

Chap I. LA GÉOMÉTRIE AFFINE

Martin Debaisieux

1 Les objets de la géométrie algébrique affine

Définition 1.1. Soit K un corps ; un *sous-ensemble algébrique (affine)* $V(S)$ de $\mathbf{A}^n(K)$ est l'ensemble des racines communes à un ensemble de polynômes S de $K[X_1, \dots, X_n]$:

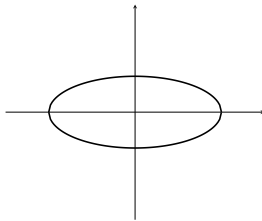
$$V(S) = \{(a_1, \dots, a_n) \in \mathbf{A}^n(K) \mid f(a_1, \dots, a_n) = 0 \text{ pour tout } f \in S\}.$$

Remarque 1.2. La terminologie de *lieu d'annulation* de S sera quelques fois employée lors de ce document afin de désigner $V(S)$. Il survient immédiatement de la définition 1.1 que si $S \subseteq S'$ sont deux ensembles de polynômes alors $V(S) \supseteq V(S')$.

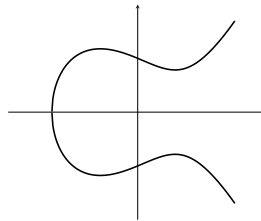
Exemple 1.3. L'ensemble vide n'impose aucune condition et donc $V(\emptyset) = \mathbf{A}^n(K)$. Par conséquent l'espace affine $\mathbf{A}^n(K)$ est un sous-ensemble algébrique de $\mathbf{A}^n(K)$; il est également le lieu d'annulation du polynôme nul. Par opposition, tout polynôme constant non nul n'admet pas de racine et définit donc l'ensemble vide pour sous-ensemble algébrique de $\mathbf{A}^n(K)$.

Remarque 1.4. Les sous-ensembles algébriques propres de $K = \mathbf{A}^1(K)$ sont finis puisque tout polynôme à une seule indéterminée possède un nombre fini de racines. Cet argument ne se généralise néanmoins pas : le polynôme XY admet une infinité de racines dans $\mathbf{A}^2(K)$ pourvu que K soit infini.

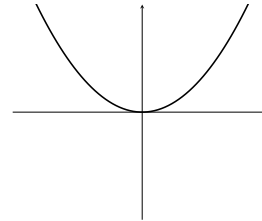
Exemple 1.5. Les esquisses suivantes représentent des *courbes planes* sur \mathbf{R} (i.e. des sous-ensembles algébriques de l'espace affine de dimension 2 sur \mathbf{R}) :



Ellipse : $\frac{X^2}{a^2} + \frac{Y^2}{b^2} - 1 = 0$,
où $a, b \in \mathbf{R}^{>0}$.



Une courbe elliptique :
 $X^3 - X + 1 - Y^2 = 0$.



Parabole : $aX^2 - Y = 0$,
où $a \in \mathbf{R}^{>0}$.

Nota Bene 1.6 (Dépendance en l'ensemble). Puisque l'idéal \mathfrak{a} engendré par un ensemble S de polynômes de $K[X_1, \dots, X_n]$ est formé des sommes finies $\sum f_i g_i$ où $f_i \in K[X_1, \dots, X_n]$ et $g_i \in S$, de telles sommes valent zéro en chaque point où les g_i s'annulent simultanément et donc $V(S) \subseteq V(\mathfrak{a})$. L'inclusion réciproque est également vérifiée car $S \subseteq \mathfrak{a}$; ainsi $V(S) = V(\mathfrak{a})$. Tout ensemble générateur de \mathfrak{a} engendre donc le même ensemble algébrique sur K . Nous noterons que les sous-ensembles algébriques de $\mathbf{A}^n(K)$ peuvent être décrits à partir des idéaux de $K[X_1, \dots, X_n]$.

Remarque 1.7. Selon l'ensemble générateur d'un idéal fixé, il sera plus ou moins aisé de déterminer l'ensemble algébrique associé. L'idéal $\mathfrak{a} = (X^2 + Y^2 + Z^2 - 1, X^2 + Y^2 - Y, X - Z)$ de $K[X, Y, Z]$ peut être engendré par $Y^2 - 2Y + 1$, $Z^2 - 1 + Y$, $X - Z$ et puisque le premier polynôme admet une racine double en 1, il s'en suit que $V(\mathfrak{a}) = \{(0, 1, 0)\}$.

Nota Bene 1.8 (Dépendance en le corps). L'ensemble des racines de $X^2 + Y^2 \in K[X, Y]$ est $\{(0, 0)\}$ si $K = \mathbf{R}$ mais est la réunion de deux droites si $K = \mathbf{C}$ (données par $X - iY$ et $X + iY$). De façon générale, $V(f) \subseteq \mathbf{A}^n(K)$ est la partie fixe de $V(f) \subseteq \mathbf{A}^n(K^{\text{sep}})$ par le groupe de Galois de K^{sep}/K .

2 Le théorème de la base d'Hilbert

Il n'a pas été exigé lors de la définition 1.1 que S soit fini ; toutefois le théorème de la base d'Hilbert nous apprend que tout ensemble algébrique est le lieu d'annulation d'un ensemble fini de polynômes. Précisément, il stipule que tout idéal de $K[X_1, \dots, X_n]$ est engendré par un nombre fini d'éléments, et nous avons déjà observé qu'un ensemble générateur d'un idéal admet les mêmes racines que l'idéal qu'il engendre.

Théorème 2.1 (de la base d'Hilbert). *Soit K un corps ; l'anneau $K[X_1, \dots, X_n]$ est noethérien.*

PREUVE. Par induction du lemme suivant. □

Lemme 2.2. *Si A est un anneau noethérien alors $A[X]$ l'est aussi.*

PREUVE. Soit \mathfrak{a} un idéal propre de $A[X]$ et désignons par $\mathfrak{a}(i)$ l'ensemble des coefficients dominants de chaque polynôme dans \mathfrak{a} de degré i (avec également 0). Alors $\mathfrak{a}(i)$ est un idéal de A et $\mathfrak{a}(i) \subseteq \mathfrak{a}(i+1)$ puisque si $aX^i + \dots \in \mathfrak{a}$ alors $X(aX^i + \dots) \in \mathfrak{a}$ aussi.

Si \mathfrak{b} un idéal de $A[X]$ contenu dans \mathfrak{a} alors $\mathfrak{b}(i) \subseteq \mathfrak{a}(i)$, et si cette égalité est vérifiée en chaque i alors $\mathfrak{b} = \mathfrak{a}$. En effet, soit f un élément de \mathfrak{a} ; comme $\mathfrak{b}(\deg f) = \mathfrak{a}(\deg f)$, il existe un $g \in \mathfrak{b}$ pour lequel $\deg(f - g) < \deg f$. Dit autrement $f = g + f_1$ avec $g \in \mathfrak{b}$ et $\deg f_1 < \deg f$. En itérant ce processus il est alors possible d'exprimer $f_1 = g_1 + f_2$ avec $g_1 \in \mathfrak{b}$ et $\deg f_2 < \deg f_1$ et ainsi de suite jusqu'à obtenir $f = g + g_1 + g_2 + \dots \in \mathfrak{b}$ (cette somme est finie de par la stricte décroissance du degré des f_i).

Comme A est noethérien, la chaîne ascendante

$$\mathfrak{a}(1) \subseteq \mathfrak{a}(2) \subseteq \dots \subseteq \mathfrak{a}(i) \subseteq \dots$$

est stationnaire, disons $\mathfrak{a}(d) = \mathfrak{a}(d+1) = \dots$ (alors $\mathfrak{a}(d)$ comprend les coefficients dominants de chacun des polynômes dans \mathfrak{a}). Pour tout $i \leq d$ il existe un ensemble générateur fini $\{a_{i1}, \dots, a_{in_i}\}$ de $\mathfrak{a}(i)$ et pour toute paire (i, j) il existe un polynôme $f_{ij} \in \mathfrak{a}$ dont le coefficient dominant est a_{ij} . L'idéal \mathfrak{b} de $A[X]$ engendré par les f_{ij} (qui sont en nombre fini) est contenu dans \mathfrak{a} et est tel que $\mathfrak{b}(i) = \mathfrak{a}(i)$ en chaque i ; ainsi $\mathfrak{b} = \mathfrak{a}$ et donc \mathfrak{a} est de type fini. □

Remarque 2.3. Il est bon de rappeler que – même si A est noethérien – il n'y aucune chance pour que $A[X_1, X_2, \dots]$ soit noethérien étant donné la chaîne strictement croissante $(X_1) \subset (X_1, X_2) \subset \dots$.

3 La topologie de Zariski sur $\mathbf{A}^n(K)$

Proposition 3.1. *Soit K un corps ; les sous-ensembles algébriques de $\mathbf{A}^n(K)$ satisfont :*

- (a) $V(0) = \mathbf{A}^n(K)$ et $V(K[X_1, \dots, X_n]) = \emptyset$.
- (b) $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ pour tous idéaux $\mathfrak{a}, \mathfrak{b}$ de $K[X_1, \dots, X_n]$.
- (c) $\bigcap_{i \in I} V(\mathfrak{a}_i) = V(\sum_{i \in I} \mathfrak{a}_i)$ pour toute famille d'idéaux $(\mathfrak{a}_i)_{i \in I}$ de $K[X_1, \dots, X_n]$.

PREUVE. (a) Fait l'objet de l'exemple 1.3.

(b) Puisque $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b}$, alors $V(\mathfrak{a}\mathfrak{b}) \supseteq V(\mathfrak{a} \cap \mathfrak{b}) \supseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. Pour les inclusions réciproques, si $a \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$ alors il existe un $f \in \mathfrak{a}$ et un $g \in \mathfrak{b}$ tel que $f(a) \neq 0$ et $g(a) \neq 0$; ainsi $(fg)(a) \neq 0$ et donc $a \notin V(\mathfrak{a}\mathfrak{b})$.

(c) Par définition, l'idéal $\sum_{i \in I} \mathfrak{a}_i$ est composée de toutes les sommes finies de la forme $\sum f_i$ avec $f_i \in \mathfrak{a}_i$. Le troisième point est alors évident. □

Conséquence 3.2. La proposition précédente montre que les sous-ensembles algébriques de $\mathbf{A}^n(K)$ satisfont les axiomes pour être les fermés d'une topologie sur $\mathbf{A}^n(K)$. Cette topologie pour laquelle les fermés sont exactement les sous-ensembles algébriques porte le nom de *topologie de Zariski* sur $\mathbf{A}^n(K)$. La topologie induite sur un sous-ensemble V de $\mathbf{A}^n(K)$ est la *topologie de Zariski* sur V .

Exemple 3.3. La topologie de Zariski sur $K = \mathbf{A}^1(K)$ est celle dont les fermés sont $\mathbf{A}^1(K)$ et les sous-ensembles finis de K (cf. remarque 1.4) : c'est la topologie cofinie sur $\mathbf{A}^1(K)$. Noter que si K est infini, il n'est en particulier pas possible de trouver des ouverts non vides disjoints ; la topologie de Zariski sur $\mathbf{A}^1(K)$ n'est donc pas de Hausdorff (T_2).

Remarque 3.4. Soit K un corps topologique de caractéristique zéro (par exemple $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Q}_p$). La topologie de Zariski sur $K = \mathbf{A}^1(K)$ est plus grossière (plus faible) que la topologie du corps. Noter que si K est fini alors la topologie de Zariski sur $K = \mathbf{A}^1(K)$ est la topologie discrète.

Exemple 3.5. Soit K un corps fini. La topologie de Zariski sur $K = \mathbf{A}^n(K)$ est la topologie discrète : en tout point $P = (a_1, \dots, a_n) \in \mathbf{A}^n(K)$, $\{P\}$ est l'ensemble des racines de $(X_1 - a_1, \dots, X_n - a_n)$. Dès lors, tous les singletons sont fermés et, comme K est fini, tous les sous-ensembles de $\mathbf{A}^n(K)$ sont fermés. Noter que le début de cet argument montre que la topologie de Zariski sur $K = \mathbf{A}^n(K)$ est T_1 (indépendamment de la finitude de K).

Remarque 3.6. Soit $\mathfrak{a} = (f_1, \dots, f_m)$ un idéal de $K[X_1, \dots, X_n]$. Dès lors $V(\mathfrak{a}) = V(f_1) \cap \dots \cap V(f_m)$ et par conséquent :

$$\mathbf{A}^n(K) - V(\mathfrak{a}) = \mathbf{A}^n(K) - \bigcap_{i=1}^m V(f_i) = \bigcup_{i=1}^m (\mathbf{A}^n(K) - V(f_i)).$$

Les $D(f) := \mathbf{A}^n(K) - V(f)$ forment ainsi une base d'ouverts pour la topologie de Zariski sur $\mathbf{A}^n(K)$.

