que  $Z$  est un espace noethérien implique qu'il admet un élément minimal  $W$  qui n'est pas réunion finie de parties irréductibles. On peut ainsi écrire  $W = W_1 \cup W_2$  pour deux fermés  $W_1$  et  $W_2$  strictement contenus dans  $W$ . Comme  $W$  est choisi minimal,  $W_1$  et  $W_2$  n'appartiennent pas à  $\mathcal{C}$  et sont réunion finie de parties irréductibles. Par suite,  $W$  est réunion finie de parties irréductibles et la contradiction est visible !  $\square$

DÉFINITION 3.2.15. — *Par définition, les  $Z_i$  sont les composantes irréductibles de  $Z$ .*

(Ce sont les fermés irréductibles maximaux contenus dans  $Z$ .)

### 3.3. Variétés algébriques affines

DÉFINITION 3.3.1. — On appelle ensemble quasi-algébrique tout ouvert d'un ensemble algébrique.

DÉFINITION 3.3.2. — Soit  $Z \subset \mathbf{A}^n$  un ensemble quasi-algébrique. On dit qu'une fonction  $f : Z \rightarrow k$  est régulière en un point  $x \in Z$  s'il existe un voisinage ouvert  $U$  de  $x$  dans  $Z$  et deux polynômes  $g, h \in k[X_1, \dots, X_n]$  tels que si  $z \in U$ ,  $h(z) \neq 0$  et  $f(z) = g(z)/h(z)$ .

Une fonction  $f : Z \rightarrow k$  est dite régulière si elle est régulière en tout point de  $Z$ .

Remarque 3.3.3. — Si  $f$  est régulière en  $x \in Z$ , alors  $f$  est régulière dans un voisinage de  $x$  dans  $Z$ .

LEMME 3.3.4. — L'ensemble des fonctions régulières sur  $Z$  est une  $k$ -algèbre notée  $\mathcal{O}(Z)$ . Les éléments inversibles de  $\mathcal{O}(Z)$  sont les fonctions régulières qui ne s'annulent pas.

Démonstration. — Laisée en exercice. □

DÉFINITION 3.3.5. — Soit  $Z$  un ensemble quasi-algébrique. Le faisceau des fonctions régulières  $\mathcal{O}_Z$  sur  $Z$  est le faisceau en  $k$ -algèbres dont l'ensemble des sections sur un ouvert  $U \subset Z$  est l'anneau  $\mathcal{O}(U)$ .

Soit  $Z \subset \mathbf{A}^n$  un ensemble quasi-algébrique  $Z \subset \mathbf{A}^n$ ; la fonction  $f : Z \rightarrow k$  induite par un polynôme de  $k[X_1, \dots, X_n]$  est manifestement régulière, d'où un homomorphisme de  $k$ -algèbres  $k[X_1, \dots, X_n] \rightarrow \mathcal{O}(Z)$  dont le noyau est par définition  $\mathcal{I}(Z)$ . Il en résulte un homomorphisme injectif

$$(3.3.6) \quad \alpha : \mathcal{A}(Z) = k[X_1, \dots, X_n] / \mathcal{I}(Z) \hookrightarrow \mathcal{O}(Z).$$

THÉORÈME 3.3.7. — Si  $Z$  est un ensemble algébrique, l'homomorphisme  $\alpha$  est un isomorphisme.

Démonstration. — Soit  $\varphi \in \mathcal{O}(Z)$ . Il existe un recouvrement ouvert fini  $(U_i)$  de  $Z$  tel que sur  $U_i$ ,  $\varphi$  s'écrit  $\varphi_i = g_i/h_i$  pour deux polynômes  $g_i$  et  $h_i$ ,  $h_i$  ne s'annulant pas sur  $U_i$ . On peut supposer que le recouvrement est fini et que  $U_i$  est de la forme  $D(f_i)$ .

Comme  $h_i$  ne s'annule pas sur  $D(f_i)$ , on a  $\mathcal{V}(h_i) \subset \mathcal{V}(f_i)$ . Par le théorème des zéros de Hilbert 3.1.14,  $\sqrt{(f_i)} \subset \sqrt{(h_i)} \subset \mathcal{A}(Z)$ . Il en résulte qu'il existe  $n_i \geq 1$  tel que  $f_i^{n_i} \in (h_i)$ . On peut ainsi supposer que  $h_i = f_i^{n_i}$ . En remplaçant  $f_i$  par  $f_i^{n_i}$ , on peut même supposer  $n_i = 1$ .

Écrivons alors que  $\varphi_i$  et  $\varphi_j$  coïncident sur  $U_i \cap U_j = D(f_i f_j)$  : pour tout  $x \in Z$ , ou bien  $f_i(x) = 0$ , ou bien  $f_j(x) = 0$ , ou bien  $f_i(x)g_j(x) = f_j(x)g_i(x)$ , si bien que

$$(f_i f_j)(f_i g_j - f_j g_i) = 0 \in \mathcal{A}(Z).$$

La réunion des  $D(f_i) = D(f_i^2)$  est égale à  $Z$ , autrement dit, l'idéal engendré par les  $f_i^2$  contient 1. Écrivons donc  $1 = \sum_j f_j^2 k_j$  pour des  $k_j \in \mathcal{A}(Z)$  et posons  $\tilde{\varphi} = \sum_j f_j g_j k_j \in \mathcal{A}(Z)$ . Alors, si  $x \in D(f_i)$ ,

$$\begin{aligned} f_i^2(x)\tilde{\varphi}(x) &= \sum_j f_j f_i^2 g_j k_j = \sum_j f_i f_j^2 g_j k_j \\ &= f_i g_i \sum_j k_j f_j^2 = f_i g_i \end{aligned}$$

et donc

$$f_i^2(\tilde{\varphi}(x) - \varphi(x)) = f_i g_i - f_i g_i = 0.$$

Finalement, pour tout  $x \in Z$ , il existe  $i$  tel que  $f_i(x) \neq 0$  et donc  $\varphi(x) = \tilde{\varphi}(x)$ . On a ainsi  $\varphi = \tilde{\varphi}$ , ce qui prouve que  $\alpha$  est surjectif.  $\square$

**DÉFINITION 3.3.8.** — *On appelle variété algébrique affine tout espace annelé isomorphe à  $(Z, \mathcal{O}_Z)$  pour un ensemble algébrique  $Z$ . Une variété algébrique quasi-affine est un ouvert d'une variété algébrique affine.*

*Si  $X$  et  $Y$  sont deux variétés algébriques quasi-affines, un morphisme de variétés algébriques quasi-affines est un morphisme d'espaces annelés. On note  $\text{Hom}(X, Y)$  l'ensemble des morphismes de  $X$  dans  $Y$ .*

*On dit qu'un morphisme  $f : X \rightarrow Y$  est un isomorphisme s'il existe un morphisme  $g : Y \rightarrow X$  tel que  $f \circ g = \text{id}_Y$  et  $g \circ f = \text{id}_X$ .*

Explicitons ce que signifie pour une application  $f : X \rightarrow Y$  d'être un morphisme de variétés : d'après la définition d'un morphisme d'espaces annelés,  $f$  est continue et pour tout ouvert  $V \subset Y$  et toute fonction régulière  $\varphi$  sur  $V$ ,  $\varphi \circ f$  est une fonction régulière sur l'ouvert  $f^{-1}(V) \subset X$ .

**THÉORÈME 3.3.9.** — *Soient  $X \subset \mathbf{A}^n$  et  $Y \subset \mathbf{A}^m$  deux variétés algébriques quasi-affines. Une application  $f : X \rightarrow Y$  est un morphisme de variétés algébriques quasi-affines si et seulement si les composantes  $(f_1, \dots, f_m)$  de  $f$  sont des fonctions régulières sur  $X$ .*

*Démonstration.* — Comme les polynômes  $X_1, \dots, X_m$  définissent des fonctions régulières  $x_1, \dots, x_m$  sur  $Y$  telles que  $x_i \circ f = f_i$ , cette condition est nécessaire.

Réciproquement, supposons que les composantes  $(f_1, \dots, f_m)$  de  $f$  sont des fonctions régulières sur  $X$ . Soit alors  $V$  un ouvert de  $Y$  et  $\varphi$  une fonction régulière sur  $V$ . On veut prouver que  $f^{-1}(V)$  est un ouvert de  $X$  sur lequel  $\varphi \circ f$  est régulière. Soit  $\xi \in f^{-1}(V)$  et posons  $\eta = f(\xi)$ . Il faut donc démontrer qu'il existe un ouvert de  $\mathbf{A}^n$  contenant  $\xi$ , et deux polynômes  $g, h \in k[X_1, \dots, X_n]$ ,  $h$  ne s'annulant pas sur  $U \cap X$  tels que pour  $x \in U \cap X$ ,  $\varphi(f(x)) = g(x)/h(x)$ .

Comme  $\varphi$  est régulière en  $\eta$ , il existe  $\psi, \gamma, \theta \in k[Y_1, \dots, Y_m]$  tels que  $\psi(\eta) \neq 0$ ,  $\theta$  ne s'annule pas sur  $D(\psi) \cap Y$ , et pour tout  $y \in D(\psi) \cap Y$ ,  $\varphi(y) = \gamma(y)/\theta(y)$ . Par suite, si

$\psi(f(x)) \neq 0$ ,

$$(\varphi \circ f)(x) = \frac{\gamma \circ f(x)}{\theta \circ f(x)}.$$

Or,  $f$  est donné dans un voisinage de  $\xi$  par une famille de fractions rationnelles (dont le dénominateur ne s'annule pas dans ce voisinage). Dans ce voisinage, la condition  $\psi(f(x)) \neq 0$  est ainsi donnée par la non-nullité d'un polynôme (le numérateur de  $\psi \circ f$ ) et l'on voit que  $\varphi \circ f$  est une application régulière dans un voisinage de  $\xi$ .  $\square$

**THÉORÈME 3.3.10.** — *Soient  $X$  une variété quasi-affine et  $Y$  une variété affine. L'application*

$$\text{Hom}(X, Y) \longrightarrow \text{Hom}(\mathcal{O}(Y), \mathcal{O}(X)), \quad f \mapsto f^* = \cdot \circ f$$

*est une bijection*

*Démonstration.* — Supposons  $X \subset \mathbf{A}^n, Y \subset \mathbf{A}^m$ .

Montrons que cette application est injective. Soient  $f : X \rightarrow Y$  et  $g : X \rightarrow Y$  deux morphismes tels que  $f^* = g^*$ . On a ainsi  $f^*(y_i) = g^*(y_i)$  pour tout  $i \in \{1, \dots, m\}$ , donc  $f_i = g_i$  et ainsi  $f = g$ .

Réciproquement, montrons qu'elle est surjective. Soit  $\varphi : \mathcal{O}(Y) \rightarrow \mathcal{O}(X)$  un homomorphisme de  $k$ -algèbres. Posons  $f_i = \varphi(y_i)$  et  $f = (f_1, \dots, f_m)$ . Chaque  $f_i$  est par définition une application régulière sur  $X$ , d'où un morphisme de variétés quasi-affines  $f : X \rightarrow \mathbf{A}^m$ .

Il reste à prouver que  $f(X) \subset Y$  et que  $f^* = \varphi$ . Soit  $P \in k[Y_1, \dots, Y_m], P = \sum c_a \prod y_i^{a_i}$ . Alors,

$$f^*(P) = P \circ f = \sum c_a \prod f_i^{a_i} = \sum c_a \prod \varphi(y_i)^{a_i} = \varphi(\sum c_a \prod y_i^{a_i}) = \varphi(P|_Y).$$

Ainsi, si  $P \in \mathcal{I}(Y), f^*(P) = 0$ , ce qui implique  $f(X) \subset Y$ . Il vient alors  $f^* = \varphi$ .  $\square$

**COROLLAIRE 3.3.11.** — *Deux variétés algébriques affines sont isomorphes si et seulement si leurs anneaux de fonctions régulières sont isomorphes. Plus précisément,  $X \mapsto \mathcal{A}(X)$  définit une équivalence de catégories entre la catégories des variétés algébriques affines et la catégorie des  $k$ -algèbres de type fini réduites.*

*Exercice 3.3.12.* — Soit  $X$  une variété algébrique affine et  $f \in \mathcal{A}(X)$ . Montrer que  $D(f) = \{x \in X; f(x) \neq 0\}$  est isomorphe à une variété algébrique affine et que  $\Gamma(D(f), \mathcal{O}_X) = \mathcal{A}(X)[1/f]$ .

*Exercice 3.3.13.* — Montrer que  $U = \mathbf{A}^2 \setminus \{(0, 0)\}$  n'est pas isomorphe à une variété algébrique affine. (Calculer  $\mathcal{O}(U)$ .)

*Exercice 3.3.14.* — Soit  $f : \mathbf{A}^1 \rightarrow \mathbf{A}^2$  donné par  $f(t) = (t^2, t^3)$ . Montrer que  $f$  est un morphisme injectif dont l'image est une variété algébrique affine  $C \subset \mathbf{A}^2$ . Déterminer l'idéal de  $C$ ; en déduire le morphisme  $f^* : \mathcal{A}(C) \rightarrow \mathcal{A}(\mathbf{A}^1)$ . Est-ce que  $f$  est un isomorphisme? Les variétés algébriques  $\mathbf{A}^1$  et  $C$  sont-elles isomorphes?

*Remarque 3.3.15.* — Le fait que le foncteur qui associe à une variété algébrique affine son anneau de fonctions régulières soit essentiellement surjectif signifie qu'il existe pour toute  $k$ -algèbre de type fini réduite  $A$  une variété algébrique  $X$  telle que  $A \simeq \mathcal{A}(X)$ . Il est remarquable que l'on puisse définir une telle variété algébrique sans faire intervenir une présentation de  $A$ . On pose en effet  $X = \text{Spm}A$  (l'ensemble des idéaux maximaux de  $A$ ). Si  $I$  est un idéal de  $A$ , on définit  $V(I)$  comme l'ensemble des  $\mathfrak{m} \in \text{Spm}A$  tels que  $I \subset \mathfrak{m}$ . Les  $V(I)$  définissent les fermés d'une topologie sur  $\text{Spm}A$  dont les  $D(f) = \text{Spm}A \setminus V((f))$  forment une base d'ouverts. Le faisceau structural est défini de sorte que  $\Gamma(D(f), \mathcal{O}_X) = A_f = A[1/f]$  : si  $a \in A$  et  $r \geq 0$ , la fonction  $a/f^r$  a pour valeur en  $\mathfrak{m} \in D(f)$  l'élément  $a/f^r \pmod{\mathfrak{m}} \in A/\mathfrak{m} = k$ .

Il reste à vérifier que  $\text{Spm}A$  est bien une variété algébrique affine. Or, écrivons  $A = k[X_1, \dots, X_n]/I$  pour un idéal radical  $I$  de  $k[X_1, \dots, X_n]$ . On définit  $f : X \rightarrow \mathbf{A}^n$  en associant à  $\mathfrak{m}$  le  $n$ -uplet  $(X_i \pmod{\mathfrak{m}})$  de  $\mathbf{A}^n$ . Le théorème des zéros de Hilbert implique que  $f$  est un homéomorphisme de  $\text{Spm}A$  sur  $\mathcal{V}(I)$  et il est alors clair que c'est un isomorphisme d'espaces annelés.

*Exercice 3.3.16.* — Soit  $k$  un corps et  $\varphi : A \rightarrow B$  un homomorphisme de  $k$ -algèbres de type fini. Montrer que pour tout idéal maximal  $\mathfrak{m} \subset B$ ,  $\varphi^{-1}(\mathfrak{m})$  est un idéal maximal de  $A$ . (Utiliser le théorème des zéros de Hilbert.)

### 3.4. Variétés algébriques

On a expliqué dans le chapitre 2 comment la géométrie différentielle étudie les espaces annelés modélés sur les ouverts de  $\mathbf{R}^n$ . En géométrie algébrique, considérer des ouverts de Zariski de l'espace affine fournirait trop peu de variétés. Ce sont ici les variétés algébriques affines qui jouent le rôle des ouverts de  $\mathbf{R}^n$ .

**DÉFINITION 3.4.1.** — *On dit qu'un espace annelé  $(X, \mathcal{O}_X)$  est une variété algébrique s'il existe un recouvrement de  $X$  par un nombre fini d'ouverts  $U_i$  tels que  $(U_i, \mathcal{O}_X|_{U_i})$  est isomorphe comme espace annelé à une variété algébrique affine.*

*Un morphisme de variétés algébriques est un morphisme en tant qu'espaces annelés.*

**DÉFINITION 3.4.2** (cf. 3.2.6). — *On dira qu'un ouvert d'une variété algébrique est un ouvert affine s'il est isomorphe à une variété algébrique affine.*

Par définition, toute variété algébrique possède un recouvrement ouvert par un nombre fini d'ouverts affines.

**DÉFINITION 3.4.3** (cf. 3.2.9 et 3.2.15). — *On dit qu'une partie non vide d'une variété algébrique est irréductible si elle n'est pas réunion de deux parties fermées pour la topologie induite strictement contenues.*

Un fermé non vide  $Z$  est irréductible si et seulement si pour tous fermés  $Z_1$  et  $Z_2$  tels que  $Z \subset Z_1 \cup Z_2$ , on a  $Z \subset Z_1$  ou  $Z \subset Z_2$ .

PROPOSITION 3.4.4. — Soit  $X$  une variété algébrique.

1. Les ouverts affines de  $X$  forment une base de la topologie de  $X$ .
2. Toute suite décroissante de fermés de  $X$  est stationnaire.
3. De tout recouvrement ouvert de  $X$ , on peut extraire un sous-recouvrement fini (la topologie de  $X$  est quasi-compacte).
4. (cf. 3.2.14) Il existe un nombre fini de fermés irréductibles maximaux (ses composantes irréductibles) dans  $X$  dont  $X$  est la réunion.

*Démonstration.* — 1) Cela signifie que tout ouvert non vide de  $X$  est réunion d'ouverts affines. Comme  $X$  est recouvert par des ouverts affines, il suffit de démontrer l'assertion lorsque  $X$  est affine. C'est alors la proposition 3.2.7.

2) Soit  $(U_i)$  un recouvrement de  $X$  par un nombre fini d'ouverts affines. L'assertion analogue a été prouvée pour les  $U_i$  (proposition 3.2.5. L'intersection avec chaque  $U_i$  d'une suite décroissante de fermés est ainsi stationnaire et comme le recouvrement est fini, la suite est elle-même stationnaire.

Les points 3) et 4) résultent directement du point précédent. Il suffit de recopier la démonstration des propositions 3.2.7 et 3.2.14.  $\square$

PROPOSITION 3.4.5. — Munie de la structure d'espace annelé induit, une partie localement fermée d'une variété algébrique est une variété algébrique.

*Démonstration.* — Soit  $X$  une variété algébrique et  $Z \subset X$  une partie localement fermée. Cela signifie que  $Z$  est un ouvert de son adhérence  $\bar{Z}$ . Ainsi, il suffit de traiter les deux cas  $Z$  ouvert et  $Z$  fermé. Mais le cas où  $Z$  est ouvert résulte de la proposition précédente, les ouverts affines formant une base des ouverts de  $X$ .

Supposons donc que  $Z$  est fermé. Soit  $(U_i)$  un recouvrement fini de  $X$  par des ouverts affines. Si l'on prouve que chaque  $(Z \cap U_i, \mathcal{O}_X|_{Z \cap U_i})$  est une variété algébrique affine, la proposition sera démontrée. Cela nous ramène au cas où  $X$  est affine. Dans ce cas,  $Z$  est défini par un idéal  $\mathcal{I}(Z)$  de  $\mathcal{A}(X)$  et est naturellement une variété algébrique. Si  $X \subset \mathbf{A}^n$ , par définition, une fonction régulière sur  $Z$  est localement la restriction d'une fonction régulière sur  $X$  (et même sur  $\mathbf{A}^n$ ). Autrement dit, les faisceaux  $\mathcal{O}_Z$  et  $(\mathcal{O}_X/\mathcal{I}_Z)|_Z$  coïncident. La proposition est ainsi prouvée.  $\square$

DÉFINITION 3.4.6. — Une sous-variété d'une variété algébrique est un fermé d'une variété algébrique muni de la structure de variété algébrique induite.

Si l'on veut construire des exemples non triviaux de variétés algébriques, la méthode de recollement est incontournable. Nous l'avons rappelée dans le contexte général des

espaces annelés dans le théorème 2.3.1 ; appliquée au cas des variétés algébriques affines, le théorème devient le suivant.

**THÉORÈME 3.4.7 (Construction de variétés par recollement)**

Soient  $(X_i)$  une famille finie de variétés algébriques affines et, pour tout couple  $(i, j)$  un ouvert  $X_{ij}$  de  $X_j$ , un isomorphisme de variétés quasi-affines,  $\varphi_{ij} : X_{ij} \rightarrow X_{ji}$ , tels que

- si  $i = j$ ,  $X_{ii} = X_i$  et  $\varphi_{ii} = \text{id}_{X_i}$  ;
- pour tous  $i$  et  $j$ ,  $\varphi_{ji} = \varphi_{ij}^{-1}$  ;
- pour tous  $i, j, k$ ,  $\varphi_{ij}(X_{ij} \cap X_{ik}) = X_{ji} \cap X_{jk}$  et on a la relation  $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$  sur l'ouvert  $X_{ij} \cap X_{ik}$  de  $X_i$ .

Alors, il existe une unique variété algébrique  $X$  munie d'un atlas  $(\varphi_i : U_i \xrightarrow{\sim} X_i)$  tel que pour tous  $i$  et  $j$ ,  $X_{ij} = \varphi_i(U_i \cap U_j)$  et  $\varphi_{ij} = \varphi_j \circ \varphi_i^{-1}$ .

Finalement, les morphismes d'une variété algébrique dans une variété affine sont donnés par le théorème suivant, qui étend le théorème 3.3.10.

