Université de Rennes 1

Reconstruction des groupes algébriques à partir de leurs noyaux de Frobenius

Alice Bouillet

Mémoire de Master 2

Sous la direction de Matthieu Romagny

Avril-Juin 2020

Table des matières

Introduction

Ce mémoire est basé sur l'étude d'un article de John Brendan Sullivan intitulé *"Simply connected groups, the hyperalgebra, and Verma's conjecture"*. Un des buts de l'article qui est celui expliqué ici est de caractériser un groupe algébrique en caractéristique positive simplement connexe par ses noyaux de Frobenius. Nous allons voir ceci à l'aide d'un nouvel objet, intitulé "l'hyperalgèbre". On peut montrer que cet objet est l'analogue de l'algèbre de Lie d'un groupe en caractéristique nulle. L'intitulé exact du théorème qui nous intéresse est celui-ci :

Théorème : Soit G un k-groupe algébrique affine et connexe, où k est parfait. Alors :

$G = \mathrm{Spec}(A)$ est simplement connexe si et seulement si $u : A \to (hy(G))^0$ est un isomorphisme

Où la notation $(-)^0$ correspond au dual fini expliqué dans la première partie, et où $hy(G)$ est l'hyperalgèbre de G.

Ce mémoire est découpé en plusieurs parties. Le lecteur ayant de bonnes connaissances sur les schémas n'a pas besoin de lire la partie 2. Celui familier avec les schémas en groupes n'a pas besoin de lire la partie 3. La première partie parle de la réflexivité des algèbres et coalgèbres, elle est importante pour la suite. L'étude de l'article à proprement parler commence à la partie 5, où l'on introduit l'objet "hyperalgèbre" dont on se sert tout du long. Pour comprendre les théorèmes intéressants nous avons besoin de manipuler des quotients de schémas en groupes. Cette théorie n'étant pas triviale, les théorèmes nécessaires y sont expliqués dans la partie 4.

L'article de J.B. Sullivan montre également un autre résultat, connu sous le nom de la "conjecture de Verma" qui dit que si un groupe algébrique G est simplement connexe, alors toute représentation de l'hyperalgèbre de G provient d'une représentation du groupe. Nous n'expliquons pas cette conjecture dans ce mémoire.

Dans ce mémoire, la lettre k désignera un corps commutatif. Toutes nos algèbre sont associatives unitaires, et donc tout nos morphismes d'algèbres sont unitaires. Des préliminaires habituels d'algèbre commutatif sont nécessaires à la compréhension de la suite mais non rappelés ici. La lectrice pourra voir dans le livre de Hideyuki Matsumura, *Commutative algebra*, notamment en ce qui concerne le produit tensoriel, la platitude des modules que nous utilisons à plusieurs reprises ou encore les propriétés des anneaux réguliers.

Je tiens à remercier Mr Matthieu Romagny pour tout le suivi et le temps qu'il m'a consacré.

1 Rappels d'algèbre commutative utiles

Comme le titre de la section l'indique, nous donnons ici les définitions et résultats classiques d'algèbre commutative, utiles pour ce que l'on va étudier ensuite dans la théorie des groupes algébriques.

1.1 Le foncteur dual fini

Soient k un corps et M, N deux k-espaces vectoriels. On a toujours une application injective :

$$\phi : M^* \otimes N^* \to (M \otimes N)^*$$

$$f \otimes g \mapsto (m \otimes n \mapsto f(m)g(n)).$$

Soit C une coalgèbre sur k. On note $\Delta : C \to C \otimes C$ sa comultiplication. Comme C est k-espace vectoriel, nous pouvons considérer l'application $\phi : C^* \otimes C^* \to (C \otimes C)^*$ définie ci-dessus.

De plus, la comultiplication de C induit en dualisant un morphisme $\Delta^* : (C \otimes C)^* \to C^*$. En composant, on obtient ainsi un morphisme

$$\Delta^* \circ \Phi : C^* \otimes C^* \to C^*$$

qui en fait une algèbre.

On aimerait bien pouvoir définir de la même façon une structure de coalgèbre sur le duale d'une algèbre A, mais ce n'est pas possible de le faire de cette façon car Φ n'est en général pas un isomorphisme (sauf si, par exemple, A est de dimension finie sur k).

C'est pour cela que l'on va définir le dual fini d'une algèbre, et le munir naturellement d'une structure de coalgèbre.

1.1.1. Définition. Soit A une algèbre sur un corps k et I un idéal de A. On dit que I est **cofini** dans A si A/I est de dimension finie en tant que k-espace vectoriel.

1.1.2. Définition. Soit A une algèbre. On note A^0 l'ensemble des formes linéaires $f \in A^*$ nulles sur un idéal bilatère cofini I de A.

Nous allons étudier quelques propriétés de cet ensemble, et le munir d'une structure de coalgèbre, et ce même si A n'est pas de dimension finie. Évidemment si A est de dimension finie, alors $A^0 \simeq A^*$, donc cet ensemble est une généralisation du dual, que l'on appelle **dual fini** ou **dual de Sweedler**.

1.1.3. Proposition. *A^0 est un sous-espace vectoriel de A^*.*

Démonstration. Soient I, J deux idéaux de A cofinis et bilatères. Alors, $I \cap J$ l'est aussi : en effet, $A/(I \cap J) \simeq A/I \times A/J$.

Soient alors $f, g \in A^0$. On a $\ker(f) \cap \ker(g) \subset \ker(f+g)$ donc $f+g \in A^0$. De plus pour $\alpha \in k$, $\ker(f) \subset \ker(\alpha f)$, et donc si $f \in A^0$, alors $\alpha f \in A^0$ également. □

1.1.4. Proposition. *Soit $f : A \to B$ un morphisme d'algèbres, et I idéal bilatère cofini de B. Alors, $f^{-1}(I)$ est un idéal bilatère cofini de A.*

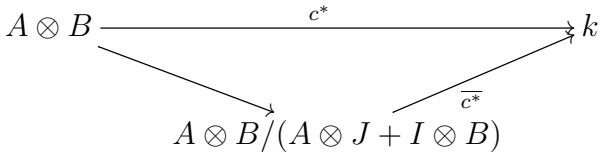
Démonstration. On regarde $A \to B/I$, dont le noyau est $f^{-1}(I)$. □

1.1.5. Lemme. *Soient A et B des algèbres sur un corps k. Soit $f \in \mathrm{Alg}(A,B)$. Alors :*
a) $f^* : B^* \to A^*$ vérifie $f^*(B^0) \subset A^0$.
b) Si on voit $A^* \otimes B^* \subset (A \otimes B)^*$, on a : $A^0 \otimes A^0 = (A \otimes A)^0$.

Démonstration. a) Soit $g \in B^0$, et $I \subset B$ un idéal cofini bilatère tel que $I \subset \ker(g)$. On a vu que $f^{-1}(I)$ était un idéal cofini de A, et il est inclu dans $\ker(g \circ f) = \ker(f^*(g))$. Ainsi $f^*(g) \in A^0$.
b) Soit K idéal cofini de $A \otimes B$. Soit $I = \{a \in A, a \otimes 1 \in K\}$. Alors I est cofini dans A car c'est l'image inverse de K par $a \mapsto a \otimes 1$. De même, $J = \{b \in B, 1 \otimes b \in K\}$ est cofini dans B. En fait, $A \otimes J + I \otimes B \subset K$ et est un idéal cofini de $A \otimes B$ car (par paltitude), c'est le noyau de :

$$A \otimes B \xrightarrow{\pi} A/I \otimes B/J$$
$$a \otimes b \mapsto \overline{a} \otimes \overline{b}.$$

Soit maintenant $c^* \in (A \otimes B)^0$ avec $A \otimes J + I \otimes B \subset K \subset \ker(c^*)$. Alors, il existe un unique $\overline{c^*}$ qui fait commuter ce diagramme :



On obtient alors que c^* se factorise avec l'isomorphisme :

$$A/I \otimes B/J \simeq A \otimes B/(A \otimes J + I \otimes B)$$

i.e. $\overline{c^*} \in (A/I \otimes B/J)^* \simeq (A/I)^* \otimes (B/J)^*$ (dimension finie).

Avec ces isomorphismes, on écrit : $\overline{c^*} = \sum_i \overline{d_i^*} \otimes \overline{e_i^*}$, avec pour tout i, $\overline{d_i^*} \in (A/I)^*$ et $\overline{c_i^*} \in (B/J)^*$. En particulier, on a pour tout $x \in A/I$, $y \in B/J$, $\overline{c^*}(x \otimes y) = \sum_i \overline{d_i^*}(x)\overline{e_i^*}(y)$.
Maintenant si on appelle $\pi_1 : A \to A/I$ et $\pi_2 : B \to B/J$, la commutativité du diagramme ci-dessus donne pour tout $a \in A$ et $b \in B$:
$c^*(a \otimes b) = \overline{c^*}(\pi_1(a) \otimes \pi_2(b)) = \sum_i \overline{d_i^*}(\pi_1(a))\overline{e_i^*}(\pi_2(b))$.
On note $d_i^* := \overline{d_i^*} \circ \pi_1$ et $e_i^* := \overline{e_i^*} \circ \pi_2$. Alors $d_i^* \in A^0$ car d_i^* s'annule sur $I = \ker(\pi_1)$. De même, $e_i^* \in B^0$. Donc, $(A \otimes B)^0 \subset A^0 \otimes B^0$.

Réciproquement, si $d^* \in A^0$ et $e^* \in B^0$, et si on note I et J les idéaux de A et B respectivements, tels que $I \subset \ker(d^*)$ et $J \subset \ker(e^*)$, alors $d^* \otimes e^*$ s'annule sur $A \otimes J + I \otimes B$ qui est cofini. D'où l'égalité. □

1.1.6. Lemme. *Soit A une algèbre sur k dont on note $M : A \otimes A \to A$ la multiplication. Alors,*

$$M^*(A^0) \subset A^0 \otimes A^0.$$

Démonstration. Soit $a^* \in A^0$ et $a, b \in A$. On a $M^*(a^*)(a \otimes b) = a^*(ab)$.

Soit I idéal bilatère cofini de A tel que $I \subset \ker(a^*)$.
Alors $A \otimes I + I \otimes A$ est un idéal cofini de $A \otimes A$, qui est inclus dans $\ker(M^*(a^*))$.

Donc $M^*(A^0) \subset (A \otimes A)^0 \simeq A^0 \otimes A^0$. □

Ainsi, on voit que l'application duale est une bonne candidate pour être une comultiplication sur cet espace vectoriel que l'on a appelé dual fini. En effet, cette application vérifie bien les axiomes voulus.

1.1.7. Corollaire. *$(A^0, M^*_{|A^0}, \epsilon)$ est une k-coalgèbre, où $\epsilon : A^0 \to k$, $a^* \mapsto a^*(1)$.*

Démonstration. Voir [SW] Chapitre VI. Proposition 6.0.2. □

On a alors montré ceci :

1.1.8. Proposition. *$A^0 = \varinjlim_I (A/I)^*$ dans la catégorie des k-coalgèbres, où la limite est prise sur tous les idéaux I bilatères et cofinis de A.*

Démonstration. En effet, c'est la limite dans la catégorie des ensembles, en considérant les inclusions. Mais comme on vient de voir que c'est également une coalgèbre, et que chaque $(A/I)^*$ est également une coalgèbre (dimension finie), c'est donc la limite de ce système dans cette catégorie. □

Maintenant que l'on a mis en place une structure sur notre dual, nous voudrions en savoir plus sur son ensemble sous-jacent.

Pour toute algèbre A, on peut considérer l'action à gauche suivante :

$$\Phi : A \times A^* \to A^*$$

$$(b, a^*) \mapsto (a \mapsto a^*(ab)).$$

1.1.9. Lemme. *Soit $f \in A^*$. Les assertions suivantes sont équivalentes :*
a) $f \in A^0$
b) $M^*(f) \in A^0 \otimes A^0$
c) $M^*(f) \in A^* \otimes A^*$
d) $\Phi(A, f)$ est un sous-espace vectoriel de dimension finie.

Démonstration. a) $\implies$ b) On a vu dans le lemme 1.1.6 l'inclusion $M^*(A^0) \subset A^0 \otimes A^0$ qui donne alors la première implication.
b) $\implies$ c) Nous utilisons simplement cette inclusion $A^0 \subset A^*$.
c) $\implies$ d) On note $M^*(f) := \sum_{i=1}^{n} a_i^* \otimes b_i^*$ où a_i^*, $b_i^* \in A^*$. soit $b \in A$. Par définition de M^*, on a :

$$f(ab) = \sum_{i=1}^{n} a_i^*(a) b_i^*(b) \ , \ \forall a \in A.$$

Alors $\Phi(b, f) = \sum_{i=1}^{n} a_i^*(.) b_i^*(b)$. Donc $\Phi(A, f) \subset \ < (a_i^*)_{i=1,\dots n} >$ où "<,>" désigne le sous-espace vectoriel engendré par les a_i^*. Ainsi, $\Phi(A, f)$ est un sous-espace vectoriel de dimension finie.
d) $\implies$ a) Soit $N = \Phi(A, f)$ sous-espace vectoriel de dimension finie.
Soit $I = \{a \in A, \Phi(a, N) = 0\} = \ker(\pi)$ où $\pi : A \to End(N)\,;\, a \mapsto (m \mapsto \Phi(a, m))$. Donc I est un idéal bilatère et cofini car $\pi(A) \subset End(N)$ de dimension finie. Maintenant, soit $a \in I$. $f(a) = (a, f)(1) = 0(1) = 0$ donc $I \subset \ker(f)$, donc $f \in A^0$. □

En particulier, nous avons montré que $a) \Leftrightarrow c)$ et donc $A^0 = (M^*)^{-1}(A^* \otimes A^*)$, où M est la multiplication de A.

