Georges COMTE

GÉOMÉTRIE ALGÉBRIQUE

Georges COMTE
Laboratoire de Mathématiques de l'Université de Savoie, UMR CNRS 5127,
Bâtiment Chablais, Campus scientifique, 73376 Le Bourget-du-Lac cedex, France.
E-mail : georges.comte@univ-savoie.fr
Url : http://gc83.perso.sfr.fr/

25 janvier 2016

GÉOMÉTRIE ALGÉBRIQUE

Georges COMTE

TABLE DES MATIÈRES

CHAPITRE 1

INTRODUCTION

1.1. Introduction générale

1.2. Ensembles ordonnés

Commençons par rappeler quelques éléments de vocabulaire de la théorie des ensembles, autour de la notion d'ordre.

Soit $\mathcal{E}$ un ensemble. Cet ensemble est dit **ordonné** s'il est muni d'une relation binaire (ie formellement un sous-ensemble de $\mathcal{E} \times \mathcal{E}$ [(1)]), notée $\prec$ et appelée un **ordre sur** $\mathcal{E}$, telle que

1. cette relation est anti-réflexive : (x, x) n'est pas dans $\prec$,
2. cette relation est transitive : $\forall x, y \in \mathcal{E},\ x \prec y$ et $y \prec z \Longrightarrow x \prec z$.

L'ensemble ordonné $(\mathcal{E}, \prec)$ est dit **totalement ordonné**, ou **l'ordre** $\prec$ **est dit total** lorsque deux éléments quelconques x, y de $\mathcal{E}$ sont comparables pour l'ordre $\prec$, ie que $x \prec y$ ou $y \prec x$ ou $x = y$. **Un majorant** $M \in \mathcal{E}$ **d'une partie** $A \subset \mathcal{E}$ est par définition tel que $\forall a \in A, a \prec M$. On dit lors que la partie A est **majorée**. Un **élément maximal** $m \in A$ **de la partie** A est un élément m de A tel que $m \prec a$ n'est vraie pour aucun élément a de A (de sorte que soit $a \in A$ n'est pas comparable à m, soit $a \prec m$, soit $a = m$).

1.2.1 Remarque. — Un majorant $M \in \mathcal{E}$ de $A \subset \mathcal{E}$ n'est pas nécessairement un élément maximal de A (si $M \notin A$), tandis qu'un élément maximal m de A ne majore pas nécessairement A (des éléments de A peuvent ne pas être comparables à m).

Lorsqu'un élément est à la fois un majorant et un élément maximal de A, on dit que cet élément est un **plus grand élément de** A. Un tel élément g est unique dans A et est défini par $g \in A$ et $\forall a \in A, a \prec g$.

On définit de la même manière que les notions de majorant, d'élément maximal et de plus grand élément, les notions de **minorant**, d'**élément minimal** et de **plus petit élément**. Pour cela il suffit d'écahnger les rôles des symboles M (resp. m, g) et a dans les trois définitions ci-dessus.

[(1)] On note $(x, y) \in \prec$ par $x \prec y$

1.2.2 Remarque. — Si $(\mathcal{E}, \prec)$ est un ensemble ordonné, il en est de même de $(\mathcal{E}, \succ)$, où $\succ$ est la relation binaire sur $\mathcal{E}$ définie par $x \succ y \iff y \prec x$. Il s'ensuit que $x \in A \subset \mathcal{E}$ est un majorant de A pour $\prec$ (resp. un élément maximal, un plus grand élément) si et seulement si x est un minorant pour $\succ$ (resp. un élément minimal, un plus petit élément).

1.2.3 Définition. — On dit qu'un ensemble ordonné $(\mathcal{E}, \prec)$ est **bien ordonné**, ou muni d'un **bon ordre** si toute partie non vide A de $\mathcal{E}$ admet un **plus petit élément**, ie un élément $p \in A$ tel que $\forall a \in A,\ p \prec a$. Dans ce cas

1. $\mathcal{E}$ est totalement ordonné, puisque toute partie de $\mathcal{E}$ de cardinal 2 admet un plus petit élément.
2. $\mathcal{E}$ admet un plus petit élément et est donc minoré.

1.2.4 Définition. — Un ensemble ordonné $(\mathcal{E}, \prec)$ est dit **inductif** lorsque toute partie totalement ordonnée de $\mathcal{E}$ est majorée dans $\mathcal{E}$.

On dispose dans notre théorie de l'axiome du choix

Axiome du choix. — Tout produit d'ensembles non vides est non vide. Autrement dit si I est un ensemble non vide, $X_i, i \in I$ des ensembles non vides, alors $\prod_{i\in I} X_i := \{f : I \to \bigcup_{i\in I} X_i; \forall i \in I,\ f(i) \in X_i\}$ est non vide.

Cet axiome est alors équivalent (dans le système de Zermelo-Fraenkel) aux énoncés suivants Théorèmes 1.2.5 et 1.2.6, que l'on peut énoncer comme des théorèmes déduits de l'axiome du choix ([**10**], Théorème 5.2.5, par exemple).

1.2.5 Théorème **(Lemme de Zorn)**. — *Tout ensemble ordonné inductif admet un élément maximal.*

1.2.6 Théorème **(Lemme de Zermelo)**. — *Tout ensemble peut être muni d'un bon ordre.*

1.3. Anneaux

Pour un entier n donné, on appelle **espace affine de dimension** n l'ensemble $\mathbf{k}^n$ (le produit cartésien de n copies de $\mathbf{k}$, qui est par définition l'ensemble des n-uplets $(x_1, \cdots, x_n)$, $x_1, \ldots, x_n \in \mathbf{k}$). Cet ensemble sera parfois noté $\mathbb{A}^n(\mathbf{k})$ lorsqu'on le minira de sa structure de variété algébrique (ou même simplement lorsqu'on le verra comme un ensemble algébrique).

On rappelle qu'étant donné un anneau commutatif A, on note $A[x]$ l'ensemble des suites presque partout nulles dont les termes sont dans A. Il s'agit d'un sous-groupe de $A^{\mathbb{N}}$ sur lequel on considère le produit $(a_0, a_1, \cdots, a_d, 0\cdots)(b_0, b_1, \cdots, b_d, 0\cdots) := (c_0 = a_0b_0, \cdots, c_k = \Sigma_{i=0}^{d} a_i b_{k-i}, \cdots, 0, \cdots)$ qui fait de $A[x]$ un anneau, dans lequel s'injecte A par $a \mapsto (a, 0, \cdots)$. On l'appelle **l'anneau des polynômes à** n **indéterminées et à coefficients dans** A. On note x^ℓ, pour $\ell \in \mathbb{N}$ l'élément $(0, \cdots, 1, 0, \cdots)$, le 1 figurant à la ℓième place dans cette suite. Pour $P \in A[x]$, il

existe une unique écriture $P = \sum_{i=0}^{d} a_i x^i$ et le produit sur $A[x]$ fait que $x^\ell \cdot x^s = x^{\ell+s}$. On note $deg(P) = \max\{j \in \mathbb{N}; P = (a_0, a_1, \cdots), a_j \neq 0\}$. Avec ces notations, on appelle $a_{deg(P)}$ le coefficient directeur de P. On note $A[x_1, \cdots, x_n] = (\cdots((A[x_1])[x_2])\cdots)[x_n]$. Nous considèrerons essentiellement des anneaux de polynômes $\mathbf{k}[x_1, \cdots, x_n]$ sur un corps k. Dans ce cas on dispose d'une $\mathbf{k}$-algèbre.

La principale propriété que nous voulons rappeler ici est la noethérianité de l'anneau $\mathbf{k}[x_1, \cdots, x_n]$. Rappelons cette notion.

1.3.1 Définition. — Soit A un anneau, les propositions suivantes sont équivalentes. On dit qu'un anneau qui satisfait une de ces trois propositions est **noethérien**

(i) Tout idéal de A est de type fini ie que si I est un idéal de A existent $a_1, \cdots, a_\ell \in I$, tels que quel que soit $a \in I$, existent $\lambda_1, \cdots, \lambda_\ell \in I$, tels que $a = \sum_{i=1}^{\ell} \lambda_i a_i$,
(ii) Toute suite croissante d'idéaux de A est stationnaire,
(iii) Tout ensemble non vide $\mathcal{E}$ d'idéaux de A admet un élément maximal pour l'inclusion, ie un élément $I_0 \in \mathcal{E}$ tel que si $I_0 \subset I$ et $I \in \mathcal{E}$ alors $I = I_0$.

Démonstration. — $(i) \Rightarrow (ii)$ Si $I_1 \subset I_2 \subset \cdots$ est une suite croissante d'idéaux de A, $\cup_{i\in I} I_i$ est un idéal de A, qui étant de type fini possède des générateurs $a_1, \cdots, a_\ell$. Mais alors existe $k \in \mathbb{N}^*$ tel que ces générateurs sont tous dans I_k, et il s'ensuit que la suite $I_1 \subset I_2 \subset \cdots$ est stationnaire à partir du rang k.

$(ii) \Rightarrow (iii)$ Soit en effet $\mathcal{E}$ un ensemble non vide d'idéaux de A sans élément maximal. Soit alors $I_1 \in \mathcal{E}$, comme I_1 n'est pas maximal, il existe $I_2 \in E$ tel que $I_1 \subsetneq I_2$, et I_2 n'est pas maximal. On contruit ainsi par récurrence une suite strictement croissante d'idéaux de A, ce qui contredit (ii).

$(iii) \Rightarrow (i)$ Soit I un idéal de A qui n'est pas de type fini et $a_1 \in I$. Puisque $I \neq (a_1)$, il existe $a_2 \in I$ tel que $a_2 \notin (a_1)$. Mais alors $(a_1) \subsetneq (a_1, a_2)$ et $I \neq (a_1, a_2)$ et ainsi de suite on construit une suite strictement croissante d'idéaux de A. Le support de cette suite ne saurait alors avoir d'élément maximal, ce qui contredit (iii). □

1.3.2 Remarque. — Les idéaux d'un corps $\mathbf{k}$ étant (0) et (1) = $\mathbf{k}$, un corps est en particulier un anneau noethérien.

Le résultat qui nous sera trés utile dans la suite de ce chapitre est le théorème de transfert suivant, dû à Hilbert

1.3.3 Théorème. — *Soit A un anneau noethérien, alors $A[x]$ est noethérien. En particulier $\mathbf{k}[x_1, \cdots, x_n]$ est noethérien.*

Démonstration. — Soit I un idéal de A[X]. Pour $d \in \mathbb{N}$, On note C_d l'ensemble des coefficients directeurs des polynômes de degré d de I et $J_d = C_d \cup \{0\}$. Alors J_d est clairement un idéal de A. De plus si $D \geq d$, on a $J_d \subset J_D$ (en multipliant les polynômes de degré d de I par x^{D-d}). Comme par hypothèse A est noethérien, il existe $\ell \in \mathbb{N}$ tel que, pour tout $d \geq \ell$, $J_d = J_\ell$ et de plus J_ℓ est finiment engendré. Soit alors S_d un ensemble fini de polynômes de degré d dont les coefficients directeurs

engendrent C_d. On montre que $\cup_{d\leq\ell} S_d$ est une partie finie de I qui engendre I. Soit pour cela $P \in I$.

Si $\deg(P) = 0$, P est un polynôme constant combinaison linéaire à coefficients dans A d'éléments de C_0, donc P est bien l'idéal engendré par S_0. Supposons notre propriété démontré pour les polynômes P de I de degré $\leq k$, pour un entier $k \geq 0$, et montrons que si $\deg(P) = k+1$, P est dans l'idéal engendré par $\cup_{d\leq\ell} S_d$. Le coefficient directeur de P est $\lambda_1 a_1 + \cdots + \lambda_m a_m$ avec $\lambda_i \in A$ et a_i des coefficients directeurs de polynômes P_i de S_j ($j = \ell$ si $k+1 \geq \ell$ et $j = k+1$ si $k+1 \leq \ell$). Il s'ensuit que $P - (\lambda_1 P_1 + \cdots + \lambda_m P_m)$ (si $k+1 \leq \ell$) est un polynôme de I de degré strictement plus petit que $k+1$ et $P - (\lambda_1 x^{k+1-\ell} P_1 + \cdots + \lambda_m x^{k+1-\ell} P_m)$ (si $k+1 \geq \ell$) est un polynôme de I de degré strictement plus petit que $k+1$. Dans les deux cas, on applique l'hypothèse de récurrence qui assure que $P - (\lambda_1 P_1 + \cdots + \lambda_m P_m)$ ou $P - (\lambda_1 x^{k+1-\ell} P_1 + \cdots + \lambda_m x^{k+1-\ell} P_m)$ est combinaison A-linéaire d'éléments de $\cup_{d\leq\ell} S_d$, et donc également P. □

On prendra en général garde de ne pas identifier un polynôme, formellement définit comme ci-dessus, avec la fonction polynôme qu'il induit sur $\mathbf{k}^n$. En effet si $\mathbf{k}$ est un corps fini les deux notions ne coïncident en général pas, comme le montre l'exemple suivant :

1.3.4 Exemple. — Considérons $P(x) \in \mathbb{Z}_2[x]$ défini par $P(x) = x^2 + x$. Formellement $P = (0, 1, 1, 0, \cdots)$, il ne s'agit donc pas du polynôme nul $(0, \cdots)$. Cependant la fonction polynôme f_P qu'induit P sur $\mathbf{k}$ et qui est définie par $f_P(x) = x^2 + x$ est la fonction nulle.

1.3.5 Exercice. — *Notons $\mathcal{F}(\mathbf{k}^d; \mathbf{k})$ l'algèbre des fonctions polynomiales de $\mathbf{k}^n$ vers $\mathbf{k}$. Montrer que si $\mathbf{k}$ est infini l'application*

$$\begin{array}{ccc} \mathbf{k}[x_1, \cdots, x_n] & \to & \mathcal{F}(\mathbf{k}^n; \mathbf{k}) \\ P & \mapsto & f_P : \begin{array}{ccc} \mathbf{k}^n & \to & \mathbf{k} \\ (x_1, \cdots, x_n) & \mapsto & f_P(x_1, \cdots, x_n) := P(x_1, \cdots, x_n) \end{array} \end{array}$$

qui à un polynôme associe sa fonction polynôme naturelle est un isomorphisme de $\mathbf{k}$-algèbres.

Bien entendu lorsque le contexte sera clair, et après cette mise en garde, nous écrirons souvent P au lieu de f_P, même lorsque $\mathbf{k}$ est un corps fini...

Nous rappelons ici le principe de division euclidienne dans un anneau.

1.3.6 Théorème. — *Étant donné un anneau A, si P, S sont deux éléments de $A[x]$ tels que le coefficient directeur de S est inversible dans A, il existe un unique couple $(Q, R) \in A[x]^2$ tel que $P = QS + R$ et $deg(R) < deg(S)$ ou $R = 0$.*

1.3.7 Remarque. — Rappelons que si A est un anneau intègre, $A[x]$ aussi et que les inversibles de $A[x]$ sont ceux de A.

1.3.8 Définition. — Un anneau intègre A est dit **principal** lorsque tous ses idéaux sont engendrés par un seul élément (on dit aussi d'un tel idéal qu'il est principal). Un tel anneau est évidemment noethérien.

1.3.9 Définition. — Un idéal I d'un anneau A est dit **premier** ssi A/I est intègre ie $A/I \neq \{0\}$ et $\forall a, b \in A$, $ab = 0$ implique $a = 0$ ou $b = 0$ ssi $I \neq A$ et $\forall \alpha, \beta \in A$, $\alpha\beta \in I$ implique $\alpha \in I$ ou $\beta \in I$.

1.3.10 Définition. — Un élément a, non inversible, d'un anneau A est dit **irréductible** lorsque quels que soient $b, c \in A$, $a = bc$ implique b ou c inversible.

1.3.11 Proposition. — *Soit A un anneau intègre et $a \in A$ non nul et non inversible.*

(i) L'idéal (a) est premier ssi $\forall b, c \in A$, si a divise bc, alors a divise b ou c.
(ii) Si (a) est premier alors a est irréductible.
(iii) On suppose A principal. Alors un idéal de I, noté $I := (a)$ est premier ssi a est irréductible ssi I est maximal.

1.3.12 Définition. — Un anneau A est dit **local** s'il possède un unique idéal maximal $\mathfrak{m}$. Dans ce cas le quotient $A/\mathfrak{m}$ est appelé le corps résiduel de A.

1.3.13 Remarque. — L'anneau A est local si et seulement si les éléments non inversibles de A forment un idéal, qui est alors l'idéal maximal de A. En effet soit A un anneau et N l'ensemble de ses éléments non inversibles.

Si A est local, il est clair que $\mathfrak{m}$ ne peut contenir un inversible car sinon $\mathfrak{m}$ serait A et donc ne serait pas maximal, donc $\mathfrak{m} \subset N$. Mais si x est non inversible, l'idéal qu'il engendre n'est pas A et est contenu dans un idéal maximal qui ne peut être que $\mathfrak{m}$. On en conclut que $N = \mathfrak{m}$.

Réciproquement, supposons que N soit un idéal. Celui-ci est alors maximal, puisque N est contenu dans un idéal maximal mais ne saurait contenir d'inversible. Enfin tout autre idéal de A, s'il n'est pas contenu dans N possède un inversible et donc est A. L'idéal N est ainsi l'unique idéal maximal de A.

Une manière de construire des anneaux locaux consiste à localiser un anneau A par une de ses parties multiplicatives S bien choisie. Nous donnons ici cette construction.

1.3.14 Définition. — Soit A un anneau commutatif.

1. Une partie S de A est dite une **partie multiplicative de** A si
$$1 \in S \text{ et } \forall a, b \in S,\ ab \in S.$$
2. On définit le **localisé**[(2)] **de** A **par une partie multiplicative** S **de** A, ou **l'anneau quotient de** A **par** S, ou encore **l'anneau des fractions de** A **par**

[(2)] Ici le vocabulaire est trompeur puisque le *localisé de A par une de ses parties multiplicatives S* n'est pas nécessairement un anneau local, comme le montre la Remarque 5 de 1.3.15 ci-dessous.

S , et on note A_S ou $S^{-1}A$, l'anneau défini comme le quotient de $A \times S$ par la relation d'équivalence

$$(a, s) \sim (a', s') \Longleftrightarrow \exists t \in S,\ t(as' - a's) = 0.$$

On note a/s la classe de (a, s) et on vérifie que A_S est bien un anneau pour les lois $a/r + b/s = (as + br)/(rs)$ et $(a/r) \cdot (b/s) = (ab)/(rs)$. Le neutre de cet anneau étant $0/1$ et l'unité $1/1$.

Notons que dans le cas particulier où A est intègre, la relation d'équivalence devient ci-dessus devient

$$(a, s) \sim (a', s') \Longleftrightarrow as' = a's.$$

Ceci est clair si $0 \notin S$ et dans le cas où $0 \in S$, on a :

1.3.15 Remarque. — 1. Si $0 \in S$, $S^{-1}A$ est l'anneau nul, puisque tous les éléments de $A \times S$ sont équivalents à $(0, 0)$.

2. Dans le cas où A est intègre, on dispose d'un morphisme injectif $i : A \to A_s$ défini par $i(a) = a/1$. Dans le cas où A n'est pas intègre, i est seulement un morphisme d'anneau.
3. Si A est intègre, $S = A \setminus \{0\}$ est une partie multiplicative de A et A_S s'appelle le corps des fractions de A. Il s'agit du plus petit anneau dans lequel A s'injecte et contenant les inverses des images par cette injection des éléments non nuls de A. Toujours pour A intègre et pour S général, A_S est un sous-anneau du corps des fractions de A, le plus petit contenant les inverses des éléments de S. Dans le cas où A n'est pas intègre, on ne peut pas voir A_S comme un sous-anneau du corps de fractions de A, ce corps n'étant pas défini. Cependant, dans l'anneau A_S, les éléments de S sont des inversibles.
4. Si I est un idéal premier de A, alors $A \setminus I$ est une partie multiplicative de A. On note la localisation correspondante de A par A_I.
5. Soit $P \in A$ et $S = \{P^k; k \in \mathbb{N}\}$, qui est multiplicative. Notons que si A est intègre alors P n'est pas nilpotent, et donc S est une partie multiplicative de A ne contenant pas 0. En revanche si aucune hypothèse n'est faite sur A ou P, S peut contenir 0. On note alors A_S par A_P et on appelle A_P la localisation de A en P. Lorsque A est intègre, on a

$$A_P \simeq A[X]/(PX - 1).$$

En effet, considérons le morphisme d'anneaux $\varphi : A[X] \to A_P$, défini par $\varphi(X) = 1/P$. Ce morphisme est clairement surjectif. Montrons que son noyau est $(PX-1)$. Si $\sum_{i=1}^{n} a_i P^{-i} = 0/1$, par définition, $\sum_{i=1}^{n} a_i P^{d-i} = 0$. La division par le polynôme unitaire $X - P$, montre qu'existe $Q \in A[X]$ de degré $n-1$ tel que $\sum_{i=1}^{n} a_i P^{d-i} = (X - P)Q(X)$. Les coefficients de Q s'obtiennent alors en fonction de ceux des a_i, et ces relations montrent que $(1 - pX)(X^{n-1}Q(1/X)) = \sum_{i=1}^{n} a_i X^i$ (avec $X^{n-1}Q(1/X)$ le polynôme de $A[X]$ défini par $\sum_{i=1}^{n-1} \alpha_i X^{d-i}$, lors que $Q(X) = \sum_{i=1}^{n-1} \alpha_i X^i$).

Dans le cas où $P = 1$ et où A est intègre, il apparaît par conséquent que $A_P \simeq A$, égalité qui reste trivialement vraie même si A n'est pas intègre. On voit ici que si A n'est pas lui-même local, A_P n'est pas local.

En toute généralité, il convient donc d'appeler $S^{-1}A$ **l'anneau quotient de** A **par** S, ou **l'anneau des fractions de** A **par** S, plutôt que la localisation de A par S.

1.3.16 Proposition. — *(i) Soit I un idéal premier d'un anneau commutatif A. Alors A_I est un anneau local, d'idéal maximal $\{a/s \in A_I; a \in I, s \notin I\}$.*
(ii) Si A est un anneau local d'idéal maximal $\mathfrak{m}$, alors $A_\mathfrak{m} \simeq A$.

Démonstration. — Montrons (i). Notons $S = A \setminus I$. Si $a/s \in A_I$ est inversible, il existe $a' \in A, s' \in S$ tels que $a/s \cdot a'/s' = aa'/ss' = 1/1$, donc il existe $t \in S$ tel que $t(aa' - ss') = 0$. Comme S est multiplicative, $tss' \in S$. L'égalité $taa' = tss'$ est ainsi impossible si $a \in I$, car dans ce cas on aurait $taa' \in I = A \setminus S$. On en conclut que si a/s est inversible, $a \in s$. Réciproquement, si $a \in S$, l'élément a/s de A_I est bien inversible, d'inverse s/a. En conclusion, les éléments a/s de A_I sont non inversibles dans A_I si et seulement si $a \in I$ et ils forment alors facilement un idéal. L'anneau A_I est donc bien local.

Pour montrer (ii), commençons par montrer que le morphisme d'anneaux $A \to A_\mathfrak{m}$ défini par $a \mapsto a/1$ est injectif. Si $a/1 = 0/1$ dans $A_\mathfrak{m}$, il existe $t \in A \setminus \mathfrak{m}$, ie t inversible dans A, tel que $ta = 0$. Ceci oblige alors $a = 0$ puisque t est inversible dans A. Montrons maintenant que $A \to A_\mathfrak{m}$ est surjective, car si $a/s \in A_\mathfrak{m}$, du fait que $s \notin \mathfrak{m}$ et que dans A les inversibles sont précisément les éléments de $A \setminus \mathfrak{m}$, l'élément a/s est (s'identifie à l'élément $a \cdot s^{-1}$) dans A. □

1.4. Corps

Nous rappelons ici quelques éléments de la théorie des corps, les références classiques sont entre autres [**2**], [**11**].

1.4.1 Définition **(Base de transcendance)**. — Soit $\mathbf{r} \subset \mathbf{k}$ une extension de corps. on dit qu'une famille $\mathscr{F}$ d'éléments de $\mathbf{k}$ est **algébriquement libre sur** $\mathbf{r}$, si pour toute sous-famille finie $(k_1, \cdots, k_d)$ de $\mathscr{F}$, pour tout $P \in \mathbf{r}[x_1, \cdots, x_d]$, $P(k_1, \cdots, k_d) = 0 \Rightarrow P = 0$.

Soit $\mathbf{r}(\mathscr{F})$ le sous-corps de $\mathbf{k}$ engendré par $\mathscr{F}$. On a : $\mathbf{r} \subset \mathbf{r}(\mathscr{F}) \subset \mathbf{k}$. On dit que $\mathscr{F}$ est **algébriquement génératrice sur** $\mathbf{r}$, si $\mathbf{k}$ est algébrique sur $\mathbf{r}(\mathscr{F})$. La famille $\mathscr{F}$ est une **base de transcendance de** $\mathbf{k}$ **sur** $\mathbf{r}$ lorsqu'elle est algébriquement libre et génératrice. On montre à l'aide du lemme de Zorn que pour toute extension $\mathbf{r} \subset \mathbf{k}$ existe des bases de transcendance et que celles-ci ont toutes même cardinal, on l'appelle le degré de transcendance de $\mathbf{k}$ sur $\mathbf{r}$, et on le note $\partial_\mathbf{r}(K)$. Cette définition généralise le fait que $\partial_\mathbf{r}(\mathbf{r}(x_1, \cdots, x_d)) = d$ et que $(x_1, \cdots, x_d)$ est une base de transcendance de $\mathbf{r}(x_1, \cdots, x_d)$ sur $\mathbf{r}$, puisque si $(k_1, \cdots, k_d)$ est algébriquement libre, $\mathbf{r}(k_1, \cdots, k_d)$ est isomorphe au corps des fractions $\mathbf{r}(y_1, \cdots, y_d)$. Enfin on peut

compléter des familles algébriquement libres en base de transcendance et extraire des base de transcendance de familles algébriquement génératrices

1.4.2 Définition. — Soient $\mathbf{k}$ et $\mathbf{k}'$ deux corps et un morphisme de corps $\mathbf{k} \to \mathbf{k}'$. Ce morphisme étant injectif, on peut supposer, quitte à ne considérer que son image, qu'en réalité $\mathbf{k} \subset \mathbf{k}'$. On appelle **extension de corps** la donnée d'un tel morphisme $\mathbf{k} \to \mathbf{k}'$, ou plus simplement, conformément à ce que l'on vient de remarquer, la donnée d'une inclusion de corps $\mathbf{k} \subset \mathbf{k}'$. Une telle extesion est dite **algébrique** lorsque tout élement de $\mathbf{k}'$ est algébrique sur $\mathbf{k}$, ie est annulé par un élément de $\mathbf{k}[x]$. L'extension $\mathbf{k} \subset \mathbf{k}'$ est dite **finie** lorsque le $\mathbf{k}$-espace $\mathbf{k}'$ est de dimension finie.

Les relations qu'entretiennent les notions définies ci-dessus sont données par les énoncés qui suivent (cf [**16**], Chapitre 9.1, p.113).

1.4.3 Proposition. — *Si $\mathbf{k} \subset \mathbf{k}'$ est une extension finie de corps, cette extension est algébrique.*

1.4.4 Proposition. — *Soient $\mathbf{k} \subset \mathbf{k}'$ une extension de corps et $x_1, \cdots, x_n \in \mathbf{k}'$ algébriques sur $\mathbf{k}$. Alors $\mathbf{k}[x_1, \cdots, x_n]$ est un corps.*

Ces deux propositions sont des équivalences dans le cas d'une extension par un seul élément.

1.4.5 Proposition. — *Soit $\mathbf{k} \subset \mathbf{k}'$ est une extension de corps et $x \in \mathbf{k}'$. On a alors les équivalences*

(i) x est algébrique sur $\mathbf{k}$.
(ii) L'extension $\mathbf{k} \subset \mathbf{k}[x]$ est finie (et donc algébrique par la Proposition 1.4.3).
(iii) La $\mathbf{k}$-algèbre $\mathbf{k}[x]$ est un corps.

1.5. Topologie

Une notion essentielle pour la suite qu'il convient également de rappeler dans cette partie préliminaire est la notion de topologie sur un ensemble.

1.5.1 Définition. — Soit X un ensemble. Une **topologie $\mathcal{T}_X$ sur** X est la donnée d'un ensemble de parties de X, c'est-à-dire la donnée d'un sous-ensemble de l'ensemble des parties de X. Les éléments de $\mathcal{T}_X$ sont appelés les **ouverts de la topologie** $\mathcal{T}_X$. Les ouverts doivent satisfaires les axiomes suivants

1. X et $\emptyset$ sont des ouverts de $\mathcal{T}_X$,
2. Une union arbitraire d'ouverts est un ouvert,
3. Une intersection finie d'ouverts est un ouvert.

Un sous-ensemble de X est un **fermé pour** $\mathcal{T}_X$ s'il est le complémentaire dans X d'un ouvert. Se donner la collection des ouverts ou des fermés d'une topologie revient donc au même, pourvu que les fermés satisfassent les axiomes suivants, déduits des axiomes des ouverts à l'aide de l'opération de prise de complémentaire

1. X et $\emptyset$ sont des fermés pour $\mathcal{T}_X$,

2. Une union finie de fermés est un fermé,
3. Une intersection arbitraire de fermés est un fermé.

La donnée $(X, \mathcal{T}_X)$ s'appelle un **espace topologique**. Un sous-ensemble Y de X est muni naturellement à son tour d'une topologique $\mathcal{T}_Y$ lorsque l'on pose $\mathcal{T}_Y = \{\mathcal{U} \cap Y ; \mathcal{U} \in \mathcal{T}_X\}$. On dit que $\mathcal{T}_Y$ est **la topologie induite sur** Y **par** $\mathcal{T}_X$ (ou par la topologie de X lorsque le contexte est sans ambiguité).

Un **voisinage** d'un point x d'un espace topologique X est un sous-ensemble de X contenant un ouvert de X qui contient le point x.

Un espace topologique est dit $\mathbf{T_1}$ lorsque les points de cet espace sont des fermés, c'est-à-dire lorsque pour tout $x, y \in X$, $x \neq y$, existe un ouvert U tel que $y \in U$ et $x \notin U$.

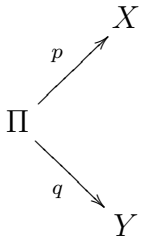
Un espace topologique est dit $\mathbf{T_2}$, **séparé ou de Hausdorff** lorsque deux points disctincts de cet espace possèdent des voisinages disjoints.

Un espace topologique X est dit **quasi-compact** si de tout recouvrement de X par une famille $(U_i)_{i \in I}$ d'ouverts U_i on peut extraire un recouvrement fini $(U_{i_1}, \cdots, U_{i_\ell})$ de X. Un espace topologique est dit **compact** s'il est séparé et quasi-compact.

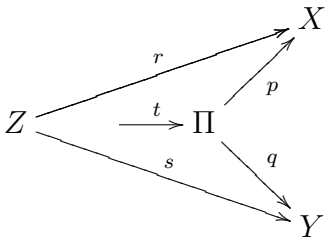
Les notions liées à celle de topologie que nous étuiderons particuliérement sont les notions d'adhérence et d'irréductibilité, nous les rappellerons au moment voulu dans la suite du chapitre.

Nous aurons à formaliser la notion de variété produit et pour cela il est pratique d'envisager le produit de manière catégorielle. C'est ce que nous faisons ici maintenant.

***1.5.2 Définition* (Produit dans une catégorie).** — Soit $\mathcal{C}$ une catégorie et X, Y deux objets de $\mathcal{C}$. Un **produit de** X **et de** Y est la donnée d'un objet Π de $\mathcal{C}$ et de deux flèches p, q de la sorte



vérifiant la propriété universelle suivante : pour tout objet Z de $\mathcal{C}$ et tout couple de flèches r, s de Z vers X et Y respectivement, il existe une unique flèche t telle que le diagramme suivant commute



On dit que p et q sont **les projections** du produit.

1.5.3 Remarque. — Si le produit de X et Y existe, il est unique à un unique isomorphisme près, l'isomorphisme commutant avec les projections. La propriété universelle du produit assure que la donnée de deux morphismes r et s d'un objet Z vers Π est la donnée t, puisque qu'à partir de t on retrouve r par $r = p \circ t$ et on retrouve s par $s = q \circ t$. Et réciproquement, la donnée de t induit deux morphismes uniques r et s. Autrement dit cette propriété universelle signifie

$$\mathrm{Mor}(Z, \Pi) \simeq \mathrm{Mor}(Z, X) \times \mathrm{Mor}(Z, Y)$$

le produit ci-dessus étant le produit cartésien. Si l'on pense à la catégorie des ensembles, Π est le produit cartésien de X et Y, t est le morphisme que l'on note (r, s), celui dont les composantes sont précisément r et s, et p est la projection usuelle sur la première composante de $X \times Y$, tandis que q est la projection sur la seconde composante de $X \times Y$.

CHAPITRE 2

VARIÉTÉS ALGÉBRIQUES

Nous définissons dans ce chapitre les variétés algébriques. Pour cela il faut dans un premier temps définir les ensembles algébriques affines de $\mathbf{k}^n$ (dits ensembles algébriques affines plongés), puis les variétés algébriques affines, les prévariétés et enfin les variétés.

2.1. Les ensembles algébriques affines et la topologie de Zariski

2.1.1 Définition. — Soit S un sous-ensemble *a priori* quelconque de $\mathbf{k}[x_1, \cdots, x_n]$. On définit **l'ensemble des zéros communs de** S par

$$\mathcal{Z}(S) := \{(x_1, \cdots, x_d) \in \mathbf{k}^n; f_P(x_1, \cdots, x_n) = 0,\ \forall P \in S\},$$

où f_P est la fonction polynôme associée au polynôme P. Notons que si S est la partie vide de $\mathbf{k}[x_1, \cdots, x_n]$, $\mathcal{Z}(S) = \mathbf{k}^n$.

Un tel sous-ensemble $\mathcal{Z}(S)$ de $\mathbf{k}^n$, pour $S \subset \mathbf{k}[x_1, \cdots, x_n]$, s'appelle un **ensemble algébrique de** $\mathbf{k}^n$. Notons $\mathcal{A}(\mathbf{k}^n)$ l'ensemble des ensembles algébriques de $\mathbf{k}^n$, il s'agit d'un sous-ensemble de l'ensemble $\mathcal{P}(\mathbf{k}^n)$ des parties de $\mathbf{k}^n$.

2.1.2 Remarque. — Conformément à ce qui a été annoncé en préliminaire, nous n'utiliserons pas de notation différentes pour un polynôme et la fonction polynôme qui lui est associée, on écrira ainsi abusivement

$$\mathcal{Z}(S) := \{(x_1, \cdots, x_n) \in \mathbf{k}^d; P(x_1, \cdots, x_n) = 0,\ \forall P \in S\} = \bigcap_{P \in S} \{P = 0\}.$$

2.1.3 Exemples. — Voyons quelques exemples d'ensembles algébriques

1. L'ensemble vide est un ensemble algébrique de $\mathbf{k}^n$, quel que soit $n \geq 1$. Il suffit de considérer $S = \{1\}$ (1 étant le polynôme de degré 0 égal à 1).
2. L'espace affine de dimension n, quel que soit $n \geq 1$, est un ensemble algébrique de $\mathbf{k}^n$. Il suffit de considérer $S = \{0\}$ (0 le polynôme de degré 0 égal à 0). On le note $\mathbb{A}^n_{\mathbf{k}}$ ou $\mathbb{A}^n(\mathbf{k})$ ou encore $\mathbb{A}^n$ s'il n'y a pas d'ambiguité sur le corps $\mathbf{k}$.

3. Tout singleton $(a_1, \ldots, a_n)$ de $\mathbf{k}^n$ est un ensemble algébrique de $\mathbf{k}^n$. Il suffit de considérer le singleton $S = \{(x_1 - a_1) \cdots (x_n - a_n)\}$.
4. Tout sous-espace vectoriel ou affine de $\mathbf{k}^n$ est un ensemble algébrique de $\mathbf{k}^n$ puisqu'il est l'ensemble des zéros communs de formes linéaires ou affines, qui sont des polynômes.
5. Les ensembles algébriques de $\mathbf{k}$ sont $\emptyset$, $\mathbf{k}$ et les sous-ensembles finis de $\mathbf{k}$.

2.1.4 Notations. — On peut définir une application $\mathcal{Z}$ de l'ensemble des parties $\mathcal{P}(\mathbf{k}[x_1, \cdots, x_n])$ de $\mathbf{k}[x_1, \cdots, x_n]$ vers l'ensemble des ensembles algébriques $\mathcal{A}(\mathbf{k}^n)$ de $\mathbf{k}^n$, en posant

$$\begin{array}{rccc} \mathcal{Z}: & \mathcal{P}(\mathbf{k}[x_1, \cdots, x_n]) & \to & \mathcal{A}(\mathbf{k}^n) \\ & S & \mapsto & \mathcal{Z}(S) \end{array}$$

Notre premier objectif est d'étudier l'application $\mathcal{Z}$. Pour cela il convient de comprendre son comportement relativement aux opérations ensemblistes naturelles faites sur les parties de l'algèbre des polynômes qui sont les variables de $\mathcal{Z}$, comme la réunion et l'intersection, mais aussi relativement aux opérations algébriques naturelles liées à ces parties : par exemple comparer $\mathcal{Z}(S)$ et $\mathcal{Z}(\mathcal{I}(S))$, $\mathcal{I}(S)$ étant l'idéal engendré par la partie S de $\mathbf{k}[x_1, \cdots, x_n]$. La proposition qui suit concerne les opérations ensemblistes faites sur les parties de $\mathbf{k}[x_1, \cdots, x_n]$.

2.1.5 Proposition. — *Avec les notations précédentes, on a*

(i) L'application $\mathcal{Z}$ est décroissante (pour les ordres partiels donnés par l'inclusion des parties de $\mathbf{k}[x_1, \cdots, x_n]$ et l'inclusion des parties de $\mathbf{k}^n$), autrement dit si $S \subset T$ alors $\mathcal{Z}(T) \subset \mathcal{Z}(S)$,

(ii) Si I est un ensemble et $(S_i)_{i \in I}$ une famille de parties de $\mathbf{k}[x_1, \cdots, x_n]$,

$$\bigcap_{i \in I} \mathcal{Z}(S_i) = \mathcal{Z}(\bigcup_{i \in I} S_i),$$

(iii) Si $S, T \subset \mathbf{k}[x_1, \cdots, x_n]$, alors

$$\mathcal{Z}(S) \cup \mathcal{Z}(T) = \mathcal{Z}(S \cdot T),$$

où $S \cdot T = \{PQ; P \in S, Q \in T\}$.

Démonstration. — (i) Si un élément de $\mathbf{k}^n$ annule tous les polynômes de T, il annule en particulier tous les polynômes de S.
(ii) Cette proposition est tautologique.
(iii) Un élément $a \notin \mathcal{Z}(S) \cup \mathcal{Z}(T)$ si et si seulement existent $P \in S$ et $Q \in T$ tels que $P(a) \cdot Q(a) \neq 0$ ie que $a \notin \mathcal{Z}(S \cdot T)$.

□

En conséquence de la Proposition 2.1.5, nous observons que les ensembles algébriques de $\mathbf{k}^n$ définissent les fermés d'une topologie. Ceci conduit à la définition suivante.

2.1.6 Définition. — Les ensembles algébriques de $\mathbf{k}^n$ définissent les fermés d'une topologie, appelée **la topologie de Zariski de $\mathbf{k}^n$**. Si X est un ensemble algébrique

de $\mathbf{k}^n$, **la topologie de Zariski de** X est la topologie induite sur X par la topologie de Zariski de $\mathbf{k}^n$. Les ouverts de la topologie de Zariski de X sont appelés familièrement les **ouverts de Zariski de** X ou les **variétés quasi-affines de** X. Les ouverts du type $X \setminus \mathcal{Z}(P)$, pour $P \in \mathbf{k}[x_1, \cdots, x_n]$, sont appelés les **ouverts fondamentaux ou distingués de** X. Afin de la distinguer de la topologie de Zariski, on appelle, lorsque $\mathbf{k} = \mathbb{R}$ ou $\mathbb{C}$, la topologie usuelle de $\mathbf{k}^n$ fournie par le produit scalaire standard la **topologie transcendante**.

2.1.7 Remarque. — Notons que si Y est un fermé de X, $Y = X \cap \mathcal{Z}(J)$, pour un certain idéal J de $\mathbf{k}[x_1, \cdots, x_n]$. Or si $X = \mathcal{Z}(I)$, pour un idéal I de $\mathbf{k}[x_1, \cdots, x_n]$, on en déduit que $Y = \mathcal{Z}(I) \cap \mathcal{Z}(J) = \mathcal{Z}(I + J)$ par la Proposition 2.1.5 (i). En conséquence les fermés de X sont du type $\mathcal{Z}(I')$, pour I' un idéal de $\mathbf{k}[x_1, \cdots, x_n]$ contenant I.

La topologie de Zariski est moins fine que la topologie usuelle, lorsque $\mathbf{k} = \mathbb{R}$ ou $\mathbf{k} = \mathbb{C}$. En effet, les ouverts de Zariski sont des ouverts au sens de la topologie usuelle sur $\mathbb{R}^n$ et $\mathbb{C}^n$, puisque les polynômes sont des fonctions continues pour la topologie usuelle. Bien entendu la topologie de Zariski est strictement plus grossiére que la topologie usuelle sur $\mathbb{R}$ ou $\mathbb{C}$.

2.1.8 Exercice. — *Montrer que la topologie de Zariski sur $\mathbb{R}^n$ contient strictement moins d'ouverts que la topologie euclidienne n'en contient.*

Un fermé de Zariski de $\mathbf{k}^n$ est l'ensemble des zéros communs d'un ensemble donné S de polynômes de $\mathbf{k}[x_1, \cdots, x_n]$. Une des conséquence principales du Théorème 1.3.3 de noethérianité de $\mathbf{k}[x_1, \cdots, x_n]$ est qu'il suffit pour générer les ensembles algébriques de ne considérer que les parties finies S de $\mathbf{k}[x_1, \cdots, x_n]$. Cette propriété est l'objet de la proposition qui suit.

2.1.9 Notations. — On note, pour une partie S de $\mathbf{k}[x_1, \cdots, x_n]$, (S) l'idéal de $\mathbf{k}[x_1, \cdots, x_n]$ engendré par S. Par définition,

$$(S) = \{\sum_{i=0}^{k} A_i P_i; k \in \mathbb{N}, A_i \in \mathbf{k}[x_1, \cdots, x_n], P_i \in S\}.$$

2.1.10 Proposition. — *Soit S une partie (arbitraire) de $\mathbf{k}[x_1, \cdots, x_n]$.*

(i) On a $\mathcal{Z}(S) = \mathcal{Z}((S))$,

(ii) Il existe des polynômes $P_1, \cdots, P_\ell$ de $\mathbf{k}[x_1, \cdots, x_n]$ en nombre fini tels $\mathcal{Z}(S) = \mathcal{Z}(\{P_1, \cdots, P_\ell\})$.

Démonstration. — Un élément de $\mathbf{k}^n$ est annulé par tous les éléments de S si et seulement s'il est annulé par tous les éléments de (S). D'autre part, d'après le Théorème 1.3.3 de noethérianité de $\mathbf{k}[x_1, \cdots, x_n]$, (S) est finiment engendré. Supposons que $(S) = (P_1, \cdots, P_\ell)$, c'est-à-dire que $(S) = \{\sum_{i=0}^{\ell} A_i P_i; A_i \in \mathbf{k}[x_1, \cdots, x_n]\}$. Alors un élément de $\mathbf{k}^n$ est annulé par tous les éléments de (S) si et seulement s'il est annulé par tous les polynômes P_i, $i = 1, \ldots, \ell$. □

Parmi les ensembles algébriques, qui sont tous du type $\mathcal{Z}(P_1, \cdots, P_\ell)$, pour $P_i \in \mathbf{k}[x_1, \cdots, x_n], i = 1, \cdots, \ell$, on distingue ceux donnés par les zéros d'un seul polynôme.