4 Le théorème des zéros d'Hilbert (Nullstellensatz)

Il est légitime de se demander sous quelle(s) condition(s) un sous-ensemble S de $A = K[X_1, \dots, X_n]$ admet une racine commune. Bien sûr, un système d'équations $g_i(X_1, \dots, X_n) = 0$ où $i = 1, \dots, m$ est inconsistent s'il existe des $f_i \in A$ pour lesquels $f_1 g_1 + \dots + f_m g_m = 1$ ou, dit autrement, si $(g_1, \dots, g_m) = A$. Le Nullstellensatz (quelque peu malheureusement traduit en français par "théorème des zéros d'Hilbert") fournit une condition suffisante afin que $V(S)$ soit non vide.

Lemme 4.1 (de normalisation de Noether). *Soit K un corps et soit A une K -algèbre de type fini. Alors il existe des éléments $x_1, \dots, x_d \in A$ (où $d \geq 0$) algébriquement indépendants sur K tels que A est une extension finie de $K[x_1, \dots, x_d]$.*

PREUVE. La preuve suggérée suppose que K est infini (ce n'est pas indispensable) ; toutefois cette hypothèse ne gênera pas à la suite de ce document puisque nous travaillerons sur des corps algébriquement clos [Préface, Lemme 5.3].

Soient $x_1, \dots, x_n \in A$ tels que $A = K[x_1, \dots, x_n]$. Si ces éléments sont algébriquement indépendants sur K alors il n'y a rien à prouver. Sinon le lemme 4.3 implique que A est une extension finie d'un sous-anneau $B = K[y_1, \dots, y_{n-1}]$. En procédant par induction, B est une extension finie d'un sous-anneau $C = K[z_1, \dots, z_d]$ où $z_1, \dots, z_d \in A$ sont algébriquement indépendants sur K ; ainsi A est une extension finie de C . \square

Lemme 4.2. *Soit K un corps infini ; si $f \in K[X_1, \dots, X_n, T]$ est non nul alors il existe $c_1, \dots, c_n \in K$ tels que :*

$$f(X_1 + c_1 T, \dots, X_n + c_n T, T) = a_0 T^m + a_1 T^{m-1} + \dots + a_m$$

avec $a_0 \in K^\times$ et les coefficients $a_i \in K[X_1, \dots, X_n]$. Autrement dit, il est possible de rendre monique en T le polynôme f .

PREUVE. Soit f_d la partie homogène de plus haut degré de f et posons $d = \deg(f_d)$. Quels que soient $c_1, \dots, c_n \in K$, nous avons que

$$f_d(X_1 + c_1T, \dots, X_n + c_nT, T) = f_d(c_1, \dots, c_n, 1)T^d + \text{termes de degré} < d \text{ en } T$$

puisque le polynôme $f_d(X_1 + d_1T, \dots, X_n + d_nT, T)$ reste homogène de degré d en X_1, \dots, X_n, T et donc le coefficient du monôme T^d s'obtient en évaluant chaque X_i à 0 et T à 1 dans f_d . Comme f_d est non nul homogène, $f_d(X_1, \dots, X_n, 1)$ est également non nul. Nous pouvons alors choisir les $c_i \in K$ de manière à ce que $f_d(c_1, \dots, c_n, 1) \neq 0$ étant donné que K est infini [Préface, Lemme 1.6]. Ainsi :

$$f(X_1 + c_1T, \dots, X_n + c_nT, T) = f_d(c_1, \dots, c_n, 1)T^d + \text{termes de degré} < d \text{ en } T,$$

avec $f_d(c_1, \dots, c_n, 1) \in K^\times$. □

Lemme 4.3. Soient K un corps infini, $A = K[x_1, \dots, x_n]$ une K -algèbre de type fini et $\{x_1, \dots, x_d\}$ le sous-ensemble algébriquement indépendant maximal de $\{x_1, \dots, x_n\}$. Si $d < n$ alors il existe des éléments $c_1, \dots, c_d \in A$ tels que A est une extension finie de $K[x_1 - c_1x_n, \dots, x_d - c_dx_n, x_{d+1}, \dots, x_{n-1}]$.

PREUVE. L'ensemble $\{x_1, \dots, x_d, x_n\}$ est par hypothèse algébriquement dépendant sur K et donc il existe un polynôme non nul $f \in K[X_1, \dots, X_d, T]$ tel que

$$f(x_1, \dots, x_d, x_n) = 0. \quad (4.1)$$

Toutefois, l'ensemble $\{x_1, \dots, x_d\}$ est algébriquement indépendant sur K ; dès lors T doit apparaître dans f . Donc

$$f(X_1, \dots, X_d, T) = a_0T^m + a_1T^{m-1} + \dots + a_m$$

avec chaque $a_i \in K[X_1, \dots, X_d]$, a_0 non nul et un certain $m > 0$. Si $a_0 \in K$ alors (4.1) implique que x_n est entier sur $K[x_1, \dots, x_d]$ et donc que x_1, \dots, x_n est entier sur $K[x_1, \dots, x_{n-1}]$. Ainsi A est une extension finie de $K[x_1, \dots, x_{n-1}]$. Si $a_0 \notin K$ alors, pour un choix convenable de $c_1, \dots, c_d \in K$ (voir lemme 4.2), le polynôme

$$g(X_1, \dots, X_d, T) := f(X_1 + c_1T, \dots, X_d + c_dT, T) = b_0T^r + b_1T^{r-1} + \dots + b_r$$

avec $b_0 \in K^\times$. Étant donné que $g(x_1 - c_1x_n, \dots, x_d - c_dx_n, x_n) = 0$, cela montre que x_n est entier sur $K[x_1 - c_1x_n, \dots, x_d - c_dx_n]$ et donc que A est fini sur $K[x_1 - c_1x_n, \dots, x_d - c_dx_n, x_{d+1}, \dots, x_{n-1}]$. □

Remarque 4.4. Si $A = K[x]$ est obtenu par un seul élément alors $K[x]$ est un K -espace vectoriel de dimension finie.

Exemple 4.5. Illustrons le procédé de la preuve à partir d'un exemple. Soit $A = K[X, Y]/(XY - 1)$. Dans A , le polynôme $f(X, Y) = XY - 1$ est nul. Or $X \notin K$; nous avons alors recours à la partie homogène de plus haut degré de f , à savoir ici $f_2(X, Y) = XY$. On remarque que $f_2(1, 1) = 1$ et donc nous prenons $c_1 = 1$. Posons x et y l'image respective de X et Y dans le quotient. En adoptant les notations de la preuve précédente :

$$g(x - 1.y, y) = y^2 + (x - y) - 1 = f(x, y) = 0.$$

Par conséquent y est entier sur $K[x - y]$ et donc A est une extension finie de $K[x - y]$. Noter que les rôles de X et Y peuvent être intervertis.

Corollaire 4.6 (Lemme de Zariski). Soient $K \subseteq L$ deux corps. Si L est une K -algèbre de type fini alors L/K est une extension (finie) algébrique. En particulier, $L = K$ si K est algébriquement clos.

PREUVE. Le lemme de normalisation de Noether fournit l'existence d'éléments $x_1, \dots, x_d \in L$ tels que L est une extension finie de $K[x_1, \dots, x_d]$. Or $A = K[x_1, \dots, x_d]$ est un corps : soit x un élément non

nul de A , alors $x^{-1} \in L$ et est donc entier sur $K[x_1, \dots, x_d]$; il satisfait donc à une équation de la forme

$$(x^{-1})^d + a_{d-1}(x^{-1})^{d-1} + \dots + a_1 x^{-1} + a_0 = 0$$

avec les coefficients $a_i \in K[x_1, \dots, x_d]$. En multipliant cette équation de part et d'autre par x^{d-1} , cela montre que $x^{-1} \in K[x_1, \dots, x_d]$. Puisque cet anneau est un corps et que x_1, \dots, x_d sont algébriquement indépendants sur K , nécessairement $K[x_1, \dots, x_d] = K$. Ainsi L/K est une extension finie et en particulier algébrique. \square

Théorème 4.7. (Nullstellensatz faible) *Soit K un corps algébriquement clos; l'application suivante*

$$\begin{aligned} \mathbf{A}^n(K) &\longrightarrow \operatorname{Spm} K[X_1, \dots, X_n] \\ (a_1, \dots, a_n) &\longmapsto (X_1 - a_1, \dots, X_n - a_n) \end{aligned} \quad (4.2)$$

est une bijection.

Nota Bene 4.8. L'application (4.2) est bien définie : l'idéal $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ est le noyau du morphisme $K[X_1, \dots, X_n] \rightarrow K$ d'évaluation en (a_1, \dots, a_n) , qui est clairement surjectif. Dès lors $K[X_1, \dots, X_n]/\mathfrak{m} \simeq K$ est un corps, i.e. \mathfrak{m} est un idéal maximal de $K[X_1, \dots, X_n]$.

PREUVE. Soit $\mathfrak{m} \in \operatorname{Spm} K[X_1, \dots, X_n]$ un idéal maximal. Le quotient $K[X_1, \dots, X_n]/\mathfrak{m}$ est un corps et est de type fini en tant que K -algèbre (il est engendré par $X_1 + \mathfrak{m}, \dots, X_n + \mathfrak{m}$). Ainsi, le lemme de Zariski nous apprend qu'il est algébrique sur K . Or K est algébriquement clos, ils sont donc égaux. En posant $a_i \in K$ la classe de X_i dans $K[X_1, \dots, X_n]/\mathfrak{m}$ pour tout i , il s'en suit que $X_i - a_i \in \mathfrak{m}$ et donc que \mathfrak{m} contient l'idéal $(X_1 - a_1, \dots, X_n - a_n)$. Puisqu'il est maximal, ils sont égaux. L'unicité de (a_1, \dots, a_n) provient du fait que si (b_1, \dots, b_n) est un n -uplet vérifiant la même propriété alors $a_i - b_i = (X_i - b_i) - (X_i - a_i)$ est un élément de \mathfrak{m} en chaque i , et sont donc forcément nuls (sinon \mathfrak{m} comprendrait des inversibles de K). \square

Corollaire 4.9 (Existence des zéros). *Soit K un corps algébriquement clos; pour tout idéal propre \mathfrak{a} de $K[X_1, \dots, X_n]$ il existe un point de $\mathbf{A}^n(K)$ qui est racine de tout élément de \mathfrak{a} .*

PREUVE. Soit \mathfrak{a} un idéal propre de $K[X_1, \dots, X_n]$; il est alors contenu dans un idéal maximal \mathfrak{m} et il suit du Nullstellensatz que $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ pour un n -uplet $(a_1, \dots, a_n) \in \mathbf{A}^n(K)$. Ainsi (a_1, \dots, a_n) est une racine commune aux éléments de \mathfrak{a} . \square

Nota Bene 4.10. Autrement dit, sous l'hypothèse (indispensable) que K est algébriquement clos : un ensemble algébrique $V(\mathfrak{a})$ sur K est vide à la seule et unique condition que $\mathfrak{a} = K[X_1, \dots, X_n]$.

Exemple 4.11. Soit K un corps algébriquement clos; dans le cas particulier où $\mathfrak{a} = (f)$, l'ensemble algébrique $V(f)$ est vide si et seulement si $f \in K^\times$.

Remarque 4.12. Ce résultat n'est pas vrai lorsque K n'est pas algébriquement clos : l'idéal $(X^2 + 1)$ de $\mathbf{R}[X]$ est maximal bien que $X^2 + 1$ n'admet aucune racine réelle.

5 Les idéaux radicaux

Définition 5.1. Le *nilradical* d'un anneau A est l'idéal de A constitué des éléments nilpotents de A :

$$\operatorname{Nil}(A) = \{a \in A \mid a^n = 0 \text{ pour un certain } n > 0\}.$$

Remarque 5.2. Noter qu'un anneau est réduit si et seulement si son nilradical est réduit à $\{0\}$. Ainsi tout anneau intègre admet un nilradical réduit à $\{0\}$ (mais ce ne sont pas les seuls : si $n \in \mathbf{Z}$ est sans facteur carré alors $\mathbf{Z}/n\mathbf{Z}$ est réduit). Également, $\operatorname{Nil}(A) = A$ si et seulement si $A = 0$.

Exemple 5.3. Soit $n \in \mathbf{Z} - \{0\}$ dont la factorisation en nombres premiers est $n = \pm p_1^{s_1} \cdots p_m^{s_m}$; alors

$$\text{Nil}(\mathbf{Z}/n\mathbf{Z}) = (p_1 \cdots p_m)\mathbf{Z}/n\mathbf{Z}.$$

En effet, si $a^k \equiv 0 \pmod n$ alors n divise a^k et donc $p_1 \cdots p_m$ divise a . Réciproquement, si $p_1 \cdots p_m$ divise a alors $a^s \equiv 0 \pmod n$ où $s \geq \text{Max}\{s_1, \dots, s_m\}$. En particulier, si n est sans facteur carré (*i.e.* $s_1 = \dots = s_m = 1$) alors $\text{Nil}(\mathbf{Z}/n\mathbf{Z}) = n\mathbf{Z}/n\mathbf{Z} = 0$.