1.2 Algèbre propre, faiblement réflexive, réflexive

La réflexivité va jouer un rôle important dans le résultat qui nous intéresse dans ce mémoire. A priori, le dual fini n'est en général pas un dual parfait, mais nous allons voir des particularités dans les cas qui nous intéressent.

Soit A une algèbre sur k.

1.2.1. Proposition. *Soit $j_A : A \to (A^0)^*$ l'application linéaire définie par :*
$j_A(a)(a^0) = a^0(a)$ pour $a \in A$ et $a^0 \in A^0$. Alors j_A est un morphisme d'algèbre.

Démonstration. On va remettre au propre la structure d'algèbre de A^{0*}. Elle provient de la structure de coalgèbre de A^0. On a une multiplication dans A notée M, qui donne par dualité une application de A^0 dans $A^0 \otimes A^0$. On les note :

$$\begin{array}{cc} A \otimes A \xrightarrow{M} A & A^0 \xrightarrow{M^*} (A \otimes A)^0 \\ a \otimes b \mapsto a.b & f \mapsto (a \otimes b \mapsto f(ab)) \end{array}$$

Et on a une bijection :

$$A^0 \otimes A^0 \xrightarrow{\psi} (A \otimes A)^0$$

$$f \otimes g \mapsto (a \otimes b \mapsto f(a)g(b)).$$

On définit alors :

$$\Delta : A^0 \xrightarrow{M^*} (A \otimes A)^0 \xrightarrow{\phi^{-1}} A^0 \otimes A^0$$

qui fait de A^0 une coalgèbre.
La structure d'algèbre de A^{0*} est donc définie ainsi :

$$A^{0*} \otimes A^{0*} \to A^{0*}$$

$$f \otimes g \mapsto f \times g := (a^0 \mapsto f \otimes g(\Delta(a^0)).$$

Montrons alors que le morphisme d'évaluation est un morphisme d'algèbres avec ces structures. Soient $a, b \in A$. Soit $a^0 \in A^0$. Alors $j_A(ab)(a^0) = a^0(ab)$. Calculons $(j_A(a) \times j_A(b))(a^0)$.

$$(j_A(a) \times j_A(b))(a^0) = j_A(a) \otimes j_A(b)(\Delta(a^0)) = (j_A(a) \otimes j_A(b))\,(\phi^{-1}(c \otimes d \mapsto a^0(cd)))$$

Soit alors $h \in A^0 \otimes A^0$, $h = \sum h_1 \otimes h_2$ tel que $\phi^{-1}(h) = (c \otimes d \mapsto a^0(cd))$ alors on a :
$(j_A(a) \times j_A(b))(a^0) = (j_A(a) \otimes j_A(b))(h) = \sum h_1(a)h_2(b) = \phi(h)(a \otimes b) = a^0(ab)$
Et donc $(j_A(a) \times j_A(b))(a^0) = a^0(ab)$, c'est l'égalité que l'on voulait. □

1.2.2. Définition. Soit A une algèbre. On dit que :
1) A est **propre** si j_A est injective.
2) A est **faiblement réflexive** si j_A est surjective.
3) A est **réflexive** si j_A est bijective.

1.2.3. Lemme. *Une algèbre A est propre si et seulement si pour tout $a \in A$ non nul, il existe un idéal I cofini de A tel que $a \notin I$.*

Démonstration. Supposons que A soit propre. Soit $a \in A$ non nul. Alors par définition il existe $f \in A^0$ tel que $f(a) \neq 0$. soit $I \subset \ker(f)$ idéal cofini de A. Alors $a \notin I$ et la première

implication est prouvée.
Réciproquement supposons que la deuxième condition soit vraie. Soit $a \in A$ non nul et $I \subset A$ idéal cofini de A qui ne contient pas a. Alors il existe K un sous-espace vectoriel de A tel que $I \subset A$ et $A = ka \oplus K$. On définit alors une application linéaire $f \in A^*$ par : $f(a) = 1$ et $f \equiv 0$ sur K. Alors $I \subset ker(f)$ donc $f \in A^0$ et $f(a) \neq 0$. □

1.2.4. Proposition. *Une algèbre A de type fini est toujours propre.*

Démonstration. Soit $a \in A$. On va montrer qu'il existe un idéal cofini J de A qui ne contient pas a. Soit $I = \{b \in A \ , \ ba = 0\}$. Soit M un idéal maximal contenant I. Alors il existe $n \in \mathbb{N}$ tel que $a \notin M^n$. En effet, supposons le contraire, i.e. supposons $a \in \cap_n M^n$. Alors par le théorème d'intersection de Krull, il existe $m \in M$ tel que $(m-1)a = 0$. Ainsi, $m-1 \in I \subset M$ et donc $1 \in m$. Ceci est impossible. Soit alors $n \in \mathbb{N}$ tel que $a \notin M^n$. Le lemme de Zariski nous dit que tout quotient d'une algèbre de type fini sur un corps k par un idéal maximal est une extension finie de k. Ainsi M est un idéal cofini de A, on peut alors montrer que A noethérien implique que M^n est également cofini. On a donc exhibé un idéal cofini de A qui ne contient pas a, et donc grâce au lemme précédent, on en conclu que A est propre. □

1.2.5. Remarque. On voit alors que cette proposition implique celle-ci : Tout localisé d'une algèbre de type fini est propre. En effet l'hypothèse de type fini est utilisée pour montrer que :
1) L'idéal M^n que l'on a trouvé était cofini quand M l'était, ce qui utilise seulement le fait que A soit noethérien ce qui reste vrai en localisant, et
2) Pour montrer que cet idéal M est bien cofini, on utilise le lemme de Zariski qui nous dit que A/M est un k-espace vectoriel de dimension finie, mais lorque M est maximal, on a toujours cet isomorphisme :

$$A/M \simeq S^{-1}A/S^{-1}M$$

qui nous donnera alors le même résultat pour un localisé.

On verra que ce résultat peut être utile lors des parties 5 et 6 si par exemple nous avons un groupe localement algébrique G, on pourra appliquer ce résultat à l'anneau local $\mathcal{O}(G)_e$ et on aura alors des conséquences sur l'hyperalgèbre de G.

1.2.6. Proposition. *Toute sous-algèbre d'une algèbre propre est propre.*

1.3 Coalgèbres réflexives

1.3.1. Proposition. *Soit C une coalgèbre. On définit $j_C : C \to (C^*)^*$ par $c \mapsto (c^* \mapsto c^*(c))$. Alors :*
1) j_C est injective (i.e. toute coalgèbre est propre).
2) $\mathrm{im}(j_C) \subset (C^*)^0$ *et j_C est alors un morphisme de coalgèbres.*

Démonstration. 1) Soit $c \in C$. Supposons c non nul. Puisque nous sommes sur un corps, on complète $\{c\}$ en une base de C. On peut alors prendre une application linéaire qui vaut 1 en c et 0 sur les autres éléments de la base. Ainsi, il existe toujours une application linéaire non nulle sur un élément non nul d'un espace vectoriel.
2) Soit $c^* \in C^*$ et $c \in C \subset C^{**}$. Alors, en reprenant les notations introduites au lemme 1.1.9 et en les appliquant à $A := C^*$ on a :

$$\Phi(c^*, c) = (b^* \mapsto b^*(c)c^*(c)) \subset \langle c^*(c) \rangle$$

i.e. est un espace vectoriel de dimension finie. Donc d'après que l'on a vu, $c \in C^{*0}$, ce que l'on voulait.

□

1.3.2. Définition. Soit C une coalgèbre sur k. On dit que C est **réflexive** si $j_C : C \to C^{*0}$ est bijective.

Nous énonçons maintenant un résultat important pour la suite.

1.3.3. Définition. Une algèbre sur k est dite **presque noethérienne à gauche** si tous ses idéaux à gauche cofinis sont de type fini.

1.3.4. Proposition. *Soit A une algèbre presque noethérienne à gauche. Alors A^0 est une coalgèbre réflexive.*

Démonstration. Voir [HR] Corollaire 3.3.4. □

1.3.5. Proposition. *Si $A = C^*$ est le dual d'une cogèbre, alors A est propre.*

Démonstration. Soit V un espace vectoriel. On pose pour un sous-espace vectoriel $W \subset V$, $W^\perp = \{f \in V^*,\ f(W) = 0\}$.

Si $X \subset V^*$, on pose $X^\perp = \{v \in V,\ f(v) = 0\ \forall f \in X\}$. Alors une algèbre A est propre si et seulement si $A^{0\perp} = 0$. Or si $A = C^*$, comme on a $C \subset C^{*0}$, alors $C^{*0\perp} \subset C^\perp = 0$ i.e. $A^{0\perp} = 0$. □

1.3.6. Proposition. *On a finalement défini un foncteur contravariant :*

$$\begin{aligned} \{k\text{-}algèbres\} &\longrightarrow \{k\text{-}coalgèbre\} \\ A &\longmapsto A^0 \\ (f : A \to B) &\longmapsto f^*_{|B^0} \end{aligned}$$

qui est adjoint du dual habituel :

$$\begin{aligned} \{k\text{-}coalgèbres\} &\longrightarrow \{k\text{-}algèbre\} \\ C &\longmapsto C^* \\ (f : C \to D) &\longmapsto f^* \end{aligned}$$

Démonstration. On veut montrer que pour toute algèbre A, pour toute coalgèbre C, on a une bijection

$$\mathrm{Alg}(A, C^*) \simeq \mathrm{Coalg}(C, A^0)$$

Soit alors $f : A \to C^*$. On lui associe la composée

$$C \hookrightarrow C^{*0} \xrightarrow{f^0} A^0.$$

Réciproquement, soit $g : C \to A^0$. On lui associe la composée

$$A \hookrightarrow A^{0*} \xrightarrow{g^*} C^*.$$

On vérifie que ces deux applications sont inverses l'une de l'autre. □

Dans la suite, nous travaillerons avec des algèbres de Hopf, c'est-à-dire des bialgèbres munies d'une antipode. Voici alors un résultat important lorsque l'on travaille avec des bialgèbres.

1.3.7. Proposition. *Soit A une bialgèbre sur un corps k et soit $j_A : A \to (A^0)^*$ l'application linéaire définie par $j_A(a)(a^0) = a^0(a)$ pour tout $a \in A$ et tout $a^0 \in A^0$. Alors* $\mathrm{im}(j_A) \subset A^{00}$ *et c'est un morphisme de bialgèbre.*

Démonstration. L'inclusion $i : A^0 \to A^*$ induit un morphisme de coalgèbre $i^0 : (A^*)^0 \to A^{00}$ défini par $i^0(\alpha) = \alpha \circ i = \alpha_{|A^0}$ pour tout $\alpha \in (A^*)^0$. Regardons A comme une coalgèbre. Alors $i_A : A \to (A^*)^0$, défini par $i_A(a)(a^0) = a^0(a)$ pour tout $a \in A$ et tout $a^0 \in A^0$ est un morphisme de coalgèbre. Or, $j_A = i^0 \circ i_A$, alors $\mathrm{im}(j_A) \subset A^{00}$ et j_A est aussi un morphisme de coalgèbre. □

1.3.8. Remarque. On peut imaginer dans la catégorie des algèbres de Hopf des k-groupes algébriques, l'application de bidualité des algèbres de Hopf $A \to A^{00}$ soit un isomorphisme. Mais nous n'avons pas de référence bibliographique à ce sujet pour le moment.

2 Bases sur la théorie des schémas

Cette section s'intéresse tout d'abord aux propriétés générales sur les schémas.

2.1 Changements de base, fibres d'un morphisme

Tout ce que l'on dit dans ce paragraphe est valable dans toute catégorie où les produits fibrés existent. Ici on se place dans celle des schémas que l'on note $\mathcal{C}$.

2.1.1. Définition. Un diagramme commutatif

$$\begin{array}{ccc} Z & \xrightarrow{u} & X \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow[g]{} & S \end{array}$$

est appelé **cartésien** si le morphisme canonique $Z \to X \times_S Y$ est un isomorphisme.

2.1.2. Proposition. *Le diagramme ci-dessus est cartésien si et seulement si pour tout objet T de $\mathcal{C}$, le diagramme suivant est cartésien dans la catégorie des ensembles :*

$$\begin{array}{ccc} \mathrm{Hom}(T,Z) & \xrightarrow{u(T)} & \mathrm{Hom}(T,X) \\ {\scriptstyle v(T)}\downarrow & & \downarrow{\scriptstyle f(T)} \\ \mathrm{Hom}(T,Y) & \xrightarrow[g(T)]{} & \mathrm{Hom}(T,S) \end{array}$$

Démonstration. Provient directement du lemme de Yoneda. □

2.1.3. Définition. Soient S un schéma, X et S' deux S-schémas et $f : X \to S$ et $u : S' \to S$ les morphismes structuraux. Alors $X \times_S S'$ est un S'-schéma, noté $X_{S'}$. On l'appelle **le changement de base de X par u**. Le morphisme de schéma $X \times_S S' \to S'$ est appelé le **changement de base de f par u**.

$$\begin{array}{ccc} X \times_S S' & \longrightarrow & X \\ {\scriptstyle ch(f)}\downarrow & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow[u]{} & S \end{array}$$

2.1.4. Définition. On dit qu'une propriété $(\mathcal{P})$ de morphismes schémas est **stable par changement de base** si pour tout morphisme $X \to S$ vérifiant $(\mathcal{P})$, et tout S-schéma S', le morphisme de changement de base $X \times_S S' \to S'$ vérifie $(\mathcal{P})$.

2.1.5. Proposition. *Le changement de base est transitif.*

Démonstration. En effet, Le morphisme naturel $(X \times_S S') \times_{S'} S'' \to X \times_S S''$ est un isomorphisme.

En effet, considérons ce diagramme que l'on suppose commutatif dans $\mathcal{C}$.

$$\begin{array}{ccccc} X'' & \xrightarrow{g'} & X' & \xrightarrow{g} & X \\ \downarrow & & \downarrow & & \downarrow \\ S'' & \xrightarrow[u']{} & S' & \xrightarrow[u]{} & S \end{array}$$

On suppose de plus que le carré de droite est cartésien. Alors on sait que le carré de gauche l'est si et seulement si le rectangle l'est.