**THÉORÈME 3.4.8.** — Soit  $X$  une variété algébrique et  $Y$  une variété affine. L'application

$$\text{Hom}(X, Y) \rightarrow \text{Hom}(\mathcal{A}(Y), \mathcal{O}(X)), \quad \varphi \mapsto \varphi^*$$

est une bijection.

*Démonstration.* — Notons  $\theta$  cette application. Si  $X$  est réunion d'ouverts affines  $U_i$ , on a pour tout  $i$  une bijection  $\theta_i : \text{Hom}(U_i, Y) \rightarrow \text{Hom}(\mathcal{A}(Y), \mathcal{A}(U_i))$  en vertu du théorème 3.3.10. De plus, pour toute  $f \in \mathcal{A}(Y)$ ,  $\theta_i(f) = \theta(f)|_{U_i}$ .

Montrons que l'application  $\theta$  est injective : si  $\theta(\varphi) = \theta(\varphi')$ , cela signifie que pour toute fonction régulière  $f \in \mathcal{A}(Y)$ ,  $f \circ \varphi = f \circ \varphi'$ . En particulier,  $f \circ \varphi|_{U_i} = f \circ \varphi'|_{U_i}$ , d'où  $\theta_i(\varphi) = \theta_i(\varphi')$  et  $\varphi|_{U_i} = \varphi'|_{U_i}$ . Comme les  $U_i$  recouvrent  $X$ ,  $\varphi = \varphi'$ .

Montrons maintenant que  $\theta$  est surjective. Soit  $\psi$  un homomorphisme  $\mathcal{A}(Y) \rightarrow \mathcal{O}(X)$ . On en déduit des homomorphismes  $\psi_i : \mathcal{A}(Y) \rightarrow \mathcal{O}(U_i)$  qui sont donc de la forme  $\theta_i(\varphi_i)$  pour un unique morphisme  $\varphi_i : U_i \rightarrow Y$ . Sur  $U_i \cap U_j$ , l'homomorphisme  $\psi_{ij} : \mathcal{A}(Y) \rightarrow \mathcal{O}(U_i \cap U_j)$  s'écrit  $\theta_{ij}(\varphi_i) = \theta_{ij}(\varphi_j)$ , si bien que  $\varphi_i$  et  $\varphi_j$  coïncident sur  $U_i \cap U_j$ . Par recollement, on en déduit un morphisme  $\varphi : X \rightarrow Y$  tel que  $\varphi|_{U_i} = \varphi_i$ . Il faut prouver que  $\theta(\varphi) = \psi$ . Or, si  $f \in \mathcal{A}(Y)$ ,

$$\theta(\varphi)(f)|_{U_i} = f \circ \varphi|_{U_i} = f \circ \varphi_i = \theta_i(\varphi_i)(f) = \psi(f)|_{U_i}$$

et comme les  $U_i$  recouvrent  $X$ ,  $\theta(\varphi)(f) = \psi(f)$ . Comme c'est vrai pour tout  $f$ ,  $\theta(\varphi) = \psi$  et  $\theta$  est surjective.  $\square$

### 3.5. Localisation

DÉFINITION 3.5.1. — Soit  $X$  une variété algébrique. Si  $x \in X$ , on appelle anneau local de  $X$  en  $x$  la  $k$ -algèbre

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

lorsque  $U$  parcourt les voisinages de  $x$  dans  $X$ .

Il convient d'expliciter cette définition : on considère les couples  $(U, f)$  formés d'un voisinage  $U$  de  $x$  et d'une fonction régulière  $f$  sur  $U$ . On les munit de la relation d'équivalence selon laquelle  $(U, f) \sim (V, g)$  si  $f = g$  sur un voisinage de  $x$  contenu dans  $U \cap V$ . L'ensemble quotient est naturellement muni d'une structure de  $k$ -algèbre et s'interprète comme l'ensemble des fonctions régulières sur un voisinage de  $x$  dans  $X$ . Une telle fonction sur un voisinage non précisé est appelé *germe* de fonction régulière en  $x$ . Autrement dit,  $\mathcal{O}_{X,x}$  est la  $k$ -algèbre des germes de fonctions régulières en  $x$ .

PROPOSITION 3.5.2. — Soient  $X$  une variété algébrique,  $x$  un point de  $X$  et  $U \subset X$  un ouvert affine contenant  $x$ . Soit  $\mathfrak{m}_x$  l'idéal maximal de  $\mathcal{A}(U)$  correspondant au point  $x$ . Alors, la  $k$ -algèbre  $\mathcal{O}_{X,x}$  est canoniquement isomorphe à l'anneau localisé  $\mathcal{A}(U)_{\mathfrak{m}_x}$ . C'est ainsi un anneau local dont l'idéal maximal est l'idéal des germes de fonctions régulières qui s'annulent en  $x$ .

*Démonstration.* — On a une application naturelle  $\varphi : \mathcal{A}(U) \rightarrow \mathcal{O}_{X,x}$  ; par cette application, un élément  $f \notin \mathfrak{m}_x$  a pour image un élément inversible de  $\mathcal{O}_{X,x}$  puisque la fonction  $1/f$  est alors définie sur le voisinage  $U \cap D(f)$  de  $x$ . Il en résulte un homomorphisme  $\mathcal{A}(U)_{\mathfrak{m}_x} \rightarrow \mathcal{O}_{X,x}$ .

Cet homomorphisme est injectif : si  $f/g$  a pour image 0, cela signifie que la fonction  $f/g$  est nulle dans un voisinage de  $x$ , donc  $f = 0$  dans un voisinage ouvert  $V \subset U$  de  $x$ . Soit  $Z = U \setminus V$  le fermé complémentaire. D'après le lemme d'évitement 1.1.2, il existe  $h \in \mathcal{I}(Z) \subset \mathcal{A}(U)$  tel que  $h(x) \neq 0$ . Alors,  $fh = 0$  mais  $h \notin \mathfrak{m}_x$  ce qui implique  $f/1 = 0$  dans  $\mathcal{A}(U)_{\mathfrak{m}_x}$ .

Cet homomorphisme est surjectif : un élément de  $\mathcal{O}_{X,x}$  est la classe d'un couple  $(V, f)$  pour un voisinage  $V$  de  $x$  et une fonction régulière  $f$  sur  $V$ . Quitte à restreindre  $V$ , on peut supposer que  $f = g/h$  pour deux polynômes  $g$  et  $h$  avec  $h$  ne s'annulant pas sur  $V$ . Comme  $h(x) \neq 0$ , on voit que  $(V, f)$  est l'image de l'élément noté  $g/h$  dans  $\mathcal{A}(U)_{\mathfrak{m}_x}$ .

Comme  $\mathcal{A}(U)_{\mathfrak{m}_x}$  est un anneau local,  $\mathcal{O}_{X,x}$  aussi. □

Par construction, l'anneau  $\mathcal{O}_{X,x}$  « voit » ce qui se passe dans un voisinage de  $x \in X$ . Par exemple :

PROPOSITION 3.5.3. — Le point  $x$  appartient à une seule composante irréductible de  $X$  si et seulement si l'anneau local  $\mathcal{O}_{X,x}$  est intègre.

En général, c'est un anneau réduct dont les idéaux premiers minimaux s'identifient aux composantes irréductibles de  $X$  qui passent par  $x$ .

*Démonstration.* — Soit  $U$  un voisinage affine de  $x$ . Comme l'anneau  $\mathcal{A}(U)$  est réduct, ses localisés aussi et  $\mathcal{O}_{X,x}$  aussi.

Les idéaux premiers de  $\mathcal{A}(U)_{\mathfrak{m}_x}$  correspondent aux idéaux premiers de  $\mathcal{A}(U)$  contenus dans  $\mathfrak{m}_x$ . Alors, les idéaux premiers minimaux de  $\mathcal{A}(U)$  correspondent aux idéaux premiers minimaux de  $\mathcal{A}(U)$  contenus dans  $\mathfrak{m}_x$ , c'est-à-dire aux composantes irréductibles de  $U$  qui contiennent  $x$ . Comme ces dernières ont pour adhérence les composantes irréductibles de  $X$  qui contiennent  $x$  et que réciproquement, l'intersection avec  $U$  d'une composante irréductible de  $X$  est ou vide, ou une composante irréductible, la deuxième partie de la proposition est prouvée.

La première partie en résulte, compte-tenu du lemme 1.3.1 selon lequel un anneau réduct n'ayant qu'un seul idéal premier minimal est intègre.  $\square$

DÉFINITION 3.5.4. — Soit  $X$  une variété algébrique irréductible. On appelle corps des fonctions de  $X$  la  $k$ -algèbre

$$k(X) = \varinjlim_{U \neq \emptyset} \mathcal{O}_X(U)$$

lorsque  $U$  parcourt les ouverts non vides de  $X$ .

PROPOSITION 3.5.5. — Soit  $X$  une variété algébrique irréductible. Le corps des fonctions de  $X$  est un corps ; pour tout ouvert affine non vide  $U \subset X$ , il s'identifie canoniquement au corps des fractions de l'algèbre intègre  $\mathcal{A}(U)$ .

*Démonstration.* — Comme  $k(X)$  est une limite inductive de  $k$ -algèbres, c'est une  $k$ -algèbre. C'est aussi un corps : si  $f$  est une fonction régulière sur un ouvert  $U$  non vide de  $X$  et si  $f \neq 0$ , la fonction  $1/f$  est régulière sur l'ouvert non vide  $U \setminus \mathcal{V}(f)$ .

Soit  $U$  un ouvert affine non vide de  $X$  ; par définition de la limite inductive, on peut ne prendre la limite que sur les ouverts affines contenus dans  $U$ . Autrement dit, l'homomorphisme naturel  $k(X) \rightarrow k(U)$  est un isomorphisme.

Il reste à prouver que si  $X$  est affine,  $k(X) = \text{Frac } \mathcal{A}(X)$ . L'homomorphisme injectif naturel  $\mathcal{A}(X) \rightarrow k(X)$  induit une injection  $\text{Frac } \mathcal{A}(X) \hookrightarrow k(X)$  puisque  $k(X)$  est un corps. Réciproquement, si  $f \in k(X)$ , il existe un ouvert  $U \subset X$  tel que  $f$  est une fonction régulière sur  $U$ . Quitte à restreindre  $U$ , on peut supposer que  $U = D(\varphi)$  pour une fonction non nulle  $\varphi \in \mathcal{A}(X)$ . D'après l'exercice 3.3.12,  $\mathcal{O}_X(D(\varphi)) = \mathcal{A}(X)[1/\varphi]$  ce qui prouve que  $f$  est de la forme  $g/\varphi^n$  pour une fonction  $g \in \mathcal{A}(X)$  et  $n \geq 1$ . Cela implique visiblement  $f \in \text{Frac } \mathcal{A}(X)$ .  $\square$

Remarque 3.5.6. — En géométrie différentielle ou en géométrie analytique complexe, une telle proposition serait totalement fautive : une fonction holomorphe sur  $\mathbf{C} \setminus \{0\}$

ne s'écrit pas forcément comme le quotient de deux fonctions holomorphes sur  $\mathbf{C}$ , par exemple  $z \mapsto e^{1/z}$ .

Elle permet aussi de vérifier le bien fondé d'avoir défini les variétés algébriques comme localement isomorphes à une variété affine, et non un simple ouvert de  $\mathbf{A}^n$ . En effet, si  $X$  est une variété algébrique irréductible contenant un ouvert isomorphe à un ouvert non vide de  $\mathbf{A}^n$ , on aura  $k(X) \simeq k(X_1, \dots, X_n)$ . Une telle variété est dite *rationnelle*.

La proposition suivante interviendra dans la démonstration du théorème 5.4.11.

**PROPOSITION 3.5.7.** — *Soient  $X$  et  $Y$  deux variétés algébriques irréductibles. Si leurs corps de fonctions  $k(X)$  et  $k(Y)$  sont isomorphes, il existe des ouverts non vides  $U \subset X$  et  $V \subset Y$  tels que  $U \simeq V$ .*

*Démonstration.* — On peut supposer que  $X$  et  $Y$  sont affines et que  $\mathcal{A}(X)$  et  $\mathcal{A}(Y)$  sont deux sous- $k$ -algèbres de type fini de  $K = k(X)$ . Comme  $K = \text{Frac } \mathcal{A}(Y)$  et  $\mathcal{A}(X)$  est de type fini, il existe  $f \in K$ ,  $f \neq 0$  tel que  $\mathcal{A}(X) \subset \mathcal{A}(Y)[1/f]$ . De même, il existe  $g \in K$ ,  $g \neq 0$  tel que  $\mathcal{A}(Y) \subset \mathcal{A}(X)[1/g]$ . On a alors

$$\mathcal{A}(X)[1/fg] \subset \mathcal{A}(Y)[1/fg] \subset \mathcal{A}(X)[1/fg],$$

autrement dit,  $\mathcal{A}(X)[1/fg] = \mathcal{A}(Y)[1/fg]$ .

Soit  $a \in \mathcal{A}(X)$  tel que  $\mathcal{A}(X)[1/fg] = \mathcal{A}(X)[1/a]$  (le numérateur de  $fg$  convient). De même, choisissons  $b \in \mathcal{A}(Y)$  tel que  $\mathcal{A}(Y)[1/fg] = \mathcal{A}(Y)[1/b]$ . D'après l'exercice 3.3.12, on a  $\mathcal{A}(D(a)) = \mathcal{A}(X)[1/a]$  et  $\mathcal{A}(D(b)) = \mathcal{A}(Y)[1/b]$  ce qui implique que  $D(a) \subset X$  et  $D(b) \subset Y$  sont isomorphes, ainsi qu'il fallait démontrer.  $\square$



## CHAPITRE 4

### EXEMPLES

*It's time for examples!* Même si, bien sûr, les variétés affines et les variétés quasi-affines du chapitre précédent sont des variétés algébriques.

#### 4.1. Espaces projectifs

**4.1.1. Droite projective.** — L'exemple le plus simple de variété algébrique qui n'est pas une variété affine est la droite projective  $\mathbf{P}^1$ . Classiquement, celle-ci est définie comme l'ensemble des droites vectorielles du plan  $k^2$ , mais cette définition ne rend pas apparente la structure de variété algébrique, ni celle de variété différentielle lorsque  $k = \mathbf{R}$  ou  $\mathbf{C}$ , ni même dans ces cas celle d'espace topologique. En associant à un couple  $(a, b) \in k^2 \setminus \{(0, 0)\}$  la droite d'équation  $ax + by = 0$ , on voit quand même que  $\mathbf{P}^1$  est le quotient de  $k^2 \setminus \{0\}$  par  $k^*$ , d'où au moins une structure d'espace topologique quotient. Pour la structure de variété, cela nécessite encore du travail...

Cependant, les droites du plan ont ou bien une équation  $ax + y = 0$  avec  $a \in k$ , ou bien une équation  $x + by = 0$  avec  $b \in k$ . À part les deux axes de coordonnées, toutes les droites ont une équation de chaque forme et si une droite est représentée par  $ax + y = 0$  avec  $a \neq 0$ , elle a aussi l'équation  $x + by = 0$  avec  $b = 1/a \neq 0$ . Autrement dit, on obtient l'ensemble des droites vectorielles de  $k^2$  en prenant deux copies de la droite affine  $\mathbf{A}^1$  et en les *recollant* le long de l'ouvert  $\mathbf{A}^1 \setminus \{0\}$  via l'isomorphisme  $\mathbf{A}^1 \setminus \{0\} \rightarrow \mathbf{A}^1 \setminus \{0\}$  défini par  $t \mapsto 1/t$ .

**4.1.2. Espace projectif.** — Plus généralement, l'espace projectif  $\mathbf{P}^n$  est l'ensemble des hyperplans vectoriels de  $k^{n+1}$ . Montrons comment le munir d'une structure de variété algébrique. Si  $(y_0, \dots, y_n)$  sont les coordonnées de  $k^{n+1}$ , un hyperplan possède une équation  $x_0Y_0 + \dots + x_nY_n = 0$ . Si  $x_i \neq 0$ , on peut diviser l'équation par  $x_i$  et supposer  $x_i = 1$ . On considère ainsi  $n + 1$  copies  $U_0, \dots, U_n$  de l'espace affine  $\mathbf{A}^n$ , où  $U_i$  est la sous-variété d'équation  $x_i = 1$  de  $\mathbf{A}^{n+1}$ . Pour tout couple  $(i, j)$  avec  $i \neq j$ , l'ouvert  $U_{ij}$  de  $U_i$  est défini

par  $x_j \neq 0$  et

$$\varphi_{ij} : (x_0, \dots, x_n) = (x_0/x_j, x_1/x_j, \dots, x_n/x_j)$$

définit un isomorphisme  $U_{ij} \rightarrow U_{ji}$ . Il est facile de constater que  $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ . Par recollement, on obtient une variété algébrique, appelée *espace projectif* de dimension  $n$  et noté  $\mathbf{P}^n$  dont les points sont exactement les  $(x_0, \dots, x_n) \in k^{n+1} \setminus \{0\}$  modulo l'action par multiplication de  $k^*$ .

Dans la suite, on notera  $(x_0 : \dots : x_n)$  le point de  $\mathbf{P}^n(k)$  qui est la classe de  $(x_0, \dots, x_n)$ . Inversement,  $(x_0, \dots, x_n)$  seront appelées *coordonnées homogènes* de ce point.

PROPOSITION 4.1.3. — *L'application  $\theta : \mathbf{A}^{n+1} \setminus \{(0, \dots, 0)\} \rightarrow \mathbf{P}^n$  qui associe  $(x_0 : \dots : x_n)$  à  $(x_0, \dots, x_n)$  est un morphisme.*

*Démonstration.* — Soit  $V_i \subset \mathbf{A}^{n+1}$  l'ouvert défini par  $x_i \neq 0$  et  $U_i$  l'ouvert de  $\mathbf{P}^n$  défini par  $x_i \neq 0$ . On a donc  $U_i = \theta(V_i)$ .

On a identifié  $U_i$  à la variété algébrique affine d'équation  $x_i = 1$  dans  $\mathbf{A}^{n+1}$ . Ainsi,  $\theta : V_i \rightarrow U_i$  s'écrit  $(x_0, \dots, x_n) \rightarrow (x_0/x_i, \dots, x_n/x_i)$ . Comme  $X_i$  ne s'annule pas sur  $V_i$ ,  $\theta$  est ainsi un morphisme  $V_i \rightarrow \mathbf{P}^n$ . Comme les  $V_i$  recouvrent  $\mathbf{A}^{n+1} \setminus \{0\}$ ,  $\theta$  est un morphisme.  $\square$

La proposition suivante prouve que  $\mathbf{P}^n$  n'est pas une variété affine.

PROPOSITION 4.1.4. — *On a  $\mathcal{O}(\mathbf{P}^n) = k$ .*

*Démonstration.* — Soit  $f \in \mathcal{O}(\mathbf{P}^n)$ . Il existe des polynômes  $P_0, \dots, P_n$  tels que sur l'ouvert  $U_i \simeq \mathbf{A}^n$ , on a

$$f((x_0 : \dots : x_n)) = P_i(x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots, x_n/x_i).$$

On peut rajouter  $X_i$  comme variable à  $P_i$  et supposer que pour tout  $i$ ,  $P_i$  est homogène de degré  $d$ . Sur  $U_i \cap U_0$ , on a ainsi la relation

$$P_i(x_0/x_i, \dots, x_n/x_i) = P_0(1, x_1/x_0, \dots, x_n/x_0),$$

d'où une égalité de polynômes

$$P_i(X_0, \dots, X_n)X_0^d = P_0(X_0, \dots, X_n)X_i^d.$$

Comme  $X_i$  est irréductible et est premier à  $X_0$ , le lemme de Gauß implique que  $X_i^d$  divise  $P_i$ , c'est-à-dire  $P_i = X_i^d Q_i$ . On a alors  $Q_i = Q_0$ . Le degré de  $Q_i$  est égal à  $d - d = 0$ , c'est-à-dire que  $Q_i$  est un élément  $a$  de  $k$  et  $f((x_0 : \dots : x_n)) = a$ . Autrement dit, toute fonction algébrique sur  $\mathbf{P}^n$  est constante.  $\square$

Nous nous intéressons maintenant aux sous-variétés de l'espace projectif. Rappelons que le degré d'un monôme  $\prod_{i=0}^n X_i^{a_i}$  est égal à  $\sum_{i=1}^n a_i$  et qu'un polynôme est dit homogène si tous les monômes dont il est la somme ont le même degré. Un idéal homogène de  $k[X_0, \dots, X_n]$  est un idéal engendré par des polynômes homogènes.

*Exercice 4.1.5.* — 1) Vérifier qu'un idéal  $I \subset k[X_0, \dots, X_n]$  est homogène si et seulement si pour tout  $P \in I$ , décomposé sous la forme  $P = \sum_d P_d$ ,  $P_d$  étant un polynôme homogène de degré  $d$ , chacun des  $P_d$  appartient à  $I$ .

2) Montrer que le radical d'un idéal homogène est encore un idéal homogène.

**DÉFINITION 4.1.6.** — Soit  $I \subset k[X_0, \dots, X_n]$  un idéal homogène. On définit  $\mathcal{P}(I)$  comme l'ensemble des  $(x_0 : \dots : x_n) \in \mathbf{P}^n(k)$  tels que pour tout polynôme homogène  $P \in I$ ,  $P(x_0, \dots, x_n) = 0$  (cela a un sens car  $P$  est homogène).

