MÉMOIRE DE SÉMINAIRE : LE THÉORÈME D'AX-GROTHENDIECK

par

Aurore Boitrel

Table des matières

1. Introduction

Le théorème d'Ax-Grothendieck, prouvé dans les années 1960 indépendamment par James Ax et Alexandre Grothendieck, déclare dans le cas particulier traité dans ce document que toute application polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^n$ qui est injective est également surjective. On dit que $P : \mathbb{C}^n \to \mathbb{C}^n$ est polynomiale si

$$P(X_1,\dots,X_n) = (P_1(X_1,\dots,X_n),\dots,P_n(X_1,\dots,X_n)),$$

où chaque $P_i \in \mathbb{C}[X_1,\dots,X_n]$. Ainsi, P est un n-uplet de polynômes en n variables. Cela semble être beaucoup d'informations qu'il nous faut indexer correctement et dont il nous faut garder trace, mais la clé de la preuve est que l'information requise est en fait "finie". Nous allons utiliser l'un des théorèmes fondamentaux de l'algèbre commutative et de la géométrie algébrique pour le montrer : le théorème des zéros de Hilbert (aussi connu sous le nom de "Nullstellensatz"). Nous verrons aussi comment l'énoncé de ce dernier dans sa forme "générale" nous permet de traduire certaines relations algébriques dans $\mathbb{C}$ en des relations algébriques dans un corps fini, nous autorisant ainsi à utiliser l'arithmétique des corps finis pour démontrer un énoncé sur $\mathbb{C}$, ce qui est remarquable.

2. Deux versions dites classiques du Nullstellensatz

Définition 2.1. — Soient k un corps et $S \subseteq k[X_1,\dots,X_n]$. On définit l'ensemble des zéros communs des polynômes de S par

$$V(S) := \{(x_1,\dots,x_n) \in k^n : P(x_1,\dots,x_n) = 0 \ \ \forall P \in S\}$$

Soit Z un sous-ensemble de k^n. On note $\mathcal{I}(Z)$ l'idéal de $k[X_1,\dots,X_n]$ défini par :

$$\mathcal{I}(Z) := \{f \in k[X_1,\dots,X_n] : \forall\, (x_1,\dots,x_n) \in Z \quad f(x_1,\dots,x_n) = 0\}$$

Théorème 2.2. — *(Nullstellensatz version faible)*
Soit k un corps ***algébriquement clos***. *Si $I \subseteq k[X_1,\dots,X_n]$ est un idéal propre, alors $V(I) \neq \varnothing$.*

Corollaire 2.3. — *Soit $f_1,\dots,f_r$ une collection de polynômes de $k[X_1,\dots,X_n]$. Alors soit les polynômes f_i ont un zéro commun dans k^n, soit il existe des polynômes $g_1,\dots,g_r$ dans $k[X_1,\dots,X_n]$ tels que $g_1f_1+\cdots+g_rf_r = 1$.*

Démonstration. — (du Corollaire 2.3.)
Soit $I = < f_1,\dots,f_r >$. Ou bien $V(I) \neq \varnothing$ et les polynômes f_i ont un zéro commun dans k^n, ou bien $V(I) = \varnothing$ et dans ce cas $1 \in I$. □

Théorème 2.4. — *(Nullstellensatz version forte)*
Soit k un corps ***algébriquement clos***. *Pour tout idéal I de $k[X_1,\dots,X_n]$, on a*

$$\mathcal{I}(V(I)) = \sqrt{I},$$

où $\sqrt{I}$ désigne le radical de I.

En particulier, si $f \in k[X_1,\dots,X_n]$ est tel que $f \in \mathcal{I}(V(I))$ où $I = < g_1,\dots,g_r >$ avec g_i polynôme de $k[X_1,\dots,X_n]$ pour tout $i \in \{1,\dots,r\}$, alors il existe des polynômes $Q_i \in k[X_1,\dots,X_n]$ et un entier $m \geqslant 1$ tels que $g_1Q_1+\cdots+g_rQ_r = f^m$.