2.1.11 Définition. — On appelle **hypersurface de $\mathbf{k}^n$** un ensemble algébrique X de $\mathbf{k}^n$ tel que $X = \mathcal{Z}(P)$, où $P \in \mathbf{k}[x_1, \cdots, x_n]$.

2.1.12 Exercice. — *Montrer que tous les ensembles algébriques de $\mathbb{R}^n$ sont des hypersurfaces. En est-il de même pour $\mathbb{C}^n$ (Ind. Considérer par exemple un polynôme P de $\mathbb{C}[x, y]$ dont le seul zéro serait le point $a = (0, 0)$. Écrire ensuite $P(x, y) = \sum_{i=1}^{d} A_i(x)y^i$, où $A_i \in \mathbb{C}[x]$ est non nul. Choisir $\alpha \neq 0$ tel que $\prod_{i=1}^{d} A_i(\alpha) \neq 0$ et constater que le polynôme $P(\alpha, y) \in \mathbb{C}[y]$ est non constant mais sans racine sur $\mathbb{C}$.) ?*

2.1.13 Remarque. — Tout ouvert de Zariski d'un ensemble algébrique de $\mathbf{k}^n$ est réunion finie d'ouverts fondamentaux. En effet il suffit de vérifier que tout fermé de $\mathbf{k}^n$ est intersection finie d'hypersurface. Mais d'après la Proposition 2.1.10 (ii) tel est bien le cas puisque $\mathcal{Z}(\{P_1, \cdots, P_\ell\}) = \cap_{i=1}^{\ell} \mathcal{Z}(P_i)$.

2.1.14 Remarque. — Tout ensemble algébrique affine de $\mathbf{k}^n$ est un espace quasi-compact. En effet si $(U_j)_{j\in J}$ est une famille d'ouverts qui recouvrent l'ensemble algébrique affine $X = \mathcal{Z}(I)$, où I est un idéal de $\mathbf{k}[x_1, \cdots, x_n]$, les fermés $F_j = X \setminus U_j$ sont donnés par des idéaux I_j de $\mathbf{k}[x_1, \cdots, x_n]$ contenant I (cf Remarque 2.1.7) qui vérifient $\cap_{j\in J} \mathcal{Z}(I_j) = \emptyset$. Or si aucune sous-famille finie $\mathcal{F}$ de $(I_j)_{j\in J}$ ne satisfaisait $\cap_{K\in\mathcal{F}} \mathcal{Z}(K) = \emptyset$, on pourrait construire une suite strictement croissante d'idéaux de $\mathbf{k}[x_1, \cdots, x_n]$, ce qui contredirait la noethérianité de $\mathbf{k}[x_1, \cdots, x_n]$. On montre de même que tout ouvert de Zariski de X est quasi-compact.

2.2. Idéal d'un ensemble algébrique affine et Nullstellensatz

La Proposition 2.1.10 (i) établit que les ensembles algébriques de $\mathbf{k}^n$ sont donnés seulement par les zéros communs des éléments des idéaux de $\mathbf{k}[x_1, \cdots, x_n]$. C'est cette remarque qui permet d'algébriser l'étude de la géométrie des ensembles des zéros des polynômes ; aux propriétés algébriques d'un idéal vont correspondre des propriétés géométriques et topologiques de l'ensemble des zéros communs des polynômes de cet idéal. Ce sont ces correspondances que l'on va établir dans le reste du chapitre.

2.2.1 Définition. — Soit X une partie de $\mathbf{k}^n$. On appelle **idéal de** X et on note $\mathcal{I}(X)$ l'ensemble suivant de $\mathbf{k}[x_1, \cdots, x_n]$

$$\mathcal{I}(X) = \{P \in \mathbf{k}[x_1, \cdots, x_n]; P(a) = 0, \forall a \in X\},$$

dont on montre trivialement qu'il s'agit d'un idéal de $\mathbf{k}[x_1, \cdots, x_n]$.

2.2.2 Remarque. — L'application de restriction à un sous-ensemble X de $\mathbf{k}^n$ des fonctions polynomiales

$$\begin{array}{rccc} {}_{|X}: & \mathbf{k}[x_1,\cdots,x_n] & \to & \mathcal{F}(X;\mathbf{k}) \\ & P & \mapsto & f_{P|X} \end{array}$$

est un morphisme d'algèbres de $\mathbf{k}[x_1,\cdots,x_n]$ vers l'algèbre $\mathcal{F}(X;\mathbf{k})$ des fonctions sur X dont le noyau est par définition l'idéal $\mathcal{I}(X)$. L'image de ce morphisme est par conséquent isomorphe à l'algèbre $\mathbf{k}[x_1,\cdots,x_n]/\mathcal{I}(X)$, on l'appelle **l'algèbre des fonctions polynomiales sur** X ou **l'algèbre des fonctions régulières sur** X dans le cas $\mathbf{k}$ algébriquement clos (voir la Proposition 2.4.11 (ii) pour une justification de cette terminologie) ou **l'algèbre affine de** X ou **l'anneau des coordonnées de** X. Il s'agit d'une $\mathbf{k}$ algèbre de type finie (car quotient d'une algèbre de type finie) que l'on note $A(X)$ ou $\Gamma(X)$ (la notation $\Gamma(X)$ est plutôt à réserver au cas où le corps $\mathbf{k}$ est algébriquement clos, cf Proposition 2.4.11 (ii).)

2.2.3 Remarque. — La k-algèbre $A(X)$ est **réduite**, ie par définition que 0 est le seul élément nilpotent de $A(X)$. En effet, si un polynôme P est tel qu'existe un entier $r \in \mathbb{N}$ tel que $P^r \in \mathcal{I}(X)$, pour tout $x \in X$, $P^r(x) = 0$, de sorte que $P(x) = 0$ et donc $P \in \mathcal{I}(X)$. D'autre part, si $\mathcal{I}(X)$ est premier $A(X)$ est une algèbre intègre (cf Définition 1.3.9).

2.2.4 Exercice. — *Montrer que si X est un singleton de $\mathbf{k}^n$, $\mathcal{I}(X)$ est un idéal maximal de $\mathbf{k}[x_1,\cdots,x_n]$ (montrer pour cela que l'algèbre affine $A(X)$ de X est un corps). La réciproque est-elle toujours vraie (considérer l'idéal (x^2+1) de $\mathbb{R}[x]$ et montrer qu'il est maximal en montrant qu'il est isomorphe à $\mathbb{C}$) ?*

2.2.5 Remarque. — Nous verrons bientôt qu'une conséquence du théorème des zéros de Hilbert 2.2.11 est que lorsque le corps $\mathbf{k}$ est algébriquement clos les idéaux maximaux de $\mathbf{k}[x_1,\cdots,x_n]$ sont exactement les idéaux du type $\mathcal{I}(\{a\})$, $a \in \mathbf{k}^n$.

Mais pour commencer l'étude des applications $\mathcal{I}$ et $\mathcal{Z}$ on peut déjà remarquer que

2.2.6 Proposition. — *L'application*

$$\mathcal{I} : \{ \text{ ensembles algébriques de } \mathbf{k}^n \} \to \{ \text{ idéaux de } \mathbf{k}[x_1,\cdots,x_n] \ \}$$

est décroissante (pour l'inclusion des ensembles), injective, d'inverse à gauche

$$\mathcal{Z} : \{ \text{ idéaux de } \mathbf{k}[x_1,\cdots,x_n] \ \} \to \{ \text{ ensembles algébriques de } \mathbf{k}^n \}.$$

Autrement dit quel que soit X ensemble algébrique de $\mathbf{k}^n$, $\mathcal{Z}(\mathcal{I}(X)) = X$. En particulier si X et Y sont deux ensembles algébriques de $\mathbf{k}^n$ tels que $X \subsetneq Y$, il existe un polynôme P s'annulant sur X et non sur Y.

Démonstration. — L'inclusion $X \subset \mathcal{Z}(\mathcal{I}(X))$ est triviale. Montrons alors l'inclusion $\mathcal{Z}(\mathcal{I}(X)) \subset X$. L'ensemble algébrique X est du type $\mathcal{Z}(S)$, où $S \subset \mathbf{k}[x_1,\cdots,x_n]$. On a alors $S \subset \mathcal{I}(\mathcal{Z}(S))$, par décroissante de $\mathcal{Z}$ (cf Proposition 2.1.5 (i)), on obtient bien $X = \mathcal{Z}(S) \supset \mathcal{Z}(\mathcal{I}(X))$. □

2.2.7 Remarque. — En revanche l'application $\mathcal{I}$ n'est certainement pas surjective. Par exemple si $n = 1$ et si X était un ensemble algébrique de $\mathbb{R}$ tel que $\mathcal{I}(X) = (x^2)$, on aurait $\mathcal{Z}(\mathcal{I}(X)) = \mathcal{Z}(x^2) = \{0\} = X$, d'après la Proposition 2.2.6. Mais alors $\mathcal{I}(X) = (x) \neq (x^2)$. Ce qui est contradictoire. De même on montre que l'idéal principal $(x^2 + 1)$ de $\mathbb{R}[x]$ n'est pas dans l'image de $\mathcal{I}$. On peut encore remarquer que l'algèbre $\mathbb{R}[x]/(x^2)$ n'est pas réduite, puisque la classe de x y est un nilpotent, ceci contredit alors la Remarque 2.2.3 dans l'hypothèse où $\mathbb{R}[x]/(x^2)$ serait l'agèbre affine $\mathbb{R}[x]/\mathcal{I}(X)$ d'un certain ensemble algébrique X.

L'image de l'application $\mathcal{I}$ est fournie par le théorème dit "des zéros de Hilbert", ou "Nullstellensatz". Ce théorème porte sur les corps algébriquement clos, mais nous en donnons une version adaptée dans le cas $\mathbf{k} = \mathbb{R}$, eu égard à l'importance du corps $\mathbb{R}$ en géométrie algébrique. Notons qu'il existe des versions du nullstellensatz sur les corps p-adiques $\mathbb{Q}_p$, p entier premier.

2.2.8 Définition. — Soit J un idéal d'un anneau A, on on appelle **radical de** J, et on note $\sqrt{J}$, l'idéal

$$\sqrt{J} := \{P \in \mathbf{k}[x_1, \cdots, x_n]; \exists r \in \mathbb{N},\ P^r \in J\}.$$

Il est clair que $J \subset \sqrt{J}$ et que si J est premier et *a fortiori* maximal, $\sqrt{J} = J$. De manière générale on dit que J **est un idéal radical** lorsque $\sqrt{J} = J$. Il est trivial de noter que $\sqrt{\sqrt{J}} = \sqrt{J}$, ie que le radical d'un idéal est radical. On remarque aussi qu'un idéal premier est radical.

2.2.9 Proposition. — *Soit I un idéal d'un anneau A, alors*

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A, I \subset \mathfrak{p}} \mathfrak{p},$$

où $\operatorname{Spec} A$ *est l'ensemble des idéaux premiers de A.*

Démonstration. — Si $\mathfrak{p}$ est un idéal premier contenant I, on a aussi $\sqrt{I} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$. Donc $\sqrt{I} \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec} A, I \subset \mathfrak{p}} \mathfrak{p}$. Maintenant soit $a \notin \sqrt{I}$, ie tel que $1, a, a^2, \cdots \notin I$. On note $S = \{a^\ell; \ell \in \mathbb{N}\}$. L'ensemble

$$\mathcal{S} := \{J \text{ idéal de } A; I \subset J \ \&\ J \cap S = \emptyset\}$$

est non vide, puisque l'idéal $I \in \mathcal{S}$. D'autre part cet ensemble est inductif pour l'ordre donné par l'inclusion (cf Définition 1.2.4) puisque si une partie $(J_u)_{u \in U}$ de $\mathcal{S}$ est totalement ordonnée, l'ensemble $\cap_{u \in U} J_u$ est un idéal, contenant tous les idéaux de $(J_u)_{u \in U}$ et ne rencontrant pas S ; il s'agit ainsi d'un majorant pour l'inclusion de la partie $(J_u)_{u \in U}$. D'après le Lemme de Zorn 1.2.5 l'ensemble $\mathcal{S}$ possède un élément maximal $\mathfrak{J}$. En particulier $I \subset \mathfrak{J}$ et $\mathfrak{J} \cap S = \emptyset$. Nous allons prouver $\mathfrak{J}$ est un idéal premier de A, ce qui montrera que $a \notin \bigcap_{\mathfrak{p} \in \operatorname{Spec} A, I \subset \mathfrak{p}} \mathfrak{p}$. Soient $\alpha, \beta \in A$ tels que $\alpha\beta \in \mathfrak{J}$ et $\alpha \notin \mathfrak{J}$, $\beta \notin \mathfrak{J}$. On a alors $\mathfrak{J} \subsetneq \mathfrak{J} + (\alpha)$ et $\mathfrak{J} \subsetneq \mathfrak{J} + (\beta)$, ce qui par maximalité de $\mathfrak{J}$, impose l'existence d'entiers r, s tels que $a^r = j + \gamma\alpha$ et $a^s = j' + \mu\beta$, avec $j, j' \in \mathfrak{J}$ et

$\gamma, \mu \in A$. On en conclut que $a^{r+s} = jj' + \gamma\alpha j' + \mu\beta j + \gamma\mu\alpha\beta \in \mathfrak{J}$, ce qui contredit $\mathfrak{J} \cap S = \emptyset$. □

2.2.10 Remarque. — Si X est un sous-ensemble de $\mathbf{k}^n$, l'idéal $\mathcal{I}(X)$ est radical (cf Remarque 2.2.3). Le théorème des zéros de Hilbert ou Nullstellensatz, dit beaucoup plus que cette trivialité : si k est algébriquement clos et $X = \mathcal{Z}(J)$, ce théorème assure que $\mathcal{I}(X) = \sqrt{J}$.

***2.2.11 Théorème* (Nullstellensatz)**. — *Soit J un idéal de $\mathbf{k}[x_1, \cdots, x_n]$.*

(i) Si $\mathbf{k}$ est algébriquement clos

$$\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}.$$

En particulier $J = k[x_1, \cdots, x_n]$ si et seulement si $\mathcal{Z}(J)$ est vide.

(ii) Si $\mathbf{k} = \mathbb{R}$:

$$\mathcal{I}(\mathcal{Z}(J)) = \{P \in \mathbb{R}[x_1, \cdots, x_n]; \exists r \in \mathbb{N},\ Q_1, \cdots, Q_\ell \in \mathbb{R}[x_1, \cdots, x_n],$$
$$P^{2r} + Q_1^2 + \cdots + Q_\ell^2 \in J\}.$$

Démonstration. — (i) Tout d'abord il est bien clair que l'égalité $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ assure que $J = k[x_1, \cdots, x_n]$ si et seulement si $\mathcal{Z}(J)$ est vide.

En effet si $J = k[x_1, \cdots, x_n]$, alors J contient le polynôme constant 1 et $\mathcal{Z}(J)$ est vide. Réciproquement si $\mathcal{Z}(J)$ est vide, $\mathcal{I}(\mathcal{Z}(J)) = k[x_1, \cdots, x_n]$. Mais alors $1 \in \sqrt{J}$ et donc il existe $r \in \mathbb{N}$ tel que $1 = 1^r \in J$, c'est-à-dire que $J = k[x_1, \cdots, x_n]$.

On va montrer maintenant que, si pour tout $m \in \mathbb{N}^*$ et tout idéal propre L de $k[x_1, \cdots, x_m]$, $\mathcal{Z}(L)$ n'est pas vide, alors pour tout $n \in \mathbb{N}^*$ et tout idéal J de $k[x_1, \cdots, x_n]$, $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$.

Soit pour cela J un idéal de $k[x_1, \cdots, x_n]$. Il est bien clair que l'inclusion $\mathcal{I}(\mathcal{Z}(J)) \supset \sqrt{J}$ est triviale. Soit alors $P \in k[x_1, \cdots, x_n] \setminus \{0\}$ tel que $P(a) = 0$ lorsque $a \in \mathbf{k}^n$ est tel que $Q(a) = 0$ pour tout $Q \in J$. Soit L l'idéal de $\mathbf{k}[x_1, \cdots, x_n, y]$ engendré par J et $1 - yP$. Alors $\mathcal{Z}(L) = \emptyset$ et notre hypothèse implique que $L = \mathbf{k}[x_1, \ldots, x_n, y]$. Il existe par conséquent des polynômes $P_1, \ldots, P_\ell \in J$ et $R_0, \cdots, R_\ell \in \mathbf{k}[x_1, \ldots, x_n, y]$ tels que

$$1 = R_0(1 - yP) + R_1P_1 + \cdots + R_\ell P_\ell.$$

En posant $y = 1/P$ (ce qui signifie que l'on se place dans le corps des fractions rationelles $\mathbf{k}(x_1, \cdots, x_n)$), et en multipliant des deux côtés de l'égalité par une puissance suffisamment grande de P pour chasser les puissances de P aux dénominateurs des fractions du membre de droite, on obtient l'existence d'un entier r tel que $P^r \in J$.

En conclusion la démonstration du Nullstellensatz se ramène à la démonstration du Théorème 2.2.12 qui suit, dit Nullstellensatz faible.

(ii) On renvoie à [Boc-Cos-Roy], 4.1.4 pour $\mathbf{k} = \mathbb{R}$.

□

***2.2.12 Théorème* (Nullstellensatz faible).** — *Si* $\mathbf{k}$ *est algébriquement clos, et si* J *est un idéal propre de* $k[x_1, \cdots, x_n]$*, l'ensemble* $\mathcal{Z}(J)$ *n'est pas vide.*

2.2.13 Remarque. — Nous allons montrer que le Nullstellensatz faible implique le Nullstellensatz. Mais il est facile de voir que le Nullstellensatz et le Nullstellensatz faibles sont équivalents. En effet, soit $\mathbf{k}$ un corps algébriquement clos et J un idéal propre de $\mathbf{k}[x_1, \cdots, x_n]$. Le radical $\sqrt{J}$ de J est propre, sinon $1 \in \sqrt{J} \Longrightarrow \exists r \in \mathbb{N},\ 1^r = 1 \in J \Longrightarrow J = \mathbf{k}[x_1, \cdots, x_n]$. Il s'ensuit que puisque $\sqrt{J} = \mathcal{I}(\mathcal{Z}(J))$ est propre, $\mathcal{Z}(J) \neq \emptyset$.

La preuve du Nullstellensatz faible s'appuie sur le lemme algébrique suivant.

2.2.14 Lemme. — *Soient* $\mathbf{k}$ *un corps,* $\mathbf{k}'$ *un corps algébriquement clos, et* $f : \mathbf{k} \to \mathbf{k}'$ *un morphisme de corps. Il existe alors un prolongement de* f *en un morphisme d'anneau* $f' : \mathbf{k}[x_1, \cdots, x_n] \to \mathbf{k}'$*.*

Démonstration. — Voir [**11**] Chap IX-1, Théorème 1.1, p. 378.

□

Démonstration. — (Preuve du Nullstellensatz faible). On applique le Lemme 2.2.14 pour remarquer que si $\mathbf{k}[y_1, \cdots, y_m]$, extension finie (d'anneaux) de l'anneau k par des éléments $y_1, \cdots, y_m$ d'un sur-anneau A de $\mathbf{k}$, est en réalité un corps, alors cette extension est une extension de corps algébrique sur $\mathbf{k}$ [(1)] . En effet, le plongement de $\mathbf{k}$ dans sa clôture algébrique $\bar{\mathbf{k}}$ se prolonge en un morphisme de corps $\mathbf{k}[y_1, \cdots, y_m] \to \bar{\mathbf{k}}$, par le Lemme 2.2.14, qui est un isomorphisme sur son image. Si $\mathbf{k}$ est algébriquement clos, on en conclut bien sûr que $\mathbf{k}[x_1, \cdots, x_n] = \mathbf{k}$.

Maintenant si J est un idéal propre de $\mathbf{k}[x_1, \cdots, x_n]$, soit M un idéal maximal de $\mathbf{k}[x_1, \cdots, x_n]$ contenant J. Le corps $\mathbf{k}[x_1, \cdots, x_n]/M$ est une algèbre de type finie sur finie de k, car engendré par les images de $x_1, \ldots, x_n$ modulo M. Par ce qui précède, $\mathbf{k}[x_1, \cdots, x_n]/M \simeq \mathbf{k}$ et les flèches $\mathbf{k}[x_1, \cdots, x_n] \to \mathbf{k}[x_1, \cdots, x_n]/M \simeq \mathbf{k}$ se composent en un morphisme d'algèbres φ pour donner un élément $(a_1, \cdots, a_n)$ de $\mathbf{k}^n$, défini par $a_i = \varphi(x_i)$. Si $P \in J$, on a $P(a_1, \cdots, a_n) = \varphi(P) = 0$, puisque $J \subset M$. □

2.2.15 Remarque. — Nous donnerons plus loin une preuve complète du Nullstellensatz à l'aide du théorème d'élimination des quantificateurs dans le langage des corps algébriquement clos.

2.2.16 Corollaire. — *Soit* $\mathbf{k}$ *un corps algébriquement clos.*

---

(1) Cette proposition est une version possible du Nullstellensatz. Une autre, encore plus générale, est la suivante (cf [**16**], Théorème 10.11) : *Soit* $\mathbf{k} \subset \mathbf{l}$ *une extension de corps, telle que* $\mathbf{l}$ *est une* $\mathbf{k}$*-algèbre de type finie, alors* $\mathbf{l}$ *est un* $\mathbf{k}$*-espace vectoriel de dimension finie.* Autrement dit être un corps pour une algèbre $\mathbf{l}$ finiment engendrée sur $\mathbf{k}$ (en tant qu'algèbre) impose que l'extension de corps $\mathbf{k} \subset \mathbf{l}$ est finie. D'après la Proposition 1.4.3, cette dernière proposition est en effet plus forte que la version montrée dans notre preuve du Nullstellensatz faible et est une réciproque de la Proposition 1.4.4.

(i) La correspondance

$$\mathcal{I} : \{ \text{ points de } \mathbf{k}^n \} \to \{ \text{ idéaux maximaux de } \mathbf{k}[x_1, \cdots, x_n] \ \}$$

est bijective, d'inverse $\mathcal{Z}$. De plus pour $(a_1, \cdots, a_n) \in \mathbf{k}^n$, $\mathcal{I}(\{(a_1, \cdots, a_n)\}) = (x_1 - a_1, \cdots, x_n - a_n)$ et

$$X \text{ est un singleton de } \mathbf{k}^n \iff \mathcal{I}(X) \text{ est maximal } \iff \Gamma(X) = \mathbf{k}.$$

(ii) Les points de $\mathbf{k}^n$ sont en bijection avec les **caractères de** $\mathbf{k}[x_1, \cdots, x_n]$*, c'est-à-dire avec les morphismes de $\mathbf{k}$-algèbres $\mathbf{k}[x_1, \cdots, x_n] \to \mathbf{k}$.*

(iii) La correspondance

$$\mathcal{I} : \{\text{ensembles algébriques de } \mathbf{k}^n\} \to \{\sqrt{J}; J \text{ est un idéal de } \mathbf{k}[x_1, \cdots, x_n]\}$$

est bijective et d'inverse $\mathcal{Z}$.

Démonstration. — (i) Tout d'abord l'idéal $I(\{a\})$ est bien maximal car est le noyau de l'évaluation en a qui fournit l'isomorphisme $A(\{a\}) = \mathbf{k}$. On a donc montré que $\mathcal{I}$ est bien à valeurs dans les idéaux maximaux quand on l'applique sur des singletons.

Ensuite si $P \in \mathcal{I}(\{a\})$, en effectuant la division euclidienne de P par $x_1 - a_1$ (cf Théorème 1.3.6), on obtient $P = (x_1 - a_1)Q(x_1, \cdots, x_n) + R(x_2, \cdots, x_n)$, avec $R \in \mathcal{I}(Y)$, où $Y = (a_2, \cdots, a_n) \in \mathbf{k}^{n-1}$. Par récurrence, on voit que $R \in (x_2 - a_2, \cdots, x_n - a_n)$. On a ainsi caractérisé l'idéal maximal $\mathcal{I}(\{a\})$ comme étant $(x_1 - a_1, \cdots, x_n - a_n)$.

Montrons maintenant que si J est maximal, il existe $a \in \mathbf{k}^n$ tel que $J = \mathcal{I}(\{a\})$. Ceci prouvera la surjectivité de $\mathcal{I}$ entre les singletons de $\mathbf{k}^n$ et l'ensemble des idéaux maximaux de $\mathbf{k}[x_1, \cdots, x_n]$. Avec l'injectivité de $\mathcal{I}$ (Proposition 2.2.6) la bijectivité de $\mathcal{I}$ telle qu'annoncée sera alors prouvée.

Commençons par montrer que $\mathcal{I}(\mathcal{Z}(J)) = J$. On sait d'après le Nullstellensatz 2.2.11 que $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J} = J$, car J étant maximal est radical (cf Définition 2.2.8). Il nous suffit maintenant de prouver que si J est maximal, $\mathcal{Z}(J)$ est un singleton. D'après le Nullstellensatz faible 2.2.12, puisque $J \neq \mathbf{k}[x_1, \cdots, x_n]$, il existe $a \in \mathcal{Z}(J)$. Mais alors puisque $\mathcal{I}$ est décroissante, on a $J = \mathcal{I}(\mathcal{Z}(J)) \subset \mathcal{I}(a)$ ce qui impose, par maximalité de J, l'égalité $J = \mathcal{I}(a)$.

Montrons maintenant la chaîne d'équivalences. Nous avons remarqué en commençant que si X est un singleton de $\mathbf{k}^n$ alors $\mathcal{I}(X)$ est maximal. Réciproquement si $\mathcal{I}(X)$ est maximal, il existe $a \in \mathbf{k}^n$ tel que $\mathcal{I}(X) = \mathcal{I}(a)$, du fait que $\mathcal{I}$ soit la bijection annoncée. On en déduit d'une part que $X = (a)$ et ensuite que $\mathbb{A}(X) = \mathbf{k}$. Enfin, si $\Gamma(X) = \mathbf{k}$, alors $\mathcal{I}(X)$ est évidemment maximal.

(ii) Un point de $\mathbf{k}^n$ donne lieu à l'évaluation en ce point, qui est bien un caractère de $\mathbf{k}[x_1, \cdots, x_n]$. Réciproquement si $\chi : \mathbf{k}[x_1, \cdots, x_n] \to \mathbf{k}$ est un caractère de $\mathbf{k}[x_1, \cdots, x_n]$, il définit un point de $\mathbf{k}^n$ par $(\chi(x_1), \cdots, \chi(x_n))$ et l'évaluation d'un polynôme en ce point est trivialement χ, puisque χ est un morphime de $\mathbf{k}$-algèbres.

(iii) L'application $\mathcal{I}$ est bien définie entre les ensembles algébriques et les racines des idéaux de $\mathbf{k}[x_1, \cdots, x_n]$ par le Nullstellensatz 2.2.11. De plus $\mathcal{I}$ est bijective d'inverse à gauche $\mathcal{Z}$. Il suffit donc de démontrer que si J est un idéal de $\mathbf{k}[x_1, \cdots, x_n]$, $\mathcal{I}(\mathcal{Z}(\sqrt{J})) = \sqrt{J}$. Toujours d'après le Nullstellensatz 2.2.11, $\mathcal{I}(\mathcal{Z}(\sqrt{J})) = \sqrt{\sqrt{J}}$. Mais trivialement, $\sqrt{\sqrt{J}} = \sqrt{J}$.

□

2.3. Composantes irréductibles d'un ensemble algébrique

***2.3.1 Définition* (irréductibilité, connexité).** — Soit $(X, \mathcal{T}_X)$ un espace topologique.

1. On dit que X **irréductible** si et seulement si $X = F_1 \cup F_2$, avec F_1, F_2 fermés de X, implique $F_1 = X$ ou $F_2 = X$. Un espace qui n'est pas irréductible est dit **réductible** ; dans ce cas cet espace s'écrit comme réunion de deux de ses fermés propres.
2. On dit que X **connexe** si et seulement si la réunion disjointe $X = F_1 \sqcup F_2$, avec F_1, F_2 fermés de X, implique $F_1 = X$ ou $F_2 = X$. Un espace qui n'est pas connexe est dit **disconnexe** ; dans ce cas cet espace s'écrit comme réunion disjointe de deux de ses fermés propres.

2.3.2 Remarque. — Un ensemble irréductible est connexe. L'ensemble vide est irréductible (et donc connexe).

2.3.3 Remarque. — Notons que si l'espace topologique X est séparé, les seules parties irréductibles de X sont les points. En effet si X contient au moins deux points $x \neq y$, il existe un ouvert U_x contenant x et un ouvert U_y contenant y tels que $U_x \cap U_y = \emptyset$. Le fermé $X_y = X \setminus U_x$ contient y et non x tandis que le fermé $X_x = X \setminus U_y$ contient alors x et non y ; ils sont tous deux distincts de X. Comme de plus : $X = X_x \cup X_y$, X n'est pas irréductible.

Rappel. Un idéal I d'un anneau A est dit premier ssi A/I est intègre ie $A/I \neq \{0\}$ et $\forall a, b \in A$, $ab = 0$ implique $a = 0$ ou $b = 0$ ssi $I \neq A$ et $\forall \alpha, \beta \in A$, $\alpha\beta \in I$ implique $\alpha \in I$ ou $\beta \in I$. Remarquons qu'un idéal premier est radical.

2.3.4 Exercice. — *Montrer que si l'espace topologique X est irréductible, ses ouverts non vides sont denses. Montrer que si Y est un sous-ensemble d'un espace topologique X, Y est irréductible (pour la topologie induite par celle de X) si et seulement si l'adhérence de Y est irréductible. En déduire que tous les ouverts d'un espace topologique irréductible sont irréductibles.*

2.3.5 Proposition. — *Un ensemble algébrique non vide X de $\mathbf{k}^n$ est irréductible (pour sa topologie de Zariski) si et seulement si $\mathcal{I}(X)$ est un idéal premier si et seulement si $A(X)$ est intègre.*

Démonstration. — Soit $X \in \mathbf{k}^n$ irréductible et $fg \in \mathcal{I}(X)$ tels que $f_{|X} \neq 0$, $g_{|X} \neq 0$. En posant $X_f = \mathcal{Z}(f) \cap X \subset X$ et $X_g = \mathcal{Z}(g) \cap X \subset X$, les inclusions étant strictes on obtient X comme réunion de deux fermés stricts de X, ce qui est contradictoire. En conséquence $f \in \mathcal{I}(X)$ ou $g \in \mathcal{I}(X)$ et ainsi $\mathcal{I}(X)$ est premier. Réciproquement si on dispose de deux fermés X_1, X_2 tels que $X = X_1 \cup X_2$ avec $X_1 \subset X$ et $X_2 \subset X$ des inclusions strictes, comme $\mathcal{I}$ est injective, les inclusions $\mathcal{I}(X) \subset \mathcal{I}(X_1)$ et $\mathcal{I}(X) \subset \mathcal{I}(X_2)$ sont strictes. Soit alors $f \in \mathcal{I}(X_1) \setminus \mathcal{I}(X)$ et $g \in \mathcal{I}(X_2) \setminus \mathcal{I}(X)$. Alors $fg \in \mathcal{I}(X_1) \cap \mathcal{I}(X_2) = \mathcal{I}(X)$, donc $\mathcal{I}(X)$ n'est pas premier. □

2.3.6 Exercice. — *Montrer que si* $\mathbf{k}$ *est infini,* $\mathbf{k}^n$ *est un ensemble algébrique irréductible pour la topologie de Zariski. Qu'en est-il pour la topologie transcendante, lorsque* $\mathbf{k} = \mathbb{C}$ *ou* $\mathbb{R}$ *?*

Le Corollaire 2.2.16 se complète donc de la façon suivante

2.3.7 Corollaire. — *Soit* $\mathbf{k}$ *un corps algébriquement clos.*

(i) La correspondance

$$\mathcal{I} : \{ \text{ points de } \mathbf{k}^n \} \to \{ \text{ idéaux maximaux de } \mathbf{k}[x_1, \cdots, x_n] \ \}$$

est bijective, d'inverse $\mathcal{Z}$*. De plus pour* $(a_1, \cdots, a_n) \in \mathbf{k}^n$, $\mathcal{I}(\{(a_1, \cdots, a_n)\}) = (x_1 - a_1, \cdots, x_n - a_n)$ *et*

$$X \text{ est un singleton de } \mathbf{k}^n \iff \mathcal{I}(X) \text{ est maximal } \iff \Gamma(X) = \mathbf{k}.$$

(ii) La correspondance

$$\mathcal{I} : \{\text{ensembles algébriques irréductibles de } \mathbf{k}^n\} \to \{ \text{ idéaux premiers de } \mathbf{k}[x_1, \cdots, x_n]\}$$

est bijective et d'inverse $\mathcal{Z}$*.*

(iii) La correspondance

$$\mathcal{I} : \{\text{ensembles algébriques de } \mathbf{k}^n\} \to \{\sqrt{J}; J \text{ est un idéal de } \mathbf{k}[x_1, \cdots, x_n]\}$$

est bijective et d'inverse $\mathcal{Z}$*.*

En résumé si $\mathbf{k}$ *est algébriquement clos, l'application* $\mathcal{I}$ *fait bijectivement correspondre les points de* $\mathbf{k}^n$ *et les idéaux maximaux de* $\mathbf{k}[x_1, \cdots, x_n]$*, les ensembles algébriques irréductibles et les idéaux premiers, les ensembles algébriques et les idéaux radicaux.*

Démonstration. — Il suffit de montrer le point (ii) puisque les autres points sont l'objet du Corollaire 2.2.16. Or la Proposition 2.3.5 assure que l'application $\mathcal{I}$ est à valeurs dans l'ensemble des idéaux premiers de $\mathbf{k}[x_1, \cdots, x_n]$ lorsque son ensemble de définition est l'ensemble des ensembles algébriques irréductibles de $\mathbf{k}^n$. D'autre part si J est un idéal premier de $\mathbf{k}[x_1, \cdots, x_n]$, $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ d'après le Nullstellensatz 2.2.11. Mais si J est premier, J est radical, donc en notant $X = \mathcal{Z}(J)$, on a $\mathcal{I}(X) = J$, ce qui prouve la surjectivité de $\mathcal{I}$. □

Une belle conséquence du caractère nœthérien de $\mathbf{k}[x_1, \cdots, x_n]$ est la proposition suivante, qui sera utile pour définir la dimension algébrique d'un ensemble algébrique.

***2.3.8 Théorème* (Composantes irréductibles).** — *Soit X un ensemble algébrique de $\mathbf{k}^n$. Il existe $X_1, \cdots, X_\ell$ des ensembles algébriques de $\mathbf{k}^n$ irréductibles, uniques à permutation près des indices tels que : $X_i \not\subset X_j$, pour $i \neq j$, et $X = X_1 \cup \cdots \cup X_\ell$. On appelle les ensembles algébriques $X_1, \cdots, X_\ell$* **les composantes irréductibles de X.**

Démonstration. — Supposons que l'ensemble $\mathcal{N}$ des ensembles algébriques de $\mathbf{k}^n$ non décomposables (au sens spécifié dans l'énoncé) soit non vide et soit X, un tel ensemble algébrique, dont l'idéal $\mathcal{I}(X)$ soit maximal pour l'inclusion dans l'ensemble $\{\mathcal{I}(Y);\ Y \in \mathcal{N}\}$. Un tel X existe car $\mathbf{k}[x_1, \cdots, x_n]$ est nœthérien. Puisque X n'est pas décomposable, en particulier X n'est pas irréductible, il existe alors Y, Z deux ensembles algébriques de $\mathbf{k}^n$, tels que $X = Y \cup Z$ et $Y, Z \neq X$. L'application $\mathcal{I}$ étant injective, on a les inclusions strictes : $\mathcal{I}(X) \subset \mathcal{I}(Y), \mathcal{I}(X) \subset \mathcal{I}(Z)$. Mais alors, $\mathcal{I}(X)$ étant maximal pour l'inclusion, Y et Z sont nécessairement décomposables, et par conséquent X aussi, ce qui est contradictoire. Enfin si $X = X_1 \cup \cdots \cup X_\ell$ et $X = X'_1 \cup \cdots \cup X'_k$ sont deux écritures de X, on a pour tout $i \in \{1, \cdots, \ell\}$, $X_i = (X_i \cap X'_1) \cup \cdots \cup (X_i \cap X'_k)$. Par irréductibilité de X_i, il existe $j \in \{1, \cdots, k\}$ tel que $X_i = X_i \cap X'_j$, ie $X_i \subset X'_j$. Par symétrie des arguments, on a $X_i = X'_j$ et $\ell = k$. □

2.4. Fonctions régulières d'un ensemble algébrique affine

Soit X un ensemble algébrique affine de $\mathbf{k}^n$. On rappelle que X est appelé une *variété algébrique affine de* $\mathbf{k}^n$ si X est irréductible. Nous allons définir des fonctions $f : X \to \mathbf{k}$, dites *régulières sur* X, qui donnerons lieu à la notion de morphisme, adaptée aux objets de notre étude que sont les ensembles algébriques affines.

2.4.1 Définition. — Soit X un ensemble algébrique affine de $\mathbf{k}^n$ et $x \in X$. Une fonction $f : X \to \mathbf{k}$ est dite **régulière sur X en** x s'il existe un ouvert de Zariski U de X tel que $x \in U \subset X$ et des polynômes $P, Q \in \mathbf{k}[x_1, \cdots, x_n]$ tels que

- Q ne s'annule pas sur U et
- $f = \dfrac{P}{Q}$ sur U.

Noter qu'il revient au même de demander que $f = \dfrac{P}{Q}$ sur l'ouvert fondamental $X \setminus \mathcal{Z}(Q)$ (et f vaut zéro par exemple sur $\mathcal{Z}(Q)$, afin de définir f sur X tout entier) et que Q ne s'annule pas en x, car alors l'existence d'un ouvert U de X contenant x, comme dans la définition, est donné par exemple par $X \setminus \mathcal{Z}(Q)$. On dit que f est **régulière sur** X si f est régulière en chaque point de X. On note $\mathcal{O}_X(X)$ **l'anneau des fonctions régulières sur** X et $\mathcal{O}_X(V)$ l'anneau des fonctions régulières sur un ouvert V de X.

On note, pour $x \in X$, $\mathcal{O}_{X,x}$ (ou $\mathcal{O}_x$ s'il n'y a pas d'ambiguité) **l'anneau des germes de fonctions régulières sur X en x**. Il s'agit de couples (U, f) où U est un ouvert de X contenant x et f une fonction régulière sur U (et non sur X ![2]) où de telles paires (U, f) et (V, g) sont identifiées lorsque $f = g$ sur $U \cap V$. Voir la Remarque 2.4.10 pour une définition équivalente de l'anneau $\mathcal{O}_{X,x}$ en tant qu'éléments du corps des fractions de $A(X)$ ne s'annulant pas en x.

2.4.2 Remarque. — On peut évaluer un germe de fonction régulière en x en le point x, l'évaluation étant compatible avec la relation d'équivalence définissant les germes en x. Ceci fournit un morphisme surjectif $\mathcal{O}_{X,x} \to \mathbf{k}$.

2.4.3 Exercice. — *Soit la fonction f définie sur $\mathbb{A}^1_{\mathbf{k}} \setminus \{0\}$ par $f(x) = 1/x$ et $f(0) = 0$. Cette fonction est-elle régulière en des points de $\mathbb{A}^1_{\mathbf{k}}$? Sur $\mathbb{A}^1_{\mathbf{k}}$ tout entier (cf Remarque 2.4.5) ? Définit-elle un germe de fonction régulière sur $\mathbb{A}^1_{\mathbf{k}}$ et en quels points ?*

2.4.4 Proposition. — *Soit X un ensemble algébrique de $\mathbf{k}^n$.*

(i) Une fonction f, régulière sur X, est continue (pour la topologie de Zariski de X et de $\mathbf{k}$). Une application $\varphi : X \to \mathbf{k}^m$ dont les composantes sont des fonctions régulières sur X est continue (pour la topologie de Zariski de X et de $\mathbf{k}^m$).

(ii) Si deux fonctions régulières f et g sur X coïncident sur un ouvert non vide de X et que X est irréductible, alors f et g coïncident sur X tout entier.

(iii) Soit $x \in X$. L'anneau $\mathcal{O}_{X,x}$ est un anneau local, d'idéal maximal $\mathfrak{m}_{X,x}$, l'ensemble des germes de fonctions régulières en x qui s'annulent en x. De plus $\mathcal{O}_{X,x}/\mathfrak{m}_{X,x} = \mathbf{k}$, ie que le corps résiduel de $\mathcal{O}_{X,x}$ est $\mathbf{k}$. Nous verrons, cf Remarque 2.4.10, que $\mathcal{O}_{X,x}$ est isomorphe à $A(X)_{\mathcal{I}(x)}$ (X est ici supposé irréductible) où $\mathcal{I}(x)$ est l'idéal maximal de $A(X)$ attaché au point x.

2.4.5 Remarque. — La fonction f de l'Exercice 2.4.3 et la fonction g définie sur $\mathbb{A}^1_{\mathbf{k}} \setminus \{0\}$ par $g(x) = 1/x$ et $g(0) = 1$ coïncident sur $\mathbb{A}^1_{\mathbf{k}} \setminus \{0\}$ mais non sur $\mathbb{A}^1_{\mathbf{k}}$. En vue de la Proposition 2.4.4 (ii), l'une de ces fonctions n'est pas régulière.

D'autre part la fonction g n'est pas continue sur $\mathbb{A}^1_{\mathbf{k}}$ puisque $xg = 1$ sur $\mathbb{A}^1_{\mathbf{k}} \setminus \{0\}$ et toujours d'après la Proposition 2.4.4 (ii), xg serait la fonction constante égale à 1 sur l'irréductible $\mathbb{A}^1_{\mathbf{k}}$, ce qui n'est manifestement pas le cas, puisque x s'annule en 0.

Démonstration. — (i) Les fermés de Zariski de $\mathbf{k}$, outre $\mathbf{k}$ lui-même qui peut être infini, sont les parties finies de $\mathbf{k}$. Il nous suffit donc de prouver que si $y \in \mathbf{k}$, $f^{-1}(y)$ est un fermé de X. Il suffit encore de prouver que $f^{-1}(y) \cap U$ est un fermé, pour une collection d'ouverts U recouvrant X, car alors $X \setminus f^{-1}(y) = \cup_U (U \setminus f^{-1}(y))$. Or quel que soit $x \in X$ existe un ouvert U tel que, sur U, f coïncide avec une fraction rationnelle P/Q. Il s'ensuit que $f^{-1}(y) \cap U =$

[2] L'introduction des germes en x est ici essentielle, contrairement à la définition des fonctions régulières sur X qui sont globalement définies sur X en tant que fonctions, ceci en vue de la Proposition 2.4.4 (*iii*) qui montre que l'anneau $\mathcal{O}_{X,x}$ est local.

$\{z \in U; P(z) - yQ(z) = 0\}$, qui est un fermé de U. Enfin de tels voisinages U recouvrent bien X.

Maintenant si φ a ses composantes $\varphi_1, \cdots, \varphi_m$ régulières sur X, comme $\varphi = \sum_{i=1}^m \pi_i \circ \varphi_i$, où $\pi_i(x) = (0, \cdots, 0, x, 0, \cdots, 0)$ est l'insertion de $\mathbf{k}$ dans la $i$éme composante de $\mathbf{k}^m$, la continuité des φ_i implique celle de φ.

(ii) Puisque f et g sont continues sur X, l'ensemble des points $x \in X$ tels que $f(x) = g(x)$ est un fermé de X, qui contient par hypothèse un ouvert non vide U, celui-ci étant dense puisque X est irréductible, par l'Exercice 2.3.4. Le fermé $\{x \in X; f(x) = g(x)\}$ est donc égal à X.

(iii) D'après la Remarque 1.3.13 il nous suffit de montrer que les germes en x de fonctions régulières non inversibles sont les germes de fonctions régulières en x qui s'annulent en x et qu'ils forment un idéal de $\mathcal{O}_{X,x}(X)$. Si f est un germe de fonction régulière en x, il existe un ouvert U de X contenant x et des polynômes P, Q tels que $f = P/Q$ sur U. Cette fonction est alors inversible dans l'anneau des germes de fonctions régulières en x ssi $P(x) \neq 0$, et dans ce cas l'inverse est donné par $g = Q/P$ sur l'ouvert $V = X \cap \{P \neq 0\}$, puisque sur $U \cap V$, qui est un ouvert contenant x, on a bien $fg = 1$. Il est enfin trivial de remarquer que l'ensemble des germes en x de fonctions régulières non inversibles forme un idéal de $\mathcal{O}_{X,x}$, noyau du morphisme surjectif $\mathcal{O}_{X,x} \to \mathbf{k}$ (cf Remarque 2.4.2) qui évalue les germes en x. Le corps résiduel de $\mathcal{O}_{X,x}$ est par conséquent bien (isomorphe à) $\mathbf{k}$.