**THÉORÈME 4.1.7.** — Pour tout idéal homogène  $I$ ,  $\mathcal{P}(I)$  est un fermé de  $\mathbf{P}^n$ .

*Démonstration.* — En vertu du lemme 2.3.2, il suffit de le vérifier après restriction à chacun des ouverts affines  $U_i$  défini par  $x_i \neq 0$ . Pour simplifier les notations, on ne traite que le cas  $i = 0$ . Soit donc  $I_0$  l'ensemble des polynômes de  $k[X_1, \dots, X_n]$  de la forme  $P(1, X_1, \dots, X_n)$  pour  $P \in I$ . C'est un idéal car  $I$  est un idéal. Il est alors clair que  $\mathcal{P}(I) \cap U_0 = \mathcal{V}(I_0)$  si bien que  $\mathcal{P}(I) \cap U_0$  est un fermé de  $U_0$ . Par suite,  $\mathcal{P}(I)$  est un fermé de  $\mathbf{P}^n$ .  $\square$

**DÉFINITION 4.1.8.** — Soit  $X \subset \mathbf{P}^n$  une partie fermée. On appelle cône affine au-dessus de  $X$  la réunion de  $\{0\}$  et de l'image réciproque de  $X$  dans  $\mathbf{A}^{n+1} \setminus \{0\}$  par le morphisme canonique  $\theta : \mathbf{A}^{n+1} \setminus \{0\} \rightarrow \mathbf{P}^n$ . On le note  $C(X)$ ; c'est un fermé de  $\mathbf{A}^{n+1}$ .

*Justification.* — Par définition,  $C(X) \setminus \{0\} = \theta^{-1}(X)$  est fermé dans  $\mathbf{A}^{n+1} \setminus \{0\}$ . Comme  $C(X)$  contient  $\{0\}$ ,  $C(X)$  est donc fermé dans  $\mathbf{A}^{n+1}$ .  $\square$

**THÉORÈME 4.1.9 (Nullstellensatz projectif).** — Tout fermé non vide de  $\mathbf{P}^n$  est de la forme  $\mathcal{P}(I)$  pour un unique idéal homogène  $I$  tel que  $I = \sqrt{I}$  et le cône affine au-dessus de  $X$  est égal à  $\mathcal{V}(I)$ .

D'autre part,  $\mathcal{P}(I) = \emptyset$  si et seulement si  $I$  contient l'idéal  $(X_0, \dots, X_n)$ .

*Démonstration.* — Soient  $X$  un fermé non vide de  $\mathbf{P}^n$ ,  $C(X) \subset \mathbf{A}^{n+1}$  son cône affine.

Soit  $\mathcal{I}(X)$  l'idéal engendré par les polynômes homogènes  $P \in k[X_0, \dots, X_n]$  tels que  $P(x_0, \dots, x_n) = 0$  pour tout  $(x_0 : \dots : x_n) \in X$ . Il est clair que  $\mathcal{I}(X) = \sqrt{\mathcal{I}(X)}$  et que  $X \subset \mathcal{P}(\mathcal{I}(X))$ .

Montrons que  $C(X) = \mathcal{V}(\mathcal{I}(X))$ ; comme  $C(X)$  est fermé dans  $\mathbf{A}^{n+1}$ , cela revient à prouver, en vertu du Nullstellensatz usuel (théorème 3.1.14) que  $\mathcal{I}(C(X)) = \mathcal{I}(X)$ .

**LEMME 4.1.10.** — On a les inclusions

$$\mathcal{I}(C(X) \setminus \{0\}) \subset \mathcal{I}(X) \subset \mathcal{I}(C(X)).$$

Par suite, ces trois idéaux sont égaux et  $C(X) = \overline{C(X) \setminus \{0\}}$ .

*Preuve du lemme.* — En effet, si  $P$  est un polynôme homogène s'annulant sur  $X$ , il s'annule sur  $\theta^{-1}(X) \subset \mathbf{A}^{n+1}$ . Mais comme il ne peut pas être de degré nul ( $X \neq \emptyset$ ), il s'annule aussi en 0. Ainsi,  $P$  s'annule sur  $C(X)$ , d'où  $\mathcal{I}(X) \subset \mathcal{I}(C(X))$ .

Réciproquement, soit  $P$  un polynôme s'annulant sur  $C(X) \setminus \{0\}$  et montrons que  $P \in \mathcal{I}(X)$ . On peut écrire  $P$  comme une somme de polynômes homogènes :  $P = \sum_d P_d$ . Si  $(x_0 : \dots : x_n) \in X$ , pour tout  $\lambda \in k^*$ , on a  $(\lambda x_0, \dots, \lambda x_n) \in C(X) \setminus \{0\}$  si bien que  $\sum_d \lambda^d P_d(x_0, \dots, x_n) = 0$ . Cela implique que chacun des  $P_d$  s'annule en  $(x_0, \dots, x_n)$ . Ainsi, chaque  $P_d$  s'annule sur  $X$  et  $P \in \mathcal{I}(X)$ . *(Fin de la preuve du lemme.)*

On peut maintenant prouver que  $X = \mathcal{P}(\mathcal{I}(X))$ . De fait, si  $(x_0 : \dots : x_n) \in \mathcal{P}(\mathcal{I}(X))$ , cela signifie que tout polynôme homogène  $P \in \mathcal{I}(X)$  s'annule au point  $(x_0, \dots, x_n)$ , d'où  $(x_0, \dots, x_n) \in \mathcal{V}(\mathcal{I}(X)) = C(X)$ . Par suite,  $(x_0 : \dots : x_n) \in X$ .

Pour l'unicité, soit  $I$  un idéal homogène tel que  $I = \sqrt{I}$  et  $\mathcal{P}(I) = X$  ; on constate que

$$\mathcal{V}(I) \cap (\mathbf{A}^{n+1} \setminus \{0\}) = C(X) \setminus \{0\}$$

et donc que  $I \subset \mathcal{I}(C(X) \setminus \{0\})$ . Il y a alors deux solutions : soit  $\mathcal{V}(I) = C(X)$ , soit  $\mathcal{V}(I) = C(X) \setminus \{0\}$ . Mais si  $X \neq \emptyset$ ,  $C(X) \setminus \{0\}$  n'est pas fermé dans  $\mathbf{A}^{n+1}$ . Ainsi,  $C(X) = \mathcal{V}(I)$  et donc  $I = \mathcal{I}(X)$ .

Si  $X = \emptyset$ , l'égalité  $\mathcal{P}(I) = X$  implique que  $\mathcal{V}(I) \subset \{0\}$ , soit  $(X_0, \dots, X_n) \subset I$ . Le théorème est ainsi démontré.  $\square$

**DÉFINITION 4.1.11.** — *Une variété projective est une variété algébrique isomorphe à une sous-variété d'un espace projectif.*

*Une variété quasi-projective est un ouvert d'une variété projective.*

**Remarque 4.1.12.** — Les variétés affines sont quasi-projectives. En revanche, toute variété n'est pas quasi-projective, même s'il est difficile de donner un exemple. Une différence fondamentale entre les variétés affines et les variétés projectives et sur ces dernières, il n'existe pas de fonction régulière non localement constante définie partout.

**Exercice 4.1.13** (Plongement de Veronese<sup>(2)</sup>). — 1°) Soient  $n$  et  $d$  des entiers  $\geq 1$ . On pose  $N = \binom{n+d}{n} - 1$ . Montrer que le nombre des monômes de degré  $d$  en  $n+1$  variables est égal à  $N+1$ . On les note  $M_0, \dots, M_N$ .

2°) Montrer que l'application  $\phi_d : \mathbf{P}^n \rightarrow \mathbf{P}^N$  donnée par  $(x_0 : \dots : x_n) \mapsto (M_0(x) : \dots : M_N(x))$  est bien définie et est un isomorphisme de  $\mathbf{P}^n$  sur une sous-variété fermée de  $\mathbf{P}^N$ .

3°) Soit  $f \in k[X_0, \dots, X_n]$  un polynôme homogène de degré  $d$ . Montrer que le complémentaire de  $\mathcal{P}(f)$  dans  $\mathbf{P}^n$  est une variété affine.

2. Giuseppe VERONESE (1854–1917). — Il développa la géométrie projective en dimension arbitraire. Notamment, il mit en évidence les problèmes qui peuvent apparaître lorsqu'on cherche à faire vivre une surface algébrique non singulière dans  $\mathbf{P}^3$ .

## 4.2. Produits

Dans cette section, nous voulons munir le produit de deux variétés algébriques d'une structure de variété algébrique. C'est plus dur qu'il n'y paraît car le produit dans la catégorie des espaces topologiques est insuffisant : on a vu dans l'exercice 3.2.12 que  $\mathbf{A}^2$  n'est pas homéomorphe à  $\mathbf{A}^1 \times \mathbf{A}^1$  muni de la topologie produit.

Pour définir le produit de deux variétés, on commence par le cas des variétés affines.

**PROPOSITION 4.2.1.** — *Soient  $X \subset \mathbf{A}^n$  et  $Y \subset \mathbf{A}^m$  deux ensembles algébriques d'idéaux  $I \subset k[X_1, \dots, X_n]$  et  $J \subset k[Y_1, \dots, Y_m]$ . Identifions  $\mathbf{A}^n \times \mathbf{A}^m$  à  $\mathbf{A}^{n+m}$ . Alors,  $X \times Y \subset \mathbf{A}^{n+m}$  est un ensemble algébrique : son idéal est engendré par les idéaux  $I$  et  $J$  dans  $k[X_1, \dots, X_n, Y_1, \dots, Y_m]$  et son anneau des fonctions est  $\mathcal{A}(X \times Y) = \mathcal{A}(X) \otimes_k \mathcal{A}(Y)$ .*

*Démonstration.* — Un point  $(x, y)$  de  $\mathbf{A}^n \times \mathbf{A}^m$  appartient à  $X \times Y$  si et seulement si  $x \in X$  et  $y \in Y$ , donc si et seulement si les éléments de  $I$  s'annulent en  $x$  et ceux de  $J$  s'annulent en  $y$ . Ainsi,  $\mathcal{V}(I+J) = \mathcal{V}(I) \times \mathcal{V}(J)$ .

On rappelle (cf. 1.6.1) que l'on a un isomorphisme canonique

$$(k[X_1, \dots, X_n]/I) \otimes_k (k[Y_1, \dots, Y_m]/J) \simeq k[X_1, \dots, X_n, Y_1, \dots, Y_m]/(I+J).$$

Ainsi, si  $(f_i)$  et  $(g_j)$  sont des polynômes définissant des bases de  $\mathcal{A}(X)$  et  $\mathcal{A}(Y)$  respectivement, on peut écrire tout polynôme  $P \in k[X_1, \dots, X_n, Y_1, \dots, Y_m]$  de manière unique sous la forme

$$P = \sum a_{i,j} f_i(X) g_j(Y) + P_0,$$

où les  $a_{i,j} \in k$  et  $P_0 \in I+J$ . Supposons donc que  $P \in \mathcal{I}(X \times Y)$ . Il en résulte que pour tout  $x \in X$  et tout  $y \in Y$ ,  $P(x, y) = 0$ . En particulier, pour tout  $x \in X$ ,

$$P(x, Y) = \sum_j \left( \sum_i a_{i,j} f_i(x) \right) g_j(Y) + P_0(x, Y) \in \mathcal{I}(Y) = J,$$

et donc, puisque  $P_0(x, Y) \in \mathcal{I}(Y)$ , on a pour tout  $j$  et pour tout  $x \in X$  que  $\sum_i a_{i,j} f_i(x) = 0$ . Cela implique que  $a_{i,j} = 0$  pour tout  $i$  et pour tout  $j$ , d'où  $P \in I+J$  et l'idéal de  $X \times Y$  est engendré dans  $k[X_1, \dots, X_n, Y_1, \dots, Y_m]$  par  $I$  et  $J$ .

Du même coup,

$$\mathcal{A}(X \times Y) = \mathcal{A}(X) \otimes_k \mathcal{A}(Y).$$

□

**COROLLAIRE 4.2.2.** — *Le produit de deux ensembles quasi-algébriques est un ensemble quasi-algébrique.*

**PROPOSITION 4.2.3.** — *Si  $X$  et  $Y$  sont irréductibles,  $X \times Y$  aussi. (Le produit tensoriel de deux  $k$ -algèbres de type fini intègres est intègre.)*

*Démonstration.* — Supposons que  $X \times Y = Z_1 \cup Z_2$ , pour deux fermés  $Z_1$  et  $Z_2$  de  $\mathbf{A}^{n+m}$ . Pour  $i = 1$  ou  $2$ , soit  $X_i = \{x \in X; x \times Y \subset Z_i\}$ .

Soit  $x \in X$ . On peut écrire

$$Y \simeq x \times Y = (Z_1 \cap (x \times Y)) \cup (Z_2 \cap (x \times Y))$$

et comme  $Y$  est irréductible, on a  $x \times Y \subset Z_1$  ou  $Z_2$ . Autrement dit,  $x \in X_1$  ou  $x \in X_2$ , ce qui implique  $X = X_1 \cup X_2$ .

D'autre part,  $x \in X_1$  équivaut à dire que pour tout  $y \in Y$ ,  $(x, y) \in Z_1$  :

$$X_1 = \{x \in X; \forall y \in Y, \forall P \in \mathcal{S}(Z_1), P(x, y) = 0\}$$

est ainsi un ensemble algébrique fermé. De même,  $X_2$  est fermé.

Comme  $X = X_1 \cup X_2$  est irréductible,  $X = X_1$  ou  $X = X_2$ , c'est-à-dire  $X \times Y = Z_1$  ou  $Z_2$ .  $\square$

Pour définir le produit de deux variétés algébriques arbitraires, un peu de formalisme de théorie des catégories est utile.

**DÉFINITION 4.2.4.** — Soient  $\mathcal{C}$  une catégorie,  $X$  et  $Y$  deux objets de  $\mathcal{C}$ . On dit qu'un triplet  $(Z, p, q)$ , où  $Z$  est un objet de  $\mathcal{C}$ ,  $p : Z \rightarrow X$  et  $q : Z \rightarrow Y$  sont deux morphismes, est un produit si la propriété universelle suivante est satisfaite : pour tout triplet  $(W, f, g)$  formé d'un objet de  $\mathcal{C}$  et de deux morphismes  $f : W \rightarrow X$  et  $g : W \rightarrow Y$ , il existe un unique morphisme  $\varphi : W \rightarrow Z$  tel que  $f = p \circ \varphi$  et  $g = q \circ \varphi$ .

*Exercice 4.2.5.* — Vérifier qu'un produit, s'il existe, est unique à un isomorphisme unique près, autrement dit, que si  $(Z', p', q')$  est un autre produit, il existe un unique isomorphisme  $\varphi : Z \xrightarrow{\sim} Z'$  tel que  $p' = p \circ \varphi$ ,  $q' = q \circ \varphi$ .

Ainsi, on peut parler du produit de deux objets (à condition qu'il existe, bien entendu).

**PROPOSITION 4.2.6.** — Soient  $X \subset \mathbf{A}^n$  et  $Y \subset \mathbf{A}^m$  deux variétés algébriques affines. Pour tout ouvert  $U$  de  $X$  et  $V$  de  $Y$ , le produit  $U \times V$  muni des projections  $p : U \times V \rightarrow U$  et  $q : U \times V \rightarrow V$  est le produit de  $U$  et  $V$  dans la catégorie des variétés algébriques.

*Démonstration.* — Soient  $W$  une variété algébrique et  $f : W \rightarrow U$ ,  $g : W \rightarrow V$  deux morphismes. Si  $\varphi : W \rightarrow U \times V$  vérifie  $p \circ \varphi = f$  et  $q \circ \varphi = g$ , on a nécessairement  $\varphi(w) = (f(w), g(w))$ . Réciproquement, comme les coordonnées de  $\varphi$  sont  $(f_1, \dots, f_n, g_1, \dots, g_m)$ , le théorème 3.3.9 montre que  $\varphi$  est un morphisme de variétés algébriques.  $\square$

**THÉORÈME 4.2.7.** — Si  $X$  et  $Y$  sont deux variétés algébriques, il existe un produit  $X \times Y$  dans la catégorie des variétés algébriques.

*Démonstration.* — On écrit  $X = \bigcup U_i$ ,  $Y = \bigcup V_k$  comme réunion de variétés affines, avec des isomorphismes de recollement  $f_{ij} : U_{ij} \rightarrow U_{ji}$ ,  $g_{kl} : V_{kl} \rightarrow V_{lk}$  comme dans la construction du théorème 3.4.7. On va alors recoller les  $U_i \times V_k$ .

Pour cela, on remarque que les morphismes  $U_{ij} \times V_{k\ell} \rightarrow U_{ij} \rightarrow U_{ji}$  et  $U_{ij} \times V_{k\ell} \rightarrow V_{k\ell} \rightarrow V_{\ell k}$  implique l'existence d'un unique morphisme

$$\Psi_{(ik)(j\ell)} : U_{ij} \times V_{k\ell} \rightarrow V_{\ell k} \times U_{ji}.$$

(Les  $U_{ij}$  sont des ouverts de variétés affines, donc admettent des produits.) De plus, les conditions du théorème 3.4.7 sont vérifiées (grâce à l'unicité des  $\Psi_{(ik)(j\ell)}$ ) et en particulier, ce sont des isomorphismes. Cela nous fournit une variété algébrique, notée  $X \times Y$ , par recollement des  $U_i \times V_k$ .

Les morphismes  $U_i \times V_k \rightarrow U_i \rightarrow X$  se recollent en un morphisme  $p : X \times Y \rightarrow X$ , et de même, on a un morphisme  $q : X \times Y \rightarrow Y$ .

Montrons maintenant que  $(X \times Y, p, q)$  est un produit.

Soit  $W$  une variété algébrique et  $f : W \rightarrow X, g : W \rightarrow Y$  deux morphismes. On cherche à montrer qu'il existe un unique  $\psi : W \rightarrow X \times Y$  tel que  $p \circ \psi = f, q \circ \psi = g$ . Soit  $W_{ik} = f^{-1}(U_i) \cap g^{-1}(V_k)$ ; c'est un ouvert de  $W$  avec deux morphismes  $f|_{W_{ik}} : W_{ik} \rightarrow U_i$  et  $g|_{W_{ik}} : W_{ik} \rightarrow V_k$ . Comme  $U_i \times V_k$  est un produit de  $U_i$  et  $V_k$ , il en résulte un unique morphisme  $\psi_{ik} : W_{ik} \rightarrow U_i \times V_k$  tel que  $p \circ \psi_{ik} = f|_{W_{ik}}$  et  $q \circ \psi_{ik} = g|_{W_{ik}}$ . Nécessairement,  $\psi|_{W_{ik}} = \psi_{ik}$ , d'où l'unicité de  $\psi$ . Par l'unicité des  $\psi_{ik}$ , ils se recollent pour fournir un morphisme  $\psi : W \rightarrow X \times Y$ . On a donc construit le produit de  $X$  et de  $Y$  dans la catégorie des variétés algébriques.  $\square$

*Remarque 4.2.8.* — Soit  $\text{pt}$  la variété algébrique donnée par un point (elle est affine, d'anneau  $k$ ). Si  $X$  est une variété algébrique,  $\text{Hom}(\text{pt}, X)$  est l'ensemble des points de  $X$ . Comme,

$$\text{Hom}(\text{pt}, X \times Y) = \text{Hom}(\text{pt}, X) \times \text{Hom}(\text{pt}, Y),$$

l'ensemble sous-jacent à  $X \times Y$  est le produit des ensembles sous-jacents à  $X$  et  $Y$ .

Pendant, la topologie n'est pas la topologie produit : par construction,  $\mathbf{A}^1 \times \mathbf{A}^1 = \mathbf{A}^2$  et l'exercice 3.2.12 a fait remarquer que la topologie de Zariski sur  $\mathbf{A}^2$  n'est pas la topologie produit.

**LEMME 4.2.9.** — *Soient  $X$  et  $Y$  deux variétés algébriques. Si  $U$  est un ouvert de  $X$ , le morphisme canonique  $U \times Y \rightarrow X \times Y$  identifie  $U \times Y$  à un ouvert de  $X \times Y$ . Si  $Z$  est un fermé de  $X, Z \times Y$  s'identifie de même à un fermé de  $X \times Y$ .*

*Démonstration.* — Il suffit de traiter le cas d'un fermé et on peut supposer que  $X \subset \mathbf{A}^n$  et  $Y \subset \mathbf{A}^m$  sont des variétés affines. Alors,  $Z \times Y$  s'identifie à la sous-variété de  $\mathbf{A}^{n+m}$  d'idéal  $\mathcal{I}(Z) + \mathcal{I}(Y)$  qui contient l'idéal  $\mathcal{I}(X) + \mathcal{I}(Y)$ .  $\square$

**THÉORÈME 4.2.10 (Plongement de Segre).** — *L'application*

$$S : \mathbf{P}^n \times \mathbf{P}^m \rightarrow \mathbf{P}^{nm+n+m},$$

$$((x_0 : \dots : x_n), (y_0 : \dots : y_m)) \mapsto (x_0 y_0 : \dots : x_0 y_m : x_1 y_0 : \dots : x_n y_m)$$

Collado SEGRE (1863–1924)

*Grand représentant de « l'école italienne » de géométrie algébrique, Segre est connu pour ses travaux sur les quadriques et les surfaces.*



est un morphisme de variétés algébriques qui identifie  $\mathbf{P}^n \times \mathbf{P}^m$  à une sous-variété fermée de  $\mathbf{P}^{nm+n+m}$ . On l'appelle plongement de Segre.

*Démonstration.* — On commence par vérifier que cela a un sens : si on multiplie les  $x_i$  par  $\lambda \in k^*$  et les  $y_j$  par  $\mu \in k^*$ , cela multiplie les  $x_i y_j$  par  $\lambda \mu$  ; de plus, l'un des  $x_i y_j$  est non nul.