Démonstration. — (du Théorème 2.4.)
Par définition, $I \subseteq \mathcal{I}(V(I))$ et comme $\mathcal{I}(V(I))$ est radical, nous avons $\sqrt{I} \subseteq \mathcal{I}(V(I))$. Réciproquement, soit $f \in \mathcal{I}(V(I))$. Écrivons $I = < g_1,\dots,g_r >$ (I a un nombre fini de générateurs dans $k[X_1,\dots,X_n]$) et supposons donc que f est un polynôme qui s'annule sur $V(I)$. Soit Y une nouvelle variable, considérons l'idéal $J = < g_1,\dots,g_r, Yf-1 > = I + < Yf-1 >$ dans l'anneau de polynômes $k[X_1,\dots,X_n,Y]$. Alors la variété algébrique $V(J) = V(I + < Yf-1 >) = V(I) \cap V(< Yf-1 >)$ est vide.
En effet, si $(x_1,\dots,x_n,y) \in V(J)$, on doit avoir $f(x_1,\dots,x_n) = 0$ et $y.f(x_1,\dots,x_n) - 1 = 0$. Comme ceci est impossible, on a bien $V(J) = \varnothing$.
Par le Théorème 2.2, on doit donc avoir $1 \in J$. Ainsi, il existe des polynômes $q_1,\dots,q_r,h$ dans $k[X_1,\dots,X_n,Y]$ tels que

$$\sum_{i=1}^{r} q_i(X_1,\dots,X_n,Y).g_i(X_1,\dots,X_n) \;+\; h(X_1,\dots,X_n,Y).(Yf(X_1,\dots,X_n)-1) = 1.$$

On peut supposer $f \neq 0$ (sinon il est évident que $f \in \sqrt{I}$) et évaluer Y en $\dfrac{1}{f} \in k(X_1,\dots,X_n)$ pour obtenir l'égalité suivante

$$1 = \sum_{i=1}^{r} q_i(X_1,\dots,X_n,\frac{1}{f(X_1,\dots,X_n)}).g_i(X_1,\dots,X_n).$$

Multipliant désormais chaque membre de l'égalité par le dénominateur commun égal à $f(X_1,\dots,X_n)^m$ pour un certain entier m, nous obtenons une identité polynômiale de la forme

$$\sum_{i=1}^{r} Q_i(X_1,\dots,X_n).g_i(X_1,\dots,X_n) = f(X_1,\dots,X_n)^m,$$

où $Q_i \in k[X_1,\dots,X_n]$.
Ceci montre que f^m appartient à l'idéal I et donc que f est dans $\sqrt{I}$, ce que nous voulions démontrer.

□

3. La forme générale du Nullstellensatz

Nous allons maintenant nous intéresser à une forme plus générale du Nullstellensatz, énoncée pour les anneaux de Jacobson, qui sera cruciale pour la conclusion de la preuve du théorème d'Ax-Grothendieck.

Définition 3.1. — (anneau de Jacobson)
On dit que R est un anneau de Jacobson si tout idéal premier de R est l'intersection d'idéaux maximaux.

Exemples 3.2. — (de tels anneaux)
- Il est clair que tout corps k est un anneau de Jacobson.
- $\mathbb{Z}$ est un anneau de Jacobson.

On rappelle ici deux résultats essentiels sur les extensions entières d'anneaux qui vont s'avérer faire partie des principaux ingrédients de la preuve du Nullstellensatz.

Définition 3.3. — Soit $A \to B$ une extension d'anneaux. Elle est dite *entière* si pour tout $b \in B$, il existe $P \in A[X]$ unitaire tel que $P(b) = 0$. On dit alors que b est *entier* sur A.