□

2.4.6 Remarque. — Une fonction régulière sur un ensemble algébrique X est localement définie comme une fraction rationnelle de $\mathbf{k}(x_1, \cdots, x_n)$, localement signifiant que pour tout $x \in X$ existe un ouvert de Zariski U sur lequel f est une fraction rationnelle. Mais en général f n'est pas la restriction d'une fraction rationnelle de $\mathbf{k}(x_1, \cdots, x_n)$ à X tout entier. Par exemple si Y est la variété

$$Y = \{(w, x, y, z) \in \mathbb{C}^4; P(w, x, y, z) := wy - zx = 0\},$$

définissons la quasi-variété X comme étant $Y \cap \{(w, x, y, z) \in \mathbb{C}^4; x \neq 0 \vee y \neq 0\}$ et soit $f : X \to \mathbb{C}$ la fonction régulière sur X définie de la façon suivante : sur l'ouvert $U_x := X \setminus \{(w, x, y, z) \in \mathbb{C}^4; x = 0\}$, on pose $f(w, x, y, z) = w/x$ et sur $U_y := X \setminus \{(w, x, y, z) \in \mathbb{C}^4; y = 0\}$, on pose $f(w, x, y, z) = z/y$. La fonction f est bien définie puisque sur $U_x \cap U_y \cap X$, on a $w/x = z/y$. Cependant f n'est pas la restriction d'une fraction rationnelle de $\mathbf{k}(x_1, \cdots, x_n)$ à X tout entier.

En effet si f coïncidait avec une fraction rationnelle R/S sur X tout entier, S n'aurait pas de zéro sur X de sorte que l'idéal engendré par S et P n'aurait pas de zéro dans X, mais au mieux dans $Y \setminus X$. Soit $\mathcal{Z}(\mathcal{I}(S, P)) \subset \mathcal{Z}(\mathcal{I}(x, y))$ et donc d'après la décroissance de $\mathcal{I}$ (Proposition 2.2.6), $\mathcal{I}(\mathcal{Z}(\mathcal{I}(x, y))) \subset \mathcal{I}(\mathcal{Z}(\mathcal{I}(S, P)))$ et d'après le Nullstellensatz (Théorème 2.2.11) : $x \in \mathcal{I}(\mathcal{Z}(\mathcal{I}(x, y))) \subset \sqrt{\mathcal{I}(S, P)}$. On en déduirait l'existence d'un entier r et de polynômes A et B tels que $x^r = AP + BS$, soit sur Y, $x^r = BS$. Pour que S n'ait pas de zéro sur X (qui contient des points où $x = 0$), il faut que x^r divise B et donc que $R/S = RB/x^r$ soit un polynôme

sur X. Dans ces conditions f serait bornée sur X. Or sur U_x, le long des points $(1, 1/n, 1/n, 1), n \in \mathbb{N}^*$, f n'est pas bornée puisqu'égale à $w/x = n$.

2.4.7 Proposition. — *Soient* $\mathbf{k}$ *un corps algébriquement clos,* X *un ensemble algébrique de* $\mathbf{k}^n$ *et* $x \in X$*. L'anneau local* $\mathcal{O}_{X,x}$ *est réduit et ses idéaux premiers sont en bijection avec les composantes irréductibles de* X *contenant* x*. En particulier* $\mathcal{O}_{X,x}$ *est intègre si et seulement si* x *n'appartient qu'à une seule composante irréductible de* X*.*

Démonstration. — Le fait que $\mathcal{O}_{X,x}$ soit réduit découle du fait que $\mathcal{O}(U)$ est lui-même réduit, quel que soit l'ouvert U de X. Les idéaux premiers minimaux de $A(X)_{\mathcal{I}(x)}$ sont en bijection avec les idéaux premiers minimaux de $A(X)$ contenant $\mathcal{I}(x)$, c'est-à-dire avec les composantes irréductibles de X contenant x, d'après le Corollaire 2.3.7. Supposons maintenant que $\mathcal{O}_{X,x}$ soit intègre, alors $\mathcal{O}_{X,x}$ ne contient qu'un seul idéal premier minimal qui est (0), donc d'après ce qui précède, par x ne passe qu'une seule composante irréductible de X. Réciproquement, supposons que par x ne passe qu'une seule composante irréductible, alors, toujours par ce qui précède, $\mathcal{O}_{X,x}$ ne contient qu'un seul idéal premier minimal $\mathfrak{p}$. Du fait que le radical d'un idéal est l'intersection des idéaux premiers qui le contiennent (cf Proposition 2.2.9), on a $\sqrt{(0)} = \mathfrak{p}$. Mais puisque $\mathcal{O}_{X,x}$ est réduit, $\mathfrak{p} = (0)$. On en conclut que $\mathcal{O}_{X,x}$ est intègre puisque (0) est premier.

□

On peut décrire précisément $\mathcal{O}_X(X)$, lorsque X est une variété ou un ouvert du type $X \setminus \{P = 0\}$, c'est l'objet de la Remarque 2.4.10 qui suit. Mais avant d'en arriver à cette remarque, nous allons introduire le corps des fonctions d'une variété algébrique affine.

2.4.8 Définition. — Soit X une variété affine de $\mathbf{k}^n$, l'idéal $\mathcal{I}(X)$ est alors premier et l'algèbre des fonctions polynomiales $A(X)$ est un anneau intègre dont on peut considérer le **corps des fractions de** X, noté $\mathbf{k}(X)$, qui est défini comme l'ensemble des paires (P, Q) de $A(X) \times A(X)$, avec $Q \neq 0$, modulo la relation d'équivalence

$$(P, Q) \sim (R, S) \Longleftrightarrow PS - QR = 0.$$

Il s'agit du localisé de $A(X)$ par la partie multiplicative $A(X) \setminus \{0\}$. On note alors la classe de (P, Q) par P/Q et l'addition et le produit sont définis par

$$P/Q + F/G = (PG + FQ)/QG \text{ et } (P/Q) \cdot (F/G) = PF/QG$$

Il est clair que $\mathbf{k}(X)$ muni de ces deux lois est un corps.

De même que les éléments de $A(X)$ sont souvent considérés comme des restrictions de fonctions (polynomiales) sur X il est loisible de considérer un élément P/Q de $\mathbf{k}(X)$ comme une fonction (rationnelle) restreinte à X. Pour cela il faut exclure de X les points en lesquels Q s'annule. De sorte qu'étant considérés comme des fonctions sur X, les éléments de $\mathbf{k}(X)$ sont définis comme les triplets (U, P, Q) où U est un ouvert non vide de X sur lequel Q ne s'annule pas, modulo la relation d'équivalence

$$(U, P, Q) \sim (V, R, S) \Longleftrightarrow P/S - Q/R = 0 \text{ sur } U \cap V.$$

On note encore $\mathbf{k}(X)$ le corps des fractions de X lorsque les éléments de $\mathbf{k}(X)$ sont vus comme des fonctions rationnelles sur des ouverts de X. La justification de cet abus de notation est donné dans la Remarque 2.4.9 qui suit.

2.4.9 Remarque. — Dans la Définition 2.4.8 sont en réalité définis deux corps, l'un est le corps des fractions de l'anneau intègre $A(X)$, l'autre le corps des fractions rationnelles restreintes à des ouverts non vides de X. On ne distingue pas ces deux corps, car il sont isomorphes ; l'isomorphisme naturel étant fourni par

$$(P, Q) \mapsto (X \setminus \{Q = 0\}, P, Q), \text{ pour } Q \neq 0 \text{ dans } A(X).$$

On vérifiera en exercice que cette flèche définit bien un morphisme de corps, dont le morphisme inverse est

$$(U, P, Q) \mapsto (P, Q).$$

car si deux fractions rationnelles (U, P, Q) et (V, R, S) coïncident sur l'ouvert $U \cap V$, on a $PS - QR = 0$ sur $U \cap V$ et par continuité des polynômes pour la topologie de Zariski (Proposition 2.4.4) et du fait que $U \cap V$ étant non vide est dense dans l'irréductible X (Exercice 2.3.4), cette égalité est vraie sur X tout entier, de sorte que $(P, Q) = (R, S)$.

De la même façon le corps $\mathbf{k}(X)$ des fractions de X s'identifie à l'ensemble des paires (U, f) où U est un ouvert de Zariski non vide de X et f une fonction régulière sur U. Ainsi f n'est pas *a priori* une fraction rationnelle sur U tout entier mais pour tout $x \in U$ existe un ouvert U' contenant x telle que f coïncide avec une fraction rationnelle P/Q sur $U \cap U'$. Là encore on définit le même corps, un isomorphisme naturel étant fourni par $(U, f) \mapsto (P, Q)$, pour les mêmes raisons que ci-dessus.

***2.4.10 Remarque* (Définition équivalente de $\mathcal{O}_{X,x}$)**. — Si X est irréductible, une définition équivalente de $\mathcal{O}_{X,x}$, l'anneau des germes de fonctions régulières en x, est

$$\mathcal{O}_{X,x} := \{P/Q \in \mathbf{k}(X); Q(x) \neq 0\}^{(3)}.$$

Remarquons que cette caractérisation de $\mathcal{O}_{X,x}$ montre que $\mathcal{O}_{X,x}$ est aussi le localisé de $A(X)$ (anneau intègre lorsque X est irréductible) par l'idéal maximal de $\mathbf{k}[x_1, \cdots, x_n]$ correspondant au point x.

Montrons cette égalité. Si l'on dispose d'un couple (P, Q) où $Q(x) \neq 0$, $P/Q \in \mathbf{k}(X)$ induit une fonction régulière sur $U = X \setminus \mathcal{Z}(Q) \ni x$. Il suffit alors de s'assurer de la compatibilité des relations d'équivalence définissant $\mathbf{k}(X)$ et $\mathcal{O}_{X,x}$. Ainsi si (P', Q') est un autre représentant de $P/Q \in \mathbf{k}(X)$, du fait de $P'Q - PQ' = 0$, sur l'ouvert non vide $X \setminus (\mathcal{Z}(Q) \cup \mathcal{Z}(Q'))$ (contenant x), on a $P/Q = P'/Q'$. Ce qui définit bien un unique germe de fonction régulière en x.

[3] L'égalité $\mathcal{O}_{X,x} := \{P/Q \in \mathbf{k}(X); Q(x) \neq 0\}$, qui permet de voir les germes des fonctions régulières en x comme des fractions rationnelles sans pôle en x, est due au caractère local de l'anneau $\mathcal{O}_{X,x}$. Cette identification n'a en revanche pas lieu pour $\mathcal{O}_X(X)$. Être une fonction régulière sur X tout entier est une propriété plus contraignante qu'être un germe de fonction régulière ; les éléments de $\mathcal{O}_X(X)$ ne s'identifient pas aux fractions rationnelles, lorsque $\mathbf{k}$ est algébriquement clos, mais aux fonctions polynômes sur X, d'après la Proposition 2.4.11 (ii).

Réciproquement si $(U, f) \in \mathcal{O}_{X,x}$, soient U un voisinage ouvert de x, et f régulière sur U, qui représentent la classe $(U, f) \in \mathcal{O}_{X,x}$. En particulier f est régulière en x et donc existe V un voisinage ouvert de x dans U, deux polynômes $P, Q \in \mathbf{k}[x_1, \ldots, x_n]$, Q ne s'annulant pas sur V, de sorte que $f = P/Q$ sur V. Ceci définit bien $P/Q \in \mathbf{k}(X)$ avec $Q(x) \neq 0$, à condition que l'on prouve l'indépendance relativement aux choix du représentant de la classe $(U, f) \in \mathcal{O}_{X,x}$. Or si $(U, f) = (U', f')$ dans $\mathcal{O}_{X,x}$, $f' = P'/Q'$ sur un ouvert V' de U' contenant x sur lequel Q' ne s'annule pas et $f = f'$ sur $V \cap V'$, c'est-à-dire que $PQ' - P'Q = 0$ sur $V \cap V'$, mais X étant irréductible, $V \cap V'$ qui est non vide est dense dans X par l'Exercice 2.3.4, et par la Proposition 2.4.4 (i), $PQ' - P'Q$ étant continue sur X. On en conclut que $PQ' - P'Q = 0$ sur X, soit que $P/Q = P'/Q'$ dans $\mathbf{k}(X)$.

Enfin le fait que les deux flèches ci-dessus définies se composent en l'identité est encore un argument de densité.

2.4.11 Proposition. — *Soit* $\mathbf{k}$ *un corps algébriquement clos et* X *un ensemble algébrique affine de* $\mathbf{k}^n$.

(i) Soient $Q \in \mathbf{k}[x_1, \ldots, x_n]$ *et l'ouvert* $X_Q = X \setminus \{Q = 0\}$ *de* X. *Alors*

$$\mathcal{O}_X(X_Q) = \{f : X_Q \to \mathbf{k}; \exists P \in \mathbf{k}[x_1, \ldots, x_n], \exists r \in \mathbb{N}, f = P/Q^r\} = A(X)_Q{}^{(4)}.$$

(ii) En particulier

$$\Gamma(X) := \mathcal{O}_X(X) = A(X).$$

Démonstration. — (i) Clairement $\mathcal{O}_X(X_Q) \supset \{f : X_Q \to \mathbf{k}; \exists P \in \mathbf{k}[x_1, \ldots, x_n] \exists r \in \mathbb{N}, f = P/Q^r\}$. Montrons alors l'inclusion inverse. Soit $f \in \mathcal{O}_X(X_Q)$ et considérons alors les deux idéaux

$$J = \{S \in A(X); Sf \in A(X)\} \text{ et } J' = \{S \in \mathbf{k}[x_1, \ldots, x_n]; S_{|X} \in J\}.$$

Notons que pour tout $x \in X_Q$, il existe un ouvert U de X contenant x tel que sur $U \cap X_Q$, $f = R/S$ et S ne s'annule pas sur U. En particulier $S \in J'$ et S ne s'annule pas en x. Il s'ensuit les zéros communs des éléments de J' et de $\mathcal{I}(X)$ sont dans $X \setminus X_Q$. En particulier

$$\mathcal{Z}(J' + \mathcal{I}(X)) \subset \mathcal{Z}(Q).$$

Par décroissance de $\mathcal{I}$ (Proposition 2.2.6) et d'après le Nullstellensatz (Théorème 2.2.11), on obtient

$$Q \in \mathcal{I}(\mathcal{Z}(Q)) \subset \mathcal{I}(\mathcal{Z}(J' + \mathcal{I}(X))) = \sqrt{J' + \mathcal{I}(X)}.$$

Il existe donc $r \in \mathbb{N}$ tel que $Q^r \in \mathcal{I}(X) + J'$, de sorte que $Q^r_{|X} \in J$, ie $Q^r_{|X} f \in A(X)$.

(ii) Il suffit de faire $Q = 1$ dans (i).

□

(4) $A(X)_Q$ désigne la localisation de $A(X)$ en Q, ie la localisation de $A(X)$ par la partie multiplicative $\{Q^r; r \in \mathbb{N}\}$, cf Remarque 1.3.15 (5)

2.4.12 Exercice. — *Que dire de $\mathcal{O}_X(X)$ lorsque $\mathbf{k} = \mathbb{R}$ (reprendre les arguments de la preuve de la Proposition 2.4.11 et utiliser le Nullstellensatz réel 2.2.11 (ii) pour montrer que $\mathcal{O}_X(X) = \{f; \exists \ell \in \mathbb{N}, P, R, Q_1, \cdots, Q_\ell \in \mathbf{k}[x_1, \cdots, x_n], \mathcal{Z}(R) \cap X = \emptyset \; ; f = \frac{P}{R+\sum_{i=1}^{\ell} Q_i^2}|_X\}$) ?*

2.4.13 Remarque. — Confronter la fonction régulière f sur la quasi-variété X de la Remarque 2.4.6, qui ne s'exprime pas comme la restriction d'une fraction rationnelle sur X et la Proposition 2.4.11 (i).

2.4.14 Exercice. — *Trouver sur l'ensemble algébrique $A^1(\mathbb{R})$ une fonction régulière $f \in \mathcal{O}_{\mathbb{A}^1(\mathbb{R})}(\mathbb{A}^1(\mathbb{R}))$ qui ne soit pas un polynôme (confronter cet exemple à la Proposition 2.4.11 (ii)).*

2.4.15 Exercice. — *On se place sur le corps $\mathbf{k} = \mathbb{C}$ et on considére l'ouvert de Zariski de $\mathbb{C}^2$ suivant : $U = \mathbb{C}^2 \setminus \{0\}$. L'objet de cet exercice est de déterminer $\mathcal{O}_{\mathbb{C}^2}(U)$ en montrant que $\mathcal{O}_{\mathbb{C}^2}(U) = \mathbf{k}[x, y]$.*

1. *Montrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[x, y]$ tel que $U = \mathbb{C}^2 \setminus \{P = 0\}$ et qu'en conséquence on ne peut pas a priori appliquer la Proposition 2.4.11 (Ind. On pourra se souvenir de la preuve du Corollaire 2.2.16) .*
2. *Soit $f : U \to \mathbf{k}$ une fonction régulière sur U. On rappelle que par définition, pour tout $x \in U$, il existe $P, Q \in \mathbf{k}[x_1, \cdots, x_n]$ tels que $f = \dfrac{P}{Q}$ sur $U \setminus \mathcal{Z}(Q)$ et Q ne s'annule pas en x (cf. Définition 2.4.1). On pose*

$$J = \{S \in \mathbf{k}[x, y]; S \cdot f \in \mathbf{k}[x, y]\}.$$

   Montrer que J est un idéal de $\mathbf{k}[x, y]$ et que $\mathcal{Z}(J) \subset \{(0, 0)\}$.
3. *Montrer que $\sqrt{J} = (x, y)$ ou que $J = \mathbf{k}[x, y]$. Déduire de $\sqrt{J} = (x, y)$ que $f = A/x^r$ sur $\mathbb{C}^2 \setminus \mathcal{Z}(x)$, pour $A \in \mathbf{k}[x, y]$ et $r \in \mathbb{N}$ et $f = B/y^s$ sur $\mathbb{C}^2 \setminus \mathcal{Z}(y)$, pour $B \in \mathbf{k}[x, y]$ et $s \in \mathbb{N}$.*
4. *En déduire d'une part que f est bornée au voisinage de $(1, 0)$ et d'autre part que f ne l'est pas. Conclure.*

2.5. Espaces annelés et morphismes d'espaces annelés

2.5.1 Définition. — Un **préfaisceau $\mathcal{F}$ d'anneaux sur un espace topologique** X consiste en la donnée :

1. Pour tout ouvert U de X, d'un anneau $\mathcal{F}(U)$,
2. Pour tout couple $U \subset V$ d'ouverts de X, d'un morphisme d'anneaux $\rho_{V,U} : \mathcal{F}(V) \to \mathcal{F}(U)$, appelé **morphisme de restriction de V à U**, tel que
   i. $\mathcal{F}(\emptyset) = 0$,
   ii. Pour tout ouvert U de X, $\rho_{U,U} = Id_{\mathcal{F}(U)}$,
   iii. Pour tout triplet $U \subset V \subset W$ d'ouverts de X, $\rho_{V,U} \circ \rho_{W,V} = \rho_{W,U}$.

Les éléments de l'anneau $\mathcal{F}(U)$ sont appelés **les sections de $\mathcal{F}$ sur** U et on note $\rho_{V,U}(f) := f_{|U}$. Les éléments de $\mathcal{F}(X)$ sont appelés les **sections globales de** $\mathcal{F}$. On les note parfois $\Gamma(X)$[5].

Un **faisceau d'anneaux** est un préfaisceau d'anneaux qui satisfait la propriété de recollement suivante :

3. Pour tout ouvert U de X, pour tout recouvrement $U = \bigcup_{i\in I} U_i$ de U par des ouverts U_i de X et pour toute famille $(f_i)_{i\in I}$ de sections $f_i \in \mathcal{F}(U_i)$, telle que $f_{i|U_i\cap U_j} = f_{j|U_i\cap U_j}$, $i, j \in I$, il existe une unique section $f \in \mathcal{F}(U)$ telle que $f_{|U_i} = f_i$, $i \in I$.

Si X est un espace topologique et $\mathcal{F}$ un faisceau d'anneaux sur X, le couple $(X, \mathcal{F})$ est appelé un **espace annelé de faisceau structural** $\mathcal{F}$.

Si $(X, \mathcal{F})$ est un espace annelé et U un ouvert de X, on peut définir **la restriction $\mathcal{F}_{|U}$ de $\mathcal{F}$ à** U par $\mathcal{F}_{|U}(V) = \mathcal{F}(V)$, pour tout ouvert $V \subset U$.

2.5.2 Remarque. — On peut définir un faisceau non pas seulement d'anneaux, mais d'objets d'une catégorie donnée, les restrictions étant alors des flèches de cette catégorie. Pour ce qui nous concerne, nous nous concentrerons sur les faisceaux d'anneaux, en vue de la proposition qui suit.

2.5.3 Proposition. — *Soit X un ensemble algébrique affine de $\mathbf{k}^n$. Les anneaux $\mathcal{O}_X(U)$ des fonctions régulières sur les ouverts U de X, ainsi que les restrictions de ces fonctions régulières aux ouverts V contenus dans les ouverts U forment un faisceau d'anneaux sur X, noté $\mathcal{O}_X$ et appelé* **le faisceaux structural de l'ensemble algébrique** *X. Les sections globales $\mathcal{O}_X(X)$ de $\mathcal{O}_X$ sont les éléments de l'algèbre affine $A(X)$ de X lorsque $\mathbf{k}$ est algébriquement clos (cf Proposition 2.4.11 (ii))* [6].

Démonstration. — Il suffit de vérifier la propriété de recollement 3 de la Définition 2.5.1, les propriétés 1 et 2 étant triviales à vérifier. Or le recollement ensembliste définit bien une fonction f et celle-ci est alors une fonction régulière sur U car (avec les notations de la Définition 2.5.1) si $x \in U$, il existe $i \in I$ tel que $x \in U_i$ et par définition de f, $f_{|U_i} = f_i$ est une fonction régulière sur U_i, ce qui impose que $f = P_i/Q_i$ sur l'ouvert $U_i \setminus \mathcal{Z}(Q_i)$ et $Q_i(x) \neq 0$, pour $P_i, Q_i \in \mathbf{k}[x_1, \cdots, x_n]$. □

2.5.4 Exemple. — Un préfaisceau n'est un faisceau que lorsque la définition des sections sur les ouverts U a un caractère local. À titre d'exemple classique d'un préfaisceau qui n'est pas un faisceau, considérons sur un espace topologique X, non connexe, et U, V deux ouverts non vides de X tels que $U \cap V = \emptyset$ et considérons sur les ouverts W de X les fonctions constantes à valeurs dans $\mathbb{R}$, que l'on note $\mathcal{F}(W)$. Alors $\mathcal{F}$ est un préfaisceau sur X mais n'est pas un faisceau car la fonction qui vaut 0 sur U et 1 sur V n'est pas constante sur l'ouvert $W = U \cup V$, tandis que ses restrictions à U et V sont bien des sections de $\mathcal{F}$ sur U et V. La notion de fonction

[5] La notation Γ a été introduite dans la Proposition 2.4.11. On va en effet remarquer que $\mathcal{O}_X(X)$ est la section globale d'un faisceau sur X.

[6] Ceci justifie, comme annoncé, la notation $\Gamma(X)$, lorsque $\mathbf{k}$ est algébriquement clos, à la fois pour l'algèbre affine de X et pour les sections globales du faisceau $(X, \mathcal{O}_X)$.

constante sur un ouvert n'est pas une notion locale. En revanche si l'on considère pour sections sur les ouverts W de X les fonctions localement constantes, on obtient un faisceau sur X, appelé **le faisceau constant sur** X.

2.5.5 Remarque. — La définition 2.4.1 des fonctions régulières sur un ouvert de Zariski U est un notion locale qui permet sans effort de conférer à $\mathcal{O}_X$ la propriété de recollement des faisceaux. Dans le cas particulier où $\mathbf{k} = \mathbb{R}$, on aurait pu définir $\mathcal{O}_X(U)$ par

$$\mathcal{O}_X(U) := \{P/Q; P, Q \in A(X), Q^{-1}(0) \cap U = \emptyset\}.$$

Cette définition semble moins bien se prêter à la propriété de recollement des faisceaux, néanmoins le rôle des carrées dans $\mathbb{R}$ permet de montrer la Proposition suivante.

2.5.6 Proposition. — *Soit X un ensemble algébrique affine de $\mathbb{R}^n$. Avec la définition de la Remarque 2.5.5 du préfaisceau $\mathcal{O}_X$, $\mathcal{O}_X$ est un faisceau, qui est le même que celui définit en toute généralité dans la définition 2.4.1.*

Démonstration. — Il suffit de considérer un recouvrement fini $U = \cup_{i=1}^{\ell} U_i$ d'un ouvert de Zariski U de l'ensemble algébrique affine X de $\mathbb{R}^n$ par des ouverts de Zariski U_i, car un tel ouvert U est quasi-compact, par la Remarque 2.1.14. Ensuite si pour $i = 1, \cdots, \ell$, $f_i = P_i/Q_i$ est une fraction rationnelle sans pôle sur U_i, et définit une famille de sections sur U_i telle que $f_i = f_j$ sur $U_i \cap U_j$, on peut considérer sans ambigüité la fonction f sur U induite par les f_i. Montrons alors que cette fonction est une fraction rationnelle P/Q sur U sans pôle sur U. Le fermé $F_i = X \setminus U_i$ est donné par un seul polynôme $S_i \in A(X)$ et comme $\cap_i F_i = F := X \setminus U$, le polynôme $Q = \sum_{i=1}^{\ell} S_i^2 Q_i^2$ ne s'annule pas sur U. Enfin, on a $f = \frac{\sum_{i=1}^{\ell} S_i^2 P_i Q_i}{Q}$. En effet, si $\mathcal{A}$ est l'ensemble des indices $i \in \{1, \cdots, \ell\}$ tels que $a \in U_i$ et si $j \in \mathcal{A}$, en écrivant pour tout $i \in \mathcal{A}$, $P_i(a) = P_j(a)Q_i(a)/Q_j(a)$, on a

$$f(a) = \frac{\sum_{i=1}^{\ell} S_i^2(a) P_i(a) Q_i(a)}{Q(a)} = \frac{\sum_{i \in \mathcal{A}} \frac{P_j(a)}{Q_j(a)} S_i^2(a) Q_i^2(a)}{Q^2(a)} = \frac{P_j(a)}{Q_j(a)} = f(a).$$

Pour montrer que les faisceaux définis en 2.4.1 et dans la Remarque 2.5.5 sont les mêmes il suffit de montrer qu'une section $f \in \mathcal{O}_X(U)$ du faisceau structural de X (au sens de 2.4.1), au-dessus d'un ouvert U de X est une section au-dessus de U du faisceau défini dans la remarque 2.5.5. L'inclusion inverse étant triviale. Or si $f \in \mathcal{O}_X(U)$, on peut considérer un recouvrement fini $(U_i)_{i \in \{1, \cdots, \ell\}}$ de U tel que sur chaque U_i, f est donné par une fraction rationnelle P_i/Q_i, c'est-à-dire par des sections au-dessus de U_i du faisceau défini dans la Remarque 2.5.5. L'application f étant le recollement des P_i/Q_i, il s'agit bien par ce qui précède d'une fraction rationnelle sur U tout entier. □

2.5.7 Définition. — Soit $\mathcal{F}$ un (pré-)faisceau d'anneaux sur un espace topologique X et $x \in X$. On définit l'ensemble des paires $(U, f) \in \mathcal{T}_X \times \mathcal{F}(U)$ où $x \in U$,

modulo la relation d'équivalence

$$(U, f) \sim (V, g) \Longleftrightarrow \exists W \in \mathcal{T}_X, x \in W \text{ tel que } f_{|W} = g_{|W}.$$

Ce quotient est un anneau, noté $\mathcal{F}_x$ et appelé **la fibre en x du faisceau $\mathcal{F}$**. Lorsque cette fibre est un anneau local, on dit que $(X, \mathcal{F})$ est un **espace géométrique** ou **espace localement annelé**.

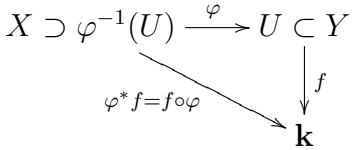
2.5.8 Remarque. — Soit X un ensemble algébrique affine, $x \in X$ et $\mathcal{O}_X$ son faisceau structural. Par définition des germes de fonctions régulières sur X en x (cf Définition 2.4.1) la fibre en $x \in X$ du faisceau structural $\mathcal{O}_X$ est l'anneau des germes en x des fonctions régulières sur X. Ceci justifie les notations $\mathcal{O}_X$ et $\mathcal{O}_{X,x}$ pour le faisceau structural de X et pour la fibre de ce faisceau en x. D'autre part d'après la Proposition 2.4.4 (*iii*), on a

2.5.9 Proposition. — *Le faisceau structural $(X, \mathcal{O}_X)$ d'un est un espace géométrique.*

2.5.10 Définition. — Soient $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$ deux espaces annelés dont les sections sont des fonctions à valeurs dans $\mathbf{k}$ et $\varphi : X \to Y$ une application.

(i) On dit que φ est un **morphisme d'espaces annelés** lorsque

1. φ est continue,
2. pour tout ouvert U de Y et toute section $f \in \mathcal{O}_Y(U)$, la composition
$$f \circ \varphi : \varphi^{-1}(U) \to \mathbf{k}$$
est une section de $\mathcal{O}_X$ sur l'ouvert $\varphi^{-1}(U)$.



On note $\varphi^* f$ la composée $f \circ \varphi$, on dit qu'il s'agit du **pullback de f par φ**. En d'autres termes, φ est un morphisme entre les espace annelés $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$ lorsque φ est continu et $\forall U$ ouvert de Y, $\varphi^*(\mathcal{O}_Y(U)) \subset \mathcal{O}_X(\varphi^{-1}(U))$. On note $\mathrm{Mor}_{Var}(X, Y)$ l'ensemble des morphismes de l'espace annelé $(X, \mathcal{O}_X)$ dans l'espace annelé $(Y, \mathcal{O}_Y)$.

(ii) On dit que φ est un **isomorphisme d'espaces annelés** si φ est bijective et $\varphi^{-1} : Y \to X$ est un morphisme.

2.5.11 Remarque. — Un morphisme de variétés qui est bijectif n'est pas nécessairement un isomorphisme, voir l'Exercice 2.5.18.

2.5.12 Proposition. — *Soit $\varphi : X \to Y$ une application continue entre deux ensembles algébriques affines X et Y, resp. de $\mathbf{k}^n$ et $\mathbf{k}^m$. On a les équivalences*

(i) φ est un morphisme, ie pour tout ouvert U de Y, $\varphi^*(\mathcal{O}_Y(U)) \subset \mathcal{O}_X(\varphi^{-1}(U))$,
(ii) $\varphi^*(\mathcal{O}_Y(Y)) \subset \mathcal{O}_X(X)$,
(iii) Pour tout $x \in X$, $\varphi^*(\mathcal{O}_{Y,\varphi(x)}) \subset \mathcal{O}_{X,x}$, où φ^* est induit par φ sur $\mathcal{O}_{X,x}$.

Démonstration. — $(i) \Longrightarrow (ii)$ est trivial en posant $U = Y$.

Montrons $(ii) \Longrightarrow (iii)$. Si $f \in \mathcal{O}_{Y,\varphi(x)}$, soit (V, g) un représentant de la classe f, alors V est un ouvert de Y contenant $\varphi(x)$ et g est une fonction régulière sur V. On peut supposer que $g = P/Q$, avec $P, Q \in \mathbb{A}(Y) \subset \mathcal{O}_Y(Y)$ et $Q(\varphi(x)) \neq 0$. Dans ce cas $\varphi^* g = \varphi^* P/\varphi^* Q$ et puisque par hypothèse $\varphi^* P \in \mathcal{O}_X(X)$, $\varphi^* Q \in \mathcal{O}_X(X)$ et $(\varphi^* Q)(x) = Q(\varphi(x)) \neq 0$, $\varphi^* g$ définit bien un germe de fonction régulière en x (en écrivant $\varphi^* P$ et $\varphi^* Q$ comme des fractions rationnelles sur des ouverts contenant x). Il reste à s'assurer que nous avons défini une classe $\varphi^* f$ indépendamment du représentant (V, g) de f dans $\mathcal{O}_{X,x}$, ce qui est direct.

Pour montrer $(iii) \Longrightarrow (i)$ il suffit de remarquer que si U est un ouvert de Y, une fonction régulière sur U est donnée par ses germes en tous les points de U. □

2.5.13 Corollaire. — *Soit $\varphi : X \to Y$ une application entre deux ensembles algébriques affines X et Y, resp. de $\mathbf{k}^n$ et $\mathbf{k}^m$.*

(i) φ est un morphisme si et seulement ses composantes $\varphi_1, \cdots, \varphi_m$ sont dans $\mathcal{O}_X(X)$. De plus ses composantes sont $\varphi^* y_1, \cdots, \varphi^* y_m$, où y_i sont les classes dans $A(Y)$ des indéterminés.

(ii) Si $\mathbf{k}$ est algébriquement clos, φ est un morphisme si et seulement ses composantes $\varphi_1, \cdots, \varphi_m$ sont dans $A(X)$, ie sont des restrictions à X de fonctions polynomiales sur $\mathbf{k}^n$. De plus ses composantes sont $\varphi^* y_1, \cdots, \varphi^* y_m$, où y_i sont les classes dans $A(Y)$ des indéterminés.

(iii) $\varphi^* : \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ est un morphisme de $\mathbf{k}$-algèbres.

Démonstration. — (i) Les composantes de φ sont par définition $\varphi^* y_1, \cdots, \varphi^* y_m$, or d'après la Proposition 2.5.12 si φ est un morphisme, $\varphi_1, \cdots, \varphi_m \in \mathcal{O}_X(X)$. Réciproquement, il est clair que si φ a pour composantes des fonctions régulières, φ est continue par la Proposition 2.4.4 (i) et que pour tout $f \in \mathcal{O}_X(Y)$, $\varphi^* f \in \mathcal{O}_X(X)$.

(ii) Dans le cas où $\mathbf{k}$ est algébriquement clos, $\mathcal{O}_Y(Y) = A(Y)$ et $\mathcal{O}_X(X) = A(X)$.

(iii) Trivial (noter que $\mathcal{O}_Y(Y) = A(Y)$ et $\mathcal{O}_X(X) = A(X)$ si $\mathbf{k}$ est algébriquement clos par la Proposition 2.4.11 (ii)).

□

2.5.14 Remarque. — On peut déterminer, pour $\varphi : X \to Y$ donné, le morphisme $\varphi^* : A(Y) \to A(X)$ de la façon suivante. Soit $P \in A(Y)$. Notons φ_i les composantes de φ ; elles sont données par $\varphi^* y_i$. Alors $\varphi * P = \varphi^* P(y_1, \cdots, y_m) = P(\varphi^* y_1, \cdots, \varphi^* y_m)$, puisque φ^* est un morphisme de k-algèbres. En conclusion $\varphi^* P$ est la classe de $P(\varphi_1, \cdots, \varphi_m)$ dans $A(X)$.

2.5.15 Exercice. — *Soit $P \in \mathbf{k}[x_1, \cdots, x_n]$. Montrer que le graphe X de P est une variété algébrique affine de $\mathbf{k}^{n+1}$, isomorphe à $\mathbf{k}^n$.*

2.5.16 Théorème. — *(i) Associer à X, un ensemble algébrique affine de $\mathbf{k}^n$, la $\mathbf{k}$-algèbre $\mathcal{O}_X(X)$ de la section globale de son faisceau structural $\mathcal{O}_X$ et associer à un morphisme $\varphi : X \to Y$ d'ensembles algébriques affines le morphisme de $\mathbf{k}$-algèbres $\varphi^* : \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ définit un* **foncteur contravariant** *de*

la catégorie des ensembles algébriques affines sur un corps $\mathbf{k}$ *munie des morphismes d'ensembles algébriques affines à la catégorie des* $\mathbf{k}$*-algèbres réduites (ie sans élément nilpotent autre que* 0*) munie des morphismes de* $\mathbf{k}$*-algèbres. On note parfois ce foncteur* Γ *lorsque* $\mathbf{k}$ *est algébriquement clos.*

(ii) Ce foncteur est **pleinement fidèle***, ie qu'il induit une bijection*

$$\mathrm{Mor}_{Var}(X,Y)) \simeq \mathrm{Mor}_{k-alg}(\mathcal{O}_Y(Y),\mathcal{O}_X(X))$$

(iii) En particulier deux ensembles algébriques affines sont isomorphes si et seulement si leurs $\mathbf{k}$*-algèbres de fonctions régulières (leurs algèbres affines dans le cas algébriquement clos) le sont, et les isomorphsmes se correspondent par le foncteur section globale, ie via* $\varphi \longleftrightarrow \varphi^*$*.*

(iv) Si $\mathbf{k}$ *est algébriquement clos, le foncteur* Γ *est une* **équivalence de catégories** *entre la catégorie des ensembles (resp. des variétés) algébriques affines de* $\mathbf{k}^n$ *munie des morphismes d'ensembles algébriques affines de* $\mathbf{k}^n$ *et la catégorie des* $\mathbf{k}$*-algèbres de type fini réduites (resp. intègres), munie des morphismes de* $\mathbf{k}$*-algèbres.*

Démonstration. — (i) Il nous faut démontrer que $(Id_X)^* = Id_{\mathcal{O}_X(X)}$, ce qui est trivial puisque si $f \in \Gamma(X)$, $Id_X^* f = f \circ Id_X = f$. Il nous faut enfin démontrer que pour tous les morphismes $\varphi : X \to Y$, $\psi : Y \to Z$ de variétés algébriques affines, on a $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$. Or si $f \in \mathcal{O}_Z(U)$, pour un ouvert U de Z, $(\psi \circ \varphi)^* f = f \circ \psi \circ \varphi = (\psi^* f) \circ \varphi = \varphi^*(\psi^* f) = (\varphi^* \circ \psi^*) f$.

(ii) Il faut par définition démontrer que pour toutes variétés algébriques affines X et Y, l'application

$$\begin{array}{ccc} \mathrm{Mor}_{Var}(X,Y)) & \to & \mathrm{Mor}_{k-alg}(\mathcal{O}_Y(Y),\mathcal{O}_X(X)) \\ \varphi & \mapsto & \varphi^* \end{array}$$

est une bijection.

(a) Montrons que cette application est injective, ie que le foncteur *section globale* est **fidèle**. Si $\varphi^* = \psi^*$, par le Corollaire 2.5.13 (i), les composantes de φ et ψ sont égales puisqu'elles sont respectivement $\varphi^* y_1, \cdots, \varphi^* y_m$ et $\psi^* y_1, \cdots, \psi^* y_m$.

(b) Montrons que cette application est surjective. Soit un morphisme de k-algèbres $L : \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$. Nécessairement si $L = \varphi^*$ pour un certain morphisme $\varphi : X \to Y$, les composantes de φ sont $L(y_1), \cdots, L(y_m)$, toujours par le Corollaire 2.5.13 (i), où les y_i sont les classes dans $\Gamma(Y)$ des monômes de $\mathbf{k}[y_1, \ldots, y_m]$. Considérons alors le morphisme $\varphi : X \to \mathbf{k}^m$ dont les composantes φ_i sont $L(y_1), \cdots, L(y_m) \in \mathcal{O}_X(X)$. Il s'agit seulement de montrer que $\varphi(X) \subset Y$, ie que $\varphi \in \mathrm{Mor}_{Var}(X,Y)$, car alors on aura automatiquement $\varphi^* = L$, puisque $\varphi^* y_1 = \varphi_i = L(y_i)$. Soit alors $x \in X$ et $P \in \mathcal{I}(Y)$, montrons que $P(\varphi(x)) = 0$; on en déduira que $\varphi(x) \in \mathcal{Z}(\mathcal{I}(Y)) = Y$ (cf Proposition 2.2.6). Or

$$P(\varphi(x)) = P(L(y_1)(x), \cdots, L(y_m)(x)) = L(P(y_1, \cdots, y_m))(x),$$

puisque L est un morphisme de k-algèbres. Or $P(y_1, \cdots, y_m)$ est la classe de P dans $\Gamma(Y)$ puisque les y_i sont les classes des monômes dans $\Gamma(Y)$. Du fait que P s'annule sur Y, on a bien $P(\varphi(x)) = L(P(y_1, \cdots, y_m))(x) = 0$.

(iii) Le fait que les algèbres $\mathcal{O}_X(X)$ et $\mathcal{O}_Y(Y)$ soient isomorphes lorsque X et Y le sont résulte de la fonctorialité, un isomorphisme étant fourni par φ^*. En revanche l'implication inverse résulte du caractère pleinement fidèle du foncteur section globale. En effet, Supposons que $L : \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ soit un isomorphisme. De $L \circ L^{-1} = Id_{\mathcal{O}_X(X)} = Id_X^*$ et du fait de la surjectivité de l'application définie en (ii), il vient l'existence de $\varphi : X \to Y$ et $\psi : Y \to X$ deux morphismes de d'ensembles algébriques affines tels que $L = \varphi^*$ et $L^{-1} = \psi^*$, de sorte que $\varphi^* \circ \psi^* = Id_X^*$. Mais par fonctorialité, $(\psi \circ \varphi)^* = Id_X^*$, ce qui par fidélité donne $\psi \circ \varphi = Id_X$ (et de même $\varphi \circ \psi = Id_Y$). Ainsi φ est bien un isomorphisme.

(iv) Dans le cas où k est algébriquement clos, le foncteur section globale peut se noter Γ. Ce foncteur étant pleinement fidèle, il suffit par définition de l'équivalence de catégories de vérifier qu'il est **essentiellement surjectif**, ce qui a le sens suivant : soit A une $\mathbf{k}$-algèbre de type finie, alors on peut écrire, à un isomorphisme près de $\mathbf{k}$-algèbre, $A = \mathbf{k}[x_1, \ldots, x_n]/I$ pour un certain idéal I, et A étant réduite, l'idéal I est radical. Soit alors $X = \mathcal{Z}(I)$. Alors, $\Gamma(X) = \mathbf{k}[x_1, \cdots, x_n]/\mathcal{I}(X) = A$, puisque $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$ par le Nullstellensatz et que $\sqrt{I} = I$.