Théorème 5.4 (de Krull). *Le nilradical de A est l'intersection de tous les idéaux premiers de A . En particulier, $\text{Nil}(A)$ est un idéal de A .*

PREUVE. Soit $\mathfrak{p} \in \text{Spec } A$ et soit $a \in \text{Nil}(A)$ avec $a^n = 0$. Comme $a^n = 0 \in \mathfrak{p}$ et \mathfrak{p} est premier, $a \in \mathfrak{p}$. Ainsi $\text{Nil}(A) \subseteq \bigcap_{\mathfrak{p}} \mathfrak{p}$.

Réciproquement supposons que A soit non nul (*i.e.* $\text{Nil}(A) \neq A$). Soient $s \in A - \text{Nil}(A)$ et posons $S = \{s^n \mid n \in \mathbf{N}\}$; alors $0 \notin S$ et donc $(0) \cap S = \emptyset$. Ainsi $X = \{\mathfrak{a} \text{ idéal de } A \mid \mathfrak{a} \cap S = \emptyset\}$ est non vide et inductivement ordonné : $\mathfrak{a} \subseteq \mathfrak{b}$, si $\mathfrak{b} \cap S = \emptyset$ alors $\mathfrak{a} \cap S = \emptyset$. Le lemme de Zorn fournit l'existence d'un élément maximal $\mathfrak{q} \in X$.

Alors \mathfrak{q} est premier : pour tout élément $a \in A$, soit $\mathfrak{q} + (a) \in X$, ce qui revient à dire que $a \in \mathfrak{q}$; soit $\mathfrak{q} + (a) \notin X$ et cela revient à dire qu'il existe un $n \in \mathbf{N}$ et un $c \in A$ tels que $s^n - ac \in \mathfrak{q}$. Dès lors, si a, b sont deux éléments de A dont seul le produit est dans \mathfrak{q} , il existe un $n, m \in \mathbf{N}$ et un $c, d \in A$ tels que $s^n - ac \in \mathfrak{q}$ et $s^m - bd \in \mathfrak{q}$. Comme $s^n - ac \in \mathfrak{q}$, il en va de même pour $bs^n - abc$ et donc $bs^n \in \mathfrak{q}$ (car ab est supposé dans \mathfrak{q}). Donc $s^{n+m} - bds^n \in \mathfrak{q}$ et ainsi $s^{n+m} \in \mathfrak{q}$ venant contredire le fait que $\mathfrak{q} \in X$. Ainsi \mathfrak{q} est premier.

Par conséquent, pour chaque élément non nilpotent s de A , il existe un idéal premier \mathfrak{p} de A vérifiant $\mathfrak{p} \cap \{s^n \mid n \in \mathbf{N}\} = \emptyset$. Ainsi $(\bigcap_{\mathfrak{p}} \mathfrak{p}) \cap (A - \text{Nil}(A)) = \emptyset$ et ceci fournit l'inclusion réciproque. \square

Définition 5.5. Le *radical* d'un idéal \mathfrak{a} de A est l'idéal de A défini par

$$\text{Rad}(\mathfrak{a}) = \{a \in A \mid a^n \in \mathfrak{a} \text{ pour un certain } n > 0\}.$$

Nota Bene 5.6. Évidemment $\text{Nil}(A) = \text{Rad}((0))$. De plus, puisque sous $\pi_{\mathfrak{a}} : A \twoheadrightarrow A/\mathfrak{a}$, $\text{Rad}(\mathfrak{a})$ est envoyé sur $\text{Rad}(\mathfrak{a})/\mathfrak{a} = \text{Nil}(A/\mathfrak{a})$, le théorème de Krull montre que le radical de \mathfrak{a} est l'intersection des idéaux premiers contenant \mathfrak{a} . En particulier $\text{Rad}(\mathfrak{a})$ est un idéal.

Proposition 5.7. *Soit \mathfrak{a} un idéal d'un anneau A ; les propriétés suivantes sont vérifiées :*

- (a) *Le radical de \mathfrak{a} est un idéal de A contenant \mathfrak{a} . En particulier $\text{Rad}(A) = A$.*
- (b) *Pour tout $a \in A$ et tout $n > 0$, $\text{Rad}((a)) = \text{Rad}((a^n))$.*
- (c) *$\text{Rad}(\text{Rad}(\mathfrak{a})) = \text{Rad}(\mathfrak{a})$.*

Remarque 5.8. Si $\mathfrak{a} \subseteq \mathfrak{b}$ sont deux idéaux d'un anneau A alors $\text{Rad}(\mathfrak{a}) \subseteq \text{Rad}(\mathfrak{b})$ mais la réciproque est fautive : nous verrons lors de la proposition 5.12 que les radicaux de $12\mathbf{Z}$ et $18\mathbf{Z}$ sont égaux (et valent $6\mathbf{Z}$) pourtant aucun de ces deux idéaux est contenu dans l'autre.

Définition 5.9. Un idéal \mathfrak{a} de A est *radical* s'il est égal à son radical. Autrement dit, si A/\mathfrak{a} est réduit.

Remarque 5.10. Comme tout anneau intègre est réduit, les idéaux premiers (et à plus forte raison, les idéaux maximaux) sont radicaux ; toutefois ce résultat se généralise à n'importe quel anneau commutatif (voir proposition 5.11). Le point (c) de la proposition 5.7 fournit que $\text{Rad}(\mathfrak{a})$ est radical et est donc le plus petit idéal radical de A contenant \mathfrak{a} .

Proposition 5.11. *Tout idéal premier (et à plus forte raison, tout idéal maximal) d'un anneau commutatif est radical.*

PREUVE. Soit \mathfrak{p} un idéal premier de A ; il suffit de vérifier que $\text{Rad}(\mathfrak{p}) \subseteq \mathfrak{p}$: si $a^n \in \mathfrak{p}$ alors il est possible de montrer par induction que $a \in \mathfrak{p}$. \square

Proposition 5.12. *Si A est factoriel alors tout élément non nul a de A se factorise de façon unique en $a = up_1^{s_1} \cdots p_m^{s_m}$ où $u \in A^\times$ et où les p_i sont des irréductibles distincts. Alors $\text{Rad}((a)) = (p_1 \cdots p_m)$.*

PREUVE. L'inclusion dans le sens contraire à la lecture s'obtient en prenant le maximum des s_i . Réciproquement, si $x \in \text{Rad}((a))$, il existe un $n \in \mathbb{N}$ tel que $x^n \in (a)$. Ainsi a divise x^n et donc chaque p_i aussi. Puisqu'ils sont premiers, chaque p_i divise x et, comme ils sont distincts, $p_1 \cdots p_m$ divise x . Autrement dit $x \in (p_1 \cdots p_m)$. \square

Remarque 5.13. Dans un anneau factoriel A , l'idéal (a) est radical si et seulement si $a = 0$ ou est sans facteur carré.

Exemple 5.14. Dans l'anneau \mathbb{Z} :

- le radical de $4\mathbb{Z}$ est $2\mathbb{Z}$ car $4 = 2^2$,
- le radical de $6\mathbb{Z}$ est $6\mathbb{Z}$ car $6 = 2 \times 3$; en particulier, la réciproque de 5.11 n'est pas vérifiée,
- le radical de $6125\mathbb{Z}$ est $35\mathbb{Z}$ car $6125 = 5^3 \times 7^2$,
- le radical de $p\mathbb{Z}$ est $p\mathbb{Z}$ pour tout nombre premier $p \in \mathbb{Z}$; nous retrouvons la proposition 5.11.

Remarque 5.15. Si \mathfrak{a} et \mathfrak{b} sont deux idéaux radicaux de A alors leur intersection est un idéal radical, avec $\text{Rad}(\mathfrak{a} \cap \mathfrak{b}) = \text{Rad}(\mathfrak{a}) \cap \text{Rad}(\mathfrak{b}) = \text{Rad}(\mathfrak{a}\mathfrak{b})$; en revanche $\mathfrak{a} + \mathfrak{b}$ n'est en général pas radical. Pour le voir, il suffit par exemple de considérer $\mathfrak{a} = (X^2 - Y)$ et $\mathfrak{b} = (X^2 + Y)$ deux idéaux premiers de $K[X, Y]$ et pourtant $X^2 \in \mathfrak{a} + \mathfrak{b}$ et $X \notin \mathfrak{a} + \mathfrak{b}$. Plus précisément $\text{Rad}(\mathfrak{a} + \mathfrak{b}) = \text{Rad}(\text{Rad}(\mathfrak{a}) + \text{Rad}(\mathfrak{b}))$.

Conclusion 5.16. Soit \mathfrak{a} un idéal de A . Si A/\mathfrak{a} est un corps alors A/\mathfrak{a} est intègre et donc A/\mathfrak{a} est réduit. Autrement dit **tout idéal maximal est premier et tout idéal premier est radical**. Noter qu'aucune réciproque n'est vraie.

Exemple 5.17. Dans l'anneau $K[X, Y]$, l'idéal (X, Y) est maximal, l'idéal (X) est premier mais pas maximal et l'idéal (XY) est radical mais pas premier (il s'agit du noyau de $K[X, Y] \rightarrow K[X] \times K[Y]$ donnée par $f \mapsto (f(X, 0), f(0, Y))$).

Résumé 5.18. Soit A est un anneau factoriel et soit $a \in A$:

- (a) est maximal si et seulement si a est irréductible dans A : à condition que A soit principal.
- (a) est premier si et seulement si $a = 0$ ou a est irréductible dans A .
- (a) est radical si et seulement si $a = 0$ ou a est sans facteur carré.

6 Les idéaux radicaux et les ensembles algébriques

Définition 6.1. Soit K un corps ; l'idéal *rattaché* à un sous-ensemble de points W de $\mathbf{A}^n(K)$ est l'idéal $I(W)$ des polynômes de $K[X_1, \dots, X_n]$ s'annulant en tout point de W :

$$I(W) = \{f \in K[X_1, \dots, X_n] \mid f(P) = 0 \text{ pour tout } P \in W\}.$$

Remarque 6.2. Il s'agit clairement d'un idéal radical de $K[X_1, \dots, X_n]$, distinct de $K[X_1, \dots, X_n]$ pourvu que W soit non vide étant donné que 1 n'admet pas de racine peu importe la caractéristique de K . Noter que si $V \subseteq W$ alors $I(V) \supseteq I(W)$.

Proposition 6.3. *Soit K un corps infini ; les idéaux rattachés de $K[X_1, \dots, X_n]$ satisfont :*

- (a) $I(\emptyset) = K[X_1, \dots, X_n]$ et $I(\mathbf{A}^n(K)) = (0)$.
- (b) $I(\bigcup_{i \in I} W_i) = \bigcap_{i \in I} I(W_i)$ pour toute famille $(W_i)_{i \in I}$ de sous-ensembles de $\mathbf{A}^n(K)$.

PREUVE. Seulement le deuxième point de **(a)** nécessite une justification : il s'agit d'une réécriture du résultat [Préface, Lemme 1.6]. \square

Exemple 6.4. Soit P le point $(a_1, \dots, a_n) \in \mathbf{A}^n(K)$ et posons $\mathfrak{m}_P = (X_1 - a_1, \dots, X_n - a_n)$. Clairement $\mathfrak{m}_P \subseteq I(P)$ et est maximal ; ils sont alors égaux puisque $I(P)$ est un idéal propre.

Proposition 6.5. Soient K un corps et W un sous-ensemble de $\mathbf{A}^n(K)$. Alors $VI(W)$ est le plus petit ensemble algébrique de $\mathbf{A}^n(K)$ contenant W . En particulier $VI(W) = W$ si W est algébrique.

PREUVE. Il est clair que $VI(W)$ est un ensemble algébrique contenant W . Soit $V(\mathfrak{a})$ un ensemble algébrique contenant W ; alors $\mathfrak{a} \subseteq I(W)$ et donc $V(\mathfrak{a}) \supseteq VI(W)$. \square

Remarque 6.6. Soit \mathfrak{a} un idéal de $K[X_1, \dots, X_n]$. Clairement $\mathfrak{a} \subseteq IV(\mathfrak{a})$ mais cette inclusion est stricte en général : pour $m \geq 2$, $V(X_1^m) = \{(0, a_2, \dots, a_n) \in \mathbf{A}^n(K)\}$ et $IV(X_1^m) = (X_1) \supset (X_1^m)$. Toutefois $(X_1) = \text{Rad}((X_1^m))$ et ceci est au cœur du résultat suivant.

Théorème 6.7 (Nullstellensatz fort). Soit K un corps algébriquement clos ; tout idéal \mathfrak{a} de l'anneau $K[X_1, \dots, X_n]$ vérifie $IV(\mathfrak{a}) = \text{Rad}(\mathfrak{a})$. En particulier $IV(\mathfrak{a}) = \mathfrak{a}$ si et seulement si \mathfrak{a} est radical.