On applique alors ce résultat à ce diagramme commutatif :

$$\begin{array}{ccccc} (X \times_S S') \times_{S'} S'' & \longrightarrow & X \times_S S' & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow \\ S'' & \longrightarrow & S' & \longrightarrow & S \end{array}$$

□

2.1.6. Proposition. *Soit X un schéma. Soit k un corps. Alors, se donner un morphisme de schémas de* $\mathrm{Spec}(k) \to X$ *est équivalent à se donner un point $x \in X$ et un morphisme non nul de corps $\kappa(x) \to k$.*

Démonstration. "⇒" Soit $f : \mathrm{Spec}(k) \to X$ un morphisme. Soit $x \in X$ l'image (topologique) de l'unique point de $\mathrm{Spec}(k)$. On doit maintenant trouver une injection $\kappa(x) \hookrightarrow k$. On a $f_x^{\#}; \mathcal{O}_{X,x} \to \mathcal{O}_{\mathrm{Spec}(k),0} = k$. Mais $f_x^{\#}$ est un morphisme local et donc envoie $m_{X,x}$ dans (0) et donc par propriété universelle du quotient, on obtient un morphisme : $\kappa(x) \to k$.

"⇐" Soit $x \in X$ et $\kappa(x) \hookrightarrow k$. On définit topologiquement f qui envoie (0) sur x, et pour définir le morphisme $f^{\#} : \mathcal{O}_X \to f_*\mathcal{O}_{\mathrm{Spec}(k)}$, voici comment l'on procède : Soit U un ouvert de X.

Si $x \in U$ on définit $f^{\#}(U) : \mathcal{O}_X(U) \to k$ de la manière suivante :

$$\mathcal{O}_X(U) \to \mathcal{O}_{X,x} \to \kappa(x) \to k.$$

Si $x \notin U$, c'est le morphisme nul. □

On note que pour tout $x \in X$, on a alors un morphisme de schémas $\mathrm{Spec}(\kappa(x)) \to X$, donné par $(x, \mathrm{id}_{\kappa(x)})$.

2.1.7. Proposition. *Soit $f : X \to Y$ un morphisme de schémas. Soit $y \in Y$ un point. Ensemblistement, la fibre de f en y est le sous-ensemble $f^{-1}(y)$ de X. Le produit fibré permet de munir canoniquement ce sous-ensemble d'une structure de schéma. En effet, on a un morphisme canonique* $\mathrm{Spec}(\kappa(y)) \to Y$. *Soit $X_y := X \times_Y \mathrm{Spec}(\kappa(y))$. C'est un $\kappa(y)$-schéma par la seconde projection. Alors, la projection $p : X_y \to X$ induit un homéomorphisme de X_y sur $f^{-1}(y)$.*

Démonstration. Grâce à ce diagramme commutatif,

$$\begin{array}{ccc} X \times_Y \mathrm{Spec}(\kappa(y)) & \xrightarrow{p} & X \\ \downarrow & & \downarrow f \\ \mathrm{Spec}(\kappa(y)) & \longrightarrow & Y \end{array}$$

nous avons déjà que $\mathrm{im}(p) \subset f^{-1}(y)$. Ensuite on peut raisonner localement et supposer X et Y affines, où l'homéomorphisme se prouve facilement. □

2.1.8. Définition. Le $\kappa(y)$-schéma X_y est appelé la **fibre** de f en y. Le Y-schéma X peut alors être vu comme la famille des $k(y)$-schémas X_y, lorsque y parcourt les points de Y.

Le problème avec les produits fibrés est que, en général, l'espace topologique sous-jacent du produit fibré de deux schémas n'est pas le produit fibré topologique des espaces sous-jacents. Prenons cet exemple :

2.1.9. Exemple. On a $\mathrm{Spec}(\mathbb{C}) \times_{\mathrm{Spec}(\mathbb{R})} \mathrm{Spec}(\mathbb{C}) = \mathrm{Spec}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C})$, et
$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[T]/(T^2+1) \simeq \mathbb{C}[T]/(T^2+1) \simeq \mathbb{C}[T]/(T-i) \times \mathbb{C}[T]/(T+i) \simeq \mathbb{C} \times \mathbb{C}$.
Donc topologiquement, ce produit fibré est constitué de deux points. Mais si on regarde le produit fibré des espaces topologiques sous-jacents, on obtient un singleton.

Cependant, on a ce résultat fondamental :

2.1.10. Lemme. *Soient Y et Z des X-schémas. L'application naturelle*

$$\pi : |Y \times_X Z| \to |Y| \times_{|X|} |Z|$$

est surjective.

Démonstration. Voir [DU] §5. Lemme 5.2.11.1. □

2.2 Sous-schémas

Nous allons définir deux notions de sous-schémas : les sous-schémas ouverts et fermés : la notion de sous-schéma viendra directement comme étant un sous-schéma fermé d'un sous-schéma ouvert.

2.2.1. Définition. Soit X un schéma. Un **sous-schéma ouvert** de X est un ouvert U de X, équipé de la restriction du faisceau $\mathcal{O}_X$ à U.
Une **immersion ouverte** est un morphisme de schémas $X \to Y$ qui induit un isomorphisme de X sur un sous-schéma ouvert de Y.

2.2.2. Proposition. *Pour qu'un morphisme $f : Y \to X$ soit une immersion ouverte, il faut et il suffit que f soit un homéomorphisme sur une partie ouverte de X, et que pour tout $y \in Y$, le morphisme $f^{\#}_{f(y)} : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ soit bijectif.*

Démonstration. Voir [EGA1] Chapitre I. §4. Proposition 4.2.2. □

2.2.3. Exemple. 1) Soit A un anneau et $f \in A$. Alors le morphisme de schémas
$\mathrm{Spec}(A_f) \to \mathrm{Spec}(A)$ induit par l'homomorphisme de localisation $A \to A_f$ est une immersion ouverte : en effet, c'est un isomorphisme sur l'ouvert principal $D(f)$.
2) Si $X = \mathbb{A}^1_{\mathbb{Z}/p\mathbb{Z}}$, le morphisme de Frobenius absolu $F : X \to X$, $t \mapsto t^p$ (induit par l'homomorphisme d'anneaux $\phi : t \mapsto t^p$ de $\mathbb{Z}/p\mathbb{Z}[t]$ dans lui-même) n'est pas une immersion ouverte, bien que l'application ensembliste F soit l'identité (l'image réciproque d'un idéal premier de $\mathbb{Z}/p\mathbb{Z}[t]$ par ϕ est lui-même) ; en effet ϕ n'est pas surjectif (alors que comme l'application continue sous-jacente est l'identité, si c'était une immersion ouverte, X serait isomorphe grâce à elle à X, muni de la même structure de schéma).

Regardons ce qu'il se passe dans le cas fermé :
Si $Y \hookrightarrow X$ est un fermé de l'espace topologique sous-jacent à X, alors $(Y, i^{-1}\mathcal{O}_X)$ n'est **pas** un schéma en général.

2.2.4. Contre-exemple. Soit k corps, X le k-schéma $X = \mathbb{A}^1 = \mathrm{Spec}(k[t])$. On considère $Y = \{y\} = \{(t)\}$ qui est un point fermé. Si Y est muni d'une structure de schéma, étant le seul voisinage du point y, il est nécessairement affine. Si cette structure de schéma était donnée par $i^{-1}\mathcal{O}_X$, l'anneau de fonctions de Y serait donné par $\Gamma(Y, i^{-1}O_X) = \varinjlim_{y \in U} \mathcal{O}(X \cap U) = \mathcal{O}_{X,y} = k[t]_{(t)}$. Or le spectre de ce dernier est composé de deux points d'où la contradiction.

La notion de sous-schéma fermé sera donc un peu plus subtile. La définition de sous-schéma fermé devra satisfaire la contrainte naturelle suivante : Si $X = \mathrm{Spec}(A)$, les sous-schémas fermés sont les schémas de la forme $V(I) = \mathrm{Spec}(A/I)$ avec I idéal de A. On veut que des idéaux différents donnent des sous-schémas différents (pas comme en géométrie algébrique classique).

2.2.5. Définition. Soit X un schéma. Soit $\mathcal{M}$ un $\mathcal{O}_X$-module. On appelle son **support** l'ensemble

$$Supp(\mathcal{M}) = \{x \in X, \mathcal{M}_x \neq 0\}.$$

Notation :
Soit J un idéal de $\mathcal{O}_X$, on pose

$$\begin{aligned} V(J) &= Supp(\mathcal{O}_X/J) \\ &= \{x \in X, \mathcal{O}_{X,x}/J_x \neq 0\} \\ &= \{x \in X, J_x \neq \mathcal{O}_{X,x}\} \end{aligned}$$

C'est un fermé de X.

2.2.6. Proposition. *Soit X un schéma et J un idéal de $\mathcal{O}_X$. Posons*

$$Z = Supp(^{\mathcal{O}_X}/_J)$$

$$i := Z \hookrightarrow X$$

et

$$\mathcal{O}_Z = (^{\mathcal{O}_X}/_J)_{|Z} = i^{-1}(\mathcal{O}_X/J).$$

Alors le couple $(Z, \mathcal{O}_Z)$ est un schéma si et seulement si J est quasi-cohérent.

2.2.7. Définition. Soit X un schéma. Un sous-schémas fermé de X est un schéma $(Z, \mathcal{O}_Z)$ de la forme

$$(Z, \mathcal{O}_Z) = (V(J), (^{\mathcal{O}_X}/_J)_{|V(J)})$$

où J est un idéal quasi-cohérent de $\mathcal{O}_X$.

On a un morphisme de schémas $z : Z \longrightarrow X$ défini comme suit : sur les espaces topologiques, c'est l'inclusion, sur les faisceaux d'anneaux,

$$\mathcal{O}_X \to {}^{\mathcal{O}_X}/_J = z^\star(^{\mathcal{O}_X}/_J)_{|Z} = z^\star\mathcal{O}_Z$$

Ce morphisme est appelée l'immersion fermée canonique.
Remarque : Le morphisme $\mathcal{O}_X \to z^\star\mathcal{O}_Z$ est surjectif et J est son noyau.

2.2.8. Définition. Un morphisme de schémas $i : Y \longrightarrow X$ est une immersion fermée si :

(i) i est un homéomorphisme sur un fermé de X.
(ii) le morphisme canonique

$$\mathcal{O}_X \to i^\star \mathcal{O}_Y$$

est surjectif.

2.2.9. Lemme. *Un morphisme $i : Y \longrightarrow X$ est une immersion fermée si et seulement si :*
(i) i est un homéomorphisme sur un fermé
(ii) $\forall y \in Y$, le morphisme canonique

$$i_y^\# : \mathcal{O}_{X,i(y)} \longrightarrow \mathcal{O}_{Y,y}$$

est surjectif.

2.2.10. Remarque.
Il y a une bijection entre les sous-schémas fermés de X et les idéaux quasi-cohérents de $\mathcal{O}_X$.
On peut avoir plusieurs sous-schémas fermés qui ont le même fermé sous-jacent.

Nous pouvons alors définir la notion de "sous-schéma" :

2.2.11. Définition. Soit X un schéma. On appelle **sous-schéma** de X un objet Y qui est un sous-schéma fermé d'un sous-schéma ouvert de X.

Ces définitions seront essentielles lorsque nous devrons définir un sous-groupe d'un groupe algébrique.

2.2.12. Définition. Soient X et Y deux schémas. Une **immersion** $i : Y \to X$ est un morphisme de schémas dont la fonction continue sous-jacente est un homéomorphisme de Y sur un sous-espace localement fermé de X (i.e. l'intersection d'un ouvert et d'un fermé), et tel que pour tout $y \in Y$, le morphisme d'anneaux $i_y^\# : \mathcal{O}_{X,i(y)} \to \mathcal{O}_{Y,y}$ entre les anneaux locaux est surjective.

2.2.13. Exemple. Quand Y est un sous-schéma de X, le morphisme naturel $Y \subset X$ est une immersion.

2.3 Schémas et morphismes de schémas particuliers

Souvent, on se placera dans un contexte particulier (plus agréable que le cas général) : nos schémas seront au moins localement algébriques, quelquefois algébriques ou finis. On explique ce que c'est ici :

2.3.1. Définition. On dit qu'un morphisme de schémas $f : X \to S$ est **fini** si pour tout ouvert affine $U = \mathrm{Spec}(R)$ de S, la préimage $V = f^{-1}(U)$ est un ouvert affine $V = \mathrm{Spec}(A)$ et le morphisme $R \to A$ fait de A un R-module de type fini.

2.3.2. Définition. Un k-schéma X est dit **fini** sur k si X est affine, $X = \mathrm{Spec}(A)$ avec A une k-algèbre finie sur k (ie un k-espace vectoriel de dimension finie).
Un k-schéma X est dit **algébrique** si il est de type fini sur k (i.e. le morphisme de structure est de type fini) (i.e. X est réunion finie d'ouverts affines et pour tout $U \subset X$ ouvert, $\mathcal{O}_X(U)$ est une k-algèbre de type fini).

Un k-schéma X est dit **localement algébrique** si il est localement de type fini sur k (i.e. le morphisme de structure est localement de type fini : on enlève la condition X réunion finie d'ouverts affines).

2.3.3. Remarque. Fini implique de type fini (car une k-algèbre finie est de type fini).

Ces schémas particuliers vérifient des propriétés sympathiques. Par exemple, on va montrer que :

2.3.4. Proposition. *Un k-schéma de type fini possède un nombre fini de composantes connexes.*

Pour cela, on introduit une nouvelle notion : les schémas noethériens.

2.3.5. Définition. Un schéma affine $X = \mathrm{Spec}(A)$ est dit **noethérien** si A l'est.
Un schéma est noethérien s'il est réunion finie d'ouverts affines noethériens.