Les coordonnées homogènes de  $\mathbf{P}^{nm+n+m}$  sont notées par la lettre  $z$  et indexées par  $(i, j) \in \{0, \dots, n\} \times \{0, \dots, l\}$ . Notons  $U_i$ ,  $V_j$  et  $W_{ij}$  les ouverts affines de  $\mathbf{P}^n$ ,  $\mathbf{P}^m$  et  $\mathbf{P}^{nm+n+m}$  où respectivement  $x_i \neq 0$ ,  $y_j \neq 0$  et  $z_{ij} \neq 0$ .

On a  $S^{-1}(W_{\alpha\beta}) = U_\alpha \times V_\beta$  : si  $S(x, y) \in W_{\alpha\beta}$ ,  $x_\alpha y_\beta \neq 0$ , d'où  $x \in U_\alpha$  et  $y \in V_\beta$ .

Montrons que  $S$  est injective : si  $S(x, y) = S(x', y') \in W_{\alpha\beta}$ , on peut supposer  $x_\alpha = x'_\alpha = 1$  et  $y_\beta = y'_\beta = 1$ , d'où  $x_\alpha y_\beta = x'_\alpha y'_\beta = 1$ , ce qui implique que pour tous  $i$  et  $j$ ,  $x_i y_j = x'_i y'_j$ . En particulier, si  $i = \alpha$ , on trouve  $y_j = y'_j$  pour tout  $j$ , et pour  $j = \beta$ , on trouve  $x_i = x'_i$  pour tout  $i$ .

Montrons que  $S$  définit un isomorphisme de  $U_\alpha \times V_\beta$  sur une sous-variété de  $W_{\alpha\beta}$ . Or, l'image de  $S$  est formée des  $(z_{ij})$  tels que  $z_{ij} = x_i y_j$ . Comme  $x_\alpha = 1$  et  $y_\beta = 1$ , on en déduit  $x_i = z_{i\beta}$  et  $y_j = z_{\alpha j}$ , si bien que l'image de  $S$  est contenue dans la sous-variété  $Z_{\alpha\beta}$  de  $W_{\alpha\beta}$  définie par les équations  $z_{ij} = z_{i\beta} z_{\alpha j}$ . Réciproquement, l'application  $T : Z_{\alpha\beta} \rightarrow U_\alpha \times V_\beta$  définie par  $T(z_{ij}) = ((z_{i\beta}), (z_{\alpha j}))$  est un morphisme et il est facile de constater que  $T \circ S = \text{id}_{Z_{\alpha\beta}}$  et  $S \circ T = \text{id}_{U_\alpha \times V_\beta}$ . Autrement dit,  $S$  définit un isomorphisme de  $U_\alpha \times V_\beta$  sur une sous-variété fermée de  $W_{\alpha\beta}$ .

Notons  $Z$  l'image de  $\mathbf{P}^n \times \mathbf{P}^m$  par  $S$ . On a ainsi prouvé que la restriction de  $S$  à  $S^{-1}(W_{\alpha\beta}) = U_\alpha \times V_\beta$  définit un isomorphisme  $U_\alpha \times V_\beta \rightarrow Z \cap W_{\alpha\beta}$  et que  $Z \cap W_{\alpha\beta}$  est fermé dans  $W_{\alpha\beta}$ . Il en résulte que  $Z$  est fermé et que  $S : \mathbf{P}^n \times \mathbf{P}^m \rightarrow \mathbf{P}^{nm+n+m}$  est un isomorphisme de  $\mathbf{P}^n \times \mathbf{P}^m$  sur  $Z$ .  $\square$

*Exemple 4.2.11.* — Lorsque  $n = m = 1$ , on obtient le morphisme

$$\mathbf{P}^1 \times \mathbf{P}^1 \rightarrow \mathbf{P}^3, \quad ((u, v) : (s, t)) \mapsto (x : y : z : w) = (us : ut : vs : vt).$$

Hermann Günter GRASSMANN (1809–1877)

*Un des fondateurs du calcul vectoriel en inventant notamment l'algèbre extérieure, il a aussi travaillé sur l'électricité, la couleur, la botanique. Déçu du manque d'intérêt porté à ses travaux, il s'est consacré l'étude du sanscrit ; son dictionnaire est toujours utilisé !*



Son image est la quadrique d'équation homogène  $xy - zw = 0$ .

En général, l'idéal homogène de l'image de  $\mathbf{P}^n \times \mathbf{P}^m$  dans  $\mathbf{P}^{m+n+m}$  est engendré par les  $z_{ij}z_{\alpha\beta} - z_{i\beta}z_{\alpha j}$ . C'est ainsi une intersection de quadriques.

**COROLLAIRE 4.2.12.** — *Un produit de variétés projectives est une variété projective.*

*Démonstration.* — Soient  $X \subset \mathbf{P}^n$  et  $Y \subset \mathbf{P}^m$  deux variétés projectives. Alors,  $X \times Y$  s'identifie à une sous-variété de  $\mathbf{P}^n \times \mathbf{P}^m$  laquelle s'identifie par le plongement de Segre à une sous-variété de  $\mathbf{P}^{m+n+m}$ . Ainsi,  $X \times Y$  est isomorphe à une sous-variété de  $\mathbf{P}^{m+n+m}$  et est donc une variété projective.  $\square$

### 4.3. Grassmanniennes

Les grassmanniennes sont des variétés algébriques dont les points sont en bijection avec les sous-espaces vectoriels d'un  $k$ -espace vectoriel donné. Les espaces projectifs en sont un cas particulier.

**4.3.1. Construction.** — Soient  $p$  et  $n$  deux entiers  $\geq 1$ , avec  $p \leq n$ . Pour se donner un  $p$ -plan de  $k^n$ , il suffit de s'en donner une base, c'est-à-dire une matrice  $A \in \mathcal{M}_{p,n}(k)$  de  $p$  vecteurs lignes dont le rang est  $p$ . Dire qu'une matrice  $A \in \mathcal{M}_{p,n}(k)$  est de rang  $p$  équivaut à dire qu'il existe un mineur  $p \times p$  inversible, c'est-à-dire une partie  $I \subset \{1, \dots, n\}$  de cardinal  $p$  telle que la matrice  $A_I$  formée en prenant les colonnes d'indices dans  $I$  soit inversible. (Géométriquement, cela signifie que le  $p$ -plan défini par  $A$  et le  $(n-p)$ -plan engendré par les vecteurs de base d'indices non dans  $I$  sont en somme directe.) Comme deux matrices  $A$  et  $A'$  représentent le même  $p$ -plan si et seulement s'il existe  $g \in \text{GL}_p(k)$  tel que  $A' = gA$ , quitte à multiplier  $A$  par  $A_I^{-1}$ , on peut supposer que  $A_I = \text{id}$ .

Si  $I \subset \{1, \dots, n\}$  est de cardinal  $p$ , soit ainsi  $G_I \subset \mathcal{M}_{p,n}(k)$  l'ensemble des matrices  $A$  dont le mineur  $A_I$  est l'identité. C'est une sous-variété affine de  $M_{p,n}(k) \simeq k^{np}$ , isomorphe à  $k^{p(n-p)}$  ( $p(n-p)$  est le nombre de coefficients de  $A$  qui restent indéterminés). Si  $J$  est une autre partie à  $p$  éléments de  $\{1, \dots, n\}$ , soit  $G_{IJ}$  l'ensemble des  $A \in G_I$  telles que  $A_J$  est inversible. Cette condition s'écrit  $\det A_J \neq 0$ ; comme le déterminant est une fonction polynomiale,  $A \mapsto \det A_J$  est une fonction régulière sur  $G_I$  et  $G_{IJ}$  est un ouvert de  $G_I$ . De même, l'application

$$\varphi_{IJ} : G_{IJ} \rightarrow G_{JI}, \quad A \mapsto A_J^{-1} \cdot A$$

est un morphisme (car  $A \mapsto A_J^{-1}$  est donné selon les formules de Cramer<sup>(3)</sup> par le quotient de polynômes par la fonction régulière  $A \mapsto \det A_J$  et celle-ci ne s'annule pas sur  $G_{IJ}$ ).

Si  $K$  est une troisième partie de  $\{1, \dots, n\}$ , on constate que pour  $A \in G_{IJ} \cap G_{IK}$ ,

$$\begin{aligned} \varphi_{JK} \circ \varphi_{IJ}(A) &= \varphi_{JK}(A_J^{-1} \cdot A) = (A_J^{-1} \cdot A_K)^{-1} (A_J^{-1} \cdot A) \\ &= A_K^{-1} \cdot A_J \cdot A_J^{-1} \cdot A = A_K^{-1} \cdot A = \varphi_{IK}(A) \end{aligned}$$

et donc que les  $(G_I, G_{IJ}, \varphi_{IJ})$  vérifient la condition de recollement du théorème 3.4.7 pour fournir une variété algébrique  $\mathbf{G}_{p,n}$ , appelée *grassmannienne* des  $p$ -plans de  $k^n$ .

**4.3.2. Le plongement de Plücker.** — Montrons maintenant que  $\mathbf{G}_{p,n}$  est une variété projective. Soit  $N = \binom{n}{p} - 1$ . On définit une application  $\theta : \mathbf{G}_{p,n} \rightarrow \mathbf{P}^N$ . La restriction de  $\theta$  à  $G_I$  est donnée par  $A \mapsto \theta_I(A) = (\det A_K)_I$ , où  $K$  décrit les  $N+1$  parties à  $p$  éléments de  $\{1, \dots, n\}$ . Comme le déterminant est donné par un polynôme,  $\theta_I$  est un morphisme de variétés algébriques. Si  $A \in G_{IJ}$ , on a

$$\det(\varphi_{IJ}(A))_K = \det(A_J^{-1} \cdot A)_K = \det(A_J^{-1} \cdot A_K) = \det(A_J)^{-1} \det A_K,$$

si bien que

$$\theta_J(\varphi_{IJ}(A)) = (\det A_J)^{-1} \theta_I(A) = \theta_I(A).$$

Ainsi, les  $\theta_I$  se recollent en un morphisme  $\mathbf{G}_{p,n} \rightarrow \mathbf{P}^N$ .

Montrons que  $\theta$  est un isomorphisme de  $\mathbf{G}_{p,n}$  sur une sous-variété fermée de  $\mathbf{P}^N$ . Pour cela, on remarque qu'un point  $\lambda \in \theta(\mathbf{G}_{p,n})$  de coordonnées homogènes  $(\lambda_I)$  est dans l'image de  $G_I$  si et seulement si  $\lambda_I \neq 0$ . Ainsi, pour prouver que l'image de  $\mathbf{G}_{p,n}$  est fermée, il suffit de prouver que l'image par  $\theta_I$  de  $G_I$  dans la sous-variété  $U_I$  de  $\mathbf{A}^{N+1}$  définie par  $\lambda_I = 1$  est fermée.

3. Gabriel CRAMER (1704–1752). — Surtout connu pour ses travaux sur les déterminants, il étudia aussi l'analyse, la physique et l'histoire des mathématiques.

Or, si  $A \in G_I$ , la donnée de  $\lambda = \theta_I(A)$  permet de retrouver  $A$ . Pour simplifier les notations, supposons  $I = \{1, \dots, p\}$ . Alors, si  $J = I \setminus \{i\} \cup \{j\}$ , on a

$$\lambda_J = \det \begin{pmatrix} 1 & \dots & 0 & & & a_{1,j} \\ \vdots & \ddots & \vdots & & 0 & \vdots \\ 0 & \dots & 1 & 0 & & a_{i-1,j} \\ 0 & \dots & 0 & 0 & \dots & 0 & a_{i,j} \\ & & & 1 & \dots & 0 & a_{i+1,j} \\ & 0 & & \vdots & \ddots & \vdots & \vdots \\ & & & 0 & \dots & 1 & a_{p,j} \end{pmatrix} = (-1)^{p-i} a_{i,j}.$$

Ainsi, on peut poser

$$\varphi_I : U_I \rightarrow G_I, \quad (\lambda_I) \mapsto \begin{pmatrix} 1 & \dots & 0 & (-1)^{p-1} \lambda_{I-1+(p+1)} & \dots & (-1)^{p-1} \lambda_{I-1+n} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & 1 & \lambda_{I-p+(p+1)} & \dots & \lambda_{I-p+n} \end{pmatrix}.$$

L'application  $\varphi_I$  est un morphisme et l'on a  $\varphi_I \circ \theta_I = \text{id}$  si bien que la restriction de  $\theta_I \circ \varphi_I$  à  $\theta_I(G_I)$  est l'identité aussi. Il en résulte que  $\theta_I(G_I)$  est une partie fermée de  $U_I$ , définie par le système d'équations polynomiales  $\lambda = \theta_I(\varphi_I(\lambda))$ . On a ainsi prouvé que  $\theta(\mathbf{G}_{p,n}) \cap U_I$  est fermé dans  $U_I$  pour toute partie  $I \subset \{1, \dots, n\}$  de cardinal  $p$ . Par suite,  $\theta(\mathbf{G}_{p,n})$  est fermé dans  $\mathbf{P}^N$ .

De plus,  $\theta_I : G_I \rightarrow \theta(G_I) = \theta(\mathbf{G}_{p,n}) \cap U_I$  est un isomorphisme, ce qui implique que  $\theta$  est un isomorphisme, appelé *plongement de Plücker*<sup>(4)</sup> de  $\mathbf{G}_{p,n}$  sur une sous-variété algébrique de  $\mathbf{P}^N$ .

**4.3.3. Relations de Grassmann.** — Nous allons maintenant déterminer les équations de l'image d'une grassmannienne par le plongement de Plücker et démontrer que celle-ci est une intersection de quadriques.

De manière intrinsèque, le plongement de Plücker associe au  $p$ -plan de  $V = k^n$  engendré par les vecteurs  $v_1, \dots, v_p$  la droite de  $\Lambda^p V$  engendrée par le  $p$ -vecteur *décomposable*  $v_1 \wedge \dots \wedge v_p$ . Réciproquement, on cherche une condition nécessaire et suffisante sur un  $p$ -vecteur  $w \in \Lambda^p V$  pour être décomposable.

Soit  $V^*$  le dual de  $V$ . Pour tout entier  $k$ , l'unique application bilinéaire  $\Lambda^k V^* \times \Lambda^k V \rightarrow k$  telle que

$$\langle \varphi_1 \wedge \dots \wedge \varphi_k, v_1 \wedge \dots \wedge v_k \rangle = \det(\varphi_i(v_j))$$

identifie  $\Lambda^k V^*$  au dual de  $\Lambda^k V$ . Si  $\varphi \in \Lambda^k V^*$ , soit  $\iota(\varphi)$  l'opérateur de contraction  $\Lambda^p V \rightarrow \Lambda^{p-k} V$ , adjoint de l'opérateur  $\Lambda^{p-k} V^* \rightarrow \Lambda^p V^*$  tel que  $\psi \mapsto \varphi \wedge \psi$ . Si  $(e_1, \dots, e_n)$  et  $(e_1^*, \dots, e_n^*)$  sont des bases de  $V$  et  $V^*$  duales l'une de l'autre, une base de  $\Lambda^p V$  est formée

4. Julius PLÜCKER (1801–1868). — Ses travaux ont porté aussi bien sur les mathématiques (configuration de droites, combinatoire) que la physique (magnétisme, physique atomique, électronique).

des  $e_I = e_{i_1} \wedge \cdots \wedge e_{i_p}$  pour  $I = \{i_1 < i_2 < \cdots < i_p\}$  une partie de  $\{1, \dots, n\}$  à  $p$  éléments. De même pour  $\wedge^p V^*$  et les bases  $(e_I)$  et  $(e_I^*)$  sont duales l'une de l'autre. Alors, on a la formule suivante pour la contraction :

$$\langle e_K^*, \iota(e_J^*)(e_I) \rangle = \langle e_J^* \wedge e_K^*, e_I \rangle = \varepsilon_I JK,$$

où  $\varepsilon_I^{JK}$  vaut 0 si  $I \neq J \cup K$  et vaut la signature de la permutation qui envoie la suite  $I$  sur la suite  $J \cup K$  sinon. Autrement dit,

$$\iota(e_J^*)(e_I) = \sum_K \varepsilon_I^{JK} e_K$$

d'où on déduit que

$$(4.3.4) \quad \begin{aligned} \iota(f_1 \wedge \cdots \wedge f_{p-1})(v_1 \wedge \cdots \wedge v_p) \\ = \sum_{i=1}^p \langle f_1 \wedge \cdots \wedge f_{p-1}, v_1 \wedge \cdots \wedge v_{i-1} \wedge v_{i+1} \wedge \cdots \wedge v_p \rangle v_i. \end{aligned}$$

Autrement dit, on a pour tout  $\psi \in \wedge^{p-1} V^*$  et tout  $w \in \wedge^p V$  l'égalité

$$\langle \psi, \iota(\varphi)w \rangle = \langle \varphi \wedge \psi, w \rangle.$$

LEMME 4.3.5. — Soit  $\alpha$  un élément non nul de  $\wedge^p V$ . Il existe un plus petit sous-espace vectoriel  $V_\alpha$  de  $V$  tel que  $\alpha \in \wedge^p V_\alpha$ .

Il admet les deux caractérisations supplémentaires suivantes :

- son orthogonal dans  $V^*$  est égal à l'espace vectoriel  $V_\alpha^*$  des  $f \in V^*$  tels que  $\iota(f)(\alpha) = 0$  ;
- c'est l'image de l'application linéaire  $\wedge^{p-1} V^* \rightarrow V$  donnée par  $\varphi \mapsto \iota(\varphi)(\alpha)$ .

*Démonstration.* — Soit  $V_\alpha$  l'intersection des sous-espaces vectoriels  $W$  de  $V$  tels que  $\alpha \in \wedge^p W$ . Si  $W$  et  $W'$  sont deux sous-espaces vectoriels de  $V$ , on constate en prenant une base de  $W \cap W'$  et en la complétant en des bases de  $W$  (resp.  $W'$ ) que  $\wedge^p(W \cap W') = \wedge^p W \cap \wedge^p W'$ . Par suite,  $\alpha$  appartient à  $\wedge^p V_\alpha$  et  $V_\alpha$  est le plus petit sous-espace vectoriel de  $V$  ayant cette propriété.

Soit  $f$  une forme linéaire sur  $V$ . La définition de l'opérateur de contraction implique que  $\iota(f)(\alpha)$  ne dépend que de la restriction de  $f$  à  $V_\alpha$ . Ainsi, si  $f$  est nulle sur  $V_\alpha$ ,  $\iota(f)(\alpha) = 0$ . Il en résulte que  $V_\alpha^\perp$  est contenu dans le noyau  $V_\alpha^*$  de l'application linéaire  $f \mapsto \iota(f)(\alpha)$ . Par dualité,  $W = (V_\alpha^*)^\perp \subset V_\alpha$ .

Réciproquement, on veut montrer que  $V_\alpha \subset W$ , c'est-à-dire  $\alpha \in \wedge^p W$ . Soit  $U$  un supplémentaire de  $W$  ; on a ainsi une décomposition

$$\wedge^p V = \wedge^p W \oplus \left( \wedge^{p-1} W \otimes U \right) \oplus \cdots \oplus \wedge^p U.$$

On a aussi une décomposition  $V^* = W^* \oplus U^*$ , où  $W^*$  et  $U^*$  sont des formes linéaires sur  $V$  nulles sur respectivement  $U$  et  $W$ . (Par définition de  $W$ , on a  $U^* = \Phi$ .) D'où encore

une décomposition de  $\wedge^p V^*$ . On écrit donc  $\alpha = \sum_{k=0}^p \alpha_k \otimes \beta_k$ , avec  $\alpha_k \in \wedge^{p-k} W \otimes \wedge^k U$ , d'où

$$0 = \iota(\varphi)(\alpha) = \sum_{k=1}^p \alpha_k \otimes \iota(\varphi)(\beta_k).$$

Cela signifie que pour  $k \geq 1$ ,  $\alpha_k \otimes \iota(\varphi)(\beta_k)$  est nul, autrement dit  $\alpha_k = 0$  ou  $\iota(\varphi)(\beta_k) = 0$ . Supposons que  $\alpha_k \neq 0$ . Alors, pour tout  $\varphi \in U^*$ ,  $\iota(\varphi)(\beta_k) = 0$ , et donc, pour tout  $\beta^* \in \wedge^{k-1} U^*$ ,  $\langle \varphi \wedge \beta^*, \beta_k \rangle = 0$ . Par suite,  $\beta_k = 0$ . Ainsi,  $\alpha \in \wedge^p W$ .

Par dualité, l'autre caractérisation résulte du fait que les applications linéaires

$$V^* \rightarrow \wedge^{p-1} V, \quad f \mapsto \iota(f)(\alpha)$$

et

$$\wedge^{p-1} V^* \rightarrow V, \quad \varphi \mapsto \iota(\varphi)(\alpha)$$

sont (au signe près) transposées l'une de l'autre. □

**PROPOSITION 4.3.6.** — *Soit  $\alpha$  un élément non nul de  $\wedge^p V$ . Les conditions suivantes sont équivalentes :*

- (i)  $\alpha$  est décomposable ;
- (ii)  $\dim V_\alpha = p$  ;
- (iii) pour tout  $\beta \in V_\alpha$ ,  $\beta \wedge \alpha = 0$  ;
- (iv) pour tout  $\varphi \in \wedge^{p-1} V^*$ ,  $\iota(\varphi)(\alpha) \wedge \alpha = 0$ .

*Démonstration.* — Les conditions (i) et (ii) sont trivialement équivalentes et impliquent visiblement (iii).

Réciproquement, si  $d = \dim V_\alpha > p$ , l'accouplement  $\wedge^p W \otimes \wedge^{d-p} W \rightarrow \wedge^d W \simeq k$  est non dégénéré. Par suite, il existe un  $d - p$ -vecteur  $\beta \in \wedge^{d-p} W$  tel que  $\alpha \wedge \beta \neq 0$ , et donc un vecteur  $w \in W$  tel que  $\alpha \wedge w \neq 0$ .