PREUVE. Nous venons de remarquer que $IV(\mathfrak{a}) \supseteq \mathfrak{a}$ et donc $IV(\mathfrak{a}) \supseteq \text{Rad}(\mathfrak{a})$. Pour l'inclusion réciproque, considérons un polynôme h s'annulant sur $V(\mathfrak{a})$ et déduisons qu'il existe un $N > 0$ pour lequel $h^N \in \mathfrak{a}$. Supposons h non nul (trivial sinon) et soit $\{g_1, \dots, g_m\}$ un ensemble générateur de \mathfrak{a} . Considérons le système de $m + 1$ équations à $n + 1$ indéterminées :

$$\begin{cases} g_i(X_1, \dots, X_n) &= 0 & \text{pour } i = 1, \dots, m \\ 1 - Yh(X_1, \dots, X_n) &= 0. \end{cases}$$

Si (a_1, \dots, a_n, b) satisfait les m premières équations alors $(a_1, \dots, a_n) \in V(\mathfrak{a})$ et dès lors h s'annule en (a_1, \dots, a_n) ; par conséquent (a_1, \dots, a_n, b) ne satisfait pas la dernière équation. Ainsi ce système d'équations est inconsistent et donc, selon le Nullstellensatz faible, il existe des $f_i \in K[X_1, \dots, X_n, Y]$ tels que

$$1 = \sum_{i=1}^m f_i g_i + f_{m+1} (1 - Yh)$$

en tant qu'éléments de $K[X_1, \dots, X_n, Y]$. Le morphisme $K[X_1, \dots, X_n, Y] \rightarrow K(X_1, \dots, X_n)$ déterminé par $X_i \mapsto X_i$ et $Y \mapsto h^{-1}$ appliqué à la précédente égalité montre que

$$1 = \sum_{i=1}^m f_i(X_1, \dots, X_n, h^{-1}) g_i(X_1, \dots, X_n) \quad (6.1)$$

en tant qu'éléments de $K(X_1, \dots, X_n)$ cette fois-ci. Chaque $f_i(X_1, \dots, X_n, h^{-1})$ est le quotient d'un polynôme de $K[X_1, \dots, X_n]$ par une puissance $N_i > 0$ de h . Soit $N = \text{Max}\{N_1, \dots, N_m\}$ la plus grande de ces puissances ; en multipliant (6.1) par h^N , il s'en suit que h^N est un élément de \mathfrak{a} :

$$h^N = \sum_{i=1}^m (\text{polynôme en } X_1, \dots, X_n) g_i(X_1, \dots, X_n) \in \mathfrak{a}.$$

\square

Remarque 6.8. Puisque $V(0) = \mathbf{A}^n(K)$, $I(\mathbf{A}^n(K)) = IV(0) = \text{Rad}((0)) = (0)$: seul le polynôme nul s'annule en tout point de $\mathbf{A}^n(K)$. Ceci vient en partie justifier la fin du point **(a)** de la prop. 6.3.

Nota Bene 6.9. Le Nullstellensatz fort implique sa version faible, justifiant la terminologie. Si $V(\mathfrak{a})$ est vide alors $IV(\mathfrak{a}) = I(\emptyset) = K[X_1, \dots, X_n]$. Par la version forte du Nullstellensatz, ceci est équivalent à $\text{Rad}(\mathfrak{a}) = K[X_1, \dots, X_n]$ et donc $\mathfrak{a} = K[X_1, \dots, X_n]$ puisque $1 \in \text{Rad}(\mathfrak{a})$ implique $1 \in \mathfrak{a}$.

Corollaire 6.10. *Soit K un corps algébriquement clos ; le radical d'un idéal de $K[X_1, \dots, X_n]$ est égal à l'intersection des idéaux maximaux le contenant.*

PREUVE. Soit \mathfrak{a} un idéal de $K[X_1, \dots, X_n]$; puisque tout idéal maximal est radical, tout idéal maximal contenant \mathfrak{a} contient aussi $\text{Rad}(\mathfrak{a})$ par minimalité et donc :

$$\text{Rad}(\mathfrak{a}) \subseteq \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}.$$

En tout $P = (a_1, \dots, a_n) \in \mathbf{A}^n(K)$ l'idéal $\mathfrak{m}_P = (X_1 - a_1, \dots, X_n - a_n)$ est maximal dans $K[X_1, \dots, X_n]$ et $f \in \mathfrak{m}_P$ si et seulement si $f(P) = 0$ (exemple 6.4). Ainsi $\mathfrak{m}_P \supseteq \mathfrak{a}$ si et seulement si $P \in V(\mathfrak{a})$. Si $f \in \mathfrak{m}_P$ en tout point $P \in V(\mathfrak{a})$ alors f s'annule sur $V(\mathfrak{a})$ et donc $f \in IV(\mathfrak{a}) = \text{Rad}(\mathfrak{a})$. Dès lors :

$$\text{Rad}(\mathfrak{a}) \supseteq \bigcap_{P \in V(\mathfrak{a})} \mathfrak{m}_P \supseteq \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}.$$

□

Corollaire 6.11 (Correspondance). *Soit K un corps algébriquement clos ; l'application $\mathfrak{a} \mapsto V(\mathfrak{a})$ définit une correspondance entre les idéaux radicaux de $K[X_1, \dots, X_n]$ et les sous-ensembles algébriques de $\mathbf{A}^n(K)$, d'inverse I .*

PREUVE. Le théorème 6.7 nous apprend que $IV(\mathfrak{a}) = \mathfrak{a}$ puisque \mathfrak{a} est supposé radical ; la proposition 6.5 nous apprend quant-à-elle que $VI(W) = W$ lorsque W est un ensemble algébrique. Ainsi V et I sont inverses l'une de l'autre. □

Remarque 6.12. Cette correspondance renverse les inclusions ; ainsi les idéaux radicaux maximaux propres correspondent aux ensembles algébriques minimaux non vides. Or les idéaux radicaux maximaux propres sont exactement les idéaux maximaux de $K[X_1, \dots, X_n]$ et les ensembles algébriques minimaux non vides sont les singletons. Puisque $I((a_1, \dots, a_n)) = (X_1 - a_1, \dots, X_n - a_n)$ (cf. exemple 6.4), les idéaux maximaux de $K[X_1, \dots, X_n]$ sont précisément les idéaux $(X_1 - a_1, \dots, X_n - a_n)$ où (a_1, \dots, a_n) est un point de $\mathbf{A}^n(K)$.

Proposition 6.13. *Soit K un corps ; un polynôme $h \in \text{Rad}(\mathfrak{a})$ si et seulement si $1 \in (\mathfrak{a}, 1 - Yh)$ (l'idéal de $K[X_1, \dots, X_n, Y]$ engendré par les éléments de \mathfrak{a} et $1 - Yh$).*

PREUVE. Au cours de la preuve du théorème 6.7 nous avons montré que $1 \in (\mathfrak{a}, 1 - Yh)$ implique que $h \in \text{Rad}(\mathfrak{a})$. Réciproquement, les égalités

$$1 = Y^N h^N + (1 - Y^N h^N) = Y^N h^N + (1 - Yh)(1 + Yh + \dots + Y^{N-1} h^{N-1})$$

impliquent que si $h^N \in \mathfrak{a}$ alors $1 \in \mathfrak{a} + (1 - Yh)$. □

Exemple 6.14. Soient W, W' deux ensembles algébriques. Comme $W \cap W'$ est le plus grand ensemble algébrique contenu à la fois dans W et à la fois dans W' , $I(W \cap W')$ est le plus petit idéal radical contenant à la fois $I(W)$ et à la fois $I(W')$:

$$I(W \cap W') = \text{Rad}(I(W) + I(W')).$$

Par exemple si $W = V(X^2 - Y)$ et $W' = V(X^2 + Y)$ alors $I(W \cap W') = \text{Rad}((X^2, Y)) = (X, Y)$ en caractéristique différente de 2. En effet, on montre facilement que $(X^2 - Y) + (X^2 + Y) = (X^2, Y)$ dans ces conditions. Clairement $(X, Y) \in \text{Rad}((X^2, Y))$ et l'inclusion réciproque découle du fait que (X, Y) est maximal dans $K[X, Y]$.

7 Quelques propriétés de la topologie de Zariski

Lors de cette section, nous étudions plus en profondeur la topologie de Zariski sur $\mathbf{A}^n(K)$, ainsi que sur ses sous-ensembles algébriques. La proposition 6.5 affirme que $VI(W)$ est la fermeture de W quel que soit le sous-ensemble W de $\mathbf{A}^n(K)$. Le corollaire 6.11 exhibe une correspondance entre les sous-ensembles fermés de $\mathbf{A}^n(K)$ et les idéaux radicaux de $K[X_1, \dots, X_n]$. Sous cette correspondance, les sous-ensembles fermés d'un ensemble algébrique V correspondent aux idéaux radicaux de $K[X_1, \dots, X_n]$ contenant $I(V)$.

Proposition 7.1. *Soit K un corps et soit V un sous-ensemble algébrique de $\mathbf{A}^n(K)$. Les points de V sont fermés pour la topologie de Zariski. En particulier la topologie de Zariski sur $\mathbf{A}^n(K)$ est T_1 .*

PREUVE. Soit $P = (a_1, \dots, a_n)$ un point de V ; le singleton $\{P\}$ est l'ensemble algébrique défini par l'idéal $(X_1 - a_1, \dots, X_n - a_n)$. \square

Proposition 7.2. *Soit K un corps et soit V un sous-ensemble algébrique de $\mathbf{A}^n(K)$. Toute chaîne ascendante de sous-ensembles ouverts de V est ultimement constante. De façon équivalente, toute chaîne descendante de sous-ensembles fermés de V est ultimement constante.*

PREUVE. Nous le montrons pour les sous-ensembles fermés de V : une chaîne descendante $V_1 \supseteq V_2 \supseteq \dots$ de sous-ensembles fermés de V donne lieu à une chaîne ascendante $I(V_1) \subseteq I(V_2) \subseteq \dots$ d'idéaux radicaux qui est ultimement constante puisque $K[X_1, \dots, X_n]$ est noethérien. \square

Définition 7.3. Un espace topologique satisfaisant la condition de chaîne descendante sur les sous-ensembles fermés est dit *noethérien*.

Remarque 7.4. La topologie de Zariski sur $\mathbf{A}^n(K)$ fait de lui un espace topologique noethérien. Pour rappel, la condition de chaîne descendante sur V est équivalente au fait que tout sous-ensemble non vide d'un sous-ensemble fermé de V possède un élément minimal.

Proposition 7.5. *Soit K un corps et soit V un sous-ensemble algébrique de $\mathbf{A}^n(K)$. Tout recouvrement de V par des ouverts possède un sous-recouvrement fini.*

PREUVE. Étant donné un recouvrement de V par des ouverts, considérons \mathcal{U} la collection des sous-ensembles ouverts de V s'exprimant comme union finie des ensembles du recouvrement. Si V n'est pas compris dans \mathcal{U} alors il existe une chaîne ascendante infinie d'ensembles dans \mathcal{U} (axiome du choix dépendant), venant contredire la condition de chaîne ascendante sur les ouverts. \square

Remarque 7.6. La topologie de Zariski sur $\mathbf{A}^n(K)$ fait de lui un espace compact (mais pas T_2). La preuve précédente montre que tout espace topologique noethérien est compact. Puisque un sous-ensemble ouvert d'un espace topologique noethérien est lui-même noethérien, il est également compact.

8 Décomposition des espaces topologiques

Définition 8.1. Un espace topologique est *irréductible* s'il ne peut s'écrire comme l'union de deux sous-ensembles propres fermés.

Remarque 8.2. Soit X un espace topologique. Les assertions suivantes sont équivalentes et chaleureusement laissées en exercice au lecteur :

- (a) X est irréductible.
- (b) Toute paire d'ouverts de X admet une intersection non vide.
- (c) Tout ouvert non vide de X est dense dans X .

Par convention, l'espace vide n'est pas irréductible. Tout sous-ensemble ouvert non vide d'un espace topologique irréductible est également irréductible.

Exemple 8.3. Dans un espace T_2 , toute paire de points possède des voisinages ouverts disjoints ; ainsi les seuls espaces irréductibles à être T_2 sont ceux constitués d'un unique point.

Proposition 8.4. *Soit K un corps ; un ensemble algébrique W sur K est irréductible si et seulement si l'idéal $I(W)$ est premier.*

PREUVE. Soit W un ensemble algébrique sur K irréductible et soit $fg \in I(W)$. En chaque point de W , au moins f ou g s'annule et donc $W \subseteq V(f) \cup V(g)$. Ainsi W se décompose en :

$$W = (W \cap V(f)) \cup (W \cap V(g)).$$

Puisqu'il est supposé irréductible, l'un de ces deux ensembles doit être égal à W ; impliquant que f ou g s'annule sur tout W et donc que $I(W)$ est premier.

Soit W un ensemble algébrique sur K non irréductible et soient W_1, W_2 deux fermés distincts de W tels que $W = W_1 \cup W_2$. Comme $W_i \subset W$, nous avons $I(W) \subset I(W_i)$. En effet, si $I(W) = I(W_i)$ alors

$$W = VI(W) = VI(W_i) = W_i.$$

Soient $f_i \in I(W_i) - I(W)$. Alors $f_1 f_2 \in I(W_1) \cap I(W_2) = I(W)$ et donc $I(W)$ n'est pas premier. \square

Résumé 8.5. Il existe des correspondances entre certains idéaux de $K[X_1, \dots, X_n]$ et les sous-ensembles algébriques de $\mathbf{A}^n(K)$:

idéaux radicaux	\leftrightarrow	sous-ensembles algébriques
idéaux premiers	\leftrightarrow	sous-ensembles algébriques irréductibles
idéaux maximaux	\leftrightarrow	singletons.