□

2.5.17 Corollaire. — *Soit X un ensemble algébrique affine de $\mathbf{k}^n$, alors $\mathcal{O}_X(X)$ ($A(X)$ dans le cas algébriquement clos) est en bijection avec l'ensemble des morphismes* $\mathrm{Mor}_{Var}(X, \mathbf{k})$ *de X dans $\mathbf{k}$:*

$$\mathcal{O}_X(X) \simeq \mathrm{Mor}_{Var}(X, \mathbf{k}).$$

Démonstration. — D'après le Théorème 2.5.16 (ii), lorsque $Y = \mathbf{k}$, on obtient

$$\mathrm{Mor}_{Var}(X, \mathbf{k})) \simeq \mathrm{Mor}_{k-alg}(\mathcal{O}_{\mathbf{k}}(\mathbf{k}), \mathcal{O}_X(X)).$$

Or un morphisme de $\mathbf{k}$-algèbres entre les fonctions régulières sur $\mathbf{k}$ et les fonctions régulières sur X, disons $L : \mathcal{O}_{\mathbf{k}}(\mathbf{k}) \to \mathcal{O}_X(X)$, est déterminé par sa valeur sur le monôme x (L passe au travers des fractions rationnelles). Mais se donner pour chaque élément L de $\mathcal{O}_{\mathbf{k}}(\mathbf{k})$ une valeur dans $\mathcal{O}_X(X)$ en x, revient à établir une bijection entre $\mathrm{Mor}_{k-alg}(\mathcal{O}_{\mathbf{k}}(\mathbf{k}), \mathcal{O}_X(X))$ et $\mathcal{O}_X(X)$. □

2.5.18 Exercice. — *Soit X l'ensemble algébrique de $\mathbf{k}^2$ défini par $X = \mathcal{Z}(y^2 - x^3)$.*

1. *Montrer que l'application $\varphi : \mathbf{k} \to X$ définie par $\varphi(t) = (t^2, t^3)$ est une application bijective dont on déterminera son inverse.*
2. *On veut montrer que $\mathcal{I}(X) = (y^2 - x^3)$. Pour cela considérons $P \in \mathcal{I}(X)$ et divisons P par $y^2 - x^3$ relativement à l'indéterminée y. On écrit $P(x, y) = (y^2 - x^3)Q(x, y) + R(x)y + S(x)$. D'après 1, tout point de X peut s'écrire (t^2, t^3) ; on obtient alors $R(t^2)t^3 + S(t^2) = 0$. En déduire si $\mathbf{k}$ est nfini que $R = S = 0$.*

3. *Montrer que $\varphi : \mathbf{k} \to X$ est un morphisme d'ensembles algébriques affines.*
4. *On suppose maintenant $\mathbf{k}$ algébriquement clos. Déterminer $\varphi^* : \Gamma(X) \to \Gamma(\mathbf{k})$. Montrer que φ^* n'est pas un isomorphisme de $\mathbf{k}$-algèbres (On pourra par exemple montrer que l'image de φ^* ne contient pas de polynôme linéaire).*
5. *Montrer que φ^* est injectif et que X est irréductible (utiliser la Proposition 2.5.20). En déduire que $A(X) \simeq \mathbf{k}[t^2, t^3] \subset \mathbf{k}[t]$.*
6. *On veut montrer que $A(X)$ et $\mathbf{k}[t]$ ne sont pas isomorphes, ie que X et $\mathbf{k}$ ne sont pas isomorphes (cf Théorème 2.5.16 (iii)).*
   - 6.a *Montrer que $A(X) = \{\sum_{i=0}^{n} a_i t^i ; n \in \mathbb{N}, a_1 = 0\}$, puis que t^2 et t^3 sont deux irréductibles [7] de l'anneau $A(X)$.*
   - 6.b *Montrer que t^6 est un élément de $A(X)$ possédant des écritures distinctes sur la famille d'irréductibles (t^2, t^3). En déduire que $A(X)$ n'est pas un anneau factoriel.*
   - 6.c *On pouvait aussi montrer que l'élément t^3/t^2 du corps des fractions de l'aneau $\mathbf{k}[t^2, t^3]$ est entier [8] sur $\mathbf{k}[t^2, t^3]$ mais n'appartient pas à $\mathbf{k}[t^2, t^3]$, ainsi $\mathbf{k}[t^2, t^3]$ n'est pas intégralement clos [9] tandis que $\mathbf{k}[t]$, qui est factoriel, est intégralement clos.*

On peut caractériser topologiquement le fait que φ^* soit injectif lorsque φ est un morphisme d'ensembles algébriques affines. Pour cela nous donnons la définition suivante

2.5.19 Définition. — Soient X et Y deux ensembles algébriques affines et $\varphi : X \to Y$ un morphisme. On dit que le morphisme φ est **dominant** lorsque $\overline{\varphi(X)} = Y$

2.5.20 Proposition. — *Soient X et Y deux ensembles algébriques affines et $\varphi : X \to Y$ un morphisme.*

(i) φ est dominant si et seulement si $\varphi^* : \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ est injectif,
(ii) Si $\mathbf{k}$ est algébriquement clos, X irréductible et φ dominant, alors Y est irréductible.

Démonstration. — (i) Soit $f \in \ker \varphi^*$. Alors $\varphi \circ f$ est nulle, donc f est nulle sur l'image de φ. Mais celle-ci est dense dans Y et f est continue (cf Proposition 2.4.4 (i)), donc $f = 0$. Réciproquement, supposons φ^* injective et soit $W = \overline{\varphi(X)}$. Si $W \subsetneq Y$, il existe $f \in A(Y)$ non nulle sur Y et nulle sur W (par la

[7] Un élément a d'un anneau A est dit **irréductible** si pour tout élément $b, c \in A$, $a = bc$ implique b ou c inversible.

[8] Soit A un anneau. Un élément x d'une A-algèbre B est dit **entier sur** A s'il vérifie une équation du type

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

avec $a_i \in A$.

[9] Un anneau intègre A est dit **intégralement clos** si l'ensemble des éléments entiers sur A de son corps des fractions est réduit à A. Tout anneau factoriel (et donc tout anneau principal) est intégralement clos.

Proposition 2.2.6). Mais alors $\varphi^* f = f \circ \varphi = 0$ et $f \neq 0$ contredit l'injectivité de φ^*.

(ii) Par (i) $\varphi^* : A(Y) \to A(X)$ est injectif de sorte que $A(Y) \simeq \varphi^*(A(Y))$. Or puisque $A(X)$ est intègre, il en va de même de $\varphi^*(A(Y))$ et donc de $A(Y)$. On en conclut que Y est irréductible.

□

2.6. Variétés algébriques affines et variétés algébriques

Nous allons étendre notre champ d'étude des variétés algébriques affines de $\mathbf{k}^n$ aux variétés algébriques affines, qui sont des objets isomorphes (au sens des espaces annelés) à des variétés algébriques affines de $\mathbf{k}^n$ (Définition 2.6.1). Les variétés algébriques affines permettrons enfin de définir les variétés algébriques dans leur généralité (Définition 2.6.24).

2.6.1 Définition. — Une **variété algébrique affine sur le corps k** est un espace annelé $(X, \mathcal{F})$ tel que

1. l'espace topologique X est irréductible,
2. $\mathcal{F}$ est un faisceau d'anneaux de fonctions sur X à valeurs dans le corps $\mathbf{k}$,
3. l'espace annelé $(X, \mathcal{F})$ est isomorphe (cf Définition 2.5.10) à une variété algébrique affine $(Y, \mathcal{O}_Y)$ de $\mathbf{k}^n$. Cette dernière s'appelle un **plongement de** $(X, \mathcal{F})$ **dans** $\mathbf{k}^n$.

Pour différencier les variétés algébriques affines et les variétés algébriques affines de $\mathbf{k}^n$, nous dirons souvent des dernières qu'elles sont des **variétés algébriques affines plongées**.

2.6.2 Remarque. — Suivant les auteurs, le point 1 de la Définition 2.6.1 est optionnel, ie qu'une variété affine n'est pas nécessairement isomorphe à un ensemble algébrique de $\mathbf{k}^n$ irréductible.

On peut motiver cette définition en rappelant que lorsque le corps $\mathbf{k}$ est algébriquement clos, la donnée d'une $\mathbf{k}$-algèbre intègre de type fini est la donnée d'une variété algébrique affine de $\mathbf{k}^n$ (Théorème 2.5.16), mais qu'en revanche celle-ci n'est donnée qu'à isomorphisme près, en ce sens que deux variétés algébriques affines de $\mathbf{k}^n$ isomorphes correspondent à la même algèbre. Dans notre volonté d'algébriser nos objets d'étude, il importe donc de considérer les objets à isomorphismes près ou encore de manière indépendante de leur plongement dans un espace $\mathbf{k}^n$.

On a de plus réellement étendu la classe d'ensembles à étudier, en ce sens que des sous-ensembles de $\mathbf{k}^n$ qui ne sont pas des variétés algébriques affines de $\mathbf{k}^n$ sont tout même des variétés algébriques affines, ie peuvent se plonger dans un espace $\mathbf{k}^m$, pour un certain m, comme le montre la proposition suivante.

2.6.3 Proposition. — *Soit X une variété affine de $\mathbf{k}^n$ (ie plongée) et $P \in A(X)$. Notons X_P l'ouvert fondamental $X \setminus \mathcal{Z}(P)$ de X. Alors $(X_P, \mathcal{O}_{X|X_P})$ est une variété*

algébrique affine qui se plonge dans $\mathbf{k}^{n+1}$ *en une variété algébrique affine de* $\mathbf{k}^{n+1}$ *(qui est d'algèbre affine* $\simeq A(X)_P$ [(10)] *lorsque* $\mathbf{k}$ *est algébriquement clos).*

Démonstration. — D'après l'Exercice 2.3.4, X_P, muni de la topologie induite par la topologie de Zariski de X, est un espace topologique irréductible. Notons encore $P \in \mathbf{k}[x_1, \cdots, x_n]$ un représentant de $P \in A(X)$. Soit alors Y l'ensemble algébrique affine de $\mathbf{k}^{n+1}$ défini par

$$Y = \{(x_1, \cdots, x_n, t) \in \mathbf{k}^{n+1}; P(x_1, \cdots, x_n) = 0, 1 - tP(x_1, \cdots, x_n) = 0\}.$$

Montrons que X_P et Y sont isomorphes. Pour cela considérons $\varphi : Y \to X_P$ défini par $\varphi(x_1, \cdots, x_n, t) = (x_1, \cdots, x_n)$. L'application φ est bien à valeurs dans X_P et est bien continue car si U est un ouvert de Zariski de X, $\varphi^{-1}(U) = Y \cap \pi^{-1}(U)$ où $\pi : \mathbf{k}^{n+1} \to \mathbf{k}^n$ est la projection sur les n premières composantes et $\pi^{-1}(U)$ est un ouvert de Zariski de $\mathbf{k}^{n+1}$ (on peut aussi invoquer la Proposition 2.4.4 (i)). D'autre part φ est bien un morphisme d'espaces annelés entre $(Y, \mathcal{O}_Y)$ et $(X_P, \mathcal{O}_{X|X_P})$, car si f est une application régulière sur un ouvert U de Y, $\varphi^* f(x_1, \cdots, x_n, t) = f(x_1, \cdots, x_n)$ est bien régulière sur $\varphi^{-1}(U)$. Enfin φ est une bijection d'inverse $\psi : X_P \to Y$ où $\psi(x_1, \cdots, x_n) = (x_1, \cdots, x_n, 1/P(x_1, \cdots, x_n))$. L'application ψ est bien un morphisme, en vertu de Proposition 2.5.13 (i).

Les sections globales des faisceaux $\mathcal{O}_{X|X_P}$ et $\mathcal{O}_Y$ sont des $\mathbf{k}$-algèbres isomorphes et par la Proposition 2.4.11, si $\mathbf{k}$ est algébriquement clos, $\mathcal{O}_{X|X_P}(X_P) = \mathcal{O}_X(X_P)$ est $A(X)_P$. □

2.6.4 Exemple. — L'ensemble des matrices inversibles de taille n à coefficients dans le corps $\mathbf{k}$ est une variété algébrique affine, puisqu'un ouvert du type $\mathbf{k}^{n^2} \setminus \mathcal{Z}(P)$, avec P le déterminant des matrices de taille n, qui est un polynôme en n^2 indéterminées.

Suppsons ici que par exemple $\mathbf{k} = \mathbb{R}$ ou $\mathbb{C}$. Comme un ouvert du type $X \setminus \mathcal{Z}(P)$, pour X une variété algébrique affine de $\mathbf{k}^n$ et $P \in \mathbf{k}[x_1, \cdots, x_n]$, ne saurait en général être une variété algébrique affine de $\mathbf{k}^n$, puisque $X \setminus \mathcal{Z}(P)$ n'est pas fermé pour la topologie transcendante lorsque $\mathcal{Z}(P) \cap X \neq \emptyset$, la catégorie des variétés algébriques affines sur $\mathbf{k}$ contient strictement plus d'objets que la catégorie des variétés algébriques affines des espaces $\mathbf{k}^n$. Cependant ces deux catégories sont équivalentes via le foncteur qui consiste à munir une variété algébrique affine de $\mathbf{k}^n$ de sa structure de variété algébrique affine. Ce foncteur revient à identifier les variétés algébriques affines isomorphes ; modulo cette identification, la catégorie des variétés algébriques affines n'est donc pas plus riche que celle des variétés algébriques affines plongées dans un espace $\mathbf{k}^n$.

2.6.5 Théorème. — *Le foncteur covariant de la catégorie des variétés algébriques affines plongées munie des morphismes de variétés algébriques affines plongées vers la catégorie des variétés algébriques affines munie des morphismes de variétés algébriques affines, qui consiste à associer à une variété algébrique affine de* $\mathbf{k}^n$ *sa*

(10) cf Remarque 1.3.15 (iv) pour la notation.

structure de variété algébrique affine, est une équivalence de catégories. Dans le cas où $\mathbf{k}$ *algébriquement clos, ces catégories sont donc équivalentes à la catégorie des* $\mathbf{k}$*-algèbres intègres de type finie munie des morphismes de* k*-algèbres.*

Démonstration. — Laissée en exercice, elle consiste à s'assurer que les arguments dans la preuve du Théorème 2.5.16 se reproduisent ici. □

2.6.6 Remarque. — Le Théorème 2.6.5, signifie en particulier qu'étant donnée une variété affine $(U, \mathcal{O}_U)$ isomorphe via un isomorphisme φ à une variété affine $(X, \mathcal{O}_X)$ plongée dans $\mathbf{k}^n$, on dispose du diagramme

$$\begin{array}{ccc} (U, \mathcal{O}_U) & \rightsquigarrow & \mathcal{O}_U(U) \\ {\scriptstyle\varphi}\downarrow & & \uparrow{\scriptstyle\varphi^*} \\ (X, \mathcal{O}_X) & \rightsquigarrow & \mathcal{O}_X(X) \end{array}$$

où $\rightsquigarrow$ désigne le foncteur section globale. Dans ce diagramme, la correspondance

$$\begin{array}{rcl} \mathrm{Mor}_{Var}(U, X)) & \to & \mathrm{Mor}_{k-alg}(\mathcal{O}_X(X), \mathcal{O}_U(U)) \\ \psi & \mapsto & \psi^* \end{array}$$

est bijective. Un morphisme $L \in \mathrm{Mor}_{k-alg}(\mathcal{O}_X(X), \mathcal{O}_U(U))$ étant donné, lui correspond un morphisme $\psi \in \mathrm{Mor}_{Var}(U, X)$ tel que $L = \psi^*$, de la manière suivante : x_i étant la iéme fonction coordonnée restreinte à X, $L(x_i) = \psi^* x_i = x_i \circ \psi$ est la iéme composante de ψ, $i = 1, \cdots, n$.

On peut définir **l'algèbre affine de la variété algébrique affine** U à l'aide de celle de la variété algébrique affine plongée X, au travers de l'isomorphisme de $\mathbf{k}$-algèbre φ^*, en posant $A(U) = \varphi^*(A(X))$. Notons qu'alors les fermés de U sont bien donnés par les zéros des éléments de $A(U)$, puisque si Y est un fermé de U, $\varphi(Y)$ est un fermé de X (du fait que φ est un homéomorphisme) donné par l'annulation d'un nombre fini $P_1, \cdots, P_k$ d'éléments de $A(X)$, et qu'ainsi $Y = \varphi^{-1}(\varphi(Y)) = \mathcal{Z}(\varphi \circ P_i)$, avec $\varphi \circ P_i = \varphi^* P_i \in \varphi^*(A(X)) := A(U)$.

2.6.7. Tous les ouverts d'une variété algébrique affine plongée ne sont pas des variétés algébriques affines. — D'après l'Exercice 2.4.15 l'ouvert de Zariski de $\mathbb{C}^2$ défini par $U = \mathbb{C}^2 \setminus \{(0,0)\}$ n'est pas un ouvert du type $\mathbb{C}^2 \setminus \mathcal{Z}(P)$, pour $P \in \mathbb{C}[x, y]$. Ainsi la Proposition 2.6.3 ne s'applique pas et on ne peut déduire de celle-ci que $(U, \mathcal{O}_{\mathbb{C}^2|U})$ est une variété algébrique affine. On montre en réalité que $(U, \mathcal{O}_{\mathbb{C}^2|U})$ n'est pas une variété algébrique affine. En effet nous avons vu dans ce même exercice que $\mathcal{O}_{\mathbb{C}^2}(U) = \mathbb{C}[x, y]$. Dès lors si $(U, \mathcal{O}_{\mathbb{C}^2|U})$ était une variété algébrique affine, du fait que $\mathbb{C}[x, y] = \mathcal{O}_{\mathbb{C}^2}(\mathbb{C}^2)$, on disposerait, conformément à la Remarque 2.6.6, du diagramme

$$\begin{array}{ccc} (U, \mathcal{O}_U) & \rightsquigarrow & \mathbf{k}[x, y] \\ {\scriptstyle\varphi}\downarrow & & \uparrow{\scriptstyle\varphi^*} \\ (\mathbb{C}^2, \mathcal{O}_{\mathbb{C}^2}) & \rightsquigarrow & \mathbf{k}[x, y] \end{array}$$

où du fait que le foncteur section globale $\rightsquigarrow$ est pleinement fidèle d'après le Théorème 2.6.5, tout isomorphisme φ^* provient d'un unique isomorphisme φ. Or si φ^* est choisi comme étant $Id_{\mathbf{k}[x,y]}$, nécessairement $\varphi = Id_{\mathbb{C}^2|U}$. Mais ceci est absurde, donc $(U, \mathcal{O}_{\mathbb{C}^2|U})$ n'est pas une variété affine. Cependant U est recouvert par deux variétés affines (deux ouverts fondamentaux) qui sont $X = \mathbb{C}^2 \setminus \mathcal{Z}(x)$ et $Y = \mathbb{C}^2 \setminus \mathcal{Z}(y)$.

2.6.8 Exemple **(Un fermé irréductible d'une variété affine est une variété affine)**

Soit $(X, \mathcal{O}_X)$ une variété affine sur $\mathbf{k}$ et Y un sous-ensemble de X qui soit fermé et irréductible (au sens de la topologie induite sur Y par celle de X). On définit sur Y le faisceau $\mathcal{O}_Y$ suivant, induit par $\mathcal{O}_X$. Si V est un ouvert de Y (ie la trace sur Y d'un ouvert de X), $\mathcal{O}_Y(V)$ est l'ensemble des fonctions $f : V \to \mathbf{k}$ telles que pour tout $x \in V$ existe un voisinage U de x dans X et $F \in \mathcal{O}_X(U)$ tels que $f = F_{|U \cap V}$. Alors $(Y, \mathcal{O}_Y)$ est une variété affine sur $\mathbf{k}$. En effet, soit X' une variété algébrique affine plongée dans $\mathbf{k}^n$ à laquelle X soit isomorphe par l'isomorphisme ϕ. Alors cet isomorphisme associe à Y un fermé irréductible Y' de X'. Montrons que $(Y, \mathcal{O}_Y)$ et la variété affine plongée $(Y', \mathcal{O}_{Y'})$ sont isomorphes. La restriction de ϕ à Y définit un homéomorphisme, noté $\phi_Y : Y \to Y'$. Il s'agit de montrer que ϕ_Y et ϕ_Y^{-1} sont des morphismes d'espaces annelés. Or si $f \in \mathcal{O}_{Y'}(Y')$, on peut écrire $f = P/Q$ sur Y'_Q et dans ce cas f est la restriction à Y' de $\tilde{f}$ donnée sur X'_Q par P/Q. Avec ces notations, $\phi_Y^* f_{|Y'_Q} = f_{|Y'_Q} \circ \phi_Y$ est la restriction à $\phi^{-1}(Y'_Q)$ de $\tilde{f}_{|X'_Q} \circ \phi$, qui est une fonction régulière sur $\phi^{-1}(X_Q)$. Donc $\phi_Y^* f_{|Y'_Q} \in \mathcal{O}_{Y'}(\phi_Y^{-1}(Y'_Q))$. Les arguments sont similaires pour ϕ_Y^{-1}.

2.6.9. Produit de variétés algébriques affines. — Nous allons maintenant définir la notion de variété algébrique affine produit. Ceci fournit des exemples naturels de variétés affines. Étant données deux variétés algébriques affines X et Y sur le corps $\mathbf{k}$ nous sommes à la recherche d'une variété algébrique affine Π sur le corps $\mathbf{k}$ et de deux morphismes $p : \Pi \to X$ et $q : \Pi \to Y$, vérifiant de plus la propriété universelle de la définition catégorielle du produit (cf Définition 1.5.2). Nous commençons par remarquer que du point de vue ensembliste, Π (qui est unique à unique isomorphisme près de variétés algébriques affines) est nécessairement le produit cartésien de X et Y. En effet, si Z est la variété algébrique affine ne contenant qu'un point, $\mathrm{Mor}(Z, \Pi)$ est identifié aux points de Π, de même $\mathrm{Mor}(Z, X) \simeq X$ et $\mathrm{Mor}(Z, Y) \simeq Y$. Enfin, d'après la Remarque 1.5.3, $\mathrm{Mor}(Z, \Pi)$ est en bijection avec $\mathrm{Mor}(Z, X) \times \mathrm{Mor}(Z, Y)$.

Il reste désormais à munir le produit cartésien $X \times Y$ d'une structure de variété affine produit. C'est l'objet de la proposition suivante.

2.6.10 Proposition. — *Soient X et Y deux variétés algébriques affines. On peut munir le produit cartésien $X \times Y$ d'une structure de variété algébrique affine de la manière suivante*

1. *Une base d'ouverts de l'espace topologique $X \times Y$ est donnée par les ouverts fondamentaux*

$$\{(x,y) \in X \times Y; \sum_{i=1}^{\ell} f_i(x)g_i(y) \neq 0, \ell \in \mathbb{N}^*, f_i \in A(X), g_i \in A(Y)\}.$$

2. *Le faisceau structural de $X \times Y$ est donné ainsi : si U est un ouvert de $X \times Y$, $\mathcal{O}_{X\times Y}(U)$ est l'anneau des fonctions $f : U \to \mathbf{k}$ telles que pour tout $(x,y) \in U$, sur un voisinage V de (x,y), on ait $f = P/Q$, avec $P, Q \in A(X) \otimes_k A(Y) \simeq A(X \times Y)$ et $Q(x,y) \neq 0$.*

De plus

- *Les deux projections naturelles de ce produit sont des morphismes ouverts,*
- *L'anneau $\mathcal{O}_{X\times Y,(x,y)}$ est le localisé de $\mathcal{O}_{X,x} \otimes_k \mathcal{O}_{Y,y}$ par l'idéal maximal $\mathfrak{m}_x\mathcal{O}_{Y,y} + \mathfrak{m}_y\mathcal{O}_{X,x}$ (qui est l'idéal des germes de fonctions régulières en (x,y) s'annulant en (x,y)),*
- *La variété algébrique affine $X \times Y$ satisfait la propriété universelle du produit catégoriel.*

Démonstration. — Les variétés algébriques affines X et Y sont par définition en bijection avec des variétés algébriques affines X' et Y' plongées dans $\mathbf{k}^n$ et $\mathbf{k}^p$. On en déduit que $\phi(a,b) := (\varphi(a), \psi(b))$ est une bijection entre les ensembles $X \times Y$ et $X' \times Y'$.

Notons ensuite que $X' \times Y'$ est bien un ensemble algébrique de $\mathbf{k}^{n+p}$ défini par $X' \times Y' = \mathcal{Z}(I + J)$, où I est un idéal de $\mathbf{k}[x]$ tel que $\mathcal{Z}(I) = X'$, J est un idéal de $\mathbf{k}[y]$ tel que $\mathcal{Z}(J) = Y'$ et où les polynômes en les indéterminés $x := (x_1, \cdots, x_n)$ et $y := (y_1, \cdots, y_p)$ sont naturellement considérés comme des éléments de $\mathbf{k}[x,y] := \mathbf{k}[x_1, \cdots, x_n, y_1, \cdots, y_p]$.

On a d'autre part $A(X' \times Y') \simeq A(X') \otimes_{\mathbf{k}} A(Y')$. En effet le morphisme de $\mathbf{k}$-algèbres

$$\begin{array}{rccc} \mathfrak{a} : & A(X') \otimes_{\mathbf{k}} A(Y') & \to & A(X' \times Y') \\ & \sum_{i=1}^{\ell} P_i \otimes Q_i & \mapsto & \mathfrak{a}(\sum_{i=1}^{\ell} P_i \otimes Q_i) \end{array}$$

défini par $\mathfrak{a}(\sum_{i=1}^{\ell} P_i \otimes Q_i)(a',b') = \sum_{i=1}^{\ell} P_i(a')Q_i(b')$ est un isomorphisme de $\mathbf{k}$-algèbres. La surjectivité est claire. Pour montrer l'injectivité, soit $(\mathbb{R}_i)_i$ une base du $\mathbf{k}$-espace vectoriel $A(X')$, $(S_j)_j$ une base du $\mathbf{k}$-espace $A(Y')$. On sait alors que $(R_i \otimes S_j)_{i,j}$ est une base du $\mathbf{k}$-espace $A(X') \otimes_{\mathbf{k}} A(Y')$. Maintenant si pour tout $(a',b') \in X' \otimes Y'$, $\mathfrak{a}(\sum_{i,j} \alpha_{ij} R_i \otimes S_j)(a',b') = \sum_{i,j} \alpha_{ij} R_i(a')S_j(b') = 0$, en fixant b' quelconque dans Y', la liberté des R_i donne, pour tout i, $\sum_{i,j} \alpha_{ij} S_j(b') = 0$, ce qui d'après la liberté des S_j donne, pour tout i,j, $\alpha_{ij} = 0$.

Par définition de $A(X)$ et $A(Y)$, ϕ est un homéomorphisme entre l'espace topologique $X \times Y$ dont une base d'ouverts est définie dans l'énoncé et $X' \times Y'$, dont les fermés sont donnés par les les zéros des polynômes de $\mathbf{k}[x,y]$ restreints à $X' \times Y'$, ces restrictions s'identifiant à $A(X') \otimes_{\mathbf{k}} A(Y')$.

Montrons maintenant que $\mathcal{I}(X' \times Y') = \mathcal{I}(X') + \mathcal{I}(Y')$. L'inclusion $\mathcal{I}(X') + \mathcal{I}(Y') \subset \mathcal{I}(X' \times Y')$ est évidente. inversement, soit $P \in \mathbf{k}[x,y]$ s'annulant sur

$X' \times Y'$. En idenfiant $\mathbf{k}[x,y]$ et $\mathbf{k}[x] \otimes_k \mathbf{k}[y]$, écrivons P sous la forme $\sum_i^L P_i \otimes Q_i$. Considérons une sous-famille maximale, disons $(P_i)_{i=1,\cdots,\ell}$, de la famille $(P_i)_{i=1,\cdots,L}$ telle que l'image de $(P_i)_{i=1,\cdots,\ell}$ dans $A(X')$ soit libre. On peut alors écrire des relations entre les P_j, $j \geq \ell+1$ et les éléments de la famille $(P_i)_{i=1,\cdots,\ell}$, du type

$$P_{\ell+1} = \sum_{i=1}^{\ell} \alpha_i^{\ell+1} P_i + p_{\ell+1}, \cdots, P_L = \sum_{i=1}^{\ell} \alpha_i^L P_i + p_L$$

avec $p_j \in \mathcal{I}(X')$, $j = \ell+1, \cdots, L$. Ainsi le polynôme P s'écrit sous la forme

$$P = \sum_{i=1}^{\ell} P_i \otimes \tilde{Q}_i + \sum_{i=\ell+1}^{L} p_i \otimes Q_i \tag{2.6.10.1}$$

où $\tilde{Q}_i \in \mathbf{k}[y]$. Comme pour tout $(a',b') \in X' \times Y'$ on a par hypothèse $P(a',b') = \sum_{i=1}^{\ell} P_i(a')\tilde{Q}_i(b') = 0$, en fixant b' quelconque dans Y', la liberté de la famille $(P_i)_{i=1,\cdots,\ell}$ donne $\tilde{Q}_i(b') = 0$ pour tout $b' \in Y'$ et donc $\tilde{Q}_i \in \mathcal{I}(y')$. D'après 2.6.10.1, on a bien $P \in \mathcal{I}(X') + \mathcal{I}(Y')$.

Du fait que ϕ est un homéomorphisme entre l'espace topologique $X \times Y$ et l'ensemble algébrique $X' \times Y'$ muni de sa topologie de Zariski, pour montrer que $X \times Y$ est irréductible il suffit de prouver que $X' \times Y'$ est un ensemble algébrique de $\mathbf{k}^{n+p}$ irréductible.

Pour cela nous commençons à prouver que les projections $p' : X' \times Y' \to X'$ et $q' : X' \times Y' \to Y'$ sont des morphismes ouverts. Il suffit de prouver que l'image par p' d'un ouvert fondamental $(X' \times Y')_P := \{(x',y') \in X' \times Y'; P(x',y') \neq 0\}$, $P \in \mathbf{k}[x,y]$, est un ouvert de X'. Soit $x'_0 \in p'((X' \times Y')_P)$. Il existe alors $y'_0 \in Y'$ tel que $P(x'_0, y'_0) \neq 0$. Notons P_{y_0} le polynôme $P(x, y_0) \in \mathbf{k}[x]$. On a $x_0 \in X_{P_{y_0}} \subset p'((X' \times Y')_P)$, ce qui montre que $p'((X' \times Y')_P)$ est un voisinage ouvert du point x'_0.

Supposons maintenant que $X' \times Y' = Z_1 \cup Z_2$, avec Z_1, Z_2 des fermés de $X' \times Y'$. On considère

$$X_1 = \{x' \in X'; \{x'\} \times Y' \subset Z_1\},\ X_2 = \{x' \in' X; \{x'\} \times Y' \subset Z_2\}.$$

Montrons que X_1 et X_2 sont des fermés de X'. Pour cela on constate que $X_1 = X' \setminus (p'(Z_2 \setminus Z_1))$. En effet $X' \setminus (p'(Z_2 \setminus Z_1)$ est l'ensemble des points x' de X' au-dessus desquels n'existe pas y' tel que $(x',y') \in Z_2 \setminus Z_1$; il s'agit bien de X_1. Or $Z_2 \setminus Z_1 = (X' \times Y') \setminus Z_1$ est un ouvert de $X' \times Y'$ et p' est ouverte. on en conclut que X_1 est un fermé de X' (de même pour X_2).

Remarquons ensuite que $\{x'\} \times Y'$ est la fibre de p' au-dessus de x' et celle-ci est irréductible, car isomorphe à Y'. De plus les deux fermés $Z_1 \cap (\{x'\} \times Y)$ et $Z_2 \cap (\{x'\} \times Y)$ se réunissent en $\{x'\} \times Y'$. On a donc $\{x'\} \times Y' \subset Z_1$ ou $\{x'\} \times Y' \subset Z_2$, ou encore $X' = X_1 \cup X_2$. Mais X' étant irréductible et X_1, X_2 étant fermés, on a par exemple $X' = X_1$. Dans ce cas, $X' \times Y' = Z_1$.

maintenant que nous avons prouvé que $X' \times Y'$ et $X \times Y$ sont des espaces irréductibles, il s'agit de prouver qu'en tant qu'espace annelé, $X \times Y$ est isomorphe

à une variété algébrique affine plongée. Mais clairement, étant donné la définition du faisceau structural de $X \times Y$, $X \times Y$ et $X' \times Y'$ sont isomorphes par ϕ.

Déterminons maintenant $\mathcal{O}(X\times Y)_{(x,y)}$. Par définition, $\mathcal{O}(X\times Y)_{(x,y)}$ est le localisé de $A(X\times Y) \simeq A(X)\otimes_{\mathbf{k}} A(Y)$ par l'idéal maximal $S \subset A(X)\otimes_{\mathbf{k}} A(Y)$ des fonctions régulières s'annulant en (x, y). Or l'inclusion

$$A(X) \otimes_{\mathbf{k}} A(Y) \subset \mathcal{O}(X)_x \otimes \mathcal{O}(Y)_y \subset \mathcal{O}(X \times Y)_{(x,y)}$$

montre que l'on a

$$\mathcal{O}(X \times Y)_{(x,y)} = [A(X) \otimes_{\mathbf{k}} A(Y)]_S \subset [\mathcal{O}(X)_x \otimes \mathcal{O}(Y)_y]_T \subset \mathcal{O}(X \times Y)_{(x,y)},$$

où T est l'idéal maximal de $\mathcal{O}(X)_x \otimes \mathcal{O}(Y)_y$ des fonctions qui s'annulent en (x, y). Il s'ensuit que $[\mathcal{O}(X)_x \otimes \mathcal{O}(Y)_y]_T = \mathcal{O}(X \times Y)_{(x,y)}$. Finalement, pour remarquer que $T = \mathfrak{m}_x\mathcal{O}_{Y,y} + \mathfrak{m}_y\mathcal{O}_{X,x}$, on considère $f = \sum_i f_i \otimes g_i \in \mathcal{O}(X)_x \otimes \mathcal{O}(Y)_y$ s'annulant en (x, y) et l'on écrit $f = \sum_i (f_i - f_i(x)) \otimes g_i + \sum_i f_i(x) \otimes (g_i - g_i(y)) \in \mathfrak{m}_x\mathcal{O}_{Y,y} + \mathfrak{m}_y\mathcal{O}_{X,x}$.

Il s'agit maintenant de démontrer que la variété $X \times Y$ vérifie la propriété catégorielle du produit. Nous disposons sur le produit catésien $X \times Y$ des deux projections p et q sur X et Y qui sont des morphismes (ouverts). Soit alors Z une variété algébrique affine sur $\mathbf{k}$ munie de deux morphismes $r : Z \to X$ et $s : Z \to Y$. Nous devons prouver qu'existe un unique morphisme $t : Z \to X \times Y$ tel que $r = p \circ t$ et $s = q \circ t$. D'un point de vue ensembliste, il existe une unique application t telle que $r = p \circ t$ et $s = q \circ t$, celle dont les composantes sont r et $s : t(z) = (r(z), s(z)) \in X \times Y$. Il reste à vérifier que t est un morphisme de variétés algébriques affines. D'après la Proposition 2.5.12 (ii), il suffit de prouver que $t^*(\mathcal{O}_{X\times Y}(X \times Y)) \subset \mathcal{O}_Z(Z)$. Soit $g \in \mathcal{O}_{X\times Y}(X \times Y))$, montrons que $t^*g = g \circ t \in \mathcal{O}_Z(Z)$. Or $g(t(z)) = g(r(z), s(z))$, d'où comme r, s et g sont des morphismes, t^*g aussi.

□

2.6.11. Prévariétés. — Rappelons qu'en toute généralité, d'après la Remarque 2.1.13, tout ouvert de Zariski d'un ensemble algébrique de $\mathbf{k}^n$ est réunion finie d'ouverts fondamentaux et donc réunion finie de variétés affines. Ainsi admettre les ensembles qui sont réunion finie de variétés affines dans notre champ d'investigation, comme les ouverts qui en général ne sont pas des variétés affines, revient à enrichir notre catégorie. Ceci est l'objet de la Définition suivante.

2.6.12 Définition. — Un espace annelé $(X, \mathcal{F})$ est appelé une **prévariété algébrique sur $\mathbf{k}$** lorsque

1. l'espace topologique X est irréductible,
2. $\mathcal{F}$ est un faisceau de fonctions à valeurs dans le corps $\mathbf{k}$,
3. il existe un recouvrement fini $\{U_i\}_{i=1,\cdots,\ell}$ de X par des ouverts de X tels que $(U_i, \mathcal{F}_{|U_i})$ est une variété affine pour tout $i \in \{1, \cdots, \ell\}$.

Un **morphisme de prévariétés** $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ est un morphisme entre les espaces annelés $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$, au sens de la Définition 2.5.10. Un ouvert U d'une prévariété algébrique X est appelé un **ouvert affine** lorsque $(U, \mathcal{O}_{X|U})$ est

isomorphe à une variété affine (et donc isomorphe à une variété algébrique affine plongée dans un espace $\mathbf{k}^n$).

2.6.13 Proposition. — *Soient $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$ deux prévariétés sur le corps $\mathbf{k}$ et $f : X \to Y$ une application. Soient $(V_i)_i$ des ouverts affines recouvrant Y et $(U_i)_i$ des ouverts affines de X recouvrant X tels que*

1. $f(U_i) \subset V_i$,
2. $f^*(\mathcal{O}_Y(V_i)) \subset \mathcal{O}_X(U_i)$.

Alors f est un morphisme de prévariétés.

Démonstration. — On peut laisser cette preuve en exercice. Voir [**14**], Proposition 6, page 30. □

2.6.14 Remarque. — L'espace topologique sous-jacent à une prévariété algébrique est quasi-compact. En effet un recouvrement par des ouverts d'une prévariété induit un recouvrement par des ouverts de chaque ouvert U_i qui définit la prévariété. Or un tel ouvert U_i est quasi-compact puisque isomorphe par définition à une variété algébrique affine plongée, qui est quasi-compacte (cf Remarque 2.1.14). Enfin les ouverts U_i sont en nombre fini et recouvrent la prévariété.

Voici quelques exemples de prévariétés.

2.6.15 Exemple **(Les ouverts d'une prévariété algébrique)**
Soit $(X, \mathcal{O}_X)$ une prévariété sur le corps $\mathbf{k}$ et U un ouvert de X. Alors $(U, \mathcal{O}_{X|U})$ est une prévariété sur le corps $\mathbf{k}$. En effet, U est un espace irréductible d'après l'Exercice 2.3.4. D'autre part soit $\{U_i\}_{i=1,\cdots,\ell}$ un recouvrement de X par des ouverts tels que $(u_i, \mathcal{O}_{X|U_i})$ est isomorphe, par un isomorphisme φ_i, à une variété algébrique $(X_i, \mathcal{O}_{X_i})$ plongée. Alors $\{U \cap U_i\}_{i=1,\cdots,\ell}$ est un recouvrement de U par les ouverts $U \cap U_i$ qui sont chacun isomorphes à un ouvert $V_i := \varphi(U \cap U_i)$ de X_i. Mais l'ouvert V_i est réunion finie d'ouverts fondamentaux V_{i_j} qui sont isomorphes à des variétés plongées. On en déduit que $\{\varphi^{-1}(V_{i_j})\}$ est un recouvrement de U par des ouverts qui sont des variétés affines.

2.6.16 Exemple **(Les fermés irréductibles d'une prévariété algébrique)**
Soit $(X, \mathcal{O}_X)$ une prévariété algébrique sur $\mathbf{k}$ et Y un sous-ensemble de X qui soit fermé et irréductible (au sens de la topologie induite sur Y par celle de X). On définit sur Y le faisceau $\mathcal{O}_Y$ suivant, induit par $\mathcal{O}_X$. Si V est un ouvert de Y (ie la trace sur Y d'un ouvert de X), $\mathcal{O}_Y(V)$ est l'ensemble des fonctions $f : V \to \mathbf{k}$ telles que pour tout $x \in V$ existe un voisinage U de x dans X et $F \in \mathcal{O}_X(U)$ tels que $f = F_{|U \cap V}$. Alors $(Y, \mathcal{O}_Y)$ est une prévariété sur $\mathbf{k}$ (il s'agit d'adapter les arguments de l'Exemple 2.6.8).

2.6.17 Exemple **(Recollement de deux prévariétés le long d'un morphisme)**
Soient $(X_1, \mathcal{O}_{X_1})$ et $(X_2, \mathcal{O}_{X_2})$ deux prévariétés sur le corps $\mathbf{k}$, $U_1 \subset X_1$ et $U_2 \subset X_2$ deux ouverts non vides et $\varphi : (U_1, \mathcal{O}_{X_1|U_1}) \to (U_2, \mathcal{O}_{X_2|U_2})$ un isomorphisme. On

considère l'espace topologique $X := X_1 \cup X_2/\sim$ où $\sim$ est la relation d'équivalence sur $X_1 \cup X_2$ définie par $x \sim y$ ssi $y = \varphi(x)$ et où les ouverts de X sont les sous-ensembles de X dont les images réciproques par la surjection canonique $\pi : X_1 \cup X_2 \to X$ sont du type $V_1 \cup V_2$, avec V_1 ouvert de X_1 et V_2 ouvert de X_2[(11)].

1. L'espace X est irréductible. En effet, soient U un ouvert non vide de X. Alors $\pi^{-1}(U) \cap X_1$ est un ouvert non vide de X_1 ou $\pi^{-1}(U) \cap X_2$ un ouvert non vide de X_2. Mais si par exemple $\pi^{-1}(U) \cap X_1$ est un ouvert non vide de X_1, du fait que X_1 est irréductible, $\pi^{-1}(U) \cap X_1$ coupe U_1, disons en x_1 et ainsi $\pi^{-1}(U) \cap X_2$ n'est pas vide puisque contient $\varphi(x_1)$. Finalement $\pi^{-1}(U) \cap X_1$ est un ouvert non vide de X_1, donc est dense dans X_1 (X_1 étant irréductible) et $\pi^{-1}(U) \cap X_2$ est un ouvert non vide de X_2, donc est dense dans X_2 (X_2 étant irréductible). Si V est un ouvert non vide de X, $\pi^{-1}(U) \cap X_1$ coupe $\pi^{-1}(V) \cap X_1$ ou $\pi^{-1}(U) \cap X_2$ coupe $\pi^{-1}(V) \cap X_2$, de sorte que nécessairement U coupe V.

On munit X de la structure d'espace annelé $(X, \mathcal{O}_X)$ de la façon suivante. Soit U un ouvert de X, on définit $\mathcal{O}_X(U)$ par

$$\mathcal{O}_X(U) := \{f : U \to \mathbf{k}; \exists f_1 \in \mathcal{O}_{X_1}(\pi^{-1}(U) \cap X_1), \exists f_2 \in \mathcal{O}_{X_2}(\pi^{-1}(U) \cap X_2),$$

$$(f \circ \pi)_{|\pi^{-1}(U)\cap X_1} = f_{1|\pi^{-1}(U)\cap X_1} \ \& \ (f \circ \pi)_{|\pi^{-1}(U)\cap X_2} = f_{2|\pi^{-1}(U)\cap X_2}\}$$

Notons que se donner $f \in \mathcal{O}_X(U)$ revient à se donner un couple

$$(f_1, f_2) \in \mathcal{O}_{X_1}(\pi^{-1}(U) \cap X_1) \times \mathcal{O}_{X_2}(\pi^{-1}(U) \cap X_2)$$

tel que $f_1(x) = f_2(\varphi(x))$, pour tout $x \in \pi^{-1}(U) \cap U_1$.

2. Ceci définit bien un faisceau $\mathcal{O}_X$ de fonctions à valeurs dans $\mathbf{k}$ sur X.
3. L'espace annelé $(X, \mathcal{O}_X)$ est une variété algébrique affine. Il suffit de vérifier que X est recouvert par un nombre fini d'ouverts qui sont des variétés affines. Soit V_1 un ouvert affine de X_1. L'ensemble $\pi(V_1)$ est un ouvert de X puisque $\pi^{-1}(\pi(V_1)) = V_1 \cup \varphi(V_1 \cap U_1)$ est une union d'un ouvert de X_1 et de X_2. D'autre part π réalise un isomorphisme de V_1 sur l'ouvert $\pi(V_1)$. Donc $\pi(V_1)$ est une variété affine. Enfin, X_1 est recouvert part un nombre fini d'ouverts affines du type V_1. De même X_2 est couvert par un nombre fini d'ouverts affines V_2 qui induisent via π des ouverts affines de X. Les ouverts du type $\pi(V_1)$ et $\pi(V_2)$ recouvrent X.

Le procédé de recollement décrit ci-dessus est général en ce sens que toute prévariété s'obtient par ce procédé, comme le montre la remarque triviale suivante.

2.6.18 Remarque. — Soit $(X, \mathcal{O}_X)$ une prévariété algébrique sur le corps $\mathbf{k}$. On considère deux copies X_1 et X_2 de X, les ouverts $U_1 = U_2 = X$ et l'isomorphisme identité $\varphi : U_1 \to U_2$. Il est clair que X est le recollement de X_1 et X_2 le long de φ.

(11) Cette topologie est la plus grossière rendant continue π. On l'appelle la topologie quotient.

2.6.19 Exemple **(Recollement de plusieurs variétés le long de morphismes)**

L'exemple 2.6.17 se généralise de la manière suivante. Soient $(X_i, \mathcal{O}_{X_i})$, $i = 1, \cdots, \ell$ des prévariétés sur le corps $\mathbf{k}$ et pour chaque i, soient U_{i_j}, $j = 1, \cdots, \ell$ des ouverts de X_i et $f_{i_j} = U_{i_j} \to U_{j_i}$ des isomorphismes tels que

- $f_{i_i} = Id_{U_{i_i}}$,
- $f_{i_j}^{-1} = f_{j_i}$,
- $f_{i_j} = f_{k_j} \circ f_{i_k}$ sur $U_{i_j} \cap U_{i_k} \cap f_{i_k}^{-1}(U_{k_j})$.

