Le Nullstellensatz, diverses preuves et applications en algèbre commutative et théorie de la dimension.

Laurent Dietrich *

9 septembre 2010

Résumé

Mon stage de M1 à l'institut mathématique de Bordeaux a consisté à étudier profondément un des théorèmes fondamentaux de l'algèbre commutative et de la géométrie algébrique : le théorème des zéros de Hilbert ("Nullstellensatz"). Dans ce rapport, je tenterai de présenter ses tenants et aboutissants : présenter ses différentes formes, une liste de ses preuves (du moins de preuves utilisant des idées fondamentalement différentes), tenter d'esquisser quelques généralisations et l'illustrer à l'aide de diverses applications. J'ai ensuite évolué vers des aspects plus géométriques tout en appronfondissant l'algèbre dans le détail de certains outils intéréssants.

*http://perso.eleves.bretagne.ens-cachan.fr/∼ldiet783

Table des matières

1 Introduction, notations **3**

2 Les différentes formes **3**
2.1 Les trois formes courantes 3
2.2 Des formes différentes 5

3 Différentes démonstrations, différentes hypothèses **6**
3.1 Le cas simple d'un corps algébriquement clos indénombrable 6
3.2 Le cas général. 7
3.3 La généralisation de Bourbaki 9
3.3.1 Le théorème 9
3.3.2 le Nullstellensatz 10
3.3.3 Annexe : anneaux de Jacobson – vers le Nullstellensatz 11

4 Applications **12**
4.1 Espace tangent 12
4.2 Décomposition en irréductibles 15
4.3 Quelques calculs : la puissance des bases de Grœbner 16
4.4 Équivalence de deux catégories 19

5 Un peu de théorie de la dimension **21**
5.1 Introduction, énoncé 21
5.2 Le going-up de Cohen-Seidenberg 21
5.3 Preuve du théorème 23

6 Conclusion **25**

1 Introduction, notations

Soit A un anneau et I un idéal de A. On notera $\sqrt{I}$ le radical de I (l'ensemble des éléments de A dont une puissance figure dans I). On utilisera les applications bien connues $\mathcal{Z}$ et $\mathcal{J}$: si k est un corps et S une partie de $k[X_1, \cdots, X_n]$, $\mathcal{Z}(I)$ dénotera l'ensemble algébrique défini par S (l'ensemble des zéros communs dans k^n de tous les éléments de S). Si V est un ensemble algébrique de k^n, $\mathcal{J}(V)$ dénotera l'idéal des polynômes de $k[X_1, \cdots, X_n]$ s'annulant sur V. On utilisera à maintes reprises les propriétés de base sur ces applications, qu'on ne redémontrera pas, en vrac :

- elles renversent les inclusions.
- $\mathcal{Z}(S) = \mathcal{Z}(\langle S \rangle)$.
- $\mathcal{Z}(I) = \mathcal{Z}\left(\sqrt{I}\right)$.
- $\mathcal{Z}(S \cup S') = \mathcal{Z}(S) \cap \mathcal{Z}(S')$.
- $\mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.
- $\mathcal{J}(V) = \sqrt{\mathcal{J}(V)}$.
- $\mathcal{J}(V \cup V') = \mathcal{J}(V) \cap \mathcal{J}(V')$.
- $I \subset \mathcal{J}(\mathcal{Z}(I))$.
- $S \subset \mathcal{Z}(\mathcal{J}(S))$ avec égalité si et seulement S est algébrique (c'est-à-dire est dans l'image de $\mathcal{Z}$).

Ainsi l'application

$$\begin{array}{rcl} \{\text{ensembles algébriques de } k^n\} & \to & \{\text{idéaux radiciels de } k[X_1, \cdots, X_n]\} \\ V & \mapsto & \mathcal{J}(V) \end{array}$$

est injective d'inverse à gauche

$$\begin{array}{rcl} \{\text{idéaux de } k[X_1, \cdots, X_n]\} & \to & \{\text{ensembles algébriques de } k^n\} \\ I & \mapsto & \mathcal{Z}(I) \end{array}$$

Le théorème des zéros de Hilbert ou *Nullstellensatz* fournit la réponse à la question (entre autres) : à quelle classe d'ideaux faut-il se restreindre pour avoir une bijection ? Ce sont les *idéaux radiciels*.

2 Les différentes formes

2.1 Les trois formes courantes

C'est les trois versions qu'on rencontre le plus dans la littérature. Les deux premières prennent les noms de "forme faible" et "forme forte", car on a tendance à démontrer la première, puis de s'en servir pour démontrer la deuxième, même si elles sont équivalentes. En effet, elles sont toutes deux équivalentes à une troisième forme, que j'appellerai "intermédiaire". Une fois ceci pris en compte, il est clair que les locutions "faible" et "forte" n'ont plus vraiment de sens dans un mémoire qui voyagera entre ces différentes formes équivalentes, aussi je continuerai de les utiliser pour leur côté historique, mais entre guillemets.

Théorème 2.1.1. *(Théorème des zéros de Hilbert ou Nullstellensatz.) Soit k un corps algébriquement clos, alors les trois propositions équivalentes suivantes sont vérifiées.*

1. *(Forme "faible"). Soit $\mathfrak{m} \subsetneq k[X_1, \cdots, X_n]$ un idéal maximal, alors il existe $(a_1, \cdots, a_n) \in k^n$ tel que*

$$\mathfrak{m} = \langle X_1 - a_1, \cdots, X_n - a_n \rangle.$$

2. *(Forme "forte"). Pour tout idéal* $I \subsetneq k[X_1, \cdots, X_n]$ *on a*
$$\mathcal{J}(\mathcal{Z}(I)) = \sqrt{I}.$$
3. *(Forme "intermédiaire"). Soit* $I \subsetneq k[X_1, \cdots, X_n]$ *un idéal strict, alors*
$$\mathcal{Z}(I) \neq \varnothing.$$

Ce théorème est le début du dictionnaire algèbre commutative – géométrie, au sens où il établit via la forme "faible", une bijection entre les points de k^n et les idéaux maximaux de l'anneau polynôme, et plus généralement (forme "forte") entre les ensembles algébriques de k^n de façon générale, et les idéaux radiciels (égaux à leur racine) de l'anneau polynôme. La forme "forte", de façon purement algébrique, décrète que si f est nul sur $\mathcal{Z}(I)$, alors il existe un entier positif m tel que $f^m \in I$. Ces différentes formes seront montrées de plusieurs façons dans la partie suivante. Pour l'instant on va se contenter de démontrer leur équivalence. Il y a une moitié du travail assez facile : prouver la forme intermédiaire à partir d'une autre. Mais l'autre moitié l'est clairement moins. On se doute qu'il y a un peu de travail à fournir, tant ces formulations ne se ressemblent pas *a priori*, en atteste leurs dénominations.

Démonstration. (De la moitié facile.)
- $1 \Rightarrow 3$: soit I un idéal strict, par le théorème de Krull il existe un idéal maximal $I \subset \mathfrak{m}$, donc $\mathcal{Z}(\mathfrak{m}) \subset \mathcal{Z}(I)$. Or par 1, $\mathcal{Z}(\mathfrak{m})$ est clairement non vide puisqu'il contient $(a_1, \cdots, a_n)$.
- $2 \Rightarrow 3$ par contraposée : soit I un idéal, si $\mathcal{Z}(I) = \varnothing$, alors $\sqrt{I} = \mathcal{J}(\varnothing) = k[X_1, \cdots, X_n]$ Donc $1 \in \sqrt{I}$ donc $1 \in I$ soit $I = k[X_1, \cdots, X_n]$.

□

Nous allons avoir besoin d'un lemme un tantinet technique pour la suite.

Lemme 2.1.2. *Soit* $(a_1, \cdots, a_n) \in k^n$*, l'idéal* $\langle X_1 - a_1, \cdots, X_n - a_n \rangle$ *est maximal et égal à* $\mathcal{J}(\{a_1, \cdots, a_n\})$.

Démonstration. Par définition, $\mathcal{J}(\{a_1, \cdots, a_n\})$ est le noyau du morphisme (surjectif) d'évaluation des polynômes en $(a_1, \cdots, a_n)$, morphisme qu'on notera $\text{éval}_{(a_1, \cdots, a_n)}$. Clairement,
$$\langle X_1 - a_1, \cdots, X_n - a_n \rangle \subset \ker \text{éval}_{(a_1, \cdots, a_n)}.$$
On montre l'autre inclusion par récurrence. Le cas $n = 1$ est résolu par une simple division euclidienne dans $k[X_1]$ suivie d'une évaluation en a_1. Supposons le résultat vrai au rang $n-1$ et soit $f \in \ker \text{éval}_{(a_1, \cdots, a_n)}$. On divise f par $X_1 - a_1$ (unitaire) dans $k[X_2, \cdots, X_n][X_1]$, ce qui donne
$$f = (X_1 - a_1)g + r \text{ avec } deg_{X_1} r < 1, \text{ soit } r \in k[X_2, \cdots, X_n].$$
L'évaluation en $(a_1, \cdots, a_n)$ donne alors $0 = r(a_2, \cdots, a_n)$, donc $r \in \ker \text{éval}_{(a_2, \cdots, a_n)}$ donc $r \in \langle X_2 - a_2, \cdots, X_n - a_n \rangle$ et au final $f \in \langle X_1 - a_1, \cdots, X_n - a_n \rangle$, ce qui achève la récurrence. Enfin pour finir, $\langle X_1 - a_1, \cdots, X_n - a_n \rangle$ est maximal car $\text{éval}_{(a_1, \cdots, a_n)}$ réalise un isomorphisme entre $k[X_1, \cdots, X_n]/\langle X_1 - a_1, \cdots, X_n - a_n \rangle$ et k, corps.

□

On retourne maintenant à nos équivalences :

Démonstration. (De l'autre moitié).
- $3 \Rightarrow 1$: soit $\mathfrak{m}$ un idéal maximal. Par 3 on a $\mathcal{Z}(\mathfrak{m}) \neq \varnothing$. Soit $(a_1, \cdots, a_n) \in \mathcal{Z}(\mathfrak{m})$. Alors $\mathfrak{m} \subset \mathcal{J}(\mathcal{Z}(\mathfrak{m})) \subset \mathcal{J}(\{a_1, \cdots, a_n\}) = \langle X_1 - a_1, \cdots, X_n - a_n \rangle$ par 2.1.2 et on conclut par maximalité.

– $3 \Rightarrow 2$: voilà la partie la plus corsée du travail, celle qui fera comprendre pourquoi on appelle cette forme "forte". L'idée est une astuce que la littérature anglophone nomme "Rabinovitch's trick". Probablement introduite à l'origine par un certain Rabinovich (dont je trouve peu de traces), elle consiste à considérer une variable supplémentaire puis ensuite à la particulariser. Ce qui est intéréssant, c'est que je n'ai rencontré aucune autre façon d'aboutir à cette forme forte, comme s'il fallait impérativement disposer de toute la puissance et la généralité d'une variable supplémentaire dans notre anneau polynôme, pour ensuite revenir à notre anneau initial. C'est un aspect des mathématiques que j'ai rencontré plusieurs fois (je me souviens d'une démonstration concernant l'orthogonalité dans un espace pré-hilbertien où il fallait utiliser deux variables et ensuite particulariser en une seule) et qui m'intrigue : aller chercher plus de généralité pour montrer du particulier. Bref, retournons à notre preuve.
Une inclusion est triviale : $I \subset \mathcal{J}(\mathcal{Z}(I))$ et en passant à la racine on obtient $\sqrt{I} \subset \mathcal{J}(\mathcal{Z}(I))$. Réciproquement, soit $f \in \mathcal{J}(\mathcal{Z}(I))$. On introduit notre variable supplémentaire, posons

$$J = \langle I, 1 - X_{n+1}f \rangle \subset k[X_1, \cdots, X_{n+1}].$$

Dans cet anneau avec une variable supplémentaire, on verra les éléments de I comme des éléments de $k[X_1, \cdots, X_{n+1}]$ qui ne dépendant pas de X_{n+1}. Le secret réside dans le fait que $\mathcal{Z}(J) = \varnothing$. En effet, si ce n'est pas vrai, soit $(a_1, \cdots, a_{n+1}) \in \mathcal{Z}(J)$, alors dans notre anneau initial, $(a_1, \cdots, a_n) \in \mathcal{Z}(I)$ donc $1 = 1 - a_{n+1}f(a_1, \cdots, a_n)$. Mais d'autre part, $1 - X_{n+1}f \in J$ et $(a_1, \cdots, a_{n+1}) \in \mathcal{Z}(J)$ donc $1 - a_{n+1}f(a_1, \cdots, a_n) = 0$ et on obtient la plus sympathique des contradictions. Ainsi par hypothèse (peu importe n dans le Nullstellensatz !), $J = k[X_1, \cdots, X_{n+1}]$ donc il existe des $g_i \in I$ et $h, h_i \in k[X_1, \cdots, X_{n+1}]$ tels que

$$1 = (1 - X_{n+1}f)h + \sum_{i=1}^{r} h_i g_i \text{ dans } k[X_1, \cdots, X_{n+1}].$$

On particularise x_{n+1} en $\dfrac{1}{f}$ et on obtient une égalité dans $k(X_1, \cdots, X_{n+1})$:

$$1 = \sum_{i=1}^{r} h_i(X_1, \cdots, X_n, \frac{1}{f}) g_i(X_1, \cdots, X_n). \tag{1}$$

Fixons un entier m tel que pour tout $i = 1...r$, $m \geq deg_{X_{n+1}} h_i$. On peut donc écrire chaque h_i sous la forme

$$h_i = \sum_{j=0}^{m} h_{ij}(X_1, \cdots, X_n) X_{n+1}^j$$

puis on multiplie (1) par f^m toujours en évaluant X_{n+1} en $\dfrac{1}{f}$:

$$f^m = \sum_{i=1}^{r} \sum_{j=0}^{m} k_{ij}(X_1, \cdots, X_n) g_i(X_1, \cdots, X_n) \text{ avec } k_{ij} = f^m \times h_{ij} \times \left(\frac{1}{f}\right)^j = f^{m-j} \times h_{ij}.$$

donc $f^m \in I$.

