E.N.S. Cachan-IRMAR

Rapport de stage de M1

Utilisation des corps finis pour des problèmes concernant les corps infinis en Géométrie Algébrique

BENGUŞ-LASNIER Andrei

Maître de stage : Matthieu ROMAGNY

Résumé

Dans ce texte, nous avons expliqué les premiers résultats exposés dans l'article de J.P. Serre [Ser09] concernant le théme de la finitude en géomètrie algébrique. Nous avons relevé les différentes occurences de l'ambiguïté qui consiste à assimiler variété algébrique au sens classique et son pendant schématique. Nous nous sommes enfin intéressés à une difficulté quant au relèvement d'une action agissant sur un corps fini en une action en caractéristique 0, qui peut alors être considérée comme une action sur $\mathbb{C}$. Au sein de l'article, cette chose est présupposée mais ne semble pas immédiate. Nous avons mis en place une stratégie parallèle, afin de contourner la difficulté.

Nous commençons alors par rappeler quelques notions de base de la géomètrie algébrique classique et moderne, avant de passer aux résultats de l'article.

Table des matières

1 Introduction

Pour ma deuxième année à l'E.N.S. de Cachan j'ai décidé d'effectuer mon stage à l'IRMAR [1] sous la tutelle de Mr Matthieu ROMAGNY sur un théme touchant à la géométrie algébrique. Nous nous sommes mis d'accord pour étudier certains paragraphes d'un article publié par Serre en 2009 [Ser09]. Celui-ci se base sur une conférence tenue par l'auteur et présente plusieurs avantages :

- les résultats sont frappants.
- le texte est plutôt accessible pour un étudiant de Master.
- il permet d'aborder plusieurs aspects de la géométrie algébrique.

Les questions soulevées par J.P. Serre dans son cours sont encore d'actualité comme le prouve encore la publication d'articles comme [HE11] ou encore [HAU15].

Mon stage débuta le 1er mars 2015 et se termina le 15 juillet avec une soutenance devant mon maître de stage. Je fus très bien accueilli à l'Institut : on m'accorda un bureau avec un ordinateur et un casier, un badge pour pouvoir acceder au bâtiment ainsi que la possibilité de fréquenter la bibliothéque de l'IRMAR et d'y emprunter des ouvrages. J'ai eu également la possibilité de discuter avec les éléves doctorants.

Le sujet en lui-même fut traité en plusieurs étapes. Tout d'abord nous nous sommes mis d'accord pour m'initier aux objets fondamentaux qui me m'étaient indispensables : le Nullstellensatz, les schémas ainsi que de nombreux exemples. Par la suite nous nous sommes attaqués à l'article. Nous nous sommes focalisés sur deux théorèmes. Le premier porte sur les points fixes d'action de p-groupes.

Théorème *Si un p-groupe G agit sur l'espace affine $\mathbb{A}^n$ défini sur un corps algébriquement clos k, de caractéristique première avec p, alors l'action a des points fixes.*

Le second s'interesse aux endomorphismes des variétés. C'est le théorème d'Ax-Grothendieck.

Théorème *Soit X une variété affine (ou schéma affine de type fini) définie sur k, algébriquement clos. Si un morphisme $f : X \to X$ est injectif alors il est bijectif.*

Le but de mon étude fut de relever les ambiguïtés qui pouvaient subsister dans ces énoncés ainsi que leurs démonstrations. En effet à tout moment nous pouvons nous situer dans un contexte plutôt classique où nous travaillons qu'avec des variétés, comprises comme ensembles de solutions à un système d'équations, ou dans un

1. Institut de Recherche MAthématique de Rennes

contexte bien plus moderne où nous travaillons avec des schémas. Au cours de mon stage j'ai pris l'article et j'ai tenté de poser les résultats dans ce dernier en faisant usage du langage schématique. Nous avons exploré aussi des résultats mettant en perspective le théorème d'Ax-Grothendieck. Ceux-cis viennent de l'algèbre commutative. Au cours de cette investigation nous nous sommes particulièrement intéressés au relèvement des actions algébriques de caractéristique non-nulle en caractéristique nulle. Nous avons fini par noous rendre compte que nous ne pouvions pas répondre définitivement à cette question, néanmoins nous avons mis en évidence le lien avec une conjecture encore ouverte aujourdh'hui, appelée problème de la linéarisation. Nous y faisons appel à des outils venant de la cohomolgie des groupes.

2 Les notions fondamentales de la géométrie algébrique et le Nullstellensatz

Nous commençons par donner une introduction brève à la géométrie algébrique avant d'apporter deux preuves du théorème des zéros de Hilbert qui est à la base de cette branche des mathématiques.
Références : [Har77], [Per09], [Mat89], [Mum99], [Mac78].

2.1 Les variétés au sens classique

2.1.1 Les objets

La géomètrie algébrique étudie les apports géométriques à l'algèbre et vice-versa. Plus précisément, la géométrie algébrique classique s'interesse à l'étude des solutions d'équations polynomiales définies sur un corps k à n variables.

$$\text{Pour } E \subseteq k[X_1, \dots, X_n] \text{ on pose } Z(E) = \{x \in k^n \mid P(x) = 0 \quad \forall P \in E\}$$

Le Z vient d'Oscar **Z**ariski, mathématicien qui effectua un grand travail de formalisation algébrique des résultats de l'école italienne de géométrie, qui souffraient d'un manque de rigueur, allant jusqu'à publier des résultats faux ou non-justifiés. Désormais on appelle **ensemble algébrique** tout ensemble de cette forme, que l'on note, U, V, W, X ou Y [2].

Nous définissons également une opération duale qui consiste regarder les polynômes qui s'annulent sur un même ensemble $S \subseteq k^n$:

$$\mathfrak{I}(S) = \{P \in k[X_1, \dots, X_n] \mid P(x) = 0 \quad \forall x \in S\}$$

Cet ensemble est d'ailleurs un idéal. Afin de fixer les idées nous allons poser désormais k un corps, $n \in \mathbb{N}$ et $A = k[X_1, \dots, X_n]$. Nous pouvons déjà énoncer certaines propriétés :

Propriété – *$\mathfrak{I}$ et Z sont décroissantes pour l'ordre de l'inclusion :*

$$\textit{Si } S_1 \subseteq S_2 \textit{ dans } k^n \textit{ alors } \mathfrak{I}(S_1) \supseteq \mathfrak{I}(S_2)$$

$$\textit{Si } K_1 \subset K_2 \textit{ dans } A \textit{ alors } Z(K_1) \supseteq Z(K_2)$$

– *Pour un ensemble algebrique, nous pouvons considérer l'idéal engendré par les polynômes donnés :*

$$Z(E) = Z(\langle E \rangle)$$

Ainsi dans la suite nous allons considérer des ensembles algébriques d'idéaux. Comme A est noetherien, les idéaux sont génerés par un nombre fini de polynômes.

– *$\mathfrak{I}$ est quasi-injective car, si V est un ensemble algébrique*

$$Z(\mathfrak{I}(V)) = V$$

– *Les ensembles algébriques sont stables par intersection :*

$$Z(\bigcup_{\alpha} I_\alpha) = \bigcap_{\alpha} Z(I_\alpha)$$

2. Il est très important d'adopter de bonnes conventions de notations car nous pouvons nous retrouver avec des notations confuses du type $Z = Z(E)$.

– *Ils sont stables par union finie :*

$$Z(IJ) = Z(I \cap J) = Z(I) \cup Z(J)$$

Où IJ désigne l'idéal engendré par les produits délèments de I et J.

– *$\emptyset$ et k^n sont algébriques. Nous notons désormais k^n, $\mathbb{A}^n(k)$ ou encore $\mathbb{A}^n$ pour abréger*[3].

Démonstration
Tous les points sauf le *3)* et le *5)* sont tautologiques. On a clairement $V \subseteq Z(\mathfrak{I}(V))$. Supposons maintenant que $V = Z(I)$, alors $\mathfrak{I}(V) \supseteq I$ et donc par décroissance nous avons $Z(\mathfrak{I}(V)) \subseteq I$.
Vu que $IJ \subseteq I \cap J \subseteq I, J$ nous avons déjà $Z(IJ) \supseteq Z(I \cap J) \supseteq Z(I) \cup Z(J)$. Soit $x \in Z(IJ)$ et supposons que $x \notin Z(I)$. Ainsi on dispose de $P \in I$ tel que $P(x) \neq 0$; mais pour tout $Q \in J$, $\quad PQ(x) = P(x)Q(x) = 0$ par hypothèse, donc $\forall Q \in J,\ Q(x) = 0$ donc $x \in Z(J)$. □

Nous pouvons remarquer déjà que nos ensembles algébriques forment les fermés d'une topologie particulière appellée **topologie de Zariski**. Elle n'est pas habituelle puisqu'elle n'est pas de Hausdorff dès lors que le corps k est infini : si nous considérons deux ouverts d'intersection vide nous avons donc l'union de deux fermés, $Z(I)$ et $Z(J)$, qui recouvrent tout $\mathbb{A}^n$; d'après la propriété nous avons donc deux idéaux I et J tels que $Z(IJ) = \mathbb{A}^n$ or si un polyôme n'est pas nul alors d'après le lemme suivant il prend des valeurs non nulles ; par conséquent $IJ = (0)$ donc l'un des deux idéaux est nul (sinon on trouverait deux éléments non-nuls $P \in I$ et $Q \in J$, et alors $0 \neq PQ \in IJ$), disons $I = (0)$ ainsi $Z(I) = \mathbb{A}^n$ ce qui montre que, forcèment l'un des deux ouverts est vide.

Lemme *Soit k un corps infini. Alors pour tout $P \in k[X_1, \ldots, X_n]$ non-nul, nous avons $x \in k^n$ tel que $P(x) \neq 0$. Par la même occasion nous avons $\mathfrak{I}(\mathbb{A}^n) = \emptyset$.*

Remarque L'énoncé est faux dans le cas des corps finis : soit $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier et $q = p^r$ une puissance de p :

$$\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p \,|\, x^q - x = 0\}$$

Pourtant $X^q - X$ n'est pas nul dans $\mathbb{F}_q[X]$.

Démonstration
Nous faisons une démonstration par récurrence sur $n \in \mathbb{N}^*$. Pour $n = 1$ celà va de soi : un polynôme non nul de $k[X]$ (une seule variable), n'a qu'un nombre fini de solutions dans k, or k est infini. Supposons l'hypothèse de récurrence vraie au rang $n > 0$. Pour P polynôme non-nul à $n+1$ variables nous avons donc

$$P(X_1, \ldots, X_n, X) = \sum_{0 \leqslant i \leqslant m} a_i(X_1, \ldots, X_n) X^i$$

où, par hypothèse a_m est un polynôme non-nul à n variables, donc nous disposons de $x = (x_1, \ldots, x_n) \in k^n$ tel que $a_m(x) \neq 0$. Nous pouvons donc appliquer le cas $n = 1$ à $P(x_1, \ldots, x_n, X)$ polynôme non nul car le coefficient dominant est non nul. □

Nous munissons de manière naturelle $\mathbb{A}^n(k)$ de cette topologie de Zariski, néanmoins un ensemble algébrique en hérite de la topologie induite.
Dans ces cas il est pertinent de considérer les ensembles irréductibles d'une telle topologie que l'on surnommera ensemble algébrique affine :

Définition Un espace topologique X est dit **irréductible** lorsqu'il ne peux pas s'ecrire sous la forme d'une union de deux fermés propres de X, autrement dit, nous avons les propriétés équivalentes suivantes :

– X est irréductible.

– Si $X = F \cup G$ où F et G sont fermés dans X, alors $F = X$ ou $G = X$.

– Si $U \cap V = \emptyset$ où U et V sont des ouverts dans X, alors $U = \emptyset$ ou $V = \emptyset$.

3. Nous expliquerons la raison derrière cette notation un peu plus tard

– Tout ouvert de X est dense.
  Un sous-ensemble $Y \subseteq X$ est dit irréductible lorsque c'est un espace topologique irréductible pour la topologie induite.

Remarque Nous venons de démontrer plus haut que l'ensemble $\mathbb{A}^n$ est irréductible. Celà permet entre autres d'énoncer la principe de prolongement des identités algébriques pour k infini : On suppose que P s'annule en dehors d'un ensemble algébrique différent de $\mathbb{A}^n$; alors P s'annule sur tout $\mathbb{A}^n$.

Nous pouvons nous demander comment se traduit cette propriètè pour les ensembles algébriques et si nous avons une bonne caractérisation. Nous avons la première equivalence dans notre futur dictionnaire algebrico-géomètrique :

Propriété *V est irréductible ssi $\mathfrak{I}(V)$ est premier.*

Démonstration
Supposons d'abord V irréductible, et soient $f, g \in A$ tels que $fg \in \mathfrak{I}(V)$. Nous avons alors

$$V = Z(\mathfrak{I}(V)) \subseteq Z(fg) = Z(f) \cup Z(g) \text{ donc } V = (V \cap Z(f)) \cup (V \cap Z(g))$$

Par conséquent, vu que $V \cap Z(f)$ et $V \cap Z(g)$ sont des fermés de V nous avons par exemple $V \subseteq Z(f)$ ainsi $f \in \mathfrak{I}$. Réciproquement si l'idéal est premier, on peut supposer $V \subseteq Z(I) \cup Z(J) = Z(IJ)$ alors nous avons

$$IJ \subseteq \mathfrak{I}(Z(IJ)) \subseteq \mathfrak{I}(V)$$

Ainsi nous avons par exemple $I \subseteq \mathfrak{I}(V)$ ainsi $V \subseteq Z(I)$. □

Définition Nous allons désormais appeller **variété algébrique affine** un ensemble algébrique irréductible.

Cette notion est assez pertinente puisque tout ensemble algébrique se décompose en ensemble irréductibles.

Théorème *Tout ensemble algébrique V s'écrit de manière unique sous la forme*

$$V = V_1 \cup \ldots \cup V_m \quad \text{où} \quad V_i \not\subseteq V_j \quad \text{si} \quad i \neq j$$

*Où les V_k sont des ensembles irréductibles. Nous les appellons les **composantes irréductibles de** V.*

Démonstration
Pour l'existence nous supposons par l'absurde qu'il existe des ensembles algébriques qui ne se décomposent de cette façon. Nous considérons alors $S = \{\mathfrak{I}(V) \mid V \text{ ne se décompose pas}\}$. Comme A est noetherien (théorème de la base de Hilbert), nous pouvons donc considèrer un W tel que $I = \mathfrak{I}(W)$ soit maximal dans S. Comme W n'est pas irréductible, il peut donc s'ecrire comme union de deux fermés stricts : $W = F \cup G$ avec $F, G \subsetneq V$ ainsi $I \subsetneq \mathfrak{I}(F), \mathfrak{I}(G)$; par maximalité nous avons donc F, G décomposables donc V aussi, d'où la contradiction. Pour l'unicité nous considérons une double-décomposition comme dans l'énoncé $W_1 \cup \ldots \cup W_p = V_1 \cup \ldots \cup V_q$. Alors nous avons par irréductibilité $W_1 = (W_1 \cap V_1) \cup \ldots \cup (W_1 \cap V_q)$ qui est contenu dans un certain V_i, et ce dernier l'est aussi dans un certain W_k par conséquent $W_1 \subseteq V_i \subseteq W_k$, celà implique donc $k = 1$ et $W_1 = V_i$. Nous pouvons réiterer notre argument. □

Arrivés à ce stade nous avons déjà établi certaines correspondences entre objets algébriques, des idéaux, et géomètriques, des ensembles de points annulant une certaine collection de polynômes. Nous pouvons nous contenter de manipuler ce que l'on appelle **l'algébre affine de** V ou encore **l'anneau des coordonnés affines de** V :

$$\Gamma(V) = \frac{k[X_1, \ldots, X_n]}{\mathfrak{I}(V)}$$

Grosso-modo, nous avons identifié tous les polynômes, ou plutôt toutes les fonctions polynomiales qui prennent les mêmes valeurs sur V. Ainsi on peut voir $\Gamma(V)$ comme l'ensemble des fonctions polynomiales réstreintes à V.

Remarque Chose évidente que nous n'avons pas encore dit est que tout idéal $\mathfrak{I}(V)$ est radical, ce qui implique donc que $\Gamma(V)$ est une algèbre réduite (ne contient pas d'éléments nilpotents), de type fini sur k : si f^r s'annule sur tout V alors f s'annule sur tout V.