2.3.6. Exemple. La droite projective $\mathbb{P}^1_k$ sur un corps k est un schéma noethérien non affine. En effet Soit $U_1 = \mathrm{Spec}(k[x])$ et $U_2 = \mathrm{Spec}(k[y])$. Soit $0 \in U_1$ le point correspondant à l'idéal maximal (x). Soit ∞ celui correspondant à l'idéal (y) dans X_2. Soit $U_{1,2} = U_{1\setminus\{0\}} = D(x) = \mathrm{Spec}(k[x, x^{-1}])$ et $U_{2,1} = U_{2\setminus\{\infty\}} = D(y) = \mathrm{Spec}(k[y, y^{-1}])$. Soit $\phi_{2,1} : U_{2,1} \to U_{1,2}$, $y \mapsto x^{-1}$. On considère X le schéma obtenu en recollant $(X_1, X_2, U_{1,2}, U_{2,1}, \phi_{2,1}, \phi_{2,1}^{-1})$. Le schéma X est appelé la **droite projective**. Il est clair que X est noethérien car $U_1 \cup U_2$ est un recouvrement de X par des ouverts affines noethériens.
Montrons maintenant que X n'est pas affine. Le théorème de recollement nous dit que $U_{1,2} \simeq U_1 \cap U_2$, et de même pour $U_{2,1}$. Regardons les sections globales de X. Se donner une section globale sur X, c'est la même chose que se donner une section s_1 sur U_1, une section s_2 sur U_2 telles que s_1 et s_2 coïncident sur $U_1 \cap U_2 = U_{1,2}$: i.e. c'est se donner un polynôme $P(x) \in k[x]$, un autre $Q(y) \in k[y]$ tels que P et Q soient égaux dans $k[x, x^{-1}]$, i.e. on veut que $P(x) = Q(x^{-1})$. La seule solution pour qu'un polynôme en x soit égal à un polynôme en x^{-1}, c'est qu'il soit constant. Ainsi, $\mathcal{O}_X(X) = k$ donc si X était affine, on aurait $X = \mathbb{P}^1_k = \mathrm{Spec}(k)$. Ceci est impossible pour une raison de cardinal.

2.3.7. Proposition. *Tout k-schéma de type fini (i.e. algébrique) est noethérien.*
En fait, on a même quelque chose de plus fort : tout schéma de type fini sur un schéma noethérien est noethérien.

Démonstration. Soit X un k-schéma de type fini. Alors X est réunion finie d'ouverts affines déterminés par des k-algèbres de type fini. Mais une k-algèbre de type fini est juste un quotient de l'anneau des polynômes à coefficient dans k à plusieurs indéterminées : c'est donc noethérien. □

2.3.8. Définition. On dit qu'un espace topologique E est **noethérien** si toute chaîne décroissante de fermés est stationnaire.

2.3.9. Définition. Soit X un schéma. On appelle **composante irréductible** de X tout sous-espace irréductible (espace non vide qui ne peut pas s'écrire comme union de deux fermés) maximal pour l'inclusion.

2.3.10. Proposition. *Un espace topologique noethérien n'a qu'un nombre fini de composantes irréductibles.*

Démonstration. Supposons qu'il existe un espace topologique noethérien X avec un nombre infini de composantes irréductible. Alors X n'est pas irréductible et $X = F_1 \cup F$ est union de deux fermés. On peut supposer F_1 non irréductible, donc union de deux fermés. On crée comme ceci une chaîne strictement décroissante de fermés : ceci est impossible. □

Il ne nous reste donc plus qu'à monter :

2.3.11. Proposition. *Un schéma noethérien possède un nombre fini de composantes connexes, celles-ci sont alors ouvertes et fermées.*

Démonstration. On note F_i les composantes irréductibles de X. Soit C une composante connexe de X. Soit $f \in C$. Soit F_i tel que $f \in F_i$. Comme F_i est connexe, $F_i \subset C$. Ainsi, C est union (finie !) de composantes irréductibles de X, il y en a donc un nombre fini. □

Donc les schémas que l'on va souvent considérer, i.e. les schémas "de type fini" ou (c'est la même chose) "algébriques" sont noethériens, et donc ne possèdent qu'un nombre fini de composantes connexes.

2.3.12. Définition. Un schéma est dit **régulier** s'il est localement noethérien (i.e. tout point possède un voisinage affine noethérien) et si tous ses anneaux locaux sont réguliers, c'est-à-dire que la dimension en tant que k-espace vectoriel de leur espace tangent de Zariski est égal à leur dimension de Krull.

Remarque : On peut montrer avec le lemme de Nakayama qu'un anneau local d'idéal maximal m est régulier si et seulement si m peut être engendré par $\dim(A)$ éléments.

2.3.13. Définition. Soit $f : X \to S$ un morphisme de schéma. f est dit **lisse** en $x \in X$ si :
a) f est **localement de présentation finie** en x, i.e ; il existe V voisinage affine de $f(x)$ et U voisinage affine de x tels que $f(U) \subset V$ et $\mathcal{O}_S(V)$ est un quotient de l'anneau des polynômes en plusieurs indéterminées à coefficients dans $\mathcal{O}_X(U)$, par un idéal de type fini.
b) f est **plat** en x : $\mathcal{O}_{X,x}$ est un $\mathcal{O}_{S,f(x)}$-module plat.
c) Pour toute extension L de $\kappa(x)$, si on note $\overline{s} := \mathrm{Spec}(L) \to S$ le point géométrique, le produit fibré $X \times_S \overline{s}$ est régulier.

On dit que X est **lisse** s'il l'est en tout point x de X.

Qu'est-ce que cela veut dire dans le cas d'un schéma algébrique sur un corps ?

2.3.14. Définition. Soit X un k-schéma de type fini. Alors X est **lisse** si :
a) $\forall x \in X, \exists V$ voisinage affine de x, $V = \mathrm{Spec}(A)$ avec $A = k[X_1, \ldots, X_n]/I$.
b) $\forall x \in X$, $O_{X,x}$ est un k-ev plat : condition vide ! (Tout module libre est plat).
c) $X_x \times_k \overline{k}$ est régulier, où on a

$$\begin{array}{ccc} X_x \times_k \overline{k} & \longrightarrow & X_x \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\overline{k}) & \longrightarrow & \mathrm{Spec}(k) \end{array}$$

et $X_x := X \times_k \mathrm{Spec}(\kappa(x))$ est la fibre de x du morphisme structural.

On va montrer une autre condition équivalente, qui se rapproche de l'idée que l'on se fait d'être "lisse".

2.3.15. Proposition. *Un k-schéma X est lisse en $x \in X$, (de dimension d), si $\exists U$ un voisinage ouvert affine de x et une immersion ouverte :*

$$j : U \hookrightarrow \mathrm{Spec}(k[T_1, \ldots, T_n]/(f_1, \ldots, f_d))$$

de k-schémas pour un certain n et des polynômes f_i, tels que la matrice jacobienne :

$$\left(\frac{\partial f_i}{\partial T_j}(x)\right)_{i,j}) \in M_{d,n}(\kappa(x))$$

a rang $n - d$. Ici, $\dfrac{\partial f_i}{\partial T_j}(x)$ est l'image de $\dfrac{\partial f_i}{\partial T_j}$ dans $\kappa(x)$ (remarque : si $\kappa(x) = k$, c'est seulement l'évaluation habituelle).

Démonstration. Voir [RO] §3. □

2.3.16. Définition. Soit X un k-schéma. On dit que X est **réduit** si $\mathcal{O}_X(U)$ est réduit pour tout ouvert U, si et seulement si $\mathcal{O}_{X,x}$ est réduit pour tout point $x \in X$.
Soit X un k-schéma. On dit que X est **géométriquement réduit** s'il l'est après changement de base à n'importe quelle extension de corps de k. En particulier, un k-schéma géométriquement réduit est réduit : en effet $X \times_k k = X$.

Nous voulons définir une notion de séparation sur nos schémas. Bien sûr, ce ne sera pas exactement la notion habituelle car si on repense au point de vue classique et que l'on se place dans la topologie de Zariski, aucune variété algébrique n'est séparée (sauf les discrètes) car la topologie de Zariski est trop grossière pour ça.
Seulement nous pouvons remarquer qu'en topologie, un espace E est séparé si et seulement si sa diagonale : $\{(x, x), x \in E\} \subset E \times E$ est fermée. Cela nous amène à cette définition :

2.3.17. Définition. Soit X , Y des schémas et $f : X \to Y$. Le morphisme canonique $\Delta_{X/Y} : X \to X \times_Y X$ est appelé **morphisme diagonal**.

Noter que le morphisme diagonal est toujours (ensemblistement) injectif par définition du produit fibré.
On dit que f est un morphisme **séparé** si $\Delta_{X/Y}$ est une immersion fermée.
Un k-schéma est dit **séparé** si le morphisme diagonal de X dans $X \times_k X$ induit par le morphisme structural sur $\mathrm{Spec}(k)$ et l'identité est une immersion fermée.
Un k-schéma qui est géométriquement réduit et séparé est une **variété algébrique**.

2.3.18. Proposition. *Tout morphisme entre deux schémas affines est séparé.*

Démonstration. On suppose $X = \mathrm{Spec}(B)$, $Y = \mathrm{Spec}(A)$. Alors un morphisme de schémas $f : X \to Y$ vient d'un homomorphisme d'anneaux $A \to B$ et par définition du produit fibré, le morphisme diagonal $\Delta : X \to X \times_Y X$ est induit par l'homomorphisme d'anneaux $\phi : B \otimes_A B \to B$, qui envoie $b \otimes b'$ sur bb'. Comme ϕ est clairement surjectif, Δ est bien une immersion fermée. □

2.3.19. Définition. Soit $X = \mathrm{Spec}(A)$ un k-schéma fini. On dit que X est **étale** sur k s'il vérifie une des conditions équivalentes suivantes :
1) A est étale en tant que k-algèbre

2) X est lisse et de dimension 0 (Ici $\dim(X) = \dim(A)$)
3) X est géométriquement réduit
4) X est une variété algébrique.

Démonstration. (De l'équivalence).
1) $\Rightarrow$ 2) Un schéma étale est lisse. Pour la dimension 0, c'est parce que un produit de corps est de dimension de Krull 0 : en effet soient A et B deux anneaux, alors
$\dim(A \times B) = \max(\dim(A), \dim(B))$ car les idéaux de $A \times B$ sont de la forme $I \times J$ avec I et J des idéaux de A et B et les idéaux premiers sont de la forme $A \times P$ ou $P \times B$.
2) $\Rightarrow$ 3) Provient du fait qu'un schéma régulier est réduit.
3) $\Rightarrow$ 4) Il faut juste montrer qu'un k-schéma est séparé : mais tout morphisme entre schémas affines est séparé.
4) $\Rightarrow$ 1) Une variété algébrique est géométriquement réduite, et donc A est étale. □

2.3.20. Exemple. Soit $X = \mathrm{Spec}(k[X]/(f))$. Alors X est étale sur k si et seulement si f est séparable.

Démonstration. On écrit $f = \prod f_i^{m_i}$ la décomposition de f en facteurs irréductibles. Alors avec le théorème chinois, $k[X]/(f) = \prod k[x]/f_i^{m_i}$. Or, $k[x]/f_i^{m_i}$ est un corps si et seulement si $m_i = 1$, et est séparable si et seulement si f_i l'est. Donc $k[X]/(f)$ étale si et seulement si f séparable. □

2.3.21. Définition. On dit qu'un morphisme de schémas $f : X \to Y$ est **quasi-compact** si, pour tout sous-ensemble ouvert quasi-compact U de Y, l'ouvert $f^{-1}(U)$ de X est quasi-compact.

3 Schémas en groupes

Maintenant, nous allons voir des propriétés spécifiques aux schémas en groupes. On en fait tout d'abords une petite présentation.

3.1 Propriétés générales

Soit $\mathcal{C}$ une catégorie possédant des produits finis.

3.1.1. Définition. Un **objet en groupes** dans $\mathcal{C}$ est un objet G de $\mathcal{C}$ que l'on voit grâce à Yoneda comme un foncteur $G : \mathcal{C}^\circ \to Sets$ avec une transformation naturelle : $\mu : G \times G \to G$ telle que, pour tout objet $S \in \mathcal{C}$,
$\mu(S) : (G \times G)(S) = G(S) \times G(S) \to G(S)$ donne une structure de groupe sur $G(S)$.

3.1.2. Proposition. *Un foncteur représentable $G : \mathcal{C} \to Sets$ est un objet en groupes si et seulement si les diagrammes suivant sont commutatifs :*
1) (Associativité) :

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mu \times \mathrm{id}} & G \times G \\ {\scriptstyle \mathrm{id} \times \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow[\mu]{} & G \end{array}$$

2) (Élément neutre). Il existe un morphisme $* \to G$ où $*$ est un objet final dans $\mathcal{C}$, tel que :

$$\begin{array}{ccccc} * \times G & \xrightarrow{e \times \mathrm{id}} & G \times G & \xleftarrow{\mathrm{id} \times e} & G \times * \\ & {\scriptstyle pr_2}\searrow & \downarrow{\scriptstyle \mu} & \swarrow{\scriptstyle pr_1} & \\ & & G & & \end{array}$$

3) (Inverse). Il existe un morphisme $i : G \to G$ qui vérifie :

$$\begin{array}{ccccc} G & \xrightarrow{(i,\mathrm{id})} & G \times G & \xleftarrow{(\mathrm{id},i)} & G \\ \downarrow & & \downarrow{\scriptstyle \mu} & & \downarrow \\ * & \xrightarrow{e} & G & \xleftarrow{e} & * \end{array}$$

Démonstration. Cela vient du lemme de Yoneda : Avec la définition ci-dessus, le foncteur G est un objet en groupes dans $\mathcal{C}$ si et seulement si ces diagrammes sont vérifiés pour tout objet $X \in \mathcal{C}$. □

3.1.3. Définition. Soit (G, μ_G) et (H, μ_H) deux objets en groupes dans une catégorie $\mathcal{C}$. Un **morphisme de groupes** de G vers H est une transformation naturelle $\phi : G \to H$ telle que

$$\phi \circ \mu_G = \mu_H \circ (\phi \times \phi).$$

Ainsi, ϕ est un morphisme de groupes si et seulement si c'est un morphisme dans la catégorie $\mathcal{C}$, et si $\phi(S) : G(S) \to H(S)$ est un morphisme de groupes pour tout objet S.