D'après le lemme précédent,  $V_\alpha$  est égal à l'ensemble des  $\iota(\varphi)(\alpha)$ , d'où l'équivalence de (iii) et (iv). □

Lorsque  $\varphi$  parcourt une base de  $\wedge^{p-1} V^*$ , on obtient ainsi une famille de  $\dim \wedge^{p-1} V^* = \binom{n}{p-1}$  équations quadratiques en les coordonnées de  $\alpha$  qui sont satisfaites si et seulement si  $\alpha$  est décomposable. Ces relations sont appelées *relations de Grassmann*.

**4.3.7. Exemple.** — Pour les expliciter un peu plus, donnons-nous une base  $(e_1, \dots, e_n)$  de  $V$ . Les formules ci-dessus montrent que si  $\alpha = \sum \alpha_I e_I$ ,

$$\langle e_J^*, \iota(e_H^*) \rangle (\alpha) \wedge \alpha = \sum_{i \in J \cap \bar{H}} \varepsilon_{i,H,J} \alpha_{H \cup \{i\}} \alpha_{J \setminus \{i\}}$$

où  $\varepsilon_{i,H,J} = 1$  si le nombre d'éléments de  $J$  qui sont  $< i$  et le nombre d'éléments de  $H$  qui sont  $< i$  ont même parité, et vaut  $-1$  dans le cas contraire.

La grassmannienne la plus simple qui n'est pas un espace projectif est  $G_{2,4}$  (2-plans de  $k^4$ ). Le plongement de Plücker l'identifie à l'hypersurface d'équation

$$z_{12}z_{34} - z_{13}z_{24} + z_{14}z_{23} = 0$$

dans  $\mathbf{P}^5$  dont les coordonnées homogènes sont indexées par les parties à deux éléments de  $\{1, 2, 3, 4\}$ .

#### 4.4. Quotients

Soit  $X$  une variété algébrique et  $G$  un groupe fini agissant sur  $X$  par des automorphismes de variétés algébriques. Autrement dit, pour  $g \in G$ , on se donne un morphisme de variétés algébriques  $\rho(g) : X \rightarrow X$  et on suppose que  $\rho(1) = \text{id}$  et  $\rho(gg') = \rho(g) \circ \rho(g')$ . On notera  $g \cdot x = \rho(g)(x)$ . On veut définir un quotient de  $X$  par  $G$ .

**DÉFINITION 4.4.1.** — *On dit qu'un couple  $(Y, p)$  formé d'une variété algébrique  $Y$  et d'un morphisme  $p : X \rightarrow Y$  est un quotient de  $X$  par (l'action de)  $G$  si :*

1.  $p$  est  $G$ -invariant : pour tout  $x \in X$  et tout  $g \in G$ ,  $p(g \cdot x) = p(x)$  ;
2. pour tout morphisme  $G$ -invariant  $\varphi : X \rightarrow W$ , il existe un unique morphisme  $\tilde{\varphi} : Y \rightarrow W$  tel que  $\varphi = \tilde{\varphi} \circ p$ .

(Cette définition est la définition générale du quotient dans une catégorie.)

**LEMME 4.4.2.** — *Si  $p : X \rightarrow Y$  et  $p' : X \rightarrow Y'$  sont deux quotients de  $X$ , il existe un unique isomorphisme  $\varphi : Y \rightarrow Y'$  tel que  $p' = \varphi \circ p$ .*

*Démonstration.* — Comme  $p'$  est  $G$ -invariant et  $p : X \rightarrow Y$  un quotient de  $X$ , il existe un unique morphisme  $\varphi : Y \rightarrow Y'$  tel que  $p' = \varphi \circ p$ . De même, il existe un unique morphisme  $\psi : Y' \rightarrow Y$  tel que  $p = \psi \circ p'$ . Alors,  $p' = \varphi \circ p = (\varphi \circ \psi) \circ p'$  et comme  $p'$  est un quotient, on a nécessairement  $\varphi \circ \psi = \text{id}_{Y'}$ . De même,  $\psi \circ \varphi = \text{id}_Y$ . Ainsi,  $\varphi$  et  $\psi$  sont des isomorphismes réciproques l'un de l'autre et le lemme est démontré.  $\square$

Si  $G$  agit sur  $X$ , il agit aussi sur  $\Gamma(X, \mathcal{O}_X)$  par la formule : si  $f \in \Gamma(X, \mathcal{O}_X)$  et  $g \in G$ , on pose  $g \cdot f$  la fonction  $x \mapsto f(g^{-1} \cdot x)$ .

On a alors la proposition :

**PROPOSITION 4.4.3.** — *Soit  $p : X \rightarrow Y$  un quotient. Par l'homomorphisme  $p^*$ ,  $\Gamma(Y, \mathcal{O}_Y)$  est isomorphe à l'anneau  $\Gamma(X, \mathcal{O}_X)^G$  des fonctions régulières sur  $X$  qui sont  $G$ -invariantes.*

*Démonstration.* — Soit  $f \in \Gamma(Y, \mathcal{O}_Y)$ . Si  $g \in G$  et  $x \in X$ ,

$$g \cdot (f \circ p)(x) = (f \circ p)(g^{-1} \cdot x) = f(x)$$

donc  $f \circ p = p^*(f) \in \Gamma(X, \mathcal{O}_X)^G$ .

Soit réciproquement  $f \in \Gamma(X, \mathcal{O}_X)^G$  de sorte que  $f$  définit un morphisme  $\varphi : X \rightarrow \mathbf{A}^1$  qui est  $G$ -invariant. Ainsi, il existe un unique  $\tilde{\varphi} : Y \rightarrow \mathbf{A}^1$  tel que  $\varphi = \tilde{\varphi} \circ p$ . La fonction régulière  $\tilde{f}$  sur  $Y$  donnée par  $\tilde{\varphi}$  est ainsi l'unique fonction régulière sur  $Y$  telle que  $f = f \circ p = p^*(\tilde{f})$ .  $\square$

Lorsque  $X$  est une variété algébrique affine, un point crucial pour l'existence du quotient de  $X$  par  $G$  est le théorème suivant.

**THÉORÈME 4.4.4 (Noether).** — *Soient  $k$  un corps,  $A$  une  $k$ -algèbre de type fini et  $G$  un groupe fini agissant sur  $A$  par des automorphismes de  $k$ -algèbres. Alors,  $A^G$  est une  $k$ -algèbre de type fini.*

*Remarque 4.4.5.* — Lorsque le groupe  $G$  n'est pas fini, la situation est beaucoup plus subtile et fait l'objet de la théorie des invariants.

*Démonstration.* — Si  $a \in A$ , le polynôme  $P(X) = \prod (X - g \cdot a) \in A[X]$  est  $G$ -invariant. Ses coefficients sont donc des éléments de  $A^G$ . Comme  $P$  est unitaire et comme  $P(a) = 0$ ,  $a$  est entier sur  $A^G$ . Il en résulte que  $A$  est entière sur  $A^G$ . Comme  $A$  est une  $k$ -algèbre de type fini sur  $k$ ,  $A$  est *a fortiori* de type fini sur  $A^G$ . Étant entière,  $A$  est un  $A^G$ -module de type fini. Le théorème résulte alors du lemme suivant.  $\square$

**LEMME 4.4.6 (Artin–Tate).** — *Soient  $k \subset A \subset B$  trois anneaux. On suppose que  $k$  est noethérien, que  $B$  est une  $k$ -algèbre de type fini et que  $B$  est un  $A$ -module de type fini. Alors,  $A$  est une  $k$ -algèbre de type fini.*

*Démonstration.* — Soient  $(x_i)_{1 \leq i \leq n}$  une famille finie de générateurs de  $B$  comme  $k$ -algèbre et  $(b_j)_{1 \leq j \leq m}$  une famille finie de générateurs de  $B$  comme  $A$ -module. IL existe alors des  $\lambda_{ij} \in A$  tels que  $x_i = \sum_j \lambda_{ij} b_j$  et des  $\mu_{ijk} \in A$  tels que  $b_i b_j = \sum_k \mu_{ijk} b_k$ . Soit  $A_0$  la sous  $k$ -algèbre de  $A$  engendrée par les  $\lambda_{ij}$  et les  $\mu_{ijk}$ . C'est une  $k$ -algèbre de type fini, donc un anneau noethérien.

Alors le  $A_0$ -sous-module de  $B$  engendré par les  $b_j$  est une  $k$ -algèbre et contient les  $x_i$ . Ainsi,  $B = A_0 \langle b_j \rangle$ . En particulier,  $B$  est un  $A_0$ -module de type fini. Comme  $A_0$  est noethérien, tout sous- $A_0$ -module de  $B$  est de type fini et en particulier,  $A$  est un  $A_0$ -module de type fini et *a fortiori* une  $A_0$ -algèbre de type fini.

Comme  $A_0$  est une  $k$ -algèbre de type fini,  $A$  est ainsi une  $k$ -algèbre de type fini et le lemme est démontré.  $\square$

**COROLLAIRE 4.4.7.** — *Si  $X$  est une variété algébrique affine, il existe un quotient  $p : X \rightarrow X/G$  de  $X$  par  $G$ . La variété algébrique  $X/G$  est affine d'anneau  $\mathcal{A}(X)^G$  et le morphisme  $X \rightarrow X/G$  est fini et surjectif.*

*Démonstration.* — Soit  $Z$  une variété algébrique et  $\varphi : X \rightarrow Z$  un morphisme  $G$ -invariant.

On prouve tout d'abord qu'il existe une famille finie de couples  $(f_i, U_i)$  où  $f_i \in \mathcal{A}(X)^G$  et  $U_i$  est un ouvert affine de  $Z$  contenant  $\varphi(D(f_i))$ .

On part en effet d'un recouvrement ouvert affine  $(U_i)$  de  $Z$ . Pour tout  $i$ ,  $\varphi^{-1}(U_i)$  est un ouvert de  $X$  stable par  $G$  auquel on applique le lemme suivant.

LEMME 4.4.8. — *Pour tout ouvert  $U$  de  $X$  qui est stable par  $G$ , il existe une famille  $(f_1, \dots, f_r)$  d'éléments de  $\mathcal{A}(X)^G$  telle que  $U = \bigcup D(f_i)$ .*

*Preuve du lemme.* — Soit  $Z = X \setminus U$ . Soit  $x \in U$ . Comme  $U$  est stable par  $G$ , les  $g \cdot x$  appartiennent à  $U$  pour tout  $g \in G$ . D'après le lemme d'évitement des idéaux premiers 1.1.2, il existe  $f_x \in \mathcal{I}(Z)$  tel que pour tout  $g$ ,  $f(g \cdot x) \neq 0$ . Quitte à remplacer  $f_x$  par  $\prod_g (g \cdot f_x)$ , on peut supposer que  $f_x \in \mathcal{A}(X)^G$ . Alors,  $D(f_x) \subset U$  et  $x \in D(f_x)$ . Comme  $U = \bigcup_{x \in U} D(f_x)$  et que l'espace topologie sous-jacent à variété algébrique est quasi-compact, on peut en extraire un sous-recouvrement fini. (*Fin de la preuve du lemme*)

Alors,  $\varphi_i = \varphi|_{D(f_i)} : D(f_i) \rightarrow U_i$  correspond à un morphisme de  $k$ -algèbres

$$\varphi_i^* : \mathcal{A}(U_i) \rightarrow \mathcal{A}(D(f_i)) = \mathcal{A}(X)[1/f_i].$$

Comme  $\varphi$  est  $G$ -invariant, l'image de  $\varphi_i^*$  est alors contenue dans le sous-anneau

$$(\mathcal{A}(X)[1/f_i])^G = (\mathcal{A}(X))^G[1/f_i],$$

si bien que  $\varphi_i$  se factorise de manière unique par un morphisme  $\tilde{\varphi}_i : D(f_i) \rightarrow Z$ , où  $D(f_i)$  est considéré comme un ouvert de  $X/G$ , tel que  $\varphi_i = \tilde{\varphi}_i \circ p$ .

Comme les  $\tilde{\varphi}_i$  sont uniques, ils coïncident nécessairement sur  $D(f_i) \cap D(f_j) = D(f_{ij})$ , d'où finalement un unique morphisme  $\tilde{\varphi} : X/G \rightarrow Z$  tel que  $\varphi = \tilde{\varphi} \circ p$ .  $\square$

Il nous reste à constater que les points de  $X/G$  sont en bijection avec les orbites de  $G$  dans  $X$ . Un cas particulier de la proposition suivante est souvent prouvé dans les cours de théorie de Galois.

PROPOSITION 4.4.9. — *Soient  $A$  un anneau,  $G$  un groupe fini agissant sur  $A$  et  $A^G$  l'anneau des éléments  $G$ -invariants. Si  $\mathfrak{q}$  est un idéal premier de  $A^G$ , les idéaux premiers de  $A$  au-dessus de  $\mathfrak{q}$  sont conjugués par  $G$ .*

*En particulier, si  $p : X \rightarrow X/G$  est le quotient d'une variété algébrique affine par l'action d'un groupe fini  $G$ ,  $p$  induit une bijection entre les  $G$ -orbites de points de  $X$  et les points de  $X/G$ .*

*Démonstration.* — On commence par remarquer que  $A$  est entière sur  $A^G$ . Soient  $\mathfrak{p}$  et  $\mathfrak{p}'$  deux idéaux premiers de  $A$  au-dessus de  $\mathfrak{q}$ . On veut prouver qu'il existe  $g \in G$  tel que  $\mathfrak{p}' = g \cdot \mathfrak{p}$ .

Évariste GALOIS (1811–1832)

*Créateur de la théorie qui porte désormais son nom, Galois sut développer la théorie des groupes en elle-même pour résoudre le problème de la résolution des équations par radicaux. Son œuvre fulgurante s'acheva à l'âge de 21 ans par un suicide en forme de duel...*



Soit  $a \in \mathfrak{p}'$ ,  $b = \prod_{g \in G} g \cdot a$ . Alors,  $b \in A^G \cap \mathfrak{p}' = \mathfrak{q} = A^G \cap \mathfrak{p}$ , donc  $b \in \mathfrak{p}$ . Comme  $\mathfrak{p}$  est premier, l'un des  $g \cdot a$  appartient à  $\mathfrak{p}$  et on a l'inclusion

$$\mathfrak{p}' \subset \bigcup_{g \in G} g \cdot \mathfrak{p}.$$

D'après le lemme d'évitement 1.1.2, il existe  $g \in G$  tel que  $\mathfrak{p}' \subset g \cdot \mathfrak{p}$ . Le théorème de Cohen–Seidenberg 5.1.6 implique alors que  $\mathfrak{p}' = g \cdot \mathfrak{p}$ .

Pour le cas particulier, on rappelle que  $p : X \rightarrow X/G$  est surjective. D'autre part, si  $p(x) = p(x')$ , la première partie de la proposition implique que  $x$  et  $x'$  sont dans la même orbite sous  $G$ , autrement dit,  $p^{-1}(p(x))$  est l'orbite de  $x$  par  $G$ .  $\square$



## CHAPITRE 5

# THÉORIE LOCALE DES VARIÉTÉS ALGÈBRIQUES

### 5.1. Dimension

DÉFINITION 5.1.1. — Soit  $Z$  une variété algébrique. On appelle dimension de  $Z$  la borne supérieure des longueurs des chaînes de fermés irréductibles  $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \subset Z$ .

LEMME 5.1.2. — La dimension d'une variété algébrique est le maximum des dimensions de ses composantes irréductibles.

*Démonstration.* — C'est clair, toute chaîne étant contenue dans un fermé irréductible maximal, c'est-à-dire une composante irréductible.  $\square$

DÉFINITION 5.1.3. — Soit  $A$  un anneau. On appelle dimension de Krull de  $A$  la borne supérieure des longueurs des chaînes  $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$  d'idéaux premiers de  $A$ .

Il résulte de la correspondance entre ensembles algébriques affines irréductibles et idéaux premiers (théorème des zéros de Hilbert) le lemme :

LEMME 5.1.4. — Si  $Z$  est une variété algébrique affine,  $\dim Z = \dim \mathcal{A}(Z)$ .

*Remarque 5.1.5.* — Il n'est pas clair à ce point du cours que la dimension d'une variété algébrique soit finie ; dans le cas d'une variété algébrique affine, c'est une conséquence du théorème 5.1.9 qui est le résultat principal de ce paragraphe. Le mathématicien japonais Nagata a même donné des exemples d'anneaux noethériens de dimension infinie.

THÉORÈME 5.1.6 (Cohen–Seidenberg). — Soient  $A \subset B$  deux anneaux, avec  $B$  entier sur  $A$ .

a) Soient  $\mathfrak{q}$  un idéal premier de  $B$  et  $\mathfrak{p} = \mathfrak{q} \cap A$ . Alors  $\mathfrak{p}$  est maximal si et seulement si  $\mathfrak{q}$  est maximal.

b) Soient  $\mathfrak{q} \subset \mathfrak{q}'$  deux idéaux premiers de  $B$  tels que  $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ . Alors,  $\mathfrak{q} = \mathfrak{q}'$ .

c) Pour tout idéal premier  $\mathfrak{p}$  de  $A$ , il existe un idéal premier  $\mathfrak{q}$  de  $B$  tel que  $\mathfrak{q} \cap A = \mathfrak{p}$ .

Wolfgang KRULL (1899–1971)

*Ses contributions en algèbre commutative sont aujourd'hui inévitables : invention des anneaux locaux, de la dimension, étude des algèbres entières et notamment une première étude du relèvement des idéaux premiers dans une extension entière, mais aussi théorie de Galois des extensions infinie, théorie des valuations, etc.*



**COROLLAIRE 5.1.7.** — Soient  $A \subset B$  deux anneaux avec  $B$  entier sur  $A$ . Alors,  $A$  et  $B$  ont même dimension.

*Démonstration.* — a) on a une inclusion d'anneaux intègres  $A/\mathfrak{p} \subset B/\mathfrak{q}$  et  $B/\mathfrak{q}$  est entier sur  $A/\mathfrak{p}$ . D'après le lemme 1.5.2,  $A/\mathfrak{p}$  est un corps si et seulement si  $B/\mathfrak{q}$  est un corps. Cela revient à dire que  $\mathfrak{p}$  est maximal si et seulement si  $\mathfrak{q}$  est maximal.

b) Notons  $\mathfrak{p} = \mathfrak{q} \cap A$  et localisons par rapport à la partie multiplicative  $A \setminus \mathfrak{p}$ , d'où une inclusion entière d'anneaux  $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ . Comme  $\mathfrak{q}B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{q}'B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$  est maximal,  $\mathfrak{q}B_{\mathfrak{p}}$  et  $\mathfrak{q}'B_{\mathfrak{p}}$  sont tous deux maximaux, et par conséquent égaux. Il en résulte  $\mathfrak{q} = \mathfrak{q}'$  puisque l'application  $\mathfrak{q} \mapsto \mathfrak{q}B_{\mathfrak{p}}$  définit une bijection de l'ensemble des idéaux premiers de  $B$  ne rencontrant pas  $\mathfrak{p}$  sur l'ensemble des idéaux premiers de  $B_{\mathfrak{p}}$ .

c) Localisons par rapport à la partie multiplicative  $A \setminus \mathfrak{p}$ . D'après a), l'intersection de tout idéal maximal de  $B_{\mathfrak{p}}$  avec  $A_{\mathfrak{p}}$  est égale à l'unique idéal maximal  $\mathfrak{p}A_{\mathfrak{p}}$  de  $A_{\mathfrak{p}}$ . Un tel idéal est de la forme  $\mathfrak{q}B_{\mathfrak{p}}$  pour un idéal premier  $\mathfrak{q}$  de  $B$ . On a alors  $\mathfrak{q}B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ , d'où l'on déduit que  $\mathfrak{p} = \mathfrak{q} \cap A$ . En effet, si  $b \in \mathfrak{q} \cap A$ ,  $b/1 \in \mathfrak{q}B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ ; il existe donc  $a \in A \setminus \mathfrak{p}$  tel que  $ab \in \mathfrak{p}$ , d'où  $b \in \mathfrak{p}$  puisque  $\mathfrak{p}$  est premier. Réciproquement, si  $a \in \mathfrak{p}$ ,  $a/1 \in \mathfrak{q}B_{\mathfrak{p}}$ , ce qui implique qu'il existe  $a' \in A \setminus \mathfrak{p}$  tel que  $aa' \in \mathfrak{q}$ . Comme  $a' \notin \mathfrak{p}$ ,  $a' \notin \mathfrak{q}$  et,  $\mathfrak{q}$  étant premier,  $a \in \mathfrak{q}$ .  $\square$

*Preuve du corollaire.* — Soit  $\mathfrak{q}_0 \subsetneq \dots \subsetneq \mathfrak{q}_n$  une chaîne d'idéaux premiers de  $B$ . En prenant les intersections avec  $A$ , on obtient d'après le théorème 5.1.6, b), une chaîne d'idéaux premiers  $(\mathfrak{q}_0 \cap A) \subsetneq \dots \subsetneq (\mathfrak{q}_n \cap A)$  de  $A$ , ce qui implique  $\dim A \geq \dim B$ .

Réciproquement, soit  $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n$  une chaîne d'idéaux premiers de  $A$  et montrons qu'il existe une chaîne  $\mathfrak{q}_0 \subsetneq \dots \subsetneq \mathfrak{q}_n$  d'idéaux premiers de  $B$  telle que  $\mathfrak{q}_r \cap A = \mathfrak{p}_r$ . Choisissons un idéal premier  $\mathfrak{q}_0$  de  $B$  tel que  $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$ , ce qui est possible d'après le c) du théorème 5.1.6. Soit alors  $r < n$  et supposons avoir construit  $\mathfrak{q}_0, \dots, \mathfrak{q}_r$  par récurrence. On applique alors le même résultat à l'inclusion  $A/\mathfrak{p}_r \subset B/\mathfrak{q}_r$  et à l'idéal premier  $\mathfrak{p}_{r+1}(A/\mathfrak{p}_r)$  de  $A/\mathfrak{p}_r$ . Ainsi,  $\dim B \geq \dim A$ .  $\square$

**THÉORÈME 5.1.8** (Lemme de normalisation de Noether). — *Soit  $k$  un corps,  $A$  une  $k$ -algèbre intègre de type fini. Il existe des éléments  $x_1, \dots, x_n \in A$  algébriquement indépendants sur  $k$  tels que  $A$  soit entier sur  $k[x_1, \dots, x_n]$ .*

Avec ces notations,  $n$  n'est autre que le *degré de transcendance* du corps des fractions de  $A$  sur  $k$ .