2.1.2 Les morphismes

Généralement en mathématiques, lorsque nous considérons des objets, nous nous intéressons aux applications entre ces objets qui préservent certaines relations. Ainsi nous nous intéressons en priorité, lorsqu'on travaille avec des groupes, aux morphismes de groupes, ou aux morphismes d'anneaux quand on travaille avec des anneaux en algébre commutative. Cette démarche a été formalisée et nous travaillons désormais avec le langage de la théorie des catégories. Pour plus de details voir [Mac78] ou encore [DD05].

Définition Soient $V \subseteq k^m$ et $W \subseteq k^n$ deux variétés algébriques affines telles que nous les avons définies plus haut. Un **morphisme de variétés** $\phi : V \to W$ est une application induite d'une fonction polynomiale $k^m \to k^n$. Nous avons donc n polynômes $P_1, \ldots, P_n$ à m variables et à coéfficients dans k tels que

$$\forall x = (x_1, \ldots, x_m) \in V,\ \phi(x) = (P_1(x_1, \ldots, x_m), \ldots, P_n(x_1, \ldots, x_m))$$

Nous disons alors que ϕ est **régulière** et nous notons l'ensemble corréspondant $\mathrm{Hom}_{\mathrm{Rég}}(V, W)$

Remarque Nous pouvons identifier $\Gamma(V)$ à l'ensemble des fonctions régulières de V sur $\mathbb{A}^1_k$. Nous considérerons désormais que ce sont les mêmes objets.

Nous allons noter $\phi = (\phi_1, \ldots, \phi_n)$ pour distinguer ses composantes. Nous remarquons alors que ces applications sont continues pour la topologie de Zariski. Nous avons vu plus haut comment associer à une variété son algèbre de coordonnées. Nous voulons montrer que nous avons ainsi défini un foncteur ; nous voulons donc associer à ϕ un morphisme d'algèbres. Ici nous utilisons le fait que $\Gamma(V)$ s'identifie à une sous partie de $\mathcal{F}(V, k)$. Nous pouvons alors définir

$$\phi^* : \Gamma(W) \to \Gamma(V),\ f \mapsto \phi^*(f) = f \circ \phi$$

Nous venons donc de mettre en évidence un foncteur contravariant Γ, puisque nous avons bien la propriété fonctorielle : $(\phi \circ \psi)^* = \psi^* \circ \phi^*$.

Proposition *Le foncteur Γ est pleinement fidèle, autrement dit $\phi \mapsto \phi^*$ définit une bijection entre $Hom_{Rég}(V, W)$ et $Hom_{k-alg}(\Gamma(W), \Gamma(V))$*

Démonstration
Il suffit d'exhiber l'application inverse. Or si nous notons ν_i l'image de Y_i dans $\Gamma(W)$, à $\theta \in \mathrm{Hom}_{k-\mathrm{alg}}(\Gamma(W), \Gamma(V))$ nous pouvons associer $\phi = (\theta(\nu_1), \ldots, \theta(\nu_n)) \in \mathrm{Hom}_{\mathrm{Rég}}(V, W)$. C'est l'application inverse cherchée. □

Nous pouvons donc conclure notre paragraphe avec le théorème qui suit faisant appel au Nullstellensatz, démontré aux paragraphes suivants. Pour nos besoins il nous dit que si $\mathfrak{p}$ est un idéal premier alors on a

$$\mathfrak{I}(Z(\mathfrak{p})) = \mathfrak{p}$$

.

Théorème *Pour k corps algèbriquement clos, le foncteur Γ est une équivalence entre les catégories des variétés algébriques affines et la catégorie des k-algébres de type fini réduites. Celà signifie qu'il est pleinement fidèle et essentiellement surjectif : si A est une k-algèbre de type fini réduite alors il existe V variété telle que A soit isomorphe à $\Gamma(V)$.*

Démonstration
Nous avons déjà vu la pleine fidélité, il nous reste à montrer que c'est essentiellement surjectif. Or pour notre algèbre A nous pouvons l'ecrire sous la forme

$$A = \frac{k[X_1, \ldots, X_m]}{I},\ I \text{ idéal premier}$$

D'après le Nullstellensatz il suffit donc de poser $V = Z(I)$ □

2.2 Le Nullstellensatz : par la normalisation de Noether

Nous démontrons ici le théorème des zeros qui a sérvi dans le paragraphe précédent mais qui servira également dans la suite. Fixons k un corps.

Théorème *Supposons que A est une algébre intègre de type fini sur k, et de degré de transcendence r sur k*[4]*. Il existe alors $x_1, \ldots, x_r$, des élèments algébriquement indépendents dans A tels que, A soit entière sur $k[x_1, \ldots, x_r]$ ou encore de manière équivalente, A est un $k[x_1, \ldots, x_r]$-module de type fini.*

DÉMONSTRATION
(D'après Mumford et Nagata). Nous démontrons le théorème par récurrence sur m le nombre de générateurs de A sur k. Premièrement nous écrivons $A = k[x_1, \ldots, x_m]$, ou encore $K = k(x_1, \ldots, x_m)$, et alors $m \geq n$. Si $m = n$ alors $\{x_1, \ldots, x_m\}$ est une base de transcendence de K/k. Ainsi nous avons initialisé notre récurrence et nous pouvons considerer désormais $m > n$. Soit $P \in k[X_1, \ldots, X_m]$ non-nul tel que $P(x_1, \ldots, x_m) = 0$: en effet comme $m > n$, les x_i ne sont algébriquement indépendents. Nous effectuons le changement de variables suivant : on pose $r_i \in \mathbb{N}, \quad i = 2, \ldots, m$ que l'on déterminera plus tard

$$Z_2 = X_2 - X_1^{r_2}, \ldots, Z_m = X_m - X_1^{r_m}$$

Ce changement de variables permet de voir P comme un polynôme Q en $X_1, Z_2, \ldots, Z_m$ et si nous avons $z_i = x_i - x_1^{r_i}, \quad i = 2, \ldots, m$ alors $A = k[x_1, z_2, \ldots, z_m]$ et $Q(x_1, z_2, \ldots, z_m) = 0$. Ce qui est interessant c'est que chaque monôme de P devient dans Q un polyôme en X_1 à coéfficient dominant inversible :

$$\text{Si } P = \sum_j a_j X_1^{\alpha_{1,j}} \ldots X_m^{\alpha_{m,j}} \text{ alors}$$
$$Q = \sum_j a_j X_1^{\alpha_{1,j} + r_2\alpha_{2,j} + \ldots + r_m\alpha_{m,j}} + \text{polynôme de degré strictement inferieur en } X_1, \text{ à coéfficients dans } k[Z_i]$$

Le but est de choisir les r_i de façon à ce que les puissances en X_1 obtenues à partir des monômes, soient différentes deux à deux ; dans ce cas, on aura forcément une de ces puissances qui sera plus grande strictement que les autres ; ceci permet alors de montrer que x_1 est entier sur $B = k[z_2, \ldots, z_m]$. Supposons alors que $\mathrm{Frac}(B) = L$ soit de degré de transcendence n' sur k. Nous avons donc $y_1, \ldots, y_{n'}$ algébriquement indépendents sur k tels que l'extension $L/k(y_1, \ldots, y_{n'})$ soit algébrique. Mais alors $K = L(x_1) = L[x_1]$ étant algébrique sur L on a donc $L/k(y_1, \ldots, y_{n'})$ algébrique donc $n' = n$. Ainsi, par hypothèse de récurrence, les y_i peuvent être choisis tels que B soit entier sur $k[y_1, \ldots, y_m]$; mais alors vue que A est entier sur B on a donc A entier sur $k[y_1, \ldots, y_m]$.
Montrons alors que le choix de tels r_i est possible. On se sert d'un petit résultat d'arithmètique :

Lemme *Soit t entier naturel strictement plus grand que les $|b_i|$ où les $b_0, \ldots, b_m$ sont des entiers. Alors*

$$\sum_{i=0}^{m} b_i t^i \neq 0$$

En effet si au contraire la somme est nulle, nous pouvons supposer $b_0 \neq 0$ quitte à reindexer et considerer le plus petit indice i tel que $b_i \neq 0$ et alors

$$0 \neq |b_0| = t|\sum_{i=1}^{m} b_i t^{i-1}|$$

Mais comme cet entier est non nul alors la somme, facteur de $|t|$ est un entier non-nul donc ≥ 1 ainsi $|b_0| \geq t$ ce qui est contradictoire.
Le lemme montre alors qu'il suffit de poser $r_i = t^i$ où t est un naturel plus grand que tous les $\alpha_{i,j}$. □

Desormais nous pouvons déjà montrer le **Nullstellensatz faible** :

Théorème *Pour k corps algébriquement clos, les idéaux maximaux de $k[X_1, \ldots, X_n]$ sont de la forme*

$$(X_1 - a_1, \ldots, X_n - a_n)$$

où $a_i \in k$. Ils correspondent donc aux points a de k^n.

4. de K, le corps des fractions de A

Démonstration
Nous remarquons que ces idéaux sont maximaux : le morphisme d'évaluation en a passe au quotient :

$$\begin{aligned} k[X_1,\dots,X_n]/(X_1-a_1,\dots,X_n-a_n) &\to k \\ P \bmod X_1-a_1,\dots,X_n-a_n &\mapsto P(a_1,\dots,a_n) \end{aligned}$$

est un isomorphisme[5]. Rèciproquement si M est un idéal maximal nous posons $K = k[X_1,\dots,X_n]/M$ le corps qui en découle. k s'injecte naturellement dans K : il existe un morphisme naturel $k \hookrightarrow k[X_1,\dots,X_n] \to K$; ce morphisme est injectif puisque c'est un morphisme de corps. Nous posons alors r le degré de transcendence de K/k. Nous allons montrer que c'est 0 grâce au lemme suivant qui est utilisé pour le going-up de Cohen-Seidenberg :

Lemme *Soient A un anneau et $B \subseteq A$ un sous-anneau, et on suppose que A est entier sur B. Alors A est un corps ssi B est un corps.*

Sens direct : soit $x \in B \setminus \{0\}$ et montrons que $x^{-1} \in A$ est dans B. Comme ce dernier est entier sur B nous avons $b_0,\dots,b_{p-1} \in B$ tels que :

$$b_0 \neq 0, \quad b_0 + b_1 x^{-1} + \dots + b_{p-1}x^{-(p-1)} + x^{-p} = 0$$

On suppose $b_0 \neq 0$ puisque de base nous avons une équation avec des termes dans B mais on peut factoriser la plus grande puissance de X dans le polynôme sous-jacent et obtenir ainsi un polynôme à coéfficient constant non-nul. Nous avons donc :

$$x^{-1} = -(b_0 x^{p-1} + b_1 x^{p-2} + \dots + b_{p-1}) \in B$$

Sens inverse : soit $x \in A \setminus \{0\}$ et montronsqu'il admet un inverse. Nous avons $b_0,\dots,b_{p-1} \in B$ tels que :

$$b_0 \neq 0, \quad b_0 + b_1 x^1 + \dots + b_{p-1}x^{p-1} + x^p = 0$$

Or b_0 est alors inversible et nous avons

$$-b_0 x(b_1 + \dots + x^{p-1}) = 1$$

ainsi x admet comme inverse $-b_0(b_1 + \dots + x_{p-1})$.

Maintenant d'après le théroème de normalisation nous avons $y_1,\dots,y_r$ algebriquement indépendents tels que, K soit entier sur $k[y_1,\dots,y_r]$ mais alors d'après le lemme, ce dernier est un corps d'où $r = 0$; l'extension K/k est algébrique mais k est algébriquement clos ainsi $K = k$. Par conséquent $X_i \in k + M$ donc il existe $a_i \in k$ tels que $X_i - a_i \in M$ donc $(X_1 - a_1,\dots,X_n - a_n) \subseteq M$ or ces deux idéaux sont maximaux donc sont égaux. □

Nous sommes enfin prêts à donner notre première démonstration du **Nullstellensatz**

Théorème *Soit k algébriquement clos, I un idéal polynomial à coéfficients dans k. Nous avons alors :*

$$\mathfrak{I}(Z(I)) = \sqrt{I}$$

Où $\sqrt{I}$ désigne l'idéal radical de I.

Démonstration
L'inclusion "$\supseteq$" est immédiate. Soit f un polynôme à coéfficients dans k qui s'annule sur $Z(I)$. Nous voulons montrer qu'il existe une puissance de f appartenant à I. L'idée clef[6] est de considerer de deux façons équivalentes la localisation de $k[X_1,\dots,X_n]$ quotienté par I, en la famille multiplicative $F = \{f, f^2, f^3, \dots\}$: nous rajoutons une variable Y et nous quotientons par $(1 - fY)$. Nous inversons de manière formelle f dans l'anneau de polynômes à n variables. Nous montrons que cet anneau est nul : ainsi F contient bien un élément nul dans $k[X_1,\dots,X_n]/I$. Ce sont des propriétés de base de la localisation.
Concrétement nous voulons montrer :

$$I \cdot k[X_1,\dots,X_n,Y] + (1 - fY) \cdot k[X_1,\dots,X_n,Y] = k[X_1,\dots,X_n,Y]$$

5. Il est clairement surjectif et il est forcément injectif : pour le voir nous pouvons effectuer des divisions euclidiennes successives des reste par les $X_i - a_i$
6. Parfois appellée astuce de Borevitch.

En raisonnant par l'absurde, cet idéal est inclus dans un idéal maximal $(X_1-a_1,\dots,X_n-a_n,Y-a)$, ainsi $(a_1,\dots,a_n)$ annule tout polynôme de I et $(a_1,\dots,a_n,a)$ annule $1-fY$ ce qui est contradictoire puisque $f(a_1,\dots,a_n)=0$. Nous avons donc $Q_k \in I$ et $P_k, P \in k[X_1,\dots,X_n,Y]$ tels que

$$\sum_k P_k Q_k + P(1-fY) = 1$$

En remplaçant Y par $\frac{1}{f}$ puis en multipliant parune puissance appropriée de f nous obtenons donc le résultat souhaité [7]. □

2.3 Le Nullstellensatz par la théorie des corps

La démonstration du Nullstellensatz, ici présentée, est tirée de Matsumura et comporte quatres étapes, qui ont chacune un intérêt en soi. Nous allons travailler sur des corps pas nécessairement algébriquement clos : si k est un corps alors on note $\overline{k}$, une de ses clotûres algébriques. Nous allons parler désormais de **zéro algébrique** d'un sous-ensemble Φ de $k[X_1,\dots,X_n]$: c'est un point de $\overline{k}^n$ qui annule tout polynôme de Φ.

Théorème *Soit L/k une extension de corps, algébrique ; soient $\alpha_1,\dots,\alpha_n \in L$ alors :*

1. $k[\alpha_1,\dots,\alpha_n] = k(\alpha_1,\dots,\alpha_n)$
2. *Pour $\phi : k[X_1,\dots,X_n] \longrightarrow k(\alpha_1,\dots,\alpha_n)$ envoyant X_i sur α_i, $Ker(\phi)$ est un idéal maximal engendré par n éléments de la forme $f_1(X_1),\dots,f_i(X_1,\dots,X_i),\dots,f_n(X_1,\dots,X_n)$ où f_i est unitaire en la variable X_i.*

Démonstration
Nous pouvons démontrer le premier point en construisant les extensions intérmédiaires successives et les f_i. Soit $f_1(X_1)$ le polynôme unitaire minimal de α_1 sur k. L'idéal $(f_1(X_1))\cdot k[X_1]$ est maximal puisque f_1 est irréductible, et on a :

$$k(\alpha_1) \cong \frac{k[X_1]}{(f_1)} \cong k[\alpha_1]$$

Soit $h_2(X_2) \in k(\alpha_1)[X_2]$ le polynôme minimal de α_2 sur $k(\alpha_1)$, que l'on suppose unitaire. On dispose de $f_2(X_1,X_2) \in k[X_1,X_2]$ unitaire en X_2, tel que $h(X_2) = f_2(\alpha_1,X_2)$ et demême degré en X_2. On a

$$k[\alpha_1,\alpha_2] = k[\alpha_1][\alpha_2] = k(\alpha_1)[\alpha_2] \cong \frac{k(\alpha_1)[X_2]}{(f_2(\alpha_1,X_2))} \cong k(\alpha_1)(\alpha_2) = k(\alpha_1,\alpha_2)$$

On réitère ce processus ; au rang $i \in \{1\dots,n\}$ on dispose déjà de $f_1,\dots,f_{i-1}$, alors on dispose de $h_i \in k(\alpha_1,\dots,\alpha_{i-1})[X_i]$ polynôme minimal de α_i sur $k(\alpha_1,\dots,\alpha_{i-1}$,unitaire, donc on a $f_i(X_1,\dots,X_i) \in k[X_1,\dots,X_i]$ unitaire en X_i tel que $h_i = f_i(\alpha_1,\dots,\alpha_{i-1},X_i)$ et de même degré en X_i ; ainsi :

$$k(\alpha_1,\dots,\alpha_i) \cong \frac{k(\alpha_1,\dots,\alpha_{i-1})[X_i]}{(f_i(\alpha_1,\dots,\alpha_{i-1},X_i))}$$

Ceci permet d'en déduire la première assertion. Pour démontrerla deuxième nous "remontons" ce même raisonnement.