On définit alors un ensemble X par $X := (\cup_{i=1}^{\ell} X_i)/\sim$, où $x \sim y$ ssi $y = f_{i_j}(x)$ pour un certain couple (i, j). On munit X de la topologie quotient et du faisceau $\mathcal{O}_X$ naturellement défini grâce à la surjection canonique $\pi : \cup_{i=1}^{\ell} X_i \to X$. L'espace annelé $(X, \mathcal{O}_X)$ est alors une prévariété.

2.6.20 Remarque. — Si X est une prévariété recouverte par des ouverts affines $(U_i)_{i=1,\cdots,\ell}$, les intersections $U_{ij} := U_i \cap U_j$ définissent des isomorphismes $f_{ij} : U_{ij} \to U_{ji} = U_{ij}$ qui sont les restrictions à U_{ij} de l'identité. Dans ce cas le recollement des variétés affines U_i le long de ces morphismes est (s'identifie à) la prévariété X.

2.6.21 Exemple **(Espace projectif)**. — Soient $n \geq 1$ et $(X_i, \mathcal{O}_{X_i})$, $i = 1, \cdots, n+1$, les variétés affines de $\mathbf{k}^{n+1}$ définies par $X_i = \{x_i - 1 = 0\}$, et les ouverts fondamentaux $U_{i_j} := X_i \setminus \{x_j = 0\}, j \neq i$ de X_i. On considère alors les isomorphismes $f_{ij} : U_{i_j} \to U_{j_i}$ définis par

$$f_{i_j}(a_1, \cdots, a_{i-1}, 1, a_{i+1}, \cdots, a_{n+1})$$

$$= (\frac{a_1}{a_j}, \cdots, \frac{a_{i-1}}{a_j}, \frac{1}{a_j}, \frac{a_{i+1}}{a_j}, \cdots, \frac{a_{j-1}}{a_j}, 1, \frac{a_{j+1}}{a_j} \cdots, \frac{a_{n+1}}{a_j})$$

$$= \frac{1}{a_j}(a_1, \cdots, a_{i-1}, 1, a_{i+1}, \cdots, a_{n+1}).$$

En vertu du Corollaire 2.5.13 les applications f_{i_j} sont bien des morphismes de variétés algébriques affines puisque leurs composantes sont des fonctions régulières sur U_{i_j}. De plus ces morphismes sont bijectifs et on a bien $f_{i_j}^{-1} = f_{j_i}$, il s'agit donc bien d'isomorphismes satisfaisant les axiomes de recollement de variétés. On note $\mathbb{P}^n(\mathbf{k})$ le recollemenent des variétés X_i le long des morphismes f_{i_j}. On l'appelle **l'espace projectif de dimension** n **sur** $\mathbf{k}$.

- Ensemblistement, nous avons identifié les points de X_i et de X_j qui sont situés sur la même droite vectorielle. En effet, si une droite vectorielle D coupe X_i en $a = (a_1, \cdots, a_{n+1})$, D coupe X_j si et seulement si $a_j \neq 0$ et $D \cap X_j$ est $f_{i_j}(a)$. Dans ce procédé, toutes les droites vectorielles de l'espace affine $\mathbf{k}^n$ sont représentées par un unique point de $\mathbb{P}^n(\mathbf{k})$, ainsi $\mathbb{P}^n(\mathbf{k})$ est en bijection avec l'ensemble des droites vectorielles de $\mathbf{k}^n$.

- Du point de vue topologique, une droite passant par un point du type

$$(a_1, \cdots, a_j = 0, \cdots, a_{n+1})$$

de X_i contient dans tous ses voisinages dans $\mathbb{P}^n(\mathbf{k})$ des droites passant par des points "à l'infini", au sens de la topologie transcendante, dans les variétés X_j, $j \neq i$. Ainsi le recollement des variétés X_i le long des morphismes f_{i_j} consiste à ajouter aux droites repérées par les points de X_i, les droites de $x_i = 0$ (ie à ajouter à X_i la variété $\mathbb{P}^{n-1}(\mathbf{k})$) repérées par des points des X_j pour les $j \neq i$.

2.6.22 Exemple **(Espace à point double)**. — Soient $n \geq 1$, $X_1 = X_2 = \mathbb{A}^n(\mathbf{k})$, $U_1 = U_2 = \mathbb{A}^n(\mathbf{k}) \setminus \{0\}$ et $\varphi : U_1 \to U_2$ l'isomorphisme identité. Le recollement de X_1 et X_2 le long de φ est l'espace affine de dimension n à origine double. Il s'agit d'une prévariété.

L'Exemple 2.6.22 illustre en quoi la notion de prévariété est insuffisante : nous allons voir sur cet exemple que du point de vue du produit le comportement des prévariétés est topologiquement insatisfaisant. Mais auparavant nous allons définir le produit de prévariétés.

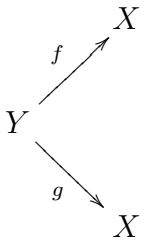
2.6.23 Exemple **(Produit de prévariétés)**. — Soient $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$ deux prévariétés sur le même corps $\mathbf{k}$. On définit la prévariété produit $(X \times Y, \mathcal{O}_{X\times Y})$ de la façon suivante. En tant qu'ensemble, $X \times Y$ est le produit cartésien des deux ensembles X et Y. En tant qu'espace topologique, une base d'ouverts est ainsi définie : soient U un ouvert affine de X et V un ouvert affine de Y, $(f_i)_{i=1,\cdots,\ell}$ des fonctions de $\mathcal{O}_X(U)$, $(g_i)_{i=1,\cdots,\ell}$ des fonctions de $\mathcal{O}_Y(V)$, et $\sum_{i=1}^{\ell} f_i g_i := \sum_{i=1,\cdots,\ell} f_i \otimes g_i$. Les ouverts de base de $X \times Y$ sont les ouverts $(U \times V)_{\sum_{i=1}^{\ell} f_i g_i}$. Notons qu'il s'agit bien d'une base d'ouverts puisque l'intersection de deux tels ouverts $(U \times V)_{\sum_{i=1}^{\ell} f_i g_i}$ et $(U' \times V')_{\sum_{i=1}^{\ell'} f'_i g'_i}$ contient un ouvert du même type, qui est $((U \cap U') \times (V \cap V')_{(\sum_{i=1}^{\ell} f_i g_i)(\sum_{i=1}^{\ell'} f'_i g'_i)}$. Les ouverts affines U et V sont irréductibles d'après l'Exercice 2.3.4, leur produit forme la variété affine produit au sens de la Proposition 2.6.10. L'espace topologique $X \times Y$ est le recollement de ces variétés le long des isomorphismes induit par les restrictions de l'identité de X et de Y sur les intersections des ouverts affines de X et Y. L'espace topologique $X \times Y$ est ainsi irréductible, d'après 2.6.17 généralisé à plusieurs variétés. En tant qu'espace annelé, nous définissions la prévariété produit comme suit. Si W est un ouvert de $X \times Y$, $\mathcal{O}_{X\times Y}(W)$ est l'ensemble des fonctions f telle que pour tout $(x_0, y_0) \in W$, existe un voisinage ouvert Z ouvert de (x_0, y_0) dans W tel que sur Z on ait $f(x, y) = (\sum_i f_i \otimes g_i)/h$ avec $f_i \in \mathcal{O}_{X,x_0}$, $g_i \in \mathcal{O}_{Y,y_0}$ et $h \in (\mathcal{O}_{X,x_0} \otimes \mathcal{O}_{Y,y_0}) \setminus \mathfrak{m}_{x_0}\mathcal{O}_{Y,y_0} + \mathfrak{m}_{y_0}\mathcal{O}_{X,x_0}$ ($\mathfrak{m}_{x_0}\mathcal{O}_{Y,y_0} + \mathfrak{m}_{y_0}\mathcal{O}_{X,x_0}$ étant l'idéal maximal des fonctions de $\mathcal{O}_{X,x_0} \otimes \mathcal{O}_{Y,y_0}$ s'annulant en (x_0, y_0)).

On vérifie que $X \times Y$ munie de cette structure d'espace annelé est une prévariété, dite **prévariété produit de X et Y** et qu'elle vérifie la propriété universelle du produit catégoriel (on utilise pour cela la Proposition 2.6.13).

La notion de prévéariété algébrique produit étant définie, nous pouvons nous attacher à la notion de variété algébrique.

2.6.24 Définition **(Variété algébrique)**. — Soit $(X, \mathcal{O}_X)$ une prévariété sur le corps $\mathbf{k}$. On dit que X est une **variété algébrique sur le corps $\mathbf{k}$** lorsque pour toute

prévariété $(Y, \mathcal{O}_Y)$ sur le corps $\mathbf{k}$ et tout couple f, g de morphismes (de prévariétés)



l'ensemble $\{y \in Y; f(y) = g(y)\}$ est un fermé de Y. Un **morphisme de variétés** est un morphisme entre les prévariétés sous-jacentes, ie un morphisme d'espaces annelés.

2.6.25 Remarque. — **Toutes les prévariétés ne sont pas des variétés**. Par exemple l'espace à point double X défini dans l'exemple 2.6.22 est une prévariété, mais n'est pas une variété. En effet considérons $Y = \mathbb{A}^1(\mathbf{k})$ et $f : Y \to X$ l'inclusion de Y dans X, $g : Y \to X$ l'inclusion de Y dans X de sorte que f et g coïncident sur $Y \setminus \{0\}$ mais que $f(0)$ et $g(0)$ soient les deux origines distinctes de X. Dans ce cas f et g sont bien des morphismes mais $\{y \in Y; f(y) = g(y)\} = Y \setminus \{0\}$ n'est pas un ouvert de Y.

En revanche toute variété affine est une variété. Considérons une variété algébrique affine X, que nous supposons plongée dans $\mathbf{k}^n$, à isomorphisme près. Si $X = \mathcal{Z}(I)$ où I est l'idéal de $\mathbf{k}[x_1, \cdots, x_n]$ engendré par $f_1, \cdots, f_\ell$, $\Delta(X) := \{(x, x) \in X \times X\}$ est l'ensemble algébrique de $\mathbf{k}^{2n}$ donné par $\mathcal{Z}(f_1, \cdots, f_n, x_1 - y_1, \cdots, x_n - y_n)$, où $\mathbf{k}^{2n}$ a pour coordonnées $x_1, \cdots, x_n, y_1, \cdots, y_n$. Ainsi $\Delta(X)$ apparaît comme un ensemble algébrique de $\mathbf{k}^{2n}$, donc un fermé de la variété affine $X \times X$ et en vertu de la Proposition 2.6.26 qui suit, X est bien une variété algébrique.

2.6.26 Proposition. — *La prévariété $(X, \mathcal{O}_X)$ sur le corps $\mathbf{k}$ est une variété si et seulement si l'ensemble $\Delta(X) = \{(x, x) \in X \times X\}$ est un fermé de la prévariété produit $X \times X$.*

Démonstration. — Supposons que X soit une variété. Alors $\Delta(X) = \{z \in X \times X; p(z) = q(z)\}$, où p, q sont les deux projections du produit $X \times X$. Ce sont deux morphismes de prévariétés. Il s'ensuit que $\Delta(X)$ est un fermé de $X \times X$. Réciproquement, si $\Delta(X)$ est un fermé de $X \times X$, et si $f, g : Y \to X$ sont deux morphismes de prévariétés, alors

$$\{y \in Y; f(y) = g(y)\} = (f, g)^{-1}(\Delta(X)),$$

où (f, g) est le morphisme induit sur le produit $X \times X$ par f et g. Un morphisme de prévariétés étant par définition continu, X est bien une variété. □

Nous avons vu dans la Remarque 2.6.25 que les variétés affines sont des variétés. On peut facilement généraliser cette remarque.

2.6.27 Proposition. — *Soit $(X, \mathcal{O}_X)$ une variété algébrique sur le corps $\mathbf{k}$. Alors tout fermé et tout ouvert de X est une variété algébrique.*

Démonstration. — Soit E un ouvert ou un fermé de X. Alors $\Delta(E) = \Delta(X) \cap (E \times E)$. Donc si $\Delta(X)$ est un fermé de $X \times X$, il en est de même de $\Delta(E)$ dans $E \times E$, la topologie de $E \times E$ étant la topologie de $X \times X$ induite sur $E \times E$. □

2.6.28 Exercice. — *Soit $(X, \mathcal{O}_X)$ une prévariété algébrique telle que pour tout $x, y \in X$ existe un ouvert affine U contenant x et y. Montrer que $(X, \mathcal{O}_X)$ est une variété algébrique.*

Pour cela considérons $f, g : Y \to X$ deux morphismes de prévariétés et notons $Z = \{y \in Y ; f(y) = g(y)\}$. Soit $z \in \bar{Z}$, notons $x = f(z)$ et $y = g(z)$ et soit $U \subset X$ un ouvert affine de X contenant à la fois x et y. On note $W = f^{-1}(U) \cap g^{-1}(U)$; il s'agit d'un ouvert de Y contenant z. On note $f' = f_{|W} : W \to U$ et $g' = g_{|W} : W \to U$. Du fait que U est une variété algébrique, $Z' := \{y \in W ; f'(y) = g'(y)\}$ est un fermé de W. Or z est dans l'adhérence de Z', donc est dans Z' et finalement est dans Z.

CHAPITRE 3

LE LANGAGE DE LA THÉORIE DES MODÈLES

Nous donnons dans ce chapitre une introduction élémentaire à la théorie des modèles. Les lecteurs soucieux d'approfondir le sujet peuvent se reporter entre autres aux références [**3**], [**4**], [**5**], [**9**], [**10**], [**12**], [**17**] sur lesquelles s'appuie ce cours. Il s'agit dans ce chapitre de voir comment on peut envisager certaines propositions comme conséquences seulement des axiomes que l'on se donne au départ dans le cadre le plus général, comme ceux définissant les corps algébriquement clos en toute indépendance d'un corps algébriquement clos particulier. Le Nullstellensatz est ainsi une conséquence facile d'une propriété logique très forte du système d'axiomes définissant les corps algébriquement clos, cette propriété est l'élimination des quantificateurs.

3.1. Structures et Langages

3.1.1 Définition **(Structure)**. — Une **structure** $\mathbf{A} = (A, (c_h^A)_{h\in H}, (f_i^A)_{i\in I}, (R_j^A)_{j\in J})$ est la donnée

- d'un ensemble $A \neq \emptyset$, appelé l'**univers** de la structure.
- d'une famille d'éléments de A, appelés les **constantes** $(c_h^A)_{h\in H}$, $c_h \in A$,
- d'une famille applications appelées les **opérations** $f_i^A : A^{n(i)} \to A$, $n(i) \in \mathbb{N}$. On dit que $n(i)$ est l'**arité** de f_i^A.
- d'une famille de sous-ensembles d'espaces produits $A^{m(j)}$ appelés les **relations** $R_j^A \subset A^{m(j)}$, $m(j) \in \mathbb{N}^*$.

3.1.2 Remarque. — Lorsque $n(i) = 0$, f_i^A est une constante.

3.1.3 Exemple. — $A = \mathbb{R}$, $c_0 = 0, c_1 = 1$, $f_1(x, y) = x + y$, $f_2(x, y) = x \cdot y$, $f_3(x) = -x$, $R_0 = \{(x, y) \in \mathbb{R}^2; x < y\}$.

3.1.4 Définition **(Langage)**. — À la structure **A** on associe le **langage**

$$\mathbf{L} = \{(c_h)_{h\in H}, (f_i)_{i\in I}, (R_j)_{j\in J}, (x_k)_{k\in\mathbb{N}}\} \text{ où}$$

- à chaque c_h^A on associe un symbole c_h,
- à chaque f_i^A on associe un symbole f_i d'arité $n(i)$,
- à chaque R_j^A on associe un symbole R_j d'arité $m(j)$,
- $(x_k)_{k\in\mathbb{N}}$ est un ensemble de symboles, dits les **variables** du langage.

Si **L** est le langage associé à la structure **A**, on dit que **A** est une **L-structure**.

3.1.5 Remarque. — On peut se donner un langage sans se donner au préalable une structure. Par exemple $\mathbf{L}_{ord} := \{0, 1, +, \cdot, -, <, (x_k)_{k\in\mathbb{N}}\}$ est un langage *a priori*, le **langage des anneaux ordonnés** dont $\mathbb{R} := (\mathbb{R}, 0, 1, +, \cdot, -, <)$ est une structure. $\mathbf{L}_{rings} := \{0, 1, +, \cdot, -, (x_k)_{k\in\mathbb{N}}\}$ est le **langage des anneaux** dont $\mathbf{C} := (\mathbb{C}, 0, 1, +, \cdot, -)$ est par exemple une structure.

3.1.6 Définition. — Soit **L** un langage et **A** une **L**-structure.

1. Un **L-terme** par une suite finie de symboles, engendrée par les règles :
   - les variables et les constantes sont des **L**-termes,
   - si $t_1, \cdots, t_{n(i)}$ sont des **L**-termes, $f_i(t_1, \cdots, t_{n(i)})$ aussi.
2. Une **L-formule atomique** est une suite finie de symboles, engendrée par les règles :
   - $t_1 = t_2$
   - ou $R_j(t_1, \cdots, t_m)$, lorsque $t_1, \cdots, t_m$ sont des **L**-termes.

   On peut écrire
   $$R_j(t_1(x_1, \cdots, x_\ell), \cdots, t_m(x_1, \cdots, x_\ell))$$
   pour $R_j(t_1, \cdots, t_m)$ et $t_1(x_1, \cdots, x_\ell)) = t_2(x_1, \cdots, x_\ell))$ pour $t_1 = t_2$, afin de faire apparaître les variables d'une **L**-formule atomique.
3. Une **L-formule** ou **formule élémentaire** ou **formule du premier ordre** est une suite finie de symboles, engendrée par les règles :
   - une **L**-formule atomique est une **L**-formule,
   - si ϕ et ψ sont des **L**-formules, $(\neg\phi)$ et $(\phi \vee \psi)$ et $(\phi \wedge \psi)$ aussi,
   - si ϕ est une **L**-formule et x_k une variable, $(\exists x_k)\phi$ et $(\forall x_k)\phi$ sont des **L**-formules.
4. Les formules construites sans la dernière règle sont dites **sans quantificateur**. On écrit $\phi(x_1, \cdots, x_\ell)$ pour indiquer que les **variables libres** (ie non assujetties à des quantificateurs) dans cette formule sont les variables $x_1, \cdots, x_\ell$.
5. Les formules dans lesquelles toutes les variables sont régies par des quantificateurs sont dites des **L-phrases**.

3.2. Interprétation des formules

On étend le langage **L** en un langage $\mathbf{L}_A$ en ajoutant à **L** le symbole a (vu comme une constante), pour chaque $a \in A$; alors **A** est une $\mathbf{L}_A$-structure.

Étant donnée une $\mathbf{L}_A$-formule $\phi(x_1, \cdots, x_\ell)$ et $a_1, \cdots, a_\ell \in A$, on définit une $\mathbf{L}_A$-phrase en remplaçant les variables libres $x_1, \cdots, x_\ell$ respectivement par $a_1, \cdots, a_\ell$. On obtient une **interprétation** de $\phi(x_1, \cdots, x_\ell)$. La $\mathbf{L}_A$-phrase $\phi(a_1, \cdots, a_\ell)$ est alors **vraie** ou **fausse** dans A. On définit la véracité dans A en se donnant la liste des formules atomiques vraies dans A. En effet les interprétations des fonctions et

des relations étant donnés on est à même d'attribuer la valeur vrai ou faux à une formule atomique, puis par récurrence sur la complexité des formules définies à partir des formules atomiques.

Lorsque la $\mathbf{L}_A$-phrase σ est vraie dans $\mathbf{A}$, on écrit : $\mathbf{A} \models \sigma$ ($\mathbf{A}$ satisfait σ).

La vérité d'une formule ou d'un énoncé ϕ dans $\mathbf{A}$ se définit par récurrence sur la longueur de la formule ϕ, pour se ramener à la vérité de l'interprétation de ϕ dans A. Cette récurrence procède des règles :

1. $A \models t_1 = t_1$ ssi $t_1^A = t_2^A$ pour les termes t_1 et t_2,
2. $A \models R_j(t_1, \cdots, t_{m(j)})$ ssi $R_j^A(t_1^A, \cdots, t_{m(j)}^A)$ pour les termes $t_1, \cdots, t_{m(j)}$,
3. $A \models \neg\phi$ ssi $A \not\models \phi$
4. $A \models (\phi \wedge \psi)$ ssi $A \models \phi$ et $A \models \psi$
5. $A \models (\phi \vee \psi)$ ssi $A \models \phi$ ou $A \models \psi$
6. $A \models (\phi \longrightarrow \psi)$ ssi $A \models \phi$ implique $A \models \psi$
7. $A \models (\phi \longleftrightarrow \psi)$ ssi $A \models \phi$ équivaut à $A \models \psi$
8. $A \models \forall x\phi$ ssi $A \models \phi(x/a)$ pour tout $a \in A$
9. $A \models \exists x\phi$ ssi $A \models \phi(x/a)$ pour un $a \in A$

$\phi(x/a)$ signifie que l'on remplace x par a toutes les fois que la variable x apparaît dans la formule ϕ.

Noter que la véracité de formules interprétées dans A est une donnée au même titre que la donnée des opérations et des relations du langage, puisque les relations ou les opérations de la structures sont des ensembles, et leur appartenir ou pas ne souffre pas de preuve. La donnée de la structure revient à se donner les éléments qui appartiennent aux différents ensembles sous-jacents, cette donnée impose ainsi formellement les formules vraies et celles qui ne le sont pas.

3.2.1 Exemple. — Soit $\mathbf{A} = (A, \cdots)$ une structure où A est un anneau. Dans $\mathbf{L}_{rings\ A}$ La formule : $y^2 = zx$ est une formule atomique et si $\phi(z)$ est : $\forall x \exists y, y^2 = zx$, $\phi(1) : \forall x \exists y, y^2 = x$ est une $\mathbf{L}_{rings\ A}$-phrase, interprétation de ϕ. Celle-ci est vraie ou pas selon le choix de A.

3.2.2 Définition **(Preuve formelle)**. — Si Σ est un ensemble de $\mathbf{L}$-phrases, et si ϕ est une $\mathbf{L}$-phrase, on note $\Sigma \vdash \phi$ (Σ prouve ϕ) si l'on peut **formellement prouver ϕ à partir de Σ**. On dit aussi que ϕ est une **conséquence syntaxique** de Σ. Prouver formellement signifie prouver à l'aide de règles d'inférences portant sur les formules (une preuve formelle à partir de Σ est une suite finie de $\mathbf{L}$-formules, qui soit sont des phrases de Σ, soit déduites de la formule précédente de la suite par les règles logiques usuelles). On parle donc ici d'une notion plus forte que la vérité d'un énoncé dans une structure donnée, puisque si $\Sigma \vdash \phi$, la phrase ϕ sera en particulier vraie dans toute $\mathbf{L}$-structure $\mathbf{A}$ dans laquelle toutes les phrases $\sigma \in \Sigma$ sont vraies (une telle structure est appelée un **modèle de** Σ), par compatibilité des règles d'inférence qui prouvent ϕ formellement à partir de Σ et des règles d'inférence qui prouvent l'interprétation de ϕ dans A. Remarquons que si $\Sigma \vdash \phi$, un sous-ensemble fini $\Sigma' \subset \Sigma$ est tel que $\Sigma' \vdash \phi$, par définition de la notion de preuve formelle.

Lorsque quel que soit le modèle $\mathbf{M}$ de Σ, on a $\mathbf{M} \models \phi$, on dit que ϕ est une **conséquence sémantique** de Σ. Nous verrons que le théorème de complétude de Gödel (Théorème 3.2.12) affirme qu'il n'y a en réalité pas lieu de distinguer entre conséquence sémantique et syntaxique.

3.2.3 Définition **(Théorie sur un langage)**. — Une **théorie sur le langage** $\mathbf{L}$ est un ensemble de $\mathbf{L}$-phrases (ie de $\mathbf{L}$-formules sans variable libre). Si $\mathcal{C}$ est une classe de $\mathbf{L}$-structures, on note $Th(\mathcal{C})$ l'ensemble des $\mathbf{L}$-phrases vraies pour toutes les $\mathbf{L}$-structures de $\mathcal{C}$. Dans le cas où $\mathcal{C}$ est réduite à la seule $\mathbf{L}$-structure $\mathbf{A}$, on note $Th(\{\mathbf{A}\})$ simplement par $Th(\mathbf{A})$. Il s'agit de l'ensemble des phrases du langage $\mathbf{L}$ vraies dans $\mathbf{A}$.

3.2.4 Définition **(modèle)**. — Un **modèle** d'une $\mathbf{L}$-théorie $\mathbf{T}$ est une $\mathbf{L}$-structure $\mathbf{A}$ qui satisfait toutes les phrases de $\mathbf{T}$. On note $\mathbf{A} \models \mathbf{T}$.

3.2.5 Définition **(Théorie non contradictoire, complète)**
Une théorie $\mathbf{T}$ (sur le langage $\mathbf{L}$) est

1. **non contradictoire** si elle admet un modèle. On dit parfois qu'une théorie est **consistante** ou **cohérente** au lieu de non contradictoire, mais parfois consistant ou cohérent signifie que l'on ne peut prouver la phrase $\forall x(x \neq x)$ à partir des axiomes de la théorie. Cela n'a aucune importance en vue du théorème de complétude Gödel qui assure que ces définitions sont équivalentes.
2. **complète** si pour chacune des $\mathbf{L}$-phrases ϕ de $\mathbf{L}$, soit ϕ est vraie dans tous les modèles de $\mathbf{T}$ soit $\neg\phi$ est vraie dans tous les modèles de $\mathbf{T}$. Une phrase Φ d'un langage $\mathbf{L}$ est dite **indécidable dans une théorie** $\mathbf{T}$ (nécessairement incomplète) si l'on ne peut pas prouver Φ ni $\neg\Phi$ à partir de $\mathbf{T}$.

3.2.6 Exemple. — Par exemple si $\mathbf{A}$ est une $\mathbf{L}$-structure alors $Th(A)$ est complète. En effet si ϕ est une phrase de $\mathbf{L}$, dans A elle est soit vraie, soit fausse de sorte que soit $\phi \in Th(A)$, soit $\neg\phi \in Th(A)$ et par définition les modèles de $Th(A)$ satisfont donc ϕ ou $\neg\phi$ de la même façon que $Th(A)$.

3.2.7 Définition. — Deux $\mathbf{L}$-structures sont dites **élémentairement équivalentes** ssi elles saisfont les mêmes phrases du langage $\mathbf{L}$. Ainsi une théorie est complète ssi ses modèles sont tous élmentairement équivalents.

Le **théorème de complétude de Gödel** assure que si $\mathbf{T}$ est complète, toutes les phrases de $\mathbf{L}$, ou leur négation, sont des conséquences logiques de $\mathbf{T}$:

$$\textit{si } \phi \textit{ est une phrase de } \mathbf{L},\ \mathbf{T} \vdash \phi \textit{ ou } \mathbf{T} \vdash \neg\phi.$$

3.2.8 Remarque. — Dans le cas où $\mathbf{T} = Th(A)$, le théorème de Gödel assure que les phrases de $\mathbf{L}$, ou leur négation, sont toutes des conséquences logiques de $Th(A)$, puisque $Th(A)$ est complète. Ceci est sans intérêt dans ce cas, car ici les phrases de $\mathbf{L}$ sont exactement partagées en deux, celles qui sont vraies dans A ie qui sont dans $Th(A)$ et celles qui ne le sont pas. Or les formules de $Th(A)$ sont des conséquences logiques de $Th(A)$, par définition-même, et les phrases ϕ qui ne sont pas dans $Th(A)$

sont telles que $\neg\phi$ sont dans $Th(A)$, elles sont donc aussi des conséquences logiques de $Th(A)$.

3.2.9 Exemple. — La théorie $\mathbf{T}_{\mathbf{groups}}$ donnée par l'ensemble des phrases du langage des groupes $\mathbf{L}_{groups} = \{^{-1}, \cdot, e\}$ contenant les conséquences logiques des formules suivantes

- $(\forall x)(\forall y)(\forall z)x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $(\forall x)x \cdot e = e \cdot x$
- $(\forall x)x \cdot x^{-1} = x^{-1} \cdot x = e$

est incomplète puisque la $\mathbf{L}_{groups}$-phrase $(\forall x)(\forall y)x \cdot y = y \cdot x$ est indécidable : il existe des groupes abéliens et des groupes non abéliens et ceux-ci, munis de leur $\mathbf{L}_{groups}$-structure naturelle sont des modèles de $\mathbf{T}_{\mathbf{groups}}$.

3.2.10 Définition. — On dit qu'une théorie $\mathbf{T}$ est

- **axiomatisée** par l'ensemble de phrases Σ, si $\mathbf{T}$ est conséquence de Σ.
- **consistante** si elle ne permet pas de prouver à la fois une formule et sa négation. Notons que si une théorie $\mathbf{T}$ n'est pas cohérente, elle permet de prouver toutes les formules car si ϕ et $\neg\phi$ sont prouvés par $\mathbf{T}$, $\phi \Longrightarrow (\neg\phi \Longrightarrow \psi)$, quelle que soit la formule ψ.

3.2.11 Remarque. — Bien sûr si une théorie $\mathbf{T}$ admet un modèle, elle est consistante. En revanche rien ne dit *a priori* que si $\mathbf{T}$ est consistante, $\mathbf{T}$ admet un modèle. C'est cependant bien le cas, et c'est l'objet du théorème de compétude de Gödel (voir sa preuve ci-dessous). Il y a donc équivalence entre non contradictoire et consistant.

À ce stade nous disposons de la prouvabilité formelle d'une phrase ϕ à partir d'un ensemble de phrases Σ, dans le langage $\mathbf{L}$, que l'on a noté $\Sigma \vdash \phi$ et de la notion de véracité de ϕ dans une structure $\mathbf{A}$ dans laquelle toutes les phrases de Σ sont vraies, ie dans un modèle $\mathbf{A}$ de Σ. On a noté $\mathbf{A} \models \phi$.

On a déjà souligné que les règles d'inférence logique qui permettent de prouver ϕ formellement à partir de Σ donne une preuve de l'interprétation de ϕ dans A à partir de l'ensemble d'énoncés Σ. On a la réciproque suivante :

3.2.12 Théorème **(Théorème de complétude de Gödel (1929))**

Soit Σ un ensemble de phrases d'un langage $\mathbf{L}$ et ϕ une phrase de $\mathbf{L}$. On a l'équivalence :

- *$\Sigma \vdash \phi$.*
- *ϕ est vraie dans tout modèle de Σ.*

La preuve établit que si une théorie est consistante, elle admet un modèle, ce qui prouve que les définitions de théorie cohérente, consistante ou non contradictoire sont équivalentes.

Remarque. *Si Σ est une théorie complète et si ϕ est une phrase de Σ, ϕ ou $\neg\phi$ étant vraie dans tout modèle de Σ, on a $\Sigma \vdash \phi$ ou $\Sigma \vdash \neg\phi$.*

Démonstration. — On montre que si ϕ n'est pas formellement démontrable à partir de Σ, alors Σ admet un modèle qui ne satisfait pas ϕ. Pour cela il suffit de prouver que si E est un ensemble consistant de phrases contenant toutes ses conséquences formelles, alors E admet un modèle ie est non contradictoire. Car on pourra alors prendre pour E l'ensemble fermé pour les conséquences contenant Σ et $\neg\phi$. Cet ensemble est consistant puisque ϕ n'est pas démontrable à partir de Σ et si E admet un modèle, dans celui-ci la formule ϕ n'est pas satisfaite, puisque $\neg\phi$ l'est. Voir [Cha-Keis] par exemple. □

3.2.13 Définition. — Le **cardinal d'un langage L** est le plus petit cardinal infini supérieur ou égal au cardinal de $\mathbf{L}$ (vu comme ensemble de symboles). Si l'on considère que le langage contient une quantité infinie et dénombrable de symboles de variables, on peut donc dire que le cardinal de $\mathbf{L}$ est son cardinal en tant qu'ensemble. Le cardinal de l'ensemble des formules (modulo le choix des variables, ie modulo le remplaçant des variables par d'autres) d'un langage $\mathbf{L}$ étant $\max(\mathrm{card}(\mathbf{L}), \aleph_0) = \mathrm{card}(\mathbf{L}) + \aleph_0$, il résulte de notre définition du cardinal d'un langage que celui-ci est aussi le cardinal de l'ensemble de ses formules (modulo le choix des variables). Néanmoins lorsque le langage contient un nombre fini de symboles, on voudra le souligner en s'autorisant à dire que ce langage est de cardinalité finie. Le **cardinal d'une structure** est celui de son univers.

3.2.14 Corollaire. — *La preuve du Théorème de complétude montre aussi au passage les propositions suivantes*

1. *Soit* $\mathbf{T}$ *une théorie consistante sur un langage* $\mathbf{L}$. *Alors* $\mathbf{T}$ *admet un modèle de cardinal au plus égal à celui de* $\mathbf{L} \cup \mathbb{N}$.
2. *Toute théorie consistante peut être étendue en une théorie complète sur un langage ayant les mêmes symboles de fonctions et de relations et éventuellement des constantes supplémentaires.*

Une conséquence du théorème de complétude de Gödel est le théorème de compacité. La preuve qui suit du Théorème de compacité s'appuie sur le Théorème de complétude et on montre inversement que le Théorème de de complétude est une conséquence du Théorème de compacité.

***3.2.15 Théorème* (Théorème de compacité).** — *Soit* $\mathbf{T}$ *est une théorie sur le langage* $\mathbf{L}$. *Si tout sous-ensemble fini de* $\mathbf{T}$ *possède un modèle, alors* $\mathbf{T}$ *possède un modèle.*

***3.2.16 Corollaire* (Théorème de compacité avec paramètres)**

Soit $\mathbf{T}$ *une théorie sur le langage* $\mathbf{L}$, Σ *un ensemble de formules de variables libres* $\{x_1, \cdots, x_n\}$ *et* $\Phi(x_1, \cdots, x_n)$ *une* $\mathbf{L}$*-formule quelconque. S'il n'existe pas de modèle* $\mathbf{M}$ *de* $\mathbf{T}$ *tel qu'existe* $(a_1, \cdots, a_n) \in M^n$ *vérifiant*

1. $\mathbf{M} \models \Phi(a_1, \cdots, a_n)$,
2. $\mathbf{M} \models \sigma(a_1, \cdots, a_n)$, *pour toute formule* $\sigma \in \Sigma$,

alors il existe un nombre fini de formules $\sigma_1, \cdots, \sigma_\ell \in \Sigma$ *telles que*

$$\mathbf{T} \vdash (\forall x_1, \cdots, x_n, \bigwedge_{i=1}^{\ell} \sigma_i(x_1, \cdots, x_n) \Longrightarrow \neg\Phi(x_1, \cdots, x_n)).$$

3.2.17 Remarque. — On peut considérer sur la classe des **L**-structures la topologie dont les ouverts de base sont :

$$mod(\phi) = \{\mathbf{A};\ \mathbf{A} \text{ est une } \mathbf{L}\text{-structure } \ \&\ \ \mathbf{A} \models \phi\},$$

où ϕ est une **L**-phrase. Maintenant dire que **T** est une théorie sur **L** telle que $\bigcup_{\phi\in\mathbf{T}} mod(\phi)$ est un recouvrement de la classe des **L**-structures équivaut à dire que $\bigcap_{\phi\in\mathbf{T}} mod(\neg\phi)$ est vide, ou encore que $\{\neg\phi;\ \phi \in \mathbf{T}\}$ est sans modèle. Mais d'après le théorème de compacité cela équivaut encore à dire qu'existe un sous ensemble fini $\mathbf{T}'$ de **L**-phrases de **T** tel que $\{\neg\phi;\ \phi \in \mathbf{T}'\}$ est sans modèle. Mais alors $\bigcup_{\phi\in\mathbf{T}'} mod(\phi)$ est un recouvrement fini de la classe des **L**-structures.

Preuve du théorème de compacité. — (Voir par exemple [**9**], Théorème 5.1.1) On suppose que **T** n'admet pas de modèle bien que tout sous-ensemble fini de **T** en possède un. Dans ce cas la formule $\exists x\ x \neq x$ est vraie dans tout modèle de **T**. Par le théorème de complétude de Gödel, on obtient $\mathbf{T} \vdash \exists x\ x \neq x$. Or une preuve formelle dans **L** à partir de **T** comporte un nombre fini de formules du langage et un nombre fini de phrases de **T**. En notant $\mathbf{T}'$ cet ensemble fini de **L**-formules et de phrase de **T**, $\mathbf{T}' \vdash \exists x\ x \neq x$ et ainsi l'ensemble fini $\mathbf{T}'$ ne peut avoir de modèle, mais alors il en est de même d'un sous-ensemble fini de **T**, celui qui est sous-jacent à $\mathbf{T}'$. Ce qui est contradictoire de l'hypothèse. □

Preuve du théorème de compacité avec paramètres. — Soit $\Sigma' = \{\sigma_1, \cdots, \sigma_\ell\}$ un sous-ensemble fini de formules de Σ. On note $\alpha_{\Sigma'}$ la **L**-formule

$$\forall x_1, \cdots, x_n, \bigwedge_{i=1}^{\ell} \sigma_i(x_1, \cdots, x_n) \Longrightarrow \neg\Phi(x_1, \cdots, x_n)$$

Suppsosons que la conclusion de notre Corollaire n'est pas vérifiée, alors pour tout sous-ensemble fini $\mathbf{T}'$ de **T**, on n'a pas $\mathbf{T}' \vdash \alpha_{\Sigma'}$, de sorte que la théorie $\mathbf{T}', \Sigma', \Phi$ ne permet pas de montrer $\neg\Phi$, elle est donc consistante (si elle ne l'était pas toutes les formules du langage seraient prouvable à l'aide de **T**, voir la remarque faite dans la Définition 3.2.10 de la consistance), elle admet donc un modèle d'après le Corollaire 3.2.14. Or si tout sous-ensemble fini de $\mathbf{T} \cup \Sigma \cup \{\Phi(x_1, \cdots, x_n)\}$ admet un modèle, par le théorème de compacité, $\mathbf{T} \cup \Sigma \cup \{\Phi(x_1, \cdots, x_n)\}$ admet un modèle, ce qui contredit notre hypothèse. □

Une conséquence du théorème de compacité est le théorème suivant, uitle pour produire des modèles de grande cardinalité.

***3.2.18 Théorème* (Löwenheim-Skolem).** — *Soit* $\mathbf{T}$ *une théorie sur le langage* $\mathbf{L}$ *qui admet un modèle infini. Alors pour tout cardinal* $\kappa \geq Card(\mathbf{L})$*, il existe un modèle de* $\mathbf{T}$ *de cardinal* κ*.*

Démonstration. — Soit $\mathbf{M}$ un modèle infini de $\mathbf{T}$ et M son univers. Soit κ un cardinal infini $\geq \mathrm{Card}(\mathbf{L})$ et E un ensemble disjoint de $\mathbf{L}$ de cardinal κ. On définit le langage $\mathbf{L}'$ par $\mathbf{L}$ auquel on adjoint les éléments de E, vus comme des symboles de constantes. On considère alors $\mathbf{T}' := \mathbf{T} \cup \{e_i \neq e_j, (i,j) \in E \times E, i \neq j\}$. Maintenant $\mathbf{T}'$ admet un modèle car un sous-ensemble fini de $\mathbf{T}'$ contient un nombre fini de constantes que l'on peut interpréter dans $\mathbf{M}$, puisque M est infini. Le théorème de compacité assure alors l'existence d'un modèle pour $\mathbf{T}'$. Le Corollaire 3.2.14 montre qu'existe alors un modèle $\mathbf{M}'$ de cardinalité inférieure à $\mathrm{Card}(\mathbf{L}') + \aleph_{\mathbf{0}}$. Mais ce modèle $\mathbf{M}'$ de $\mathbf{T}'$ est de cardinalité supérieure à κ, du fait que les formules $e_i \neq e_j, (i,j) \in E \times E, i \neq j$ y sont vraies. Ona donc

$$\mathrm{Card}(\mathbf{L}') \leq \kappa \leq \mathrm{Card}(\mathbf{M}') \leq \mathrm{Card}(\mathbf{L}') + \aleph_{\mathbf{0}} = \mathrm{Card}(\mathbf{L}')$$

il s'ensuit que $\mathrm{Card}(\mathbf{M}') = \kappa$ et qu'étant un modèle de $\mathbf{T}'$, $\mathbf{M}$ est aussi un modèle de $\mathbf{T}$. □

***3.2.19 Définition* (élimination des quantificateurs)**

• On dit qu'une $\mathbf{L}$-théorie $\mathbf{T}$ **élimine les quantificateurs**, si toute $\mathbf{L}$-formule est équivalente modulo $\mathbf{T}$ à une $\mathbf{L}$-formule sans quantificateur.

Précisément, étant donnée une $\mathbf{L}$-formule $\psi(x)$ (éventuellement quantifiée), il existe une $\mathbf{L}$-formule $\varphi(x)$, de même variables libres et sans quantificateur, telle que $\mathbf{T} \models \forall x(\psi(x) \longleftrightarrow \varphi(x))$, ie que l'équivalence [(1)] $\forall x(\psi(x) \longleftrightarrow \varphi(x))$ est vraie dans tous les modèles de $\mathbf{T}$.

***3.2.20 Remarque*.** — Il suffit de savoir éliminer le quantificateur existentiel d'une formule ne comportant que ce quantificateur existentiel, par récurrence sur la longueur des formules quantifiées et par le fait que $\forall x \phi(x)$ est équivalente à $\neg\exists x \neg\phi(x)$.

***3.2.21 Définition* (Sous-structure).** — Étant donné un langage $\mathbf{L}$ et deux $\mathbf{L}$-structures $\mathbf{A}$ et $\mathbf{B}$, on dit que

1. **$\mathbf{A}$ est une sous-structure de $\mathbf{B}$** si l'ensemble A sous-jacent à $\mathbf{A}$ est contenu dans l'ensemble B sous-jacent à $\mathbf{B}$ et si l'interprétation des symboles de $\mathbf{L}$ dans $\mathbf{A}$ est la restriction de l'interprétation des symboles de $\mathbf{L}$ dans $\mathbf{B}$. On note $\mathbf{A} \subset \mathbf{B}$. Par exemple $\mathbf{Z} = (\mathbb{Z}, \mathbf{0}, \mathbf{1}, +, \cdot, -)$ est une sous-structure de $\mathbf{R} = (\mathbb{R}, \mathbf{0}, \mathbf{1}, +, \cdot, -)$.
2. Lorsque $\mathbf{A} \subset \mathbf{B}$, on dit que **$\mathbf{A}$ est une sous-structure élémentaire de $\mathbf{B}$** ou que **$\mathbf{B}$ est une extension élémentaire de $\mathbf{A}$**, si pour toute formule $\phi(x_1, \cdots, x_n)$ de $\mathbf{L}$, et pour tout n-uplet $a = (a_1, \ldots, a_n) \in A^n$, on a :

$$\mathbf{A} \models \phi(a) \Longleftrightarrow \mathbf{B} \models \phi(a).$$

[(1)] L'équivalence de formules dans la stucture $\mathbf{A}$ se définit ainsi : $\psi \longleftrightarrow \varphi$ ssi $\mathbf{A} \models (\neg\varphi \vee \psi) \wedge (\varphi \vee \neg\psi)$.

On note dans ce cas : $\mathbf{A} \prec \mathbf{B}$.

3. Rappelons la Définition 3.2.7 de deux $\mathbf{L}$-structures $\mathbf{A}$ et $\mathbf{B}$ **élémentairement équivalentes** : elles satisfont les mêmes phrases du langage $\mathbf{L}$. De sorte que si $\mathbf{A}$ est une sous-structure élémentaire de $\mathbf{B}$, $\mathbf{A}$ et $\mathbf{B}$ sont élémentairement équivalentes.