*Démonstration.* — Soient  $y_1, \dots, y_m$  des éléments de  $A$  qui engendrent  $A$  comme  $k$ -algèbre. S'ils sont algébriquement indépendants, le lemme de normalisation est démontré.

Supposons donc qu'ils sont algébriquement dépendants et soit  $P \in k[Y_1, \dots, Y_m]$  un polynôme non nul tels que  $P(y_1, \dots, y_m) = 0$ . On va montrer que l'on peut choisir des entiers  $r_i \geq 1$  pour  $i \geq 2$  de sorte que  $A$  est entière sur la sous-algèbre de  $A$  engendrée par les  $z_i = y_i - y_1^{r_i}$ . En effet, si  $P = \sum_{\mathbf{n}=(n_i)} a_{\mathbf{n}} \prod_i Y_i^{n_i}$ , on a

$$\begin{aligned} 0 = P(y_1, \dots, y_m) &= P(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = \sum_{\mathbf{n}} a_{\mathbf{n}} y_1^{n_1} \prod_{i=2}^m (z_i + y_1^{r_i})^{n_i} \\ &= \sum_{\mathbf{n}} \sum_{j_2=0}^{n_2} \dots \sum_{j_m=0}^{n_m} a_{\mathbf{n}} \prod_{i \geq 2} \binom{n_i}{j_i} y_1^{n_1 + \sum j_i r_i} \prod_{i \geq 2} z_i^{n_i - j_i}. \end{aligned}$$

Soit  $k$  un entier strictement plus grand que le degré de  $P$  en chaque variable et posons  $r_i = k^i$ . Ainsi, les sommes  $n_1 + \sum j_i r_i$  sont toutes distinctes et l'équation précédente fournit une relation de dépendance algébrique pour  $y_1$  donc les coefficients sont dans  $k[z_2, \dots, z_m]$  et dont le coefficient de plus haut degré est nécessairement obtenu pour  $j_i = n_i$ , donc est un coefficient non nul de  $P$ , donc inversible. Cela prouve que  $y_1$  est entier sur  $k[z_2, \dots, z_m]$ . Puis, si  $i \geq 2$ ,  $y_i = z_i + y_1^{r_i}$  est aussi entier sur  $k[z_2, \dots, z_m]$ . Par conséquent,  $A$  est entière sur  $k[z_2, \dots, z_m]$ .

Par récurrence, il existe des éléments  $x_1, \dots, x_n \in k[z_2, \dots, z_m]$  algébriquement indépendants et tels que  $k[z_2, \dots, z_m]$  est entière sur  $k[x_1, \dots, x_n]$ . Il en résulte que  $A$  est entière sur  $k[x_1, \dots, x_n]$ .  $\square$

**THÉORÈME 5.1.9.** — *Soit  $k$  un corps et  $A$  une  $k$ -algèbre intègre de type fini. On a  $\dim A = \deg \text{tr} A$ . Par suite, la dimension d'une variété algébrique affine est finie.*

*Démonstration* (d'après [?]). — Lorsque le degré de transcendance de  $A$  sur  $k$  est nul, tout élément de  $A$  est algébrique sur  $k$ , donc entier. Ainsi,  $A$  est un corps et  $\dim A = 0$ .

On démontre alors le théorème par récurrence sur le degré de transcendance de  $A$  sur  $k$ . D'après le lemme de normalisation 5.1.8,  $A$  est entière sur une sous-algèbre  $k[x_1, \dots, x_n]$  isomorphe à l'algèbre de polynômes  $k[X_1, \dots, X_n]$ . D'après le théorème de Cohen–Seidenberg 5.1.6, on a  $\dim A = \dim k[x_1, \dots, x_n] = \dim k[X_1, \dots, X_n]$ . D'autre part,  $A$  étant entière sur  $k[x_1, \dots, x_n]$ , ces deux algèbres ont même degré de transcendance  $n$ . Il

suffit ainsi de prouver que  $\dim k[X_1, \dots, X_n] = n$ , résultat qui mérite d'avoir son numéro à lui, puisqu'il signifie que l'espace affine  $\mathbf{A}^n$  est de dimension  $n$ .  $\square$

THÉORÈME 5.1.10. — *Soit  $k$  un corps. La dimension de  $k[X_1, \dots, X_n]$  est égale à  $n$ .*

*Preuve* (en supposant démontré le théorème 5.1.9 en dimension  $< n$ )

La chaîne d'idéaux premiers

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \dots \subset (X_1, \dots, X_n)$$

prouve que  $\dim k[X_1, \dots, X_n] \geq n$ . Considérons une chaîne d'idéaux premiers  $(0) \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_r$  de  $k[X_1, \dots, X_n]$ .

Considérons la  $k$ -algèbre intègre  $A' = k[X_1, \dots, X_n]/\mathfrak{p}_1$ . Comme  $\mathfrak{p}_1 \neq (0)$ , il existe une relation de dépendance algébrique non triviale entre les images  $x_i$  des  $X_i$  dans  $A'$ . Cela implique que l'un des  $x_i$ , disons  $x_n$  est algébrique sur le corps des fractions de la sous-algèbre  $k[x_1, \dots, x_{n-1}] \subset A'$  qui est de degré de transcendance  $\leq n-1$ . Ainsi, le degré de transcendance de  $A'$  est  $\leq n-1$ . D'autre part, sa dimension est au moins  $r-1$ . Par récurrence, on obtient  $r-1 \leq \dim A' \leq \deg \text{tr} A' \leq n-1$  d'où  $r \leq n$ . Ainsi,  $\dim k[X_1, \dots, X_n] \leq n$ , d'où finalement l'égalité voulue.  $\square$

COROLLAIRE 5.1.11. — *Soit  $X$  une variété algébrique irréductible. On a  $\dim X = \deg \text{tr} k(X)$ .*

*Démonstration.* — En effet, soit  $Z_0 \subsetneq \dots \subsetneq Z_r$  une chaîne de fermés irréductibles de  $X$ . Si  $U$  est un ouvert affine non vide de  $X$  tel que  $Z_0 \cap U \neq \emptyset$ , on en déduit en intersectant avec  $U$  une chaîne de fermés irréductibles de  $U$ , d'où l'inégalité

$$r \leq \dim U = \deg \text{tr} k(U) = \deg \text{tr} k(X).$$

Par suite,  $\dim X \leq \deg \text{tr} k(X)$ .

Réciproquement, soit  $U$  un ouvert affine non vide de  $X$ . Choisissons une chaîne  $Z_0 \subsetneq \dots \subsetneq Z_r$  de fermés irréductibles de  $U$ , avec  $r = \dim U$ . Alors,  $\overline{Z_0} \subsetneq \dots \subsetneq \overline{Z_r}$  est une chaîne de fermés irréductibles de  $X$ , d'où l'inégalité  $\dim X \geq \dim U = \deg \text{tr} k(X)$ .  $\square$

*Exercice 5.1.12.* — Dédurre du théorème de Cohen–Seidenberg et du lemme de normalisation de Noether le théorème des zéros de Hilbert (sous sa forme 3.1.11).

THÉORÈME 5.1.13. — *Soient  $X$  et  $Y$  deux variétés algébriques irréductibles. Alors,  $\dim(X \times Y) = \dim X + \dim Y$ .*

*Démonstration.* — Soient  $U$  et  $V$  deux ouverts affines non vides de  $X$  et  $Y$  respectivement. Ainsi,  $U$  est dense dans  $X$  et  $V$  est dense dans  $Y$  si bien que  $\dim U = \dim X$ ,  $\dim V = \dim Y$ . De plus,  $U \times V$  est dense dans  $X \times Y$ , et donc  $\dim(U \times V) = \dim(X \times Y)$ . Nous sommes ainsi ramenés au cas où  $X$  et  $Y$  sont affines.

D'après le lemme de normalisation de Noether 5.1.8 il existe un sous-anneau de  $\mathcal{A}(U)$  isomorphe à l'anneau  $k[X_1, \dots, X_n]$  des polynômes en  $n$  variables sur lequel  $\mathcal{A}(U)$  est

entier ; de même,  $\mathcal{A}(V)$  est entier sur un sous-anneau isomorphe à l'anneau des polynômes en  $m$  variables. Alors, on constate que  $\mathcal{A}(U \times V) = \mathcal{A}(U) \otimes_k \mathcal{A}(V)$  est entier sur  $k[X_1, \dots, X_n] \otimes_k k[Y_1, \dots, Y_m] = k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ . D'après le corollaire 5.1.6 au théorème de Cohen–Seidenberg, on a  $n = \dim U$ ,  $m = \dim V$  et  $n + m = \dim(U \times V)$ .  $\square$

On peut reformuler le théorème de Cohen–Seidenberg à l'aide de la notion suivante :

**DÉFINITION 5.1.14.** — Soit  $f : X \rightarrow Y$  un morphisme de variétés algébriques affines. On dit que  $f$  est fini si par l'homomorphisme de  $k$ -algèbres  $f^* : \mathcal{A}(Y) \rightarrow \mathcal{A}(X)$ ,  $\mathcal{A}(X)$  est entier sur  $\mathcal{A}(Y)$ .

Les morphismes finis vérifient les propriétés suivantes :

**PROPOSITION 5.1.15.** — Soit  $f : X \rightarrow Y$  un morphisme fini de variétés algébriques affines irréductibles.

- a) L'image d'un fermé de  $X$  par  $f$  est fermé dans  $Y$ .
- b)  $f$  est surjectif si et seulement si l'homomorphisme  $f^* : \mathcal{A}(Y) \rightarrow \mathcal{A}(X)$  est injectif.
- c) Pour tout  $y \in Y$ ,  $f^{-1}(y)$  est un ensemble fini.

Alors, le lemme de normalisation 5.1.8 prend la forme géométrique suivante :

**THÉORÈME 5.1.16 (Lemme de normalisation, forme géométrique)**

Si  $X$  est une variété algébrique affine irréductible, il existe un entier  $n \geq 0$  et un morphisme fini surjectif  $f : X \rightarrow \mathbf{A}^n$ .

*Preuve de la proposition.* — a) Soit  $I$  un idéal de  $\mathcal{A}(X)$ . Prouvons que l'image par  $f$  de  $\mathcal{V}(I)$  est fermée dans  $Y$ . Par la bijection entre idéaux maximaux et points,  $\mathcal{V}(I)$  correspond aux idéaux maximaux de  $\mathcal{A}(X)$  contenant  $I$ . Considérons l'homomorphisme injectif

$$\mathcal{A}(Y)/(f^*)^{-1}(I) \hookrightarrow \mathcal{A}(X)/I$$

induit par  $f^*$ . Cet homomorphisme est donc entier, ce qui permet d'appliquer le théorème de Cohen–Seidenberg 5.1.6 : les idéaux maximaux de  $\mathcal{A}(Y)/(f^*)^{-1}(I)$  sont les  $(f^*)^{-1}(\mathfrak{m})$  pour un idéal maximal  $\mathfrak{m}$  de  $\mathcal{A}(X)/I$ . Autrement dit, lorsque  $\mathfrak{m}$  décrit les idéaux maximaux de  $\mathcal{A}(X)$  contenant  $I$ ,  $(f^*)^{-1}(\mathfrak{m})$  décrit exactement l'ensemble des idéaux maximaux de  $\mathcal{A}(Y)$  contenant  $(f^*)^{-1}(I)$ . On a ainsi prouvé que

$$f(\mathcal{V}(I)) = \mathcal{V}((f^*)^{-1}(I)),$$

ce qui prouve que l'image d'un fermé est un fermé.

b) En appliquant le a) à  $I = 0$ , on voit que  $f(X) = \mathcal{V}(\ker f^*)$ . Ainsi,  $f$  est surjectif si et seulement si  $\mathcal{V}(\ker f^*) = Y$ , c'est-à-dire  $\sqrt{\ker f^*} = (0)$ , donc  $\ker f^* = (0)$  puisque  $\mathcal{A}(Y)$  est intègre.

c) Si  $\mathfrak{n}$  est un idéal maximal de  $\mathcal{A}(Y)$ , il faut montrer que  $\mathcal{A}(X)$  n'a qu'un nombre fini d'idéaux  $\mathfrak{m}$  tels que  $\mathfrak{n} = (f^*)^{-1}(\mathfrak{m})$ . De tels  $\mathfrak{m}$  contiennent  $f^*(\mathfrak{n})\mathcal{A}(X)$ , si bien qu'il suffit de prouver que  $\mathcal{A}(X)/f^*(\mathfrak{n})\mathcal{A}(X)$  n'a qu'un nombre fini d'idéaux maximaux. Or,

$\mathcal{A}(X)/f^*(\mathfrak{n})\mathcal{A}(X)$  est entière sur  $\mathcal{A}(Y)/\mathfrak{n} = k$ , donc de dimension finie sur  $k$  d'après le théorème des zéros de Hilbert 3.1.11. Le théorème d'Azukizuki implique alors qu'elle a un nombre fini d'idéaux maximaux.  $\square$

*Exercice 5.1.17.* — Lorsque  $k$  est un corps infini, reprendre la démonstration du lemme de normalisation de Noether en montrant que l'on peut effectuer le changement de variables  $z_i = y_i - a_i y_1$  pour des  $a_i \in k$  bien choisis. Si  $X \subset \mathbf{A}^m$  est une variété algébrique de dimension  $n$ , en déduire qu'il existe une projection linéaire  $\mathbf{A}^m \rightarrow \mathbf{A}^n$  telle que la composition  $X \hookrightarrow \mathbf{A}^m \rightarrow \mathbf{A}^n$  est un morphisme fini et surjectif.

## 5.2. Codimension

DÉFINITION 5.2.1. — Soient  $X$  une variété algébrique et  $Y \subset Z$  un fermé irréductible de  $X$ . La codimension de  $Y$  dans  $X$ , notée  $\text{codim}(Y, X)$  est la borne supérieure des entiers  $n$  tels qu'il existe une chaîne de fermés irréductibles

$$Y = Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n \subset X.$$

On voit que la codimension de  $Y$  dans  $X$  est le maximum des codimensions de  $Y$  dans les composantes irréductibles de  $X$  qui contiennent  $Y$ .

DÉFINITION 5.2.2. — Soient  $A$  un anneau et  $\mathfrak{p}$  un idéal premier de  $A$ . On appelle hauteur de  $\mathfrak{p}$ , notée  $\text{ht}(\mathfrak{p})$ , la borne supérieure des entiers  $n$  tels qu'il existe une chaîne d'idéaux premiers

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}.$$

C'est ainsi la dimension de l'anneau local  $A_{\mathfrak{p}}$ .

Si  $X$  est une variété algébrique affine, le dictionnaire entre idéaux premiers de  $\mathcal{A}(X)$  et fermés irréductibles de  $X$  implique l'égalité

$$(5.2.3) \quad \text{codim}(Y, X) = \text{ht}(\mathcal{I}(Y)) \quad \text{dans l'anneau } \mathcal{A}(X).$$

*Remarque 5.2.4.* — Nagata a prouvé que la dimension d'un anneau local noethérien est finie, cf. le théorème 5.3.7. Ainsi, la hauteur d'un idéal premier arbitraire d'un anneau noethérien est finie. Dans notre cas, celui des  $k$ -algèbres de type fini, c'est une conséquence du théorème 5.1.9 puisque par définition  $\text{codim}(Y, X) \leq \dim X$  et  $\text{ht}(\mathfrak{p}) \leq \dim A$ .

Les variétés algébriques affines irréductibles de codimension 1 dans l'espace affine  $\mathbf{A}^n$  sont les hypersurfaces :

PROPOSITION 5.2.5. — Soit  $Z \subset \mathbf{A}^n$  un fermé irréductible de codimension 1. L'idéal  $\mathcal{I}(Z)$  est principal, engendré par un polynôme irréductible de  $k[X_1, \dots, X_n]$ .

*Démonstration.* — Soit  $f \in k[X_1, \dots, X_n]$  un élément non nul quelconque de l'idéal de  $Z$ . Comme  $\mathcal{S}(Z)$  est premier,  $\mathcal{S}(Z)$  contient l'un des facteurs irréductibles de  $f$ , ce qui permet de supposer  $f$  irréductible. Comme  $k[X_1, \dots, X_n]$  est un anneau factoriel, l'idéal  $(f)$  est un idéal premier. L'inclusion  $(0) \subsetneq (f) \subset \mathcal{S}(Z)$  jointe au fait que  $\text{codim}(Z, \mathbf{A}^n) = 1$  implique que  $\mathcal{S}(Z) = (f)$ .  $\square$

*Remarque 5.2.6.* — Ce résultat s'étend en remplaçant  $\mathbf{A}^n$  par toute variété algébrique affine  $X$  telle que  $\mathcal{A}(X)$  est un anneau factoriel.

À l'aide de ce résultat, nous allons établir le lien entre dimension et codimension. Il nous faut tout d'abord expliciter le comportement de la codimension lors d'un morphisme fini.

THÉORÈME 5.2.7 (Deuxième théorème de Cohen-Seidenberg)

*Soient  $A \subset B$  deux anneaux. On suppose que  $B$  est intègre, que  $A$  est intégralement clos et que  $B$  est une  $A$ -algèbre finie (c'est-à-dire entière et de type fini). Si  $\mathfrak{p}_0 \subset \dots \subset \mathfrak{p}_r$  est une chaîne d'idéaux premiers de  $A$  et  $\mathfrak{q}_r$  un idéal premier de  $B$  tel que  $\mathfrak{q}_r \cap A = \mathfrak{p}_r$ , il existe des idéaux premiers  $\mathfrak{q}_0 \subset \dots \subset \mathfrak{q}_{r-1} \subset \mathfrak{q}_r$  tels que pour tout  $i$ ,  $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ .*

*Démonstration.* — Notons  $K$  le corps des fractions de  $A$ ,  $F$  celui de  $B$  et soit  $F'$  une extension finie de  $K$  contenant  $K$  et normale. Soit  $B'$  la clôture intégrale de  $A$  dans  $F'$ . D'après le premier théorème de Cohen-Seidenberg 5.1.6, il existe des idéaux premiers  $\mathfrak{q}'_0 \subset \dots \subset \mathfrak{q}'_r$  de  $B'$  tels que  $\mathfrak{p}_i = \mathfrak{q}'_i \cap A$ . Soit aussi  $\tilde{\mathfrak{q}}_r$  un idéal premier de  $B'$  tel que  $\tilde{\mathfrak{q}}_r \cap B = \mathfrak{q}_r$ .

Comme  $A$  est intégralement clos, le lemme suivant (une variante de la proposition 4.4.9) affirme l'existence d'un automorphisme  $\sigma$  de  $F'$  tel que  $\sigma|_K = \text{id}$  et tel que  $\sigma(\mathfrak{q}'_r) = \tilde{\mathfrak{q}}_r$ . Posons alors pour  $1 \leq i \leq r-1$ ,  $\mathfrak{q}_i = \sigma(\mathfrak{q}'_i) \cap B$ . On a  $\mathfrak{q}_0 \subset \dots \subset \mathfrak{q}_r$  et pour tout  $i$ , on a

$$\mathfrak{q}_i \cap A = \sigma(\mathfrak{q}'_i) \cap B \cap A = \sigma(\mathfrak{q}'_i \cap A) = \sigma(\mathfrak{p}_i) = \mathfrak{p}_i$$

d'où le théorème.  $\square$

LEMME 5.2.8. — *Soit  $K \subset F$  nue extension finie normale de corps. Soit  $A \subset K$  un sous-anneau intégralement clos et  $F$  la clôture intégrale de  $A$  dans  $F$ . Si  $\mathfrak{p}$  est un idéal premier de  $A$ , le groupe  $G$  des automorphismes de  $F$  qui sont l'identité sur  $K$  opère transitivement sur l'ensemble des idéaux premiers  $\mathfrak{q}$  de  $B$  tels que  $\mathfrak{q} \cap A = \mathfrak{p}$ .*

*Démonstration.* — Soient  $\mathfrak{q}$  et  $\mathfrak{q}'$  deux idéaux premiers de  $B$  au-dessus de  $A$ .

Si  $x \in \mathfrak{q}'$ ,  $y = \prod_{\sigma \in G} \sigma(x)$  est un élément de  $F$  invariant par tout élément de  $G$ . La théorie de Galois implique que  $y$  est radiciel sur  $K$ , c'est-à-dire qu'il existe  $q \geq 1$  ( $q = 1$  si  $F/K$  est séparable,  $q$  est une puissance de la caractéristique de  $K$  sinon) tel que  $y^q \in K$ . Comme  $x$  est entier sur  $A$ , tous les  $\sigma(x)$  sont aussi entiers et  $y^q$  est entier sur  $A$ . Comme  $A$  est intégralement clos,  $y^q \in A$  et donc  $y^q \in \mathfrak{q}' \cap A = \mathfrak{p}$ , donc  $y^q \in \mathfrak{q}$ . Comme  $\mathfrak{q}$  est premier, on a ainsi  $y \in \mathfrak{q}$  et il existe  $\sigma \in G$  tel que  $\sigma(x) \in \mathfrak{q}$ . Nous avons ainsi prouvé que  $\mathfrak{q}' \subset \bigcup_{\sigma \in G} \sigma(\mathfrak{q})$ .