3.1.4. Définition. Le **noyau** d'un morphisme de groupes $\phi : G \to H$ est le produit fibré muni de la première projection suivant :

$$\begin{array}{ccc} G \times_H * & \longrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle \phi} \\ * & \xrightarrow[e_H]{} & H \end{array}$$

3.1.5. Définition. Dans ce mémoire, nous allons parler de **schémas en groupes** : ce sont donc des objets en groupes dans la catégorie des schémas.

3.1.6. Définition. Un **k-groupe algébrique** est un objet en groupes dans la catégorie des k-schémas algébriques (i.e. de type fini).

Dans la suite, on aura besoin de cette proposition :

3.1.7. Proposition. *Soit G un schéma en groupes sur un corps k. Alors, la section unité :*

$$e : \mathrm{Spec}(k) \to G$$

est une immersion fermée.

Donc le morphisme e sera déterminé par son idéal.

Démonstration. Soit $e : \mathrm{Spec}(k) \to G$ la section identité. Alors, l'application suivante

$$\mathrm{Spec}(k) \xrightarrow{e} G \xrightarrow{\pi} \mathrm{Spec}(k)$$

est l'identité car la section unité est une section du morphisme structural.

On appelle e_G l'élément unité de G i.e. $e_G = e((0))$.

On choisit un voisinage ouvert de $\mathrm{Spec}(A) \subset G$ contenant e_G.

Alors cette application :

$$\mathrm{Spec}(k) \xrightarrow{e} \mathrm{Spec}(A) \xrightarrow{\pi_{\mathrm{Spec}(A)}} \mathrm{Spec}(k)$$

est l'identité. Si on passe dans le monde des anneaux ; on obtient :

$$k \hookrightarrow A \xrightarrow{\tilde{e}} k$$

est l'identité.

En particulier, $\tilde{e}$ est surjective, et donc, par définition : $e((0)) = m$ où $m = \ker(\tilde{e})$ est un idéal maximal de A, i.e. un point **fermé** de $\mathrm{Spec}(A)$.

Or on a : Si X est un espace topologique et $X = \cup U_i$ est un recouvrement de X par des ouverts, alors :

$$x \in X \text{ est fermé dans } X \Leftrightarrow x \text{ fermé dans } U_i, \text{ pour tout } \ U_i \ni x$$

Donc, e induit bien un Homéomorphisme sur un fermé de G.

De plus, l'application correspondante sur les anneaux est surjective (on l'a montré juste avant).

Donc, e est bien une immersion fermée. □

3.2 Exemples

On note S un schéma de base.

Le groupe additif

Le groupe additif sur S, noté $\mathbb{G}_{a,S}$ correspond au foncteur qui à tout S-schéma T associe le groupe additif $\Gamma(T, \mathcal{O}_T)$. Pour simplifier, supposons ici $S = \mathrm{Spec}(R)$ affine. Alors $\mathbb{G}_{a,S}$ est

représenté par le S-schéma affine $\mathbb{A}^1_S = \mathrm{Spec}(R[x])$: En effet pour tout S-schéma T on a une bijection $\mathrm{Hom}_{sch}(T, \mathbb{A}^1_S) \simeq \mathrm{Hom}_{Ann}(R[x], \mathcal{O}_T(T))$ par la correspondance habituelle, et ce dernier est bien isomorphe à $\mathcal{O}_T(T)$, La structure de groupe est donnée sur les anneaux par les morphismes suivants :
$\tilde{m} : R[x] \to R[x] \otimes R[x]\,;\, x \mapsto x \otimes 1 + 1 \otimes x.$
$\tilde{i} : R[x] \to R[x]\,;\, x \mapsto -x$
$\tilde{e} : R[x] \to R\,;\, x \mapsto 0$

Le groupe multiplicatif

On le note $\mathbb{G}_{m,S}$. Il représente le foncteur qui associe à tout S-schéma T le groupe multiplicatif $\Gamma(T, \mathcal{O}_T)^*$ des éléments inversibles. Comme schéma, on a $G_{m,S} = \mathrm{Spec}(\mathcal{O}_S(S)[x, x^{-1}])$. La structure de groupe est donnée par :
$\tilde{m} : \mathcal{O}_S(S)[x, x^{-1}] \to \mathcal{O}_S(S)[x, x^{-1}] \otimes \mathcal{O}_S(S)[x, x^{-1}]\,;\, x \mapsto x \otimes x.$
$\tilde{i} : \mathcal{O}_S(S)[x, x^{-1}] \to \mathcal{O}_S(S)[x, x^{-1}]\,;\, x \mapsto x^{-1}$
$\tilde{e} : \mathcal{O}_S(S)[x, x^{-1}] \to \mathcal{O}_S\,;\, x \mapsto 1$

Les racines n-ièmes de l'unité

Soit n un entier positif. Soit S un schéma quelconque. On a S-schéma en groupes $\mu_{n,S}$ qui à chaque S-schéma T associe le sous-groupe de $\mathbb{G}_m(T)$ des éléments dont l'ordre est fini et divise n, c'est-à-dire les éléments $x \in \mathbb{G}_m(T)$ tels que $x^n = 1$. La $\mathcal{O}_S$-algèbre qui définit ce schéma en groupes est $\mathcal{O}_S(S)[x, x^{-1}]/(x^n - 1)$ avec la loi de groupe donnée comme dans le deuxième exemple. On a alors que $\mu_{n,S}$ est un *sous-groupe fermé* de $\mathbb{G}_{m,S}$. (Voir la section ci-dessous).

Supposons $S = \mathrm{Spec}(k)$. Alors le groupe des racines n-ième de l'unité est étale sur k si et seulement si $n \neq 0$ dans k. De plus, il est toujours fini.

Racines p-ièmes de 0 Soit p un nombre premier tel que $car(S) = p$. On regarde le sous-schéma fermé : $\alpha_{p^n,S} \subset \mathbb{G}_{a,S}$ défini par l'idéal $(x^{(p^n)})$ i.e. $\alpha_{p^n,S} := \mathrm{Spec}(\mathcal{O}_S(S)[x]/(x^{(p^n)})$.

Schéma en groupes constant Soit M un groupe fini abstrait noté additivement, et R un anneau. On peut considérer la R-algèbre $A := \mathrm{Hom}_{\mathrm{Ens}}(M, R)$ de toutes les applications de M dans R, dont l'addition et la multiplication sont définies points par points, et dont les neutres de l'addition et de la multiplication sont respectivement l'application nulle et l'application constante égale à 1. On définit une comultiplication de la manière suivante :

$$A \to A \otimes A \simeq \{f : M \times M \to R\}$$

$$f \mapsto ((x, y) \mapsto f(x + y))$$

On définit de même une counité comme ceci :

$$A \to R$$

$$f \mapsto f(1)$$

Enfin, on définit une antipode de la manière suivante :

$$A \to A$$

$$f \mapsto (x \mapsto f(-x))$$

Ces opérations font de A une algèbre de Hopf, et donc de $\mathrm{Spec}(A)$ un schéma en groupes sur $\mathrm{Spec}(R)$. Il est appelé le schéma en groupes constant associé à M. Ces schémas définis ainsi sont des schémas en groupes finis sur S. En effet on peut voir que l'anneau des fonctions est engendré par l'ensemble $\{\delta_g,\, g \in M\}$ où les δ_g sont définies de la façon suivante : $\delta_g(h) = 1$ si $h = g$ et $\delta_g(h) = 0$ sinon.

En fait, cette construction correspond à ce plongement

$$\{\text{Groupes abstraits finis}\} \hookrightarrow \{\text{S-schéma en groupes fini}\}$$
$$G \mapsto \coprod_{g \in G} S$$

Par exemple, le schéma en groupe $\mathbb{Z}/n\mathbb{Z}$ est défini de cette manière.

3.3 Sous-groupes

Soit G un S-schéma en groupes.

3.3.1. Définition. Un **sous-groupe** (ouvert, fermé) de G est un sous S-schéma (ouvert, fermé) H de G tel que pour tout S-schéma T, $H(T)$ soit un sous-groupe de $G(T)$.

3.3.2. Proposition. *Si G est un groupe algébrique sur un corps k, alors tout sous-groupe de G est fermé.*

Démonstration. Voir [DG] Chapitre II §5 n°5. Proposition 5.1(b). □

3.3.3. Définition. Avec les mêmes notations, un sous-groupe H de G est dit **normal** si $H(T) \triangleleft G(T)$ pour tout S-schéma T. Dans ce cas, on note $H \triangleleft G$.

3.3.4. Définition. Le **groupe dérivé** de G, noté $[G, G]$ est défini comme étant l'intersection des sous-groupes normaux N de G tels que G/N soit commutatif.

3.4 Les algèbres de Hopf : liens avec les groupes algébriques

Soit (G, μ) un groupe algébrique sur k et $A = \mathcal{O}(G)$. Par dualité, μ correspond à un morphisme $\Delta : A \to A \otimes A$. De même, les applications e et i correspondent à des morphismes de k-algèbres : $\epsilon : A \to k$ et $S : A \to A$, qui respectent ces différents diagrammes :

$$\begin{array}{ccc} A \otimes A \otimes A & \xleftarrow{\mathrm{id} \otimes \Delta} & A \otimes A \\ {\scriptstyle \Delta \otimes \mathrm{id}} \uparrow & & \uparrow {\scriptstyle \Delta} \\ A \otimes A & \xleftarrow{\Delta} & A \end{array}$$

$$\begin{array}{ccccc} A & \xleftarrow{(S,\mathrm{id})} & A \otimes A & \xrightarrow{(\mathrm{id},S)} & A \\ \uparrow & & \uparrow {\scriptstyle \Delta} & & \uparrow \\ k & \xleftarrow{\epsilon} & A & \xrightarrow{\epsilon} & k \end{array}$$

$$\begin{array}{ccccc} k \otimes A & \xleftarrow{\mathrm{id} \otimes \epsilon} & A \otimes A & \xrightarrow{\epsilon \otimes \mathrm{id}} & A \otimes k \\ & {\scriptstyle \simeq} \nwarrow & \uparrow {\scriptstyle \Delta} & \nearrow {\scriptstyle \simeq} & \\ & & A & & \end{array}$$

3.4.1. Définition. Soit R un anneau commutatif. Une paire (A, Δ) où A est une R-algèbre et $\Delta : A \to A \otimes A$ est un morphisme d'algèbres est une **algèbre de Hopf** sur R si il existe des morphismes de R-algèbres :

$$\epsilon : A \to R \ , \ S : A \to A$$

tels que les diagrammes ci-dessus commutent

$$(\mathrm{id} \circ \Delta) \circ \Delta = (\Delta \circ \mathrm{id}) \circ \Delta$$

$$(\mathrm{id}, \epsilon) \circ \Delta = \mathrm{id} = (\epsilon, \mathrm{id}) \circ \Delta$$

$$(\mathrm{id}, S) \circ \Delta = \epsilon = (S, \mathrm{id}) \circ \Delta$$

Les applications Δ, ϵ et S sont appelées respectivement comultiplication, co-identité et antipode ou inversion.

3.4.2. Définition. Un **morphisme d'algèbres de Hopf** $f : (A, \Delta_A) \to (B, \Delta_B)$ est un morphisme $f : A \to B$ de R-algèbres tel que $(f \otimes f) \circ \Delta_A = \Delta_b \circ f$.

3.4.3. Définition. Une algèbre de Hopf est dite **de type fini** si A l'est en tant qu'algèbre.

3.4.4. Proposition. *La paire (ϵ, S) est uniquement déterminée par (A, Δ).*
De plus, si $f : (A, \Delta_A) \to (B, \Delta_B)$ est un morphisme d'algèbres de Hopf, alors on a :

$$\epsilon_B \circ f = \epsilon_A$$

$$f \circ S_A = S_b \circ f$$

Démonstration. Découle des définitions. □

3.4.5. Définition. Soit A une algèbre de Hopf. On note son dual k-linéaire A^*. Ce k-espace vectoriel a également une structure multiplicative, qui en fait une algèbre, définie par :

$$A^* \times A^* \to A^* \ ; \ (f, g) \mapsto a \mapsto (f \otimes g)(\Delta(a))$$

Où $\Delta : A \to A \otimes A$ est la comultiplication de A.
Donc A^* est également une k-algèbre.

Se donner une structure d'algèbre de Hopf sur une algèbre A est la même chose que se donner une structure de groupe algébrique sur $\mathrm{Spec}(A)$.

3.4.6. Proposition. *Soit A une k-algèbre de type fini, et $\Delta : A \to A \otimes A$ morphisme d'algèbres. Soit $m : \mathrm{Spec}(A) \times \mathrm{Spec}(A) \to Spec(A)$ le morphisme de schéma correspondant. Alors,*

$$(A, \Delta) \text{ algèbre de Hopf } \Leftrightarrow (\mathrm{Spec}(A), m) \text{ groupe algébrique.}$$

Démonstration. Voir [Mil]. Chapitre 3. c) Proposition 3.6. □

4 Quotients par des sous-groupes

Le but de cette section et des prochaines est d'expliquer (sans tout démontrer) l'existence et la caractérisation d'un quotient de groupes algébriques.