□

2.2 Des formes différentes

On a fini par montrer l'équivalence des trois formes classiques du Nullstellensatz. Voici un résultat purement algébrique qu'on nomme parfois Nullstellensatz, on verra pourquoi plus tard.

Théorème 2.2.1. *(Nullstellensatz "algébrique"). Soit k un corps. Soit K une k-algèbre de type fini qui est un corps. Alors $[K : k] < \infty$, c'est-à-dire, K est une extension algébrique finie de k.*

Enfin, avant de s'atteler aux démonstrations je présente une dernière version, que l'on peut considérer comme l'ultime généralisation du Nullstellensatz, et qui est originaire de Bourbaki.

Théorème-définition 2.2.2. *(Nullstellensatz "Bourbaki"). Un anneau de Jacobson est un anneau dont tout idéal premier est intersection d'idéaux maximaux. Soit R un anneau de Jacobson. Soit S une R-algèbre de type finie. Alors S est un anneau de Jacobson. De plus, si $\mathfrak{n} \subset S$ est un idéal maximal, alors $\mathfrak{m} := \mathfrak{n} \cap R$ est un idéal maximal de R, et $S/\mathfrak{n}$ est une extension algébrique finie de $R/\mathfrak{m}$.*

3 Différentes démonstrations, différentes hypothèses

3.1 Le cas simple d'un corps algébriquement clos indénombrable

J'ai rencontré la démonstration suivante, pour $k = \mathbb{C}$ dans le cours d'algèbre commutative de Florian Ivorra à Rennes 1. En fait, le corps des complexes n'est jamais utilisé en soi : tout ce qu'on utilise, c'est la non dénombrabilité. On obtient donc une version un peu plus générale. Moralement, en dehors de $\mathbb{C}$, on peut penser aux clôtures algébriques des $\mathbb{F}_p((T))$ ainsi qu'à la clôture de $\mathbb{C}(X)$. Historiquement (du moins selon mes recherches), la preuve provient à l'origine de Krull et de Van der Waerden. L'idée principale réside dans le lemme suivant.

Lemme 3.1.1. *Soit k un corps infini indénombrable. Alors $k(X)$ est une k-algèbre de dimension infinie non dénombrable.*

Démonstration. C'est clairement une extension de corps de k. Concernant sa dimension, il suffit de considérer la famille indénombrable suivante $(\frac{1}{X-a})_{a\in k}$. Pour toute somme finie vérifiant $\sum_{j=1}^{n} \frac{\lambda_j}{X-a_j} = 0$, il suffit de multiplier cette égalité par $X - a_{j_0}$ puis de l'évaluer en a_{j_0} pour obtenir $\lambda_{j_0} = 0$. □

On peut maintenant s'atteler au

Théorème 3.1.2. *(Nullstellensatz indénombrable – version "intermédiaire"). Soit k un corps algébriquement clos indénombrable et I un idéal strict de $k[X_1, \cdots, X_n]$. Alors $\mathcal{Z}(I)$ est non vide.*

Démonstration. Le théorème de Krull affirme qu'il existe un idéal maximal $\mathfrak{m}$ qui contient I. Alors $\mathcal{Z}(\mathfrak{m}) \subset \mathcal{Z}(I)$ et on peut se ramener à démontrer le théorème pour $\mathfrak{m}$. Posons

$$K := k[X_1, \cdots, X_n]/\mathfrak{m}.$$

et notons $\pi : k[X_1, \cdots, X_n] \to k[X_1, \cdots, X_n]/\mathfrak{m}$ la projection canonique. K est un corps, extension de k. De plus comme $k[X_1, \cdots, X_n]$ est de dimension dénombrable, K est de dimension au plus dénombrable. Enfin, dans ce corps, le théorème est clairement vrai : pour tout $f \in \mathfrak{m}$, comme π est un morphisme de k-algèbres on a $f(\pi(X_1), \cdots, \pi(X_n)) = \pi(f) = 0$. Il serait fortement appréciable que $K = k$. Pour cela il suffit de montrer que K est une extension algébrique de k : si ce n'était pas le cas, K contiendrait un x transcendant sur k, donc contiendrait une algèbre isomorphe à $k(X)$, ce qui par 3.1.1 donne une contradiction sur la dimension de K. □

Voici une autre preuve utilisant le même lemme, mais qui aboutit à la version "faible" :

Théorème 3.1.3. *(Nullstellensatz indénombrable – version "faible"). Soit k un corps algébriquement clos indénombrable et $\mathfrak{m}$ un idéal maximal de $k[X_1, \cdots, X_n]$. Alors il existe $(a_1, \cdots, a_n) \in k^n$ tel que*

$$\mathfrak{m} = \langle X_1 - a_1, \cdots, X_n - a_n \rangle.$$

Démonstration. Pour $i = 1...n$, on dispose d'un morphisme $\phi_i : k[X_i] \to k[X_1, \cdots, X_n]/\mathfrak{m} =: K$. Comme avant on a $K = k$ et donc ϕ_i ne peut être injectif. En effet, si c'était le cas, k contiendrait une algèbre isomorphe à $k[X_i]$ et donc une algèbre isomorphe à $k(X_i)$ aussi, ce qui n'est pas possible pour les raisons de dimensions évoquées ci-dessus. De plus ϕ_i est non nul, sinon $1 \in \mathfrak{m}$. Ainsi il existe $a_i \in k$ tel que $\ker \phi_i = \langle X_i - a_i \rangle$. (C'est un idéal premier de $k[X_i]$ donc maximal et engendré par un polynôme de degré 1, par le théorème fondamental de l'algèbre.) Ainsi $\langle X_1 - a_1, \cdots, X_n - a_n \rangle \subset \mathfrak{m}$. Or, par 2.1.2 $\langle X_1 - a_1, \cdots, X_n - a_n \rangle$ est maximal ce qui permet de conclure.

□

3.2 Le cas général.

Ces démonstrations étaient notables tant elles étaient simples. Par contre, elles ne sont pas valables sur les corps algébriquement clos dénombrables, qui existent bel et bien et peuvent être importants. Certains sous-corps de $\mathbb{C}$ sont de bons exemples : les nombres algébriques, ou encore les clôtures algébriques d'extensions transcendantes de $\mathbb{Q}$. Pour ces corps, il faut une démonstration plus générale, et donc beaucoup plus de travail. Voici la preuve classique du cas général : elle utilise le concept de *normalisation de Noether*, d'*algèbres entières*, et passe par le théorème 2.2.1. Je rappelle que B une A-algèbre (ou un plus généralement un anneau B avec $A \subset B$) est dit entière sur A si tout élément de B est entier sur A, *i.e.* est racine d'un polynôme unitaire à coefficients dans A.

Lemme 3.2.1. *(Normalisation de Noether). Soit k un corps et A une $k-$algèbre de type fini et intègre. Alors il existe des éléments $y_1, \cdots, y_d \in A$ algébriquement indépendants (i.e. il n'existe pas de polynôme annulant $(y_1, \cdots, y_d)$ dans k^d) tels que A est entière sur $k[y_1, \cdots, y_d]$. De plus d est le degré de transcendance du corps des fractions de A sur k.*

Démonstration. La démonstration est très calculatoire. aussi j'utiliserai les notations de Serge Lang (cf. [Lang][VIII,§2]) qui ont le mérite de clarifier ces calculs au maximum. Soient $x_1, \cdots, x_n$ des générateurs de A sur k. Si ces générateurs sont déjà algébriquement indépendants, c'est gagné. Sinon, on dispose d'une relation

$$\sum a_{(j)} x_1^{j_1} \cdots x_n^{j_n} = 0 \tag{2}$$

avec les $a_{(j)} \in k$ tous non nuls et la somme prise sur un nombre fini de n-uplets d'entiers positifs $(j_1, \cdots, j_n)$. Soient $m_2, \cdots, m_n$ des entiers positifs et posons

$$y_2 = x_2 - x_1^{m_1}, \cdots, y_n = x_n - x_1^{m_n}.$$

On injecte ces équations dans (2). On utilise la notation vectorielle $(m) = (1, m_2, \cdots, m_n)$, $(j) = (j_1, \cdots, j_n)$ et on notera $(m) \cdot (j)$ le produit scalaire usuel. On obtient une relation de la forme

$$\sum a_{(j)} x_1^{(j)\cdot(m)} + f(x_1, y_2, \cdots, y_n) = 0 \tag{3}$$

où f est un polynôme où aucune puissance de x_1 n'apparaît en seul facteur. Maintenant en prenant d un entier suffisamment grand (par exemple plus grand que toute composante de tous les (j)) et en posant $(m) = (1, d, d^2, \cdots, d^{n-1})$, alors tous les $(j) \cdot (m)$ sont distincts (unicité de l'écriture des entiers en base d). Quitte à augmenter d on peut supposer qu'il est plus grand que toute puissance de x_1 qui apparait dans f. Cela prouve que (3) fournit bien que x_1 est entier sur $k[y_2, \cdots, y_n]$. (La somme à gauche étant non nulle d'une part, et ne pouvant être nulle une fois sommée avec f puisqu'aucune puissance pure de x_1 n'apparaît

dans f, et le polynôme ainsi obtenu annullant x_1 étant bien unitaire). Par ailleurs, pour $i > 1$ les x_i sont entiers sur $k[x_1, y_2, \cdots, y_n]$ donc par transitivité des extensions entières, sur $k[y_2, \cdots, y_n]$.

Pour finir, et encore par transitivité, on se ramène inductivement à une famille algébriquement indépendante $(y_2, \cdots, y_d)$: si la famille ne l'est pas, on a une relation de dépendance algébrique, donc y_n est racine d'un polynôme à coefficients $k[y_2, \cdots, y_{n-1}]$ et on le retire de la famille, et ainsi de suite.

□

Quelques remarques : cet énoncé peut paraître tout à fait abstrait mais il n'en est rien. D'une part il est constructif : on a des formules explicites (et simples) des y_i. Ce choix des y_i (et donc cette preuve) provient directement de Nagata M. (1962). Le désavantage est que les équations ne sont pas linéaires en $x_1, \cdots, x_n$. Il existe des alternatives générales qui pallient ce problème, mais elles ne sont pas intéréssantes ici et sont développées dans [Lang, VIII, §2]. En particulier, la version originale de Noether (1926) prenait un corps infini (ce qui est toujours notre situation vu qu'on travaille avec des corps algébriquement clos) et $y_i = x_i - a_i x_1$ pour certains a_i. D'autre part, le théorème (avec encore un peu de travail derrière) fournit un profond sens géométrique que je ne saurais détailler ici mais que l'on peut trouver dans [Eis][p.288]. Dans cet esprit, il me servira à la fin de ce rapport pour prouver un théorème fondamental sur la dimension des variétés algébriques.