Exemple 8.6. Soit $f \in K[X_1, \dots, X_n]$. Puisque l'anneau $K[X_1, \dots, X_n]$ est factoriel, (f) est premier si et seulement si f est irréductible. Par conséquent, si f est irréductible alors $V(f)$ l'est aussi. Réciproquement si f se factorise en $f = u f_1^{s_1} \cdots f_m^{s_m}$ où u est un inversible et les f_i sont des irréductibles distincts alors :

- $(f) = (f_1^{s_1}) \cap \cdots \cap (f_m^{s_m})$ et les $(f_i^{s_i})$ sont des idéaux distincts,
- $\text{Rad}(f) = (f_1) \cap \cdots \cap (f_m)$ et les (f_i) sont des idéaux premiers distincts,
- $V(f) = V(f_1) \cup \cdots \cup V(f_m)$ et les $V(f_i)$ sont des ensembles algébriques irréductibles distincts.

Lemme 8.7. *Soit X un espace topologique irréductible ; si $X = X_1 \cup \cdots \cup X_m$ où chaque X_i est fermé alors X est égal à l'un des X_i .*

PREUVE. Par induction sur m . Si $m = 2$ alors il s'agit de la définition d'irréductible. Sinon $m > 2$, alors $X = X_1 \cup (X_2 \cup \cdots \cup X_m)$ et donc $X = X_1$ ou $X = (X_2 \cup \cdots \cup X_m)$; si $X \neq X_2$ alors nous recommençons avec soit $X = X_2$, soit $X = X_3 \cup \cdots \cup X_m$ et ainsi de suite tant que $X \neq X_i$. \square

Proposition 8.8. *Soit X un espace topologique noethérien ; alors X est une union finie de sous-ensembles fermés irréductibles : $X = X_1 \cup \cdots \cup X_m$. Cette décomposition est de plus unique sous l'hypothèse d'absence d'inclusion entre les X_i (non-redondance) et à ordre des éléments près. Il s'agit exactement des sous-ensembles fermés irréductibles maximaux de X .*

PREUVE. Supposons que X ne peut s'écrire comme union finie d'irréductibles. Alors, puisque X est noethérien, il existe un sous-ensemble fermé non vide Y de X étant minimal parmi ceux ne pouvant s'écrire de cette manière. En particulier Y n'est pas irréductible et donc $Y = F_1 \cup F_2$ pour certains F_1, F_2 sous-ensembles fermés propres de Y . Puisque Y a été choisi minimal, F_1 et F_2 sont des unions finies de sous-ensembles fermés irréductibles, donc Y aussi et cela est absurde.

Pour l'unicité supposons que $X = X_1 \cup \dots \cup X_m = Y_1 \cup \dots \cup Y_\ell$ sont deux décompositions non-redondantes de X . Ainsi $X_i = \bigcup_{j=1}^\ell (X_i \cap Y_j)$ et donc, puisque X_i est irréductible, $X_i = X_i \cap Y_j$ pour un certain j . Il existe par conséquent une fonction $f: \{1, \dots, m\} \rightarrow \{1, \dots, \ell\}$ telle que $X_i \subseteq Y_{f(i)}$ en tout i . De façon analogue il existe une fonction $g: \{1, \dots, \ell\} \rightarrow \{1, \dots, m\}$ telle que $Y_j \subseteq X_{g(j)}$ en tout j . Étant donné que $X_i \subseteq Y_{f(i)} \subseteq X_{g \circ f(i)}$, il faut que $g \circ f(i) = i$ et donc $X_i = Y_{f(i)}$; similairement $f \circ g$ est l'identité sur $\{1, \dots, \ell\}$ et donc f et g sont inverses l'une de l'autre. Ces décompositions diffèrent ainsi uniquement par l'ordre dans lequel apparaisse les éléments. \square

Définition 8.9. Les X_i apparaissant dans la décomposition d'un espace topologique X noethérien (proposition 8.8) sont appelés les *composantes irréductibles* de X .

Exemple 8.10. Dans l'exemple 8.6, les $V(f_i)$ sont les composantes irréductibles de $V(f)$.

Exemple 8.11. Soit K un corps. Les composantes irréductibles de $V(Y^2 - XZ, Y - XZ)$ dans $\mathbf{A}^3(K)$ sont $V(X, Y)$, $V(Y, Z)$ et $V(Y - 1, XZ - 1)$.

Corollaire 8.12. Soit K un corps; l'espace affine $\mathbf{A}^n(K)$ est irréductible si et seulement si K est infini.

PREUVE. Si K est infini alors $I(\mathbf{A}^n(K)) = (0)$ est premier. En revanche, lorsque K est fini la topologie de Zariski sur $\mathbf{A}^n(K)$ est discrète, empêchant $\mathbf{A}^n(K)$ d'être irréductible. \square

Corollaire 8.13 (Principe de prolongement des identités algébriques). Soient K un corps infini, V un ensemble algébrique sur K strictement contenu dans $\mathbf{A}^n(K)$ et $f \in K[X_1, \dots, X_n]$. Si f s'annule en tout point de $\mathbf{A}^n(K) - V$ alors f s'annule en tout point de $\mathbf{A}^n(K)$.

PREUVE. Si f s'annule en tout point de $\mathbf{A}^n(K) - V$ alors $\mathbf{A}^n(K) - V \subseteq V(f)$ et donc $\mathbf{A}^n(K) = V \cup V(f)$. Toutefois K est infini et donc $\mathbf{A}^n(K)$ est irréductible. De plus V est supposé distinct de $\mathbf{A}^n(K)$; dès lors $V(f) = \mathbf{A}^n(K)$. \square

Remarque 8.14. Si K est infini alors tout ouvert non vide est dense dans $\mathbf{A}^n(K)$. Sous les mêmes hypothèses, tout $f \in K[X_1, \dots, X_n]$ définit une application polynomiale $\mathbf{A}^n(K) \rightarrow K: P \mapsto f(P)$ continue pour la topologie de Zariski : pour tout $a \in K$, $f^{-1}(\{a\}) = V(f - a)$ est un fermé de Zariski.

Exemple 8.15. Soit K un corps infini. Identifions topologiquement $M_n(K)$ à $\mathbf{A}^{n^2}(K)$. Noter que l'application $\det: M_n(K) \rightarrow K$ est polynomiale et donc $V = \det^{-1}(\{0\}) = \{M \in M_n(K) \mid \det M = 0\}$ est fermé. Dès lors $GL_n(K) = M_n(K) - V$ est un ouvert non vide et est donc dense dans $M_n(K)$. Ainsi, si une propriété polynomiale est vérifiée sur $GL_n(K)$ alors elle l'est aussi sur $M_n(K)$.

9 L'anneau des coordonnées et les fonctions régulières

Définition 9.1. Soit K un corps algébriquement clos; l'anneau des coordonnées d'un sous-ensemble algébrique V de $\mathbf{A}^n(K)$ est

$$K[V] := K[X_1, \dots, X_n]/I(V).$$

Nota Bene 9.2 (catégorique). L'anneau des coordonnées de V est une K -algèbre de type fini (nous donnerons un argument général en 11.3). C'est aussi un anneau réduit étant donné que $I(V)$ est radical; mais pas nécessairement intègre (à la seule et unique condition que V soit irréductible).

Définition 9.3. Soit K un corps algébriquement clos; une *fonction régulière* est la restriction d'une application polynomiale $f \in K[X_1, \dots, X_n]$ à un sous-ensemble algébrique de $\mathbf{A}^n(K)$.

Remarque 9.4. Deux polynômes $f, g \in K[X_1, \dots, X_n]$ définissent la même fonction régulière sur V si et seulement s'ils définissent le même élément de $K[V]$:

$$f|_V = g|_V \quad \text{ssi} \quad f \bmod I(V) = g \bmod I(V).$$

Ainsi $K[V]$ est l'anneau des fonctions régulières sur V . En chaque i la fonction renvoyant la i -ème coordonnée $x_i: V \rightarrow K: (a_1, \dots, a_n) \mapsto a_i$ est régulière; ainsi une autre manière de voir $K[V]$ est via l'isomorphisme de K -algèbres $K[V] \simeq K[x_1, \dots, x_n]$: l'anneau des coordonnées de V est la K -algèbre de type fini engendrée par les fonctions coordonnées sur V .

Exemple 9.5. Soit K algébriquement clos; l'application $V(Y - X^2) \subseteq \mathbf{A}^2(K) \rightarrow K: (x, y) \mapsto x$ est une fonction régulière. Par contre $V(Y^2 - X^3) \subseteq \mathbf{A}^2(K) \rightarrow K: (x, y) \mapsto y/x$ si x est non nul et $(0, y) \mapsto 0$ n'en est pas une.

Lemme 9.6. Soient K un corps algébriquement clos; un sous-ensemble algébrique V de $\mathbf{A}^n(K)$ est fini si et seulement si son anneau des coordonnées $K[V]$ est un K -ev de dimension finie.

PREUVE. Si $V = \{P_1, \dots, P_m\}$ est fini, avec chaque P_i distinct, alors $I(V) = \mathfrak{m}_{P_1} \cap \dots \cap \mathfrak{m}_{P_m}$ et le théorème chinois des restes implique que $K[V] \simeq K^m$. Noter que $\dim_K(K[V]) = \#V$.

Réciproquement $K[V] \simeq K[x_1, \dots, x_n]$ où les $x_i: V \rightarrow K$ sont les fonctions coordonnées. Puisque $\dim_K(K[V])$ est finie, la suite $(x_i^j)_{j \in \mathbf{N}}$ est K -linéairement dépendante en chaque i . Autrement dit, il existe en chaque i un naturel m_i et des scalaires $\lambda_{ij} \in K$ non tous nuls tels que $\sum_{j=0}^{m_i} \lambda_{ij} x_i^j = 0$. Dès lors, pour tout $(a_1, \dots, a_n) \in V$ et pour tout i , $\sum_{j=0}^{m_i} \lambda_{ij} a_i^j = 0$: seul un nombre fini de a_i est alors possible. \square

Remarque 9.7. Bien que toute K -algèbre de dimension finie soit une K -algèbre de type fini, la réciproque n'est pas vraie: le contre-exemple typique est $K[X]$ qui est une K -algèbre de type finie bien que $(1, X, X^2, X^3, \dots)$ est K -base de $K[X]$.

Remarque 9.8. Soit K un corps algébriquement clos, fixons V un sous-ensemble algébrique de $\mathbf{A}^n(K)$. Soit $W \subseteq V$ un ensemble algébrique sur K ; l'application de restriction à W :

$$-|_W: K[x_1, \dots, x_n] \longrightarrow K[x_1|_W, \dots, x_n|_W]$$

est un morphisme de K -algèbres (où les $x_i: V \rightarrow K$ sont les fonctions coordonnées sur V). Puisque $I(V) \subseteq I(W)$, le morphisme $\pi_W: K[X_1, \dots, X_n] \twoheadrightarrow K[W]$ se factorise et le diagramme suivant commute:

$$\begin{array}{ccc} K[V] & \xrightarrow{\pi_W} & K[W] \\ \downarrow \wr & & \downarrow \wr \\ K[x_1, \dots, x_n] & \xrightarrow{-|_W} & K[x_1|_W, \dots, x_n|_W]. \end{array}$$

L'ensemble $I_V(W) := \text{Ker}(\pi_W) = I(W)/I(V) \simeq \text{Ker}(-|_W)$ est alors un idéal radical de $K[V]$.

Théorème 9.9 (Nullstellensatz relatif). Soit K un corps algébriquement clos et soit V un sous-ensemble algébrique de $\mathbf{A}^n(K)$; l'application $W \mapsto I_V(W)$ définit une correspondance décroissante entre les ensembles algébriques sur K contenus dans V et les idéaux radicaux de $K[V]$.

Résumé 9.10 (Nullstellensatz relatif). Soit K un corps algébriquement clos et soit V un sous-ensemble algébrique de $\mathbf{A}^n(K)$; il existe des correspondances à l'échelle de V entre certains idéaux de $K[V]$ et les sous-ensembles algébriques de $\mathbf{A}^n(K)$ contenus dans V :

idéaux radicaux de $K[V]$	\leftrightarrow	ensembles algébriques contenus dans V
idéaux premiers de $K[V]$	\leftrightarrow	ensembles algébriques irréductibles contenus dans V
idéaux maximaux de $K[V]$	\leftrightarrow	singletons contenus dans V .

Remarque 9.11. Soit V un ensemble algébrique sur un corps algébriquement clos K ; si V_1, \dots, V_m sont ses composantes irréductibles alors $K[V] \rightarrow K[V_1] \times \dots \times K[V_m]$ par $f \mapsto (f|_{V_1}, \dots, f|_{V_m})$. Les $I_V(V_i)$ sont donc des idéaux premiers (puisque les V_i sont irréductibles) minimaux de $K[V]$: soit \mathfrak{p} un idéal premier contenu dans $K[V]$. S'il ne contient aucun des $I_V(V_i)$ alors il existe en chaque i un $f_i \in I_V(V_i) - \mathfrak{p}$. Ainsi $f_1 \dots f_m \in I_V(V) = (0)$ et donc $f_1 \dots f_m = 0 \in \mathfrak{p}$ ce qui est absurde.