Théorème 3.4. — *Soit R un anneau et soit S une R-algèbre. L'ensemble de tous les éléments de S entiers sur R est une sous-algèbre de S. En particulier, si S est engendrée par des éléments **entiers** sur R, alors $R \to S$ est une extension entière.*

Proposition 3.5. — *Si $R \hookrightarrow S$ est une extension entière d'anneaux **intègres**, alors S est un corps si et seulement si R est un corps.*

Nous commençons par énoncer un lemme dont nous aurons aussi besoin dans la preuve du Nullstellensatz. Nous en donnons une démonstration, très largement inspirée de [**EIS**].

Lemme 3.6. — *Soit R un anneau. Sont équivalents*
a) R est un anneau de Jacobson.
b) Si $p \subset R$ est un idéal premier et si $S := R/p$ contient un élément $b \neq 0$ tel que le localisé $S[b^{-1}]$ est un corps, alors S est un corps.

Démonstration. — (Lemme 3.6.)
Montrons $a) \Rightarrow b)$ en montrant que (0) est un idéal maximal de S. Supposons $a)$ ainsi que l'hypothèse de $b)$. Comme R est de Jacobson, S l'est aussi donc l'intersection de tous les idéaux maximaux de S est incluse dans l'intersection de ses idéaux premiers, i.e. son nilradical. En effet,

$$\bigcap_{m\,\text{maximal}} m \quad \subset \quad \bigcap_{p\,\text{premier}} \bigcap_{p=\cap m_p} m_p \quad = \quad \bigcap_{p\,\text{premier}} p \; = \; \mathrm{Nil}(S),$$

où $\mathrm{Nil}(S)$ désigne le nilradical de S.
Or, S étant *intègre* (puisque p est premier), 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 par hypothèse, on sait qu'il n'y a alors qu'*un seul* idéal de S qui ne contienne pas b : c'est (0). En effet,
considérons $\varphi : S \to S[b^{-1}]$. Alors $\varphi^{-1}((0)) = \{a \in S \,;\, \exists n, b^n a = 0\} = \{0\}$.
Ainsi, (0) doit être un idéal maximal, sinon l'intersection de tous les idéaux maximaux de S contiendrait b, ce qui est impossible. Donc S est un corps.

Montrons maintenant $b) \Rightarrow a)$.
Soit Q un idéal premier de R, et soit $I = \bigcap_{Q \subset m \text{ maximal}} m \supseteq Q$.
On veut montrer que $I = Q$.
Supposons par l'absurde que l'inclusion est *stricte* , et prenons $c \in I \setminus Q$. On note b l'image de c par le morphisme quotient $R \xrightarrow{\pi} R/Q$. En particulier, on a le diagramme de correspondances suivant

$$\begin{array}{ccc}
\left\{ \begin{array}{c} \text{premiers} \\ \text{de } S[b^{-1}] \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{premiers de } S \\ \text{qui ne contiennent pas } b \end{array} \right\} \\
\updownarrow & & \updownarrow \\
\left\{ \begin{array}{c} \text{premiers de } R[c^{-1}] \\ \text{qui contiennent } Q.R[c^{-1}] \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{premiers de } R \\ \text{qui contiennent } Q \text{ et pas } c \end{array} \right\}
\end{array}$$

Par le lemme de Zorn, il existe un idéal premier p maximal parmi les idéaux premiers J de R vérifiant $Q \subset J \subsetneq < Q, c >$, c'est-à-dire contenant Q mais ne contenant pas c (l'union des éléments d'une chaîne de cet ensemble donne classiquement un majorant de la chaîne).
De plus, p n'est *pas* maximal car $p \subsetneq < Q, c > \subset I$ qui est stricte. Ainsi, R/p n'est *pas* un corps. Mais par définition, p engendre dans le localisé $R[c^{-1}]$ un idéal $p.R[c^{-1}] = p[c^{-1}]$ *maximal*, donc $(R/p)[c^{-1}] = R[c^{-1}]/p[c^{-1}]$ (par exactitude de la localisation) est un corps. Ceci est en contradiction avec l'hypothèse de $b)$, donc $I = Q$ et R est un anneau de Jacobson.