Supposons désormais $P \in Ker(\phi)$; ainsi $\phi(P) = P(\alpha_1,\dots,\alpha_n) = 0$. Si $U_n = P(\alpha_1,\dots,\alpha_{n-1},X_n)$ alors clairement $U_n(\alpha_n) = 0$ et donc par dédinition $f_n(\alpha_1,\dots,\alpha_{n-1},X_n)$ divise U_n dans $k(\alpha_1,\dots,\alpha_{n-1})[X_n]$. Posons maintenant la division euclidienne dans $k([X_1,\dots,X_{n-1}])[X_n]$ [8] de P par f_n :

$$P = Q_n f_n + R_n, \quad \deg_{X_n} R_n < \deg_{X_n} f_n$$

En évaluant en $\alpha_1,\dots,\alpha_{n-1}$ nous avons $U_n = Q_n(\alpha_1,\dots,\alpha_{n-1},X_n)f_n(\alpha_1,\dots,\alpha_{n-1})$ d'après ce qu'on a dit plus haut. Ainsi $R(\alpha_1,\dots,\alpha_{n-1},X_n) = 0$. On recommence : on procède à la division euclidienne selon X_{n-1} de R_n par f_{n-1} :

$$R_n = Q_{n-1} f_{n-1} + R_{n-1}, \quad \deg_{X_{n-1}} R_{n-1} < \deg_{X_{n-1}} f_{n-1}$$

Regardons maintenant $R_{n-1}(\alpha_1,\dots,\alpha_{n-2},X_{n-1},X_n)$ comme un polynôme en X_n à coéfficients dans $k(\alpha_1,\dots,\alpha_{n-2})[X_{n-1}]$. Chacun de ces coéficients s'annulent en α_{n-1}, mais sont de degré en X_{n-1} strictement

7. Nos calculs se font dans $k(X_1,\dots,X_n)$
8. Donc en la variable X_n, ce qui est possible vu que f_n est unitaire en X_n

inférieur à celui de $f_{n-1}(\alpha_1,\dots,\alpha_{n-1},X_{n-1})$ par conséquent nous avons que chaque coéfficient est nul : $R_{n-1}(\alpha_1,\dots,\alpha_{n-2},X_{n-1},X_n)=0$. On réitère ce procédé : nous sommes à l'étape $i\in\{1,\dots,n\}$ et nous avons $P=R_{n-i+1}+\sum_{k=n-i+1}^{n}Q_kf_k$ et $R_{n-i+1}(\alpha_1,\dots,\alpha_{n-i},X_{n-i+1},\dots,X_n)=0$; si $i<n$ alors on pose la division euclidienne en X_{n-i} :

$$R_{n-i+1}=Q_{n-i}f_{n-i}+R_{n-i},\quad \deg_{X_{n-i}}R_{n-i}<\deg_{X_{n-i}}R_{n-i}$$

On écrit alors :

$$R_{n-i}(\alpha_1,\dots,\alpha_{n-i-1},X_{n-i},\dots,X_n)=\sum_j P_j(X_{n-i})X_{n-i+1}^{\nu_{n-i+1}^j}\dots X_n^{\nu_n^j}$$

où $P_j(X_{n-i})\in k(\alpha_1,\dots,\alpha_{n-i+1})[X_{n-i}]$ et comme $R_{n-i+1}(\alpha_1,\dots,\alpha_{n-i},X_{n-i+1},\dots,X_n)=0$ on a $P_j(\alpha_{n-i})=0$, de plus $\deg P_j<\deg_{X_{n-i}}f_{n-i}=\deg h_{n-i}$ ainsi $P_j=0$, par conséquent $R_{n-i}(\alpha_1,\dots,\alpha_{n-i-1},X_{n-i},\dots,X_n$. Ainsi, une fois arrivé à $i=n$, nous avons $P=R_1+\sum_{k=1}^{n}Q_kf_k$ avec $R_1(X_1,\dots,X_n)=0$ c'est-à-dire $R_1=0$. Donc $P\in(f_1,\dots,f_n)$. Ceci prouve $Ker(\phi)\subseteq(f_1,\dots,f_n)$, et l'inclusion réciproque est évidente. □

Nous passons maintenant à une sorte de réciproque de ce premier théorème. Celui-ci s'avère être utile dans un sens général, et pas seulement dans le cadre de la démonstration du Nullstellensatz.

Théorème *Pour k corps, $A=k[\alpha_1,\dots,\alpha_n]$ une k-algébre intègre de type fini, on pose $r=\deg.\mathrm{tr}_k(L)$ le degré de transcendence de $L=Frac(A)=k(\alpha_1,\dots,\alpha_n)$ sur k. Si $r>0$ alors A ne peut pas être un corps.*

Démonstration
On extrait de $\alpha_1,\dots,\alpha_n$ une base de transcendence $\alpha_1,\dots,\alpha_r$, posons alors $K=k(\alpha_1,\dots,\alpha_r)$, alors $\alpha_{r+1},\dots,\alpha_n$ sont algébriques sur K, donc par le théorème 1, nous disposons de $f_i(X_{r+1},\dots,X_i)\in k[X_{r+1},\dots,X_i]$ unitaire et de degré d_i en X_i, tels que :

$$\begin{aligned}L=K(\alpha_1,\dots,\alpha_n)&\cong\frac{K[X_{r+1},\dots,X_n]}{(f_{r+1},\dots,f_n)}\\ K(\alpha_1,\dots,\alpha_i)&\cong\frac{K(\alpha_1,\dots,\alpha_{i-1})[X_i]}{(f_i)}\\ d_i&=[K(\alpha_1,\dots,\alpha_i):K(\alpha_1,\dots,\alpha_{i-1})]\end{aligned}$$

On a à notre disposition un nombre fini de polynômes à un nombre fini de coefficients dans K. Il y a donc $g\in k[\alpha_1,\dots,\alpha_r]$ tel que $\forall i,\quad gf_i\in k[\alpha_1,\dots,\alpha_r][X_{r+1},\dots,X_n]$. Ainsi il suffit de travailler dans $B=k[\alpha_1,\dots,\alpha_r,g^{-1}]\subset K$. Nous allons montrer que $B[\alpha_{r+1},\dots,\alpha_n]=A[g^{-1}]$ est un B-module libre de type fini, de base $E=\{\prod_{i=r+1}^{n}\alpha_i^{e_i}\mid 0\le e_i\le d_i-1\}$. Déjà, E est libre sur K, et donc sur B aussi, puisqu'elle engendre L[9] de degré $\prod d_i$ et E est de cardinal $\prod d_i$. Montrons qu'elle est génératrice : soit $x\in B[\alpha_{r+1},\dots,\alpha_n]$ et $P\in B[X_{r+1},\dots,X_n]$ tel que $x=P(\alpha_{r+1},\dots,\alpha_n)$. Quite à faire la divison euclidienne en X_n de P par f_n puis remplacer P par le reste, on peut supposer $\deg_{X_n}P<\deg_{X_n}f_n=d_n$. Nous pouvons faire de même pour les degrés en $X_{n-1},\dots,X_{r+1}$. Ainsi x est combinaison linéaire d'éléments de E à coéfficients dans B. Maintenant $A[\alpha_1,\dots,\alpha_r]$ n'est pas un corps puisque c'est un anneau polynômial à $r>0$ variables. De la même façon que nous montrons qu'il y a une infinité d'entiers premiers, nous montrons qu'il y a une infinité de polynômes irréductibles dans $A[\alpha_1,\dots,\alpha_r]$. On dispose alors de $h\in A[\alpha_1,\dots,\alpha_r]$ qui est premier avec g et donc h n'est pas inversible dans B ; on a alors I idéal de B tel que $(0)\subsetneq I\subsetneq B$. Vu que $A[g^{-1}]$ est libre sur B, on a $(0)\subsetneq I\cdot A[g^{-1}]\subsetneq A[g^{-1}]$ or $I\cdot A[g^{-1}]$ est un idéal de $A[g^{-1}]$. Ainsi A n'est pas un corps car alors on aurait $A=A[g^{-1}]$ qui est un corps ce qui est manifestement faux. □

Nous arrivons enfin au **Nullstellensatz faible**.

Théorème *Si k est un corps et $\mathfrak{m}$ un idéal maximal de $k[X_1,\dots,X_n]$. Le corps résiduel $k[X_1,\dots,X_n]/\mathfrak{m}$ est algébrique sur k et peut être engendréparn éléments. En particulier si $k=\overline{k}$ alors on a $a_i\in k$ tels que $\mathfrak{m}=(X_1-a_1,\dots,X_n-a_n)$.*

Démonstration
Posons $K=k[X_1,\dots,X_n]/\mathfrak{m}$ et α_i l'image de X_i dans K. Par le deuxième théorème K/k algébrique et $\mathfrak{m}$ est bien engendrée par n éléments. De plus si k est algébriquement clos, $K\cong k$, $\alpha_i=a_i\in k$ et donc $X_i\in a_i+\mathfrak{m}$ par conséquent $(X_1-a_1,\dots,X_n-a_n)\subseteq\mathfrak{m}$, or ces deux idéaux sont maximaux donc sont égaux. □

9. En fait là-dessous se cache le théorème des bases téléscopiques

Nous voici à la **version forte du Nullstellensatz**.

Théorème *Ici k est un corps et $\Phi \subset k[X_1, \ldots, X_n]$.*

1. *Si Φ n'a pas de zéro algébrique alors $\langle \Phi \rangle = k[X_1, \ldots, X_n] = (1)$*
2. *Si $f \in k[X_1, \ldots, X_n]$ annule tout zéro algébrique de Φ, alors il existe une puissance de f qui appartient à $\langle \Phi \rangle$: $\exists \nu \in \mathbb{N}^*, \exists g_i \in k[X_1, \ldots, X_n],\ h_i \in \Phi$ tels que $f^\nu = \sum_i g_i h_i$.*

Démonstration
Notons $I = \langle \Phi \rangle$ et supposons que $1 \notin I$, alors on peut inclure I dans un idéal maximal $\mathfrak{m}$, donc par le deuxième théorème on a $K = k[X_1, \ldots, X_n]/\mathfrak{m}$ algébrique sur k. Par le théorème de prolongement des morphismes d'algébres, on a un plongement $\theta : K \hookrightarrow \overline{k}$. On pose $\alpha_i = \theta(X_i \ mod \ \mathfrak{m})$. Pour tout $g \in \mathfrak{m}$,

$$0 = \theta(0 \ mod \ \mathfrak{m}) = \theta(g \ mod \ \mathfrak{m}) = g(\alpha_1, \ldots, \alpha_n)$$

Ainsi tout polynôme de $\mathfrak{m}$, donc par extension de ϕ, a $(\alpha_1, \ldots, \alpha_n)$ comme zéro algébrique. Si $\Phi' = \Phi \cup \{1 - fY\}$, on observe que Φ' n'a pas de zéro algébrique donc par le premier point, on a $P_i, Q \in k[X_1, \ldots, X_n, Y],\ h_i \in \Phi$ tels que :

$$1 = \sum_i P_i(X, Y) h_i(X) + Q(X, Y)(1 - f(X)Y)$$

Nous prenons cette identité dans $k(X)$ et y remplaçons $Y = f(X)^{-1}$. Pour obtenir une identité polynomiale et non fractionnaire nous multiplions par une puissance adéquate de f : on a donc ν entier non nul tel que

$$f^\nu = \sum_i g_i(X) h_i(X)$$

Ceci conclut la preuve du Nullstellensatz □

3 Schémas

Nous avons construit dans la séction précédente un "dictionnaire" algèbre-géométrie :

$$\left\{ \begin{matrix} \text{Variétés algèbriques} \\ \text{affines sur } k \\ \text{algébriquement clos} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} k-\text{algèbres de type} \\ \text{fini réduites} \end{matrix} \right\}$$

Le grand succés de la géométrie algébrique au milieu du XX^e siècle fut d'étendre cette correspondance en :

$$\begin{array}{ccc} \left\{ \begin{matrix} \text{Variétés algèbriques} \\ \text{affines sur } k \\ \text{algébriquement clos} \end{matrix} \right\} & \longleftrightarrow & \left\{ \begin{matrix} k-\text{algèbres de type} \\ \text{fini réduites} \end{matrix} \right\} \\ \downarrow & & \downarrow \\ \{\text{Schémas affines}\} & \longleftrightarrow & \{\text{Anneaux unitaires commutatifs}\} \end{array}$$

Néanmoins nous nous sommes rendus compte que le concept pertinent est celui de schéma général qui lui, est localement affine.

3.1 Évidences

Nous présentons ici des notions de base sur les schémas tout en omettant les concepts liés aux faisceaux car celà alourdirait bien trop notre texte.
Références : [EH00], [Bos13], [Mum99].

3.1.1 Les schémas sont des espaces localement annelés

Une fois connue la définition de faisceau, nous pouvons définir un **schéma** comme étant un espace topologique X muni d'un **faisceau structural** O_X, le rendant localement affine. Nous pouvons donc trouver une famille d'ouverts U_i tels que $(U_i, O_X|_{U_i})$ soit isomorphe à un $(\mathrm{Spec}(A_i), O_{\mathrm{Spec}(A_i)})$ où A est un anneau.

3.1.2 Les sections de O_X peuvent être vues comme de vraies fonctions

Afin de donner un sens à $a \in O_X(U)$, $x \in U$, a s'annule en x nous devons montrer que nous pouvons voir les éléments des $O_X(U)$, U ouvert de X, comme des fonctions. Or pour un élément $x \in U$ fixé on a les morphismes

$$O_X(U) \longrightarrow O_{X,x} \longrightarrow \kappa(x)$$

où $\kappa(x)$ désigne le corps résiduel de $O_{X,x}$, que nous allons juste nommer *corps résiduel en x*. Maintenant, $a \in O_X(U)$ est envoyé sur un élément de ce corps, et nous allons dire que a prend cette valeur en x, notée donc $a(x)$.

3.1.3 Les morphismes sont des morphismes locaux d'espaces localement annelés

Un **morphisme de schémas** c'est alors un morphisme d'espaces localement annelés. Plus précisément nous avons

$$(\phi, \phi^{\#}) : (X, O_X) \longrightarrow (Y, O_Y)$$

Avec

$$\phi : X \longrightarrow Y$$

fonction continue, et

$$\phi^{\#} : O_Y \longrightarrow \phi_* O_X$$

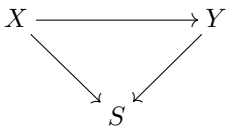
morphisme de faisceaux au-dessus de Y tel que, si $q = \phi(p)$ alors $\forall f \in O_Y(U)$, $U \subseteq Y$ ouvert de Y, f s'annule en q ssi $\phi^{\#}(f) \in O_X(\phi^{-1}U)$ s'annule en p. De manière équivalente nous avons $\phi^{\#}$ qui engendre un morphisme de fibres :

$$\phi_p^* : O_{Y,q} \xrightarrow{\varinjlim_{q \in U} \phi^{\#}(U)} \varinjlim_{q \in U} O_X(\phi^{-1}(U)) \longrightarrow O_{X,p}$$

tel que $\phi_p^*(m_{Y,q}) \subseteq m_{X,p}$, où les $m_{\bullet,\bullet}$ représentent les idéaux maximaux des anneaux locaux $O_{\bullet,\bullet}$.

3.2 S-schémas

Très souvent nous allons adopter le point de vue relatif qui consiste à considérer des **S-schémas**, c'est-à-dire un schéma X [10] muni d'un morphisme $X \longrightarrow S$. Nous pouvons toujours nous mettre en cette situation quitte à prendre $S = (\mathrm{Spec}(\mathbb{Z}), O_{\mathrm{Spec}(\mathbb{Z})})$. La plupart de notre travail se placera dans le cas où $S = (\mathrm{Spec}(k), O_{\mathrm{Spec}(k)})$ pour un corps pré-détérminé k. Nous allons abréger et parler de *k-schéma*. Dans ce cas, les anneaux que nous considérons sont des k-algèbres.

Desormais, quand nous parlons de morphisme de S-schéma nous allons considérer des $X \longrightarrow Y$ tels que :  soit commutatif.