10 Les applications régulières

Définition 10.1. Soit K un corps algébriquement clos et soient $V \subseteq \mathbf{A}^n(K)$ et $W \subseteq \mathbf{A}^m(K)$ deux ensembles algébriques sur K ; une application $\phi: V \rightarrow W$ est *régulière* si $\phi_i := x_i \circ \phi$ est une fonction régulière pour tout $i = 1, \dots, m$ (où les $x_i: W \rightarrow K$ sont les fonctions coordonnées sur W).

Nota Bene 10.2 (catégorique). Pour tout ensemble algébrique V sur K , $\text{Id}_V: V \rightarrow V$ est une application régulière, et la composition de deux applications régulières (compatibles) est régulière. Les ensembles algébriques sur K munis des applications régulières constituent une catégorie, notée **AlgSet** $_K$.

Remarque 10.3. Toute application régulière est continue pour la topologie de Zariski (dit Zariski-continue). La réciproque est fautive : l'application $\mathbf{A}^1(K) \rightarrow \mathbf{A}^1(K)$ échangeant seulement deux points et fixant les autres est Zariski-continue sur $\mathbf{A}^1(K)$ mais n'est pas régulière.

Exemple 10.4. Soient K un corps algébriquement clos et V un sous-ensemble algébrique de $\mathbf{A}^n(K)$:

- Les applications constantes entre deux ensembles algébriques sur K sont régulières.
- L'application $V \rightarrow \mathbf{A}^m(K): (x_1, \dots, x_n) \mapsto (x_1, \dots, x_m)$ où $m \leq n$ est régulière.
- L'application $V \rightarrow \mathbf{A}^{n+m}(K): (x_1, \dots, x_n) \mapsto (x_1, \dots, x_n, a_1, \dots, a_m)$ avec $m > 0$ est régulière.

Exemple 10.5. Soit K algébriquement clos ; l'application $\mathbf{A}^1(K) \rightarrow V(Y - X^2) \subseteq \mathbf{A}^2(K): t \mapsto (t, t^2)$ est un isomorphisme de la catégorie **AlgSet** $_K$: son inverse est donnée par $(x, y) \mapsto x$. Attention, l'application $\mathbf{A}^1(K) \rightarrow V(Y^2 - X^3) \subseteq \mathbf{A}^2(K): t \mapsto (t^2, t^3)$ est régulière bijective mais n'est pas pour autant un isomorphisme (sa réciproque n'est pas régulière, voir la deuxième de 9.5).

Remarque 10.6 (catégorique). Puisque les fonctions coordonnées sur V engendrent $K[V]$, une application $\phi: V \rightarrow W$ est régulière si et seulement si $f \circ \phi$ est une fonction régulière sur V pour toute fonction régulière f sur W . Ainsi toute application régulière $\phi: V \rightarrow W$ entre deux ensembles algébriques sur K définit un morphisme $\phi^*: K[W] \rightarrow K[V]: f \mapsto f \circ \phi$ de K -algèbres (contravariance).

Exemple 10.7. Soit K algébriquement clos et soit $\phi: \mathbf{A}^1(K) \rightarrow V(Y^2 - X^3) \subseteq \mathbf{A}^2(K): t \mapsto (t^2, t^3)$. Alors $\phi^*: K[V(Y^2 - X^3)] \rightarrow K[T]$ est donnée par $x \mapsto T^2$ et $y \mapsto T^3$ où x et y sont les fonctions coordonnées sur $V(Y^2 - X^3)$. Noter que ϕ^* est injective – tout comme ϕ – mais n'est pas surjective car son image est $K[T^2, T^3]$ et diffère de $K[T]$.

Exemple 10.8. Soit K algébriquement clos et soit $\phi: \mathbf{A}^1(K) \rightarrow V(Y - X^2) \subseteq \mathbf{A}^2(K): t \mapsto (t, t^2)$. Alors $\phi^*: K[V(Y - X^2)] \rightarrow K[T]$ est donné par $x \mapsto T$ et $y \mapsto T^2$ où x et y sont les fonctions coordonnées sur $V(Y - X^2)$. Le morphisme ϕ^* est un isomorphisme – tout comme ϕ – dont l'inverse est donné par $T \mapsto x$.

Remarque 10.9 (catégorique). Nous formaliserons à la section suivante le fait que $K[-]$ soit un foncteur ; en conséquence il transporte les isomorphismes : si $\phi: V \rightarrow W$ est un isomorphisme alors $\phi^*: K[W] \rightarrow K[V]$ est un isomorphisme. Par exemple $K[T^2, T^3] \not\cong K[T]$ et donc le morphisme de l'exemple 10.7 ne peut pas être un isomorphisme.

11 Fonctorialité

Notation 11.1. Soit K un corps algébriquement clos ; nous désignons la catégorie des K -algèbres de type fini et réduites munies des morphismes de K -algèbres par \mathbf{RedAlg}_K .

Théorème 11.2. Soit K un corps algébriquement clos ; le foncteur $K[-]: \mathbf{AlgSet}_K \rightarrow \mathbf{RedAlg}_K$ associant $V \mapsto K[V]$ et $(\phi: V \rightarrow W) \mapsto (\phi^*: K[W] \rightarrow K[V])$ réalise une anti-équivalence de catégories.

PREUVE. Les discussions catégoriques précédentes montrent que $K[-]$ est contravariant et bien défini. Les propositions 11.4 et 11.5 impliquent que $K[-]$ est une anti-équivalence de catégories. \square

Lemme 11.3. Soit K un corps et soit A une K -algèbre ; A est de type fini si et seulement si A est le quotient d'un $K[X_1, \dots, X_n]$ par un de ses idéaux (avec $n > 0$).

PREUVE. Si $A \simeq K[X_1, \dots, X_n]/\mathfrak{a}$ alors A est engendré en tant que K -algèbre par l'image des $X_i \bmod \mathfrak{a}$ dans A . Réciproquement, si a_1, \dots, a_n engendrent A en tant que K -algèbre alors le morphisme $K[X_1, \dots, X_n] \twoheadrightarrow A: f \mapsto f(a_1, \dots, a_n)$ est surjectif ; il suffit alors de quotienter par son noyau. \square

Proposition 11.4. Soit K un corps algébriquement clos ; le foncteur $K[-]: \mathbf{AlgSet}_K \rightarrow \mathbf{RedAlg}_K$ est essentiellement surjectif. Autrement dit, toute K -algèbre de type fini et réduite est isomorphe à l'anneau des coordonnées d'un ensemble algébrique sur K .

PREUVE. Soit A une K -algèbre ; alors A est de type fini si et seulement si $A \simeq K[X_1, \dots, X_n]/\mathfrak{a}$ pour un certain $n > 0$ et un certain idéal \mathfrak{a} de A . De plus, A est réduite si et seulement si \mathfrak{a} est radical. Puisque K est supposé algébriquement clos, $\mathfrak{a} = IV(\mathfrak{a})$ et donc $A \simeq K[V(\mathfrak{a})]$. \square

Proposition 11.5. Soit K un corps algébriquement clos ; le foncteur $K[-]: \mathbf{AlgSet}_K \rightarrow \mathbf{RedAlg}_K$ est pleinement fidèle. Autrement dit, l'application $\mathrm{Hom}(V, W) \rightarrow \mathrm{Hom}(K[W], K[V]): \phi \mapsto \phi^*$ est bijective pour tous ensembles algébriques V et W sur K .

PREUVE. Notons $K[W] \simeq K[x_1, \dots, x_m]$ où les $x_i: W \rightarrow K$ sont les fonctions coordonnées sur W . Si $\phi: V \rightarrow W$ et $\psi: V \rightarrow W$ sont deux applications régulières telles que $\phi^* = \psi^*$ alors $\phi^*(x_i) = x_i \circ \phi$ et $\psi^*(x_i) = x_i \circ \psi$ en chaque i . Dès lors $\phi = \psi$ puisqu'elles coïncident sur chaque composante.

Soit $\xi: K[W] \rightarrow K[V]$ un morphisme de K -algèbres ; alors $\phi_i := \xi(x_i)$ est une fonction régulière sur V en chaque i . Soit $\phi = (\phi_1, \dots, \phi_m): V \rightarrow \mathbf{A}^m(K)$ l'application régulière. Alors $\mathrm{Im}(\phi) \subseteq W$ si et seulement si $f \circ \phi = 0$ pour tout $f \in I(W)$ étant donné que $VI(W) = W$. Or, pour tout $f \in I(W)$:

$$f \circ \phi = f(\xi(x_1), \dots, \xi(x_m)) = \xi(f(x_1, \dots, x_m)) = \xi(0) = 0.$$

Donc $\phi: V \rightarrow W$ est une application régulière, vérifiant $\phi^*(f) = f \circ \phi = f(\phi_1, \dots, \phi_m) = \xi(f)$ pour tout $f: W \rightarrow K$. \square

Lemme 11.6. Soit $F: \mathbf{C} \rightarrow \mathbf{D}$ un foncteur pleinement fidèle entre deux catégories ; alors pour tous objets A, B de \mathbf{C} : $A \simeq B$ si et seulement si $F(B) \simeq F(A)$. De plus, si $f: A \rightarrow B$ est un isomorphisme alors $F(f^{-1}) = F(f)^{-1}$. En particulier $K[-]: \mathbf{AlgSet}_K \rightarrow \mathbf{RedAlg}_K$ vérifie ce résultat.

PREUVE. Supposons que F soit contravariant, comme $K[-]$ (un léger changement constituant à retourner les flèches doit être opéré sinon). Il est clair que si $A \simeq B$ alors $F(B) \simeq F(A)$ puisque F est un foncteur. Désormais supposons l'existence d'un isomorphisme $f: F(B) \rightarrow F(A)$. Puisque F est plein, il existe $g: A \rightarrow B$ et $h: B \rightarrow A$ tels que $F(g) = f$ et $F(h) = f^{-1}$. Alors :

$$F(h \circ g) = F(g) \circ F(h) = f \circ f^{-1} = \mathrm{Id}_{F(A)} = F(\mathrm{Id}_A)$$

et comme F est fidèle, $h \circ g = \mathrm{Id}_A$. Similairement, $g \circ h = \mathrm{Id}_B$. \square

Exemple 11.7. Soit K un corps algébriquement clos dont la caractéristique diffère de 2 et soit $i \in K$ une racine de $X^2 + 1$. Soient $C = V(X^2 + Y^2 - 1)$ et $H = V(XY - 1)$ deux sous-ensembles algébriques de $\mathbf{A}^2(K)$. Or $X^2 + Y^2 - 1$ et $XY - 1$ sont irréductibles dans $K[X, Y]$ (nous utilisons l'hypothèse sur la caractéristique) et donc $I(C) = (X^2 + Y^2 - 1)$ et $I(H) = (XY - 1)$ par le Nullstellensatz. Noter que $K[H] = K[X, Y]/(XY - 1) \simeq K[Z, \frac{1}{Z}]$. L'application $\xi: K[C] \rightarrow K[H]$ donnée par

$$x \mapsto \frac{1}{2} \left(Z + \frac{1}{Z} \right) \quad \text{et} \quad y \mapsto \frac{1}{2i} \left(Z - \frac{1}{Z} \right),$$

où x et y sont les fonctions coordonnées sur C , est un isomorphisme de K -algèbres. En effet, son inverse est $Z \mapsto x + iy$ (et donc $\frac{1}{Z} \mapsto x - iy$). Au niveau des ensembles algébriques, le morphisme correspondant $\phi: H \rightarrow C: (a, b) \mapsto ((a+b)/2, (a-b)/(2i))$ est un isomorphisme, dont l'inverse est $(a, b) \mapsto (a + ib, a - ib)$.

Remarque 11.8. Il est primordial que K soit algébriquement clos ; dans l'exemple précédent, si $K = \mathbf{R}$ alors C est le cercle unité et H est une hyperbole !

Exemple 11.9. Soit K un corps algébriquement clos. Considérons les deux ensembles algébriques sur K suivant : $E = V(Y^2 - X^3 + 1) \subseteq \mathbf{A}^2(K)$ et $D = V(Y^2 - X^3 + 1, Z - X^2) \subseteq \mathbf{A}^3(K)$. À nouveau le Nullstellensatz implique que $I(E) = (Y^2 - X^3 + 1)$ et $I(D) = (Y^2 - X^3 + 1, Z - X^2)$. Remarquons cette fois que la composée

$$\begin{array}{ccccc} K[X, Y, Z] & \twoheadrightarrow & K[X, Y] & \twoheadrightarrow & K[X, Y]/(Y^2 - X^3 + 1) \\ f(X, Y, Z) & \mapsto & f(X, Y, X^2) & \mapsto & f(X, Y, X^2) \bmod (Y^2 - X^3 + 1). \end{array}$$

a pour noyau $\{f \in K[X, Y, Z] \mid f(X, Y, X^2) \in (Y^2 - X^3 + 1)\} = (Y^2 - X^3 + 1, Z - X^2)$. Ainsi, par factorisation du morphisme précédent, $K[D] \rightarrow K[E]: x \mapsto x, y \mapsto y$ et $x = z^2 \mapsto x^2$ est un isomorphisme de K -algèbres. Donc $D \simeq E$ par $E \rightarrow D: (a, b) \mapsto (a, b, a^2)$; d'inverse $(x, y, z) \mapsto (x, y)$.