Lemme 3.2.2. *Soient A et B deux anneaux, et $A \subset B$ avec B entier sur A et intègre. Si B est un corps, A est un corps et réciproquement.*

Démonstration. Supposons que B est un corps. Soit $x \in A$ non nul. Il existe $y \in B$ tel que $xy = 1_B$. Comme y est entier sur A on dispose d'une relation $y^n + c_1 y^{n-1} + \cdots + c_n = 0$ avec $c_i \in A$. On multiplie cette relation par x^{n-1} et on obtient

$$y = -c_1 - c_2 x - \cdots - c_n x^{n-1} \in A$$

donc en fait x est inversible dans A. Ainsi, A est un corps. On n'utilisera jamais l'autre sens mais c'est tout simplement le fait bien connu que dans une algèbre sur un corps qui est intègre, les éléments algébriques sont inversibles (et leurs inverses algébriques eux aussi). □

Théorème 3.2.3. *(Nullstellensatz "algébrique"). Soit k un corps et K une k-algèbre de type fini qui est un corps, alors K est une extension algébrique finie de k.*

Démonstration. K est un corps donc est intègre ; par le lemme de normalisation de Noether on peut trouver $y_1, \cdots, y_d \in A$ tels que que K soit entière sur $k[y_1, \cdots, y_d]$. On a donc $k \subset k[y_1, \cdots, y_d] \subset K$. Par le lemme 3.2.2, comme K est un corps, $k[y_1, \cdots, y_d]$ est un corps, or comme $y_1, \cdots, y_d$ sont algébriquement indépendants, on a $k[y_1, \cdots, y_d] \cong k[X_1, \cdots, X_d]$ donc $d = 0$ et au final K est entière sur k, c'est-à-dire K est une extension algébrique finie de k. □

On en déduit rapidement, justifiant ainsi la dénomination du théorème précédent (déjà estampillé 2.2.1), la forme faible :

Théorème 3.2.4. *(Nullstellensatz – forme "faible"). Soit k un corps algébriquement clos et $\mathfrak{m} \subset k[X_1, \cdots, X_n]$ un idéal maximal. Alors il existe $(a_1, \cdots, a_n) \in k^n$ tel que*

$$\mathfrak{m} = \langle X_1 - a_1, \cdots, X_n - a_n \rangle.$$

Démonstration. Notons $\pi : k[X_1, \cdots, X_n] \to k[X_1, \cdots, X_n]/\mathfrak{m} =: K$ la projection canonique. Si k est un corps algébriquement clos, par le lemme précédent on a $K = k$. Il existe donc $a_1, ..., a_n \in k$ tels que $\pi(X_i) = a_i$, donc $X_i - a_i \in \mathfrak{m}$. Puis $\langle X_1 - a_1, \cdots, X_n - a_n \rangle \subset \mathfrak{m}$. De plus, le lemme 2.1.2 prouve que cet idéal est maximal et donc $\langle X_1 - a_1, \cdots, X_n - a_n \rangle = \mathfrak{m}$ □

Au final, voilà la preuve la plus simple que j'ai pu trouver concernant le cas général. (N'oublions pas que pour prouver la forme "forte", il faut encore rajouter à cela le "Rabinovitch's trick" développé dans la deuxième moitié de la preuve de 2.1.1). [Lang] propose une preuve du cas général assez différente et qui se base sur l'extension de morphismes de corps pour aboutir sur la forme intermédiaire et utilise, encore et toujours, l'astuce de Rabinovitch.

3.3 La généralisation de Bourbaki

Le concept de dépendance entière est en fait très utile dans le champ du Nullstellensatz. En particulier, le lemme 3.2.2 est un ingrédient principal de la démonstration de la forme Bourbaki 2.2.2. Afin de prouver cette dernière nous avons besoin d'un lemme. Cette démonstration est largement inspirée de [Eis][4.5] et est plutôt longue et difficile. On verra ensuite en quoi ce théorème généralise le Nullstellensatz, et je donnerai quelques compléments d'information sur les anneaux de Jacobson.

3.3.1 Le théorème

Lemme 3.3.1. *Soit R un anneau. Sont équivalents*

a) R est un anneau de Jacobson.

b) Si $\mathfrak{p} \subset R$ est un idéal principal et $S := R/\mathfrak{p}$ contient $b \neq 0$ tel que le localisé $S[b^{-1}]$ est un corps, alors S est un corps.

Démonstration. Montrons $a) \Rightarrow b)$ en montrant que (0) est un idéal maximal de S. Supposons $a)$ et l'hypothèse de $b)$. Comme R est de Jacobson, S l'est aussi donc l'intersection de tous ses idéaux maximaux est incluse dans l'intersection de ses idéaux premiers, son nilradical. En effet :

$$\bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} \subset \bigcap_{\mathfrak{p} \text{ premier}} \bigcap_{\mathfrak{p}=\bigcap \mathfrak{m}_\mathfrak{p}} \mathfrak{m}_\mathfrak{p} = \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p} = \mathrm{Nil}(S).$$

Or, S étant intègre son nilradical est nul donc l'intersection des idéaux maximaux de S est (0). Maintenant, les idéaux premiers de $S[b^{-1}]$ correspondant bijectivement aux idéaux premiers de S ne contenant pas b, et $S[b^{-1}]$ étant un corps, on sait qu'il n'y a qu'un seul idéal de S ne contenant pas b, c'est (0). Ainsi, (0) est contenu dans l'intersection des idéaux maximaux de S, sinon cette dernière contiendrait b.

Montrons $b) \Rightarrow a)$. Soit Q un idéal premier de R, montrons que

$$Q = \bigcap_{Q \subset \mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

Supposons l'inclusion stricte, et prenons $f \in (\cap_{Q\subset\mathfrak{m}}\mathfrak{m}) \setminus Q$. Par le lemme de Zorn, il existe un idéal premier $\mathfrak{p}$ maximal parmi les idéaux premiers I de R vérifiant $Q \subset I \subsetneq \langle Q, f\rangle$ (l'union des éléments d'une chaîne de cet ensemble donne classiquement un majorant de la chaîne). De plus $\mathfrak{p}$ n'est pas maximal car $\mathfrak{p} \subsetneq \langle Q, f\rangle \subset \cap_{Q\subset\mathfrak{m}}\mathfrak{m}$ qui est strict. Ainsi $R/\mathfrak{p}$ n'est pas un corps. Mais par définition $\mathfrak{p}$ engendre dans le localisé $R[f^{-1}]$ un idéal $(\mathfrak{p}[f^{-1}])$ maximal, donc $(R/\mathfrak{p})[f^{-1}] = R[f^{-1}]/\mathfrak{p}[f^{-1}]$ (exactitude de la localisation) est un corps et $b)$ donne une contradiction qui permet de conclure. □

On peut désormais prouver le théorème 2.2.2 qu'on rappelle :

Théorème 3.3.2. *(Nullstellensatz "Bourbaki"). Soit R un anneau de Jacobson et S une R-algèbre de type finie. Alors S est un anneau de Jacobson. De plus, si $\mathfrak{n} \subset S$ est un idéal maximal, alors $\mathfrak{m} := \mathfrak{n} \cap R$ est un idéal maximal de R, et $S/\mathfrak{n}$ est une extension algébrique finie de $R/\mathfrak{m}$.*

Démonstration. La démonstration est un peu longue mais n'utilise rien de nouveau en dehors du lemme démontré à l'instant et du lemme 3.2.2. Aussi je préfère n'en donner que les ingrédients principaux et renvoyer le lecteur à [Eis][p.133]. En fait, on traite sans trop de problème le cas où S est générée par un unique élément et on traite le cas général par récurrence sur le nombre de générateurs. Il est plus intéréssant de voir en quoi ce théorème généralise le Nullstellensatz. □

3.3.2 le Nullstellensatz

Avant de terminer sur le Nullstellensatz on a besoin d'un dernier lemme, qui est une généralisation de la forme faible et qui va donner un sens géométrique au théorème. Cela permet de prouver le Nullstellensatz fort de façon très jolie, quasi purement algébriquement, en ne maniant que des intersections d'idéaux (radical de Jacobson, nilradical).

Lemme 3.3.3. *Soit k un corps algébriquement clos et X un ensemble algébrique de k^n. Alors les idéaux maximaux de $k[X_1, \cdots, X_n]/\mathcal{J}(X)$ sont de la forme $\langle X_1 - a_1, \cdots, X_n - a_n\rangle/\mathcal{J}(X)$ pour $(a_1, \cdots, a_n) \in X$. En particulier on a le Nullstellensatz faible en prenant $X = k^n$.*

Démonstration. Notons $p = (a_1, \cdots, a_n)$ et $\mathfrak{m}_p = \langle X_1 - a_1, \cdots, X_n - a_n\rangle$. On a $\mathfrak{m}_p \supset \mathcal{J}(X)$ si et seulement si $p \in X$ par le lemme 2.1.2 [1]. Ensuite, les idéaux maximaux de $k[X_1, \cdots, X_n]/\mathcal{J}(X)$ sont les $\mathfrak{n}/\mathcal{J}(X)$ avec $\mathfrak{n}$ idéal maximal de $k[X_1, \cdots, X_n]$. Reste à montrer que ceux-ci sont de la forme $\mathfrak{m}_p$: c'est le Nullstellensatz faible. On l'a déjà montré, mais soyons cohérent et montrons le dans notre cadre, grâce au théorème 2.2.2. On applique celui-ci avec $R = k$ et $S = k[X_1, \cdots, X_n]$. Il dit que $S/\mathfrak{n}$ est une extension algébrique finie de $k/(\mathfrak{n} \cap k) = k$. k étant algébriquement clos on a donc $S/\mathfrak{n} = k$ et en notant a_i la classe de X_i dans $S/\mathfrak{n} = k$ et $p = (a_1, \cdots, a_n)$, on a $\mathfrak{m}_p \subset \mathfrak{n}$ et on conclut par maximalité des deux idéaux. [2] □

On peut maintenant montrer le Nullstellensatz fort : $\mathcal{J}(\mathcal{Z}(I)) = \sqrt{I}$.

Démonstration. Par les propriétés de l'introduction et le lemme 2.1.2, on a :

$$\mathcal{J}(\mathcal{Z}(I)) = \mathcal{J}\left(\bigcup_{x\in\mathcal{Z}(I)}\{x\}\right) = \bigcap_{x\in\mathcal{Z}(I)}\mathcal{J}(\{x\}) = \bigcap_{x\in\mathcal{Z}(I)}\mathfrak{m}_x$$

Maintenant considérons l'intersection de tous les idéaux maximaux de S contenant I, je prône que

$$\bigcap_{I\subset\mathfrak{m}}\mathfrak{m} = \bigcap_{x\in\mathcal{Z}(I)}\mathfrak{m}_x \tag{4}$$

car pour tout $x \in \mathcal{Z}(I)$, $I \subset \mathfrak{m}_x$ ce qui prouve la première inclusion. Réciproquement un $\mathfrak{m}$ dans $\bigcap_{I\subset\mathfrak{m}}\mathfrak{m}$ est, par 3.3.3 (le Nullstellensatz faible en fait), un $\mathfrak{m}_x$ qui de plus contient I. Ainsi $x \in \mathcal{Z}(\mathfrak{m}_x) \subset \mathcal{Z}(I)$ donc $\bigcap_{I\subset\mathfrak{m}}\mathfrak{m} \supset \bigcap_{x\in\mathcal{Z}(I)}\mathfrak{m}_x$. D'autre part, par le théorème de Bourbaki 2.2.2, comme on a à faire à un anneau de Jacobson on peut écrire

$$\bigcap_{I\subset\mathfrak{q}\text{ premier}}\mathfrak{q} = \bigcap_{I\subset\mathfrak{q}\text{ premier}}\left(\bigcap\mathfrak{m}_\mathfrak{q}\right)$$ [3]

1. Si $p \in X$, un polynôme nul sur X est nul en p donc est dans $\mathcal{J}(\{p\}) = \mathfrak{m}_p$ par le lemme et réciproquement, $p \in \mathcal{Z}(\mathfrak{m}_p) = \mathcal{Z}(\mathcal{J}(\{p\})) \subset \mathcal{Z}(\mathcal{J}(X)) = X$).

2. On remarquera que cette preuve est identique à celle suite à la normalisation de Noether : la seule chose qui change est le procédé qui sert à montrer que $S/\mathfrak{n} = k$. La première fois, c'était le lemme de normalisation, ici, c'est le théorème de Bourbaki.