□

Remarque 3.7. — Soient R un anneau de Jacobson intègre, $b \in R \setminus \{0\}$ et $p = (0)$. Alors $R[b^{-1}]$ est un corps $\Rightarrow R$ est un corps.

On énonce enfin le Nullstellensatz dans sa forme générale, dont nous sommes à même de donner une démonstration, tirée de [**EIS**].

Théorème 3.8. — *(Nullstellensatz - Forme générale)*
Soient R un anneau de Jacobson et S une R-algèbre de type fini. Alors S est un anneau de Jacobson. De plus, si $n \subset S$ est un idéal maximal, alors $m := n \cap R$ est un idéal maximal de R, et $R/m \hookrightarrow S/n$ est une extension finie de corps.

Démonstration. — (Théorème 3.8.)

On va procéder à la preuve de ce théorème en trois étapes.

1. **Première étape** : On commence par un cas particulier. Supposons $R = K$ un corps, $S = K[x]$ et montrons que S est de Jacobson. On a

$$\begin{aligned}\mathrm{Spec}(S) &= \{(0)\} \bigcup \{n = (F),\ F \text{ irréductible unitaire}\} \\ &= \{(0)\} \bigcup \mathrm{Spm}(S).\end{aligned}$$

Puisque tous les idéaux premiers non nuls de S sont maximaux, il nous faut seulement vérifier que (0) est l'intersection d'idéaux premiers (donc maximaux) de S.
Comme aucun polynôme non nul ne peut avoir un nombre infini de facteurs irréductibles, il suffit de montrer que S a une infinité d'idéaux premiers, c'est-à-dire une infinité de polynômes irréductibles. En effet, dans ce cas,

$$\bigcap_{n \in \mathrm{Spm}(S)} n \quad = \quad \bigcap_{\text{infinie}, F_i \text{ irréd}} (F_i) \quad = \quad \{P;\ F_i \,|\, P\ \forall i\} = (0).$$

Pour cela, on utilise un argument bien connu d'Euclide :
Supposons que S ait un nombre fini de polynômes unitaires irréductibles $F_1, \ldots, F_k$.
Soit alors $P = \prod_{i=1}^{k} F_i + 1$. Comme K est un corps, les irréductibles de S sont au moins de degré 1, et donc P n'est pas l'un des F_i. Comme P est unitaire, P n'est pas irréductible. En particulier, l'un au moins des F_i divise P. Supposons que ce soit F_1 : $\exists\, Q \in S, P = F_1 Q$. Alors $F_1(Q - \prod_{i=2}^{k} F_i) = 1$. Donc F_1 est inversible, ce qui est faux.
Ainsi, S est bien de Jacobson.
Par ailleurs, si $n = (F)$ maximal, alors $m := K \cap n = (0)$ (polynômes constants et divisibles par F) et (0) est bien maximal puisque K est un corps. De plus,
$K/(0) = K \to K[x]/(F)$ est finie de dimension égale au degré de F. Donc la seconde conclusion du théorème est bien vérifiée dans ce cas.

2. **Deuxième étape** : Soient R un anneau de Jacobson quelconque et S une R-algèbre engendrée par *un seul* élément (i.e. $S = R[x]/I$ pour un certain idéal I).
Par le lemme 3.6, pour montrer que S est un anneau de Jacobson, il suffit de montrer :

$$\forall\, P \subset S \text{ premier}, \forall\, b \in S' := S/P,\ b \neq 0,\ S'[b^{-1}] \text{ est un corps} \Rightarrow S' \text{est un corps.} \qquad (1)$$

Posons $\pi = P \cap R$ premier dans R, $R_1 = R/\pi$ intègre, $S_1 = S' = S/P$ intègre contenant R_1, $b_1 = b$, $P_1 = P.S_1 = (0)$ et $S_1' = S_1/P_1 = S_1$.
On voit que R_1, S_1, P_1 et b_1 vérifient les mêmes hypothèses que dans (1).
De plus, on note que R_1 est intègre et $R_1 \to S_1$ est injectif, ce qui se lit très bien sur le diagramme suivant