Comme  $B$  est intégralement clos, tout  $\sigma \in G$  est tel que  $\sigma(B) = B$ . Les idéaux  $\sigma(\mathfrak{q})$  sont alors des idéaux premiers de  $B$  et d'après le lemme d'évitement des idéaux premiers 1.1.2,  $\mathfrak{q}'$  est contenu dans l'un d'entre eux. Si  $\mathfrak{q}' \subset \sigma(\mathfrak{q})$ , comme  $\mathfrak{q}' \cap A = \mathfrak{q} \cap A = \sigma(\mathfrak{q}) \cap A$ , on a d'après le théorème 5.1.6, b) que  $\mathfrak{q}' = \sigma(\mathfrak{q})$ .

Le lemme est ainsi démontré.  $\square$

**COROLLAIRE 5.2.9.** — *Soit  $A \subset B$  deux anneaux. On suppose que  $B$  est intègre, fini sur  $A$  et que  $A$  est intégralement clos. Alors, pour tout idéal premier  $\mathfrak{q}$  de  $B$ ,  $\text{ht}(\mathfrak{q}) = \text{ht}(\mathfrak{q} \cap A)$ .*

**THÉORÈME 5.2.10.** — *Soit  $X$  une variété algébrique affine irréductible et  $Y \subset X$  un fermé irréductible. On a  $\text{codim}(Y, X) + \dim Y = \dim X$ .*

La version algébrique de ce théorème est la suivante.

**THÉORÈME 5.2.11.** — *Soit  $A$  une  $k$ -algèbre de type fini intègre. Pour tout idéal premier  $\mathfrak{p}$  de  $A$ ,  $\text{ht}(\mathfrak{p}) = \dim A - \dim A/\mathfrak{p}$ .*

*Démonstration.* — L'inégalité  $\text{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p}) \leq \dim A$  est claire (considérer une chaîne d'idéaux premiers contenue dans  $\mathfrak{p}$ , une autre contenant dans  $\mathfrak{p}$  et les mettre bout à bout).

D'après le lemme de normalisation de Noether, il existe  $x_1, \dots, x_n \in A$  algébriquement indépendants tels que  $A$  est entière et de type fini sur  $B = k[x_1, \dots, x_n]$ . Soit  $\mathfrak{q} = \mathfrak{p} \cap B$ . D'après le théorème 5.1.6, on a ainsi  $\dim A = n$  et  $\dim A/\mathfrak{p} = \dim B/\mathfrak{q}$ . D'après le corollaire 5.2.9 au deuxième théorème 5.2.7 de Cohen-Seidenberg, on a aussi  $\text{ht}(\mathfrak{q}) = \text{ht}(\mathfrak{p})$ . Ainsi, il suffit de démontrer le résultat lorsque  $A = k[x_1, \dots, x_n]$ . Par récurrence, il suffit aussi de le vérifier lorsque  $\text{ht}(\mathfrak{p}) = 1$ .

Dans ce cas,  $A$  étant factoriel,  $\mathfrak{p}$  est principal engendré par un polynôme irréductible  $f$  (proposition 5.2.5). Le degré de transcendance de  $k[x_1, \dots, x_n]/(f)$  est alors au moins  $n - 1$  : si  $f$  fait intervenir la variable  $x_n$ ,  $x_1, \dots, x_{n-1}$  sont algébriquement indépendants dans  $A/(f)$ . En effet, toute relation de dépendance  $P(x_1, \dots, x_{n-1}) = 0$  dans  $A/(f)$  signifie que  $P \in (f) \subset k[x_1, \dots, x_n]$  ce qui implique  $P = 0$  si  $\deg_{x_n} f \neq 0$ .

D'après le théorème 5.1.9,  $\dim A/\mathfrak{p} \geq n - 1$ , d'où l'inégalité  $\text{ht}(\mathfrak{p}) + \dim A/\mathfrak{p} \geq n$  et compte tenu de l'autre inégalité, le théorème est démontré.  $\square$

**COROLLAIRE 5.2.12.** — *Soit  $X$  une variété algébrique irréductible. Toutes les chaînes maximales de fermés irréductibles dans  $X$  ont pour longueur  $\dim X$ .*

**LEMME 5.2.13.** — *Si  $U \subset X$  est un ouvert non vide, pour tout fermé  $Z \subset X$  tel que  $Z \cap U \neq \emptyset$ , on a  $\text{codim}(Z, X) = \text{codim}(Z \cap U, U)$ .*

*Démonstration.* — Soient  $Z_1 \subset Z_2$  sont deux fermés irréductibles de  $X$  tels que  $Z_1 \cap U \neq \emptyset$ .

Si  $Z_1 \neq Z_2$ , on a  $Z_1 \cap U \neq Z_2 \cap U$  : dans le cas contraire, on aurait  $Z_2 \subset Z_1 \cup (X \setminus U)$ , d'où,  $Z_2$  étant irréductible et non contenu dans le fermé  $X \setminus U$ ,  $Z_2 \subset Z_1$ , ce qui est faux. Cela implique que  $\text{codim}(Z \cap U, U) \geq \text{codim}(Z, X)$ .

Réciproquement, si  $Z_1 \subset Z_2$  sont deux fermés irréductibles distincts de  $U$ ,  $\bar{Z}_1 \subsetneq \bar{Z}_2$  sont des fermés de  $X$  irréductibles. Il en résulte que  $\text{codim}(Z, X) \geq \text{codim}(Z \cap U, U)$ .  $\square$

*Démonstration du corollaire.* — Considérons une chaîne maximale de fermés irréductibles  $Z_0 \subsetneq \cdots \subsetneq Z_r = X$ . Ainsi,  $Z_0$  est un point  $\{x\}$ ; soit  $U$  un ouvert affine de  $X$  contenant  $x$ . Remarquons que la suite  $Z_0 \cap U \subset \cdots \subset Z_r \cap U$  est une chaîne maximale de fermés irréductibles de  $U$ . Par suite, les théorèmes 5.2.10 et 5.1.9 impliquent les égalités

$$r = \text{codim}(\{x\}, U) = \dim U - \dim \{x\} = \dim U = \deg \text{tr} k(U) = \deg \text{tr} k(X).$$

Le théorème est donc démontré.  $\square$

### 5.3. Systèmes de paramètres

Dans la suite de ce paragraphe, on étudie la dimension des fermés d'une variété algébrique affine définis par  $r$  équations. On commence naturellement par le cas  $r = 1$ .

**THÉORÈME 5.3.1.** — *Soient  $X$  une variété algébrique affine irréductible et  $f \in \mathcal{A}(X)$  un élément non nul. Les composantes irréductibles de  $\mathcal{V}(f)$  sont toutes de codimension 1.*

Ce théorème est la traduction géométrique du théorème algébrique suivant :

**THÉORÈME 5.3.2 (Hauptidealsatz de Krull).** — *Soient  $A$  un anneau noethérien et  $f$  un élément de  $A$ . Les idéaux premiers minimaux de  $A$  parmi ceux contenant  $f$  sont de hauteur  $\leq 1$ .*

*En particulier, si  $f$  n'est pas diviseur de 0,  $f$  n'appartient à aucun idéal premier minimal de  $A$  et les idéaux premiers minimaux de  $A$  contenant  $f$  sont de hauteur exactement 1.*

*Démonstration.* — Soit  $\mathfrak{p}$  un idéal premier minimal parmi ceux qui contiennent  $f$ . Il faut montrer que  $\mathfrak{p}$  est de hauteur 1 dans  $A$ , c'est-à-dire qu'il n'existe pas de chaîne d'idéaux premiers  $\mathfrak{q}' \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$  dans  $A$ .

Quitte à quotienter par  $\mathfrak{q}'$ , on peut supposer  $A$  intègre et il faut ainsi montrer que  $(0)$  est le seul idéal premier de  $A$  contenu dans  $\mathfrak{p}$ . En remplaçant  $A$  par  $A_{\mathfrak{p}}$  et  $f$  par son image dans  $A_{\mathfrak{p}}$ , on peut de plus supposer que  $A$  est local d'idéal maximal  $\mathfrak{p}$ .

Soit ainsi  $\mathfrak{q} \subsetneq \mathfrak{p}$  un idéal premier de  $A$  et montrons que  $\mathfrak{q} = (0)$ . L'hypothèse que  $\mathfrak{p}$  est minimal parmi les idéaux premiers contenant  $f$  implique que  $f \notin \mathfrak{q}$ . Pour tout  $n \geq 1$ , on pose alors  $\mathfrak{q}_n = \mathfrak{q}^n A_{\mathfrak{q}} \cap A$ . C'est l'ensemble des  $a \in A$  tels qu'il existe  $b \notin \mathfrak{p}$  tel que  $ab \in \mathfrak{q}^n$ . On a pour tout  $n$  l'inclusion  $\mathfrak{q}_n \supset \mathfrak{q}_{n+1}$ .

Les idéaux premiers de l'anneau  $A/fA$  correspondent aux idéaux premiers de  $A$  qui contiennent  $f$ . Ainsi,  $\mathfrak{p}(A/fA)$  est le seul idéal premier de  $A/fA$ . Cet anneau est donc de dimension 0. Comme il est noethérien, il est ainsi artinien. Par suite, la suite décroissante d'idéaux  $\mathfrak{q}_n(A/fA)$  est stationnaire et il existe en entier  $N \geq 1$  tel que pour  $n \geq N$ ,

$$\mathfrak{q}_n + fA = \mathfrak{q}_{n+1} + fA.$$

Si  $x \in \mathfrak{q}_n$ , il existe ainsi  $a \in A$  tel que  $x + af \in \mathfrak{q}_{n+1}$ , d'où en particulier  $af \in \mathfrak{q}_n$ , et donc  $a \in \mathfrak{q}_n$  puisque  $f \notin \mathfrak{q}$ . Ainsi,  $x \in \mathfrak{q}_{n+1} + f\mathfrak{q}_n$  et par conséquent, on a l'égalité

$$\mathfrak{q}_n = \mathfrak{q}_{n+1} + f\mathfrak{q}_n$$

et a fortiori, puisque  $f \in \mathfrak{p}$ ,

$$\mathfrak{q}_n = \mathfrak{q}_{n+1} + \mathfrak{p}\mathfrak{q}_n.$$

D'après le lemme de Nakayama 1.3.3, on a ainsi  $\mathfrak{q}_n = \mathfrak{q}_{n+1}$  pour tout  $n \geq N$ .

Par suite, en prenant  $n = N$ , on a

$$\mathfrak{q}^N A_{\mathfrak{q}} = \mathfrak{q}_N A_{\mathfrak{q}} = \mathfrak{q}_{N+1} A_{\mathfrak{q}} = \mathfrak{q}^{N+1} A_{\mathfrak{q}} = \mathfrak{q} \cdot \mathfrak{q}^N A_{\mathfrak{q}}.$$

Le lemme de Nakayama implique alors que  $\mathfrak{q}^N A_{\mathfrak{q}} = 0$ , et donc,  $\mathfrak{q}$  étant premier,  $\mathfrak{q}A_{\mathfrak{q}} = 0$ . On a ainsi  $\mathfrak{q} = 0$ , comme il fallait démontrer.  $\square$

On peut alors étendre par récurrence le théorème 5.3.1 aux fermés de codimension supérieure.

**COROLLAIRE 5.3.3.** — *Soient  $X$  une variété algébrique affine irréductible et  $f_1, \dots, f_r$  des éléments de  $\mathcal{A}(X)$ . Les composantes irréductibles de  $\mathcal{V}(f_1, \dots, f_r)$  sont toutes de codimension inférieure ou égale à  $r$ .*

*Démonstration.* — Le résultat est trivialement vrai pour  $r = 0$ . Supposons le vrai pour  $r - 1$  et soit  $Z$  une composante irréductible de  $\mathcal{V}(f_1, \dots, f_r)$ . Comme  $Z$  est contenu dans  $\mathcal{V}(f_1, \dots, f_{r-1})$ ,  $Z$  est contenu dans une composante irréductible  $Z'$  et est ainsi une composante irréductible de  $Z' \cap \mathcal{V}(f_r)$ . Par récurrence,  $\text{codim}(Z', X) \leq r - 1$  tandis que le théorème 5.3.1 implique que  $\text{codim}(Z, Z') \leq 1$ . Par suite,

$$\begin{aligned} \text{codim}(Z, X) &= \dim X - \dim Z = (\dim X - \dim Z') + (\dim Z' - \dim Z) \\ &= \text{codim}(Z', X) + \text{codim}(Z, Z') \leq r - 1 + 1 = r. \end{aligned}$$

$\square$

Autrement dit, les composantes irréductibles d'un ensemble algébrique défini par  $r$  équations sont de codimension au plus  $r$ . Réciproquement :

**PROPOSITION 5.3.4.** — *Soit  $Z \subset X$  un fermé irréductible de codimension  $r$ . Il existe alors  $f_1, \dots, f_r \in \mathcal{A}(X)$  tels que toutes les composantes irréductibles de  $\mathcal{V}(f_1, \dots, f_r)$  soient de codimension  $r$  et que  $Z$  soit l'une d'entre elles.*

*Démonstration.* — Si  $r = 0$ ,  $Z$  est une composante irréductible de  $X$ . Si  $r \geq 1$ ,  $Z$  ne contient aucune composante irréductible de  $X$ , donc son idéal  $\mathcal{I}(Z)$  n'est contenu dans aucun des idéaux premiers minimaux de  $\mathcal{A}(X)$ . D'après le lemme d'évitement 1.1.2,  $\mathcal{I}(Z)$  n'est pas contenu dans leur réunion et il existe ainsi  $f_1 \in \mathcal{I}(Z)$  non diviseur de 0 dans  $\mathcal{A}(X)$ . D'après le théorème 5.3.1, les composantes irréductibles de  $\mathcal{V}(f_1)$  sont toutes de codimension 1 et  $Z$  est contenu dans l'une d'entre elles. Par récurrence, il existe  $f_2, \dots, f_r \in \mathcal{A}(\mathcal{V}(f_1)) = \mathcal{A}(X)/\sqrt{(f_1)}$  tel que les composantes irréductibles de  $\mathcal{V}(f_1, f_2, \dots, f_r)$  soient toutes de codimension  $r - 1$  dans  $\mathcal{V}(f_1)$  et  $Z$  est contenu dans l'une d'entre elles. Autrement dit, les composantes irréductibles de  $\mathcal{V}(f_1, \dots, f_r)$  sont toutes de codimension  $r$  et  $Z$  est l'une d'entre elles.  $\square$

*Exercice 5.3.5.* — En utilisant le lemme d'évitement 1.1.2, montrer le résultat suivant : Soit  $Z = Z_r \subset Z_{r-1} \subset \dots \subset Z_1 \subset X$  une chaîne de fermés irréductibles, avec  $\text{codim}(Z_i, X) = i$  pour  $i \in \{1, \dots, r\}$ . Il existe  $f_1, \dots, f_r \in \mathcal{A}(X)$  tels que pour tout  $i$ , toutes les composantes irréductibles de  $\mathcal{V}(f_1, \dots, f_i)$  sont de codimension  $i$  et  $Z_i$  est l'une d'entre elles. (Voir [?], Cor. 4, p. 62, pour une démonstration.)

*Exercice 5.3.6.* — Soit  $f : \mathbf{A}^1 \rightarrow \mathbf{A}^3$  le morphisme défini par  $f(t) = (t^3, t^4, t^5)$ . Montrer que l'image de  $f$  est un fermé irréductible de codimension 2 dans  $\mathbf{A}^3$  mais que son idéal n'est pas défini par deux équations. (L'idéal  $\mathcal{I}(f(\mathbf{A}^1))$  est constitué des polynômes  $p \in k[X, Y, Z]$  tels que pour tout  $t$ ,  $p(t^3, t^4, t^5) = 0$ . On prouvera qu'il est engendré par  $Y^2 - XZ$ ,  $X^3 - YZ$  et  $X^5 - Z^3$  puis que cet idéal définit exactement  $f(\mathbf{A}^1)$ . Enfin, montrer que cet idéal n'est pas engendré par deux éléments en considérant les composantes de degré 2.) On dit que  $f(\mathbf{A}^1)$  n'est pas intersection complète dans  $\mathbf{A}^3$ .

Les corollaires 5.3.3 et 5.3.4 ont la formulation algébrique suivante :

**THÉORÈME 5.3.7.** — Soit  $A$  un anneau local noethérien ; notons  $\mathfrak{m}$  son idéal maximal. Alors, la hauteur  $\text{ht}(\mathfrak{m})$  de  $\mathfrak{m}$  est le plus petit entier  $n$  tel qu'il existe  $f_1, \dots, f_n \in \mathfrak{m}$  tels que  $\mathfrak{m} = \sqrt{(f_1, \dots, f_n)}$ .

*Démonstration.* — Remarquons tout d'abord que si  $A$  est un anneau local d'idéal maximal  $\mathfrak{m}$ , alors  $\mathfrak{m} = \sqrt{(f_1, \dots, f_n)}$  équivaut au fait que  $\mathfrak{m}$  est l'unique idéal premier de  $A$  contenant  $(f_1, \dots, f_n)$ .

Démontrons par récurrence sur  $n$  que si  $\mathfrak{m} = \sqrt{(f_1, \dots, f_n)}$ , alors  $\text{ht}(\mathfrak{m}) \leq n$ . Si  $\text{ht}(\mathfrak{m}) = 0$ , il n'y a rien à démontrer. Soit sinon  $\mathfrak{p} \subsetneq \mathfrak{m}$  un idéal premier de  $A$  maximal parmi les idéaux premiers de  $A$  distincts de  $\mathfrak{m}$ . Nous allons prouver que  $\text{ht}(\mathfrak{p}) \leq n - 1$ , d'où il résultera,  $\mathfrak{p}$  étant arbitraire, que  $\text{ht}(\mathfrak{m}) \leq n$ .

L'hypothèse sur la suite  $(f_1, \dots, f_n)$  implique que l'un des  $f_i$ , soit  $f_1$ , n'appartient pas à  $\mathfrak{p}$ . Alors,  $\mathfrak{m}$  est l'unique idéal premier de  $A$  qui contient  $\mathfrak{p} + (f_1)$ . Par conséquent,  $\mathfrak{m}$  est

nilpotent modulo  $\mathfrak{p} + (f_1)$  et il existe  $m \geq 1$ ,  $a_2, \dots, a_n \in A$  et  $g_2, \dots, g_n \in \mathfrak{p}$  tels que

$$f_2^m = a_2 f_1 + g_2, \quad \dots, \quad f_n^m = a_n f_1 + g_n.$$

Par suite, dans l'anneau  $A/(g_2, \dots, g_n)$ ,  $\mathfrak{m}$  est un idéal premier minimal contenant  $f_1$ . D'après le Hauptidealsatz 5.3.2, la hauteur de  $\mathfrak{m}$  dans cet anneau est  $\leq 1$ . Les inclusions  $\mathfrak{m} \supseteq \mathfrak{p} \supset (g_2, \dots, g_n)$  impliquent alors que  $\mathfrak{p}$  est un idéal premier minimal de  $A$  contenant  $(g_2, \dots, g_n)$ . Par récurrence,  $\text{ht}(\mathfrak{p}) \leq n - 1$  et  $\text{ht}(\mathfrak{m}) \leq n$ .

Comme tout idéal admet une famille génératrice finie, Nous avons en particulier démontré que la hauteur de tout idéal premier d'un anneau noethérien est finie. De manière équivalente, un anneau local noethérien est de dimension finie.

Démontrons maintenant par récurrence sur  $n = \text{ht}(\mathfrak{m})$  qu'il existe  $f_1, \dots, f_n \in \mathfrak{m}$  tel que  $\mathfrak{m}$  soit l'unique idéal premier de  $A$  contenant les  $f_i$ .

Si  $\text{ht}(\mathfrak{m}) = 0$ ,  $\mathfrak{m}$  est l'unique idéal premier de  $A$  et la famille vide convient.

Si  $\text{ht}(\mathfrak{m}) = n \geq 1$ , remarquons que  $\mathfrak{m}$  n'est contenu dans aucun idéal premier minimal de  $A$  et d'après le lemme d'évitement 1.1.2 n'est pas contenu dans leur réunion. Il existe ainsi  $f_1 \in \mathfrak{m}$  qui n'est contenu dans aucun idéal premier minimal de  $A$  et d'après le Hauptidealsatz (théorème 5.3.2), la hauteur de tout idéal premier de  $A$  qui est minimal parmi ceux contenant  $(f_1)$  est égale à 1. La hauteur de  $\mathfrak{m}/(f_1)$  dans  $A/(f_1)$  est ainsi inférieure ou égale à  $n - 1$ . (On peut prolonger toute chaîne d'idéaux premiers de  $A/(f_1)$  par un des idéaux premiers minimaux de  $A$ .) Par récurrence, il existe  $f_2, \dots, f_n \in \mathfrak{m}$  tels que la hauteur de  $\mathfrak{m}/(f_1, \dots, f_n)$  dans  $A/(f_1, \dots, f_n)$  est nulle. ce qui prouve que  $\mathfrak{m}$  est un idéal premier minimal parmi ceux qui contiennent  $(f_1, \dots, f_n)$ .  $\square$

## 5.4. Espace tangent

Soit  $X \subset \mathbf{A}^n$  une variété algébrique affine et  $x \in X$ . Soient  $f_1, \dots, f_r$  des éléments de  $k[X_1, \dots, X_n]$  tels que  $\mathcal{I}(X) = (f_1, \dots, f_r)$ .

DÉFINITION 5.4.1. — *L'espace tangent à  $X$  en  $x$  est le sous-espace vectoriel  $T_x(X)$  de  $k^n$  défini par les équations*

$$\sum_{i=1}^n \frac{\partial f_1}{\partial X_i}(x) u_i = \dots = \sum_{i=1}^n \frac{\partial f_r}{\partial X_i}(x) u_i = 0.$$

Cette définition est concrète mais se prête mal aux manipulations car elle dépend du plongement de  $X$  dans  $\mathbf{A}^n$  choisi. On va ainsi donner des définitions équivalentes.