3. Attention ici $\mathfrak{m}_\mathfrak{q}$ dénote un des idéaux maximaux dont l'intersection forme $\mathfrak{q}$ et non pas un idéal correspondant à un point q !

Le terme de gauche est clairement inclus dans $\bigcap_{I\subset\mathfrak{m}}\mathfrak{m}$ puisque les idéaux maximaux sont premiers. Puis $\bigcap_{I\subset\mathfrak{m}}\mathfrak{m}$ est clairement inclus dans le terme de droite. Ainsi,

$$\mathcal{J}(\mathcal{Z}(I)) = \bigcap_{I\subset\mathfrak{q}\text{ premier}} \mathfrak{q} = \sqrt{I}. \tag{5}$$

□

3.3.3 Annexe : anneaux de Jacobson – vers le Nullstellensatz

Cette preuve m'a fait découvrir la notion d'anneau de Jacobson, et en y travaillant j'ai découvert de nombreuses choses intéréssantes, notamment en topologie, que je vais tenter de retranscrire un peu ici. Voici quelques exemples concernant les anneaux de Jacobson :

- $\mathbb{Z}$ est un anneau de Jacobson, puisque ses idéaux premiers non nuls sont maximaux, et que $(0) = \bigcap_{p\in\mathbb{P}}(p)$ (infinité des nombres premiers).
- Par conséquent (2.2.2) $\mathbb{Z}[X_1, \cdots, X_n]$ est un anneau de Jacobson.
- Certains anneaux pourtant "simples" ne sont pas de Jacobson. Par exemple les anneaux principaux ne le sont pas forcément : un anneau de valuation discrète n'est pas de Jacobson. (Rappel : un anneau de valuation discrète est principal, ne possède qu'un idéal maximal, et cet idéal est non nul). En effet, (0) est premier et n'est pas intersection de maximaux.

Après toute cette section on est en droit de se poser la question : en quoi ce théorème de Bourbaki généralise-t-il le Nullstellensatz ? En fait, les anneaux de Jacobson sont le cadre parfait pour généralier le théorème des zéros. Pour voir ceci, faisons un peu de topologie : on veut développer une topologie sur l'ensemble des idéaux premiers d'un anneau polynôme. On l'obtient quasi directement avec le Nullstellensatz et la topologie de Zariski de k^n.

Soit k un corps algébriquement clos et $A = k[X_1, \cdots, X_n]$. Le Nullstellensatz met les points de k^n en bijection avec les idéaux maximaux de A, et plus généralement les points d'un ensemble algébrique X avec les idéaux maximaux de $A(X) = A/\mathcal{J}(X)$ (3.3.3). En notant maxSpec A l'ensemble des idéaux maximaux de A et spec A celui des idéaux principaux, on a donc une bijection entre X et maxSpec $A(X)$. Un sous-ensemble algébrique quelconque $\mathcal{Z}(I) \subset X$ va lui être identifié avec l'ensemble des idéaux maximaux contenant I car $\mathcal{Z}(I) = \bigcap_{x\in\mathcal{Z}(I)}\mathfrak{m}_x = \bigcap_{I\subset\mathfrak{m}}\mathfrak{m}$ par (4). Mais comme A est de Jacobson, cette intersection est identique à celle des idéaux premiers $\bigcap_{I\subset\mathfrak{p}}\mathfrak{p}$ (cf. 5). Ainsi la topologie se "transmet par bijection", et on a bien une topologie sur spec A dont on notera (abusivement) les fermés

$$\mathcal{Z}(I) := \{\mathfrak{p} \supset I,\ \mathfrak{p} \text{ idéal premier de } A\}.$$

avec évidemment :

- Spec $A = Z(\{0\})$ est fermé.
- $\varnothing = Z(A)$ est fermé.
- $Z(I) \cup Z(J) = Z(I \cdot J)$ (stabilité par union finie).
- $\bigcap_\alpha Z(I_\alpha) = Z(\sum_\alpha I_\alpha)$ (stabilité par intersection).

Mais en fait, le fait d'être de Jacobson n'a servi qu'à construire cette topologie "facilement" et visuellement à partir de la topologie de Zariski sur X ; sur un anneau quelconque, la même définition des fermés donne aussi une topologie sur spec A (on vérifie aisément que les quatre propriétés ci-dessus découlent directement de la définition d'un idéal premier) ! Où intervient le fait d'être Jacobson alors ? Résumons notre propos et avançons une réponse :

Théorème-définition 3.3.4. *Soit A un anneau. Alors les*

$$\mathcal{Z}(I) := \{\mathfrak{p} \supset I,\ \mathfrak{p} \textit{ idéal premier de } A\}$$

pour I parcourant les idéaux de A forment les fermés d'une topologie sur spec A qu'on appelle topologie de Zariski. Un point de spec A (un idéal premier) est dit fermé si le singleton

correspondant est un fermé de spec A (ce qui équivaut, par le théorème de Krull, à être un idéal maximal).

Proposition 3.3.5. *Soit A un anneau. Les deux propositions suivantes sont équivalentes :*

1. *A est un anneau de Jacobson.*
2. *Pour toute partie fermée non-vide $\mathcal{Z}(I) \subset$ spec A, l'ensemble des points fermés est dense dans $\mathcal{Z}(I)$.*

Démonstration.

$1 \Rightarrow 2$: soit un fermé $\mathcal{Z}(I)$. On veut montrer que tout voisinage (ouvert, pour simplifier) de tout $\mathfrak{p} \in \mathcal{Z}(I)$ rencontre $\{\mathfrak{m} \supset I\}$. Soit donc $\mathfrak{p} \in \mathcal{Z}(I)$ et $\mathcal{Z}(J)^c$ un voisinage ouvert de ce point. Ainsi $\mathfrak{p} \notin \mathcal{Z}(J)$ soit $\mathfrak{p}$ ne contient pas J. On veut donc trouver un idéal maximal de A qui contient I mais pas J. Comme A est de Jacobson, $\mathfrak{p}$ est intersection d'idéaux maximaux le contenant : or un des idéaux de l'intersection doit ne pas contenir J, sinon $\mathfrak{p}$ le contiendrait !

$2 \Rightarrow 1$: par la preuve de l'implication précédente on sait traduire l'hypothèse par : "soit un $\mathcal{Z}(I)$ et $\mathfrak{p} \in \mathcal{Z}(I)$, alors pour tout $J \not\subset \mathfrak{p}$, il existe $\mathfrak{m}$ maximal tel que $J \not\subset \mathfrak{m}$ et $I \subset \mathfrak{m}$." Il s'agit de montrer alors que $\mathfrak{p} = \bigcap_{\mathfrak{p} \subset \mathfrak{m}} \mathfrak{m}$. L'inclusion directe est évidente. Supposons que l'autre inclusion soit fausse, et posons $I = \mathfrak{p}$. Alors par hypothèse il existe $\mathfrak{m}$ maximal avec $\mathfrak{p} \subset \mathfrak{m}$ et $\bigcap_{\mathfrak{p} \subset \mathfrak{m}} \mathfrak{m} \not\subset \mathfrak{m}$, ce qui est absurde.

□

On termine en donnant un minimum de sens à cette proposition assez forte : elle dit qu'un élément $f \in A$ est "nul vu comme fonction régulière" (notion géométrique précisée plus loin) sur les points fermés de $\mathcal{Z}(I)$ si et seulement s'il est nul sur $\mathcal{Z}(I)$, c'est-à-dire s'il appartient à $\sqrt{I}$. C'est ainsi que les anneaux de Jacobson fournissent un bon cadre de généralisation du Nullstellensatz.

Maintenant, retournons à quelques applications plus terre-à-terre du Nullstellensatz.

4 Applications

4.1 Espace tangent

L'exercice suivant m'a été proposé par Qing Liu. On peut le voir tel quel comme un résultat d'algèbre commutative, mais il possède un sens géométrique que j'expliquerai (vaguement) après la démonstration.

Proposition 4.1.1. *Soit k un corps algébriquement clos et $\mathfrak{m} \subset k[X_1, \cdots, X_n]$ un idéal maximal. Alors $\mathfrak{m}/\mathfrak{m}^2$ est un $A/\mathfrak{m}$-espace vectoriel de dimension n.*

Je propose deux preuves de ce résultat : une tout à fait expéditive par le calcul, et une autre bien trop compliquée pour le résultat en soi, mais qui a le mérite de se généraliser dans un certain contexte : en effet, la grande partie de la preuve est adaptée d'un résultat de géométrie algébrique qui dit que la dimension de l'espace tangent à une variété en un point, est plus grande que la dimension de la variété. Je me suis un peu aventuré par pure curiosité dans cette preuve, et je la retranscris ici car je trouve qu'elle utilise de beaux résultats (localisation, lemme de Nakayama, théorème de l'idéal principal généralisé).

Démonstration. (Version expéditive).

Comme $\mathfrak{m}$ annule le A-module $\mathfrak{m}/\mathfrak{m}^2$, ce dernier module est en fait un $A/\mathfrak{m}$-espace vectoriel ($A/\mathfrak{m} = k$ comme prouvé dans 3.1.2). Par le Nullstellensatz, on peut écrire, disons,

$$\mathfrak{m} = \langle X_1, \cdots, X_n \rangle.$$

Alors

$$\mathfrak{m}/\mathfrak{m}^2 = \langle X_1, \cdots, X_n \rangle / \langle X_i X_j \rangle_{i \leq j = 1 \ldots n}$$

si bien qu'aucun produit X_iX_j n'apparait dans ce quotient : on y retrouve seulement $X_1, \cdots, X_n$. Ainsi, $(X_1, \cdots, X_n)$ est une base de cet espace vectoriel. □

Démonstration. (Version trop forte).

Montrons que sa dimension est plus petite que n. Par le Nullstellensatz, il existe $X_1 - a_1, \cdots, X_n - a_n$ des générateurs de $\mathfrak{m}$. Leurs classes modulo $\mathfrak{m}^2$ génèrent donc $\mathfrak{m}/\mathfrak{m}^2$ ce qui prouve que $dim_{A/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2 \leq n$.

L'autre inégalité est plus difficile. Je souhaite montrer qu'on ne peut pas générer l'espace avec moins de n éléments. J'ai tenté de m'inspirer d'une propriété de géométrie algébrique que j'ai adaptée, aussi j'utilise plusieurs résultats puissants, peut-être un peu trop. Tout d'abord, supposons que $f_1, \cdots, f_r \in \mathfrak{m}$ ont des classes qui génèrent $\mathfrak{m}/\mathfrak{m}^2$. Alors $\mathfrak{m} = \langle f_1, \cdots, f_r \rangle + \mathfrak{m}^2$. On reconnaît une expression du type $M = N + IM$ ce qui donne envie d'appliquer un lemme de Nakayama, à savoir :

Lemme 4.1.2. *(Nakayama). Soit A un anneau commutatif, M un A-module de type fini, N un sous-module de M et I un idéal de A. Si $M = N + IM$ avec I dans le radical de Jacobson de A, alors $M = N$.*

Le problème est qu'ici $I = \mathfrak{m}$ n'est pas dans le radical de Jacobson de $A = k[X_1, \cdots, X_n]$. Ce serait le cas si A était local. J'ai donc tenté de localiser A en $A \setminus \mathfrak{m}$ pour voir ce qui allait se passer. En fait

Proposition 4.1.3. *On a un isomorphisme de $A/\mathfrak{m}$-espaces vectoriels entre $\mathfrak{m}/\mathfrak{m}^2$ et $\mathfrak{m}A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$ qui consiste à envoyer $x + \mathfrak{m}^2$ sur $\frac{x}{1} + (\mathfrak{m}A_\mathfrak{m})^2$.*

Démonstration. Tout d'abord, $\mathfrak{m}A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$ est bien un $A/\mathfrak{m}$-espace vectoriel car $\mathfrak{m}$ annule bien ce A-module. On a le morphisme canonique $\mathfrak{m} \hookrightarrow \mathfrak{m}A_\mathfrak{m} \twoheadrightarrow \mathfrak{m}A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$. Le noyau de ce morphisme contient $\mathfrak{m}^2$ si bien que le morphisme se factorise en $\phi : \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$ qui correspond bien au morphisme annoncé. Montrons qu'il est injectif. Si $\frac{x}{1} \in (\mathfrak{m}A_\mathfrak{m})^2$ c'est qu'il existe $s \notin \mathfrak{m}$ tel que $xs \in \mathfrak{m}^2$. Comme $A/\mathfrak{m}$ est un corps où $s \neq 0$, il existe $t \in A$ et $a \in \mathfrak{m}$ tel que $st = 1 - a$. Ainsi, $x = stx + ax \in \mathfrak{m}^2$. Pour la surjectivité, en gardant les mêmes notations on a $\frac{x}{s} = \phi(tx)$. En effet, $\frac{tx}{1} - \frac{x}{s} = \frac{tx}{1} - \frac{xt}{1-a} = \frac{atx}{1-a} \in (\mathfrak{m}A_\mathfrak{m})^2$.