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ R_1 = R/\pi & \hookrightarrow & S/P = S_1 \end{array}$$

On renomme maintenant en oubliant les indices "1". On s'est donc ramenés au cas où R et S sont intègres, $P = (0)$ impliquant $S' = S$ et $R \to S$ morphisme injectif

d'anneaux.
Nous allons en fait montrer que $R \to S$ est une extension *finie* de *corps* avec les hypothèses :

$$R \hookrightarrow S \hookrightarrow S[b^{-1}] \tag{2}$$

où S est engendrée par un élément en tant que R-algèbre et $S[b^{-1}]$ est un corps. Cela montrera ainsi les deux conclusions souhaitées du théorème dans le cas "renommé".
Comme S est engendrée sur R par un élément t, on peut écrire $S = R[x]/Q \ni \overline{x} =: t$, où Q est un idéal premier de $R[x]$. Alors $Q \neq 0$.
En effet, si au contraire $Q = 0$, on aurait $b \in S = R[x]$ non nul tel que $R[x][b^{-1}]$ soit un corps. En notant $K := \mathrm{Frac}(R)$ désignant le corps de fraction de R, et en écrivant $R[x][b^{-1}] \to \mathrm{Frac}(R)[x][b^{-1}]$, $K[x][b^{-1}]$ serait également un corps. Mais comme $K[x]$ est de Jacobson par l'**étape 1**, ceci contredirait le lemme 3.6 et donc $Q \neq 0$.
Soit donc $p(x) = p_n x^n + \cdots + p_1 x + p_0 \in Q \setminus \{0\}$, avec $p_n \neq 0$.
On a le diagramme

$$\begin{array}{ccc} R[x] & \xrightarrow{\text{quotient par } Q} & S \\ \downarrow & & \downarrow \\ R[p_n^{-1}][x] & \xrightarrow{\text{quot par } Q} & S[p_n^{-1}] \end{array}$$

Alors p est tel que $p(t) = p_n t^n + \cdots + p_1 t + p_0 = 0$ dans S. Multipliant $p(t)$ par p_n^{-1}, nous obtenons $t^n + \frac{p_{n-1}}{p_n} t^{n-1} + \cdots + \frac{p_0}{p_n} = 0$ dans $S[p_n^{-1}]$. Ainsi, comme S est engendrée par t comme R-algèbre, $S[p_n^{-1}]$ est engendrée par t comme $R[p_n^{-1}]$-algèbre et t est *entier* sur $R[p_n^{-1}]$. Par le théorème 3.4, $R[p_n^{-1}] \to S[p_n^{-1}]$ est *entière*. En particulier, $b \in S \subset S[p_n^{-1}]$ est entier sur $R[p_n^{-1}]$, c'est-à-dire qu'il existe une relation $b^m + r_{m-1} b^{m-1} + \cdots + r_1 b + r_0 = 0$, avec $r_i = \frac{q_i}{p_n^{a_i}} \in R[p_n^{-1}]$. En multipliant cette égalité par $q_m = p_n^{\max(a_i)}$, on a $q(b) = q_m b^m + \cdots + q_1 b + q_0 = 0$, avec $q \in R[x] \setminus \{0\}$.
Comme S est intègre, quitte à diviser par une puissance de b si nécessaire, on peut supposer $q_0 \neq 0$. Multipliant maintenant q par $\frac{1}{q_0 b^m}$ et écrivant désormais β pour b^{-1}, nous obtenons une relation de la forme

$$\beta^m + \frac{q_1}{q_0}\beta^{m-1} + \cdots + \frac{q_m}{q_0} = 0. \tag{3}$$

La relation (3) montre que $R[(p_n q_0)^{-1}] \to S[\beta]$ est *entière*. En effet, cela se déduit clairement du diagramme suivant

$$\begin{array}{ccccc} R & \hookrightarrow & S & \hookrightarrow & S[\beta] \\ \downarrow & & \downarrow & & \| \\ R[(p_n q_0)^{-1}] & \xhookrightarrow{\text{entière}} & S[(p_n q_0)^{-1}] & \xhookrightarrow{\text{entière, (3)}} & S[(p_n q_0)^{-1}, \beta] \end{array}$$