3.3 Les points

3.3.1 Les points rationnels

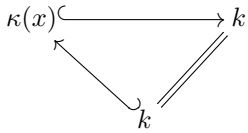
Lorsque nous avons un k-schéma X nous pouvons considérer $X(k)$ l'ensemble des **points rationnels ou k-rationnels de X** :

$$\begin{aligned} X(k) &= \{x \in |X|; \kappa(x) = k\} \\ &= \mathrm{Hom}_{\text{k-schéma}}(\mathrm{Spec}(k), X) \end{aligned}$$

En effet nous pouvons considérer un point k-rationnel $x \in \mathrm{Spec}(A) = U \subseteq |X|$ comme un morphisme $\mathrm{Spec}(k) \to X$ associé au morphisme de k-algèbre : $O_X(U) \to O_{X,x} \to \kappa(x) = k$. Réciproquement si nous avons

10. Quand nous pouvons, nous allons omettre O_X, et pour dire que nous considérons l'ensemble sous-jacent à notre schéma nous allons noter $|X|$

un morphisme $\mathrm{Spec}(k) \to X$, qui sur les ensembles donne $\bullet_k \mapsto x$ alors on a un morphisme de corps résiduels : $\kappa(x) \hookrightarrow k$ ce qui permet de nous donner $\kappa(x) = k$.



Nous pouvons généraliser par analogie et écrire pour tous S-schémas X, T :

$$X(T) = \mathrm{Hom}_{\text{S-schéma}}(T, X)$$

Nous pouvons même noter $X(T)_S$ pour préciser au-dessus de quel schéma nous opérons. Ainsi les S-schémas peuvent être vus comme des foncteurs contravariants [11] : **S-schémas** $\to$ **Ens**. Un morphisme $T \to T'$ est envoyé par post-composition en une application $X(T) \leftarrow X(T')$. Pour un morphisme $X \xrightarrow{\phi} Y$ de S-schémas, nous avons une transformation naturelle, qui donne pour tout T S-schéma, un morphisme $X(T) \xrightarrow{\phi(T)} Y(T)$, par post-composition.

Remarque Si $A \subseteq B$ sont des k-algébres, l'inclusion $A \hookrightarrow B$ donne lieu à un morphisme $\phi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ qui lui-même, par pré-composition (toujours contravariante), donne lieu au un morphisme $\mathrm{Hom}_S(\mathrm{Spec}(A), X) \to \mathrm{Hom}_S(\mathrm{Spec}(B), X)$. Nous avons donc un morphisme $X(A) \to X(B)$. Cette dernière application est, si X est affine, fait injective : soient en effet $u, v \in X(A)$ tels que $u \circ \phi = v \circ \phi$ Ces deux applications correspondent à des morphismes d'algébres $O_X(X) \rightrightarrows A \hookrightarrow B$, donc ces dernières sont égales et il en est de même pour u et v.

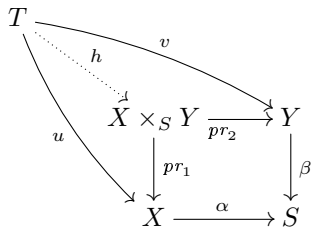
Si jamais $T = \mathrm{Spec}(A)$ pour un anneau A on abrège en $X(A)$.
Il est utile de préciser l'existence des produits dans une catégorie.

Définition *Nous appelons* ***produit fibré*** *de deux S-objets dans une catégorie $\mathscr{C}$, X et Y, tout objet noté $X \times_S Y$, muni de deux morphismes $pr_1 : X \times_S Y \to X$ et $pr_2 : X \times_S Y \to Y$ tels que le diagramme suivant commute :*

$$\begin{array}{ccc} X \times_S Y & \xrightarrow[pr_2]{} & Y \\ \downarrow{\scriptstyle pr_1} & & \downarrow{\scriptstyle \beta} \\ X & \xrightarrow{\alpha} & S \end{array}$$

et qui vérifient la propriété universelle suivante :

Pour tout autre S-objet T et touts morphismes de S-objets $u : T \to X$ et $v : T \to Y$, il existe un morphisme $h : T \to X \times_S Y$ faisant commuter le diagramme suivant :



Nous avons alors le résultat suivant sur les catégories (cf. [Mac78]) :

Théorème *Pour deux* S-objets X et Y*, nous avons la bijection naturelle entre foncteurs* ***Y-schéma*** $\to$ ***Ens*** *:*

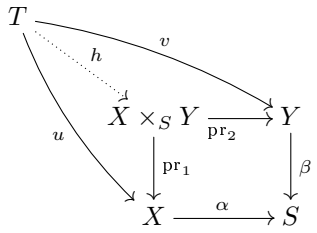
$$Hom_{S\text{-}objet}(\bullet, X) \simeq Hom_{Y\text{-}objet}(\bullet, X \times_S Y)$$

11. Ceci justifie entre autres la notation $\mathbb{A}^n$

Démonstration
Nous allons considérer T, Y-objet. Par propriété universelle du produit fibré nous avons

$$\mathrm{Hom}_Y(T, X \times_S Y) = \mathrm{Hom}_S(T, X) \times_{\mathrm{Hom}(T,S)} \mathrm{Hom}_S(T, Y)$$

Nous pouvons résumer la situation par le diagramme suivant :



Remarquons au passage que tout Y-morphisme $h : T \to X \times_S Y$ est également un S-morphisme. Ainsi vu que le morphisme v est fixé parle fait que T est un Y-schéma, nous avons la bijection souhaitée :

$$h \longmapsto \mathrm{pr}_2 \circ h \ (= u)$$

qui est clairement naturelle. □

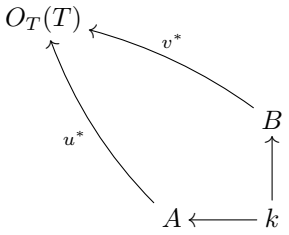
Nous pouvons montrer que les S-schémas affines ($S = \mathrm{Spec}(k)$ étant affine) admettent des produits fibrés. Le cas général est omis ici car nous obligerais de faire appel à la construction de recollement et ça n'a pas sa place ici.

Théorème *Si $X = Spec(A)$ et $Y = Spec(B)$ sont deux S-schémas affines ($S = Spec(k)$) alors nous pouvons construire leurproduit fibré. Deplus ce dernier est affine d'anneau $A \otimes_k B$.*

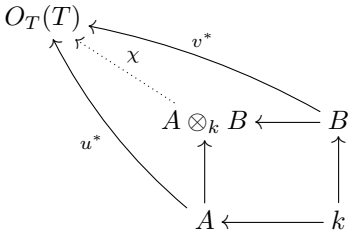
Démonstration
Il suffit de montrer que $\mathrm{Spec}(A \otimes_k B)$ vérifie la propriété universelle du produit fibré. Or nous savons que pour tout S-schéma T nous avons pour tout anneau R

$$\mathrm{Hom}_{S-schema}(T, \mathrm{Spec}(R)) = \mathrm{Hom}_{k-algebre}(O_T(T), R)$$

Ainsi nous avons pour tout couple de morphismes u et v allant de T vers X et Y respectivement, nous avons le diagramme équivalent suivant :



Cependant, d'après la propriété universelle du produit tensoriel nous avons un morphisme χ qui factorise le diagramme en



Les morphismes de$A$ et B vers le produit tensoriel sont les classiques $a \mapsto a \otimes 1$ et $b \mapsto 1 \otimes b$. □

Théorème *X, Y S-schémas et T Y-schéma, alors :*

$$X(T)_S = (X \times_S Y)(T)_Y$$

Démonstration
On a d'après le théorème précédent

$$X(T) = \mathrm{Hom_S}(T, X) = \mathrm{Hom_Y}(T, X \times_S Y) = (X \times_S Y)(T)$$

. □

3.3.2 Les points sont des morphismes à une relation d'équivalence près

Nous allons considérer des morphismes $(\phi, \phi^{\#})$ que nous allons qualifier de *surjectifs, injectifs, bijectifs*, ce qui signifiera que ϕ est respectivemet injective, surjective, bijective. Pour démontrer des énoncés concernant ces caractéristiques, nous allons reécrire X l'ensemble de base de notre k-schéma comme un ensemble de morphismes $\mathrm{Spec}(K) \longrightarrow X$ où ici K est un corps, extension de k [12]. Tout point $x = [p] \in \mathrm{Spec}(A) = U \subseteq X$ admet donc un corps résiduel $\kappa(x)$ et les morphismes

$$\kappa(x) \longleftarrow A_p \longleftarrow A$$

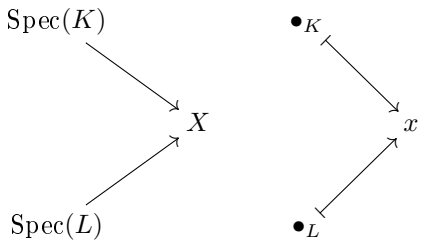
donnent lieu aux

$$\mathrm{Spec}(\kappa(x)) \longrightarrow \mathrm{Spec}(A_p) \longrightarrow \mathrm{Spec}(A) \hookrightarrow X$$

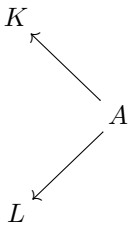
En fait, sur les ensembles nous avons :

$$\bullet_{\kappa(x)} \longmapsto [p_p] \longmapsto [p] \mapsto x$$

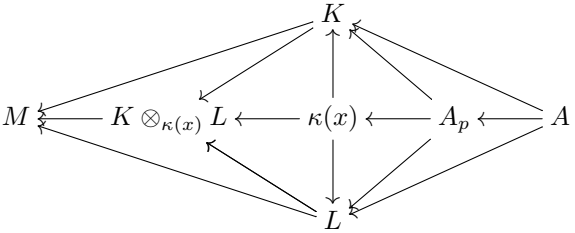
où $\bullet_{\kappa(x)}$ désigne le singleton de $\mathrm{Spec}(\kappa(x))$. Maintenant si nous avons deux morphismes qui envoient les singletons sur le même point de l'ensemble sous-jacent de X



nous voudrions identifier les morphismes $\mathrm{Spec}(K) \to X$ et $\mathrm{Spec}(L) \to X$. Or si tel est le cas nous avons $x = [p] \in Spec(A) \hookrightarrow X$ donc les deux morphismes correspondent de manière bijective fonctorielle à des morphismes :

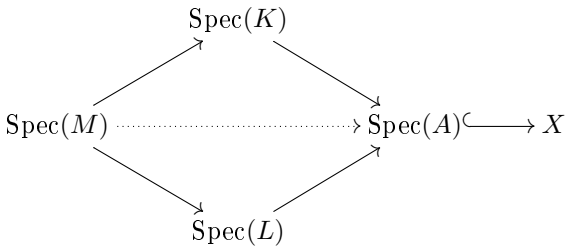


ayant même noyau p, qui se factorisent par



12. En effet nous avons forcément $\mathrm{Spec}(K)$ qui est un k-schéma donc on a un morphisme $k \to K$

Où M est un quotient du produit tensoriel par un de ses idéaux maximaux (afin d'obtenir des morphismes de corps). Ainsi nous retrouvons des factorisations



Réciproquement, toute paire de morphismes qui se factorise de cette façon envoie les points des spectres sur le même point de X.

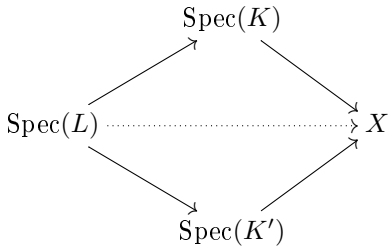
Remarque Si X est une k-varieté alors il suffit de considérer des extensions K/k finies, puisque les $\kappa(x)$ sont alors des k-algèbres de type fini. D'après le Nullstellensatz (cf. deuxième preuve) l'extension $\kappa(x)/k$ est alors finie.

Nous avons enfin :

$$|X| \simeq \{\mathrm{Spec}(K) \to X \mid K/k \text{ extension de corps}\}/\sim$$

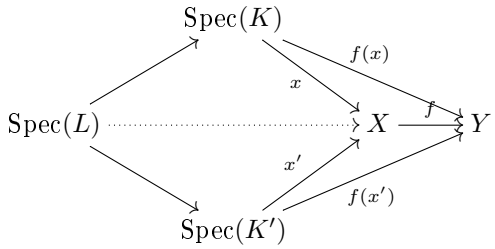
Où la relation d'équivalence est celle mise en évidence plus haut [13] :

$$\mathrm{Spec}(K) \to X \quad \sim \quad \mathrm{Spec}(K') \to X \quad \text{ssi} \quad \exists L \text{ extension de } K, K' \text{ telle que}$$



soit commutatif.

Maintenant pour $(f, f^\#)$ morphisme d'espaces annelés, nous pouvons se demander comment agit sur ces classes d'équivalence ; en fait la post-composition (toujours covariante ! ! !) des morphismes $\mathrm{Spec}(K) \to X$ est compatible avec $\sim$ comme le montre le diagramme commutatif suivant :



3.4 Morphismes surjectifs

Nous pouvons alors caractériser les morphismes que nous appelons surjectifs. Nous abrégeons $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(K)$ par $X \otimes_k K$.

Propriété *Soit $(f, f^\#) : (X, O_X) \longrightarrow (Y, O_Y)$ morphisme de k-schémas. Alors f est surjectif ssi*

$$\forall K/k \text{ extension de corps}, \forall v \in Y(K), \quad \exists N/K,\ u \in X(N) \text{ tels que } f \circ u = \text{image de } v \text{ dans } Y(N)$$

13. Le montrer c'est juste rébarbatif, la transitivité étant juste la mise en place d'un argument de composition de corps comme plus haut.

Démonstration
En prenant la définition des points de $|X|$ comme morphismes, nous voyons clairement que la condition énoncée est suffisante : Soit $\mathrm{Spec}(K) \xrightarrow{v} Y$ le représentant d'un point $y \in |Y|$. Par hypothèse nous avons donc un morphisme $\mathrm{Spec}(L) \xrightarrow{u} X$ où L/K est une extension de corps, et tel que

$$\begin{array}{ccc} \mathrm{Spec}(K) & \xrightarrow{v} & Y \\ \uparrow & \nearrow & \uparrow f \\ \mathrm{Spec}(L) & \xrightarrow[u]{} & X \end{array}$$

soit commutatif. La classe x de $\mathrm{Spec}(L) \xrightarrow{u} X$ convient comme pré-immage de y. Remarquons au passage que la fléche diagonale c'est l'image de y dans $Y(L)$.

Pour la réciproque, nous utilisons un argument de composition d'extensions. Pour $v \in Y(K)$, K/k extension, on a $y \in |Y|$ sa classed'équivalence. Alors par hypothèse nous avons $x \in |X|$ tel que $y = f(x)$.
Si $u : \mathrm{Spec}(L) \to X \quad \in X(L)$ est un représentant de x, nous avons :

$$\begin{array}{ccc} \mathrm{Spec}(K) & \xrightarrow{v} & Y \\ & & \uparrow f \\ \mathrm{Spec}(L) & \xrightarrow[u]{} & X \end{array}$$

Alors pour une extension commune N, de K et de L (par exemple $K \otimes_k L$ quotienté par un idéal maximal), nous avons

$$\begin{array}{ccccc} \mathrm{Spec}(K) & & \xrightarrow{\quad v \quad} & & Y \\ \uparrow & & & & \uparrow f \\ \mathrm{Spec}(N) & \longrightarrow & \mathrm{Spec}(L) & \xrightarrow[u]{} & X \end{array}$$

Nous avons alors $\tilde{u} : \mathrm{Spec}(N) \to X \quad \in X(N)$ qui convient. □

Remarque Pour qu'un morphisme $X \xrightarrow{\phi} Y$ soit surjectif, il suffit que $X(K) \xrightarrow{\phi(K)} Y(K)$ soit sujectif pour toute extension K/k. Bien sûr, cen'est pas une condition nécéssaire.