□

Travaillons donc sur $\mathfrak{m}A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$. Supposons qu'il soit généré, en tant que $A/\mathfrak{m}$-espace vectoriel, par les classes de r éléments $\frac{t_1}{s_1}, \cdots, \frac{t_r}{s_r}$. Alors $\mathfrak{m}A_\mathfrak{m} = \langle \frac{t_1}{s_1}, \cdots, \frac{t_r}{s_r} \rangle + (\mathfrak{m}A_\mathfrak{m})^2$. Cette fois ci ($A_\mathfrak{m}$ est local d'idéal maximal $\mathfrak{m}A_\mathfrak{m}$), on peut appliquer le lemme de Nakayama et on obtient

$$\mathfrak{m}A_\mathfrak{m} = \langle \frac{t_1}{s_1}, \cdots, \frac{t_r}{s_r} \rangle.$$

Or,

$$\mathfrak{m}A_\mathfrak{m} = \langle \frac{X_1 - a_1}{1}, \cdots, \frac{X_n - a_n}{1} \rangle. \tag{6}$$

J'utilise ensuite un résultat d'algèbre commutative du à Krull qui traite de la notion de hauteur d'un idéal :

Théorème-définition 4.1.4. *(Théorème de l'idéal principal généralisé).*

La hauteur d'un idéal premier est la borne supérieure des entiers n tels qu'il existe une chaîne strictement croissante $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_n = \mathfrak{p}$. Soit A un anneau noethérien et I un idéal propre de A, généré par n éléments. Soit $\mathfrak{p}$ un idéal premier minimal parmis les idéaux premiers contenant I. Alors la hauteur de $\mathfrak{p}$ est inférieure à n.

En fait (6) donne que $\mathfrak{m}A_\mathfrak{m}$ ne peut pas être généré par moins de n éléments. Le théorème précédent s'applique (tout localisé d'un anneau noethérien est noethérien) avec $I = \mathfrak{p} = \mathfrak{m}A_\mathfrak{m}$. Sa hauteur étant au moins n, car

$$0 \subsetneq \langle \tfrac{X_1-a_1}{1} \rangle \subsetneq \langle \tfrac{X_1-a_1}{1}, \tfrac{X_2-a_2}{1} \rangle \subsetneq \cdots \subsetneq \langle \tfrac{X_1-a_1}{1}, \cdots, \tfrac{X_n-a_n}{1} \rangle = \mathfrak{m}A_\mathfrak{m}$$

on conclut que $r \geq n$ en appliquant le théorème avec les r générateurs (en supposant qu'ils fournissent une chaîne d'inclusions strictes, quitte à réduire r). On conclut donc que $dim_{A/\mathfrak{m}}\mathfrak{m}A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2 \geq n$ et par isomorphisme, que $dim_{A/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2 \geq n$.

□

Un autre résultat intéréssant est une généralisation de ce dernier, à un corps non nécéssairement algébriquement clos, passant par une généralisation en quelque sorte, du Nullstellensatz. La proposition suivante est un exercice qui m'a aussi été suggéré par Qing Liu et qu'on peut retrouver (avec une indication de démonstration sensiblement différente de celle que j'ai effectuée) dans son livre [Liu][2.1, Exercice 1.5].

Proposition 4.1.5. *Soit k un corps quelconque et $\mathfrak{m} \subset k[X_1, \cdots, X_n]$ un idéal maximal. Alors $\mathfrak{m}$ peut être généré par n éléments $P_1(X_1), P_2(X_1, X_2), \cdots, P_n(X_1, \cdots, X_n)$ et $\mathfrak{m}/\mathfrak{m}^2$ est un $A/\mathfrak{m}$-espace vectoriel de dimension n.*

Démonstration. Le seul résultat fondamental dont on a besoin est le pré Nullstellensatz algébrique 2.2.1. Prouvons le résultat par récurrence. Pour $n = 1$, $k[X_1]$ étant principal, on a clairement le résultat. Supposons le résultat vrai au rang $n-1$. On a le résultat suivant.

Lemme 4.1.6. *$\mathfrak{m} \cap k[X_1, \cdots, X_{n-1}]$ est un idéal maximal de $k[X_1, \cdots, X_{n-1}]$.*

Démonstration. En effet par 2.2.1, $k[X_1, \cdots, X_n]/\mathfrak{m} =: k[\overline{X_1}, \cdots, \overline{X_n}]$ est une extension algébrique finie de k et on a un morphisme surjectif $k[X_1 \cdots, X_n] \to k[X_1, \cdots, X_n]/\mathfrak{m}$ de noyau $\mathfrak{m}$. Si on restreint ce morphisme à $k[X_1, \cdots, X_{n-1}]$ on obtient un morphisme surjectif $k[X_1, \cdots, X_{n-1}] \to k[\overline{X_1}, \cdots, \overline{X_{n-1}}]$ (où la barre désigne modulo $\mathfrak{m}$) de noyau $\mathfrak{m} \cap k[X_1, \cdots, X_{n-1}]$. On a donc un isomorphisme entre $k[X_1, \cdots, X_{n-1}]/(\mathfrak{m} \cap k[X_1, \cdots, X_{n-1}])$ et le corps $k[\overline{X_1}, \cdots, \overline{X_{n-1}}]$ (sous-corps de $k[\overline{X_1}, \cdots, \overline{X_n}]$) qui permet de conclure. □

Par hypothèse de récurrence on peut écrire

$$\mathfrak{m} \cap k[X_1, \cdots, X_{n-1}] = \langle P_1(X_1), \cdots, P_{n-1}(X_1, \cdots, X_{n-1}) \rangle$$

idéal qu'on notera $\mathfrak{m}_{\mathfrak{n-1}}$. Notons le corps $L := k[X_1, \cdots, X_{n-1}]/\mathfrak{m}_{\mathfrak{n-1}}$. Par 2.2.1 c'est une extension algébrique finie de k. On considère désormais le morphisme surjectif

$$\begin{aligned} \phi : k[X_1, \cdots, X_n] &\to L[X_n] \\ f &\mapsto \sum_{i=0}^{d} f_i(X_1, \cdots, X_{n-1}) X_n^i \end{aligned}$$

qui ne fait autre que mettre f sous forme canonique dans $L[X_n]$ et réduit les coefficients obtenus modulo $\mathfrak{m}_{\mathfrak{n-1}}$. Il est clair que $\mathfrak{m}_{\mathfrak{n-1}} \subset \ker \phi$, et réciproquement si $f \in \ker \phi$ alors $f = X_n Q_1 + \cdots + X_n^d Q_d$ avec $Q_i \in \mathfrak{m}_{\mathfrak{n-1}}$ donc $f \in \mathfrak{m}_{\mathfrak{n-1}}$, d'où $\ker \phi = \mathfrak{m}_{\mathfrak{n-1}}$ si bien qu'on a un isomorphisme

$$k[X_1, \cdots, X_n]/\mathfrak{m}_{\mathfrak{n-1}} \cong L[X_n]$$

et donc $\mathfrak{m}/\mathfrak{m}_{\mathfrak{n-1}} \cong \mathfrak{m}' \subset L[X_n]$ maximal. Comme $L[X_n]$ est principal on a, disons, $\mathfrak{m}' = \langle T_n(X_n) \rangle$. Prenons $P_n \in k[X_1, \cdots, X_n]$ un représentant de T_n (*i.e.* un antécédent de T_n par ϕ). Soit $P \in \mathfrak{m}$, alors il existe $A_n \in L[X_n]$ tel que $P \bmod \mathfrak{m}_{\mathfrak{n-1}} = A_n T_n$ (quitte à renommer T_n on suppose que notre isomorphisme était une égalité). Donc $P = U_n P_n + u$ où U_n est un antécédent de A_n par ϕ et $u \in \mathfrak{m}_{\mathfrak{n-1}}$. Ce qui prouve, qu'au final

$$\mathfrak{m} = \langle \mathfrak{m}_{\mathfrak{n-1}}, P_n(X_1, \cdots, X_n) \rangle = \langle P_1(X_1), P_2(X_1, X_2), \cdots, P_n(X_1, \cdots, X_n) \rangle$$

et conclut sur la première moitié de la proposition. Pour la dimension de l'espace vectoriel, il suffit de reprendre la preuve précédente et d'utiliser les n générateurs ci-dessus au lieu de ceux fournis par le Nullstellensatz. Sinon, on peut aussi démontrer directement la liberté de la famille (pour la génération, c'est strictement identique à avant) :

Démonstration. (De la liberté de la famille).

Quitte à supprimer les éléments génants, on peut supposer que la famille est effectivement échelonnée en variables, par là j'entends que $P_i(X_1, \cdots, X_i)$ comporte effectivement un terme en X_i (si ce n'était pas le cas, ce polynôme serait généré par ses prédécesseurs dans la famille) et qu'ils ne sont pas dans $\mathfrak{m}^2$. Maintenant, supposons qu'il existe $\lambda_1, \cdots, \lambda_n \in A/\mathfrak{m}$ tels que

$$\lambda_1 P_1(X_1) + \cdots + \lambda_n P_n(X_n) = 0 \text{ mod. } \mathfrak{m}^2.$$

On se place dans $\overline{A/\mathfrak{m}}$ la clôture algébrique de $A/\mathfrak{m}$. Pour toute valeur (dans $A/\mathfrak{m}$) de X_1 on peut y trouver de proche en proche des valeurs de $X_2, \cdots, X_n$ telles que

$$\begin{cases} P_2(X_1, X_2) = 0 & \text{mod. } \mathfrak{m}^2 \\ \quad \vdots & \\ P_n(X_1, \cdots, X_n) = 0 & \text{mod. } \mathfrak{m}^2 \end{cases}$$

(puisque on s'est arrangés pour que P_i présente bien un terme en X_i). Ainsi, $\lambda_1 P_1(X_1) = 0$ mod. $\mathfrak{m}^2$ et donc $\lambda_1 = 0$. On conclut par récurrence. □

□

Interprétons ce résultat : en géométrie algébrique, on a souvent à faire à des espaces vectoriels du type $\mathfrak{m}/\mathfrak{m}^2$. En fait, l'espace tangent à une variété algébrique en un point x sera de la forme $\mathfrak{m}_x/(\mathfrak{m}_x)^2$. Si sa dimension est égale à celle de la variété en ce point, c'est que la variété est régulière en ce point ; si elle est plus grande, c'est qu'il y a une singularité. Ici, le contexte est bien sûr simplifié dans le cadre de l'algèbre commutative, mais localement l'idée est la même. Pour plus de détails sur le sens géométrique et sur l'espace tangent en général, une référence assez simple d'accès (c'est rare !) est [Perrin][V].

On retiendra aussi qu'on a fourni avec 4.1.5 une généralisation intéressante du Nullstellensatz : un idéal maximal d'un anneau polynôme à n variables sur un corps (quelconque !) peut être engendré par n éléments, "échellonnés" en variables.

4.2 Décomposition en irréductibles

À cet instant au cours de mon stage, j'avais envie de faire des choses un peu plus calculatoires, aussi je m'intéressais à manipuler des idéaux "avec les mains" dans divers logiciels de calcul formel. On verra plus tard des exemples concrets de calculs, mais pour l'instant, voilà un exercice tiré de [Perrin] qui permet de déterminer précisément un ensemble algébrique défini par un polynôme réductible, ou de manière équivalente, le radical d'un idéal engendré par un tel polynôme.

Théorème-définition 4.2.1. *Soit V un ensemble algébrique non vide (sur un corps quelconque). Alors V s'écrit de manière unique, à permutation près, comme*

$$V = V_1 \cup \cdots \cup V_r$$

avec les V_i des ensembles algébriques irréductibles, et $V_i \not\subset V_j$ pour $i \neq j$. Les V_i sont appelés ***composantes irréductibles de*** *V, et ce sont les fermés irréductibles maximaux de V. Cette écriture de V est appelée* ***décomposition de*** *V* ***en irréductibles****.*

Rappel topologique : un espace topologique est dit *irréductible* s'il n'est pas union de deux fermés non triviaux. Ceci est équivalent au fait que deux ouverts non vides s'intersectent toujours en une partie non vide, ou encore que tout ouvert non vide est dense.