4.0.1. Définition. Soit G un schéma en groupes sur une base S. Une **action à gauche** de G sur un S-schéma X est donnée par un morphisme $\rho : G \times_S X \to X$ tel que la composition :

$$X \simeq S \otimes_S X \xrightarrow{e_G \times \mathrm{id}_X} G \times_S X \xrightarrow{\rho} X$$

soit l'identité sur X, et tel que le diagramme

$$\begin{array}{ccc} G \times_S G \times_S & \xrightarrow{\mathrm{id}_G \times \rho} & G \times_S X \\ \downarrow{\scriptstyle m \times \mathrm{id}_X} & & \downarrow{\scriptstyle \rho} \\ G \times_S X & \xrightarrow{\rho} & X \end{array}$$

soit commutatif.

Autrement dit : pour tout S-schéma T, le morphisme ρ induit une action à gauche du groupe $G(T)$ sur $X(T)$. On note souvent cette action sur les points (pour chaque T) $(g, x) \mapsto g \cdot x$.

4.0.2. Exemple. Si G est un schéma en groupes au-dessus de S et $H \subset G$ est un sous-schéma en groupes, alors la loi de groupe donne une action de H sur G.

La problématique de cette sous-section est la suivante : étant donné un groupe G qui agit sur un schéma X, existe t-il une bonne notion d'espace quotient G/X ? Cela nous servirait pour décrire le conoyau d'un morphisme entre deux groupes, ou un quotient d'un groupe par un sous-groupe normal.

4.0.3. Définition. Soit $\mathcal{C}$ une catégorie. Soit $X \in ob(C)$ et $G \in ob(C)$ un objet en groupes. On suppose de plus que G agit sur X. Alors, le **quotient** de X par G, s'il existe, est un objet $Y \in ob(C)$ et un morphisme $\pi : X \to Y$ tel que :
1) π est invariant : i.e. $\pi \circ \rho = \pi \circ p_2$, où $\rho : G \times X \to X$ est l'action, et $p_2 : G \times X \to X$ est la projection.
2) π satisfait la propriété universelle suivante :
Tout morphisme $X \to Z$ qui satisfait la première condition se factorise par π.

Dans les catégories habituelles, cette définition conduit à la définition habituelle de quotient.

4.1 Topologie fppf

Nous allons regarder les schémas dans une catégorie plus grande : celle des "faisceaux fppf", et voir qu'ici les quotient existent (on prend la faisceautisation du préfaisceau quotient), et enfin donner des conditions pour que ce faisceau soit représentable par un schéma. Dans cette section, nous allons voir que tout schéma est un faisceau fppf, et alors à partir de maintenant, nous considérons tout schéma comme un faisceau fppf, c'est-à-dire que nous nous placerons systématiquement dans cette catégorie.

Nous commençons avec une définition d'un diagramme exact qui nous servira dans le théorème du quotient.

4.1.1. Définition. Un diagramme

$$A \xrightarrow{u} B \underset{v_1}{\overset{v_2}{\rightrightarrows}} C$$

d'applications d'ensembles est dit **exact** si u est injectif et si son image est formée des éléments b de B tels que $v_1(b) = v_2(b)$.
Soit $\mathcal{C}$ une catégorie. Un diagramme de ce type est dit **exact** si pour tout $X \in ob(C)$, le diagramme d'ensembles correspondant est exact.
On dit alors que u fait de A un **noyau** du couple de flèches (v_1, v_2).
De manière duale, un diagramme

$$S \underset{v_1}{\overset{v_2}{\rightrightarrows}} T \xrightarrow{u} V$$

est dit exact dans $\mathcal{C}$ s'il est exact en tant que diagramme dans la catégorie opposée C°, i.e. si pour tout objet X de $\mathcal{C}$, le diagramme d'ensembles correspondant

$$X(V) \longrightarrow X(T) \rightrightarrows X(S)$$

est exact (cela implique que u est un épimorphisme). On dit alors que u fait de S un **conoyau** du couple de flèches (v_1, v_2).

4.1.2. Définition. Soit $\mathcal{C}$ une catégorie. Une **topologie de Grothendieck** sur $\mathcal{C}$ est la donnée, pour tout $X \in Ob(C)$ ("ouvert") d'une famille $Cov(X) = \{(X_i \to X)_{i\in I}\}$ dont les membres sont appelés des **recouvrements**, tels que :
1) id : $X \to X \in Cov(X)$
2) Si $\{X_i \to X\}_{i\in I} \in Cov(X)$ et $\{X_{ij} \to X_i\}_{j\in J_i} \in Cov(X_i)$, $\forall i$, alors on doit avoir $\{X_{ij} \to X\}_{i,j\in I\times\cup J_i} \in Cov(X)$
3) Si $\{X_i \to X\}_{i\in I}$ est une famille quelconque, et $\{Y_j \to X\}_{j\in I} \in Cov(X)$,
$\{X_i \times_X Y_j \to Y_j\}_{i\in I} \in Cov(Y_j)$ pour tout j $\implies$ $\{X_i \to X\}_{i\in I} \in Cov(X)$

4.1.3. Définition. Une catégorie $\mathcal{C}$ munie d'une topologie τ est appelée un **site**, on note souvent un site de cette manière : (C, τ).

4.1.4. Exemple. On se place dans la catégorie $\mathcal{C}$ des schémas étales sur S, i.e.
$C = \{X \xrightarrow{\text{étale}} S\}$. Soit $X \in \mathcal{C}$. On appelle **petit site étale de** S la catégorie $\mathcal{C}$ munie de la topologie de Grothendieck constituée des recouvrements suivants :

$$Cov(X) = \{\{X_i \to X\}_{i\in I} \text{ tel que } X_i \xrightarrow{\text{étale}} X \text{ et } \amalg X_i \to X \text{ surjective}\}.$$

Ce site est appelé **petit site étale de** S et on le note $S_{et,sm}$.

On appelle également **gros site étale de** S noté $S_{et,big}$ la catégorie $C = \mathrm{Sch/S}$ munie de cette même topologie.

Pour le prochain exemple, on rappelle quelques définitions et propriétés :

4.1.5. Définition. Soit $f : X \to S$ un morphisme de schéma. On dit que f est **localement de présentation finie en x** $\in X$ si il existe V voisinage affine de $f(x)$, et U voisinage affine de x tels que $f(U) \subset V$ et $\mathcal{O}_S(V)$ est un quotient de l'anneau des polynômes en plusieurs indéterminées (nombre fini) à coefficients dans $\mathcal{O}_X(U)$, par un idéal de type fini. On dit que f est **localement de présentation finie** si il l'est en tout point de X.

4.1.6. Lemme. *Un morphisme entre schémas affines $f : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ est localement de présentation finie si et seulement si A est une R-algèbre de présentation finie.*

Démonstration. Voir [RO]. §2. Lemme 2.1.3 □

4.1.7. Définition. Soit $f : X \to Y$ un morphisme de schémas. On dit que f est **fidèlement plat** s'il est plat et surjectif (au sens topologique).

4.1.8. Exemple. Si k est un corps, tout morphisme qui provient d'un schéma non vide X dans $\mathrm{Spec}(k)$ est fidèlement plat.

4.1.9. Définition. On dit qu'une propriété $(\mathcal{P})$ de morphismes de schémas est **locale fppf au but** si pour tout morphisme de schéma $f : X' \to X$, pour tout morphisme fppf $Y \to X$, si $f' : X \times_X \to Y$ est fppf, alors f est également fppf.

$$\begin{array}{ccc} X' \times_X Y & \xrightarrow{f'} & Y \\ \downarrow & & \downarrow{\scriptstyle fppf} \\ X' & \xrightarrow[f]{} & X \end{array}$$

4.1.10. Théorème. *Les propriétés suivantes sont locales fppf au but :*
-(localement) de type fini, ou (localement) de présentation finie
-un isomorphisme
-un monomorphisme
-une immersion ouverte ou une immersion fermée
-affine
-plat

Démonstration. Voir [GW] Chapitre 14, proposition 14.51. □

4.1.11. Exemple. On appelle **petit site fppf de S** la catégorie des schémas
$C = \mathrm{Plat/S} = \{X \to S$ fidèlement plat et localement de présentation finie$\}$, munie des ensembles suivant :

$$Cov(X) = \{(X_i \to X)_{i \in I} \text{ tel que } X_i \xrightarrow{\text{plat et loc PF}} X \text{ et } \amalg Xi \to X \text{ surjectif}\}$$

4.1.12. Lemme. *Ces ensembles forment une topologie de Grothendieck.*

Démonstration. 1) L'identité est bien un morphisme plat et localement de présentation finie.
2) Vient du fait que la composée de morphismes plats est plat et celle de morphismes localement de présentation finie est localement de présentation finie.
3) Vient du fait que la propriété pour $f : X' \to X$ d'être fppf est locale sur le but d'après le théorème 4.1.10. □

4.1.13. Lemme. *Soit X un schéma affine et $\{X_i \to X\}$ un recouvrement fppf de X. Alors, il existe un raffinement fppf $\{U_i \to X_j\}$ de ce recouvrement tel que chaque U_i soit un ouvert affine d'un X_j.*

Démonstration. Provient des définitions et du fait qu'un morphisme plat et localement de présentation finie est ouvert. □

4.1.14. Définition. Soit X un schéma affine. Un recouvrement de X constitué comme ci-dessus d'ouverts affines est appelé **recouvrement standard**.

4.1.15. Définition. Soit (C, τ) un site. On appelle **préfaisceau** (d'ensembles, de groupes, d'anneaux...) sur $\mathcal{C}$ un foncteur

$$F : \mathcal{C}^{\mathrm{op}} \to Ens/Grp/Ring$$

Si $C = Sch/S$ on parle de S-préfaisceau.

4.1.16. Remarque. En fait ici, la notion de site n'intervient pas.

4.1.17. Définition. Soit (C, τ) un site. On appelle **faisceau** (d'ensembles, de groupes, d'anneaux...) un préfaisceau F tel que $\forall X \in \mathcal{C}$ ("ouvert"), et $\forall \{X_i \to X\}_{i\in I} \in Cov(X)$, le diagramme

$$F(X) \to \prod_{i\in I} F(X_i) \underset{b}{\overset{a}{\rightrightarrows}} \prod_{i,j} F(X_i \times_X X_j)$$

est exact dans la catégorie des ensembles/groupes/anneaux.
Cela signifie que pour toute collection de sections $s_i \in F(U_i)$ telles que $s_{i|U_i\cap U_j} = s_{jU_i\cap U_j}$ pour tout i, j, il existe une unique section $s \in F(U)$ dont la restriction à U_i est s_i pour tout i.
Remarque : dans la catégorie des groupes par exemple, on peut demander de manière équivalente que cette suite :

$$0 \to F(X) \to \prod F(X_i) \xrightarrow{a-b} \prod F(X_i \times_X X_j)$$

est exacte.

Dans la prochaine définition, nous donnons plusieurs définitions d'épimorphismes.

4.1.18. Définition. Soit $Y \xrightarrow{f} X$ un morphisme de schémas. Alors
1) f est **épimorphisme** si pour tout $g_1, g_2 : X \to Z$ on a : $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$.
2) f est un **épimorphisme strict** si il fait de f le coégalisateur de ce diagramme : $Y \times_X Y \rightrightarrows Y \xrightarrow{f} X$ (où les deux flèches simples sont les deux projections).

4.1.19. Proposition. *Un épimorphisme strict est un épimorphisme. La réciproque est vraie dans la catégorie des faisceaux.*

4.1.20. Théorème. *Si $X \to S$ est un S-schéma, alors $F = \mathrm{Hom}(-, X)$ est un faisceau pour $\tau =$fppf.*

Pour démontrer ce théorème, nous avons besoin de ce lemme :

4.1.21. Lemme. *Soit F un S-préfaisceau. Les conditions suivantes sont équivalentes :*
1) F est un faisceau fppf sur S.
2) F transforme les sommes disjointes arbitraires en produits directs et pour tout S-morphisme $U' \to U$ fidèlement plat localement de présentation finie, le diagramme

$$F(U) \to F(U') \rightrightarrows F(U' \times_U U')$$

est exact.

Démonstration. Supposons que F soit un faisceau fppf sur S. Si U est une somme disjointe de schémas U_i, en appliquant la propriété de faisceau, on obtient que l'application $F(\amalg U_i) = F(U) \to \prod F(U_i)$ est bijective. Donc F transforme les sommes amalgamées en produit. De plus la deuxième partie du 2) est juste l'application de la propriété du faisceau pour le recouvrement consistant en un seul morphisme : $U' \to U$.
Réciproquement soit $\{U_i \to U\}$ un recouvrement fppf. On a alors par hypothèse

$$F(U) \to F(\amalg U_i) = \prod F(U_i) \rightrightarrows F(\amalg U_i \times_U \amalg U_i) = \prod_{i,j} F(U_i \times_U U_j)$$

exact. □

Démonstration. (Du théorème) : D'après le lemme il suffit de démontrer que le foncteur de points de X transforme les sommes disjointes en produits et que pour tout morphisme fidèlement plat localement de présentation finie de S-schémas $U' \to U$, le diagramme d'ensembles

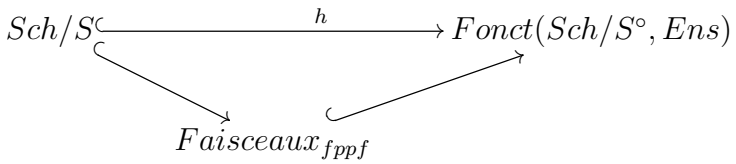
$$X(U) \to X(U') \rightrightarrows X(U' \times_U U')$$

est exact. La première partie provient directement de la définition catégorique des sommes disjointes. Vérifions la seconde condition.
Par définition du produit fibré, on a $\mathrm{Hom}_S(U, X) = \mathrm{Hom}_U(X \times_S U)$, on peut remplacer S par U et X par $X \times_S U$ et alors se ramener au cas $S = U$. On note $f : S' \to S$ le morphisme fidèlement plat localement de présentation finie à considérer, et on veut démontrer que $X(S) \to X(S') \rightrightarrows X(S' \times_S S')$ est exact.
Fait : un morphisme fidèlement plat de schémas est un épimorphisme (au sens catégorique) de schémas.
D'où l'exactitude à gauche du diagramme. Montrons l'exactitude à droite. Soit $\alpha' : S' \to X$ un morphisme tel que $\alpha' \circ pr_1 = \alpha' \circ pr_2 := g$. Alors α' est constant sur les fibres de f : en effet on a toujours une application surjective : $|S' \times_S S'| \xrightarrow{u} |S'| \times_{|S|} |S'|$. Soit alors s_1 et s_2 dans S' tels que $f(s_1) = f(s_2)$.
Alors, $(s_1, s_2) \in |S'| \times_{|S|} |S'|$. Par surjectivité, il existe $s \in |S' \times_S S'|$ tel que $u(s) = (s_1, s_2)$. Si on appelle p la fonction continue sous-jacente de la première projection $|S' \times_S S'| \to |S'|$, et q celle de la deuxième, on a $pr_1 \circ u = p$ et $pr_2 \circ u = q$. Or, $\alpha' \circ pr_1 \circ u = \alpha' \circ pr_2 \circ u$, i.e. $\alpha' \circ p = \alpha' \circ q$. Ainsi, on a $\alpha'(p(s)) = \alpha'(q(s))$, c'est-à-dire $\alpha'(s_1) = \alpha'(s_2)$.