Exemple 11.10. Soit K algébriquement clos. Considérons l'application régulière $\phi: \mathbf{A}^1(K) \rightarrow \mathbf{A}^3(K)$ donnée par $t \mapsto (t, t^2, t^3)$. Alors $\text{Im}(\phi) = V(Y - X^2, Z - X^3)$ est un sous-ensemble algébrique de $\mathbf{A}^3(K)$, notons-là V . Nous affirmons que $V \simeq \mathbf{A}^1(K)$. Pour le voir, il suffit d'appliquer le raisonnement précédent afin de montrer que $K[V] \simeq K[T]$. Dès lors $\phi^*: K[T] \rightarrow K[X]: T \mapsto X$ est un isomorphisme de K -algèbres et donc ϕ est un isomorphisme d'ensembles algébriques sur K .

12 Les morphismes dominants

Définition 12.1. Une application régulière $\phi: V \rightarrow W$ entre deux ensembles algébriques est *dominante* si son image est dense dans W . En particulier, toute application régulière surjective est dominante.

Nota Bene 12.2. Une application régulière $\phi: V \rightarrow W$ est dominante si et seulement si tout ouvert non vide de W rencontre son image, ou encore si et seulement si l'image réciproque par ϕ de tout ouvert non vide est non vide.

Lemme 12.3. La composée d'applications régulières dominantes (compatibles) est une application régulière dominante.

PREUVE. Soient $\phi: U \rightarrow V$ et $\psi: V \rightarrow W$ deux applications régulières dominantes et soit O un ouvert non vide de W . Alors $\psi^{-1}(O)$ est ouvert (car ψ est Zariski-continue) et non vide (car ψ est dominant). Dès lors $(\psi \circ \phi)^{-1}(O) = \phi^{-1}(\psi^{-1}(O))$ est non vide (car ϕ est dominant). \square

Lemme 12.4. Soit $\phi: V \rightarrow W$ une application régulière dominante. Si V est irréductible alors la restriction $\phi|_O: O \rightarrow W$ est dominante quel que soit l'ouvert non vide O de V .

PREUVE. Puisque ϕ est continue, $\overline{\phi(O)} = \phi(\bar{O})$. Toutefois V est supposé irréductible, donc O est dense dans V et le résultat s'en suit. \square

Exemple 12.5. Soit K algébriquement clos ; l'application $\phi: V(XY - 1) \subseteq \mathbf{A}^2(K) \rightarrow K: (x, y) \mapsto x$ est régulière dominante (non surjective). Noter que $\phi^*: K[T] \rightarrow K[V(XY - 1)] \simeq K[Z, \frac{1}{Z}]$ donnée par $T \mapsto Z$ est injective. Il s'agit d'un cas particulier du résultat suivant.

Proposition 12.6. Soit $\phi: V \rightarrow W$ une application régulière sur K ; alors :

- (a) ϕ^* est injective si et seulement si ϕ est dominante.
- (b) Si ϕ^* est injective et entière (i.e. $K[V]$ est entier sur $\phi^*(K[W])$) alors ϕ est surjective.
- (c) Si ϕ^* est surjective alors $\phi: V \rightarrow \overline{\phi(V)}$ est un isomorphisme. En particulier ϕ est injective.

PREUVE. (a) Si ϕ n'est pas dominante alors $I(W) \subset I(\overline{\phi(V)})$ et donc il existe une fonction régulière non nulle sur W s'annulant sur $\overline{\phi(V)}$. Dès lors ϕ^* n'est pas injective. Réciproquement, soit $f \in K[W]$. Puisque f est Zariski-continue et que ϕ est dominante, $f \circ \phi = 0$ si et seulement si $f = 0$.

(b) Ce résultat est admis ; il découle du going-up theorem.

(c) En factorisant ϕ^* par son noyau $\text{Ker}(\phi^*) = I(\overline{\phi(V)})/I(W)$, nous obtenons un isomorphisme de K -algèbres $K[\overline{\phi(V)}] \rightarrow K[V]$ donné par $f \mapsto f \circ \phi$. Puisque le foncteur $K[-]$ est pleinement fidèle $\phi: V \rightarrow \overline{\phi(V)}$ est un isomorphisme. \square

Remarque 12.7. Il est bon de noter qu'une application régulière $\phi: V \rightarrow W$ sur K injective n'a pas forcément pour homologue $\phi^*: K[W] \rightarrow K[V]$ un morphisme surjectif. Nous l'avons déjà remarqué au cours de l'exemple 10.7.

Exemple 12.8. Soit $K = \mathbf{F}_p^{\text{al}}$ une clôture algébrique de \mathbf{F}_p et soit $V = V(f_1, \dots, f_m)$ un sous-ensemble algébrique de $\mathbf{A}^n(K)$. Soit $\sigma: x \mapsto x^p$ l'automorphisme sur K . Si $f(X_1, \dots, X_n) = \sum a_i X_1^{i_1} \dots X_n^{i_n}$ alors nous notons $f^\sigma(X_1, \dots, X_n) = \sum a_i^p X_1^{i_1} \dots X_n^{i_n}$ et $V^\sigma = V(f_1^\sigma, \dots, f_m^\sigma)$. Alors $\phi: V \rightarrow V^\sigma$ donnée par $(x_1, \dots, x_n) \mapsto (x_1^p, \dots, x_n^p)$ est un isomorphisme (ϕ est surjective donc ϕ^* est injective et ϕ^* est surjective par construction de V^σ). Ce morphisme est appelé *morphisme de Frobenius*. Noter que si f_1, \dots, f_m sont à coefficients dans \mathbf{F}_p alors $V^\sigma = V$ et $\phi: V \rightarrow V$ est un automorphisme.

13 Discussion : le produit d'ensembles algébriques

Soient V et W deux sous-ensembles algébriques respectifs de $\mathbf{A}^n(K)$ et $\mathbf{A}^m(K)$. Leur produit $V \times W$ est alors un sous-ensemble algébrique de $\mathbf{A}^{n+m}(K)$ réalisé par le lieu d'annulation des polynômes définissant V et W vus en tant qu'éléments de $K[X_1, \dots, X_n, Y_1, \dots, Y_m]$. Dualelement, nous avons que $K[V \times W] \simeq K[V] \otimes_K K[W]$.

Les projections $V \times W \rightarrow V: (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}$ et $V \times W \rightarrow W: (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{y}$ sont des épimorphismes (nous noterons que les morphismes correspondants dans la catégorie \mathbf{RedAlg}_K sont injectifs). Elles sont également ouvertes.

Attention, la topologie de Zariski sur $V \times W$ ne coïncide pas (elle est plus fine) avec la topologie produit des topologies de Zariski (lorsque K est infini) : $\mathbf{A}^2(K) - V(XY - 1)$ est un ouvert mais les ouverts de $\mathbf{A}^1(K)$ sont cofinis ou vides.

Finalement il est bon de noter que V et W sont irréductibles si et seulement si $V \times W$ est irréductible.

14 Discussion : les groupes algébriques

Définition 14.1. Un *groupe algébrique* G est un ensemble algébrique muni d'une structure de groupe pour laquelle l'opération $G \times G \rightarrow G$ est un morphisme d'ensembles algébriques et le passage à l'inverse $G \rightarrow G$ est un automorphisme d'ensembles algébriques.

Exemple 14.2. Soit K algébriquement clos ; la droite affine $\mathbf{A}^1(K)$ muni de l'addition et du passage à l'inverse est un groupe algébrique, usuellement noté $\mathbf{G}_a(K)$ et désigné par le *groupe additif*.

Exemple 14.3. Similairement, la droite affine privée de son origine $\mathbf{A}^1(K) - \{0\}$ peut être munie d'une structure de groupe multiplicatif, noté $\mathbf{G}_m(K)$ et désigné par le *groupe multiplicatif*.

Définition 14.4. Soit K un corps ; un *ensemble algébrique quasi-affine* sur K est un ouvert dans un ensemble algébrique affine sur K . Les morphismes sont les mêmes.

Exemple 14.5. Soit K un corps algébriquement clos et soit $n \geq 1$ un entier. Fixons un isomorphisme de K -espaces vectoriels afin d'identifier $M_n(K) \simeq \mathbf{A}^{n^2}(K)$. Alors la multiplication matricielle et le déterminant sont des morphismes d'ensembles algébriques. Ainsi :

- $\mathrm{SL}_n(K) = \{A \in M_n(K) \mid \det(A) = 1\}$ est un groupe algébrique.
- $\mathrm{O}_n(K) = \{A \in M_n(K) \mid AA^\top = \mathbf{1}_n\}$ peut être défini par un système de n^2 polynômes quadratiques et est donc un groupe algébrique.
- $\mathrm{GL}_n(K) = \{A \in M_n(K) \mid \det(A) \neq 0\}$ est un ensemble algébrique quasi-affine et est donc ce que l'on appelle un groupe algébrique quasi-affine.

Définition 14.6. Les sous-groupes algébriques (quasi-)affines de $\mathrm{GL}_n(K)$ sont les *groupes algébriques K -linéaires*.

Proposition 14.7. Soit K un corps algébriquement clos et soit $n \geq 1$ un entier ; $\mathrm{O}_n(K)$ n'est pas irréductible quand la caractéristique de K est distincte de 2.

PREUVE. Notons que tout élément A de $\mathrm{O}_n(K)$ est tel que $\det(A) \in \{-1, 1\}$. Puisque K n'est pas de caractéristique 2 : -1 et 1 sont distincts. Il est alors possible de décomposer $\mathrm{O}_n(K)$ en

$$\mathrm{O}_n(K) = \{A \in \mathrm{O}_n(K) \mid \det(A) = 1\} \cup \{A \in \mathrm{O}_n(K) \mid \det(A) = -1\}$$

et ces deux ensembles sont des fermés non vides disjoints de $\mathrm{O}_n(K)$. □

Remarque 14.8. Soit G un groupe algébrique ; les translations $G \rightarrow G : y \mapsto xy$ pour $x \in G$ fixé sont des automorphismes d'ensembles algébriques mais pas de groupes.

15 Discussion : les applications rationnelles

Soit V un ensemble algébrique sur un corps algébriquement clos K ; alors $K[V]$ est intègre à la seule et unique condition que V soit irréductible. Sous cette hypothèse nous appelons *corps des fonctions rationnelles de V* le corps $K(V) := \mathrm{Frac} K[V]$.

Exemple 15.1. Soit K un corps algébriquement clos ; alors $K[\mathbf{A}^n(K)] = K[X_1, \dots, X_n]$ et son corps des fonctions rationnelles est naturellement $K(\mathbf{A}^n(K)) \simeq K(X_1, \dots, X_n)$.

Soient V et W deux ensembles algébriques irréductibles sur un corps algébriquement clos K et considérons les paires (O, ϕ_O) où O est un ouvert non vide (et donc dense) de V et $\phi_O : O \rightarrow W$ une application régulière. Deux telles paires (O, ϕ_O) et $(O', \phi_{O'})$ sont dites équivalentes si ϕ_O et $\phi_{O'}$ sont égales sur $O \cap O'$. Noter que la transitivité s'obtient de l'irréductibilité de V . En particulier nous obtenons $K(V)$ en prenant $W = \mathbf{A}^1(K)$ et en quotientant par cette relation.

Définition 15.2. Une classe d'équivalence pour la relation précédente est appelée une *application rationnelle* $\phi : V \dashrightarrow W$ bien qu'elles ne sont définies que sur une partie dense de V .

Remarque 15.3. Soit $\phi : V \rightarrow W$ une application régulière entre deux ensembles algébriques irréductibles sur un corps K . Alors l'application $\phi^* : K[W] \rightarrow K[V] : f \mapsto f \circ \phi$ est injective et s'étend en une application $K(W) \rightarrow K(V)$ au niveau des corps de fractions.

Fait 15.4. Soient V et W deux ensembles algébriques irréductibles sur un corps algébriquement clos K . Une application rationnelle $\phi : V \dashrightarrow W$ dominante (i.e. d'image dense dans W) donne lieu à un morphisme de K -algèbres $\phi^* : K(W) \rightarrow K(V)$ et tout tel morphisme provient de cette manière.

Définition 15.5. Soient V et W deux ensembles algébriques irréductibles sur un corps algébriquement clos K ; une application rationnelle $\phi: V \dashrightarrow W$ est *birationnelle* si elle admet un inverse (à droite et à gauche). Deux ensembles algébriques sont *birationnellement équivalents* s'il existe une application birationnelle entre-eux.