De plus, la bijection du Nullstellensatz fait correspondre *ensembles algébriques irréductibles* avec *idéaux premiers*, fait dont voici une preuve rapide :

Démonstration. Soit V un ensemble algébrique affine. Supposons $\mathcal{I}(V)$ premier. Si on peut écrire $V = V_1 \cup V_2$ avec $V_i \neq V$, on a $\mathcal{I}(V) \subsetneq \mathcal{I}(V_1)$ par décroissance et injectivité. En prenant $f \in \mathcal{I}(V_1) \setminus \mathcal{I}(V)$ et de même $g \in \mathcal{I}(V_2) \setminus \mathcal{I}(V)$ on a $fg \in \mathcal{I}(V)$ mais ni f ni g dans $\mathcal{I}(V)$: c'est absurde. Réciproquement supposons V irréductible. Soient f, g des polynômes tels que $fg \in \mathcal{I}(V)$. On a donc $\mathcal{Z}(f) \cup \mathcal{Z}(g) = \mathcal{Z}(fg) \supset V = \mathcal{Z}(\mathcal{I}(V))$. Ainsi, $V = (\mathcal{Z}(f) \cap V) \cup (\mathcal{Z}(g) \cap V)$ et l'irréductibilité permet de conclure sur l'égalité entre V et un des deux ensembles de droite, et donc à l'appartenance de f ou g à l'idéal. □

Démonstration. (Du théorème).

Pour l'existence, supposons qu'il existe des ensembles algébriques non décomposables. On en prend un, disons V, dont l'idéal est maximal parmi ceux-ci (ils sont dans un anneau noethérien). Alors $V = F \cup G$ avec $F, G \neq V$. Donc $\mathcal{I}(F), \mathcal{I}(G) \supsetneq \mathcal{I}(V)$. Par définition (maximalité) de $\mathcal{I}(V)$, F et G sont décomposables, donc V aussi. C'est absurde.
Pour l'unicité si on a une écriture similaire avec des W_i, alors $V_i = V \cap V_i = (W_1 \cap V_i) \cup \cdots (W_s \cap V_i)$. Par irréductibilité de V_i, il existe j tel que $V_i \subset W_j$. De même il existe k tel que $W_j \subset V_k$ alors $V_i \subset V_k$ donc $i = k$ et $W_j = V_i$. Enfin, pour la dernière assertion il suffit de remarquer que tout fermé irréductible est contenu dans une composante irréductible. □

Proposition 4.2.2. *Soit $F \in k[X_1, \cdots, X_n]$, $F = F_1^{\alpha_1} \cdots F_r^{\alpha_r}$ avec les F_i irréductibles et non associés et $\alpha_i > 0$. On a alors :*

1. *$\mathcal{I}(\mathcal{Z}((F))) = (F_1 \cdots F_r)$. En particulier si F est irréductible on a $\mathcal{I}(\mathcal{Z}((F))) = (F)$*
2. *La décomposition de $\mathcal{Z}(F)$ en irréductibles est donnnée par $\mathcal{Z}(F) = \mathcal{Z}(F_1) \cup \cdots \cup \mathcal{Z}(F_r)$. En particulier si F est irréductible, $\mathcal{Z}(F)$ est irréductible.*

Démonstration.

La première assertion revient à prouver (par le Nullstellensatz fort !) que $\sqrt{(F_1^{\alpha_1} \cdots F_r^{\alpha_r})} = (F_1 \cdots F_r)$. $\supset$ est claire, il suffit d'élever $F_1 \cdots F_r$ à la puissance $\max_{i=1..r}(\alpha_i)$. Pour l'autre inclusion, on remarque que pour P dans la racine (disons pour P^n dans $(F_1^{\alpha_1} \cdots F_r^{\alpha_r})$), alors pour tout $i = 1..r$, $F_i \mid F_1^{\alpha_1} \cdots F_r^{\alpha_r} \mid P^n$. Donc $F_i \mid P^n$. Par le lemme d'Euclide ($k[X_1, \cdots, X_n]$ est factoriel) et par récurrence, $F_i \mid P$. Par suite, comme les F_i sont non-associés et par décomposition en irréductibles de P, on a $F_1 \cdots F_r \mid P$, soit $P \in (F_1 \cdots F_r)$.

Pour la seconde assertion, c'est juste du calcul :

$$\mathcal{Z}((F)) = \mathcal{Z}(\sqrt{(F)}) = \mathcal{Z}((F_1 \cdots F_r)) =^4 \mathcal{Z}((F_1) \cdots (F_r)) = \mathcal{Z}((F_1)) \cup \cdots \cup \mathcal{Z}((F_r))$$

Les $\mathcal{Z}(F_i)$ sont irréductibles car les (F_i) sont des idéaux premiers et les non-inclusions sont vérifiées car les F_i sont irréductibles non associés. □

4.3 Quelques calculs : la puissance des bases de Grœbner

La géométrie algébrique finit souvent par déboucher sur de "gros" calculs d'algèbre commutative. Autant il y a quelques (dizaines d') années, c'était fastidieux, autant de nos jours il existe des outils formidables pour les résoudre. Ainsi les *bases de Grœbner*, outil extrêmement puissant d'algèbre commutative algorithmique permettent d'implémenter des algorithmes qui permettent en vrac, de calculer le radical d'un idéal, de décider si un idéal est premier, maximal, ou non, de calculer des intersections, des produits d'idéaux, etc.

Je ne m'étendrai pas dessus, toutes les bases théoriques sont dans [Ivorra]. Je dirais simplement qu'avant les bases de Grœbner (Buchberger, 1965), je n'ai pas connaissance de

4. On vérifie aisément que $(P)(Q) = PQ$

techniques effectives pour faire ces calculs, et qu'après les bases de Grœbner mais avant la puissance de calcul actuelle des ordinateurs (ou du moins : avec les bases de Grœbner et une feuille et un crayon), ces calculs sont extrêment longs. Par contre, la théorie de Grœbner, mêlée à l'outil informatique moderne donne lieu à des merveilles : ainsi **MAGMA**, logiciel payant de calcul formel calcule avec brio tous les résultats sus-cités. De même, **SAGE** (énorme logiciel de mathématiques générales, alternative libre sous GNU/GPL à Matlab, Magma, Maple... ; entretenu par toute une communauté et développé à l'origine par William Stein) contient des librairies capables de calculer tout ceci en des temps très raisonnables. J'ai un peu manipulé **SAGE** sous une distribution ArchLinux (paquet `sage-mathematics` du dépôt AUR) pour résoudre facilement quelques exercices de [Perrin].

Exercice 1. *Soit k algébriquement clos et $f : k \to k^3$ l'application qui à t associe (t, t^2, t^3) et C l'image de f (la cubique gauche). Montrer que C est un ensemble algébrique et calculer $\mathcal{I}(C)$. Montrer que $\Gamma(C)$ est isomorphe à $k[T]$.*

Démonstration. Il est clair que $C = \mathcal{Z}(\langle Y - X^2, Z - X^3\rangle)$, ainsi C est algébrique. J'ai conjecturé que $\langle Y - X^2, Z - X^3\rangle$ était radiciel. En fait, il est premier, donc radiciel. C'est probablement faisable, et pas trop compliqué, à la main, en étudiant l'anneau quotient, mais voilà ce que me répond la démonstration online gratuite de **MAGMA**, basée sur **SAGE**, en quelques dixièmes de seconde.

```
P<x, y, z> := PolynomialRing(RationalField(), 3); //Je définis l'anneau polynôme sur Q
I := ideal<P | y-x^2, z-x^3>; // Je définis l'idéal
IsPrimary(I); // Je demande s'il est premier
```

Réponse :

```
 Magma V2.16-10    Wed Jun 23 2010 00:49:49    [Seed = 3736231696]
   ------------------------------------

true

Total time: 0.280 seconds, Total memory usage: 9.03MB
```

□

Mais les calculs peuvent vite devenir un peu plus compliqués, ainsi [Perrin] propose aussi :

Exercice 2. *Soit k algébriquement clos, déterminer les idéaux des ensembles algébriques de k^2 suivants :*

1. $\mathcal{Z}(XY^3 + X^3Y - X^2 + Y)$
2. $\mathcal{Z}(\langle X^2Y, (X-1)(Y+1)^2\rangle)$
3. $\mathcal{Z}(\langle Z - XY, Y^2 + XZ - X^2\rangle)$

Démonstration. Pour 1.

```
P<x, y> := PolynomialAlgebra(RationalField(), 2);
I := ideal<P | x*y^3+x^3*y-x^2+y>;
IsPrimary(I);
```

Réponse :

```
Magma V2.16-10    Tue Jun 22 2010 23:38:28    [Seed = 2881968958]
   ------------------------------------

true

Total time: 0.260 seconds, Total memory usage: 9.03MB
```

Pour 2.

```
P<x, y> := PolynomialAlgebra(RationalField(), 2);

I := ideal<P | x^2*y, (x-1)*(y+1)^2>;
IsPrimary(I);

B := Radical(I); // On calcule le radical de I
B; // On affiche des générateurs de B

Groebner(B); // On met B sous forme de Grœbner
B; // On affiche la base de Grœbner de B

// On prend les générateurs de I mais on enlève les carrés
J := ideal<P | x*y, (x-1)*(y+1)>;
Groebner(J);
J;
```

Réponse : on constate que I n'est pas premier, et on voit que son radical est bien donné par ses générateurs une fois les puissances enlevées (comparer les deux derniers résultats). Ceci correspond à une heuristique de calcul assez connue : "le radical fait perdre les puissances". Ici on pourrait le montrer formellement via l'exercice 4.2.2 et $\mathcal{Z}(\langle I, J\rangle) = \mathcal{Z}(I) \cap \mathcal{Z}(J)$.

```
 Magma V2.16-10    Tue Jun 22 2010 23:45:40    [Seed = 73987778]
   ------------------------------------

false // I n'est pas premier

// Un système de 5 générateurs de I
Ideal of Polynomial ring of rank 2 over Rational Field
Order: Lexicographical
Variables: x, y
Radical
Basis:
[
    x*y^2 + 2*x*y + x - y^2 - 2*y - 1,
    y^3 + 2*y^2 + y,
    x^2 - y^2 - 2*y - 1,
    y^2 + y,
    x^2 - x
]

// Un système de 2 générateurs de I, qui de plus est une base de Grœbner
Ideal of Polynomial ring of rank 2 over Rational Field
Order: Lexicographical
Variables: x, y
```

```
Inhomogeneous, Dimension 0, Radical
Groebner basis:
[
    x - y - 1,
    y^2 + y
]

// J a même base de Grœbner que rad(B) : ce sont les mêmes idéaux.
Ideal of Polynomial ring of rank 2 over Rational Field
Order: Lexicographical
Variables: x, y
Inhomogeneous, Dimension 0
Groebner basis:
[
    x - y - 1,
    y^2 + y
]

Total time: 0.270 seconds, Total memory usage: 9.03MB
```

Pour 3., l'idéal est premier donc radiciel. □

4.4 Équivalence de deux catégories

L'ultime traduction de l'algèbre à la géométrie et vice-versa par le Nullstellensatz s'exprime comme une équivalence de catégories : on dispose d'un foncteur Γ qui est une équivalence entre la catégorie des ensembles algébriques munis des applications régulières, et la catégorie opposée des k-algèbres de type fini réduites, munies des homomorphismes de k-algèbres. Cette partie suppose connue les notions de base de théorie des catégories (foncteurs).