Comme $S[\beta]$ est un corps par hypothèse, la proposition 3.5 entraîne que $R[(p_n q_0)^{-1}]$ est un corps. R étant supposé de Jacobson, par la remarque 3.7

qui suit le lemme 3.6, R est lui-même un corps. Donc $R[p_n^{-1}] = R \to S[p_n^{-1}] = S$ est *entière*. De nouveau par la proposition 3.5, S est un *corps* et S est ainsi un anneau de Jacobson. De plus, comme S est de type fini sur R, $R \hookrightarrow S$ est *finie*.
En particulier, si $n \subset S$ est maximal, notons $m := n \bigcap R$. Alors l'hypothèse (2) déduite de (1), pour $P = n$, fournit ainsi le second résultat du théorème.

3. **Troisième et dernière étape** : Dans le cas général, on raisonne par récurrence sur le nombre r de générateurs de S comme R-algèbre.
Pour $r = 1$: c'est le résultat de la **deuxième étape**.
Pour $r \geqslant 2$: supposons le résultat du théorème vrai pour des R-algèbres ayant un nombre de générateurs $\leqslant r-1$. Soit S' la sous-algèbre de S engendrée par $r-1$ générateurs de S. Par hypothèse de récurrence, S' est de Jacobson, donc par le cas $r = 1$ (**étape 2**), S est aussi un anneau de Jacobson.
De la même manière, si n est un idéal maximal de S, alors $S' \bigcap n$ est un idéal maximal par le cas $r = 1$, et $R \bigcap n = R \bigcap (S' \bigcap n)$ est maximal par hypothèse de récurrence. On peut résumer la situation par le diagramme suivant

$$\begin{array}{ccccc} R \bigcap n & \hookrightarrow & S' \bigcap n & \hookrightarrow & n \\ \downarrow & & \downarrow & & \downarrow \\ R & \longrightarrow & S' & \longrightarrow & S \end{array}$$

Enfin, par un raisonnement analogue, comme les extensions $R/(R \bigcap n) \hookrightarrow S'/(S' \bigcap n)$ et $S'/(S' \bigcap n) \hookrightarrow S/n$ sont finies respectivement par l'hypothèse de récurrence et par le cas $r = 1$, alors $R/(R \bigcap n) \hookrightarrow S/n$ est *finie*, ce qui conclut la preuve du théorème.

□

4. La preuve du théorème d'Ax-Grothendieck

Nous rappelons l'énoncé du théorème que nous allons démontrer en suivant l'exposition de [**TAO10**] :

Théorème 4.1. — *(Ax-Grothendieck, cas $\mathbb{C}^n$)*
Soit $P : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale. Si P est injective, alors P est bijective.

La première observation est que le résultat de ce théorème est tout à fait trivial dans le cas d'un corps fini :

Théorème 4.2. — *Soit F un corps fini et soit $P : F^n \to F^n$ une application polynomiale. Si P est injective, alors P est bijective.*

Démonstration. — (du Théorème 4.2.)
Toute injection d'un ensemble fini dans lui-même est nécessairement une bijection.

□

Le Nullstellensatz nous permet de traduire les propriétés d'injectivité et de surjectivité des polynômes en des relations algébriques faisant intervenir une quantité finie de données, ce qui est l'idée principale de la preuve.