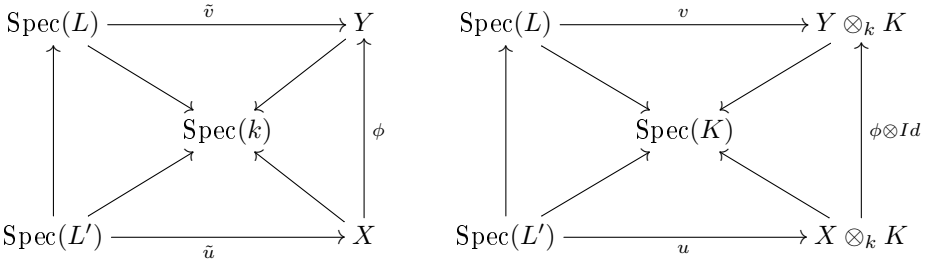
Ce bel résultat nous permet de montrer que les morphismes surjectifs passés au produit tensoriel restent surjectifs. Par produit tensoriel nous entendons pour un k-schéma X le produit fibré par un schéma affine. Si nous avons $X \xrightarrow{\phi} Y$ morphisme de k-schéma, nous pouvons le passer au produit tensoriel et obtenir $X \otimes_k K \xrightarrow{\phi \otimes Id} Y \otimes_k K$, morphisme de K-schéma :

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ \uparrow & & \uparrow \\ X \otimes_k K & \overset{\phi \otimes Id}{\cdots\cdots\rightarrow} & Y \otimes_k K \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & = & \mathrm{Spec}(K) \end{array}$$

où les morphismes vérticaux sont les projections canoniques du produit fibré. Nous allons donc avoir le théorème suivant :

Théorème *Si $X \xrightarrow{\phi} Y$ est surjectif alors pour toute extension K/k on a $X \otimes_k K \xrightarrow{\phi \otimes Id} Y \otimes_k K$ surjectif*

Démonstration
On utilise la caractérisation démontrée plus haut (sans blague), donc nous nous munissons de $v \in (Y \otimes_k K)(L)_K$ pour une extension L/K, qui correspond de manière bijective à $\tilde{v} \in Y(L)_k$ de par le dernier théorème de la séction 3.1. On a donc par hypothèse, un $\tilde{u} \in X(L')$ qui par ϕ correspond à l'image de $\tilde{v}$ dans $Y(L')$, avec L' extension de L. Il correspond bijectivement à $u \in (X \otimes_k K)(L)_K$,pré-image de v ; on peut le résumer avec les diagrammes isomorphes :



Remarquons enfin que si L' n'était pas une extension de L alors retrouver u n'aurait pas été possible à priori puisque nous aurions besoin de nous assurer que L' soit une extension de K. □

Remarque Le théorème n'a pas d'analogue avec ϕ injectif. En effet prenons l'injection des anneaux $\mathbb{R} \hookrightarrow \mathbb{C}$ qui donne donc l'injection $\phi : X = \mathrm{Spec}(\mathbb{R}) \to \mathrm{Spec}(\mathbb{C}) = Y$. En effet les deux schémas affines ont un point chacun. Si nous prenons $K = \mathbb{C}$ nous avons alors $X \otimes K = \mathrm{Spec}(\mathbb{C}) \times_{\mathbb{R}} \mathrm{Spec}(\mathbb{C})$ et $Y \otimes K = \mathrm{Spec}(\mathbb{C})$, ainsi $\phi \otimes \mathrm{Id}$ ne peut pas être injective.

4 Schémas de type fini et variétés

4.1 Les objets

Commençons par définir ce que nous entendons par "type fini" :

Définition *Un* ***k-schéma de type fini*** *est un k-schéma (X, O_X) tel que :*
- *l'espace topologique* X *est quasi-compact*
- *on peut trouver un recouvrement $(U_i)_{i \in I}$ (fini du coup) tel que*

$$\forall i \in I,\ (U_i, O_X|_{U_i}) \simeq (Spec(A_i), O_{Spec(A_i)}))$$

où les A_i sont des k-algèbres de type fini.

Nous pouvons nous demander comment retrouver une variété au sens classique avec le langage des schémas. Les **variétés affines sur** k sont des schémas affines X associés à des anneaux A qui sont des algèbres réduites, de type fini sur un corps algébriquement clos k. Réciproquement, à une variété algébrique affine au sens classique V, nous pouvons associer la variété au sens moderne $\mathrm{Spec}(\Gamma(V))$. Une **variété algébrique sur** k est un schéma qui admet un recouvrement fini par des ouverts isomorphes à des schémas affines. Une **variété de Serre** et une variété admettant un recouvrement fini par des variétés algébriques affines.

Remarque Si nous considérons les ensembles sous-jacents nous observons que le spectre premier contient bien plus de points que notre variété classique V. En fait ces points supplémentaires correspondent aux **points génériques** qui engendrent toutes les sous-variétés de V. Nous pouvons, grâce au Nullstellensatz de Hilbert, montrer qu'en fait les variétés correspondent, point par point, au **spectre maximal** $\mathrm{Spm}(A)$ de l'anneau considéré A.

Dans le cas affine $A \simeq \frac{k[X_1,\ldots,X_n]}{(P_1,\ldots,P_m)}$, et l'idéal $I = (P_1, \ldots, P_m)$ est réduit par hypothèse. À l'origine nous avions défini une variété X comme l'ensemble des solutions à un système d'équations $P_1, \ldots, P_m$, dans k^n. Alors l'idéal I caractérise notre variété, chose que nous pouvons démontrer grâce au Nullstellensatz. Quand nous avons fait les schémas nous avons vu ce que nous appellons les points rationnels. En fait on a les ismorphismes fonctoriels :

$$\begin{aligned} X(k) &= \{x \in |X|;\ \kappa(x) = k\} \\ &= \mathrm{Hom}_{\text{k-schéma}}(\mathrm{Spec}(k), X) \\ &= \mathrm{Hom}_{\text{k-algèbre}}(A, k) \\ &= \{a = (a_1, \ldots, a_n) \in k^n;\ P_j(a) = 0\ \forall j = 1, \ldots, m\} \end{aligned}$$

Ainsi, les points k-rationnels de X corréspondent exactement aux solutions de notre système d'équations. Par conséquent si k est un corps fini, alors $X(k) \subseteq k^n$ est également un ensemble fini.

Nous terminons en donnant une caractérisation des morphismes surjectifs dans notre cas particulier :

Théorème *Si* X *et* Y *sont des k-schémas de type fini, avec* $\overline{k} = k$*, alors :*
$X \xrightarrow{\phi} Y$ *est surjectif, ssi* $X(k) \xrightarrow{\phi(k)} Y(k)$ *est surjectif.*

Ceci fait partie entre autres de la démonstration du théorème d'Ax-Grothendieck.

4.2 Les points rationnels

Maintenant, nous supposons que X_1 est un k_1-schéma de type fini. Ces objets ont des propriétés particulières qui permettent entre-autre de mieux comprendre l'ensemble des points rationnels. Prenons une extension algèbrique k/k_1 [14] , et l/k_1 une sous-extension finie et notons $X = X_1 \otimes_{k_1} k$. Déjà, par le paragraphe précédent $X(k) = X_1(k)$, donc nous pouvons nous interesser juste à ce dernier. Nous pouvons injecter $X_1(l) \hookrightarrow X_1(k)$ comme nous l'avons vu dans la remarque dans la séction 3.3.1. Nous montrons une sorte d'inclusion réciproque :

$$"X_1(k) = \bigcup_{\substack{k_1 \subseteq l \subseteq k, \\ l/k_1 extension finie}} X_1(l)"$$

Soit $x^{\#} : \mathrm{Spec}(k) \to X_1$ un point k-rationnel de X_1. Nous avons sur les ensembles $\bullet \mapsto x \in U = \mathrm{Spec}(A) \subseteq X_1$. Celà se traduit sur les algèbres par un morphisme de k_1-algébres $\psi :\ A \to k$. Notons $l = Im(\psi) \subseteq k$. C'est une sous-k_1-algébre de k, de type fini (car A l'est par hypothèse). Mais les générateurs de l sont algébriques sur k_1, par hypothèse, donc l est un k_1 espace vectoriel de dimension finie. Il reste à montrerque c'est un corps : si $a \in l$ est non-nul, alors $l \xrightarrow{\times a} l$ est une application linéaire injective, donc surjective ; en particullier il existe $b \in l$ tel que $a \cdot b = 1$. Donc nous venons de montrer que l/k_1 est une extension finie et que nous pouvons représenter $x^{\#}$ par un élément de $X_1(l)$.

Nous avons en fait une très belle analogie que nous pouvons formuler rigoureusement grâce aux limites inductives :

$$\begin{aligned} k &= \varinjlim_{\substack{k_1 \subseteq l \subseteq k, \\ l/k_1 extension finie}} l \\ X(k) = X_1(k) &= \varinjlim_{\substack{k_1 \subseteq l \subseteq k, \\ l/k_1 extension finie}} X_1(l) \end{aligned}$$

4.3 Les morphismes

Nous avons à l'origine défini les morphismes de variétés comme des morphismes polynomiaux entre un k^n et un k^r restreints aux sous-ensembles correspondant à nos variétés. Maintenant avec nos schémas nous avons un morphisme $X \xrightarrow{\phi} Y$ entre schémas affines associés à des anneaux A, B. Ces anneaux sont des k-algébres de type fini qu'on peut supposer réduites :

$$A \simeq \frac{k[S_1, \ldots, S_n]}{(P_1, \ldots, P_m)} \quad et \quad B \simeq \frac{k[T_1, \ldots, T_r]}{(Q_1, \ldots, Q_s)}$$

14. Par exemple $k = \overline{k_1}$

Le morphisme ϕ est équivalent fonctoriellement à un morphisme de k-algèbres $B \xrightarrow{\psi} A$ qui peutse relèver en un morphisme polynomial $\tilde{\psi}$:

$$\begin{array}{ccc} B & \xrightarrow{\quad\psi\quad} & A \\ \uparrow & & \uparrow \\ k[T_1,\ldots,T_s] & \xrightarrow{\tilde{\psi}} & k[S_1,\ldots,S_n] \end{array}$$

Les fléches verticales représentant les projections canoniques. Se donner un morphisme entre anneaux polynomiaux revient à se donner l'image des variables du domaine (propriété universelle des morphismes d'algèbres) :

$$\tilde{\psi}(T_j) = R_j(S_1,\ldots,S_n) \quad j = 1\ldots r$$

Maintenant, si l'on transpose les équivalences du paragraphe précédent nous avons :

$$\begin{array}{ccccc} X(k) = \mathrm{Hom}_{\text{k-schéma}}(\mathrm{Spec}(k), X) = \mathrm{Hom}_{\text{k-algèbre}}(A,k) & & g & & h \\ \Big\downarrow{\scriptstyle \phi(k)} & & \Big\downarrow & & \Big\downarrow \\ Y(k) = \mathrm{Hom}_{\text{k-schéma}}(\mathrm{Spec}(k), Y) = \mathrm{Hom}_{\text{k-algèbre}}(B,k) & & \phi\circ g & & h\circ\psi \end{array}$$

où $g \in \mathrm{Hom}_{\text{k-schéma}}(\mathrm{Spec}(k), X)$ et $h \in \mathrm{Hom}_{\text{k-algèbre}}(A,k)$. Au dernier niveau d'équivalence, le point $s = (s_1,\ldots,s_n)$ qui correspond au morphisme $h : \overline{S_i} \mapsto s_i$, est envoyé sur le morphisme $h \circ \psi : \overline{T_j} \mapsto \overline{R_j} \mapsto R_j(s)$,qui correspond donc au point $R(s) = (R_1(s),\ldots,R_r(s))$. Nous retrouvons nos morphismes de variétés.

Bien évidemment, en remontant le raisonnement nous pouvons partir de l'idée classique/naïve de morphisme et retrouver un morphisme de k-schémas. En effet les polynomes R_j définis à I près donnent un morphisme $B \to A$ lui-même donnant le morphisme $X \to Y$.

4.4 Remarque sur le foncteur de points

Dans le texte sur les schémas nous avons mis en évidence une équivalence entre les points d'un k-schéma X et les morphismes $\mathrm{Spec}(K) \to X$ à une relation de congruence près, avec K/k extension de corps. En fait pour un k-schéma de type fini il suffit de considérer des extensions de type fini, puisque les corps résiduels de points sont des k-algèbres de type fini, et des corps donc ce sont des extensions finies de k (remarque déjà faite dans la séction précédente). Ceci permet de démontrer le sens indirect du théorème précédent. En effet, tout extension finie est algèbrique, donc toute extension finie K/k est triviale, $K = k$, puisque k est algébriquement clos.

5 Endomorphismes finis

Afin de mettre en perspective le théorème d'Ax-Grothendieck, de nature géométrique, nous exposons ici des résultats analogues d'algèbre. L'objectif sera de démontrer des énoncés du type :

$$A \quad \text{est de type fini et} \quad \alpha : A \longrightarrow A \quad \text{est surjectif} \quad \Rightarrow \quad \alpha \quad \text{est un isomorphisme}$$

Où A désigne une structure algèbrique particulière et le terme "type fini" nous dit que A est engendrée par un nombre fini d'éléments.

5.1 Endomorphismes surjectifs de modules de type fini : lemme de Nakayama

Nous prouvons tout d'abord le théorème de Cayley-Hamilton. Dans tout ce paragraphe, A désigne un anneau commutatif et unifère.

Théorème (Cayley-Hamilton) *Soit M un A-module fini engendré par n éléments, I un idéal de A et ϕ un endomorphisme de M. On suppose que $\phi(M) \subseteq IM$. Alors il exite un polynôme $P = X^n + a_1X^{n-1} + \ldots + a_n$ avec $a_i \in I^i$ et $P(\phi) = 0$*

Démonstration
Soient $x_1, \ldots, x_n$ les générateurs de M. Nous pouvons écrire :

$$\phi(x_1) = \sum_j a_{1,j} x_j$$
$$\ldots$$
$$\phi(x_n) = \sum_j a_{n,j} x_j$$

avec la matrice $\Delta = (a_{i,j})_{1 \leq i,j \leq n}$ à entrées dans I. Nous voyons maintenant M comme un $A[X]$-module, où X agit de manière naturelle : $X \cdot m = \phi(m)$. Notons $\mu = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$. Les relations précédentes se traduisent en

$$(XI_n - \Delta) \cdot \mu = 0$$

En multipliant par la comatrice de $XI_n - \Delta$ nous obtenons par la régle de Cramer :

$$det(XI_n - \Delta) \cdot \mu = 0$$

Le polynôme $P = det(XI_n - \Delta)$ convient. □

Nous pouvons maintenant énoncer un résultat intermédiaire :

Proposition *Supposons qu'on ait $IM = M$. Alors il existe $r \in I$ tel que $(1 - r) \cdot M = 0$.*

Démonstration
Nous appliquons le théorème de Cayley-Hamilton à Id_M. Nous obtenons donc $P = X^n + a_1 X^{n-1} + \ldots + a_n, \quad a_i \in I$ tel que $P(Id_M) = 0$. Alors $r = -(a_1 + \ldots + a_n)$ convient. □

Nous pouvons énoncer le

Lemme (Lemme de Nakayama) *Supposons M fini, $I \subseteq rad(A)$, un idéal contenu dans le radical de Jacobson de A :*
- *si $IM = M$ alors $M = 0$.*
- *si $x_1, \ldots, x_s$ ont des images qui engendrent M/IM, alors ils engendrent M.*

Démonstration
Pour le premier résultat, il suffit d'appliquer la proposition précédente et remarquer que si $r \in jac(A)$ alors $1 - r$ est une unité. Pour le second, nous posons $M' = \sum_j A \cdot x_j$ et $N = M/M'$. Nous avons $M = IM + M'$, donc $IN = N$; par le premier point nous en déduisons que $N = 0$ ouencore que $M = M'$. □

Nous arrivons au résultat principal :

Théorème *Si M est un A-module de type fini et $\alpha : M \longrightarrow M$ est un endomorphisme A-linéaire surjectif, alors c'est un isomorphisme.*

Démonstration
Nous considérons M comme un $A[X]$-module avec l'action de X définie parα ; il reste fini en tant que tel. Nous appliquons la proposition avec $I = (X)$ et en déduisons qu'il existe $P \in A[X]$ tel que $(1 - XP(X)) \cdot M = 0$. Alors $P(\alpha)$ est un inverse de α. □

5.2 Endomorphismes surjectifs d'anneaux noetheriens et d'algèbres de présentation finie

Nous rappelons qu'un **anneau noetherien** est tel que :
- tout idéal est finiment engendré OU
- toute suite croissante d'idéaux est stationnaire OU
- toute famille d'idéaux posséde un élément maximal

les trois conditions étant équivalentes.
Une **A-algèbre de présentation finie** B est une A-algèbre de type fini définie par un nombre fini de relations ; autrement dit nous disposons de $n, m \in \mathbb{N}$ et $P_1, \ldots, P_m \in A[X_1, \ldots, X_n]$ tels que

$$B \simeq \frac{A[X_1, \ldots, X_n]}{(P_1, \ldots, P_m)}$$

Nous commençons par l'énoncé concernant les anneaux noetheriens.