3.2.22 Remarque. — Une sous-structure d'une autre n'en est pas nécessairement une sous-structure élémentaire, en effet si l'on reprend l'exemple de la sous-structure $\mathbf{Z} = (\mathbb{Z}, \mathbf{0}, \mathbf{1}, +, \cdot, -)$ de $\mathbf{R} = (\mathbb{R}, \mathbf{0}, \mathbf{1}, +, \cdot, -)$, et que l'on considère la formule ϕ donnée par $\exists x(x^2 = 2)$, celle-ci est vraie dans $\mathbf{R}$ mais pas dans $\mathbf{Z}$.

***3.2.23 Définition* (Théorie modèle-complète).** — On dit qu'une $\mathbf{L}$-théorie $\mathbf{T}$ est **modèle-complète** ssi (elle admet un modèle et) étant donnés deux modèles $\mathbf{A} \subset \mathbf{B}$ de $\mathbf{T}$ (ie $\mathbf{A}$ est une sous-structure de $\mathbf{B}$), $\mathbf{A} \prec \mathbf{B}$.

3.2.24 Remarque. — Une structure avec élimination des quantificateurs est modèle-compléte. En effet, si $\phi(x)$ est une $\mathbf{L}$-formule et si $a \in A^n$ et $\mathbf{B} \models \phi(a)$, $\phi(a)$ étant équivalente dans $\mathbf{B}$ à une formule φ sans quantificateur, on a $\mathbf{B} \models \varphi$. Mais puisque φ est sans quantificateur, on a également $\mathbf{A} \models \varphi$, et l'équivalence de $\phi(a)$ et φ étant aussi vraie dans $\mathbf{A}$ (qui est un modèle de $\mathbf{T}$), on a $\mathbf{A} \models \phi(a)$.

Un exemple de théorie modèle-complète et qui n'élimine pas les quantificateurs est donnée par la théorie $\mathbf{T}$ de la $\mathbf{L}_{rings}$-structure $\mathbb{R} = (\mathbb{R}, 0, 1, +, ., -)$. On montre que cette théorie est modèle-complète, en revanche il n'existe aucune formule sans quantificateur équivalente dans tout modèle de $\mathbf{T}$ à la formule $\phi(x) : \exists y, x = y^2$, puisqu'une telle $\mathbf{L}_{rings}$-formule sans quatificateur aurait seulement x pour variable libre et serait donc obtenue comme disjonctions de conjonctions d'égalités et de non égalités polynomiales en la variable x à coefficients entiers (1 étant sans torsion dans tout modèle de $\mathbb{R}$) qui devrait donner les réels $x \geq 0$ dans le modèle $\mathbb{R}$, ce qui ne se peut (pour voir cela on peut remarquer que si un polynôme de la seule variable X à coefficients entiers ne s'annule pas pour un élément $x = a + b\sqrt{2}$ de $\mathbb{Z}[\sqrt{2}]$, il ne s'annule pas non plus pour son conjugué $\bar{x} = a - b\sqrt{2}$. On peut alors choisir x de sorte que $x > 0$ et $\bar{x} < 0$). On verra par le Théorème de Tarski-Seidenberg que dans $\mathbf{L}_{ord}$ la théorie $\mathbf{T}'$ de $(\mathbb{R}, 0, 1, +, ., -, \geq)$ élimine les quatinficateurs et en particulier la formule $\phi(x)$ équivaut dans tout modèle de $\mathbf{T}'$ à la formule non quantifiée : $x \geq 0$. Un modèle de $\mathbf{T}'$ est **un corps réel clos**, dans lequel le *cône positif* $\{x; x \geq 0\}$ est par définition l'ensemble des carrés.

3.2.25 Remarque. — On montre que la théorie $\mathbf{T}$ est modèle-complète ssi pour toute $\mathbf{L}$-formule $\phi(x)$ existe une formule existentielle $\epsilon(x)$ (ie ne comportant que le quantificateur $\exists$) telle que : $\mathbf{T} \models \forall x(\phi(x) \longleftrightarrow \epsilon(x))$. (On peut aussi énoncer la même définition d'une théorie modèle complète en remplaçant le quantificateur existentiel par le quantificateur universel, car si $\neg\phi(x)$ est équivalente à une formule existentielle, $\phi(x)$ est équivalente à une formule universelle).

3.2.26 Définition **(Ensemble définissable dans une structure)**
On dit que $X \subset A^\ell$ est **A-définissable** s'il existe une **L**-formule $\phi(x, y)$, avec $x = (x_1, \cdots, x_\ell)$, $y = (y_{\ell+1}, \cdots, y_{\ell+k})$ et $b \in A^k$ tel que :

$$X = \{a \in A^\ell; \mathbf{A} \models \phi(a, b)\}.$$

Lorsque de plus $\phi(x, y)$ est sans quantificateur, on dit que X est **A-constructible**, ie combinaison booléenne finie d'ensembles atomiques **L**-définissables.

3.2.27 Définition **(Ensembles semi-algébriques)**. — Dans le langage $\mathbf{L}_{ord}$, les ensembles $\mathbb{R}$-constructibles sont appelés les **ensembles semi-algébriques réels**. Il s'agit des sous-ensembles de $\mathbb{R}^n$, pour un certain n, qui sont solution d'un système d'équations polynomiales et d'inéquations polynomiales strictes.

3.2.28 Remarque. —
1. Une **L**-structure admet l'**élimination des quantificateurs** ssi tout ensemble **A**-définissable est **A**-constructible ssi toute projection de constructible est constructible.
2. Une **L**-structure est **modèle-complète** sur **L** ssi tout ensemble **A**-définissable est la projection d'un **A**-constructible.

3.3. La théorie des corps réels clos

La présentation du théorème de Tarski-Seidenberg que nous donnons ici suit celle donnée dans [**5**]. Elle repose sur l'algorithme de Sturm ([Stu]), qui date de 1835 et qui permet de décider combien un polynôme réel d'une seule variable possède de racines sur un intervalle choisi (sans bien sûr les donner). Le procédé amélioré permet ensuite de décider si un polynôme réel, ou mieux un système fini d'égalités et d'inégalités polynomiales admet des solutions ; c'est ainsi que peut s'énoncer le théorème de Tarski-Seidenberg.

3.3.1. Le théorème de Sturm. — Soit un polynôme $P \in \mathbb{R}[X]$, que l'on suppose **sans racine multiple pour commencer**. Cette condition équivaut à P et son polynôme dérivé P' sont premiers entre-eux et cette condition se teste en calculant effectivement le PGCD(P, P') [(2)]

3.3.2 Exercice. — *Montrer que Q_k divise Q_0 et Q_1 et que si le polynôme D divise Q_0 et Q_1, D divise aussi Q_k, ie que PGCD(Q_0, Q_1)= Q_k.*

3.3.3 Exercice. — *Montrer que $P \in \mathbb{R}[X]$ possède une racine multiple si et seulement si PGCD(P, P') est un polynôme non constant.*

[(2)] Rappelons l'algorithme de calcul du PGCD de deux polynômes d'une variable Q_0, Q_1. On construit la suite finie de polynômes $(Q_0, Q_1, \cdots, Q_k)$ de la façon suivante : Q_0 et Q_1 sont les deux polynômes dont on veut calculer le PGCD et pour $i > 2$, Q_i est le reste de la division euclidienne de Q_{i-2} par Q_{i-1}. Cette suite est strictement décroissante en degré et si Q_k est le dernier reste non nul dans ce processus, Q_k est un PGCD de Q_0 et Q_1.

On associe à P une suite finie de polynômes $(P_0 = P, P_1 = P', \cdots, P_k)$, dite **suite de Sturm** de P et de P', de la même façon que pour le calcul du PGCD de P et de P', mais ici pour $i > 2$, P_i est *l'opposé* du reste de la division euclidienne de P_{i-2} par P_{i-1}. Cette suite est strictement décroissante en degré et P_k est le dernier reste non nul dans le processus de division.

3.3.4 Exemple. — $P(X) = P_0(X) = (X-1)(X-2)(X-3) = X^3-6X^2+11X-6$, $P'(X) = P_1(X) = 3X^2 - 12X + 11$, $P_2(X) = \mathbf{D}\frac{2}{3}X - \frac{4}{3}$, $P_3(X) = 1$.

Soit $s_P(a)$ le nombre de changements de signe dans la suite $(P_0(a), P_1(a), \cdots, P_k(a))$, lorsque a n'est pas une racine de P (l'apparition d'un zéro ne comptant pas comme un changement de signe).

3.3.5 Exemple. — Pour P donné dans l'exemple 1, $s_P(-1)$ est 3, puisque :

$$P_0(-1) = -24, P_1(-1) = 26, P_2(-1) = -2, P_3(-1) = 1,$$

et $s_P(4)$ est 0, puisque :

$$P_0(4) = 6, P_1(4) = 11, P_2(4) = 4/3, P_3(4) = 1.$$

Regardons maintenant la variation de la fonction $s_P : \mathbb{R} \setminus \mathcal{R} \to \mathbb{N}$, $\mathcal{R}$ étant l'ensemble des racines de P. L'entier $s_P(x)$ ne varie qu'au passage d'une racine d'un des polynômes P_i.

3.3.6. Comportement des signes de $P_0(x)$ et $P_1(x)$ lorsque x passe une racine r de $P_0 = P$. — Dans ce cas $P_1(r) = P'(r) \neq 0$, puisque r n'est pas une racine multiple de P. La fonction $P'(x)$ garde ainsi une signe constant en passant r, ce qui oblige $P(x)$ à en changer. Les deux premiers termes P_0 et P_1 de la suite de Sturm de P ont des signes opposés avant le passage de r, et identiques après, comme résumé par les tableaux de variations suivants

x		r		x		r	
$sgn(P_0(x))$	$-$	0	$+$	$sgn(P_0(x))$	$+$	0	$-$
$sgn(P_1(x))$	$+$	$+$	$+$	$sgn(P_1(x))$	$-$	$-$	$-$

3.3.7. Comportement des signes de $P_{i-1}(x), P_i(x)$ et $P_{i+1}(x)$ lorsque x passe une racine r de P_i, pour $i > 0$.— Notons que $P_i(r) = 0$ implique que $P_{i-1}(r) \neq 0$ et $P_{i+1}(r) \neq 0$, car en remontant les égalités $P_{i-1}(r) = P_i(r) = 0$ jusqu'à $P_0(r) = P_1(r) = 0$, on aurait une contradiction. D'autre part, puisque $P_{i-1}(r) = P_i(r) \times Q_i(r) - P_{i+1}(r) = -P_{i+1}(r)$, au voisinage de r les signes de $P_{i-1}(x)$ et $P_i(x)$ sont opposés. En conclusion quelle que soit la variation de signe de P_i au passage de r, le nombre de changements de signe dans la sous-suite $(P_{i-1}(x), P_i(x), P_{i+1})$ de la suite de Sturm est le même avant et après r, comme résumé (par exemple) dans les

tableaux suivants de changement de signes :

x		r		x		r	
$sgn(P_{i-1}(x))$	$+$	$+$	$+$	$sgn(P_{i-1}(x))$	$-$	$-$	$-$
$sgn(P_i(x))$	$+$	0	$+$	$sgn(P_i(x))$	$-$	0	$+$
$sgn(P_{i+1}(x))$	$-$	$-$	$-$	$sgn(P_{i+1}(x))$	$+$	$+$	$+$

On a donc démontré que $s_P(x)$ ne varie qu'au passage d'une racine de P et qu'au passage de chaque racine de P, $s_P(x)$ diminue d'exactement une unité, d'où le résultat suivant

3.3.8 Lemme. — *Soient $P \in \mathbb{R}[X]$ sans racine réelle multiple et $a < b$ deux réels qui ne sont pas des racines de P. Le nombre de racines réelles de P sur $[a, b]$ est $s_P(a) - s_P(b)$.*

3.3.9 Exemple. — Pour P donné dans l'exemple 1, le nombre de racines de P dans $[-1, 4]$ est $s_P(-1) - s_P(4) = 3 - 0 = 3$.

Considérons maintenant le cas général où P n'est pas nécessairement sans racine multiple. Dans la suite de Sturm de P, le dernier polynôme non nul P_k est un PGCD de P et de P' et n'est pas nécessairement une constante mais divise tous les polynômes P_i. Les racines du polynôme P_0/P_k sont celles de P_0, puisque P_k est un PGCD de P et de P'. La suite de polynômes $(P_0/P_k, P_1/P_k, \cdots, P_{k-1}/P_k, 1)$ est alors telle que :

- Au passage d'une racine de P, le produit $\mathbf{D}\frac{P_0}{P_k}\frac{P_1}{P_k} = \frac{P_0P_1}{P_k^2}$ change de signe comme P_0P_1, ie une fois en décroissant (faire le tableau lorsque $P(r) = P'(r) = 0$!).

- Si r est une racine de $\mathbf{D}\frac{P_i}{P_k}$, pour $i > 0$, $P_{i-1}(r)P_{i+1}(r) \neq 0$, car P_0/P_k et P_1/P_k n'ont pas de racine commune et $P_{i-1}/P_k(r) \cdot P_{i+1}/P_k(r) < 0$, pour les mêmes raisons que dans le cas où P_0 et P_1 sont premiers entre-eux.

Ainsi en notant $S_P(a)$ le nombre de changements de signe de la suite

$$(P_0/P_k(a), P_1/P_k(a), \cdots, P_{k-1}/P_k(a), 1),$$

pour a non racine de P, la différence $S_P(a) - S_P(b)$ est le nombre de racines de P dans $[a, b]$. Mais puisque le nombre de changements de signe de la suite

$$(P_0/P_k(a), P_1/P_k(a), \cdots, P_{k-1}/P_k(a), 1)$$

est bien sûr celui de la suite $(P_0(a), P_1(a), \cdots, P_k(a))$, on a démontré :

***3.3.10 Théorème* (Sturm)**. — *Soient $P \in \mathbb{R}[X]$ et $a < b$ deux réels qui ne sont pas des racines de P. Le nombre de racines réelles de P sur $[a, b]$ est $s_P(a) - s_P(b)$.*

3.3.11 Corollaire. — *Soient $P \in \mathbb{R}[X]$. Le nombre de racines réelles de P est $s_P(-\infty) - s_P(+\infty)$, où $s_P(-\infty)$ est le nombre de changement de signe dans la suite des coefficients directeurs de la suite de Sturm $(P_0(X), P_1(X), \cdots, P_k(X))$ de P, et $s_P(-\infty)$ est le nombre de changements de signe dans la suite des coefficients directeurs de la suite $(P_0(-X), P_1(-X), \cdots, P_k(-X))$.*

Démonstration. — Puisque le nombre de racines de P est fini, il existe $a \in \mathbb{R}$ tel que sur $]-\infty, a[$, $x \mapsto s_P(x)$ est constant, puisque $s_P(x)$ ne change qu'au passage d'une racine de P. De même il existe $b \in \mathbb{R}$ tel que sur $]b, +\infty[$, $x \mapsto s_P(x)$ est constant. La quantité $s_P(a) - s_P(b)$ mesurant le nombre de racines réelles de P sur $[a, b]$, $s_P(a) - s_P(b)$ est le nombre de racines réelles de P sur $\mathbb{R}$ tout entier. Quitte à augmenter $|a|$ et $|b|$, on peut supposer que le signe des P_i ne change plus sur $]-\infty, a]$ et $]b, +\infty]$. Dans ces conditions le signe de $P_i(x)$, $x \in]-\infty, a]$, est égal au signe du coefficient directeur de $P_i(-X)$ et le signe de $P_i(x)$, $x \in [b, +\infty[$, est égal au signe du coefficient directeur de $P_i(X)$. Ainsi $s_P(a)$ est le nombre de changements de signe dans $(P_0(-X), P_1(-X), \cdots, P_k(-X))$ ie $s_P(-\infty)$ et $s_P(b)$ est le nombre de changements de signe dans $(P_0(X), P_1(X), \cdots, P_k(X))$ ie $s_P(+\infty)$. □

3.3.12. Systèmes d'équations et d'inéquations polynomiales.— On va montrer que l'on peut décider après calculs si un tel système admet des solutions et calculer ce nombre s'il est fini. Pour cela on peut encore calculer des changements de signe dans des suites de Sturm bien choisies.

3.3.13. On commence par calculer le nombre de solutions du système particulier suivant qui ne comporte qu'une seule équation et une seule inéquation :

$$(S) \ : \ P = 0, \ Q > 0,$$

où $P, Q \in \mathbb{R}[X]$. Construisons pour cela la suite de Sturm $(P_0, P_1, \cdots, P_k)$ de $P_0 = P$ et $P_1 = P'Q$. Si a n'est pas une racine réelle de P, on note $s_{P,Q}(a)$ le nombre de changements de signe dans la suite $(P_0(a), P_1(a), \cdots, P_k(a))$. Regardons la variation de $s_{P,Q}(x)$ au passage des racines r de P, en fonction du signe de $Q(r)$.

• Si P et $P'Q$ sont premiers entre-eux (ie si P_k est constant non nul),

- Une racine de P n'est ni racine de P', ni racine de Q, de sorte que le signe de $P_1 = P'Q$ est constant au voisinage de r, tandis que celui de $P_0 = P$ change nécessairement, suivant les tableaux ci-dessous.

Quand $Q > 0$ au voisinage de r :

x		r		x		r	
$sgn(P_0(x))$	$-$	0	$+$	$sgn(P_0(x))$	$+$	0	$-$
$sgn(P'(x))$	$+$	$+$	$+$	$sgn(P'(x))$	$-$	$-$	$-$
$sgn(P'Q(x))$	$+$	$+$	$+$	$sgn(P'Q(x))$	$-$	$-$	$-$

Quand $Q < 0$ au voisinage de r :

x		r		x		r	
$sgn(P_0(x))$	$-$	0	$+$	$sgn(P_0(x))$	$+$	0	$-$
$sgn(P'(x))$	$+$	$+$	$+$	$sgn(P'(x))$	$-$	$-$	$-$
$sgn(P'Q(x))$	$-$	$-$	$-$	$sgn(P'Q(x))$	$+$	$+$	$+$

- Si r est une racine de P_i, pour $i > 0$, comme P_0 et P_1 sont supposés sans racine commune, $P_{i-1}(r) \neq 0$ et $P_{i+1}(r) \neq 0$ et le nombre de changements de signe dans la sous-suite $P_{i-1}(x), P_i(x), P_{i+1}(x)$ est le même avant et après r.

En conclusion la variation de $s_{P,Q}(x)$ n'a lieu qu'au passage des racines de P, et $s_{P,Q}(x)$ décroît d'une unité au passage d'une racine r de P telle $Q(r) > 0$, tandis que $s_{P,Q}(x)$ croît d'une unité au passage d'une racine r de P telle $Q(r) < 0$. Il s'ensuit que $s_{P,Q}(a) - s_{P,Q}(b)$, lorsque a et b ne sont pas des racines de P, est le nombre de racines réelles r de P sur $[a, b]$ telles que $Q(r) > 0$ privé du nombre de racines réelles r de P sur $[a, b]$ telles que $Q(r) < 0$.

• Dans le cas où P et $P'Q$ ne sont pas premiers entre-eux, et où leur suite de Sturm $(P_0, P_1, \cdots, P_k)$ se termine par P_k non constant, on considère la suite de Sturm :

$$(P_0/P_k, P1/P_k = P'Q/P_k, \cdots, P_{k-1}/P_k, 1)$$

et $S_{P,Q}(x)$ le nombre de changements de signe en x dans cette suite, x non racine de P. Celui-ci est le même que dans $(P_0, P_1, \cdots, P_k)$. La quantité $S_{P,Q}(a) - S_{P,Q}(b)$ est donc $s_{P,Q}(a) - s_{P,Q}(b)$. Comme $S_{P,Q}(x)$ ne varie qu'au passage des racines de P et non de P_i, $i > 0$, et que cette variation du nombre de changements de signes dans la suite $(P_0/P_k, P1/P_k, \cdots, P_{k-1}/P_k, 1)$ au passage d'une racine r de P décroît d'une unité quand $Q(r) > 0$ et croît d'une unité lorsque $Q(r) < 0$ (faire le tableau !), $S_{P,Q}(a) - S_{P,Q}(b)$ mesure le nombre p de racines de P sur $[a, b]$ en lesquelles Q est > 0 privé du nombre n de racines de P sur $[a, b]$ en lesquelles Q est < 0.

Enfin notons que d'après ce qui précède, $s_{P,Q^2}(a) - s_{P,Q^2}(b)$ est le nombre $n+p$ de racines rélles de P qui ne sont pas racines de Q. Donc $s_{P,Q}(a) - s_{P,Q}(b) + s_{P,Q^2}(a) - s_{P,Q^2}(b) = 2p$, ie deux fois le nombre de racines de P en lesquelles Q est > 0.

On résume tout ceci par :

3.3.14 Théorème. — *Soient $P, Q \in \mathbb{R}[X]$ et $a < b$ deux réels qui ne sont pas des racines de P. Soit p le nombre de racines réelles r de P sur $[a, b]$ telles que $Q(r) > 0$ et n le nombre de racines réelles r de P sur $[a, b]$ telles que $Q(r) < 0$. Alors :*

1. $p - n = s_{P,Q}(a) - s_{P,Q}(b)$.
2. $p = \mathbf{D}\frac{1}{2}[s_{P,Q}(a) - s_{P,Q}(b) + s_{P,Q^2}(a) - s_{P,Q^2}(b)]$.

Soit π le nombre de racines réelles r de P sur $\mathbb{R}$ telles que $Q(r) > 0$ et ν le nombre de racines réelles r de P sur $\mathbb{R}$ telles que $Q(r) < 0$. Notons $s_{P,Q}(-\infty)$ le nombre de changements de signe dans la suite des coefficients directeurs de la suite de Sturm de P et $P'Q$, où $-X$ est substitué à X, $s_{P,Q}(+\infty)$ le nombre de changements de signe dans la suite des coefficients directeurs de la suite de Sturm de P et $P'Q$. Alors :

1. $\pi - \nu = s_{P,Q}(-\infty) - s_{P,Q}(+\infty)$.
2. $\pi = \mathbf{D}\frac{1}{2}[s_{P,Q}(-\infty) - s_{P,Q}(+\infty) + s_{P,Q^2}(-\infty) - s_{P,Q^2}(+\infty)]$.

3.3.15. On en vient maintenant au cas général. Soit (S) un système d'égalités et d'inégalités polynomiales :

$$(S) \ : \ R_1 = 0, \cdots, R_m = 0, \ Q_1 \ ? \ 0, \cdots, Q_\ell \ ? \ 0$$

où $m, \ell \in \mathbb{N}$, $R_1, \cdots, R_m, \ Q_1, \cdots, Q_\ell \in \mathbb{R}[X]$ et où le symbole ? est un des symboles $<, >, \leq, \geq$. On cherche une procédure pour décider si ce système admet des solutions.

• On va dans un premier temps se ramener à un système où ? est $>$ et où $m = 1$, avec $R_1 \not\equiv 0$.

Tout d'abord on observe que dans (S) on peut supposer que ? est le symbole $>$ ou le symbole $\geq$, quitte à multiplier Q_i par -1. Ensuite on remarque x est une solution du système $Q \geq 0$ ssi x est une solution d'un des deux systèmes $Q > 0$ ou $Q = 0$, de sorte que décider si $Q \geq 0$ a des solutions revient à décider si $Q > 0$ ou $Q = 0$ a des solutions. Quitte à considerer plus de systèmes, on suppose donc que ? est le symbole $>$. On peut supposer que $m = 0$ ou $m = 1$, car si $m > 0$, en posant $P = R_1^2 + \cdots + R_m^2$, on obtient le système équivalent :

$$(\Sigma) \ : \ P = 0, \ Q_1 > 0, \cdots, Q_\ell > 0$$

Enfin si le système est $Q_1 > 0, \cdots, Q_\ell > 0$, ie si $P \equiv 0$, l'ensemble des solutions est un ouvert de $\mathbb{R}$ (réunion finie d'intervalles ouverts), qui est soit vide, soit de cardinal infini. On ne peut plus compter dans le dernier cas le nombre de solutions, mais on va déterminer si le système possède bien des solutions. On commence par décider si le système admet des solutions sur des intervalles du type $]-\infty, a]$ (resp. $[b, +\infty[$). Il suffit pour cela que les signes des coefficients directeurs des $Q_i(-X)$ (resp. des $Q_i(X)$) soient tous positifs. Dans ce cas inutile de pousser plus loin les calculs pour décider si le système admet des solutions. Si le système n'admet pas de solution à l'infini et que de plus $Q = Q_1 \cdots Q_\ell$ a moins d'une racine, le système n'admet pas de solution sur $\mathbb{R}$. En revanche si Q possède deux racines a et b distinctes, par le théorème de Rolle, $Q' = 0$ admet nécessairement une solution sur $[a, b]$ et le système : $Q_1 > 0, \cdots, Q_\ell > 0$ a un ensemble de solutions non vide ssi tel est le cas pour le système : $Q' = 0, Q_1 > 0, \cdots, Q_\ell > 0$.

• On suppose maintenant que notre système est du type de (Σ) et on va montrer comment à partir du Théorème 1.4 on peut compter ses solutions.

Pour $\mu = (\mu_1, \cdots, \mu_\ell) \in \{0,1\}^\ell$, on note $s^\mu = s_{P,Q^\mu}(-\infty) - s_{P,Q^\mu}(+\infty)$, avec $Q^\mu = Q_1^{2-\mu_1} \cdots Q_\ell^{2-\mu_\ell}$. La quantité s^μ est le nombre de solutions sur $\mathbb{R}$ du système $P = 0, Q^\mu > 0$ moins le nombre de solutions du système $P = 0, Q^\mu < 0$. On sait d'après le Théorème 1.4 calculer s^μ . On va montrer par récurrence sur ℓ une formule donnant le nombre de solutions σ^μ du système $P = 0, (-1)^{\mu_1} Q_1 > 0, \cdots, (-1)^{\mu_\ell} Q_\ell > 0$, pour tout $\mu \in \{0,1\}^\ell$, en fonction des s^μ, $\mu \in \{0,1\}^\ell$. On pourra alors calculer $\sigma^{(0,\cdots,0)}$ qui est le nombre de solutions de Σ, à l'aide des quantités $(s^\mu)_{\mu \in \{0,1\}^\ell}$ (les étages de cette colonne sont ordonnés par l'ordre lexicographique). Dans ce qui suit $\{r\}$ désigne l'ensemble des racines réelles de P et $\#$ le cardinal.

- Lorsque $\ell = 1$, on a $s^0 = \#\{r; Q_1^2(r) > 0\} - \#\{r; Q_1^2(r) < 0\}$ ie que $s^0 = \#\{r; Q_1(r) \neq 0\}$ et $s^1 = \#\{r; Q_1(r) > 0\} - \#\{r; Q_1(r) < 0\}$. D'autre part $\sigma^0 = \#\{r; Q_1(r) > 0\}$ et $\sigma^1 = \#\{r; Q_1(r) < 0\}$. Il s'ensuit que :

$$s^0 = \sigma^0 + \sigma^1, \ s^1 = \sigma^0 - \sigma^1.$$

En notant $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, on a :

$$\begin{pmatrix} s^0 \\ s^1 \end{pmatrix} = A_1 \begin{pmatrix} \sigma^0 \\ \sigma^1 \end{pmatrix}$$

Noter que A_1 est inversible, ce qui donne bien σ^0 et σ^1 en fonction de s^0 et s^1.

- Lorsque $\ell = 2$, on a :
$s^{(0,0)} = \#\{r; Q_1^2(r)Q_2^2(r) > 0\} - \#\{r; Q_1^2(r)Q_2^2(r) < 0\} = \#\{r; Q_1(r)Q_2(r) \neq 0\}$,

$$\begin{aligned} s^{(0,1)} &= \#\{r; Q_1^2(r)Q_2(r) > 0\} - \#\{r; Q_1^2(r)Q_2(r) < 0\} \\ &= \#\{r; Q_1(r) \neq 0, Q_2(r) > 0\} - \#\{r; Q_1(r) \neq 0, Q_2(r) < 0\}, \\ s^{(1,0)} &= \#\{r; Q_1(r)Q_2^2(r) > 0\} - \#\{r; Q_1(r)Q_2^2(r) < 0\} \\ &= \#\{r; Q_2(r) \neq 0, Q_1(r) > 0\} - \#\{r; Q_2(r) \neq 0, Q_1(r) < 0\}, \\ s^{(1,1)} &= \#\{r; Q_1(r)Q_2(r) > 0\} - \#\{r; Q_1(r)Q_2(r) < 0\}. \end{aligned}$$

Puis on a :
$\sigma^{0,0} = \#\{r; Q_1(r) > 0, Q_2(r) > 0\}$, $\sigma^{0,1} = \#\{r; Q_1(r) > 0, Q_2(r) < 0\}$,
$\sigma^{1,0} = \#\{r; Q_1(r) < 0, Q_2(r) > 0\}$, $\sigma^{1,1} = \#\{r; Q_1(r) < 0, Q_2(r) < 0\}$.
Il s'ensuit que :

$$\begin{pmatrix} \\ s^\mu \end{pmatrix} = \begin{pmatrix} A_1 & A_1 \\ A_1 & -A_1 \end{pmatrix} \begin{pmatrix} \\ \sigma^\mu \end{pmatrix}.$$

Noter que $A_2 = \begin{pmatrix} A_1 & A_1 \\ A_1 & -A_1 \end{pmatrix}$ est inversible, d'inverse $\mathbf{D}\frac{1}{2} \begin{pmatrix} A_1^{-1} & A_1^{-1} \\ A_1^{-1} & -A_1^{-1} \end{pmatrix}$.

- Supposons que pour $\ell \geq 2$, $(s^\mu) = A_\ell(\sigma^\mu)$, avec A_ℓ une matrice inversible. on montre qu'alors :

$$\begin{pmatrix} \vdots \\ s^{\mu,0} \\ \vdots \\ s^{\mu,1} \\ \vdots \end{pmatrix} = \begin{pmatrix} A_\ell & A_\ell \\ A_\ell & -A_\ell \end{pmatrix} \begin{pmatrix} \vdots \\ \sigma^{\mu,0} \\ \vdots \\ \sigma^{\mu,1} \\ \vdots \end{pmatrix}$$

et on remarque que $A_{\ell+1} = \begin{pmatrix} A_\ell & A_\ell \\ A_\ell & -A_\ell \end{pmatrix}$ est inversible, d'inverse $\mathbf{D}\frac{1}{2} \begin{pmatrix} A_\ell^{-1} & A_\ell^{-1} \\ A_\ell^{-1} & -A_\ell^{-1} \end{pmatrix}$.

Conclusion. *On a démontré qu'il existe un processus calculatoire pour décider si un système général contenant un nombre fini d'équations et d'inéquations polynomiales admet des solutions et calculer leur nombre lorsque celui-ci est fini, ie lorsque le système possède au moins une équation.*

3.3.16. Le théorème de Tarski-Seidenberg. — On en vient maintenant au but de ce chapitre, la démonstration du théorème de Tarski-Seidenberg qui possède deux interprétations : les ensembles semi-algébriques de $\mathbb{R}^n$ sont stables par projection ou bien la théorie des corps réels clos élimine les quantificateurs.

***3.3.17 Théorème* (Tarski-Seidenberg).** — *Soient n et $m > 0$ deux entiers naturels et*

$$S_1(T, X), \cdots, S_m(T, X)$$

des polynômes réels en $T = (T_1, \cdots, T_n)$ et X. On note $(S(T, X))$ le système :

$$(S(T, X)) \ : \ S_i(T, X) \ ?_i \ 0,$$

où $?_i \in \{=, >\}$, $i \in \{1, \cdots, m\}$. *Il existe alors un nombre fini de systèmes d'équations et d'inéquations polynomiales en* T, $R^1(T), \cdots, R^k(T)$, *tels que quel que soit* $t \in \mathbb{R}^n$, *le système* $S(t, X)$ *d'inconnu* X *possède (au moins) une solution ssi un des systèmes* $R^j(t)$ *est satisfait. En résumé :*

$$\exists X \ S(t, X) \Longleftrightarrow R_1(t) \ \vee \ \cdots \ \vee \ R_k(t).$$

Démonstration. — On calcule les suites de Sturm nécessaires dans le processus de décision de l'existence de solutions du système $S(T, X)$, d'inconnue X. Ce calcul se fait dans $\mathbb{R}(T)[X]$, ie en considérant que X est la variable des polynômes et que leurs coefficents sont dans le corps des fractions rationnelles en T. On divise à chaque étape en deux le processus en fonction de la nullité ou non des coefficients directeurs de chaque polynôme qui apparaît dans ce calcul. Ces coefficients sont des fractions rationnelles en T, mais leur signe qui donne l'existence à la fin du processus (et parfois le nombre, quand celui-ci est fini) de racines étant aussi celui du produit du numérateur par le dénominateur, on aboutit à des systèmes polynomiaux d'équations et d'inéquations $R_j(t) \ !_j \ = 0, j \in \{1, \cdots, k\}$, $!_j \in \{=, >\}$ qui déterminent si $S(t, X)$ possède une solution. □

3.3.18 Exemple. — $S(T_1, T_2, X) \ : \ T_1X^2 + T_2X + T_3 = 0$.

Notons $P_0(T, X) = T_1X^2 + T_2X + T_3$.

(*a*) Si $T_1 \neq 0$, $P_1(T, X) = \mathbf{D}\frac{d}{dX}P_0(T, X) = 2T_1X + T_2$ et $P_2(T, X) = \mathbf{D}\frac{T_2^2 - 4T_1T_3}{4T_1}$.

(*a′*) Supposons $\mathbf{D}\frac{T_2^2 - 4T_1T_3}{4T_1} \neq 0$.

En fonction des signes de T_1 et de $T_1(T_2^2 - 4T_1T_3)$, on calcule $s_{P_0}(-\infty) - s_{P_0}(+\infty)$, qui donne le nombre de solutions de $S(T, X)$ en X.

$sign(T_2^2 - 4T_1T_3)$	+	−	+	−	$sign(T_2^2 - 4T_1T_3)$	+	−	+	−
$P_0 : sign(T_1)$	+	+	−	−	$P_0 : sign(T_1)$	+	+	−	−
$P_1 : sign(-2T_1)$	−	−	+	+	$P_1 : sign(2T_1)$	+	+	−	−
$P_2 : sign(\mathbf{D}\frac{T_2^2 - 4T_1T_3}{4T_1})$	+	−	−	+	$P_2 : sign(\mathbf{D}\frac{T_2^2 - 4T_1T_3}{4T_1})$	+	−	−	+
$s_{P_0}(-\infty)$	2	1	2	1	$s_{P_0}(+\infty)$	0	1	0	1

Ce qui donne : $s_{P_0}(-\infty) - s_{P_0}(+\infty) = 2 > 0$ ssi $T_2^2 - 4T_1T_3 > 0$. Donc :

$$T_1 \neq 0, T_2^2 - 4T_1T_3 > 0 \Longrightarrow S(T, X) \text{ a des solutions}$$

$$T_1 \neq 0, T_2^2 - 4T_1T_3 < 0 \Longrightarrow S(T, X) \text{ n'a pas de solution}$$

(*a″*) Supposons $\mathbf{D}\frac{T_2^2 - 4T_1T_3}{4T_1} = 0$. Alors la suite de Sturm est (P_0, P_1) et :

$P_0 : sign(T_1)$	+	−	$P_0 : sign(T_1)$	+	+
$P_1 : sign(-2T_1)$	−	+	$P_1 : sign(2T_1)$	+	+
$s_{P_0}(-\infty)$	1	1	$s_{P_0}(+\infty)$	0	0

Ce qui donne : $s_{P_0}(-\infty) - s_{P_0}(+\infty) = 1 > 0$ ssi $T_2^2 - 4T_1T_3 = 0$. Donc :

$$T_1 \neq 0, T_2^2 - 4T_1T_3 = 0 \Longrightarrow S(T, X) \text{ a des solutions}$$

(b) Si $T_1 = 0$, $P_0(X) = T_2X + T_3$ et $P_1(T, X) = \mathbf{D}\frac{d}{dX}P_0(T, X) = T_2$.
(b') Supposons $T_2 \neq 0$. Alors la suite de Sturm est (P_0, P_1) et :

$P_0 : sign(-T_2)$	$-$	$+$	$P_0 : sign(T_2)$	$+$	$+$
$P_1 : sign(T_2)$	$+$	$-$	$P_1 : sign(T_2)$	$+$	$+$
$s_{P_0}(-\infty)$	1	1	$s_{P_0}(+\infty)$	0	0

Ce qui donne : $s_{P_0}(-\infty) - s_{P_0}(+\infty) = 1 > 0$. Donc :

$$T_1 = 0, T_2 \neq 0 \Longrightarrow S(T, X) \text{ a des solutions}$$

(b'') Supposons $T_2 = 0$. Alors $S(T, X)$ est T_3. Donc :

$$T_1 = 0, T_2 = 0, T_3 = 0 \Longrightarrow S(T, X) \text{ a des solutions}$$

$$T_1 = 0, T_2 = 0, T_3 \neq 0 \Longrightarrow S(T, X) \text{ n'a pas de solutions}$$

Tous les cas étant couverts, on a :

$$\exists X \; S(T, X) \Longleftrightarrow$$

$$\begin{array}{ll} & T_1 \neq 0, T_2^2 - 4T_1T_3 \geq 0 \\ \vee & T_1 = 0, T_2 \neq 0 \\ \vee & T_1 = 0, T_2 = 0, T_3 = 0 \end{array}$$

3.3.19 Exemple **(Interprétation géométrique pour l'équation $P(X) = 0$)**
Considérons le cas particulier où $T_1 = 1$ et notons $T_2 = b, T_3 = c$. Nous avons trouvé ci-dessus des conditions polynomiales sur b et c pour que le système polynomial $S(b, c, X) : P_{b,c} = X^2 + bX + c = 0$ ait des solutions x.
Considérons maintenant dans $\mathbb{R}^3$, de coordonnées (b, c, x), l'ensemble :

$$S = \{(b, c, x) \in \mathbb{R}^3; P_{a,b}(x) = 0\}.$$

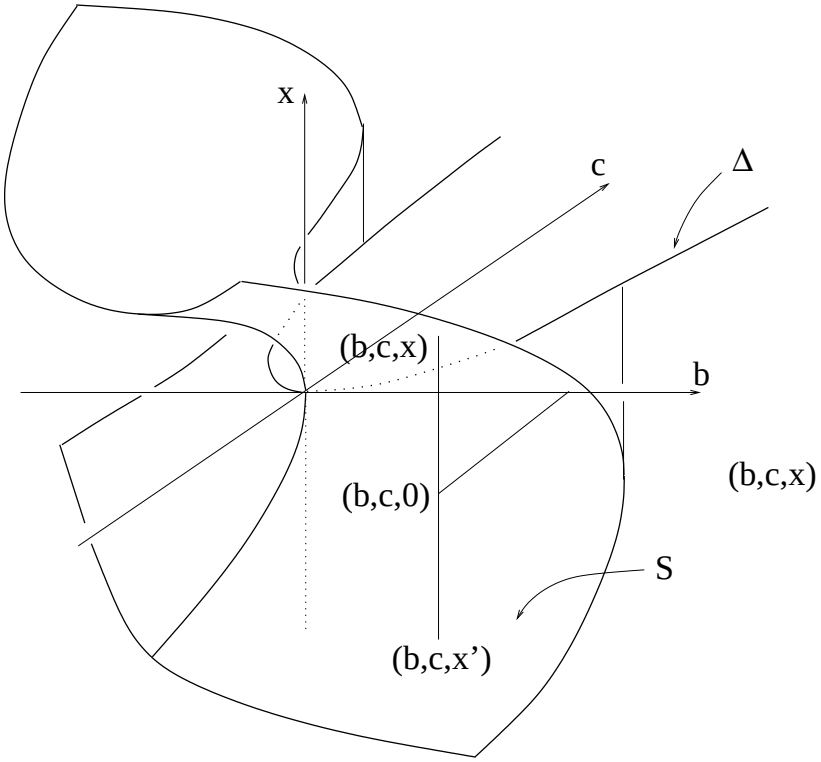


Fig. 1

Étant donné $(b, c) \in \mathbb{R}^2$, x est une racine de $P_{b,c}(X)$ ssi $(b, c, x) \in S$, autrement dit ssi $(b, c, 0)$ est un point de $\mathbb{R}^2 \times \{0\}$ qui appartient au projeté de S sur $\mathbb{R}^2 \times \{0\}$. Soit maintenant $(b, c, x) \in S$.

- Supposons que x soit la seule racine réelle de $P_{b,c}(X)$. D'après le théorème des fonctions implicites, si $\dfrac{\partial P_{b,c}(X)}{\partial X}(b, c, x) = 2x + b \neq 0$, il existe une voisinage $U_{b,c}$ de $(b, c, 0)$ dans $\mathbb{R}^2 \times \{0\}$, un voisinage V_x de x dans $\{0\}^2 \times \mathbb{R}$ et une fonction $\mathcal{C}^\infty$, $\phi : U_{b,c} \to \mathbb{R}$ tels que $S \cap (U_{b,c} \times V_x)$ est le graphe de ϕ au-dessus de $U_{b,c}$. Notons qu'il n'est pas possible que pour $(\beta, \gamma, 0) \in U_{b,c}$ arbitrairement proche de $(b, c, 0)$ et différent de $(b, c, 0)$, $P_{\beta,\gamma}(X)$ ait une racine y telle que $(\beta, \gamma, y) \notin U_{b,c} \times V_x$. En effet, tout d'abord si une suite (β_n, γ_n, y_n) est telle que $(\beta_n, \gamma_n) \to (b, c) \in \mathbb{R}^2$ et $P_{\beta_n,\gamma_n}(y_n) = 0$, on ne peut avoir $|y_n| \to \infty$. Soit alors une suite (β_n, γ_n, y_n) telle que $(\beta_n, \gamma_n) \to (b, c)$, $P_{\beta_n,\gamma_n}(y_n) = 0$, $y_n \in U_{b,c} \times V_x$ et $y_n \to y$ (quitte à extraire une sous-suite convergente de celle-ci). Par continuité y serait alors une racine de $P_{b,c}$ distincte de x, ce qui contredit notre hypothèse.

Les racines y de $P_{\beta,\gamma}(X) = 0$ pour $(\beta, \gamma, 0) \in U_{b,c}$ sont donc toutes données par $y = \phi(\beta, \gamma)$.

- De même, si $P_{b,c}(X)$ possède deux racines distinctes x et x', en lesquelles $\frac{\partial P_{b,c}(X)}{\partial X}(b,c,x) = 2x + b \neq 0$ et $\frac{\partial P_{b,c}(X)}{\partial X}(b,c,x') = 2x + b \neq 0$, on en déduit l'existence de voisinages V_x et $V_{x'}$ respectivement de x et x' dans $\mathbb{R}$, que l'on peut supposer disjoints quitte à les restreindre, puisque $x \neq x'$ et des voisinages $U_{b,c}$ et $U'_{b,c}$ de $(b,c,0)$ dans $\mathbb{R}^2$ tels que, en notant $U = U_{b,c} \cap U'_{b,c}$, les racines de $P_{\beta,\gamma}(X)$ pour $(\beta,\gamma,0) \in U$ sont donnés par deux graphes $\phi : U \to V_x$ et $\psi : U \to V_{x'}$.

- Si (b,c) est tel que $P_{b,c}(X)$ n'a pas de racine réelle, pour (β,γ) dans un voisinage de (b,c), $P_{\beta,\gamma}(X)$ ne peut pas non plus posséder de racines rélles, par le même argument de continuité que ci-dessus.

En conclusion le théorème des fonctions implicites montre que le nombre de racines de $P_{b,c}(X)$ est localement constant sur le complémentaire de l'ensemble de paramètres $\Delta \subset \mathbb{R}^2 \times \{0\}$, Δ défini par $x = -b/2$ et $P_{b,c}(x) = 0$ (ce qui donne $\Delta = \{(b,c,0); b^2 - 4c = 0\}$). Sur les composantes connexes de $(\mathbb{R}^2 \times \{0\}) \setminus \Delta$, le nombre de racines de $P_{b,c}(X)$ est donc constant et les racines sont des fonctions $\mathcal{C}^\infty$ des paramètres b, c.

On appelle Δ le discriminant de $P_{b,c}(X)$. Le théorème de Sturm met en évidence Δ et en donne, comme le théorème des fonctions implicites un équation polynomiale. De plus le théorème de Sturm met en évidence les composantes connexes du complémentaire de Δ par des inéquations polynomiales.