Exemple 15.6. Soit K un corps algébriquement clos et soit $n \geq 1$ un entier ; rappelons que nous identifions $M_n(K)$ à $\mathbf{A}^{n^2}(K)$ via le choix d'un isomorphisme. Alors $M_n(K) \dashrightarrow M_n(K): A \mapsto A^{-1}$ est birationnelle.

Fait 15.7 (Équivalence birationnelle). *Deux ensembles algébriques irréductibles V et W sur un corps algébriquement clos K sont birationnellement équivalents si et seulement si $K(V) \simeq K(W)$.*

16 Dimension

Définition 16.1. La *dimension topologique* d'un espace topologique X (non vide) est le supremum des longueurs des chaînes

$$F_0 \supset F_1 \supset \cdots \supset F_d$$

de fermés irréductibles distincts de X (la longueur de la chaîne précédente vaut d).

Exemple 16.2. Soit K algébriquement clos et considérons $X = \mathbf{A}^1(K)$ muni de la topologie de Zariski (*i.e.* de la topologie cofinie). Les fermés irréductibles de $\mathbf{A}^1(K)$ sont ses singletons et lui-même ; dès lors $\dim(\mathbf{A}^1(K)) = 1$ et $\dim(\{P\}) = 0$ (pour la topologie induite) en tout point P de $\mathbf{A}^1(K)$.

Remarque 16.3. Deux espaces topologiques équivalents sont de même dimension topologique.

Lemme 16.4. *La fermeture d'un sous-ensemble irréductible Y d'un espace topologique est irréductible.*

PREUVE. Si $\bar{Y} = F_1 \cup F_2$ est une union de fermés distincts de \bar{Y} alors Y est aussi l'union de deux fermés distincts : $Y = Y \cap \bar{Y} = (Y \cap F_1) \cup (Y \cap F_2)$. Par irréductibilité de Y , l'une de ces composantes vaut Y , disons $Y = Y \cap F_1$ et donc lors $\bar{Y} = F_1$. \square

Proposition 16.5. *Soit Y un sous-ensemble non vide d'un espace topologique X ; alors :*

- (a) $\dim(Y) \leq \dim(X)$.
- (b) *Si de plus Y est fermé et que X est supposé irréductible alors $\dim(Y) \leq \dim(X)+1$. En particulier $\dim(Y) < \dim(X)$ lorsque $\dim(X)$ est finie.*

PREUVE. (a) Nous remontons les chaînes : soit $F_0 \supset F_1 \supset \cdots \supset F_d$ une chaîne de fermés irréductibles de Y et posons \bar{F}_i la fermeture de F_i dans X . Alors $\bar{F}_0 \supset \bar{F}_1 \supset \cdots \supset \bar{F}_d$ est une chaîne de fermés de X . Puisque les F_i sont fermés dans Y chaque $\bar{F}_i \cap Y = F_i$ et les inclusions de la chaîne précédente sont strictes. Le lemme 16.4 permet alors de conclure.

(b) Toute chaîne $F_0 \supset F_1 \supset \cdots \supset F_d$ de Y s'étend en une chaîne $X \supset F_0 \supset F_1 \supset \cdots \supset F_d$ de X et donc $\dim(Y) \leq \dim(X) + 1$. \square

Proposition 16.6. *Si X_1, \dots, X_m sont les composantes irréductibles d'un espace topologique X non vide alors $\dim(X) = \text{Max}\{\dim(X_1), \dots, \dim(X_m)\}$.*

PREUVE. La proposition précédente implique que $\text{Max}\{\dim(X_1), \dots, \dim(X_m)\} \leq \dim(X)$. Pour l'inégalité réciproque, si $F_0 \supset F_1 \supset \cdots \supset F_d$ est une chaîne de fermés irréductibles de X alors

$$F_d = F_d \cap X = F_d \cap (X_1 \cup \cdots \cup X_m) = (F_d \cap X_1) \cup \cdots \cup (F_d \cap X_m)$$

et chaque $F_d \cap X_i$ est fermé dans X . Comme F_d est irréductible, $F_d = F_d \cap X_i$ pour un certain i et donc toute la chaîne est contenue dans X_i . Ainsi $\dim(X) \leq \text{Max}\{\dim(X_1), \dots, \dim(X_m)\}$. \square

Remarque 16.7. Soit V un ensemble algébrique irréductible sur un corps algébriquement clos K ; le Nullstellensatz relatif induit une bijection décroissante entre les chaînes $V = V_0 \supset V_1 \supset \cdots \supset V_d$ de longueur d de fermés irréductibles de V et les chaînes $I_V(V) = (0) \subset I_V(V_1) \subset \cdots \subset I_V(V_d)$ de longueur d d'idéaux premiers de $K[V]$. Noter que puisque K est algébriquement clos, $I_V(V_d) = K[V]$ si et seulement si V_d est vide.

Définition 16.8. La *dimension de Krull* d'un anneau commutatif A est le supremum des longueurs des chaînes

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d$$

d'idéaux premiers de A (la longueur de la chaîne précédente vaut d).

Exemple 16.9. La dimension de Krull de tout anneau principal est au plus 1. En effet, dans de tels anneaux les idéaux premiers non nuls sont maximaux. En particulier $\dim(\mathbf{Z}) = \dim(\mathbf{Z}[i]) = 1$ où $i^2 = -1$. Noter que la dimension de Krull de tout corps est nulle.

Fait 16.10. Soit K un corps et soit A une K -algèbre. On définit le *degré de transcendance* $\degtr_K(L)$ d'une extension L de K comme étant la cardinalité maximale d'un sous-ensemble algébriquement indépendant de L/K . Sous ces notations, $\dim(A) = \degtr_K(\text{Frac } A)$.

Exemple 16.11. Soit K un corps ; $\dim(K[X_1, \dots, X_n]) = n$. En effet, lorsque $A = K[X_1, \dots, X_n]$ alors $\text{Frac } A = K(X_1, \dots, X_n)$ et les X_i sont algébriquement indépendants, donc $\dim(K[X_1, \dots, X_n]) = n$.

Résumé 16.12. Soit V un ensemble algébrique irréductible sur un corps algébriquement clos K :

$$\dim_{\text{top}}(V) = \dim_{\text{Krull}}(K[V]) = \degtr_K(K(V)).$$

Remarque 16.13. En particulier, la dimension de tout ensemble algébrique est finie. De plus, si V et W sont deux ensembles algébriques birationnellement équivalents, ils sont de même dimension.

Exemple 16.14. Soit K un corps algébriquement clos ; alors en utilisant les discussions précédentes nous obtenons que $\dim(\mathbf{A}^n(K)) = \dim(K[\mathbf{A}^n(K)]) = \dim(K[X_1, \dots, X_n]) = n$.

Lorsque l'on a affaire à un ensemble algébrique quasi-affine, on utilise la proposition suivante :

Proposition 16.15. Soit V un ensemble algébrique irréductible sur un corps algébriquement clos et soit U un ouvert non vide contenu dans V ; alors $\dim(U) = \dim(V)$.

PREUVE. Puisque $U \subseteq V$ alors $\dim(U) \leq \dim(V)$. Réciproquement, soit $F_0 \supset F_1 \supset \cdots \supset F_d$ une chaîne de fermés irréductibles de V de longueur d . Alors $F_0 \cap U \supseteq F_1 \cap U \supseteq \cdots \supseteq F_d \cap U$ est une chaîne de fermés de U .

Ces inclusions sont strictes : en passant à la fermeture dans V , $\overline{F_0 \cap U} \supseteq \overline{F_1 \cap U} \supseteq \cdots \supseteq \overline{F_d \cap U}$ est une chaîne de fermés de V dont chaque $\overline{F_i \cap U} = \overline{F_i} \cap \overline{U} = F_i \cap \overline{U} = F_i$ puisque les F_i sont fermés et U est un ouvert non vide de l'irréductible V .

Chacun des $F_i \cap U$ est irréductible : soit O un ouvert non vide de $F_i \cap U$; il existe un ouvert O' de V tel que $O = O' \cap (F_i \cap U)$. Dès lors $\overline{O} = \overline{O' \cap F_i \cap U} = V \cap F_i \cap V = F_i$ par irréductibilité de V . Ainsi O est dense dans F_i et donc dense dans $F_i \cap U$ puisque $O \subseteq F_i \cap U \subseteq F_i$. \square

Exemple 16.16. Soit K un corps algébriquement clos et soit $n \geq 1$ un entier ; il en découle du résultat précédent que $\dim(\text{GL}_n(K)) = \dim(M_n(K)) = \dim(\mathbf{A}^{n^2}(K)) = n^2$.

Proposition 16.17. Soient V et W deux ensembles algébriques sur un corps algébriquement clos K ; alors $\dim(V \times W) = \dim(V) + \dim(W)$.

ESQUISSE. Nous pouvons supposer V et W irréductibles ; auquel cas $V \times W$ est irréductible. Rappelons que $K[V \times W] \simeq K[V] \otimes_K K[W]$. Les monomorphismes $K[V], K[W] \hookrightarrow K[V] \otimes_K K[W]$ associés au coproduit induisent des monomorphismes $K(V), K(W) \hookrightarrow \text{Frac}(K[V] \otimes_K K[W]) \simeq K(V \times W)$. Nous obtenons une application K -bilinéaire :

$$\begin{aligned} K(V) \times K(W) &\longrightarrow K(V \times W) \\ (f, g) &\longmapsto (f \otimes 1)(1 \otimes g). \end{aligned}$$

Ainsi $K(V) \otimes_K K(W)$ se plonge dans $K(V \times W)$. Étant donné que $K(V)$ et $K(W)$ sont linéairement disjoints sur K , le coproduit $K(V) \otimes_K K(W)$ est un corps et donc $K(V) \otimes_K K(W) \simeq K(V \times W)$.

Finalement, si L et M sont algébriquement disjoints sur K alors $\deg_K(L \otimes_K M) = \deg_K(L) + \deg_K(M)$; or c'est le cas de $K(V)$ et $K(W)$. \square

Exemple 16.18. Soient $n, m \geq 1$ deux entiers ; alors $\dim(\mathbf{A}^n(K) \times \mathbf{A}^m(K)) = \dim(\mathbf{A}^{n+m}(K)) = n + m$.

Définition 16.19. Soient A un anneau commutatif et \mathfrak{p} un idéal premier de A ; la *hauteur* de \mathfrak{p} est le supremum des longueurs des chaînes d'idéaux premiers de A contenus dans \mathfrak{p} , notée $\text{ht}(\mathfrak{p})$.

Rappel 16.20. Il y a une bijection croissante entre les idéaux de A/\mathfrak{p} et les idéaux de A contenant \mathfrak{p} ; d'où $\dim(A) \geq \dim(A/\mathfrak{p}) + \text{ht}(\mathfrak{p})$. Il s'agit même d'une égalité :

Fait 16.21. Soient A une algèbre de type fini intègre sur un corps et \mathfrak{p} un idéal premier de A ; alors la dimension de Krull de A/\mathfrak{p} est $\dim(A/\mathfrak{p}) = \dim(A) - \text{ht}(\mathfrak{p})$.

Lemme 16.22. Soit A un anneau factoriel et soit π un irréductible de A ; alors $\text{ht}(\pi) = 1$.

PREUVE. Soit \mathfrak{p} un idéal premier de A strictement contenu dans (π) . Soit $a \in \mathfrak{p}$; alors $(a) \subseteq (\pi)$ si et seulement si $a = b\pi$ pour un $b \in A$. Comme $\pi \notin \mathfrak{p}$ et que \mathfrak{p} est premier, $b \in \mathfrak{p}$. En itérant de cette manière nous obtenons que π^n divise a pour tout $n \geq 1$. Du fait que A soit factoriel, $a = 0$ et donc $\mathfrak{p} = (0)$. \square

Exemple 16.23. Comme $\mathbf{Z}[X]/(X) \simeq \mathbf{Z}$, il s'en suit que $\dim(\mathbf{Z}[X]) = \dim(\mathbf{Z}) + \text{ht}(X) = 1 + 1 = 2$.

Proposition 16.24. Soit K un corps algébriquement clos et soit $f \in K[X_1, \dots, X_n]$ non constante ; alors la dimension topologique de $V(f)$ vaut $n - 1$. De tels ensembles sont des hypersurfaces de $\mathbf{A}^n(K)$.

PREUVE. Nous pouvons supposer que $V(f)$ est irréductible et que f est irréductible dans $K[X_1, \dots, X_n]$ (sinon $V(f) = V(f_1) \cup \dots \cup V(f_m)$ avec f_i les irréductibles apparaissant dans la factorisation de f). Alors $\dim(V(f)) = \dim(K[X_1, \dots, X_n]) - \text{ht}(f) = n - 1$. \square

Références

- [Per95] Daniel PERRIN. *Géométrie algébrique. Une introduction*. InterÉditions-CNRS, 1995, p. 301. ISBN : 2-271-05271-8.
- [Vol07] Maja VOLKOV. « Géométrie algébrique : géométrie affine et dimension ». US-M1-SCMATH-003-M, Projet en géométrie algébrique. 2007.
- [Mil17] James S. MILNE. *Algebraic Geometry (v6.02)*. 2017. URL : <https://www.jmilne.org/math/CourseNotes/AG.pdf>.