Théorème *Si A est noetherien et que le morphisme $\alpha : A \longrightarrow A$ est surjectif alors c'est un isomorphisme.*

Démonstration
Supposons par l'absurde que α n'est pas injectif : soit $x \in Ker(\alpha), x \neq 0$. Soit maintenant n entier naturel ; nous avons α^n surjectif donc nous disposons de $y \in A$ tel que $x = \alpha^n(y)$. Nous avons donc $\alpha^{n+1}(y) = 0$ ainsi $y \in Ker(\alpha^{n+1}) - Ker(\alpha^n)$. La suite d'idéaux $(Ker(\alpha^n))_{n \geq 0}$ n'est pas stationnaire d'où contradiction. □

Nous énonçons le théorème pour les algèbres de présentation finie. Nous allons ramener la preuve au cas précédent.

Théorème *Si $\alpha : B \longrightarrow B$ est un morphisme de A-algèbres surjectif, et si B est de présentation finie, alors α est un isomorphisme.*

Démonstration
L'idée est de relever l'application α en une application $\tilde{\alpha} : A[X, \ldots, X_n] \longrightarrow A[X, \ldots, X_n]$ et de restreindre celle-ci à des sous-anneaux noetheriens.

Posons $\pi : A[X, \ldots, X_n] \longrightarrow B = \frac{A[X_1, \ldots, X_n]}{(P_1, \ldots, P_m)}$ la projection canonique, et notons $[S]$ la classe de $S \in A[X, \ldots, X_n]$ modulo les P_j. Supposons que nous ayons $\alpha([X_i]) = [R_i]$; nous pouvons donc définir le relèvement de α par $\tilde{\alpha}(X_i) = R_i$. Par la propriété universelle des algèbres de polynômes, ceci nous donne de manière unique un morphisme de A-algèbres. Nous avons de plus $\pi \circ \tilde{\alpha} = \alpha \circ \pi$. Dire que α est surjectif, revient à dire qu'il existe Q_i tels que $\alpha([Q_i]) = [X_i]$, ou encore que nous avons $S_{i,j}$polynômes tels que :

$$\tilde{\alpha}(Q_i) = X_i + \sum_j S_{i,j} P_j$$

Nous posons alors

$$A_0 = \text{sous-anneau de } A \text{ engendré par les coéfficients des polynômes } P_j, R_i, Q_i, S_{i,j}$$

$\tilde{\alpha}$ induit par restriction un morphisme $\tilde{\alpha_0} : A_0[X_1, \ldots, X_n] \longrightarrow A_0[X_1, \ldots, X_n]$. Nous pouvons le passer au quotient par l'idéal $(P_1, \ldots, P_m)$ [15]. On note $B_0 = \frac{A_0[X_1, \ldots, X_n]}{(P_1, \ldots, P_m)}$. De par les relations précédentes, nous avons le morphisme $\alpha_0 : B_0 \longrightarrow B_0$ qui est surjectif ; c'est entre-autres un morphisme d'anneaux noetheriens : en effet A_0 est noetherien car il peut être vu comme une $\mathbb{Z}$-algèbre de type fini donc par le théorème de la base de Hilbert A_0 est noetherien, mais alors B_0 aussi. Le résultat concernant les anneaux noetheriens s'applique et alors α_0 est un isomorphisme. Comme $B = B_0 \otimes_{A_0} A$, nous avons $\alpha = \alpha_0 \otimes Id_A$, or ce dernier est un isomorphisme. □

Remarque Cette manipulation a été rendue possible parce-que nous avons incorporé à l'anneau A_0 suffisament d'éléments, tout en n'en considérant qu'un nombre fini. C'est ce type d'obsérvation qui est à la base de l'article de Serre.

15. Remarquons ici que cet idéal est à coéfficients dans A_0 et non A

5.3 Contre-exemple

Si nous enlevons l'hypothèse centrale à nos énoncés (module de type fini, anneau noetherien, algèbre de présentation finie), le résultat devient faux. Considérons la A-algèbre, A étant un anneau quelconque, $A[X_n,\ n \geq 0]$ et le morphisme f défini par $X_0 \mapsto 0$ et si $n \geq 1,\ X_n \mapsto X_{n-1}$. f est clairement surjectif mais son noyau n'est pas trivial.

6 Le théorème d'Ax-Grothendieck

Nous démontrons dans ce paragraphe le théorème suivant découvert par J. Ax et A. Grothendieck dans les années 60. Nous exposons ici seulement le cas affine, le cas général étant un peu plus complexe.

Théorème *Soit X une variété affine (ou schéma affine de type fini) définie sur k, algébriquement clos. Si un morphisme $f : X \to X$ est injectif alors il est bijectif.*

Nous allons noter $|X| = \mathrm{Spec}(A)$ avec A une k-algèbre de type fini :

$$A = \frac{k[X_1, \ldots, X_n]}{I}, \quad I = (Q_1, \ldots, Q_m)$$

6.1 Cas fini

Supposons ici $k = \overline{k_1}$ avec k_1 corps fini et qu'il existe X_1 définie sur k_1 tel que $X = X_1 \otimes_{k_1} k$. Nous pouvons construire alors k_2 extension finie de k_1 telle que f puisse induire $f_2 : X_2 \to X_2$ où $X_2 = X_1 \otimes_{k_1} k_2$, de telle sorte que $f = f_2 \otimes_{k_2} \mathrm{Id}_{Spec(k)}$.

Le morphisme f est déterminé par un morphisme $f^{\#} :\ A \to A$, lui-même caractérisé par des polynômes $P_i \in k[X_1, \ldots, X_n],\ i = 1, \ldots, n$ tels que $f^{\#}(X_i \bmod I) = P_i \bmod I$.

Il suffit de prendre k_2, l'extension finie de k_1 qui contient les coéfficients des Q_j et des P_i.

Maintenat, pour montrer que f est surjectif il suffit de montrer que f_2 l'est, or il suffit pour celà de montrer que les $f_2(l) :\ X_2(l) \to X_2(l)$ sont surjectifs pour toute extension finie l/k_2. Or les $X_2(l)$ sont des ensembles finis et les morphismes $f_2(l)$ sont injectifs donc surjectifs.

En effet nous avons $X_2(l) \hookrightarrow X_2(k) = X(k)$ qui est cohérente avec f (cf. paragraphe Schémas) :

$$\begin{array}{ccc} X(k) = X_2(k) & \xrightarrow{\quad f(k) \quad} & X(k) = X_2(k) \\ \uparrow & & \uparrow \\ X_2(l) & \xrightarrow{\quad f_2(l) \quad} & X_2(l) \end{array}$$

or $f(k)$ est injectif.

6.2 Cas infini

Supposons par l'absurde que f n'est pas surjectif. Il existe $x \in |X|$ tel que sa fibre $\mathrm{Spec}(\kappa(x)) \otimes_k X$ est vide. Or ce dernier c'est tout simplement $\mathrm{Spec}\Big(\dfrac{k[X_1, \ldots, X_n]}{(x_1 - P_1, \ldots, x_n - P_n)}\Big)$, les$x_i$ étant les coordonnées de x (cf. paragraphe sur les variétés), par conséquent nous disposons de polynômes $R_i \in k[X_1, \ldots, X_n]$ tels que

$$1 = \sum_i R_i \cdot (x_i - P_i) \qquad (*)$$

Nous pouvons alors poser Λ le sous-anneau de k engendré par les coéfficients des polynômes P_i, Q_i, R_i et les x_i. C'est une $\mathbb{Z}$-algèbre de type fini, ainsi en passant au quotient par un idéal maximal, nous obtenons un corps fini (cf. paragraphe sur les points fixes). Le morphisme induit vérifie encore $(^*)$, ainsi nous obtenons une contradiction avec le cas fini.

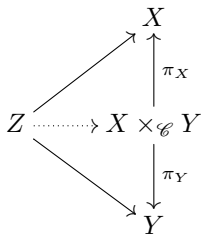
7 Schémas en groupes

7.1 Introduction

Afin de parler du premier théorème de l'article de Serre, nous avons besoin de comprendre ce que nous entendons par action du groupe G, et sutout ce que nous voulons dire par point fixe dans le langage schématique.

Commmencons par définir un objet groupe. Nous savons qu'un groupe abstrait classique, c'est juste un ensemble G, muni d'une opération $\mu : G \times G \to G$ vérifiant les propriétés d'associativité, d'élément neutre et d'inverse. Un groupe dans une catégorie $\mathscr{C}$ généralise ce concept de manière naturelle. Pour alléger les manipulations nous pouvons supposer qu'il existe dans $\mathscr{C}$ des **produits finis arbitraires** et un **objet terminal** $*$. Cela veut dire que pour toute paire d'objets X, Y dans $\mathscr{C}$ il existe une objet $X \times_{\mathscr{C}} Y$ et deux applications $\pi_X : X \times_{\mathscr{C}} Y \to X$, $\pi_Y : X \times_{\mathscr{C}} Y \to Y$ tels que :

$$\begin{aligned} \mathrm{Hom}_{\mathscr{C}}(Z, X \times_{\mathscr{C}} Y) &\longrightarrow \mathrm{Hom}_{\mathscr{C}}(Z, X) \times \mathrm{Hom}_{\mathscr{C}}(Z, Y) \\ h &\longmapsto (\pi_X \circ h, \pi_Y \circ h) \end{aligned}$$



soit une bijection. Cela veut également dire que $*$ peut être vu comme "l'objet nul" de la catégorie, de la même manière que le groupe trivial est l'objet nul de la catégorie **Grp**.

Nous abrégeons $\mathrm{Hom}_{\mathscr{C}}(Z, G)$ par $G(Z)$. Ainsi G peut être vu comme un foncteur contravariant.

Définition *Un **objet en groupe** dans une catégorie est un objet G muni d'une flèche $\mu : G \times_{\mathscr{C}} G \to G$ tel que pour tout objet Z l'application $\mu(Z) : (G \times_{\mathscr{C}} G)(Z) = G(Z) \times G(Z) \xrightarrow{\mu \circ (-)} G(Z)$ définisse une structure de groupe au sens classique, sur $G(Z)$.*

Avant de poursuivre remarquons donc qu'ici, la notion de produit n'est pas fibrée, car nous voulons obtenir une application définie sur un produit "complet" et pas un produit fibré dans le sens ensembliste.

De manière équivalente nous avons donc μ qui vérifie certaines propriétés. Nous pouvons construire une application $e : * \to G$ en prenant l'élément neutre de $G(*)$, et une application $i : G \to G$ en prenant l'inverse de $Id_G \in G(G)$. Notons au passage l'existence d'applications **injection diagonale** $\Delta : G \to G \times_{\mathscr{C}} G$ engendrées par le couple (Id_G, Id_G) et l'application **permutation des termes** $\sigma : G \times_{\mathscr{C}} G \to G \times_{\mathscr{C}} G$ engendrée par la paire (π_Y, π_X). Alors G sera un objet groupe ssi les diagrammes suivants commutent :

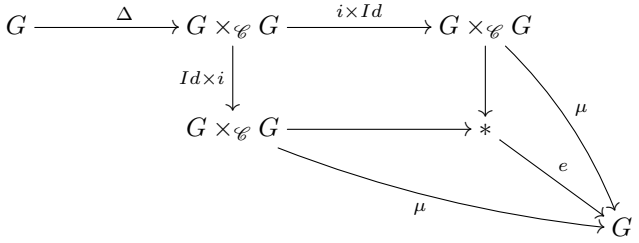
1. Associativité

$$\begin{array}{ccc} G \times_{\mathscr{C}} G \times_{\mathscr{C}} G & \xrightarrow{\mu \times Id} & G \times_{\mathscr{C}} G \\ {\scriptstyle Id \times \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times_{\mathscr{C}} G & \xrightarrow{\mu} & G \end{array}$$

2. Élément neutre

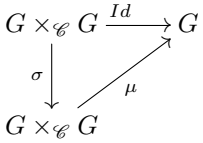
$$\begin{array}{ccc} * \times_{\mathscr{C}} G & \xrightarrow{e \times Id} & G \times_{\mathscr{C}} G \\ {\scriptstyle \sigma((-) \circ e \times Id)}\downarrow & \overset{\simeq}{\searrow}_{\mathrm{pr}_2} & \downarrow{\scriptstyle \mu} \\ G \times_{\mathscr{C}} G & \xrightarrow[\mu]{} & G \end{array}$$

3. Élément inverse



Pour montrer cette équivalence il suffitde considérer successivement $Z = G \times_{\mathscr{C}} G \times_{\mathscr{C}} G$ puis $Z = G \times_{\mathscr{C}} G$

Nous disons que l'objet groupe G est commutatif si pour tout Z le groupe classique $G(Z)$ est commutatif, ce qui revient à dire aussi que le diagramme suivant commute :

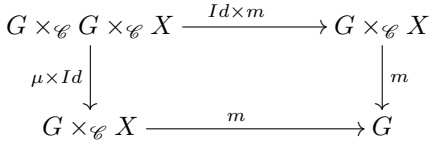


De la même façon nous pouvons définir une action d'un objet en groupe sur un autre objet d'une catégorie $\mathscr{C}$. Nous nous munissons d'abord d'un objet groupe G puis d'un objet quelconque X

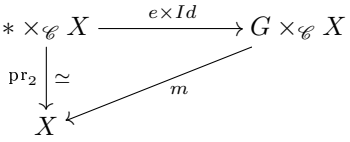
Définition *Se donner une* ***action de*** G ***sur*** X ***dans la catégorie*** $\mathscr{C}$*, c'est se donner une application* $m : G \times_{\mathscr{C}} X \to X$ *telle que pour tout objet* Z *de* $\mathscr{C}$*, nous avons* $m(Z) : G(Z) \times X(Z) \xrightarrow{m \circ (-)} X(Z)$ *qui définit une action au sens classique.*

Comme plus haut celà correspond à la commutativité de certains diagrammes :

1. Associacitivité de l'action



2. Invariance par action de l'élément neutre



Maintenant nous pouvons passer aux définitions qui nous interessent dans les catégories des schémas.

7.2 Groupes et actions dans la catégorie k-Sch

Si nous avons un groupe [16] classique G nous pouvons l'interpreter comme un schéma de la façon suivante. On note $U_g = \mathrm{Spec}(k),\ g \in G$ et nous considérons $X = \coprod_{g \in G} U_g$ sur lequel nous mettons la structure de faisceau naturelle :

X est muni canoniquement de la topologie discréte. Si $U \subseteq X$ alors on a $O_X(U) = k^{\oplus |U|}$. Plus précisément nous avons $O_X(U) = \prod_{g \in G} \delta_U(g) \cdot k$ où $\delta_U(g) \cdot k$ vaut k si $g \in U$ et 0 sinon. On fait cet effort supplémentaire pour mettre en évidence les applications de réstrictions naturelles qui apparaissent : cesont tout simplement les projection canoniques. Remarquons que c'est exactement le schéma affine de l'anneau produit $k^{\oplus |G|}$.

16. On le suppose fini pour des raisons de commodité

Nous allons noter ce schéma $\underline{G_k}$ et l'appeller **schéma groupe constant G**. Pour voir que c'est un objet groupe nous avons besoin de définir la multiplication μ. Or cela revient à définir une application

$$\underline{G_k} \times_{k-sch} \underline{G_k} \simeq \underline{G \times G_k} \longrightarrow \underline{G_k}$$

On a $\underline{G_k} \times_{k-sch} \underline{G_k}$ qui est un schéma affine associé à l'anneau $k^{\oplus|G|} \otimes_k k^{\oplus|G|} \simeq \prod_{\gamma,\gamma' \in G} k$ donc

$$\underline{G_k} \times_{k-sch} \underline{G_k} = \coprod_{\gamma,\gamma' \in G} U_{(\gamma,\gamma')} = \underline{G \times G_k} \quad \text{avec} \quad U_{(\gamma,\gamma')} = \mathrm{Spec}(k)$$

Pour définir μ il suffit de préciser où est envoyé la copie $U_{(\gamma,\gamma')}$ dans $\underline{G_k}$, mais nous l'envoyons de manière évidente dans $U_{\gamma\cdot\gamma'}$. Remarquons que celà correspond à l'application sur les anneaux :

$$\prod_{g \in G} k \longrightarrow \prod_{(\gamma,\gamma') \in G^2} k$$

$$(x_g)_g \longmapsto (y_{(\gamma\cdot\gamma')})_{(\gamma,\gamma')}$$

Maintenant nous nous munissons d'un k-schéma affine $X = \mathrm{Spec}(A)$. Définir une action consiste à se donner une application :

$$m : \underline{G_k} \times_{k-sch} X \longrightarrow X$$

qui vérifie les axiomes que l'on a vues plus haut. Nous avons donc un morphisme d'anneaux :

$$A \longrightarrow k^{\oplus|G|} \otimes A = \prod_{g \in G} A$$

$$a \longmapsto f(a) = (f_g(a))$$

Celà revient à se donner, pour tout $g \in G$ un morphisme de k-schéma $\rho_g : X \to X$, tels que $\rho_e = Id_X$, où e est l'élément neutre de G et $\rho_g \circ \rho_h = \rho_{gh}$. En fait $\rho_g^{\#} = f_g$.