Lemme 4.3. — *Soit k un corps. Une application polynomiale $P : k^n \to k^n$, avec $P = (P_1,\dots,P_n)$, est injective* ***si*** *il existe $Q_{i,j} \in k[X_1,\dots,X_n,Y_1,\dots,Y_n]$ et $r_j \geqslant 1$ tels que*

$$\sum_{i=1}^{n} (P_i(X) - P_i(Y)).Q_{i,j}(X,Y) = (X_j - Y_j)^{r_j} \tag{4}$$

pour tout $1 \leqslant j \leqslant n$.
Si de plus k est ***algébriquement clos****, alors l'injectivité de P implique l'existence d'une telle relation (4).*

Démonstration. — (Lemme 4.3.)
Si l'identité (4) ci-dessus est vérifiée, il est clair que $P_i(X) - P_i(Y) = 0$ pour tout i implique $X_j - Y_j = 0$ pour tout j, i.e. $X - Y = 0$, et donc (4) implique bien l'injectivité de P.
Réciproquement, supposons de plus k algébriquement clos et P injective. Cela veut dire que si $P_i(X) - P_i(Y) = 0$ simultanément pour tout i (i.e. $P(X) = P(Y)$), avec $X = (X_1,\dots,X_n)$ et $Y = (Y_1,\dots,Y_n)$, alors $X_j = Y_j$ pour tout j, c'est-à-dire $X = Y$.
Fixons maintenant j et considérons les hypothèses du théorème 2.4. Par injectivité, le polynôme $X_j - Y_j$ s'annule en les points en lesquels l'ensemble de polynômes $\{P_i(X) - P_i(Y)\}_i$ de $A = k[X_1,\dots,X_n,Y_1,\dots,Y_n]$ s'annule. Ainsi, par le Nullstellensatz, on a l'existence de polynômes $Q_{i,j} \in A$ et d'un entier $r_j \geqslant 1$ tels que

$$\sum_{i=1}^{n} (P_i(X) - P_i(Y)).Q_{i,j}(X,Y) = (X_j - Y_j)^{r_j},$$

ce qui nous donne bien la relation (4).

□

De même, nous exprimons le manque de surjectivité en utilisant des équations polynomiales.

Lemme 4.4. — *Soit k un corps. Une application polynomiale $P : k^n \to k^n$, avec $P = (P_1,\dots,P_n)$, n'est* ***pas*** *surjective* ***si*** *il existe $z_0 \in k^n$ et un polynôme $R : k^n \to k^n$, avec $R = (R_1,\dots,R_n)$, tels que*

$$(P(X) - z_0).R(X) = 1. \tag{5}$$

Si de plus k est ***algébriquement clos****, alors l'hypothèse P* ***non*** *surjective entraîne l'existence d'une telle égalité (5).*

Démonstration. — (Lemme 4.4.)
Si la relation (5) ci-dessus est satisfaite, alors $P(X) \neq z_0$ pour tout $X \in k^n$, et donc P n'est *pas* surjective.
Réciproquement, si k est supposé algébriquement clos et si P n'est pas surjective, il existe un élément $z_0 = (z_{01},\dots,z_{0n}) \in k^n$ pour lequel $P(X) - z_0 \neq (0,\dots,0)$ quelque soit $X \in k^n$.
Notons $I = < P_1 - z_{01},\dots,P_n - z_{0n} >$. Alors $V(I) = \varnothing$ par hypothèse, et donc $1 \in I$ par les théorème 2.2 et corollaire 2.3. Le Nullstellensatz nous donne ainsi l'existence de polynômes $R_1,\dots,R_n \in k[X_1,\dots,X_n]$ tels que

$$\sum_{i=1}^{n} (P_i(X) - z_{0i}).R_i(X) = 1,$$

d'où l'égalité (5).

□

Nous sommes maintenant en mesure de prouver le théorème d'Ax-Grothendieck.