Donc α' se factorise en une fonction continue $\alpha : S \to X$ (car f est un surjectif).

Il reste à définir un morphisme de faisceau $\alpha^\# : \mathcal{O}_X \to \alpha_* \mathcal{O}_S$. La construction est donnée dans [RO] §2, théorème 2.4.7. □

4.1.22. Remarque. On peut reformuler le théorème de la manière suivante : Yoneda se factorise :



Un cas particulier du théorème (celui qui nous intéresse) est celui-ci :

4.1.23. Corollaire. *Tout schéma en groupes G/S définit un faisceau fppf de groupes.*

4.1.24. Corollaire. *Un morphisme $f : Y \to X$ de schéma qui est fppf est un épimorphisme strict.*

4.1.25. Définition. On dit qu'une suite de schémas en groupes plats

$$0 \to G_1 \xrightarrow{i} G_2 \xrightarrow{q} G_3 \to 0$$

est **exacte** si elle l'est comme suite de faisceaux : i.e.
-i est injectif (injectif sur le foncteur de points pour tout schéma affine) et
-q est une application surjective en tant qu'application de faisceaux : i.e. pour tout schéma affine $\mathrm{Spec}(R) \to S$ de G_3, pour tout $x \in G_3(R)$, il existe $y : \mathrm{Spec}(R') \to G_2$ tel que $f : \mathrm{Spec}(R') \to \mathrm{Spec}(R)$ soit un recouvrement fppf, et tel que y relève x dans le sens où ce diagramme est commutatif :

$$\begin{array}{ccc} G_2 & \xrightarrow{\quad q \quad} & G_3 \\ {\scriptstyle y}\uparrow & & \uparrow{\scriptstyle x} \\ \mathrm{Spec}(R') & \xrightarrow{\exists \text{ fppf}} & \mathrm{Spec}(R). \end{array}$$

Cela nous amène à la définition des quotients fppf.

Soit G un S-schéma en groupes et X un S-schéma. En général, il n'y a pas de procédure simple pour construire un "bon" quotient de X par G dans la catégorie des schémas sur S. En général, un schéma quotient n'existe pas forcément. On a toujours la notion de quotient catégorique mais sa définition ne dit pas quand il existe, et s'il existe, comment le décrire. On peut alors procéder comme ceci :
a) On remplace la catégorie des schémas sur S par une plus grande, dans laquelle la formation du quotient est plus simple.
b) On forme le quotient $Y := X/G$ dans cette catégorie.
c) On étudie les conditions pour que Y soit représentable par un schéma.
Ici, la catégorie que l'on va considérer est celle des faisceaux fppf.

4.2 Existence des quotients par des groupes plats de présentation finie

4.2.1. Théorème. *Soit G/S un schéma en groupes fidèlement plat et localement de présentation finie. Soit H/S, $H \subset G$ sous-schéma en groupes fidèlement plat et localement de présentation finie sur S. Alors le faisceau quotient G/H est représentable par un schéma si* $\dim(S) = 0$ *ou S est régulier de dimension inférieure ou égale à* 1. *Le morphisme canonique $G \to G/H$ est alors un morphisme fppf.*

Démonstration. Voir [RAY] théorème 1. □

4.2.2. Remarque. Quand le quotient d'un S-groupe G par un sous-groupe H existe, c'est alors le faisceautisé du préfaisceau quotient. On peut alors le décrire ainsi : c'est l'unique groupe Q tel qu'il existe un morphisme de groupes $G \xrightarrow{\pi} Q$ de noyau H et tel que pour tout T un S-schéma, pour tout $x \in G/H(T)$, il existe T'/T fppf et $y \in G(T')$ tel que $x_{|T'} = \pi_{|T'}(y)$.

Pour la suite, nous aurons besoin de ces quelques propositions.

4.2.3. Proposition. *Soit G groupe algébrique sur un corps k et $H \subset G$ sous groupe algébrique. Alors, G/H est un groupe algébrique et lisse si G l'est.*

Démonstration. Voir [SGA3] VI_A 3.2 □

Lorsque l'on se place dans la topologie fppf, de nouveaux résultats apparaissent.

4.2.4. Proposition. *Soit G un groupe affine ou lisse. Alors :*
1) Si G est connexe, $[G,G]$ l'est aussi.
2) Pour toute k-algèbre R, le groupe $[G,G](R)$ est constitué des éléments x de $G(R)$ tels qu'il existe $R' \to R$ un morphisme d'algèbres fidèlement plat tel que $x_{|R'} \in [G(R'), G(R')]$.

Démonstration. Voir [MIL]. Chapitre 6. §d corollaire 6.19. □

4.2.5. Proposition. *Soit G un k-schéma algébrique, et $[G,G]$ son groupe dérivé. Le quotient $G/[G,G]$ est commutatif (alors $[G,G]$ est le plus petit sous-groupe normal avec cette propriété).*

Lorsqu'un quotient existe dans la catégorie des groupes algébriques, nous retrouvons les théorèmes d'isomorphismes habituels de la théorie des groupes classique.

4.2.6. Théorème. *Soit $q : G \to G/N$ un morphisme de G dans un quotient de G. Soit $\phi : G \to H$ un morphisme de groupes algébriques, tel que $N \subset \ker(\phi)$.Alors ϕ se factorise de manière unique*

$$\begin{array}{ccc} G & \xrightarrow{q} & G/N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists ! \overline{\phi}} \\ & & H \end{array}$$

Démonstration. Voir [Mil]. Chapitre 5. §b. Théorème 5.13. □

4.2.7. Théorème. *Soient H et N des sous-groupes algébriques d'un groupe algébrique G tels que N est normal dans G. Alors $H \cap N$ est un sous-groupe normal de H et l'application naturelle*

$$H/H \cap N \to HN/N$$

est un isomorphisme.

Voir [Mil]. Chapitre 5. §g. Théorème 5.52.

4.2.8. Théorème. *Soit N un sous-groupes normal d'un groupe algébrique G. Un groupe algébrique H de G qui contient N est normal dans G si et seulement si H/N est normal dans G/N. Dans ce cas, l'application naturelle*

$$G/H \to (G/N)/(H/N)$$

est un isomorphisme.

Démonstration. Voir [Mil]. Chapitre 5. §g. Théorème 5.55. □

5 L'hyperalgèbre d'un groupe en caractéristique positive

5.1 Morphisme de Frobenius pour un schéma en groupes en caractéristique p

Dans cette section, on fixe ces notations : soit k un corps de caractéristique $p > 0$.
Soit G un k-groupe algébrique affine, $G = \mathrm{Spec}(A)$.

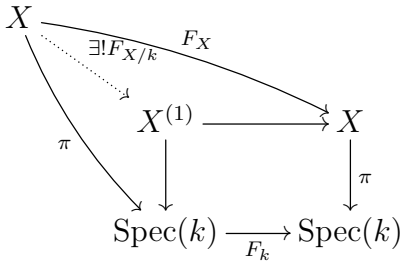
5.1.1. Définition. On appelle M le noyau de $\tilde{e} : A \to k$, et on note : $M^{(p^n)} := \{a^{p^n} | a \in M\}$.

Sur un k-groupe algébrique G en caractéristique p (i.e. $car(k) = p$), on peut décrire plusieurs morphismes de Frobenius : le morphisme de Frobenius absolu et le morphisme de Frobenius relatif.

5.1.2. Définition. On écrit F_G le **morphisme de Frobenius absolu** défini par : F_G est l'identité sur l'espace topologique sous-jacent et est l'application : $x \mapsto x^p$ sur $\mathcal{O}_X(U)$ pour tout U ouvert de X. Comme on est en caractéristique p, c'est un morphisme de schémas. Cependant, en général, ce n'est pas un morphisme de k-schémas, sauf si par exemple $k = \mathbb{F}_p$. Pour y remédier, on définit un autre morphisme : le morphisme de Frobenius relatif (sous-entendu relatif à $\mathrm{Spec}(k)$).
Pour cela, remarquons déjà que ce diagramme est commutatif :

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathrm{Spec}(k) & \xrightarrow[F_k]{} & \mathrm{Spec}(k) \end{array}$$

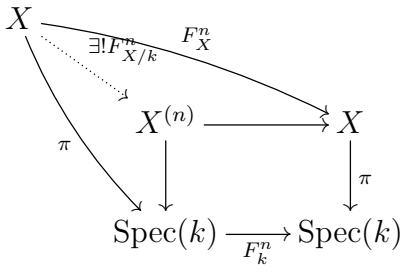
On considère alors ce diagramme :



Où $X^{(1)}$ est le produit fibré du carré cartésien. On définit alors $F_{X/k} : X \to X^{(1)}$ comme étant le **morphisme de Frobenius relatif de X sur** $\mathrm{Spec}(k)$.

5.1.3. Définition. On peut itérer les morphismes de Frobenius. Pour le morphisme absolu il n'y a rien à dire : on considère les itérés du morphisme comme habituellement, que l'on note F_X^n.

Pour le morphisme relatif, on appelle le **n-ième itéré du morphisme relatif de Frobenius** le morphisme $F_{X/k}^n : X \to X^{(p^n)}$ défini ainsi :



On ne peut pas voir le n-ième morphisme de Frobenius relatif comme une itération à proprement parler, car la source et le but de ce morphisme ne sont pas identiques. Cependant, on a des isomorphismes canoniques :

$$(X^{(1)})^{(1)} \simeq X^{(2)}, (X^{(2)})^{(1)} \simeq X^{(3)}...$$

En effet, on applique la transitivité du produit fibré à ce diagramme :

$$\begin{array}{ccccc} (X^{(1)})^{(1)} & \longrightarrow & X^{(1)} & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(k) & \xrightarrow[F_k]{} & \mathrm{Spec}(k) & \xrightarrow[F_k]{} & \mathrm{Spec}(k) \end{array}$$

Les deux carrés sont cartésiens, donc

$$(X^{(1)})^{(1)} \simeq X \times_{\{F_k \circ F_k\}} \mathrm{Spec}(k) \simeq X^{(2)}$$

Et on continue par récurrence.
De plus, on a un isomorphisme naturel :

$$F^n_{X/k} = (X \xrightarrow{F_{X/k}} X^{(1)} \xrightarrow{F_{X^{(1)}/k}})(X^{(1)})^{(1)} = X^{(2)} \to \cdots \to X^{(n-1)} \xrightarrow{F_{X^{(n-1)}/k}} X^{(n)}$$

D'où l'idée de l'itération.

5.1.4. Définition. On appelle le **n-ième voisinage infinitésimal de l'identité de** G le noyau que l'on note G^n du n-ième itéré du Frobenius relatif de G.

5.1.5. Proposition. *G^n est un groupe affine, avec comme anneau de coordonnées $A/M^{(p^n)}A$.*

Démonstration. Tout d'abord, par définition du produit fibré et par l'équivalences des catégories {Schémas affines} et {Anneaux}, on peut dire que $G^{(n)}$ est affine, d'anneau de coordonnées

$$A^{(n)} := A \otimes_{k,F^n_k} k$$

que l'on écrit :

$$A \otimes k'$$

Ensuite, par définition du noyau et toujours par cette même équivalence, l'anneau que l'on cherche est

$$A \otimes_{A^{(n)}} k$$

De plus, si on a un anneau k et un k-morphisme $A \to A/I$ qui décrit une immersion fermée $\mathrm{Spec}(A/I) \hookrightarrow \mathrm{Spec}(A)$, si on fait un changement de base $k \to k'$, on obtient la suite exacte :

$$0 \to I \to A \to A/I \to 0.$$

En prenant $- \otimes_k k'$ on obtient une suite exacte :

$$I \otimes k' \to A \otimes_k k' \to (A/I) \otimes k' \to 0.$$

La flèche de gauche n'est pas injective (en général), et son image est $(I \otimes k') \cdot (A \otimes_k k')$. Donc comme la flèche de gauche est surjective, on a $\dfrac{A \otimes k'}{(I \otimes k') \cdot (A \otimes_k k')} \simeq (A/I \otimes k')$.

En prenant $I = M$, et comme $A/M \simeq k$, on trouve que $A^{(n)}/MA^{(n)} \simeq k$.

Ainsi, l'idéal de $e : \mathrm{Spec}(k) \to G^{(n)}$ est l'idéal engendré par M dans $A^{(n)} := A \otimes_{F^n,k} k$.