7.3 Points fixes

Nous reprenons les notations du paragraphe précédent. Quand nous avons une action comme celle décrite plus haut nous pouvons nous demander à quoi peuvent correspondre les points fixes. En fait nous pouvons donnerun sens à cette phrase de deux manières différentes. Soit nous pouvons entendre par la les points fixes k-rationnels $X(k)$, soit nous pouvons nous referer à la **variété des points fixes** de l'action.

Définition C'est la sous-variété $Y = X^G$ telle que $\forall T$ S-schéma on a

$$(X^G)(T) = X(T)^G$$

Nous nous plaçons desormais dans la catégorie des schémas affines **SchAff**[17]

Proposition *Pour un schéma affine $X = Spec(A)$ et tout groupe fini, la variété des points fixes existe toujours et c'est un sous-schéma fermé.*

Démonstration
En effet soit $Y = Spec(A/I)$ la variété que nous cherchons. Par hypothèse on a $\forall g \in G,\ a \in A, \quad f_g(a) = a \bmod I$. Par conséquent

$$I \supseteq \left\langle f_g(a) - a \ ; \ {a \in A \atop g \in G} \right\rangle$$

Par maximalité nous avons donc

$$\boxed{I_{\text{fixe}} = \left\langle f_g(a) - a \ ; \ {a \in A \atop g \in G} \right\rangle}$$

17. C'est bien plus technique de montrer l'existence dans le cas général

Nous montrons que c'est l'objet recherché. Soit T un S-schéma. Les deux termes $(X^G)(T)$ et $X(T)^G$ correspondent respéctivement aux morphismes $O_T(T) \leftarrow A/I_{\text{fixe}}$ et $O_T(T) \leftarrow A$ ces derniers étant invariants par la pré-composition des morphismes $f_g^{\#}$. Ils correspondent donc aux mêmes morphismes ainsi nous retrouvons notre propriété. Remarquons au passage, qu'ils'agissait juste de représenter le foncteur $X(\bullet)^G$. Nous montrons alors de surcroît, que cette variété est unique à isomorphisme prés. □

7.4 Exemples

7.4.1 La droite affine

Nous considérons ici k algébriquement clos et n entier naturel tel que $(car(k), n) = 1$. On pose $G = \mathbb{Z}/n\mathbb{Z} = \mu_n(k)$. Nous définissons une action sur $\mathbb{A}^1_k = \text{Spec}(k[X])$:

$$f_\zeta : \ k[X] \longrightarrow k[X] \quad X \longmapsto \zeta^{-1}X$$

Nous calculons I_{fixe}. Par les calculs menés plus haut nous avons

$$I_{\text{fixe}} = \Big\langle P(\zeta X) - P(X), {}^{\zeta \in G}_{P \in k[X]} \Big\rangle$$

Mais tout $P(\zeta X) - P(X)$ est divisible par $\zeta X - X = (\zeta - 1)X$. Notons ζ_0 une racine primitive de G (existe puisque nous avons supposé $(car(k), n) = 1$). Alors notre $\zeta = \zeta_0^r$ donne $\zeta X - X$ divisible par $\zeta_0 X - X$, mais nous avons $\zeta_0 - 1 \in k^*$ ainsi

$$I_{\text{fixe}} = \langle X \rangle$$

Ainsi

$$X^G = \text{Spec}\left(\frac{k[X]}{\langle X \rangle}\right) \simeq \text{Spec}(k) \hookrightarrow X$$

nous pouvons dire qu'il n'y a qu'un seul point fixe l'origine.

Remarque Si nous considérons maintenant la droite projective $\mathbb{P}^1_k$, sur laquelle nous faisons agir G sur les deux copies de la droite affine, on obtient deux points fixes : 0 l'origine et ∞.

7.4.2 La droite projective

Nous pouvons considérer maintenant $\mathbb{A}^1_k$ plongée dans $\mathbb{P}^1_k$, elle-même "recouverte" par deux droites affines : l'une A_0 centrée en l'origine et l'autre A_∞ en ∞. $A_0 \cap A_\infty$ est isomorphe à $k\Big[X, \frac{1}{X}\Big]$ ou $k\Big[T, \frac{1}{T}\Big]$ et le changement de carte de l'une à l'autre consiste à prendre le morphisme se réduisant à $X \mapsto \frac{1}{T}$.

Nous posons $p = car(k)$ et $G = \mathbb{Z}/p\mathbb{Z} = \langle \sigma \rangle$. Nous posons B l'algébre des polynômes $k[T]$ localisée en $T+1, T+2, \ldots, T+p-1$. Ceci revient en fait à enlever l'orbite de l'origine[18]. Celà définit la variété $Y = \text{Spec}(B)$. Nous transposons l'action de translation $X \mapsto X + 1$ de A_0 sur la carte A_∞ :

$$f_\sigma : \ T \longmapsto \frac{T}{1+T}$$

Comme précédemment, nous avons

$$\begin{aligned} I_{\text{fixe}} &= \Big\langle f_\sigma(T) - T \Big\rangle \\ &= \Big\langle \frac{-T^2}{1+T} \Big\rangle \end{aligned}$$

Mais $1 + T$ est inversible dans B donc $I_{\text{fixe}} = \Big\langle T^2 \Big\rangle$ Ainsi nous avons $Y^G = \text{Spec}\Big(\frac{B}{T^2}\Big)$ or nous avons

$$\frac{B}{T^2} = \left(\frac{k[T]}{T^2}\right)\left[\frac{1}{T+1}, \ldots, \frac{1}{T+p-1}\right] = \frac{k[T]}{T^2}$$

En effet, pour $x \in \mathbb{F}_p^*$ on $(x+T)(x-T) = x^2 - T^2 = x^2$ et $x^2 \in \mathbb{F}_p^*$. Ainsi, l'action nous donne comme points fixes, le point ∞ compté deux fois.

18. Localiser revient en termes de variétés, à enlever les points annulant les polynômes en lesquels nous localisons. Nous n'avons pas besoin de localiser en T puisque nous n'avons pas besoin d'enlever l'origine 0 puisqu'elle se trouve en dehors de notre carte.

Remarque Nous voyons qu'en caractéristique non-première avec le cardinal de G nous obtenons des dégénérescences, néanmoins si nous comptons les multiplicités, nous avons toujours le même nombre de points fixes.

8 Points fixes

Le but ici est de démontrer le théorème 1.2 de l'article de Serre. On fixe p un nombre premier :

Théorème *Soit G un p-groupe fini, qui agit algébriquement sur l'espace affine $\mathbb{A}_k^n$ défini sur un corps algébriquement clos k, $car(k) \neq p$. Alors l'action a un point fixe.*

8.1 Cas fini

Nous démontrons tout d'abord le "cas fini" où $k = \overline{\mathbb{F}}_l$ avec l nombre premier différent de p. En résumé, nous avons donc l'action qui se caractérise par des morphismes polynomiaux

$$P_g = (P_{g,1}, \ldots, P_{g,n}) \quad g \in G \quad P_{g,i} \in k[X_1, \ldots, X_n]$$

Nous pouvons trouver donc une extension finie $\mathbb{F}_{l^m}$ de $\mathbb{F}_l$ qui contient tous les coéfficients de tous ces polynômes. Ils sont en nombre fini ce qui nous assure que l'extension existe. C'est entre autre ici qu'apparaît le phénomène à l'origine des résultats cités dans l'article. Nous venons donc de montrer que notre action induit une action sur $\mathbb{A}^n_{\mathbb{F}_{l^m}}$. Au passage précisons que l'action se passe vraiment sur les points de l'espace affine : c'est-à-dire $|\mathbb{A}^n_{\mathbb{F}_{l^m}}|$. Entre-autre il agit sur ses points rationnels $\mathbb{A}^n_{\mathbb{F}_{l^m}}(\mathbb{F}_{l^m}) \simeq \mathbb{F}^n_{l^m}$. Or ce dernier est un ensemble fini de cardinal premier avec p donc d'apres l'équation au classes, résultat de pure théorie des groupes, nous avons forcément une orbite réduite à un élément donc un point fixe.

Maintenant nous avons démontré qu'il existe des points k-rationnels qui sont laissés fixes par l'action de G :

$$\mathbb{A}^n(k) = \text{"} \bigcup_{m \geq 1} \mathbb{A}^n(\mathbb{F}_{l^m})\text{"}$$

donc $(\mathbb{A}^n_k)^G$ n'est pas la variété nulle, et c'est ce qu'il fallait démontrer.

8.2 Cas général

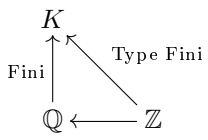
Comme avant nous avons notre action. Pour tout $g \in G$ nous avons donc $\rho_g : \mathbb{A}^n_k \longrightarrow \mathbb{A}^n_k$, ou encore des morphismes de k-algèbres $f_g : k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n]$, eux-mêmes caractérisés par les images des monômes fondamentaux : $X_i \mapsto P_{g,i}$.

Supposons maintenant que l'action n'a pas de point fixe, c'est-à-dire $(\mathbb{A}^n_k)^G = \emptyset$ [19] ou encore $I_{\text{fixe}} = k[X_1, \ldots, X_n]$. Comme $I_{\text{fixe}} = \langle (P_{g,i} - X_i),\ g, i \rangle$, il existe $Q_{g,i} \in k[X_1, \ldots, X_n]$ tels que :

$$\sum_{g,i} (P_{g,i} - X_i) Q_{g,i} = 1 \qquad (*)$$

Maintenant nous allons pouvoir réduire notre relation à un corps fini. Considérons Λ, le sous-anneau de k engendré par les coéfficients des $P_{g,i}, Q_{g,i}$. Nous allons passer auquotient par un idéal maximal $\mathfrak{m}$ et nous voulons garder un corps qui soit de caractéristique différente de p, donc nous pouvons supposer que $\frac{1}{p} \in \Lambda$.

Le corps $K = \Lambda/\mathfrak{m}$ est une $\mathbb{Z}$-algèbre de type fini, donc est de type fini sur son corps premier, mais alors par le Nullstellensatz, K est une extension finie de son corps premier. Supposons par l'absurde que K est de caractéristique nulle. Nous avons alors le diagramme d'extensions :



19. Le schéma vide existe bien : l'espace topologique est vide et au-dessus nous avons l'anneau nul.

Par le théorème d'Artin-Tate nous avons $\mathbb{Z} \longrightarrow \mathbb{Q}$ qui est de type fini, ce qui est faux. Ainsi nous avons K qui est une extension finie d'un $\mathbb{F}_l$, $l \neq p$, ainsi K est un corps fini. Nous pouvons donc réduire l'action de G à $\mathbb{A}^n_K$ et nous avons $(*)$ donc $I_{\text{fixe},K} = K[X_1, \ldots, X_n]$, ainsi nous avons contradiction avec la première partie. Nous avons donc des points fixes.

Comme le dit Terrence Tao sur son blog, ce type de démonstration utilise constamment le fait que nos objets ont des caractéristiques finies (en l'occurence un nombre fini de polynômes avec un nombre fini de coéfficients). Ensuite nous remarquons que si un énoncé n'est pas vrai en caractéristique zéro, alors celà peut s'exprimer de manière algébrique avec un nombre fini d'objets, ce qui nous permet de le réduire en caractéristique non-nulle et à fortiori aux corps finis, où l'on peut faire des raisonnements purement combinatoires.

9 Remarques sur l'algèbre Λ

Lorsque nous avons démontré notre théorème sur les points fixes, nous avons construit Λ une $\mathbb{Z}$-algébre de type fini, qui permettait de transposer nos raisonnements des corps généraux sur des corps finis. Nous ne savons pas beaucoup sur ces algèbres mais dans l'article sur lequel nous nous appuyons, il est dit que nous pouvons choisir Λ tel que $\Lambda \subset \mathbb{C}$. Cette chose n'est pas évidente et nous proposons d'abord de contourner cet argument puis d'essayer de montrer que cela est toujours possible.

9.1 Autre stratégie de démonstration

Ce que nous pouvons faire c'est de considérer les deux possibilités qui s'offrent à nous : soit k est de caractéristique nulle soit elle ne l'est pas.

9.1.1 $\mathbf{car}(k) = 0$

Nous pouvons dans ce cas précis plonger Λ dans $\mathbb{C}$.

Quitte à rajouter les inverses des entiers, nous pouvons supposer que Λ est une $\mathbb{Q}$-algèbre de type fini. Nous considérons alors $r = \deg.\mathrm{tr}_{\mathbb{Q}}(\mathrm{Frac}(\Lambda))$. En notant $K = \mathrm{Frac}(\Lambda)$, nous avons alors $t_1, \ldots, t_r \in K$ algébriquement indépendants tels que $K/\mathbb{Q}(t_1, \ldots, t_r)$ soit une extension algébrique. Or par un argument de cardinalité, nous avons $\deg.\mathrm{tr}_{\mathbb{Q}}(\mathbb{R}) = \infty$, ainsi nous pouvons plonger $\mathbb{Q}(t_1, \ldots, t_r)$ dans $\mathbb{R}$ et donc dans $\mathbb{C}$. Comme ce dernier est algébriquement clos nous pouvons l'étendre de manière unique à un plongement $\Lambda \hookrightarrow K \hookrightarrow \mathbb{C}$. Nous pouvons poursuivre nos raisonnements comme de si rien était.

9.1.2 $\mathbf{car}(k) = p > 0$

Dans ce cas nous avons alors Λ qui est une $\mathbb{F}_p$-algébre de type fini. En quotientant par un idéal maximal $\mathfrak{m}$ nous avons alors $\Lambda/\mathfrak{m}$ qui est une extension de $\mathbb{F}_p$ de type fini, donc est algébrique par le Nullstellensatz. Ainsi c'est un corps fini. Nous pouvons alors conclure nos raisonnements.

9.2 Relèvement en caractéristique 0

Pour montrer qu'un choix de Λ plongé dans $\mathbb{C}$ soit possible, nous pourrions montrer le résultat suivant :

Conjecture *Soit p un nombre premier et G un groupe fini d'ordre premier à p. Alors toute action de G sur un espace affine défini sur $\mathbb{F}_p$, ç.-à.-d. sur $\mathbb{F}_p[X_1, \ldots, X_n]$, se relève en une action sur l'espace défini sur $\mathbb{Z}_p[X_1, \ldots, X_n]$.*

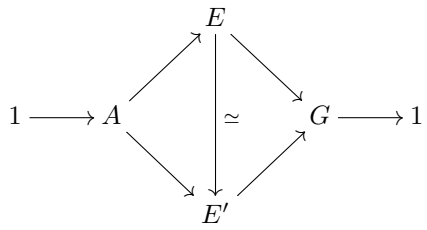
Cependant, comme nous le verrons dans la suite, ceci n'est pas encore demontré et ça reste dans l'état de conjecture. Ici il est préférable de considérer $\mathbb{Z}_p = \varprojlim_{m \geq 1} \mathbb{Z}/p^m\mathbb{Z}$

9.2.1 Extensions de groupes

Commençons par la términologie de base du problème des extensions. Nous allons desormais fixer G un groupe quelconque et A un groupe abélien. Nous disons que E est une **extension de G par A** si on peut les inscrire dans une suite exacte courte :

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

Nous disons que deux extensions E, E' sont **isomorphes** si nous pouvons trouver un diagramme commutatif :



Une fois que nous avons notre suite exacte courte il est facile de voir que G agit sur A par conjugaison : nous pouvons simplifier notre situation en supposant que $A \subseteq E$, que i désigne l'inclusion canonique et nous avons $G \simeq E/A$. Si $a \in A$ et $g \in G$ nous pouvons poser $g \cdot a = \tilde{g}a\tilde{g}^{-1}$ où $\tilde{g}$ est un relèvement de g dans E.

D'abord $g \cdot a \in A$ puisque $\pi(\tilde{g}a\tilde{g}^{-1}) = g\pi(a)g^{-1} = 1$ et l'élément ne dépends pas du relèvement de g : soit $\overline{g}$ un autre représentant de g ; on dispose de $\alpha \in A$ tel que $\overline{g} = \tilde{g}\alpha$ alors $\overline{g}a\overline{g}^{-1} = \tilde{g}\alpha a\alpha^{-1}\tilde{g}^{-1} = \tilde{g}a\tilde{g}^{-1}$ puisque A est abélien.

Desormais nous appellons tout groupe commutatif M sur lequel agit G, un G-**module** ou encore $\mathbb{Z}[G]$-module. Nous notons M^G l'ensemble des points fixes de M sous l'action de G. Les morphismes de G-modules sont les morphismes de groupes qui commutent avec l'action de G. Nous avons donc la catégorie des G-modules.