Démonstration. — (Théorème 4.1)

Supposons par l'absurde qu'il existe une application polynomiale $P : \mathbb{C}^n \to \mathbb{C}^n$, $P = (P_1, \ldots, P_n)$, qui soit *injective* mais *non surjective*. Comme $\mathbb{C}$ est un corps algébriquement clos par le théorème de d'Alembert-Gauss, on peut invoquer le Nullstellensatz comme précédemment et trouver les relations (4) et (5) respectivement des lemmes 4.3 et 4.4, pour certains $Q_{i,j}, z_0, R_i$. Considérons l'ensemble $\mathcal{C}$ constitué des coordonnées z_{0i} de z_0 et des coefficients des polynômes $P_i, Q_{i,j}$ et R_i. C'est un sous-ensemble **fini** de $\mathbb{C}$.
Considérons désormais la $\mathbb{Z}$-algèbre de type fini $B := \mathbb{Z}[\mathcal{C}] \subset \mathbb{C}$. Le lemme de Zorn nous fournit l'existence d'un idéal *maximal* $m \subset B$. L'anneau $\mathbb{Z}$ étant de Jacobson, nous pouvons appliquer le théorème 3.8. Alors $\mathbb{Z} \cap m = (p) \subset \mathbb{Z}$, avec p un nombre premier, est aussi un idéal maximal et $\mathbb{Z}/(p) = \mathbb{F}_p \hookrightarrow B/m$ est une extension *finie* de corps. Donc B/m est un corps fini. On peut alors réduire les équations polynomiales (4) et (5) via le morphisme d'anneaux $B[X,Y] \xrightarrow{\pi} (B/m)[X,Y]$; celles-ci étant maintenant vérifiées sur le corps fini B/m.
Cela implique, en notant $B/m := F$, que l'application "réduite" $\overline{P} : F^n \to F^n$ est injective et non surjective. Ceci est en contradiction avec le résultat du théorème 4.2, donc P est nécessairement surjective donc bijective.

□

5. Conclusion

Bien que l'énoncé et la preuve du théorème d'Ax-Grothendieck dans le cas $\mathbb{C}^n$ soient déjà intéressants et impressionnants, il est important de préciser que la version "complète" du théorème nous autorise à remplacer $\mathbb{C}^n$ par n'importe quelle variété algébrique X sur un corps algébriquement clos et P par un morphisme de X dans elle-même.
Par ailleurs, la conclusion du théorème est que l'application considérée est *bijective* ; ceci est plus faible que de dire que c'est un *isomorphisme*. Par exemple, le morphisme de $\mathbb{C}$-algèbres $f : \mathbb{C}[x,y]/(y^2 - x^3) \to \mathbb{C}[t]$ tel que $f(x) = t^2$ et $f(y) = t^3$, qui géométriquement induit le morphisme $\mathbb{A}^1_{\mathbb{C}} \to X = \mathrm{Spec}(\mathbb{C}[x,y]/(y^2 - x^3))$ de normalisation de la courbe avec un point de rebroussement (aussi appelée "cuspidale") $y^2 = x^3$, est bijectif mais *non* isomorphique.
On peut enfin noter que l'on obtient la conclusion *plus forte* que P est un isomorphisme en supposant de plus que c'est une immersion fermée ; et cette hypothèse *plus forte* rend alors la démonstration *plus facile*. Précisément, disons dans le cas affine, si $P : \mathrm{Spec}(A) \to \mathrm{Spec}(A)$ est une immersion fermée de schémas affines noethériens, alors il est assez facile de montrer que c'est un isomorphisme. Le théorème d'Ax-Grothendieck est ainsi une généralisation d'une version affaiblie de ce dernier résultat.

Références

[TAO10] Terence Tao. An epsilon of room, II : pages from year three of a mathematical blog. American Mathematical Society, 2010. Billet de blog *Infinite fields, finite fields, and the Ax-Grothendieck theorem* accessible à l'adresse : https ://terrytao.wordpress.com/2009/03/07/infinite-fields-finite-fields-and-the-ax-grothendieck-theorem/. 7

[EIS] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1996 (Corrected second printing). 3, 4

AURORE BOITREL