Les ensembles S et Δ sont représentés sur la figure 1.

On vient de voir que le théorème de Tarski-Seidenberg assure que le projeté d'un ensemble semi-algébrique est un semi-algébrique. Mais ce qui est utilisé dans la preuve du théorème est la possibilité d'"éliminer le quantificateur $\exists$" dans les formules quantifiées définies à partir d'un semi-algébrique. Précisément on énonce :

3.3.20 Théorème **(Tarski-Seidenberg forme logique)**
Soit Φ une formule logique (ie du premier ordre dans $\mathbf{L}_{ord}$ mais sans quantificateurs, ne faisant intervenir que des polynômes réels en les variables $X_1, \cdots, X_{n+m}$, les signes $= 0$, > 0 et les symboles $\vee$, $\neg$, $\wedge$). Les $(x_1, \cdots, x_n) \in \mathbb{R}^n$ qui vérifient une formule quantifiée du type :

$$!_1 x_{n+1}, \cdots, !_m x_{n+m}\ \Phi(x_1, \cdots x_n, x_{n+1}, \cdots x_{n+m}),$$

où $!_j$ est le quantificateur $\exists$ ou bien le quantificateur $\forall$, $j = 1, \cdots, m$, définissent aussi un semi-algébrique de $\mathbb{R}^n$. Autrement dit les $\mathbf{R}$-définissables sont les $\mathbf{R}$-constructibles, ou encore $\mathbf{R}$ est à élimination des quantificateurs.

Démonstration. — En réalité le Théorème de Tarski-Seidenberg prouve qu'une formule ne contenant qu'un seul quantificateur $\exists$ est équivalente à une formule sans aucun quantificateur. Mais la stabilité des semi-algébriques par complémentaire permet de ramener toute formule à une formule ne comportant que le quantificateur existentiel, en usant un nombre fini de fois la règle $\forall x \Psi \longleftrightarrow \neg(\exists x \neg \Psi)$. □

Les ensembles $\mathbf{R}$-constructibles sont les combinaisons booléennes finies d'ensembles de la forme $\{x \in \mathbb{R}^\ell; f(x) \diamond 0\}$, où $\diamond \in \{=, <\}$ et $f \in \mathbb{R}[x_1, \cdots, x_\ell]$. On

les appelle les **ensembles semi-algébriques réels**, tandis que les ensembles $\mathbb{R}$-définissables sont les combinaisons booléennes finies d'ensembles du même type mais où apparaissent des suites finies de quantificateurs portant sur des variables, par exemple : $\{x \in \mathbb{R}^\ell; \exists y \forall z, w \exists t f(x, y, z, w, t) \diamond 0\}$, où $f \in \mathbb{R}[x, y, z, w, t]$ et $\diamond \in \{=, <\}$. Le théorème de Tarski-Seidenberg dans la version du Théorème 3.3.20 assure que les seconds sont aussi les premiers.

3.3.21 Exercice. — *Trouver par l'algorithme de Sturm des conditions polynomiales sur les paramètres b, c qui assurent que $P(X) = X^3 + bX^2 + cX + 1$ ait un nombre déterminé de racines. Représenter Σ l'ensemble des points de S en lesquels ne s'applique pas le théorème des fonctions implicites (l'obtenir comme l'intersection de S et de l'ensemble Z des zéros du polynôme $\dfrac{\partial P}{\partial x}$). Trouver l'équation de Δ. La figure correspondante est donnée ci-dessous.*

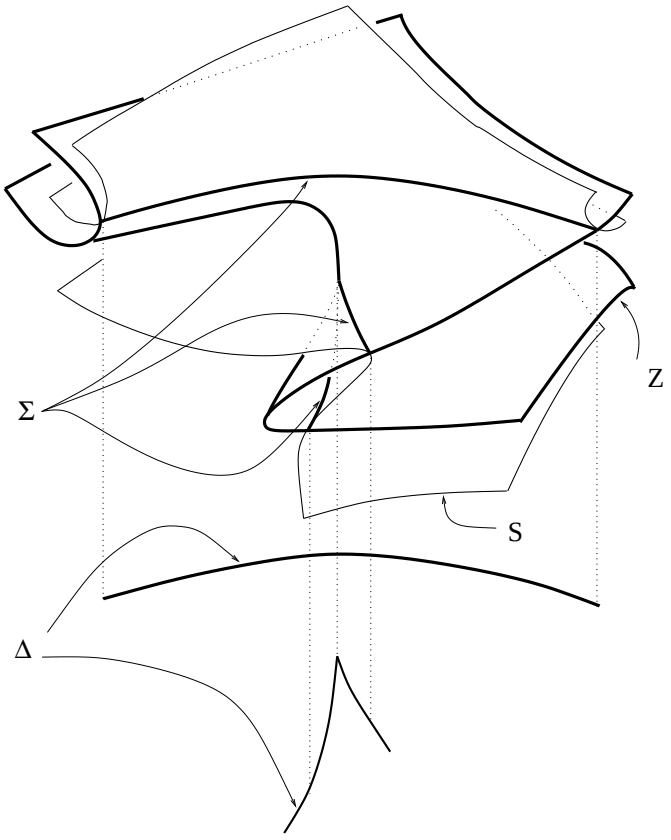


Fig. 2

3.3.22 Remarque. — L'objet du 10ème problème de Hilbert est de savoir s'il existe un algorithme décidant (négativement ou positivement) si une équation *diophantienne*, ie une équation polynomiale à coefficients entiers dont on recherche les

solutions entières possède, une solution. La réponse est négative, d'après le théorème de Matiyasevich : l'équivalent arithmétique de l'algorithme de Sturm n'existe pas.

Soit $\mathbf{L}_{ord} := \{0, 1, +, -, ., <\}$ le langage des anneaux ordonnés et $\mathbb{R}$ la $\mathbf{L_{ord}}$-structure

$$\mathbf{R} = \{\mathbb{R}, 0, 1, +, -, ., <\}.$$

On montre (**principe de transfert de Tarski**) que si $\mathbf{A} = \{A, 0, 1, +, -, ., <\}$ est une $\mathbf{L_{ord}}$-structure, élémentairement équivalente à $\mathbf{R}$, alors A est un corps réel clos, c'est-à-dire un corps ordonné dans lequel tout élément positif est un carré et tel que tout polynôme, à une variable, à coefficients dans ce corps et de degré impair possède une racine. Les axiomes des corps réels clos sont donnés par les $\mathbf{L_{ord}}$-formules suivantes, de sorte que si A est élémentairement équivalent à $\mathbf{R}$, A satisfait aussi ces axiomes, et donc est un corps réels clos :

1. Axiomes de corps ordonné. Par exemple :

$$\forall x \exists y (x + y = 0)$$
$$\forall x (x \neq 0 \longrightarrow \exists y, xy = 1)$$
$$\forall xyz (x < y \wedge 0 < z \longrightarrow xz < yz)$$
$$\forall xyz (x < y \longrightarrow x + z < y + z)$$

2. Le cône positif est l'ensemble des carrés :

$$\forall x (0 < x \longrightarrow \exists y, x = y^2)$$

3. Tout polynôme de degré impair possède une racine :

$$\forall x_0 x_1 \cdots x_{2n} (\exists y, y^{2n+1} + x_{2n} z^{2n} + \cdots + x_0 = 0)$$

L'implication réciproque est plus difficile à obtenir : si la $\mathbf{L_{ord}}$-structure satisfait les axiomes des corps réels clos, celle-ci est élémentairement équivalente à $\mathbf{R}$. Il s'agit en réalité d'une conséquence du théorème de Tarski-Seidenberg, qui dit que la théorie des corps réels clos élimine les quantificateurs :

Preuve du principe de transfert de Tarski. — Il s'agit de montrer que si une structure $\mathbf{A}$ est un modèle de la théorie $\mathbf{T_{rcf}}$ des corps réels clos, ie est une structure dans laquelle toutes les phrases de la théorie ci-dessus des corps réels clos est vraie, alors cette structure est élémentairement équivalente à $\mathbf{R}$. Soit donc φ une phrase de $\mathbf{L_{ord}}$ telle que $\mathbf{A} \models \varphi$. Comme la théorie des corps réels clos élimine les quantificateurs (c'est le théorème de Tarski-Seidenberg, prouvé dans $\mathbb{R}$ dans ce chapitre, mais qui se prouve de la même façon dans tout corps réel clos) il existe une phrase Ψ de $\mathbf{L_{ord}}$ sans quantificateur telle que :

$$\mathbf{T_{rcf}} \models (\varphi \longleftrightarrow \Psi)$$

On a donc $\mathbf{A} \models \varphi$ qui implique $\mathbf{A} \models \Psi$. Mais puisque Ψ est sans quantificateur, on a aussi $\mathbf{Q} \models \Psi$, car $\mathbf{Q} := (\mathbb{Q}, \mathbf{0}, \mathbf{1}, +, -, ., <)$ est une sous-structure commune de $\mathbf{A}$ (et $\mathbf{R}$), un corps réel clos étant de caractéristique nulle. Maintenant $\mathbf{Q} \models \Psi$ implique $\mathbf{R} \models \Psi$, et puisque $\mathbb{R}$ est un corps réel clos, on obtient $\mathbf{R} \models \varphi$.

L'implication $\mathbf{R} \models \varphi$ implique $\mathbf{A} \models \varphi$ s'obtient par symétrie des arguments. □

3.4. La théorie des corps algébriquement clos

3.4.1 Définition **(La théorie $\mathbf{T}_{ACF}$).** — On définit **la théorie des corps algébriquement clos $\mathbf{T}_{ac}$** sur le langage $\mathbf{L}_{rings}$ des anneaux par les axiomes suivants (et leurs conséquences logiques) :

(1) $\forall x, \exists y; x + y = 0$
(2) $\forall x, 0 + x = x + 0 = x$
(3) $\forall x, (x = 0) \vee (\exists y; x.y = y.x = 1)$
(4) $\forall x, 1.x = x.1 = x$
(5.1) $\forall a_0, a_1 \neq 0, \exists y; a_1 \cdot y + \cdots + a_0 = 0$
$\vdots$
(5.n) $\forall a_0, \ldots, a_n \neq 0, \exists y; a_n \cdot y^n + \cdots + a_0 = 0$
$\vdots$

On définit **la théorie $\mathbf{T}_{ACF_p}$ des corps algébriquement clos de caractéristique** p, où p est soit 0 soit un nombre premier, en ajoutant aux axiomes de $\mathbf{T}_{ACF}$ les axiomes suivants :

- (6.1) $\underbrace{1 + \cdots + 1}_{p \ fois} = 0$, lorsque $p \neq 0$
- (6.2) $1 + 1 \neq 0$
$\vdots$
(6.n) $\underbrace{1 + \cdots + 1}_{n \ fois} \neq 0$
$\vdots$
lorsque $p = 0$.

Par définition d'un corps, l'univers d'un modèle de la théorie $\mathbf{T}_{ACF_p}$ est appelé **un corps algébriquement clos de caractéristique** p.

Rappelons le théorème de Steinitz (cf [**2**], chap. v.4 ou [**11**] Partie II, chap. V.2) : si $\mathbf{k}$ est un corps, il existe un corps K algébriquement clos qui soit un sur-corps de $\mathbf{k}$ et que si K' est un autre tel sur-corps de $\mathbf{k}$, il existe un $\mathbf{k}$-isomorphisme de corps entre K et K'. On dit que K est **la clôture algébrique de $\mathbf{k}$**. Celle-ci est donc définie à $\mathbf{k}$-isomorphismes près.

On en tire le théorème suivant

3.4.2 Proposition. — *Soient* $\mathbf{k}$ *et* $\mathbf{k}'$ *deux corps algébriquement clos de même caractéristique et de même cardinal non dénombrable. Alors* $\mathbf{k}$ *et* $\mathbf{k}'$ *sont isomorphes.*

Démonstration. — Soit p la caractéristique commune de $\mathbf{k}$ et $\mathbf{k}'$. On note F leur sous-corps premier, qui est aussi commun ; celui-ci étant soit $\mathbb{Q}$ si $p = 0$, soit $\mathbf{F}_p$ si $p \neq 0$. Soient maintenant $\mathcal{B}$ et $\mathcal{B}'$ deux bases de transcendance de $\mathbf{k}$ et $\mathbf{k}'$ sur

F. Du fait que $\mathrm{Card}(\mathbf{k}) = \mathrm{Card}(\mathbf{k}')$, $\mathbf{k}$ est non dénombrable et F est dénombrable, on a $\mathrm{Card}(\mathcal{B}) = \mathrm{Card}(\mathcal{B}')$. Soient maintenant $F(\mathcal{B})$, resp. $F(\mathcal{B}')$, le plus petit sous-corps de $\mathbf{k}$, resp. $\mathbf{k}'$, contenant $\mathcal{B}$, resp. $\mathcal{B}'$. Le corps $F(\mathcal{B})$ est le corps des fractions rationnelles à coefficients dans F et inconnues dans $\mathcal{B}$. Les deux corps $F(\mathcal{B})$ et $F(\mathcal{B}')$ sont isomorphes du fait que $\mathcal{B}$ et $\mathcal{B}'$ sont en bijection. Comme $\mathbf{k}$ est algébriquement clos et est un sur-corps de $F(\mathcal{B})$, $\mathbf{k}$ est la clôture algébrique de $F(\mathcal{B})$. De même $\mathbf{k}'$ est la clôture algébrique de $F(\mathcal{B}')$, donc aussi de $F(\mathcal{B})$. Par unicité de la clôture algébrique à isomorphisme près, $\mathbf{k}$ et $\mathbf{k}'$ sont bien isomorphes. □

3.4.3 Proposition. — *Deux (structures de) corps isomorphes sont élémentairement équivalentes.*

Démonstration. — Soient $\mathbf{k}$ et $\mathbf{k}'$ deux corps isomorphes, $\varphi : \mathbf{k} \to \mathbf{k}'$ un isomorphisme et $\Phi(x_1, \cdots, x_n)$ une $\mathbf{L}_{rings}$-formule. Nous allons prouver que si $\Phi(a_1, \cdots, a_n)$ est vraie (resp. fausse) pour $(a_1, \cdots, a_n) \in \mathbf{k}^n$, $\Phi(\phi(a_1), \cdots, \phi(a_n))$ est vraie (resp. fausse). La preuve se fait par récurrence sur le longueur des formules.

Si Φ est une égalité, comme les isomorphismes préservent les égalités dans le langage $\mathbf{L}_{rings}$, nous n'avons rien à prouver. Si Φ est la conjonction de deux formule, l'hypothèse de récurrence s'applique à chacune de ces formules. De même si Φ est la négation d'une formule, l'hypothèse de récurrence s'applique à celle-ci.

Regardons maintenant de près le cas où $\Phi(x_1, \cdots, x_n)$ est $\exists x, \Psi(x_1, \cdots, x_n, x)$.

Si $\Phi(a_1, \cdots, a_n)$ est vraie, il existe $a \in \mathbf{k}$ tel que $\Psi(a_1, \cdots, a_n, a)$ soit vraie. Mais par hypothèse de récurrence $\Psi(\varphi(a_1), \cdots, \varphi(a_n), \varphi(a))$ est vraie dans la structure $\mathbf{k}'$, donc $\Phi(\varphi(a_1), \cdots, \varphi(a_n))$ est vraie dans $\mathbf{k}'$. L'argument est le même si $\Phi(a_1, \cdots, a_n)$ est fausse, la bijectivité de φ garantissant que si $\forall a \in \mathbf{k}$, $\Psi(\varphi(a_1), \cdots, \varphi(a_n), \varphi(a))$ est fausse, on a $\forall a' \in \mathbf{k}'$, $\Psi(\varphi(a_1), \cdots, \varphi(a_n), a')$ est fausse dans la structure $\mathbf{k}'$. □

Nous en venons maintenant au principe de Lefschetz, qui assure que la théorie $\mathbf{T}_{ACF_0}$ est complète et qui établit l'équivalence entre la véracité d'une phrase de $\mathbf{L}_{rings}$ dans un modèle de $\mathbf{T}_{ACF_0}$ et sa véracité dans un modèle de $\mathbf{T}_{ACF_p}$, pour une infinité de nombres premiers p.

***3.4.4 Théorème* (Principe de Lefschetz)**. — *La théorie $\mathbf{T}_{ACF_0}$ est complète. D'autre part soit Φ une phrase du langage $\mathbf{L}_{rings}$ des anneaux, les propositions suivantes sont alors équivalentes*

(i) Il existe un modèle $\mathbf{k}$ de la théorie $\mathbf{T}_{ACF_0}$ tel que $\mathbf{k} \models \Phi$.
(ii) Pour tout modèle $\mathbf{k}$ de la théorie $\mathbf{T}_{ACF_0}$, on a $\mathbf{k} \models \Phi$.
(iii) Il existe un modèle $\mathbf{k}_p$ de la théorie $\mathbf{T}_{ACF_p}$ tel que $\mathbf{k}_p \models \Phi$, pour une infinité de nombres premiers p (on peut prendre $p \geq p_0$, pour un certain entier p_0).

Démonstration. — Commençons par prouver que la théorie $\mathbf{T}_{ACF_0}$ est complète. Par définition il nous faut prouver qu'une phrase quelconque Φ de $\mathbf{L}_{rings}$ prend les mêmes valeurs de vérité dans tous les modèles de $\mathbf{T}_{ACF_0}$, ou encore que tous les modèles de $\mathbf{T}_{ACF_0}$ sont élémentairement équivalents. La structure $\mathbf{C}$ des nombres complexes étant un modèle de $\mathbf{T}_{ACF_0}$, il nous suffit donc de montrer que tous les modèles de $\mathbf{T}_{ACF_0}$ sont élémentairement équivalents à $\mathbf{C}$. Soit donc $\mathbf{k}$ un modèle

de $\mathbf{T}_{ACF_0}$. Soit $\mathbf{T}$ la théorie de toutes les $\mathbf{L}_{rings}$-phrases vraies dans $\mathbf{k}$. D'après l'Exemple 3.2.6, $\mathbf{T}$ est complète, et bien sûr $\mathbf{k}$ est un modèle de $\mathbf{T}$. D'autre part $\mathbf{k}$ est infini car contient $\mathbb{Q}$ comme sous-corps premier. On peut donc appliquer le Théorème de Löwenheim-Skolem 3.2.18, le langage $\mathbf{L_{rings}}$ étant fini, il existe un modèle $\mathbf{M}$ de $\mathbf{T}$ de cardinalité $\aleph_1 = \mathrm{Card}(\mathbb{C})$. Or la théorie $\mathbf{T}$ étant complète, $\mathbf{M}$ et $\mathbf{k}$ sont élémentairement équivalents. En particulier l'univers M de $\mathbf{M}$ est un corps algébriquement clos, de caractéristique nulle et de même cardinal que $\mathbb{C}$. Par la Proposition 3.4.2, M et $\mathbb{C}$ sont isomorphes et par la Proposition 3.4.3, les structures $\mathbf{M}$ et $\mathbf{C}$ sont élémentairement équivalentes. Il s'ensuit que $\mathbf{k}$ et $\mathbf{C}$ sont élémentairement équivalentes.

Montrons maintenant l'équivalences des trois propositions $(i), (ii)$ et (iii).

$(i) \iff (ii)$. Seule l'implication $(i) \implies (ii)$ mérite d'être prouvée. Mais cette implication résulte par définition de la complétude de $\mathbf{T}_{ACF_0}$.
$(iii) \implies (i)$. On suppose que Φ est vraie dans un modèle $\mathbf{k}_p$ de la théorie $\mathbf{T}_{ACF_p}$, pour une infinité de nombres premiers p. Soit alors $\mathbf{T}$ la théorie obtenue en ajoutant aux axiomes de $\mathbf{T}_{ACF_0}$ la formule Φ. Tous les sous-ensembles finis de $\mathbf{T}$ forment une théorie ayant un modèle. En effet à un tel ensemble fini Σ est associé un nombre premier p, supérieur au plus grand entier n tel que le formule $\underbrace{1 + \cdots + 1}_{n\ fois} \neq 0$ soit dans Σ et tel que $\mathbf{k}_p \models \Phi$. Donc $\mathbf{k}_p$ est un modèle de Σ. D'après le Théorème de compacité, $\mathbf{T}$ admet un modèle et celui-ci est nécessairement un corps algébriquement clos de caractéristique nulle dans lequel Φ est vraie.
$(ii) \implies (iii)$. Supposons maintenant que Φ soit vraie dans tout modèle de $\mathbf{T}_{ACF_0}$. D'après le Théorème de complétude, $\mathbf{T}_{ACF_0} \vdash \Phi$. Une preuve formelle de Φ dans $\mathbf{T}_{ACF_0}$ ne faisant intervenir qu'un nombre fini d'axiomes de $\mathbf{T}_{ACF_0}$, il existe des nombres premiers $p_1, \cdots, p_\ell$ tels que $\mathbf{T}_{ACF_0} \cup \{p_1 \cdot 1 \neq 0\} \cup \cdots, \cup \{p_\ell \cdot 1 \neq 0\} \vdash \Phi$. Or pour tout nombre premier p tel que $p \geq \ell$, la clôture algébrique de $\mathbf{F}_p$ rend vrai tous les axiomes de $\mathbf{T}_{ACF_0} \cup \{p_1 \cdot 1 \neq 0\} \cup \cdots, \cup \{p_\ell \cdot 1 \neq 0\}$ et par conséquent rend vraie Φ. On obtient bien une infinité de modèles de $\mathbf{k}_p$ qui rendent vraie Φ.

□

3.4.5 Exercice **(Théorème d'Ax)**. — *Le but de cet exercice est de démontrer l'enonce suivant*

Si $f : \mathbb{C}^n \to \mathbb{C}^n$ est une application polynomiale injective, f est surjective.

Notons qu'en vertu du Principe de Lefschetz (Théorème 3.4.4), il suffit de démontrer cet énoncé pour la clôture algébrique $\bar{\mathbf{F}}_p$ du corps à p éléments $\mathbf{F_p}$, pour tout nombre premier p, puisque pour tout corps $\mathbf{k}$ pour toute famille $f_1, \ldots, f_n$ de polynômes à coefficients dans $\mathbf{k}$, à n indéterminés, et de degré borné par un entier d, il existe un énoncé ϕ de $\mathbf{L}_{rings}$ exprimant que l'injectivité de $(f_1, \ldots, f_n) : \mathbf{k}^n \to \mathbf{k}^n$ implique sa surjectivité.

1. *Le but de cette question est de démontrer que toute partie finie de $\bar{\mathbf{F}}_p$ est contenue dans un sous-corps fini de $\bar{\mathbf{F}}_p$. Rappelons que si $\mathbf{k}$ est un corps, quelle*

que soit sa caractéristique, pour tout polynôme P (non nul) de $\mathbf{k}[x]$, $a \in \mathbf{k}$ est racine simple de P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$[3].

1.a. Montrer que quel que soit $\ell \in \mathbb{N}^*$, les racines dans $\bar{\mathbf{F}}_p$ de $x^{p^\ell} - x$ sont simples. En déduire que celles-ci forment un sous-corps de $\bar{\mathbf{F}}_p$ de cardinal fini (égal à p^ℓ). On note $\mathbf{F}_{p^\ell}$ ce corps.

1.b. Soit $a \in \bar{\mathbf{F}}_p$. Montrer que $\mathbf{F}_p[a]$ est un sous-corps de $\bar{\mathbf{F}}_p$ de cardinal une puissance de p (montrer que $\mathbf{F}_p[a]$ est fini et considérer que $\mathbf{F}_p[a]$ est $\mathbf{F}_p$-espace vectoriel). En déduire qu'existe $\ell \in \mathbb{N}$ tel que $a^{p^\ell} = a$.

1.c. Montrer que $\bar{\mathbf{F}}_p$ est réunion de ses sous-corps $\mathbf{F}_{p^\ell}$, puis de $\mathbf{F}_{p^\ell} \subset \mathbf{F}_{(p^\ell)^k}$, pour tout $k \geq 1$, en déduire que toute partie finie de $\bar{\mathbf{F}}_p$ est dans un sous-corps de $\bar{\mathbf{F}}_p$ du type $\mathbf{F}_{p^s}$, pour $s \geq 1$.

2. Soit $f = (f_1, \cdots, f_n) : \bar{\mathbf{F}}_p^n \to \bar{\mathbf{F}}_p^n$ une application polynomiale ($f_i \in \bar{\mathbf{F}}_p[x]$) injective mais non surjective et $y = (y_1, \cdots, y_n) \in \bar{\mathbf{F}}_p^n$ qui n'est pas dans l'image de f. On considère le sous-corps K de $\bar{\mathbf{F}}_p$ engendré par les y_j et les coefficients des f_i.

2.a. Montrer que K est fini.

2.b. Montrer que l'application f induit une application $f_{|K^n} : K^n \to K^n$ qui est injective mais non surjective. Conclure.

Nous allons maintenant donner des propositions qui nous amènent à une formulation équivalente à celle qui dit que $\mathbf{T}_{ACF}$ élimine les quantificateurs dans le langage des anneaux.

3.4.6 Proposition. — *Soit $\mathbf{T}$ une théorie sur un langage $\mathbf{L}$ et $\phi(x_1, \cdots, x_n)$ une $\mathbf{L}$-formule (dont les variables libres sont $x := (x_1, \cdots, x_n)$). On a les équivalences*

(i) Il existe une $\mathbf{L}$-formule $\psi(x)$ sans quantificateur telle que

$$\mathbf{T} \vdash \forall x(\phi(x) \iff \psi(x))$$

(ii) Pour tous $\mathbf{M}, \mathbf{N}$ modèles de $\mathbf{T}$ et $\mathbf{A}$ sous-structure de $\mathbf{M}$ et $\mathbf{N}$, on a pour tout $a_1, \cdots, a_n \in A$

$$\mathbf{M} \models \phi(a) \iff \mathbf{N} \models \phi(a)$$

Démonstration. — $(i) \implies (ii)$ Soient $\mathbf{M}, \mathbf{N}$ deux modèles de $\mathbf{T}$ et $\mathbf{A}$ une sous-structure de $\mathbf{M}$. Soient $a_1, \cdots, a_n \in A$. Par hypothèse $\mathbf{T} \vdash (\phi(a) \iff \psi(a))$, donc $\mathbf{M} \models \phi(a) \iff \mathbf{M} \models \psi(a)$. Maintenant remarquons que la véracité d'une formule sans quantificateur est préservée dans les sous-structures, donc

$$\mathbf{M} \models \psi(a) \iff \mathbf{A} \models \psi(a) \iff \mathbf{N} \models \psi(a) \iff \mathbf{N} \models \phi(a)$$

$(ii) \implies (i)$ Montrons l'existence d'une formule ψ sans quantificateur équivalente à ϕ, sous l'hypothèse (ii). Pour cela considérons

$$\Gamma(x) := \{\gamma \text{ sans quantificateur } ; \mathbf{T} \vdash \forall x(\phi(x) \implies \gamma(x))\}$$

[3] Cette caractérisation de l'ordre d'une racine par le polynôme dérivé ne se généralise toutefois pas au-delà de l'ordre 1 en caractéristique nulle. Par exemple 0 est racine d'ordre p de $P(x) = x^p \in \mathbf{F}_p$, tandis que $P'(0) = \cdots = P^{(p)}(0) = 0$.

Considérons des symboles additionnels de constantes $d := (d_1, \cdots, d_n)$ qui ne soient pas dans $\mathbf{L}$ et que l'on ajoute à $\mathbf{L}$ et à et montrons que

$$\mathbf{T} \cup \Gamma(d) \vdash \phi(d).$$

Par le théorème de complétude (Théorème 3.2.12), si tel n'est pas le cas existe un modèle $\mathbf{M}$ tel que $\mathbf{M} \models \mathbf{T} \cup \Gamma(d) \cup \{\neg\phi(d)\}$. Soit alors la sous-structure $\mathbf{A}$ de $\mathbf{M}$ (auquel on a ajouté formellement les symboles d) engendrée par d [4] et soit $\mathrm{Diag}(\mathbf{A})$ le diagramme de $\mathbf{A}$, ie les formules $\sigma(a)$, où $a = (a_1, \cdots, a_k) \in A^k$ et $\sigma(x_1, \cdots, x_k)$ est une formule sans quantificateur de $\mathbf{L}$ telle que $\mathbf{A} \models \sigma(\mathbf{a})$. Nous allons montrer que la théorie $\Sigma := \mathbf{T} \cup \mathrm{Diag}(\mathbf{A}) \cup \{\phi(d)\}$ admet un modèle. En effet si tel n'est pas le cas, il existe par le Théorème 3.2.16 des formules sans quantificateurs $\sigma_1(d), \cdots, \sigma_\ell(d) \in \mathrm{Diag}(\mathbf{A})$ telles que

$$\mathbf{T} \vdash (\bigwedge_{i=1}^{\ell} \sigma_i(d) \Longrightarrow \neg\phi(d))$$

Or les symboles d n'apparaissant pas par construction dans dans $\mathbf{L}$ (ni $\mathbf{T}$), on a

$$\mathbf{T} \vdash \forall x(\bigwedge_{i=1}^{\ell} \sigma_i(x) \Longrightarrow \neg\phi(x))$$

ou encore

$$\mathbf{T} \vdash \forall x(\phi(x) \Longrightarrow \bigvee_{i=1}^{\ell} \neg\sigma_i(x))$$

Par définition de $\Gamma(x)$, on a alors $\bigvee_{i=1}^{\ell} \neg\sigma_i(x) \in \Gamma(x)$ avec $\sigma_i(d) \in \mathrm{Diag}(\mathbf{A})$ et par définition de $\mathrm{Diag}(\mathbf{A})$, on aurait $\mathbf{A} \models \bigvee_{i=1}^{\ell} \neg\sigma_i(d)$ avec $\mathbf{A} \models \sigma_i(d)$, pour tout $i \in 1, \cdots, \ell$, ce qui serait contradictoire.

Nous savons maintenant que la théorie Σ admet un modèle $\mathbf{N}$. Il s'ensuit que $\mathbf{N} \models \phi(d)$ tandis que $\mathbf{M} \models \neg\phi(d)$. Ceci étant en contradiction avec notre hypothèse (ii), nous pouvons enfin affirmer que

$$\mathbf{T} \cup \Gamma(d) \vdash \phi(d).$$

Ceci nous donne un nombre fini de formules sans quantificateur $\gamma_1(d), \cdots, \gamma_\ell(d)$ de $\Gamma(d)$ telles que

$$\mathbf{T} \vdash \bigwedge_{i=1}^{\ell} \gamma_i(d) \Longrightarrow \phi(d)$$

et donc

$$\mathbf{T} \vdash \forall x(\bigwedge_{i=1}^{\ell} \gamma_i(x) \Longrightarrow \phi(x))$$

[4] Soit $\mathbf{M}$ une $\mathbf{L}$-structure et D une partie de $\mathbf{M}$. Il existe une plus petite sous-structure de $\mathbf{M}$ contenant D, la **sous-structure engendrée par** D, qui est la clôture de D et de l'ensemble des constantes de $\mathbf{L}$ par les fonctions de $\mathbf{L}$. Dans la cas où $n = 0$, il est nécesaire de supposer que le langage $\mathbf{L}$ possède au moins un symbole de constante afin que $\mathbf{A}$ ne soit pas vide.

L'implication $\Longleftarrow$ dans la formule ci-dessus est obtenue auomatiquement du fait que les formules $\gamma(x)$ de $\Gamma(x)$ sont impliqués par $\phi(x)$. On pose enfin $\psi(x) := \bigwedge_{i=1}^{\ell} \gamma_i(x)$, qui est sans quantificateur.

□

La Remarque 3.2.20 et la Proposition 3.4.6 misent ensemble donnent le critère suivant d'élimination des quantificateurs

3.4.7 Théorème. — *Soit* $\mathbf{T}$ *une théorie sur le langage* $\mathbf{L}$ *telle que*

- *pour tout triplet* $(\mathbf{M}, \mathbf{N}, \mathbf{A})$ *où* $\mathbf{M}$ *et* $\mathbf{N}$ *sont deux modèles de* $\mathbf{T}$ *et* $\mathbf{A}$ *une sous-structure commune à* $\mathbf{M}$ *et* $\mathbf{N}$*,*
- *pour toute* $\mathbf{L}$*-formule sans quantificateur* $\phi(y, x)$*,* $x := (x_1, \ldots, x_n)$*, on a pour tout* $a_1, \cdots, a_n \in A$*,*

$$\mathbf{M} \models \exists y \phi(y, a) \Longleftrightarrow \mathbf{N} \models \exists y \phi(y, a).$$

Alors $\mathbf{T}$ *élimine les quantifcateurs dans le langage* $\mathbf{L}$*.*

On en tire le théorème d'élimination des quantificateurs dans $\mathbf{T}_{ACF}$.

3.4.8 Théorème. — *La théorie* $\mathbf{T}_{ACF}$ *élimine les quantificateurs dans le langage des anneaux.*

Démonstration. — Il suffit de prouver que si F et K sont deux corps algébriquement clos (univers de deux modèles $\mathbf{F}$ et $\mathbf{K}$ de $\mathbf{T}_{ACF}$), avec $F \subset K$ et $\phi(y, x)$, $x := (x_1, \cdots, x_n)$ une $\mathbf{L_{rings}}$-formule sans quantificateur, alors pour tout $a_1, \cdots, a_n \in F$, on a

$$\mathbf{F} \models \exists y \phi(y, a) \Longleftrightarrow \mathbf{K} \models \exists y \phi(y, a) \tag{3.4.8.2}$$

En effet supposons que la propriété 3.4.8.2 soit vérifiée. D'après le Théorème 3.4.7, pour prouver l'élimination des quantifiateurs il suffit de considérer deux corps algébriquement clos M et N, et A un sous-ensemble tel que $\mathbf{A}$ soit une sous-structure commune à $\mathbf{M}$ et $\mathbf{N}$, ie un sous-anneau intègre de M et N, puis de montrer que pour tout $a \in A$, s'il existe $p \in M$ tel que $\mathbf{M} \models \phi(p, a)$ alors existe $q \in N$ tel que $\mathbf{N} \models \phi(q, a)$. Or s'il existe $p \in M$ tel que $\mathbf{M} \models \phi(p, a)$, en notant F la clôture algébrique de A dans M, la propriété 3.4.8.2 assure qu'existe $g \in F$ tel que $\mathbf{F} \models \phi(g, a)$. Or si F' est la clôture algébrique de A dans N, F et F' étant deux corps isomorphes et les isomorphismes d'anneaux conservant les $\mathbf{L}_{rings}$-formules vraies, nous avons $\mathbf{F}' \models \phi(g', a)$ pour un certain $g' \in F'$, soit $\mathbf{N} \models \phi(g', a)$.

Montrons alors la propriété 3.4.6, dont seule l'implication de droite à gauche est pertinente. La formule $\phi(y, x)$ est équivalente à une formule du type

$$\bigvee_{i=1}^{m} \bigwedge_{j=1}^{\ell} \phi_{i,j}(y, x),$$

avec $\phi_{i,j}$ atomique ou négation de formule atomique. Si $\mathbf{F} \models \exists y \phi(y, a)$ il existe $i \in \{1, \cdots, m\}$ tel que $\mathbf{F} \models \exists y \bigwedge_{j=1}^{\ell} \phi_{i,j}(y, a)$. Or la formule $\phi_{i,j}$ est du type $p_{i,j} = 0$ ou $q_{i,j} \neq 0$ avec $p_{i,j}$ et $q_{i,j}$ des polynômes à coefficients dans F. On suppose donce

que ϕ est de la forme $\bigwedge_{j=1}^{\ell}(p_{i,j}=0)\wedge(q_{i,j}\neq 0)$. Si pour un certain $j\in\{1,\cdots,\ell\}$, existe $b\in K$ tel que $p_{i,j}(b,a)=0$ alors b étant algébrique sur F, $b\in F$. D'autre part si $\mathbf{K}\models\exists y\bigwedge_{j=1}^{\ell}q_{i,j}(y,a)\neq 0$, les polynômes $q_{i,j}$ ne sont pas nuls, et n'ayant qu'un nombre fini de racines et F étant infini puisqu'algébriquement clos, on peut trouver $b\in F$ tel que $\bigwedge_{j=1}^{\ell}q_{i,j}(y,a)\neq 0$.

□

3.4.9 Remarque. — Du Théorème 3.4.7 découle également l'élimination des quantificateurs pour la théorie des corps réels clos dans le langage des anneaux ordonnés (Voir [**12**], Théorème 2.3).

3.4.10 Définition. — Soit $\mathbf{k}$ un corps algébriquement clos et $n\in\mathbb{N}^*$. On appelle **ensemble constructible de $\mathbf{k}^n$** un ensemble définissable de $\mathbf{k}^n$ dans le langage des anneaux à l'aide d'une formule non quantifiée. Les ensembles constructibles sont donc les réunions finies d'ensembles du type $\mathbf{k}^n\setminus X$, où X est un ensemble algébrique de $\mathbf{k}^n$ ou les ensembles algébriques.

Une reformulation du Théorème 3.4.7 est donc :

3.4.11 Théorème. — *Soien $n,p,m\in\mathbb{N}^*$ tels que $n=p+m$ et C un ensemble constructible de $\mathbf{k}^n$. Si $\pi:\mathbf{k}^n\to\mathbf{k}^p$ désigne la projection standard sur $\mathbf{k}^p$, $\pi(C)$ est un ensemble constructible de $\mathbf{k}^p$.*

Une conséquence rapide du théorème d'élimination des quantificateurs dans les corps algébriquement clos est une preuve agréable du Nullstellensatz (faible).

Preuve du Nullstellensatz faible. — Soit I un idéal de $k[X_1,\cdots,X_n]$ et k algébriquement clos. Montrons que si $\mathcal{Z}(I)$ est vide nécessairement $I=k[X_1,\cdots,X_n]$.

L'idéal I est engendré par les polynômes $P_1,\cdots,P_m$, puisque $k[X_1,\cdots,X_n]$ est nœthérien. Si le système $\{P_i=0\}$ est sans solution, comme cette condition est du premier ordre dans le langage des corps algébriquement clos, qui est avec élimination des quantificateurs, cette condition équivaut à une formule sur les seuls coefficients des P_i. Ce système ne possède alors pas de solution dans tout autre corps algébriquement clos contenant k. Or comme tout corps contenant k peut être plongé dans un corps algébriquement clos, le système $\{P_i=0\}$ est sans solution dans tout corps contenant k. Si $I\neq k[X_1,\cdots,X_n]$, on peut supposer que I est un idéal maximal, car tout idéal strict d'un anneau est contenu dans un idéal maximal. Le corps $K=k[X_1,\cdots,X_n]/I$ contient k, et $(\bar{X}_1,\cdots,\bar{X}_n)\in K^n$ est alors une solution du système $\{P_i=0\}$, ce qui est contradictoire. □

CHAPITRE 4

DIMENSION

CHAPITRE 5

SCHÉMAS

Dans toute la suite la lettre R désigne un anneau commutatif que nous supposerons toujours unitaire. Nous allons tout d'abord associer à un tel anneau un espace topologique, $\mathrm{Spec}\, R$, qui sera ensuite muni d'une structure d'espace localement annelé et qui permettra de généraliser la notion de variété sur un corps, en un sens que nous préciserons tout au long de ce chapitre. L'espace $\mathrm{Spec}\, R$ jouera le même rôle pour les schémas celui des ensembles algébriques de $\mathbf{k}^n$ pour les variétés algébriques.

5.1. Le spectre $\mathrm{Spec}\, R$ d'un anneau R

Nous définissons dans cette sous-section la notion de spectre d'un anneau R, noté $\mathrm{Spec}\, R$, lorsque R est un anneau commutatif (unitaire). Il s'agira d'une notion comparable à celle d'ensemble algébrique de $\mathbf{k}^n$, pour un corps $\mathbf{k}$, puisqu'à l'aide de $\mathrm{Spec}\, R$ seront ensuite construits les pré-schémas et les schémas comme l'ont été, à l'aide des ensembles algébriques de $\mathbf{k}^n$, les variétés affines, les prévariétés et les variétés.

5.1.1 Définition. — Soit R un anneau commutatif et unitaire. L'ensemble des idéaux premiers de R est noté $\mathrm{Spec}\, R$, on appelle cet ensemble **le spectre de** R ou **le schéma affine associé à** R. Si $\mathfrak{p} \in \mathrm{Spec}\, R$, on note $k(\mathfrak{p})$ le corps des fractions de l'anneau intègre $R/\mathfrak{p}$.

5.1.2 Remarque. — L'anneau R n'est pas un idéal premier de R, tandis que l'idéal nul n'est premier que si et seulement si R est intègre.

5.1.3 Lemme. — *Soit A un anneau (commutatif), I un idéal de A et $\pi : A \to A/I$ la surjection canonique. L'application*

$$\tilde{\pi} : \{\textit{idéaux de } A \textit{ contenant } I\} \to \{\textit{idéaux de } A/I\}$$

définie par $\tilde{\pi}(J) = \pi(J)$ est une bijection croissante qui établit une bijection entre les idéaux premiers de A contenant I et les idéaux premiers de A/I.

Démonstration. — L'application π, qui transforme un idéal en un idéal, induit bien l'injection $\tilde{\pi}$, car si J, K sont deux idéaux distincts de A contenant I, il existe par exemple $j \in J, j \notin K$, et du fait que $j - k \notin I \subset K$, pour tout $k \in K$, on a $\pi(j) \notin \pi(K)$, donc $\tilde{\pi}(J) \neq \tilde{\pi}(K)$. La surjectivité de $\tilde{\pi}$ découle du fait que si J est un idéal de A/I, $\pi^{-1}(J)$ est un idéal de A. La croissance de $\tilde{\pi}$ est immédiate. Enfin, si J est un idéal premier de A contenant I, et si $\tilde{x}, \tilde{y} \in A/I$ sont tels que $\tilde{x}\tilde{y} \in \tilde{\pi}(J)$, alors il existe $j \in J, i \in I$ tels que $xy = j + i \in J$, donc $x \in J$ ou $y \in J$ et ainsi $\tilde{x} \in \pi(J)$ ou $\tilde{y} \in \pi(J)$, c'est-à-dire que $\tilde{\pi}(J)$ est premier. Réciproquement, si $\tilde{J}$ est un idéal premier de A/I, soit $L = \pi^{-1}(\tilde{J})$ et $x, y \in A$ tels que $xy \in L$. Alors $\tilde{x}\tilde{y} \in \tilde{J}$, donc $\tilde{x} \in \tilde{J}$ par exemple, ie $x - j = i$, pour $j \in L$ et $i \in I$. On en conclut que $x \in L$. □

5.1.4 Exemples. — Voyons quelques exemples remarquables de spectres d'anneaux.

(1) Dans le cas où R est un corps $\mathbf{k}$, $\mathrm{Spec}\, R$ est le singleton (0), seul idéal premier de $\mathbf{k}$.
(2) Dans le cas où $R = \mathbb{Z}$, $\mathrm{Spec}\, R$ est l'ensemble des idéaux premiers (principaux) $\mathfrak{p} := p\mathbb{Z}$, où p est un nombre premier, auquel il convient d'ajouter l'idéal nul (0), puisque $\mathbb{Z}$ est intègre. Notons que dans ce cas les idéaux premiers $p\mathbb{Z}$ sont aussi maximaux.
(3) Dans le cas où $R = \mathbf{k}[x]$, avec $\mathbf{k}$ algébriquement clos, l'anneau R étant principal, ses idéaux premiers sont les idéaux engendrés par les irréductibles (cf Proposition 1.3.11), ie les idéaux du type $(x - a)$, $a \in \mathbf{k}$ et l'idéal nul (0) (puisque $\mathbb{R}$ est intègre). Ainsi $\mathrm{Spec}\, R$ est la réunion d'un ensemble en bijection avec $\mathbf{k}$ et de l'idéal nul.
(4) Dans le cas où $R = \mathbb{R}[x]$, les idéaux premiers de R sont donnés par l'idéal nul, les idéaux $(x - a)$, $a \in \mathbb{R}$ et les idéaux $(x^2 + ax + b)$, avec $a^2 - 4b < 0$.
(5) Dans le cas où $R = \mathbf{k}[x, y]$, le corps $\mathbf{k}$ étant algébriquement clos, les idéaux premiers de $\mathbf{k}[x, y]$ sont en bijection, via l'application $\mathcal{I}$, avec les variétés algébriques de $\mathbf{k}^2$. La théorie de la dimension nous apprend alors que celles-ci sont de dimension $0, 1$ ou 2 et que leurs idéaux sont les idéaux maximaux de $\mathbf{k}[x, y]$, qui sont du type $(x - a, y - b)$ avec $a, b \in \mathbf{k}$, les idéaux principaux (P), avec P polynôme irréductible de $\mathbf{k}[x, y]$ et l'idéal nul.
(6) Dans le cas où X est une variété affine de $\mathbf{k}^n$, $\mathbf{k}$ étant algébriquement clos, $X = \mathcal{Z}(I)$, pour un idéal premier I de $\mathbf{k}[x_1, \cdots, x_n]$, et $R = A(X) = \mathbf{k}[x_1, \cdots, x_n]/I$ son algèbre affine, les idéaux premiers de R sont donnés par les images par la surjection canonique $\pi : \mathbf{k}[x_1, \cdots, x_n] \to R = \mathbf{k}[x_1, \cdots, x_n]/I$ des idéaux premiers de $\mathbf{k}[x_1, \cdots, x_n]$ contenant I (en vertu du Lemme 5.1.3), l'idéal nul étant aussi un idéal premier de R, puisque X étant irréductible, R est intègre. Ainsi $\mathrm{Spec}(A(X))$ est constitué de l'idéal nul, et d'après le Corollaire 2.3.7, d'un ensemble en bijection avec les sous-variétés fermées de X. En conclusion $\mathrm{Spec}\, R$

contient un point pour chaque sous-variété fermée de X et un point particulier qui est l'idéal nul. Parmi les idéaux premiers de $\operatorname{Spec} R$ se trouvent en particulier les idéaux maximaux de $\mathbf{k}[x_1, \cdots, x_n]$ contenant I, qui sont en bijection avec les points de X (toujours d'après le Corollaire 2.3.7).