9.2.2 Cohomologie des groupes

Nous commençons par remarquer que le foncteur $(\bullet)^G$ qui va de $\mathbf{G-Mod}$ dans $\mathbf{Ab}$ est exact à gauche : Pour toute suite exacte courte (sec.)

$$1 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 1$$

nous avons une sec.

$$1 \longrightarrow M^G \longrightarrow N^G \longrightarrow P^G$$

Remarque Nous pouvons montrer que ce foncteur n'est pas exact à gauche en exhibant un contre-exemple qui nous vient de l'algèbre linéaire : soit k un corps et $G = \mathbb{Z}$ qui agit sur $N = k^2$ par la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ Maintenant posons $M = k \times 0 \subseteq N$ et $P = N/M \simeq 0 \times k$. Alors G agit trivialement sur P, M mais nous $N^G = M$.

En prenant les foncteurs dérivés à droite de $(\bullet)^G \simeq \mathrm{Hom}_{G-Mod}(\mathbb{Z}, \bullet)$, nous pouvons prolonger la suite exacte

$$1 \longrightarrow M^G \longrightarrow N^G \longrightarrow P^G$$

en une suite exacte longue

$$\begin{aligned}
&0 \longrightarrow H^0(G,M) \longrightarrow H^0(G,N) \longrightarrow H^0(G,P) \\
&\xrightarrow{\alpha^0} H^1(G,M) \longrightarrow H^1(G,N) \longrightarrow H^1(G,P) \\
&\xrightarrow{\alpha^1} H^2(G,M) \longrightarrow H^2(G,N) \longrightarrow H^2(G,P) \\
&\longrightarrow \cdots \\
&\longrightarrow H^n(G,M) \longrightarrow H^n(G,N) \longrightarrow H^n(G,P)
\end{aligned}$$

où les $H^0(G,\bullet)$ représentent en fait le foncteurs $(\bullet)^G$, et chaque H^i est un groupe abelien.

Nous pouvons maintenant énoncer nos deux théorèmes qui serviront dans la démonstration. Pour les preuves et les constructions voir [Rot09] et [Wei95].

Théorème *$H^2(G,M)$ classifie les extensions :*

$$H^2(G,M) = \{\textit{classes d'isomorphisme des extensions de } G \textit{ par } A \textit{ où } G \textit{ agit par conjugaison}\}$$

De plus, l'élément neutre correspond à l'extension scindée, c'est-à-dire au produit semi-direct.

Théorème *Lorsque G est fini, son cardinal annule tous les $H^i(G,M)$ pour tout $i \geq 1$.*

9.2.3 Démonstration

Ici nous allons nous servir d'un lemme que nous démontrons dans le paragraphe sur les endomorphismes surjectifs :

Lemme *Tout endomorphisme surjectif d'anneau noetherien est un isomorphisme*

Maintenant, ce que nous voulons faire, c'est relever par récurrence un automorphisme de $\mathbb{Z}/p^i[X_1,\dots,X_n]$ à un automorphisme de $\mathbb{Z}/p^{i+1}[X_1,\dots,X_n]$. Notons $I = p^i\mathbb{Z}/p^{i+1}[X_1,\dots,X_n] \simeq \mathbb{F}_p[X_1,\dots,X_n]$ le noyau du morphisme canonique $\mathbb{Z}/p^{i+1}[X_1,\dots,X_n] \to \mathbb{Z}/p^i[X_1,\dots,X_n]$. Nous remarquons que $I^2 = 0$. C'est dans ce cadre que nous énonçons alors un lemmme qui se rapproche du lemme de Nakayama :

Lemme *Soit A un anneau noetherien et I un idéal de A tel que $I^2 = 0$ et $A_0 = A/I$. Soit f_0 un automorphisme de $A_0[X_1,\dots,X_n]$ et $P_j = f_0(X_j)$. N'importe quel choix de $Q_j \in A[X_1,\dots,X_n]$ qui relève les P_j détermine un automorphisme f de $A[X_1,\dots,X_n]$ vérifiant $f(X_j) = Q_j$.*

Démonstration
En appliquant le premier lemme, nous voyons qu'il suffit de montrer que f est surjectif. Posons $M = \mathrm{Coker}(f) = A[X_1,\dots,X_n]/\mathrm{Im}(f)$. Mais nous avons $\bullet \bmod I = \bullet \otimes_A A_0$ qui est exact à droite et on a

$$M/I\cdot M = M \otimes_A A_0 = \mathrm{Coker}(f \otimes \mathrm{Id}_{A_0}) = \mathrm{Coker}(f_0) = 0$$

Ainsi $M = I\cdot M = I^2 \cdot M = 0$ □

Nous nous retrouvons donc avec une suite exacte

$$1 \longrightarrow I^n \longrightarrow \mathrm{Aut}_A(A[X_1,\dots,X_n]) \longrightarrow \mathrm{Aut}_{A_0}(A_0[X_1,\dots,X_n]) \longrightarrow 1$$

puisqu'un choix d'un relèvement ne dépend que du représentant des P_j modulo I.

Maintenant nous partons de l'action $G \xrightarrow{\rho} \mathrm{Aut}(\mathbb{F}[X_1,\dots,X_n])$, que nous relevons par récurrence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I^n & \longrightarrow & \mathrm{Aut}_{\mathbb{Z}/p^{i+1}}(\mathbb{Z}/p^{i+1}[X_1,\dots,X_n]) & \twoheadrightarrow & \mathrm{Aut}_{\mathbb{Z}/p^i}(\mathbb{Z}/p^i[X_1,\dots,X_n]) & \longrightarrow & 1 \\ & & & & & & \uparrow{\scriptstyle \rho} & & \\ & & & & & & G & & \end{array}$$

Nous notons alors

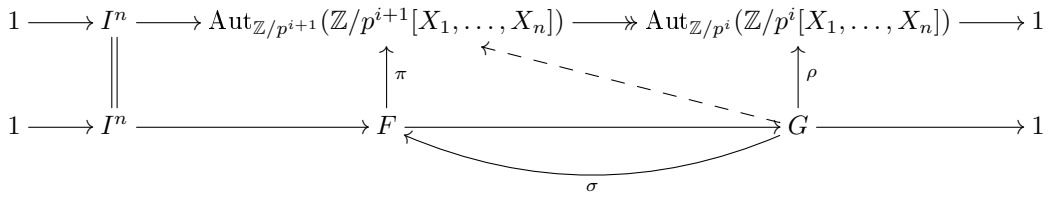
$$F = \mathrm{Aut}_{\mathbb{Z}/p^{i+1}}(\mathbb{Z}/p^{i+1}[X_1,\dots,X_n]) \times_{\mathrm{Aut}_{\mathbb{Z}/p^i}(\mathbb{Z}/p^i[X_1,\dots,X_n])} G$$

le groupe produit fibré. En d'autres termes c'est tout simplement $\{(f,g)\,|\,f_0 = \rho(g)\}$. Ce n'est rien d'autre que le pull-back. Nous avons donc le diagramme suivant où les lignes sont exactes :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I^n & \longrightarrow & \mathrm{Aut}_{\mathbb{Z}/p^{i+1}}(\mathbb{Z}/p^{i+1}[X_1,\dots,X_n]) & \twoheadrightarrow & \mathrm{Aut}_{\mathbb{Z}/p^i}(\mathbb{Z}/p^i[X_1,\dots,X_n]) & \longrightarrow & 1 \\ & & \| & & \uparrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & I^n & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Cependant nous allons montrer que $H^2(G; I[X_1,\dots,X_n]^n) = 0$. En effet, $I[X_1,\dots,X_n]^n$ est un $\mathbb{F}_p$-espace vectoriel, donc par construction H^2 l'est aussi. Mais alors, H^2 est annulé par $|G|$, par le deuxième théorème admis,

et par p, qui sont premiers entre-eux. En faisant apparaître une relation de type Bezout, nous arrivons donc à montrer que F est isomorphe au produit semi-direct $I[X_1,\dots,X_n]^n \rtimes G$. En d'autres termes, la suite exacte du ba est scindée par σ ce qui permet de définir l'action $G \xrightarrow{\pi\circ\sigma} \mathrm{Aut}_{\mathbb{Z}/p^{i+1}}(\mathbb{Z}/p^{i+1}[X_1,\dots,X_n])$:



Ceci permet de passer l'action à la limite. $\varprojlim_{i\geq 1} \mathrm{Aut}_{\mathbb{Z}/p^i}(\mathbb{Z}/p^i[X_1,\dots,X_n])$

Néanmoins il est faux que ce groupe soit isomorphe à $\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{Z}_p[X_1,\dots,X_n])$ pour les mêmes raisons que $\varprojlim_{i\geq 1} \mathbb{Z}/p^i[X_1,\dots,X_n]$ n'est pas isomorphe à $\mathbb{Z}_p[X_1,\dots,X_n]$. Il n'est pas évident de conclure en l'existence d'une action relevée sur l'anneau des p-adiques.

Nous pouvons en fait relier ce problème à une conjecture encore ouverte.

9.3 Lien avec le problème de linéarisation

En lien avec la question des actions de groupes, cette conjecture se pose la question suivante :

Conjecture *Est-ce que tout action de G réductif sur $\mathbb{A}^n_k$ est conjuguée à une action linéaire ?*

Expliquons les termes. Il n'est pas important de savoir ce que réductif veut dire mais il suffit de savoir qu'un groupe de cardinal premier avec la caractéristique de k est réductif. Nous savons que le groupe $\mathrm{GL}(n,k)$ agit de manière canonique sur n'importe quel espace vectoriel de dimension n. Il agit par conséquent sur $V = k\cdot X_1 \oplus \dots \oplus k\cdot X_n$ le sous-espace vectoriel de $k[X_1,\dots,X_n]$ constitué des polynômes de degré 1. Nous pouvons donc définir une action sur $k[X_1,\dots,X_n]$ tout entier en posant :

$$A \in \mathrm{GL}(n,k),\ P(X) \in k[X_1,\dots,X_n], \quad A\cdot P(X) = P(A\cdot X)$$

Le groupe linéaire agit donc sur $\mathbb{A}^n_k$. Nous disons qu'une **action est linéaire** si elle s'identifie à l'action d'un sous-groupe de $\mathrm{GL}(n,k)$.

Par **actions conjuguées** nous entendons l'existence de $\phi : \mathbb{A}^n_k \to \mathbb{A}^n_k$ telle que $\forall \rho \in G,\ \phi\rho\phi^{-1}$ soit linéaire.

Le relèvement peut en effet être construit si cet énoncé est valide. En effet nous aurions alors

$$\mathrm{GL}_{\mathbb{Z}_p}(\mathbb{Z}_p^{\oplus n}) = \varprojlim_{i\geq 1} \mathrm{GL}_{\mathbb{Z}/p^i}(\mathbb{Z}/p^{i\oplus n})$$

et vu que notre action est équivalente à une sous-action de $\mathrm{GL}_{\mathbb{F}_p}(\mathbb{F}_p^n)$, elle peut alors se relèver en les $\mathrm{GL}_{\mathbb{Z}/p^i}(\mathbb{Z}/p^{i\oplus n})$. En passant à la limite, nous obtenons l'action en caractéristique nulle. Si néanmoins nous trouvons un groupe qui ne peut pas se relèver en caractéristique nulle nous obtenons alors un contre-exemple au problème de linéarisation. Il est cependant plus probable de montrer la conjecture que d'en trouver un contre-exemple.

9.3.1 Petit mot sur l'algèbre symétrique

Nous avons choisi V comme sous-espace vectoriel de $k[X_1,\dots,X_n]$ car il l'engendre tout entier en tant qu'algèbre. Nous avons construit ce que nous appellons l'algébre symetrique de V. Nous pouvons généraliser cette construction.

Partons d'un A-module M. Nous pouvons construire son **algèbre tensorielle** :

$$T(M) = \bigoplus_{n\geq 0} M^{\otimes n}$$

C'est un A-module, mais nous pouvons le munir d'un produit de manière évidente :

$$u_1 \otimes \dots \otimes u_m \cdot v_1 \otimes \dots \otimes v_n = u_1 \otimes \dots \otimes u_m \otimes v_1 \otimes \dots \otimes v_n$$

Ce produit est bien défini[20]. Nous pouvons étendre ce produit en décomposant chaque vecteur en une somme d'éléments homogènes et effectuer les différents produits. Cette algèbre n'est pas commutative à priori doncnous la "symétrisons" et nous obtenons l'**algèbre symétrique** $Sym(M)$:

$$Sym(M) = \frac{T(M)}{\langle x \otimes y - y \otimes x \rangle}$$

Nous avons ainsi $Sym(k^2) = k[X,Y]$ car $k^2 \cong k \cdot X \oplus k \cdot Y$, alors $T(k^2) = k\{X,Y\}$ l'algèbre non-commutative de polynômes que nous symétrisons en l'algèbre des polynômes à deux variables.

Nous considérons cette construction car c'est le meilleur moyen d'associer une A-algèbre à un A-module. En effet nous avons le foncteur d'oubli de structure multiplicative :

$$\omega : \mathbf{A-algebres} \to \mathbf{A-modules}$$

et notre foncteur algèbre symétrique :

$$Sym(\bullet) : \mathbf{A-modules} \to \mathbf{A-algebres}$$

qui forment une paire de foncteurs adjoints : si B est une algèbre et M un module on a :

$$\mathrm{Hom}_{A-\mathrm{module}}(M, \omega(B)) = \mathrm{Hom}_{A-\mathrm{algèbre}}(Sym(M), B)$$

10 Conclusion

Pour conclure nous avons réussi à démontrer les énoncés qui apparaissent sous forme classique dans l'article, dans le cadre moderne. Les démonstrations omettent de préciser les arguments nécessaires contexte schématique, néanmoins ces morceaux de preuve apparaissent naturellement une fois le langage moderne maîtrisé. Nous nous sommes confronté également, de manière inattendue, à des problèmes plus difficiles, notamment lorsque nous essayions de montrer le théorème d'Ax-Grothendieck en essayant de généraliser le principe exposé dans l'article (démontrer le cas sur des corps finis puis en utilisant le Nullstellensatz, réduire à ce cas les cas généraux). Le résultat peut être facilement démontré dans le cas affine avec cette méthode néanmoins nous ne pouvons pas trouver une preuve élégante du résultat général. Nous avons de même été surpris de tomber sur une conjecture encore ouverte aujourd'hui, lorsque nous nous sommes intéressés à l'algèbre Λ. En effet, si le problème de linéarisation serait résolu, nous pourrions effectuer le relèvement en caractéristique nulle (donc un corps infini) et réussir à nous réduire à des énoncés sur des corps infinis.

Ce stage a été une très belle expérience pour moi. J'ai appris énormément de choses dans un sujet qui m'intéressait depuis longtemps. Je fus accueilli dans un institut de recherche et j'ai eu l'occasion d'observer le milieu des doctorants et des chercheurs qui y travaillaient. J'ai M. Romagny à remercier ainsi que ses élèves de thèse. Dans les conditions d'isolement j'ai appris à me servir moi-même, à exercer mon esprit critique ainsi devenant autonome, indépendant. Aujourd'hui j'ai beaucoup plus de portes ouvertes qu'au début de mon stage.

Références

[Bos13] Siegfried Bosch. *Algebraic Geometry and Commutative Algebra.* Springer, 2013.

[DD05] Adrien Douady and Régine Douady. *Algèbre et théories galoisiennes.* Cassini, 2005.

[EH00] David Eisenbud and Joe Harris. *The Geometry of Schemes.* Springer, 2000.

[Har77] Robin Hartshorne. *Algebraic Geometry.* Springer, 1977.

[HAU15] Olivier HAUTION. On finite group actions on the affine space and their fixed points. http ://arxiv.org/abs/1507.04582, 2015.

[HE11] J. Nicaise H. Esnault. Finite group actions, rational fixed points and weak neron models. *Pure Appl. Math. Q. 7, no. 4, Special Issue : In memory of Eckart Viehweg*, 2011.

[Mac78] Saunders MacLane. *Categories for the Working Mathematician.* Springer, 1978.

20. Nous le montrons grâce à la propriété universelle du produit tensoriel.

[Mat89] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1989.

[Mum99] David Mumford. *The Red Book of Varieties and Schemes*. Springer-Verlag, 1999.

[Per09] Daniel Perrin. *Géomètrie Algébrique, Une introduction*. EDP Sciences, 2009.

[Rot09] Joseph Rotman. *An introduction to Homological Algebra*. Springer, 2009.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. *Contemporary Mathematics*, 2009.

[Wei95] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1995.