Précisions les termes mis en jeu :

Définition 4.4.1. *(Les morphismes). Si $V \subset k^n$ et $W \subset k^m$ sont deux ensembles algébriques et $\phi : V \to W$. On dit que ϕ est* ***régulière*** *(est un morphisme) si ses composantes ϕ_i sont polynomiales, i.e. sont dans $\Gamma(V) := k[X_1, \cdots, X_n]/\mathcal{I}(V)$,* ***l'algèbre des fonctions polynomiales*** *sur V. Les fonctions régulières sont évidemment continues pour la topologie de Zariski (et c'est même la topologie la plus faible telle que ce soit vrai).*

Théorème-définition 4.4.1. *Soit V un ensemble algébrique. Alors $\Gamma(V)$ est* ***réduite****, c'est-à-dire n'a pas d'élément nilpotent.*

Démonstration. Il suffit de remarquer que $\mathcal{I}(V)$ est radiciel, c'est la traduction exacte du résultat. □

On va voir maintenant en quoi les ensembles algébriques et leurs algèbres se ressemblent :

Propriété 4.4.2. *Soit $\phi : V \to W$ un morphisme. On pose pour $f \in \Gamma(W)$, $\Gamma(\phi)(f) = f \circ \phi \in \Gamma(V)$. Donc $\Gamma(f) : \Gamma(W) \to \Gamma(V)$ est un morphisme de k-algèbres de type fini (réduites). Plus précisément, Γ est un* ***foncteur contravariant*** *(il change le sens des flèches) entre la catégorie des ensembles algébriques munis des applications régulières, et la catégorie des k-algèbres de type fini réduites, munies des homomorphismes de k-algèbres.*

Démonstration. Il faut vérifier que $\Gamma(f \circ g) = \Gamma(g) \circ \Gamma(f)$: c'est clair. Puis que l'identité de chaque objet est transformée en l'identité de l'objet associé : c'est clair. □

Propriété 4.4.3. *Le foncteur Γ est pleinement fidèle, i.e. $\phi \mapsto \Gamma(\phi)$ est une bijection entre $Reg(V,W)$ et $Hom_{k-alg}(\Gamma(W),\Gamma(V))$. Par conséquent, ϕ est un isomorphisme si et seulement si $\Gamma(\phi)$ en est un, ainsi les ensembles algébriques V et W sont isomorphes si et seulement si leurs algèbres le sont !*

Démonstration.

Pour la fidélité (injectivité), on remarque que si $\Gamma(\phi) = \Gamma(\psi)$, alors en prenant η_i la $i^{\text{ème}}$ fonction coordonnée sur W, on a $\phi_i = \Gamma(\phi)(\eta_i) = \Gamma(\psi)(\eta_i) = \psi_i$ pour $i = 1..m$ donc $\phi = \psi$.

Pour le caractère plein (surjectivité), considérons $u : \Gamma(W) \to \Gamma(V)$. Posons $\phi_i = u(\eta_i)$ et soit $\phi : V \to k^m$ la fonction dont les coordonnées sont les ϕ_i. Comme ϕ est à valeurs dans W [5], on a bien $\Gamma(\phi) = u$ (on le vérifie aisément sur les générateurs de l'algèbre). □

On énoncera une dernière propriété pour terminer ce dictionnaire, mais avant on donne un exemple de traduction au niveau des morphisme. Par exemple :

ϕ est *dominant* (*i.e.* d'image dense dans W) si et seulement si $\Gamma(\phi)$ est injectif

Pour le montrer, dans un sens utiliser la densité et la continuité des fonctions régulières pour la topologie de Zariski, et dans l'autre, l'injectivité de $\mathcal{I}$.

Voici la dernière propriété du foncteur Γ, celui qui va rendre les catégories équivalentes. C'est la première fois qu'on a besoin du Nullstellensatz, et il est indispensable, c'est ici qu'il est vraiment mis en valeur :

Propriété 4.4.4. *Si k est algébriquement clos, le foncteur Γ est une équivalence de catégories. C'est-à-dire, en plus d'être pleinement fidèle, il est* ***essentiellement surjectif*** *: pour toute k-algèbre de type fini réduite A, il existe un ensemble algébrique V tel que $A \simeq \Gamma(V)$.*

Démonstration. A est de type fini et réduite, donc $A = k[X_1, \cdots, X_n]/I$ pour un certain entier n et un idéal I radiciel. Soit $V = \mathcal{Z}(I)$. Par le Nullstellensatz fort, $\mathcal{I}(V) = I$ et donc $A \simeq \Gamma(V)$. □

Cette sous-partie règle donc le compte de la géométrie algébrique affine : moyennant un corps algébriquement clos, on a un dictionnaire parfait entre les ensembles algébriques et les algèbres de type fini réduites. C'est le résultat optimal dans le cadre affine. Cependant, la géométrie algébrique a besoin de beaucoup plus, en réalité. On travaille avec des ensembles bien plus généraux : on se place dans le *projectif* pour généraliser les énoncés, de plus on a besoin des notions de *faisceaux* pour pouvoir définir les *variétés algébriques*, d'espaces "localement ensembles algébriques". C'est dans le cadre des variétés algébriques projectives qu'on peut énoncer les grands théorèmes, du type Bézout : "deux courbes planes projectives C et C' de degrés resp. d et d' définies sur un corps algébriquement clos et sans composante commune ont une intersection composée de dd' points, comptés avec multiplicité". (À un stade supérieur, il y a encore une généralisation de tout cela, due à Grothendieck : les schémas. C'est le stade ultime de la géométrie algébrique et je n'en parlerai pas du tout ici.)

Comme pour toute variété, on peut définir une notion de *dimension* pour ces objets, qui est leur invariant le plus fondamental. Aussi je vais m'y atteler, mais en supposant connue la notion de variété algébrique. J'ai profité de ce stage pour pouvoir comprendre ce qu'est une variété algébrique, mais je trouve que définir ce terme dans ce présent rapport prendrait une dizaine de pages que l'on pourrait retrouver un peu partout, par exemple dans [Perrin][II,III,IV]. J'ai donc trouvé plus ludique et intéréssant d'exposer dans la suite de ce rapport un résumé de mon étude de la théorie de la dimension, même dans un cadre un peu restreint.

5. Soit $F \in \mathcal{I}(W)$ et $x \in V$. On veut montrer que $F(\phi(x)) = 0$. On a $F(\phi(x)) = F(u(\eta_1), \cdots, u(\eta_m))(x)$. Mais u est un morphisme d'algèbres donc cette quantité est aussi $u(F(\eta_1, \cdots, \eta_m))(x)$, et comme $F(\eta_1, \cdots, \eta_m)$ n'est autre que la classe modulo $\mathcal{I}(W)$ de $F \in \mathcal{I}(W)$ (ou plutôt ici, mais c'est équivalent : la restriction à W de F), donc est nul, on conclut.

5 Un peu de théorie de la dimension

5.1 Introduction, énoncé

En parallèle d'une étude jusque là plutôt algébrique, j'ai passé un temps non négligeable à m'intéresser à des aspects plus géométriques dans mon stage. J'avais pour objectif de me clarifier l'esprit et de pouvoir poser des idées précises sur le concept de variété algébrique. Aussi, je ne développerai pas ce concept dans ce rapport car il y prendrait beaucoup trop de place et pour peu d'intérêt, étant donné qu'il est explicité dans à peu près tout livre de géométrie algébrique.

L'outil majeur dans l'étude des variétés est évidemment la notion de dimension. J'ai commencé par m'intéresser plus ou moins longuement à la notion de dimension pour un anneau (dimension de Krull). En fait, c'est même le lien entre la dimension de Krull d'un anneau et la dimension des variétés algébriques qui m'a poussé vers l'étude de la dite notion de variété algébrique.

Je me contenterai dans cette partie de proposer un joli résultat fondamental en théorie de la dimension qui mélange tous ces concepts et utilise beaucoup d'outils que j'ai étudié précédemment. Il supposera connues les notions de variété algébrique, ou du moins ici, de variété algébrique affine (espace localement annelé isomorphe à un $(\mathcal{V}, \mathcal{O}_\mathcal{V})$ où $\mathcal{V}$ est un ensemble algébrique affine et $\mathcal{O}_\mathcal{V}$ son faisceau structural) irréductible. Le passage aux variétés algébriques tout court, irréductibles, se fera simplement par l'intermédaire des ouverts. Cette section est la résolution que je propose d'un problème (un peu modifié à mon goût) posé à la fin de [Perrin].

Théorème 5.1.1. *(Dimension d'une variété algébrique affine irréductible). Soit V une variété algébrique affine irréductible, et K le corps des fractions de $\Gamma(V)$ la k-algèbre des fonctions régulières. Alors la dimension de V (au sens général, topologique) est égale au degré de transcendance de K sur le corps de base k :*

$$dim V = \partial_k K$$

Remarque : selon [Eis][VIII], cette propriété était utilisée par les algébristes comme définition (!) de la dimension d'une algèbre de type fini jusqu'en 1935, où Krull étendit la notion aux anneaux quelconques, avec la définition bien connue désormais de *dimension de Krull* : le supremum des longueurs de chaînes d'idéaux premiers dans l'anneau.

5.2 Le going-up de Cohen-Seidenberg

Avant d'entrer dans le vif du sujet, je choisis de présenter dès maintenant un outil fondamental qui sera utilisé dans la preuve du théorème et dont la preuve longue et technique alourdirait celle du théorème. D'autre part, c'est un outil intéréssanet et très puissant : de ce que j'en ai compris, il s'agit de montrer dans quelle mesure deux anneaux dont l'un est entier sur l'autre se ressemblent topologiquement (au niveau de leurs spectres). Il mérite donc sa place à part.

Lemme 5.2.1. *(Going-up de Cohen-Seidenberg). Soient A, B deux anneaux avec $A \subset B$ et B entier sur A. On a les propriétés suivantes :*

1. *L'application $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ de spec B dans spec A est surjective. On a de plus : pour tous $\mathfrak{p}, \mathfrak{p}'$ de spec A avec $\mathfrak{p} \subset \mathfrak{p}'$ et pour tout $\mathfrak{q} \in$ spec B tel que $\mathfrak{q} \cap A = \mathfrak{p}$, il existe $\mathfrak{q}' \in$ spec B avec $\mathfrak{q}' \cap A = \mathfrak{p}'$ et $\mathfrak{q} \subset \mathfrak{q}'$.*
2. *L'application $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ est "presque" injective : si on a $\mathfrak{q}, \mathfrak{q}' \in$ spec B avec $\mathfrak{q} \subset \mathfrak{q}'$ et si $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$, alors $\mathfrak{q} = \mathfrak{q}'$.*
3. *A et B ont même dimension de Krull.*

Démonstration. Cette preuve est plutôt longue et technique, mais intéréssante : elle utilise beaucoup de résultats importants, et fait grandement appel à la localisation. On peut dire, en un certain sens, qu'une grande partie du théorème qu'on souhaite démontrer réside dans ce résultat. L'assertion 3) pouvait le laisser penser tant elle est forte ! Commençons par le premier point, pour lequel nous avons besoin du résultat suivant.

Soit J un ideal de B et soit $I = J \cap A$. Par propriété universelle du quotient, A/I **est un sous-anneau de** B/J **et l'extension est entière** : il suffit de passer les relations au quotient par J, par la propriété universelle (on le voit aisément sur un diagramme) les coefficients (dans A) deviennent ni plus ni moins que quotientés par I puis injectés dans B/J.

Maintenant on suppose A local d'idéal maximal $\mathfrak{m}$. On veut montrer que idéaux premiers $\mathfrak{q}$ de B vérifiant $\mathfrak{q} \cap A = \mathfrak{m}$ sont exactement les maximaux de B. Pour cela, on utilise l'assertion que l'on vient de montrer. On obtient une extension entière $A/\mathfrak{m} \subset B/\mathfrak{q}$ et on conclut par le lemme 3.2.2 : dans un sens, $\mathfrak{q}$ est maximal, dans l'autre, on obtient que $\mathfrak{q} \cap A$ est maximal donc n'est autre que $\mathfrak{m}$.

Avant de finir, un dernier résultat, pour se raccrocher au cas général : on rappelle que pour un idéal premier $\mathfrak{p}$ de A, le localisé $A_\mathfrak{p}$ est un anneau local (d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$). Par propriété universelle du localisé (les éléments de $A \setminus \mathfrak{p}$ sont bien inversibles dans $B_\mathfrak{p} = B[A \setminus \mathfrak{p}]^{-1}$ – attention ça n'est pas la notation usuelle) on a une injection $A_\mathfrak{p} \subset B_\mathfrak{p}$, et cette extension est entière : il suffit de remarquer que pour un élément courant $\dfrac{b}{s}$ de $B_\mathfrak{p}$, avec la relation initiale $b^n + a_{n-1}b^{n-1} + ... + a_0 = 0$ on obtient par division par s^n la relation satisfaisante :

$$\frac{b^n}{s^n} + \frac{a_{n-1}}{s}\frac{b^{n-1}}{s^{n-1}} + ... + \frac{a_0}{s^n} = 0$$

On peut maintenant appliquer les 2 résultats précédents pour conclure sur le point du lemme. On se place dans les localisés $A_\mathfrak{p}$ (anneau local) et $B_\mathfrak{p} = B[A \setminus \mathfrak{p}]^{-1}$ afin de tomber dans le cas déjà un peu traité. L'application du point précédent montre alors que tout idéal maximal de $B_\mathfrak{p}$ contenant $\mathfrak{p}B_\mathfrak{p}$, par exemple $\mathfrak{p}B_\mathfrak{p}$ lui-même, contiendra $\mathfrak{p}A_\mathfrak{p}$ une fois intersecté avec $A_\mathfrak{p}$ donc sera $\mathfrak{p}A_\mathfrak{p}$.