DÉFINITION 5.4.2. — *On appelle dérivation en  $x$  tout homomorphisme  $k$ -linéaire  $D : \mathcal{A}(X) \rightarrow k$  tel que pour tous  $f, g \in \mathcal{A}(X)$ ,*

$$D(fg) = f(x)D(g) + g(x)D(f).$$

On note  $\text{Der}_x(X)$  l'ensemble des dérivations en  $x$ .

PROPOSITION 5.4.3. — On a des isomorphismes canoniques de  $k$ -espaces vectoriels :

$$T_x(X) \simeq \text{Der}_x(X) \simeq (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee.$$

*Démonstration.* — On construit trois homomorphismes.

Si  $\mathbf{u} = (u_i) \in T_x(X)$ , on définit un homomorphisme de  $k$ -espaces vectoriels  $D_{\mathbf{u}} : k[X_1, \dots, X_n] \rightarrow k$  en posant

$$D_{\mathbf{u}}(f) = \sum_{i=1}^n \frac{\partial f}{\partial X_i}(x) u_i.$$

Il est clair que  $D_{\mathbf{u}}$  est une dérivation en  $x$ , mais sur  $\mathbf{A}^n$ . Il reste ainsi à prouver que  $\mathcal{S}(X)$  est contenu dans le noyau de  $D_{\mathbf{u}}$ . Or, si  $f \in \mathcal{S}(X)$ , on peut écrire  $f = \sum a_j f_j$  pour des polynômes  $a_j \in k[X_1, \dots, X_n]$ . Alors,

$$\sum_{i=1}^n \frac{\partial f}{\partial X_i}(x) u_i = \sum_j a_j(x) \sum_i \frac{\partial f_j}{\partial X_i}(x) u_i + \sum_i f_j(x) \sum_i \frac{\partial a_j}{\partial X_i}(x) u_i = 0$$

car  $\mathbf{u} \in T_x(X)$  (pour la première somme) et  $x \in X$  (pour la seconde). On a ainsi construit une application  $T_x(X) \rightarrow \text{Der}_x(X)$  dont il est clair qu'elle est  $k$ -linéaire.

Si  $D \in \text{Der}_x(X)$ , on peut restreindre  $D$  à  $\mathfrak{m}_x$ . Comme  $f$  est une dérivation, on voit que  $D(\mathfrak{m}_x^2) = 0$ , d'où une application linéaire  $(\mathfrak{m}_x/\mathfrak{m}_x^2) \rightarrow k$ .

Enfin, on construit un homomorphisme  $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \rightarrow T_x(X)$  en associant à  $D$  le vecteur  $\mathbf{u}$  de coordonnées  $u_i = D(X_i - x_i)$ . Si  $f \in k[X_1, \dots, X_n]$ , on peut écrire

$$f = f(x) + \sum_{i=1}^n a_i(X - x_i) + \text{termes de degrés} \geq 2$$

d'où il ressort que  $D(f - f(x)) = \sum a_i u_i$ . De plus, on a  $a_i = (\partial f / \partial X_i)(x)$ . Ainsi, si  $f \in \mathcal{S}(X)$ ,  $\sum (\partial f / \partial X_i)(x) u_i = 0$  et cela implique que  $\mathbf{u} \in T_x X$ .

Il est alors facile de vérifier que la composition de ces trois homomorphismes est l'identité. Ce sont les isomorphismes cherchés.  $\square$

*Remarque 5.4.4.* — Il est facile de prouver que toute dérivation en  $x$  s'étend de manière unique en une dérivation locale en  $x$ , c'est-à-dire un homomorphisme  $k$ -linéaire,  $D : \mathcal{O}_{X,x} \rightarrow k$ , vérifiant  $D(fg) = f(x)D(g) + g(x)D(f)$  et que l'on obtient ainsi toutes les dérivations locales.

De même,  $\mathfrak{m}_x/\mathfrak{m}_x^2$  peut être calculé, au choix, dans  $\mathcal{A}(X)$  ou dans l'anneau local  $\mathcal{O}_{X,x}$ .

DÉFINITION 5.4.5. — Soit  $X$  une variété algébrique et  $x \in X$ . On appelle espace tangent à  $X$  en  $x$  le  $k$ -espace vectoriel  $T_x(X) = (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$ , où  $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$  est l'idéal maximal de l'anneau local de  $X$  en  $x$ .

DÉFINITION 5.4.6. — On dit que  $X$  est régulière au point  $x$  de  $X$  si  $\dim_k T_x(X) = \text{codim}(x, X)$ . Cela équivaut à la relation

$$\dim \mathcal{O}_{X,x} = \dim_k \mathfrak{m}_x / \mathfrak{m}_x^2.$$

On dit aussi que  $x$  est un point régulier et, dans le cas contraire, que  $x$  est un point singulier de  $X$ .

Exercice 5.4.7. — Résoudre l'exercice 3.3.14.

DÉFINITION 5.4.8. — On dit qu'un anneau local noethérien d'idéal maximal  $\mathfrak{m}$  est régulier si la dimension de  $A$  est égale à la dimension du  $A/\mathfrak{m}$ -espace vectoriel  $\mathfrak{m}/\mathfrak{m}^2$ .

Remarque 5.4.9. — On a toujours l'inégalité  $\dim \mathfrak{m}/\mathfrak{m}^2 \geq \dim A$ . En effet, si des éléments  $f_1, \dots, f_r$  de  $\mathfrak{m}$  engendrent  $\mathfrak{m}/\mathfrak{m}^2$ , on peut écrire  $\mathfrak{m} = (f_1, \dots, f_r) + \mathfrak{m}^2$  et le lemme de Nakayama implique que  $\mathfrak{m} = (f_1, \dots, f_r)$ . D'après le théorème 5.3.7, on a  $\dim A \leq r$ .

Autrement dit, on a pour tout  $x \in X$ ,  $\dim T_x(X) \geq \text{codim}(x, X)$  et cette dernière codimension n'est autre que  $\dim X$  si  $X$  est irréductible.

DÉFINITION 5.4.10. — On note  $\text{Sing}(X)$  et  $\text{Reg}(X)$  les ensembles des points singuliers (resp. réguliers) de  $X$ .

THÉORÈME 5.4.11. — L'ensemble  $\text{Reg}(X)$  est un ouvert dense de  $X$ .

La démonstration de ce théorème est un peu délicate et va occuper la fin de ce paragraphe.

Si  $X$  est affine et irréductible,  $\text{Sing}(X)$  est fermé. — Soit  $\mathcal{I}(X) = (f_1, \dots, f_r)$  l'idéal de  $X$ . On voit que la dimension de  $T_x(X)$  est égale à  $n - \text{rang} \left( \frac{\partial f_j}{\partial X_i}(x) \right)$ . (Cette formulation, fondamentale, porte le nom de *critère jacobien*.) Le rang de la matrice des dérivées partielles des  $f_j$  en  $x$  est donc inférieur ou égal à  $n - \dim X$ , avec égalité si et seulement si  $x$  est un point régulier de  $X$ . Ainsi,  $x \in X$  est un point singulier si et seulement si ce rang est  $< n - \dim X$ , ce qui signifie que tous les mineurs d'ordre  $n - \dim X$  de la matrice des dérivées partielles des  $f_j$  s'annulent en  $x$ . On a prouvé que  $x \in \text{Sing}(X)$  si et seulement si  $x$  annule un ensemble fini d'équations polynomiales. Autrement dit,  $\text{Sing}(X)$  est fermé dans  $X$ .

Si  $X$  est irréductible,  $\text{Sing}(X)$  est fermé. — Pour tout ouvert affine  $U \subset X$ ,  $\text{Sing}(X) \cap U = \text{Sing}(U)$  est fermé dans  $U$ . Par suite,  $\text{Sing}(X)$  est fermé dans  $X$ .

Si  $X$  est une hypersurface irréductible de  $\mathbf{A}^n$ ,  $\text{Sing}(X)$  est d'intérieur vide. — Supposons  $X = \mathcal{V}(f)$  pour un polynôme irréductible  $f \in k[X_1, \dots, X_n]$ . On a donc  $\text{Sing}(X) = \mathcal{V} \left( f, \frac{\partial f}{\partial X_1}, \dots, \frac{\partial f}{\partial X_n} \right)$ .

Supposons par l'absurde que  $\text{Sing}(X)$  n'est pas d'intérieur vide. Comme  $X$  est irréductible, on a alors  $\text{Sing}(X) = X$ , autrement dit, les dérivées partielles  $\frac{\partial f}{\partial X_i}$  s'annulent sur  $X$ .

Mais si le polynôme  $\partial f/\partial X_i$  n'est pas nul, il ne peut pas appartenir à l'idéal ( $f$ ) car son degré en  $X_i$  est strictement inférieur à celui de  $f$ . Ainsi, on a  $\frac{\partial f}{\partial X_i} = 0$  pour tout  $i$ .

Si  $k$  est de caractéristique nulle, cela implique que  $f$  est constant, ce qui est absurde. Si  $k$  est de caractéristique  $p > 0$ , on peut écrire  $f = g(X_1^p, \dots, X_n^p)$ , puis,  $k$  étant algébriquement clos,  $f = h(X_1, \dots, X_n)^p$ . Ceci contredit l'hypothèse que  $f$  est irréductible. Autrement dit,  $\text{Sing}(X) \subsetneq X$ .

*Si  $X$  est irréductible,  $\text{Sing}(X)$  est d'intérieur vide.* — Pour cela, il suffit de prouver qu'il existe un ouvert  $U$  de  $X$  isomorphe à un ouvert  $V$  d'une hypersurface irréductible de  $\mathbf{A}^{\dim X+1}$ .

**PROPOSITION 5.4.12.** — *Soit  $X$  une variété algébrique affine irréductible de dimension  $d$ . Il existe une hypersurface irréductible  $Y \subset \mathbf{A}^{d+1}$  et des ouverts non vides  $U \subset X$  et  $V \subset Y$  tels que  $U \simeq V$ .*

*Démonstration.* — D'après la proposition 3.5.7, il suffit de prouver que le corps  $k(X)$  des fonctions de  $X$  est engendré par  $d+1$  éléments.

Si  $k(X) = k(x_1, \dots, x_n)$  avec  $n$  minimal, il faut donc prouver que  $n \leq d+1$ . Supposons au contraire  $n > d+1$ . D'après le théorème 5.1.9, le degré de transcendance de  $k(X)$  sur  $k$  est égal à  $d$  et on peut supposer que  $x_1, \dots, x_d$  sont algébriquement indépendants. Il existe alors un polynôme irréductible  $f \in k[X_1, \dots, X_{d+1}]$  tel que  $f(x_1, \dots, x_{d+1}) = 0$ . Comme  $f$  est irréductible, il existe  $i$  tel que  $\partial f/\partial X_i \neq 0$  (l'argument vient d'être détaillé) et on peut supposer que  $i = d+1$ , ce qui signifie que l'extension  $k(x_1, \dots, x_d) \subset k(x_1, \dots, x_{d+1})$  est séparable. De plus,  $x_{d+2}$  est algébrique sur  $k(x_1, \dots, x_d)$ . Le théorème de l'élément primitif (théorème 1.5.3) implique alors qu'il existe  $y \in k(x_1, \dots, x_{d+2})$  tel que

$$k(x_1, \dots, x_d, y) = k(x_1, \dots, x_d, x_{d+1}, x_{d+2}).$$

Cela contredit l'hypothèse que  $n$  est minimal. Par suite,  $n \leq d+1$ . □

*Remarque 5.4.13.* — Les précisions contenues dans la preuve du théorème de l'élément primitif impliquent que si  $X \subset \mathbf{A}^n$  est une variété irréductible de dimension  $d$ , il est possible de trouver une projection linéaire  $\pi : \mathbf{A}^n \rightarrow \mathbf{A}^{d+1}$  telle que  $Y = \overline{\pi(X)}$  convienne.

*Preuve du théorème quand  $X$  n'est plus supposé irréductible.* — Il suffit en fait de prouver le lemme suivant qui impliquera que  $\text{Sing}(X)$  est une réunion finie de fermés d'intérieurs vides.

**LEMME 5.4.14.** — *Soit  $X$  une variété algébrique, notons  $(X_i)$  ses composantes irréductibles. On a alors*

$$\text{Sing}(X) = \bigcup_i \text{Sing}(X_i) \cup \bigcup_{i \neq j} (X_i \cap X_j).$$

*Démonstration.* — Si  $x$  n'appartient qu'à une composante irréductible  $X_i$ , celle-ci est un voisinage de  $x$ . Un tel  $x$  est donc régulier dans  $X$  si et seulement s'il est régulier dans  $X_i$ . SI au contraire  $x$  appartient à plusieurs composantes irréductibles de  $X$ , le théorème 5.4.15 implique que l'anneau local  $\mathcal{O}_{X,x}$  n'est pas régulier, si bien que  $x \in \text{Sing}(X)$ .  $\square$

THÉORÈME 5.4.15. — *Un anneau local noethérien régulier est intègre.*

*Démonstration.* — Soit  $A$  un anneau local noethérien régulier. On démontre par récurrence sur la dimension de  $A$  que  $A$  est intègre.

Si  $\dim A = 0$ , on a  $\dim \mathfrak{m}/\mathfrak{m}^2 = 0$ , si bien que  $\mathfrak{m} = \mathfrak{m}^2$ . D'après le lemme de Nakayama,  $\mathfrak{m} = 0$  et  $A$  est un corps.

Soient  $(\mathfrak{p}_i)$  les idéaux premiers minimaux de  $A$ . (Géométriquement, les  $\mathfrak{p}_i$  correspondent aux composantes irréductibles de  $\text{Spec} A$ .) Comme  $\dim A > 0$ ,  $\mathfrak{m} \neq \mathfrak{p}_i$  et  $A$  étant régulier,  $\mathfrak{m} \neq \mathfrak{m}^2$ . D'après le lemme d'évitement 1.1.2, il existe  $a \in \mathfrak{m}$  tel que  $a \notin \mathfrak{m}^2 \cup \bigcup \mathfrak{p}_i$ . Soit  $B$  l'anneau  $A/(a)$ ; si  $b \notin \mathfrak{n} = \mathfrak{m}B$ ,  $b$  est inversible, donc  $B$  est un anneau local d'idéal maximal  $\mathfrak{n}$ . De plus,  $a$  n'est pas diviseur de zéro dans  $A$ . D'après le Hauptidealsatz 5.3.2, on a donc  $\dim B = \dim A - 1$ . D'autre part,  $\mathfrak{n}/\mathfrak{n}^2 = \mathfrak{m}/(\mathfrak{m}^2 + (a))$  est un quotient de  $\mathfrak{m}/\mathfrak{m}^2$ ; comme  $a \notin \mathfrak{m}^2$ , ces deux espaces vectoriels ne sont pas isomorphes, si bien que

$$\dim A - 1 = \dim B \leq \dim \mathfrak{n}/\mathfrak{n}^2 < \dim \mathfrak{m}/\mathfrak{m}^2 = \dim A$$

d'où l'on déduit que  $\dim \mathfrak{n}/\mathfrak{n}^2 = \dim B$ . Autrement dit,  $B$  est un anneau local noethérien régulier. Par récurrence,  $B$  est intègre :  $(a)$  est un idéal premier de  $A$ . Par le lemme d'évitement 1.1.1, l'un des  $\mathfrak{p}_i$ , soit  $\mathfrak{p}$ , est contenu dans  $(a)$ . (Géométriquement,  $\mathcal{V}(\mathfrak{p})$  est la composante irréductible de  $\text{Spec} A$  qui contient le fermé irréductible  $\mathcal{V}(a)$ .) Comme  $a \notin \mathfrak{p}$ ,  $\mathfrak{p} \subsetneq (a)$ .

Soit  $x \in \mathfrak{p}$ . On peut écrire  $x = ay$  avec  $y \in A$ . Comme  $\mathfrak{p}$  est premier,  $y \in \mathfrak{p}$ , d'où il vient  $x \in a\mathfrak{p} \subset \mathfrak{m}\mathfrak{p}$  et donc  $\mathfrak{p} = \mathfrak{m}\mathfrak{p}$ . D'après le lemme de Nakayama 1.3.3,  $\mathfrak{p} = 0$ . Ainsi,  $(0)$  est un idéal premier de  $A$  qui est donc intègre.  $\square$

## Épilogue

Au moment où ce cours se termine, il me paraît souhaitable d'ajouter quelques mots d'introduction à un cours de géométrie algébrique plus avancé dans lequel la théorie des schémas serait développée.

Ce cours s'est attaché à décrire quelques propriétés géométriques liées aux algèbres de type fini, sur un corps algébriquement clos. Or, on a vu à plusieurs reprises des énoncés géométriques qui étaient la traduction d'un énoncé algébrique analogue concernant les algèbres de type fini sur un corps quelconque, voire même les anneaux noethériens. Il en est ainsi du lemme de normalisation de Noether ou de certains aspects de la théorie de la dimension. Cependant, le théorème des zéros de Hilbert ne donne apparemment une signification géométrique qu'aux algèbres de type fini sur un corps algébriquement clos. Pour contourner cette difficulté, une possibilité est de ne considérer non plus les seules solutions dans  $k^n$  d'un système d'équations polynomiales à coefficients dans un corps  $k$  mais toutes les solutions dans la clôture algébrique de  $k$ , autrement dit à prendre en compte tous les idéaux maximaux d'une  $k$ -algèbre de type fini, et non seulement ceux de corps résiduel  $k$ .

Mais l'opération algébrique de localisation fait sortir fatalement de la catégorie des algèbres de type fini sur un corps, tout en ayant une signification géométrique très simple. Pourquoi ne pas disposer d'une théorie géométrique dans laquelle ces anneaux locaux auraient droit de cité comme anneaux des fonctions sur un objet géométrique à part entière (une espèce de « germe » de variétés algébriques) ?

De même, si l'on étudie les morphismes entre variétés algébriques les plus honnêtes, et en particulier la fibre d'un tel morphisme au-dessus d'un point de l'image, on est amené à introduire des objets nouveaux comme des « points avec multiplicités » : si  $f : \mathbf{A}^1 \rightarrow \mathbf{A}^1$  est donnée par  $f(x, y) = x^2$ , la fibre au-dessus de  $t \neq 0$  est formée de deux points  $(+\sqrt{t})$  et  $(-\sqrt{t})$ , tandis que la fibre au-dessus de 0 est formée du point 0 dont on sait qu'il faut le compter avec multiplicité 2. L'anneau de la fibre au-dessus de  $t \neq 0$  est isomorphe à  $k \times k$ , tandis que l'anneau de la fibre au-dessus de  $t = 0$  devrait être l'anneau *non réduit*  $k[t]/(t^2)$ .

L'arithmétique considère des anneaux d'un type un peu différent : si l'on s'intéresse aux équations polynomiales à coefficients dans  $\mathbf{Z}$ , l'anneau qui intervient naturellement est une  $\mathbf{Z}$ -algèbre de type fini.

Au point où on en est, pourquoi ne pas essayer de donner sens, pour tout anneau  $A$ , à une « variété algébrique » dont l'anneau des fonctions serait  $A$  ? La réponse est fournie par la théorie des schémas développée dans les années 50–60 par Alexander Grothendieck. L'ensemble sous-jacent à une telle variété algébrique (le *schéma affine* d'anneau  $A$ ) est le spectre de  $A$ , l'ensemble des idéaux premiers de  $A$ , muni d'une topologie (analogue à celle que nous avons définie sur le spectre maximal d'une algèbre de type fini sur un corps) et d'un faisceau d'anneaux (dont les sections globales sont les éléments de  $A$ ).

## Alexander GROTHENDIECK (1928–)

*Après sa thèse au cours de laquelle il résolut une dizaine de problèmes majeurs d'analyse fonctionnelle, il consacra toute son énergie à la refondation prodigieuse de la géométrie algébrique (théorie des schémas) en vue de la démonstration des conjectures de Weil, démonstration achevée en 1974 par son élève P. Deligne. Depuis la fin des années 80, Grothendieck s'est progressivement retiré du monde mathématique, puis du monde tout cours.*



L'intérêt est qu'un morphisme d'anneaux  $A \rightarrow B$  donne lieu automatiquement à une application  $\text{Spec } B \rightarrow \text{Spec } A$  qui est un morphisme d'espaces annelés, alors que l'on ne dispose pas en général d'une application entre les spectres maximaux.

La théorie des schémas fournit alors la souplesse et l'intuition géométrique nécessaires, au prix de difficultés nouvelles qui pourront amener à n'étudier tout de même que les variétés algébriques, mais à les étudier dans ce langage (on parle alors de schéma de type fini sur un corps). Il ne paraîtra peut-être pas surprenant au lecteur que les anneaux quelconques n'aient pas les propriétés algébriques nécessaires à une bonne intuition géométrique. Plus étonnant est que les anneaux noethériens ne suffisent pas toujours. En effet, deux résultats importants du cours ne sont pas vrais pour tous les anneaux noethériens : ceux-ci ne sont pas forcément de dimension finie et leur lieu régulier (ensemble des idéaux premiers  $\mathfrak{p}$  de  $A$  tels que l'anneau local  $A_{\mathfrak{p}}$  est régulier) n'est pas forcément ouvert.

Néanmoins, il est légitime de penser que la théorie des schémas, par la souplesse qu'elle apporte, est devenue incontournable, quand bien-même on ne s'intéresserait qu'aux variétés algébriques telles que nous les avons étudiées. C'est dans cet esprit que nous conseillons au lecteur d'aborder la lecture des ouvrages modernes, nécessairement ardues, de géométrie algébrique. En souhaitant qu'il y trouvera de l'intérêt et pourquoi pas, du plaisir...