5.2. L'espace topologique $\operatorname{Spec} R$

D'un point de vue ensembliste, lorsque R est l'algèbre affine d'une variété algébrique de $\mathbf{k}^n$, $\operatorname{Spec} R$ est l'ensemble des sous-variétés fermées de X (cf l'exemple 5.1.4 (6)). Il faut en réalité voir $\operatorname{Spec} R$ comme l'ensemble X , dont les points sont identifiés aux idéaux maximaux de $\mathbf{k}[x_1, \cdots, x_n]$ contenant l'idéal I de X, enrichi de points supplémentaires, les idéaux premiers (non maximaux) de $\mathbf{k}[x_1, \cdots, x_n]$ contenant l'idéal I. On va introduire sur $\operatorname{Spec} R$ une topologie qui va nous permettre de pousser plus loin l'identification de $\operatorname{Spec} R$ à la variété X "enrichie".

Pour cela rappelons que la topologie de Zariski sur une variété X est donnée par ses fermés qui sont les sous-variétés fermées de X. Sur la variété algébrique X de $\mathbf{k}^n$ on dispose des restrictions des fonctions polynomiales qui définissent ces fermés. De quelles fonctions disposons-nous sur $\operatorname{Spec} R$? Si l'on veut poursuivre notre parallèle entre le spectre d'une algèbre affine d'une variété, ou plus généralement le spectre d'un anneau R et les variétés, il faut bien admettre qu'à l'algèbre affine d'une variété va correspondre l'anneau R, selon le principe illustré ci-dessous

$$\begin{array}{rcl} \text{fonctions sur } X \text{ définissant la topologie de } X & = & A(X) \\ \text{variété } X \text{ de } \mathbf{k}^n & \longleftrightarrow & \operatorname{Spec}(A(X)) \\ \text{fonctions sur } \operatorname{Spec} R \text{ définissant la topologie de } \operatorname{Spec} R & = & R \end{array}$$

Comment alors voir les éléments de R comme des fonctions sur $\operatorname{Spec} R$? Il suffit pour cela de savoir évaluer un élément $f \in R$ en un point $\mathfrak{p} \in \operatorname{Spec} R$. Dans le cas où $R = A(X)$, l'évaluation d'une fonction f de $A(X)$ en un point $a = (a_1, \cdots, a_n) \in X$ s'identifie avec la classe de f dans $\mathbf{k}[x_1, \cdots, x_n]/(x - a_1, \cdots, x - a_n) \simeq \mathbf{k}$. On peut donc poser la définition suivante

5.2.1 Définition. — Soit R un anneau commutatif et unitaire. Pour $\mathfrak{p} \in \operatorname{Spec} R$, notons $k(\mathfrak{p})$ le corps des fractions de l'anneau intègre $R/\mathfrak{p}$ et pour $f \in R$ désignons par $f(\mathfrak{p})$ la classe de f dans ce corps. On dit que $f(\mathfrak{p})$ est l'évaluation de f en l'idéal $\mathfrak{p}$, ou la valeur de f en $\mathfrak{p}$.

5.2.2 Remarque. — Contrairement au cas des fonctions polynomiales sur un ensemble algébrique, les valeurs des fonctions ne caractérisent pas celles-ci. Ainsi deux éléments $f, g \in R$ peuvent prendre les mêmes valeurs sur $\operatorname{Spec} R$ sans être égaux, comme on va le voir dans l'Exemple 5.2.3.

Les valeurs de l'élément f de R en l'idéal premier $\mathfrak{p}$ ne sont pas des éléments d'un même corps en général, mais l'évaluation de f en les points de $\operatorname{Spec} R$ permet tout de même de définir l'ensemble des points de $\operatorname{Spec} R$ en lesquels f s'annule.

5.2.3 Exemple. — Soit $\mathbf{k}$ un corps. Considérons l'anneau $R = \mathbf{k}[x]/(x^2)$. D'après le Lemme 5.1.3, les idéaux premiers de cet anneau sont les idéaux premiers de $\mathbf{k}[x]$ contenant (x^2). Or les idéaux premiers de $\mathbf{k}[x]$ sont principaux (et même maximaux), engendrés par les irréductibles de $\mathbf{k}[x]$, d'après la Proposition 1.3.11. Il suffit de considérer les irréductibles de degré 1 et parmi ceux-ci seul x engendre un idéal contenant x^2. Il s'ensuit que $\mathrm{Spec}R = \{(x)\}$ (notons que R n'étant pas intègre, 0 n'est pas dans $\mathrm{Spec}R$). Notons $\mathfrak{p} = (x)$. Si $f = ax + b \in R$, $f(\mathfrak{p})$ est par définition la classe de f dans $R/\mathfrak{p}$, c'est-à-dire $f(\mathfrak{p}) = b$. Il s'ensuit que si $f = x$, $f(\mathfrak{p}) = 0_{R/\mathfrak{p}}$. En particulier les éléments $g = 0_R$ et $f = x$ de R, vus comme des fonctions, induisent deux fonctions nulles sur $\mathrm{Spec}R$ (certes à valeurs dans deux corps formellement distincts), bien qu'étant deux éléments distincts de R.

5.2.4 Définition. — Soit R un anneau commutatif et unitaire. Pour $S \subset R$, nous définissons le lieu $\mathcal{Z}(S)$ des zéros de S par

$$\mathcal{Z}(S) := \{\mathfrak{p} \in \mathrm{Spec}R; f(\mathfrak{p}) = 0_{k(\mathfrak{p})}, \forall f \in S\}.$$

Il est immédiat que

$$\mathcal{Z}(S) = \{\mathfrak{p} \in \mathrm{Spec}R; f \in \mathfrak{p}, \forall f \in S\} = \{\mathfrak{p} \in \mathrm{Spec}R; S \subset \mathfrak{p}\}.$$

5.2.5 Remarque. — En notant (S) l'idéal de R engendré par la partie S de R, on voit que $\mathcal{Z}(S) = \mathcal{Z}((S))$, puisque $S \subset \mathfrak{p} \Leftrightarrow (S) \subset \mathfrak{p}$. On pourra donc considérer que $\mathcal{Z}(S)$ est $\mathcal{Z}((S))$ au besoin.

5.2.6 Proposition. — *Soit R un anneau commutatif et unitaire.*

(i) $\mathcal{Z}(0_R) = \mathrm{Spec}R$, $\mathcal{Z}(R) = \emptyset$,
(ii) Si $(S_i)_{i\in J}$ *est une famille de parties de* R, $\bigcap_{i\in I} \mathcal{Z}(S_i) = \mathcal{Z}(\bigcup_{i\in I} S_i)$,
(iii) Si $S, T \subset R$, $\mathcal{Z}(S) \cup \mathcal{Z}(T) = \mathcal{Z}((S \cdot T))$, *où* $S \cdot T = \{s.t; f \in S, t \in T\}$.

On en conclut que les parties $\mathcal{Z}(S), S \subset R$ forment les fermés d'une **topologie sur** $\mathrm{Spec}R$, *dont une base d'ouverts est donnée par les ouverts* $\mathrm{Spec}R_f$, $f \in R$, *dits* **ouverts fondamentaux de** $\mathrm{Spec}R$ *et définis par*

$$(\mathrm{Spec}R)_f = \mathrm{Spec}R \setminus \mathcal{Z}(f) := \{\mathfrak{p} \in R; f \notin \mathfrak{p}\}.$$

(iv) Si $I, J \subset R$ *sont deux idéaux,* $\mathcal{Z}(I) \subset \mathcal{Z}(J)$ *ssi* $\sqrt{J} \subset \sqrt{I}$.
(v) Si I *est un idéal de* R, $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$.

Démonstration. — Soit R un anneau commutatif et unitaire.

(ii) L'idéal premier $\mathfrak{p}$ contient tous les S_i ss'il contient leur réunion.
(iii) L'idéal premier $\mathfrak{p}$ contient S ou T ss'il contient $S \cdot T$. Notons que tout ouvert $\mathrm{Spec}R \setminus \mathcal{Z}(S)$ de $\mathrm{Spec}R$ est réunion (non nécessairement finie, contrairement au cas de la topologie de Zariski pour laquelle la noethérianité de $\mathbf{k}[x_1, \cdots, x_n]$ joue) des ouverts fondamentaux $(\mathrm{Spec}R)_f, f \in S$, de sorte que $((\mathrm{Spec}R)_f)_{f\in R}$ est bien une base d'ouverts de la topologie dont les fermées sont les $(\mathcal{Z}(S))_{S\subset R}$.

(iv) Si un idéal premier contenant I contient nécessairement J, alors du fait que le radical d'un idéal est l'intersection des idéaux premiers contenant cet idéal, on a bien $\sqrt{J} \subset \sqrt{I}$. Réciproquement, si $\sqrt{J} \subset \sqrt{I}$ et si $\mathfrak{p}$ est un idéal premier contenant I, alors il contient $\sqrt{I}$ (qui est l'intersection des idéaux premiers de R contenant I) et donc $\sqrt{J} \subset \mathfrak{p}$. Du fait que $J \subset \sqrt{J}$, on a bien $J \subset \mathfrak{p}$, soit $\mathfrak{p} \in \mathcal{Z}(J)$.

(v) Puisque $I \subset \sqrt{I}$, $\mathcal{Z}(\sqrt{I}) \subset \mathcal{Z}(I)$. Montrons que $\mathcal{Z}(I) \subset \mathcal{Z}(\sqrt{I})$. Si $\mathfrak{p} \in \mathcal{Z}(I)$, $I \subset \mathfrak{p}$. Mais alors $\sqrt{I} \subset \mathfrak{p}$, car si $a \in \sqrt{I}$, c'est-à-dire $a^n \in I$, pour $n \in \mathbb{N}$, on a aussi $a^n \in \mathfrak{p}$ et $\mathfrak{p}$ étant premier, $a \in \mathfrak{p}$.

□

Les points de $\mathrm{Spec}\, R$ ne sont pas nécessairement fermés pour la topologie que l'on vient de considérer, c'est-à-dire que l'espace topologique $\mathrm{Spec}\, R$ n'est pas $\mathbf{T_1}$ (cf section 1.5). Ceci découle de la caractérisation suivante de la clôture d'un point.

5.2.7 Proposition. — *Soit R un anneau commutatif unitaire et $\mathfrak{p} \in \mathrm{Spec}\, R$. Alors l'adhérence de $\mathfrak{p}$ est $\bar{\mathfrak{p}} = \mathcal{Z}(\mathfrak{p}) = \{\mathfrak{q} \in \mathrm{Spec}\, R; \mathfrak{p} \subset \mathfrak{q}\}$. En particulier le point $\mathfrak{p} \in \mathrm{Spec}\, R$ est fermé si et seulement l'idéal $\mathfrak{p}$ est maximal.*

Démonstration. — Par définition de la topologie sur $\mathrm{Spec}\, R$, $\mathcal{Z}(\mathfrak{p})$ est fermé. D'autre part si F est un fermé qui contient le singleton $\mathfrak{p}$, du fait que $F = \mathcal{Z}(S) = \{\mathfrak{q} \in \mathrm{Spec}\, R; S \subset \mathfrak{q}\}$ pour un certain $S \subset R$, on a $S \subset \mathfrak{p}$. Il s'ensuit que tout idéal premier $\mathfrak{q}$ contenant $\mathfrak{p}$, ie tout élément de $\mathcal{Z}(\mathfrak{p})$, contient aussi S, ie est un élément de $\mathcal{Z}(S)$. □

5.2.8 Remarque. — La Proposition 5.2.7 nous permet d'identifier de la façon suivante une variété X et $\mathrm{Spec}\, A(X)$. Jusque-là nous avions considéré $\mathrm{Spec}\, A(X)$ comme les idéaux maximaux de $A(X)$, identifiés aux points de X, enrichi des idéaux premiers de $A(X)$ (non maximaux), que l'on sait être en bijection avec les sous-variétés fermées de X (non réduites à des points de X). Désormais nous regardons $\mathrm{Spec}\, A(X)$ comme l'union de ses points non fermés $\mathfrak{p}$, chacun identifié à la sous-variété $\mathcal{Z}(\mathfrak{p})$ de X, et des points fermés de $\mathcal{Z}(\mathfrak{p})$ (ie les idéaux maximaux de $\mathrm{Spec}\, A(X)$ contenant $\mathfrak{p}$), en bijection avec les points de la variété $\mathcal{Z}(\mathfrak{p}) \subset X$. De sorte que $\mathrm{Spec}\, A(X)$ est la réunion des variétés fermées de X et des points de chacune d'elles. Dans cette représentation de $\mathrm{Spec}\, A(X)$, les points non fermés jouent un rôle particulier, comme nous allons le voir dans la suite.

Cette remarque nous conduit à la définition suivante.

5.2.9 Définition. — Soit R un anneau (unitaire) et Z un fermé irréductible de $\mathrm{Spec}\, R$. Un point $\mathfrak{p} \in Z$ est **un point générique de** Z lorsque $\bar{\mathfrak{p}} = Z$.

5.2.10 Proposition. — *Soit R un anneau commutatif unitaire.*

(i) Soit $\mathfrak{p} \in \mathrm{Spec}\, R$. Alors $\bar{\mathfrak{p}} = \mathcal{Z}(\mathfrak{p}) = \{\mathfrak{q} \in \mathrm{Spec}\, R; \mathfrak{p} \subset \mathfrak{q}\}$ est irréductible.

(ii) Réciproquement tout fermé irréductible Z de $\mathrm{Spec}\, R$ possède un unique point générique $\mathfrak{p}$, c'est-à-dire tel que $\bar{\mathfrak{p}} = \mathcal{Z}(\mathfrak{p}) = Z$.

Démonstration. — (i) D'après la Proposition 5.2.7, $\bar{\mathfrak{p}} = \mathcal{Z}(\mathfrak{p})$. Il s'agit alors de démontrer que $\bar{\mathfrak{p}}$ est irréductible. Or si $\bar{\mathfrak{p}} = Z_1 \cup Z_2$, où Z_1, Z_2 sont deux fermés de $\operatorname{Spec} R$, on a par exemple $\mathfrak{p} \in Z_1$, donc $Z_1 \subset \bar{\mathfrak{p}} \subset Z_1$, puisque $\bar{\mathfrak{p}}$ est le plus petit fermé contenant $\mathfrak{p}$. Soit $Z_1 = \mathcal{Z}(\mathfrak{p})$.

(ii) Soit Z un fermé irréductible de $\operatorname{Spec} R$. Montrons qu'existe $\mathfrak{p} \in \operatorname{Spec} R$ tel que $\mathcal{Z}(p) = Z$. On suppose que $Z = Z(I)$ où I est un idéal de R, en vertu de la Remarque 5.2.5, et d'après la Proposition 5.2.6 (v), on peut aussi supposer que $I = \sqrt{I}$. Nous allons montrer que I est un idéal premier de R, ce qui montrera que Z est l'adhérence d'un point de $\operatorname{Spec} R$. Pour cela supposons qu'existent $f, g \in R$ tels que $f \cdot g \in I$ et $f \notin I, g \notin I$. Notons $J = I + (f)$ et $K = I + (g)$. Alors si $h = a + \alpha \cdot f = b + \beta \cdot g \in J \cap K$, où $a, b \in I, \alpha, \beta \in R$, on a $h^2 = \alpha \cdot \beta \cdot f \cdot g + a \cdot (\beta \cdot g + b) + b \cdot (\alpha \cdot f) \in I$. Par conséquent, du fait que I est supposé radical, $h \in I$, ce qui prouve que $I = J \cap K$ et donc $Z = \mathcal{Z}(J) \cup \mathcal{Z}(K)$. Maintenant puisque I est radical, I est l'intersection des idéaux premiers le contenant et il existe alors un idéal premier $\mathfrak{p}$ de R contenant I mais ne contenant pas f. On a d'une part $\mathfrak{p} \in Z = \mathcal{Z}(I)$, puisque $I \subset \mathfrak{p}$ et d'autre part $\mathfrak{p} \notin \mathcal{Z}(J) = \{\mathfrak{q} \in \operatorname{Spec} R; J \subset \mathfrak{q}\}$, puisque $f \in J, f \notin \mathfrak{p}$. Il s'ensuit que $\mathcal{Z}(J) \subsetneq Z$. Et de même $\mathcal{Z}(K) \subsetneq Z$. En conclusion l'hypothèse que I tel que $Z = \mathcal{Z}(I)$ n'est pas premier contredit le fait que Z est irréductible. Montrons enfin l'unicité du point $\mathfrak{p}$ tel que $\mathcal{Z}(\mathfrak{p}) = Z$, lorsque Z est irréductible. S'il existe $\mathfrak{q}$ tel que $\bar{\mathfrak{q}} = \bar{\mathfrak{p}}$, de $\bar{\mathfrak{q}} = \mathcal{Z}(\mathfrak{q}) = \{\mathfrak{s} \in \operatorname{Spec} R; \mathfrak{q} \subset \mathfrak{s}\} =$ et de $\mathfrak{p} \in \bar{\mathfrak{q}}$, il vient $\mathfrak{q} \subset \mathfrak{p}$. Par symétrie on obtient $\mathfrak{p} = \mathfrak{q}$.

□

5.2.11 Remarque. — Un idéal premier non maximal $\mathfrak{p} \in \operatorname{Spec} R$ s'appelle le *point générique* de $\mathcal{Z}(\mathfrak{p})$ pour la raison suivante. Considérons que R est l'anneau $\mathbf{k}[x, y]$. les idéaux (x) et (y) de R sont des idéaux premiers de R ($R/(x) = \mathbf{k}[y]$ est intègre) non maximaux, donc sont les points génériques de $\mathcal{Z}(x)$ et $\mathcal{Z}(y)$ respectivement. Notons que $(y) \in \operatorname{Spec} R \setminus \mathcal{Z}(x)$, puisque $x \notin (y)$. Autrement dit le point générique de $\mathcal{Z}(y)$ ne rencontre pas $\mathcal{Z}(x)$, ce qui correspond à l'interprétation géométrique que l'on a en tête en songeant aux ensembles algébriques $y = 0$ et $x = 0$ de $\mathbf{k}^2$, qui, bien que s'intersectant en l'origine, ne se rencontrent pas pour un ensemble générique de points (ie ouvert pour la topologie de Zariski) de chacun d'eux. De plus, les ensembles fermés $\mathcal{Z}(x)$ et $\mathcal{Z}(y)$ de $\operatorname{Spec} R$ (et non plus seulement de $\mathbf{k}^2$) s'intersectent bien, puisque $\mathfrak{p} \in \mathcal{Z}(x) \cap \mathcal{Z}(y)$ si et seulement si $x, y \in \mathfrak{p}$, soit $\mathcal{Z}(x) \cap \mathcal{Z}(y) = (x, y)$. Autrement dit $\mathcal{Z}(x) \cap \mathcal{Z}(y)$ est l'idéal maximal (x, y) de R, qui s'identifie à l'origine de $\mathbf{k}^2$.

5.2.12 Remarque. — La Proposition 5.2.10 nous apprend que l'application

$$\begin{array}{rccc} \mathcal{Z} : & \{ \text{ idéaux de } R \} & \to & \{ \text{ fermés de } \operatorname{Spec} R \} \\ & I & \mapsto & \mathcal{Z}(I) \end{array}$$

induit une bijection

$$\begin{array}{rccc} \mathcal{Z}' : & \{ \text{ idéaux premiers de } R \} = \operatorname{Spec} R & \to & \{ \text{ fermés irréductibles de } \operatorname{Spec} R \} \\ & \mathfrak{p} & \mapsto & \mathcal{Z}(\mathfrak{p}) \end{array}$$

Mais en général l'application $\mathcal{Z}$ n'est pas injective, car d'après par exemple la Proposition 5.2.6 (v), donne $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$. La Proposition 5.2.6 (iv) nous dit même que $\mathcal{Z}(I) = \mathcal{Z}(J)$ ssi $\sqrt{I} = \sqrt{J}$.

D'autre part, on pourrait comme on l'a fait dans le cas des ensembles algébriques sur $\mathbf{k}^n$ définir une application $\mathcal{I}$

$$\begin{array}{rccc} \mathcal{I} : & \{ \text{ fermés de } \operatorname{Spec} R \} \} & \to & \{ \text{ idéaux de } R \} \\ & Z & \mapsto & \mathcal{I}(Z) \end{array}$$

par $\mathcal{I}(Z) := \{f \in R; f(\mathfrak{p}) = 0_{k(\mathfrak{p})}, \forall \mathfrak{p} \in Z\} = \{f \in R; f \in \mathfrak{p}, \forall \mathfrak{p} \in Z\} = \cap_{\mathfrak{p} \in Z} \mathfrak{p}$. Si $Z = \mathcal{Z}(I)$, pour un certain idéal I, nous obtenons $\mathcal{I}(Z(I)) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R, I \subset \mathfrak{p}} \mathfrak{p} = \sqrt{I}$. On peut dons énoncer la première égalité de la Proposition suivante.

5.2.13 Proposition. — *Soit R un anneau unitaire et I un idéal de R. On a*

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}.$$

De plus l'application

$$\begin{array}{rccc} \mathcal{I} : & \{ \textit{ fermés de } \operatorname{Spec} R \} \} & \to & \{ \textit{ idéaux de } R \} \\ & Z & \mapsto & \mathcal{I}(Z) \end{array}$$

est injective, d'inverse à gauche l'application $\mathcal{Z}$.

On obtient donc dans notre cadre, assez directement depuis les définitions, le Nullstellensatz. La seconde partie de la Proposition 5.2.13 se montre comme suit. Si I est un idéal de R et $Z = \mathcal{Z}(I)$, $\mathcal{Z}(\mathcal{I}(Z)) = \mathcal{Z}(\sqrt{I})$. Mais par la Proposition 5.2.6 (v), $\mathcal{Z}(\sqrt{I}) = \mathcal{Z}(I)$, ce qui donne finalement

$$\mathcal{Z}(\mathcal{I}(Z)) = Z.$$

L'application $\mathcal{I}$ est ainsi injective, comme dans le cas des ensembles algébriques de $\mathbf{k}^n$.

La Proposition 5.2.13 nous donne une version, pour le spectre d'un anneau, du Nullstellensatz. Rappelons que le Nullstellensatz, dans le cas des corps algébriquement clos est facilement équivalent au Nullstellensatz faible qui stipule lui que si I est un idéal propre de $\mathbf{k}[x_1, \cdots, x_n]$, $\mathcal{Z}(I)$ n'est pas vide. Ou encore que si $\mathcal{Z}(I)$ est vide, $1 \in I$. Notons, en passant au complémentaire, que dire que $\mathcal{Z}(I) = \emptyset$ revient à dire que $\mathbf{k}^n = \cup_{f \in I} \mathbf{k}^n_f$. Nous disposons dans le cadre du spectre d'un anneau de la version suivante du Nullstellensatz faible.

5.2.14 Proposition. — *Soit $(f_i)_{i \in E}$ une famille d'éléments d'un anneau unitaire R et I l'idéal que cette famille engendre. Alors*

$$\operatorname{Spec} R = \cup_i (\operatorname{Spec} R)_{f_i} \Longleftrightarrow 1_R \in I$$

Démonstration. — Nous avons $\mathrm{Spec}R = \cup_i (\mathrm{Spec}R)_{f_i}$ si et seulement si pour tout $\mathfrak{p} \in \mathrm{Spec}R$ existe f_i tel que $f_i \notin \mathfrak{p}$. Ainsi aucun élément $\mathfrak{p} \in \mathrm{Spec}R$ ne contient I, ce qui oblige $I = R$. □

5.2.15 Proposition. — *Soit un anneau unitaire R et $f \in R$. L'espace topologique $(\mathrm{Spec}R)_f$ est quasi-compact. En particulier l'espace topologique $\mathrm{Spec}R$ est quasi-compact.*

Démonstration. — Il suffit de prouver que de tout recouvrement de $(\mathrm{Spec}R)_f$ par des ouverts fondamentaux $(\mathrm{Spec}R)_{f_i}, i \in E$ de $\mathrm{Spec}R$, on peut extraire un sous-recouvrement fini. Notons I l'idéal engendré par la famille $(f_i)_{i\in E}$. L'égalité $(\mathrm{Spec}R)_f = \cup_i (\mathrm{Spec}R)_{f_i}$ signifie que quel que soit $\mathfrak{p} \in \mathrm{Spec}R$, $f \notin \mathfrak{p} \iff \exists i \in E, f_i \notin \mathfrak{p}$. Soit

$$\forall \mathfrak{p} \in \mathrm{Spec}R, f \in \mathfrak{p} \iff \forall i \in E, f_i \in \mathfrak{p} \iff I \subset \mathfrak{p}.$$

On en déduit que

$$\sqrt{(f)} = \sqrt{I}.$$

Puisque $f \in \sqrt{I}$, il existe $n, \ell \in \mathbb{N}$, $f_{i_1}, \cdots, f_{i_\ell}, \alpha_1 \in R, \cdots, \alpha_\ell \in R$ tels que $f^n = \sum_{j=1}^{\ell} \alpha_j f_{i_j}$. Notons I' l'idéal de type fini engendré par les $f_{i_j}, j \in \{1, \cdots, \ell\}$. Si $\mathfrak{p} \in \mathrm{Spec}R$ est tel que $\mathfrak{p} \in \mathcal{Z}(I')$, on a $I' \subset \mathfrak{p}$, donc $f^n \in \mathfrak{p}$ et du fait que $\mathfrak{p}$ est premier, on obtient $f \in \mathfrak{p}$, soit $\mathfrak{p} \in \mathcal{Z}(f)$. Il s'ensuit que les zéros de I' sont dans ceux de f et que par conséquent $(\mathrm{Spec}R)_f = \bigcup_{j=1,\cdots,\ell} (\mathrm{Spec}R)_{f_{i_j}}$.

La quasi-compacité de $\mathrm{Spec}R$ s'obtient en considérant $f = 1$. □

Rappelons que la Remarque 2.1.14 et la Remarque 2.6.14 montrent respectivement que les ensembles algébriques de $\mathbf{k}^n$ et les prévariétés sur $\mathbf{k}$ sont des espaces quasi-compacts.

5.3. L'espace localement annelé $\mathrm{Spec}R$

Lorsque X est un ensemble algébrique de $\mathbf{k}^n$, nous avons défini un faisceau $\mathcal{O}_X$, dit faisceau structural de X, en définissant tout d'abord les fibres de ce faisceau qui sont les germes de fonctions régulières en un point donné. Nous avons ensuite défini, pour un ouvert U de X, $\mathcal{O}(U)$, les fonctions régulières sur U comme les fonctions sur U qui en chaque point de U représentent un germe de fonction régulière en ce point. Les germes des fonctions régulières en $a \in X$ forment l'anneau localisé de l'algèbre affine de X par l'idéal maximal $(x_1 - a_1, \cdots, x_n - a_n)$ de $\mathbf{k}[x_1, \cdots, x_n]$ correspondant au point a (cf Remarque 2.4.10). L'anneau $\mathcal{O}_X(U)$ est obtenu comme l'intersection de tous les anneaux $\mathcal{O}_{X,a} = A(X)_{I(\{a\})}$, $a \in U$, ce qui a un sens car les éléments des anneaux locaux $\mathcal{O}_{X,a}$ sont tous dans le même ensemble, le corps des fractions $\mathbf{k}(X)$ de X. Imiter cette démarche reviendrait à former, pour un ouvert U

de $\operatorname{Spec} R$, l'intersection des anneaux locaux $R_{\mathfrak{p}}$[(1)], pour $\mathfrak{p} \in U$ (ici on n'exige pas que le point $\mathfrak{p}$ soit fermé, ie que l'idéal $\mathfrak{p}$ soit maximal), mais ceci n'aurait pas de sens puisque les anneaux $R_{\mathfrak{p}}$ ne sont pas dans un anneau commun. En effet aucune hypothèse n'étant faite sur l'intégrité de l'anneau R, on ne peut pas considérer que les localisés $R_{\mathfrak{p}}$ sont dans le corps des fractions de R. On peut cependant considérer qu'un élément de l'anneau $\mathcal{O}_X(U)$, anneau que l'on cherche à définir, est la donnée

1. d'une famille $(f_{\mathfrak{p}})_{\mathfrak{p}\in U}$, avec $f_{\mathfrak{p}} \in R_{\mathfrak{p}}$,
2. de sorte que les membres de cette famille coïncident tous, Zariski-localement, avec un même élément fractionnaire en un certain sens.

La condition 2 assure que le famille $(f_{\mathfrak{p}})_{\mathfrak{p}\in U}$ représente un seul élément (fractionnaire en un certain sens) et la condition 1 que cette fraction est bien définie en tout point de U, c'est-à-dire est sans pôle sur U. Nous sommes donc conduit à la définition suivante.

5.3.1 Définition. — Soit R un anneau commutatif et unitaire, U un ouvert de $\operatorname{Spec} R$. On définit

$$\mathcal{O}_{\operatorname{Spec} R}(U) := \{f = (f_{\mathfrak{p}})_{\mathfrak{p}\in U}; f_{\mathfrak{p}} \in R_{\mathfrak{p}} \ \ \& \ \ \forall \mathfrak{u} \in U, \ \exists V \text{ un ouvert de } U \text{ contenant } \mathfrak{u}$$
$$g, h \in R \text{ tels que } \forall \mathfrak{p} \in V, f_{\mathfrak{p}} = \frac{g}{h}\}.$$

5.3.2 Remarque. — Dans la Définition 5.3.1 l'écriture $f_{\mathfrak{p}} = \frac{g}{h}$ signifie implicitement que h n'est pas dans l'idéal premier $\mathfrak{p}$ (ie $h(\mathfrak{p}) \neq 0$) et que $\frac{g}{h}$ est l'élément fractionnaire $\frac{g}{h}$ de $R_{\mathfrak{p}}$ formé avec g et h. Ainsi pour un ensemble d'indices V, avec V ouvert de U, les éléments $(f_{\mathfrak{p}})_{\mathfrak{p}\in V}$ de la famille f, coïncident tous avec une paire fractionnaire $(g, h) \in R^2$ qui se réalise dans tous les anneaux locaux $R_q, \mathfrak{q} \in V$ du fait que $h(\mathfrak{q}) \neq 0$.

5.3.3 Proposition. — *Soit R un anneau commutatif et unitaire et notons $\mathcal{T}$ la topologie définie sur R dans la Proposition 5.2.6. La famille $(\mathcal{O}_{\operatorname{Spec} R}(U))_{U\in\mathcal{T}}$ définit un faisceau d'anneaux $\mathcal{O}_{\operatorname{Spec} R}$ sur* $\operatorname{Spec} R$.

Démonstration. — Il est clair que pour $U \in \mathcal{T}$, l'ensemble $\mathcal{O}_{\operatorname{Spec} R}(U)$ est un anneau, puisqu'il s'agit d'un sous-anneau de l'anneau $\{\varphi : U \to \prod_{\mathfrak{p}\in U} R_{\mathfrak{p}}\}$. L'application de restriction est ainsi donnée : si $U \subset V$ est une inclusion d'ouverts de $\mathcal{T}$, et si $f = (f_{\mathfrak{p}})_{\mathfrak{p}\in V}$, $f_{|U} = (f_{\mathfrak{p}})_{\mathfrak{p}\in U}$. Il est alors immédiat de constater que les propriétés définissant $\mathcal{O}_{\operatorname{Spec} R}(U)$ sont héritées de celles définissant $\mathcal{O}_{\operatorname{Spec} R}(V)$. Enfin la propriété de recollement a lieu. En effet, soit $(U_i)_{i\in I}$ une famille d'ouverts d'un ouvert $U \in \mathcal{T}$ et $(f_i)_{i\in I}$ une famille de sections f_i sur U_i (ie $f_i \in \mathcal{O}_{\operatorname{Spec} R}(U_i)$) telle que pour tout $i, j \in I$, $f_{i|U_i\cap U_j} = f_{j|U_i\cap U_j}$. On définit la famille $f = (f_{\mathfrak{p}})_{\mathfrak{p}\in U}$ par $f_{\mathfrak{p}} = f_{i_{\mathfrak{p}}}$, quel que soit $i \in I$ tel que $\mathfrak{p} \in U_i$. Ceci définit bien une famille en vertu de $i, j \in I$,

(1)La notation $R_{\mathfrak{p}}$ désigne sans ambigüité le localisé de R par l'idéal premier $\mathfrak{p}$, cf Remarque 1.3.15, 4. Rappelons que d'après la Proposition 1.3.16 (i), $R_{\mathfrak{p}} = \{g/h; g \in R, h \notin \mathfrak{p}\}$ est un anneau local d'idéal maximal $\{g/h; g \in \mathfrak{p}, h \notin \mathfrak{p}\}$.

$f_{i|U_i\cap U_j} = f_{j|U_i\cap U_j}$ et on a de plus $f_{\mathfrak{p}} = f_{i_{\mathfrak{p}}} \in R_{\mathfrak{p}}$. Maintenant si $\mathfrak{u} \in U$, il existe $i \in I$ tel que $\mathfrak{u} \in U_i$ et il existe V un ouvert de U_i contenant $\mathfrak{u}$, $g, h \in R$ tels que pour tout $\mathfrak{p} \in V$, $f_{\mathfrak{p}} = f_{i_{\mathfrak{p}}} = \dfrac{g}{h} \in R_{\mathfrak{p}}$. Mais étant un ouvert de U_i, V est a fortiori un ouvert de U. □

***5.3.4 Remarque* (Fibre $\mathcal{O}_{\mathrm{Spec}\,R,\mathfrak{p}}$ du faisceau $\mathcal{O}_{\mathrm{Spec}\,R}$ en $\mathfrak{p}$)**

D'après la Définition 2.5.7, la fibre $\mathcal{O}_{\mathrm{Spec}\,R,\mathfrak{p}}$ du faisceau $\mathcal{O}_{\mathrm{Spec}\,R}$ en $\mathfrak{p} \in R$ est définie comme l'ensemble des paires $(U, f) \in \mathcal{T} \times \mathcal{O}_{\mathrm{Spec}\,R}(U)$, avec $\mathfrak{p} \in U$, modulo la relation d'équivalence $(U, f) \sim (V, g) \iff f_{|W} = g_{|W}$, pour un certain voisinage ouvert W de $\mathfrak{p}$ inclus dans $U \cap V$. La structure d'anneau de $\mathcal{O}_{\mathrm{Spec}\,R,\mathfrak{p}}$ étant définie par celle des anneaux $\mathcal{O}_{\mathrm{Spec}\,R}(U)$. Notons $f = (f_{\mathfrak{q}})_{\mathfrak{q}\in U}$ un élément de $\mathcal{O}_{\mathrm{Spec}\,R}(U)$, conformément à la Définition 5.3.1. La fibre $\mathcal{O}_{\mathrm{Spec}\,R,\mathfrak{p}}$ est alors définie comme l'ensemble des $(f_{\mathfrak{q}})_{\mathfrak{q}\in U}$, où U est un voisinage ouvert de $\mathfrak{p}$ dans $\mathrm{Spec}\,R$ modulo la relation d'équivalence

$$(f_{\mathfrak{q}})_{\mathfrak{q}\in U} \sim (g_{\mathfrak{r}})_{\mathfrak{r}\in V} \iff (f_{\mathfrak{q}})_{\mathfrak{q}\in W} = (g_{\mathfrak{q}})_{\mathfrak{q}\in W},$$

pour un certain voisinage ouvert W de $\mathfrak{p}$ inclus dans $U \cap V$. Notons enfin que $(f_{\mathfrak{q}})_{\mathfrak{q}\in W} = (g_{\mathfrak{q}})_{\mathfrak{q}\in W}$ implique que pour tout $\mathfrak{w} \in W$ existe un voisinage ouvert W' de $\mathfrak{w}$ et $h, \ell \in R$ tels que $\forall \mathfrak{q} \in W'$, $f_{\mathfrak{q}} = g_{\mathfrak{q}} = \dfrac{h}{\ell} \in R_{\mathfrak{q}}$. Finalement, $(f_{\mathfrak{q}})_{\mathfrak{q}\in U} \sim (g_{\mathfrak{r}})_{\mathfrak{r}\in V}$ équivaut à dire qu'existe un voisinage ouvert W' de $\mathfrak{p}$ et $h, \ell \in R$ tels que $\forall \mathfrak{q} \in W'$, $f_{\mathfrak{q}} = g_{\mathfrak{q}} = \dfrac{h}{\ell} \in R_{\mathfrak{q}}$.

Le Remarque 2.4.10 nous montre que, dans le cas des ensembles algébriques irréductibles de $\mathbf{k}^n$, la fibre $\mathcal{O}_{X,x}$ du faisceau structural est l'anneau $A(X)$ localisé en l'idéal maximal correspondant au point x.

D'autre part, dans le cas où $\mathbf{k}$ est algébriquement clos, la Proposition 2.4.11 nous assure que pour tout $P \in \mathbf{k}[x_1, \cdots, x_n]$, $\mathcal{O}_X(X_P) = A(X)_P$ ($A(X)_P$ désignant la localisation de $A(X)$ par la partie multiplicative $\{P^r; r \in \mathbb{N}\}$, cf Remarque 1.3.15, 5). La conséquence de cette proposition est alors que les sections globales sur X de $\mathcal{O}_X$ sont les fonctions polynomiales sur X.

Dans le cadre du spectre d'un anneau, nous disposons de l'équivalent suivant de la Remarque 2.4.10 et de la Proposition 2.4.11.

5.3.5 Proposition. — *Soit R un anneau commutatif et unitaire.*

(i) Pour tout $\mathfrak{p} \in \mathrm{Spec}\,R$, on a

$$\mathcal{O}_{\mathrm{Spec}\,R,\mathfrak{p}} = R_{\mathfrak{p}}.$$

En particulier, l'anneau $R_{\mathfrak{p}}$ étant local (cf Proposition 1.3.16), $(\mathrm{Spec}\,R, \mathcal{O}_{\mathrm{Spec}\,R})$ est un espace localement annelé.

(ii) Pour tout $f \in R$, on a

$$\mathcal{O}_{\mathrm{Spec}\,R}((\mathrm{Spec}\,R)_f) = {R_f}^{(2)}.$$

(2) Rappelons que l'on note R_f l'anneau R_S, où S est la partie multiplicative de A donnée par les puissances de f et que $R_1 \simeq R$.

En particulier,

$$\mathcal{O}_{\operatorname{Spec} R}(\operatorname{Spec} R) = R.$$

Démonstration. — (i) Désignons par $\overline{(U, f)}$ la classe de (U, f) dans $\mathcal{O}_{\operatorname{Spec} R, \mathfrak{p}}$. On considère alors l'application

$$\begin{array}{rccc} \psi : & \mathcal{O}_{\operatorname{Spec} R, \mathfrak{p}} & \to & R_{\mathfrak{p}} \\ & \overline{(U, f)} & \mapsto & f_{\mathfrak{p}} \end{array}$$

Il est bien clair que cette application ne dépend pas du choix d'un représentant de la classe $\overline{(U, f)}$, puisque si f et g coïncident sur un ouvert W de $\operatorname{Spec} R$ contenant $\mathfrak{p}$, on a $(f_{\mathfrak{q}})_{\mathfrak{q} \in W} = (g_{\mathfrak{q}})_{\mathfrak{q} \in W}$ et en particulier $f_{\mathfrak{p}} = g_{\mathfrak{p}}$.

Montrons que ψ est injective.

Montrons que ψ est surjective.

(ii)

□

Hartshorne P. 82, schéma réduit etc...

CHAPITRE 6

COHOMOLOGIE DES FAISCEAUX

BIBLIOGRAPHIE

[1] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete 36, Springer-Verlag, Berlin, (1998)

[2] N. Bourbaki, *Éléments de Mathématiques XI. Première partie : Les structures fondamentales de l'analyse.*, Chaptitre 5, Corps commutatifs, Actualités Sci. Ind., no. 1102. Hermann et Cie., Paris, 1950

[3] Z. Chatzidakis, Introductory notes on the model theory of valued fields, Motivic Integration and its Interactions with Model Theory and Non-Archimedean Geometry Series, London Mathematical Society Lecture Note Series (No. 383), (2011)

[4] C. C. Chang, H, J. Keisler, Model Theory.Stud. Log. **73** North-Holland Publishing Company, (1973)

[5] M. Coste, An introduction to semialgebraic geometry. Universita di Pisa, Dottorato di recerca in Matematica, Istituti editoriali poligrafici internazionali, Pise-Rome, (2000)

[6] L. van den Dries, Tame topology and o-minimal structures. *London Mathematical Society Lecture Note Series*, **248**, Cambridge University Press, Cambridge, (1998)

[7] A. Gathmann, Algebraic geometry, Notes for a class taught at the university of Kaiserslautern 2002-2003, http ://www.mathematik.uni-kl.de/ gathmann/class/alggeom-2002/main.pdf

[8] R. Hartshorne, Algebraic geometry, *Graduate Texts in Mathematics*, No. **52**, Springer-Verlag, New York-Heidelberg, (1977)

[9] W. Hodges, A shorter model theory. *Cambridge University Press*, Cambridge, (1997)

[10] F. Loeser, Un premier cours de logique, http ://www.math.ens.fr/ loeser/

[11] S. Lang, Algebra, Revised third version, Graduate texts in Mathematics 211, Springer-Verlag (2002)

[12] D. Marker, M. Messmer, A. Pillay, Model theory of fields, Second edition, *Lecture Notes in Logic*, **5**, Association for Symbolic Logic, La Jolla, CA ; A K Peters, Ltd., Wellesley, MA, (2006)

[13] J.S. Milne, Algebraic geometry, http ://www.jmilne.org/math/CourseNotes/AG.pdf

[14] D. Mumford, The red book of varieties and schemes. Second, expanded edition. Includes the Michigan lectures (1974) on curves and their Jacobians. With contributions by Enrico Arbarello. *Lecture Notes in Mathematics*, **1358**, Springer-Verlag, Berlin, (1999)

[15] D. Perrin, Géométrie algébrique, une introduction, *Savoirs Actuels, InterEditions, CNRS Éditions*, (1995)

[16] C. Peskine, An algebraic introduction to complex projective geometry, 1. Commutative algebra *Cambridge studies in advanced mathematics,* **47**, (1996)

[17] A. Prestel, Model theory for the real algebraic geometer, *Universita di Pisa, Dottorato di recerca in Matematica, Istituti editoriali poligrafici internazionali, Pise-Rome* (1998)

[18] S. Seidenberg, A new decision method for elementary algebra. *Ann. of Math.* **60**, (1954), 365-374

[19] A. Tarski, A decision method for elementary algebra and geometry, 2nd ed. University of California Press, Berkeley and Los Angeles, Calif., (1951)