Encore faut-il que de tels idéaux existent, pour cela, il faut et il suffit que $\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$. Si ça n'était pas le cas, $1 \in B_\mathfrak{p}$ pourrait s'écrire comme combinaison linéaire finie d'éléments de $\mathfrak{p}B_\mathfrak{p}$, disons $a_1, \cdots, a_r$. Notons $B'_\mathfrak{p} = A_\mathfrak{p}[a_1, \cdots, a_r]$ la sous-algèbre de $B_\mathfrak{p}$ engendrée par ces éléments. Cette algèbre étant générée par un nombre **fini** d'éléments **algébriques**, elle est aussi un $A_\mathfrak{p}$-module de type fini (c'est un exercice classique que je ne referai pas ici). Mais comme elle contient 1, on a, au sens des modules $\mathfrak{p}B'_\mathfrak{p} = B'_\mathfrak{p}$ et le lemme de Nakayama permet d'affirmer que $B'_\mathfrak{p} = 0$ ce qui est absurde.

Ainsi, on a bien l'existence d'un idéal maximal de $B_\mathfrak{p}$ qui contient $\mathfrak{p}B_\mathfrak{p}$, disons $\mathfrak{n}$. Ce qui nous permet d'écrire finalement $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ comme voulu.

Maintenant, "délocalisons" : en prenant dans cette relation les images réciproques par l'application (notée disons $l_{A\setminus\mathfrak{p}} : b \mapsto \frac{b}{1}$) d'envoi dans le localisé $B_\mathfrak{p}$ on obtient

$\mathfrak{q} \cap A = \mathfrak{p}$ avec $\mathfrak{q} = l^{-1}_{A\setminus\mathfrak{p}}(\mathfrak{n})$ qui est un idéal premier de B par théorème sur la localisation des idéaux premiers. [6]

Ceci donne la surjectivité énoncée ; la remarque supplémentaire s'obtient directement en faisant la même chose avec $\mathfrak{p}'$ et en remarquant que les éléments de B envoyés dans $\mathfrak{p}B_\mathfrak{p}$ sont bien évidemment aussi envoyés dans $\mathfrak{p}'B_{\mathfrak{p}'}$.

Deuxième point : il est peut-être un peu plus rapide mais demande aussi un résultat intermédiaire.

6. Par ailleurs, le théorème mentionne aussi que cet idéal ne touche pas $A \setminus \mathfrak{p}$, ce qui est rassurant !

Lemme 5.2.2. *Soient $R \subset S$ sont deux anneaux intègres. Si $K(S)$ est algébrique sur $K(R)$ alors tout idéal non nul de S a une intersection non vide avec R.*

Démonstration. Il suffit de traiter le cas minimal : un idéal principal (b) non nul. On a une relation du type $a_0 + a_1 b + \cdots + a_n b^n = 0$ avec $a_i \in R$. Quitte à multiplier cette relation par un dénominateur commun des a_i et à diviser une puissance de b, on peut supposer $a_0 \neq 0$ et $a_i \in R$. Alors clairement, $a_0 \in (b)$. □

Retour à la quasi injectivité : supposons qu'on ait $\mathfrak{q} \subset \mathfrak{q}' \subset B$ avec $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$. On se place dans $A/\mathfrak{p}$ et $B/\mathfrak{q}$, qui sont des anneaux intègres et forment une extension entière, comme déjà vu au début de cette preuve. Les corps des fractions respectifs de ces anneaux forment donc aussi une extension algébrique. Ici on a $\mathfrak{q}'/\mathfrak{q} \cap A/\mathfrak{p} = 0$ et par le lemme précédent, $\mathfrak{q}'/\mathfrak{q} = 0$ soit $\mathfrak{q} = \mathfrak{q}'$.

Troisième point : on a tout réuni. On passe des chaînes d'idéaux premiers de B à celles de A par intersection avec A, et comme on a des inclusions, par la presque injectivité tout se passe bien (on passe d'une chaîne à une chaîne). □

5.3 Preuve du théorème

Démonstration. Tout d'abord, je rappelle que la dimension d'un espace topologique est le supremum des longueurs de chaînes de parties fermées irréductibles dans l'espace (notion développée par Brouwer en 1913, encore une fois selon [Eis][VIII]).

Pour commencer, montrons le lemme suivant qui fait en quelque sorte le lien entre algèbre et géométrie à la base du résultat.

Lemme 5.3.1. *Avec les hypothèses du théorème, $dim V = dim_k \Gamma(V)$ (où le terme de droite est pris au sens de la dimension de Krull).*

Démonstration. On pouvait s'en douter : derrière un tel lien algèbre-géométrie, on va retrouver le Nullstellensatz. En fait, le résultat découle directement de la bijection entre les idéaux premiers de $\Gamma(V)$ et les parties fermées irréductibles de V, déjà explicité précédemment au 4.2.1. □

Il faut maintenant faire un peu d'algèbre : il s'agit de montrer que $dim_k \Gamma(V) = \partial_k K$. Le théorème utilise deux outils fondamentaux de l'algèbre commutative : le *lemme de normalisation de Noether* que l'on a déjà explicité et le *going-up de Cohen-Seidenberg* découvert il y a peu.

Retour au théorème : on voulait montrer $dim_k \Gamma(V) = \partial_k K$.

On note d'abord que $\partial_k k(X_1, \cdots, X_n) = n$, $(X_1, \cdots, X_n)$ étant une base de transcendance évidente et que dim $k[X_1, \cdots, X_n] \geq n$ puisque $(0) \subsetneq (X_1) \subsetneq \cdots \subsetneq (X_1, \cdots, X_n)$ est une chaîne convenable.

Procédons par récurrence sur $\partial_k K$. Le cas $\partial_k K = 0$ est trivial, puisque dans ce cas le corps des fractions de $\Gamma(V)$ est algébrique sur $\Gamma(V)$, ce qui signifie que $\Gamma(V)$ est un corps et a donc trivialement une dimension de Krull nulle. Supposons le résultat pour $\partial_k K = n-1$. Si $\partial_k K = n$, par le lemme de normalisation de Noether 3.2.1 on a une extension entière $k[X_1, \cdots, X_n] \subset \Gamma(V)$, et par le going-up de Cohen-Seidenberg, $dim_k \Gamma(V) = dim_k k[X_1, \cdots, X_n]$. Il s'agit de montrer que cette dimension est plus petite que n. Supposons le contraire. On dispose donc d'une chaîne de $n+1$ idéaux premiers. En quotientant par le plus petit (non nul !), et en passant au quotient, on dispose donc d'une chaîne de n idéaux premiers dans l'anneau quotient. Reste à voir un petit résultat qui prouve que ce fait est impossible.

Lemme 5.3.2. *Soit $\mathfrak{p}$ un idéal premier non nul de $k[X_1, \cdots, X_n]$, alors le degré de transcendance du corps des fractions de $k[X_1, \cdots, X_n]/\mathfrak{p}$ est plus petit que $n-1$*

Démonstration. Il suffit de remarquer que pour un polynôme non nul $P \in \mathfrak{p}$, on aura dans le quotient, $P(\overline{X_1}, \cdots, \overline{X_n}) = 0$ ce qui prouve que la famille $(\overline{X_1}, \cdots, \overline{X_n})$ est algébriquement liée. □

Par hypothèse de récurrence, la dimension de l'anneau quotient est donc plus petite que $n-1$ et ainsi la chaîne trouvée à l'instant mène à une absurdité ; ceci achève la récurrence et la preuve. □

6 Conclusion

Mon stage s'est déroulé sur un peu plus de deux mois à l'Institut de Mathématiques de Bordeaux. Je remercie Qing Liu pour son encadrement et l'IMB de façon générale pour l'accueil agréable dans ses locaux, ainsi que mes co-stagiaires et les doctorants de la salle 100.

D'un point de vue professionnel, ce stage m'a été d'une grande importance. Je m'étais résolument tourné vers un M2 d'analyse à Toulouse, avant de finalement apprendre, au cours de ce stage, que j'allais passer l'agrégation contre toute attente l'année suivante. Ainsi j'ai toujours aimé l'algèbre, et tout particulièrement le cours d'algèbre commutative de Florian Ivorra que j'avais suvi, mais je ne me voyais pas non plus en faire au quotidien ; dans une certaine mesure ce stage était donc une façon d'entrer dans le vif du sujet et de me mettre dans des chaussures que je ne m'appropriais pas *a priori*. Au final j'ai été agréablement surpris : la qualité de l'accueil, de la bibliothèque de l'institut, la réactivité de mon encadrant quant à mes questions ont fait que j'avais toujours quelque chose à faire et avait constamment l'impression d'avancer dans ma compréhension et ma découverte de l'algèbre comme de la géométrie. Plus important encore, désormais je me sens beaucoup à l'aise en algèbre, de façon générale ; j'ai l'impression que le travail que j'ai effectué en algèbre commutative me donne un certain recul dans la matière désormais (j'ai été agréablement amusé lorsque j'ai relu mon cours de M1).

Mathématiquement, mon stage a commencé avec ce que j'ai annoncé dans le résumé : énoncer, prouver, et illustrer le Nullstellensatz sous tous ses aspects. Mais un point important est qu'en parallèle M. Liu me posait quelques exercices qui utilisaient la notion de dimension de Krull et reposaient sur des aspects intéréssants de géométrie que je ne connaissais pas encore (espace tangent à une variété en un point). Tout au long de ce travail, j'ai donc été amené à rencontrer beaucoup d'outils importants de l'algèbre commutative (lemmes de Nakayama, de normalisation, théorème de l'idéal principal généralisé, going-up, anneaux de Jacobson...) et me suis donc promené dans les diverses directions où ils pouvaient me mener. C'est notamment les anneaux de Jacobson et leur sens topologique, ainsi que lemme de normalisation de Noether et la notion de dimension de Krull qui m'ont donné la volonté de me tourner vers des aspects plus géométriques. La généralisation du Nullstellensatz à un corps quelconque et l'exercice qui allait avec ont fini par me faire m'intéresser sérieusement à la géométrie algébrique ; j'ai donc passé une autre grande partie de ce stage à me clarifier les idées quant à la notion de variété algébrique (en lisant et travaillant [Perrin]), par exemple lorsque je voulais mettre l'algèbre commutative en pause et/ou lorsque je butais. Cette partie de mon travail, dans ce rapport, a abouti sur la démonstration du théorème fondamental sur la dimension des variétés algébriques.

Côté algèbre commutative, ma référence principale a été indubitablement [Eis]. C'est un livre très agréable, même si l'auteur a tendance à ne pas détailler certains points dans ses preuves, il est très clair sur toute la longueur de son ouvrage qui est presque exhaustif en algèbre commutative. Un autre côté intéréssant du livre, et qui m'a contaminé, est la tendance de l'auteur à présenter l'histoire (parfois détaillée !) de la plupart de ses énoncés.

Pour terminer, je remercie encore une fois Qing Liu et l'IMB pour leur accueil.

Références

[Eis] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, 1999 (corrected third printing).

[Lang] Serge Lang, *Algebra*, Springer, 2005 (revised third edition).

[Liu] Qing Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002.

[Perrin] Daniel Perrin, *Géométrie algébrique – une introduction*, EDP Sciences / CNRS Éditions, 1995.

[Ivorra] Florian Ivorra, cours d'algèbre commutative et géométrie algébrique, *Une introduction aux bases de Grœbner* à l'Université de Rennes 1, 2009-2010.

[Debarre] Olivier Debarre, *Introduction à la géométrie algébrique*, cours de D.E.A à l'Université Louis-Pasteur, 1999-2000.

[ACL] Antoine Chambert-Loir, *Algèbre commutative et introduction à la géométrie algébrique*, cours accéléré de 3ème cycle à l'Université Pierre et Marie Curie, 1999.