On obtient alors :

$$A \otimes_{A^{(n)}} k = A \otimes_{A^{(n)}} (A^{(n)}/MA^{(n)}) = A/(MA^{(n)}) \cdot A = A/M^{(p^n)}A.$$

Et donc on obtient l'anneau de fonctions de G^n. □

5.1.6. Proposition. *Comme pour tout $n \in \mathbb{N}$, $A/M^{(p^n)}$ est l'anneau des coordonnées d'un groupe algébrique, il a une structure de k-algèbre (de type fini donc noethérienne) de Hopf. Alors, ces algèbres de Hopf sont toutes de dimension finie.*

Démonstration. Pour cela, on a besoin du lemme suivant : soit A une k-algèbre où k est un corps de caractéristique $p > 0$. Soit I un idéal de A et $I^{(n)} := \langle a^n, a \in I \rangle$. Alors :

Si I est engendré par r éléments, $\forall k$, on a :

$$I^{r(p^k-1)+1} \subset I^{(p^k)} \subset I^{p^k}$$

En particulier les suites $\{I^{p^k}\}$ et $\{I^{(p^k)}\}$ sont cofinales.

On utilise alors ce lemme avec $I = M$, et en passant au quotient, on a alors des surjections :

$$A/M^{p^k} \to A/M^{(p^k)} \to A/M^{r(p^k-1)+1}.$$

Grâce à ce lemme, on est alors ramené à montrer que $A/M^{p^n}A$ est de dimension finie pour tout $n \in \mathbb{N}$.

Grâce au troisième théorème d'isomorphisme, on a des suites exactes :

$$0 \to M/M^2 \to A/M^2 \to A/M = k \to 0.$$

On note r le cardinal d'un ensemble de générateurs de M, comme idéal. Alors M/M^2 est un A/M-module i.e. un k-module, et de dimension $\leq r$. On conclut en utilisant l'additivité de la dimension.

De même :

$$0 \to M^n/M^{n+1} \to A/M^{n+1} \to A/M^n \to 0.$$

Et la proposition est démontrée. □

Grâce au Frobenius relatif d'un groupe, on peut voir qu'un groupe localement algébrique sur un corps est "proche" d'un groupe lisse.

5.1.7. Exemple. On se place sur un corps k imparfait de caractéristique $p > 0$. Soit $t \in k \setminus k^p$. Soit $G = V(y^p - tx^p) := \mathrm{Spec}(k[x,y]/(y^p - tx^p))$. Calculons son Frobenius relatif. Déjà, par équivalence de catégories entre les schémas affines et les anneaux, on trouve que $G^{(1)} = \mathrm{Spec}(k[u,v]/(v^p - t^p u^p))$. Le morphisme de Frobenius est alors donné sur les anneaux de fonctions par

$$k[u,v]/(v^p - t^p u^p) \to k[x,y]/y^p - t^p x^p)$$

$$u \mapsto x^p$$

$$v \mapsto y^p$$

On peut également calculer le noyau du Frobenius relatif. Il est donné par le sous-schéma fermé $G_1 = V(x^p, y^p)$ dans $V(y^p - tx^p)$.

5.1.8. Théorème. *Soit G un groupe localement algébrique sur un corps k de caractéristique $p > 0$. Alors, pour tout n suffisamment grand, le quotient $L := G/G_n$ est lisse, où G_n est le noyau du Frobenius relatif : $G \to G^{(n)}$.*

Démonstration. Voir [SGA3.1] Exp VII$_A$, prop. 8.3. □

5.2 Définition avec les noyaux de Frobenius

Dans ce qui suit, on note $G = \mathrm{Spec}(A)$ un groupe localement algébrique sur $\mathrm{Spec}(k)$ avec k un corps de caractéristique $p > 0$, $M = \ker(\epsilon)$ où $\epsilon : A \to k$ est la counité de A.

5.2.1. Définition. La famille d'algèbres de Hopf $\{A/M^{(p^n)}A\}_{n=0}^{\infty}$, avec les morphismes suivants :

$$A/M^{(p^m)}A \xrightarrow{\pi_{m,n}} A/M^{(p^n)}A \text{ , pour } m \geq n$$

forme un système projectif. Leurs duales munis des applications duales forment alors un système injectif.

On appelle **hyperalgèbre de G**, et on note B la limite inductive du système

$$\{(A/M^{(p^n)}A)^*; \pi_{m,n}^*\}_{n=0}^{\infty}$$

dans la catégorie des k-algèbres de Hopf, où

$$\pi_{m,n}^* : \left(A/M^{(p^m)}A\right)^* \to \left(A/M^{(p^n)}A\right)^*$$

$$f \mapsto f \circ \pi_{m,n}.$$

On va voir une autre définition de l'hyperalgèbre, qui sera équivalente à celle ci.

5.3 Définition avec le dual fini de l'anneau localisé

On note A_e le localisé de A en l'idéal maximal M.

5.3.1. Définition. On note $hy(G)$ la limite inductive $\varinjlim (A_e/I)^*$ dans la catégorie des coalgèbres, où I varie dans l'ensemble des idéaux cofinis de A_e.

5.3.2. Proposition. *La famille* $\{M^{(p^n)}A_e\}$ *est cofinale dans celle des idéaux cofinis de* A_e.

Démonstration. On a déjà vu que cette famille était cofinale avec $\{M^{p^n}A_e,\ n \in \mathbb{N}\}$, elle-même cofinale avec $\{M^n A_e,\ n \in \mathbb{N}\}$.

Il suffit donc de montrer que pour tout I_e idéal cofini de A_e, $\exists n \in \mathbb{N}$, $M^n A_e \subset I_e$.

On sait que : A est noethérien, donc A_e l'est aussi ; MA_e est l'idéal maximal de A_e.

Soit I_e idéal cofini de A_e. On a une bijection entre les idéaux de A_e et les idéaux de A contenus dans M. On appelle I l'idéal de A qui est l'antécédent de I_e. Alors $I \subset M$ et A_e/I_eA_e est une k-algèbre de dimension finie, donc est artinien.

On conclut alors grâce à cette proposition :

5.3.3. Proposition.

Soit I un idéal dans un anneau noethérien R. Les assertions suivantes sont équivalentes pour un idéal premier P contenant I :

1)R_p/I_p est artinien

2) On a $P_P^n \subset I_p$ à partir d'un certain rang.

□

5.3.4. Proposition. *On a $B \simeq hy(G)$ (en tant que coalgèbres).*

Démonstration. En effet, on a vu que $A_e/M^{(p^n)}A_e$ est une k-coalgèbre de dimension finie, il existe donc une application naturelle :

$$\left(A/M^{(p^n)}A\right)^* \simeq \left(A_e/M^{(p^n)}A_e\right)^* \xrightarrow{f_n} \varinjlim \left(A_e/I\right)^*$$

Et donc par la propriété universelle, on trouve l'existence d'un morphisme de coalgèbres $f : B \to hy(G)$. Comme on a montré que les deux ensembles concernés étaient cofinaux, f est un isomorphisme.

□

5.3.5. Remarque. En fait, on peut même montrer que f est un isomorphisme d'algèbres de Hopf, une fois que l'on a donné une structure d'algèbre sur $hy(G)$.
On procède comme suit : la multiplication $G \times G \to G$ de notre groupe donne un morphisme d'algèbres de Hopf : $\mathcal{O}(G)_e \to \mathcal{O}(G \times G)_{e'}$ où on note e' le neutre de $G \times G$. Et en passant au dual fini, on obtient un morphisme $((\mathcal{O}(G \times G)_{e'})^0 \simeq (\mathcal{O}(G)_e)^0 \times (\mathcal{O}(G)_e)^0 \to (\mathcal{O}(G)_e)^0$. Ce morphisme donne une structure d'algèbre de Hopf sur la coalgèbre $hy(G)$, et le morphisme f devient un morphisme d'algèbres de Hopf.

5.3.6. Notation. On note w la multiplication de B en tant qu'algèbre, et on note alors $w^* : B^* \to (B \otimes B)^*$ son application duale.

On regarde $B^* \otimes B^*$ comme sous-ensemble de $(B \otimes B)^*$ grâce à l'application injective :

$$B^* \otimes B^* \to (B \otimes B)^*$$
$$f \otimes g \mapsto (a \otimes b \mapsto f(a)g(b))$$

5.3.7. Définition. On appelle **l'algèbre de Hopf duale de** B et on note
$B_0 := (w^*)^{-1}(B^* \otimes B^*)$.

Grâce au lemme 1.1.9, on sait que $B_0 = B^0$ d'où :

5.3.8. Proposition. *B_0 est en bijection avec $\bigcup_I (B/I)^*$ où I parcourt l'ensemble des idéaux cofinis bilatères de B.*

Démonstration. En effet, $\bigcup_I (B/I)^*$ est en bijection avec l'ensemble suivant :

$\{g \in B^*, I \text{ cofini et bilatère }, I \subset \ker(g)\}$ lui-même en bijection avec B_0. □

5.3.9. Remarque. Rappelons que $B_0 = B^0$ a la structure de coalgèbre induite par $\varinjlim_I (B/I)^*$ car on voit $(B/I)^*$ comme sous-coalgèbre de B^*, et le coproduit est la restriction du dual de la multiplication.

5.3.10. Proposition. *L'algèbre de Hopf B^0 est la limite projective dans la catégorie des k-algèbres de Hopf commutatives du système projectif $\{A/M^{(p^n)}, \pi_{m,n}\}$.*

Démonstration. Voir [SU.2]. □

5.3.11. Proposition. *Avec les mêmes notations, on peut voir que B^* est la limite projective suivante :*

$$B^* = \varprojlim_n A/M^{(p^n)}A$$

dans la catégorie des k-algèbres commutatives.

Démonstration. Voir [SU.2]. □

Si G n'est pas affine, nous pouvons également dans ce cas définir une hyperalgèbre de G qui coïncide avec la définition donnée précédemment si G est affine. On suppose donc maintenant que G est un groupe localement algébrique sur k un corps (i.e. on peut écrire $G = \cup \mathrm{Spec}(A_i)$ avec A_i des k-algèbres de type fini).

5.3.12. Définition. On note $hy(G) = \varinjlim_I ((\mathcal{O}(G)_e/I)^*) = (\mathcal{O}(G)_e)^0$ où I parcourt l'ensemble des idéaux cofinis de $\mathcal{O}(G)_e$ et la limite est prise dans la catégorie des coalgèbres. On l'appelle alors **l'hyperalgèbre de** G.

5.4 Liens entre l'hyperalgèbre d'un groupe et le groupe lui-même

5.4.1. Proposition. *Si on a une algèbre de Hopf H, alors H^0 est aussi une algèbre de Hopf, et le foncteur $(-)^0$ est autoadjoint dans la catégorie des algèbres de Hopf.*

Démonstration. Voir [TA.1] §0. 0.1. □

5.4.2. Proposition. *Soit G un groupe algébrique. Alors $hy(G) = (\mathcal{O}(G)_e)^0$ est réflexive en tant que coalgèbre.*

Démonstration. On a vu dans la proposition 1.3.4 que le dual d'une algèbre noethérienne est une coalgèbre réflexive. Or, $\mathcal{O}(G)_e$ est noethérien comme localisé d'anneau noethérien (car lui-même quotient d'un noethérien). □

Soit I_e un idéal cofini de $\mathcal{O}(G)_e$ et I sa préimage dans $\mathcal{O}(G)$. On a donc un morphisme d'algèbres injectif

$$\mathcal{O}(G)/I \hookrightarrow \mathcal{O}(G)_e/I_e.$$

Notre idéal I est alors cofini dans $\mathcal{O}(G)$, et donc on obtient un morphisme :

$$(\mathcal{O}(G)_e/I_e)^* \to (\mathcal{O}(G)/I)^* \to \mathcal{O}(G)^0$$

Ceci étant vérifié pour tout idéal cofini I_e de $\mathcal{O}(G)_e$, on obtient par propriété universelle de la limite inductive un morphisme de $(\mathcal{O}(G)_e)^0 = hy(G)$ dans $(\mathcal{O}(G))^0$.

Ce morphisme $hy(G) \to (\mathcal{O}(G))^0$ nous donne par adjonction un morphisme d'algèbre de Hopf :

$$u : \mathcal{O}(G) \to hy(G)^0.$$

De plus, comme on peut voir l'hyperalgèbre d'un groupe par le dual fini du localisé en l'élément neutre de son anneau de fonctions, et que chaque étape est fonctorielle, on obtient :

5.4.3. Proposition. *Soient G et H deux groupes localement algébriques. L'application suivante :*

$$\{\textit{Groupes algébriques}\} \to \{\textit{Algèbres de Hopf}\}$$

$$G \mapsto hy(G)$$

est un foncteur.

On a alors :

5.4.4. Proposition. *Soit G un groupe algébrique affine. Les assertions suivantes sont équivalentes :*
1) L'application $u : \mathcal{O}(G) \to hy(G)^0$ est bijective.
2) Pour tout groupe algébrique affine G', l'application suivante est bijective :

$$\mathrm{Hom}_{k\text{-}grp}(G, G') \to \mathrm{Hom}_{k\text{-}\mathrm{Hopf}}\,\mathrm{Hom}(hy(G), hy(G'))$$

Démonstration. Nous allons seulement montrer l'implication 1) $\implies$ 2).
On pose $\overline{G} = \mathrm{Spec}((hy(G)^0)$. Soit G un k-schéma affine. On a :

$$\mathrm{Hom}(G, G') \simeq \mathrm{Hom}(\mathcal{O}(G'), \mathcal{O}(G)) \simeq \mathrm{Hom}(\mathcal{O}(G'), hy(G)^0) \simeq \mathrm{Hom}(\overline{G}, G')$$

Or, on a vu plus haut que $(hy(G))^0 = \varprojlim_n \mathcal{O}(G)/M^{(p^n)}\mathcal{O}(G)$ dans la catégorie des algèbres de Hopf, où M est l'idéal d'augmentation. Or, un morphisme d'algèbres de Hopf $\mathcal{O}(G') \to \mathcal{O}(G)/M^{(p^n)}\mathcal{O}(G)$ envoie l'idéal d'augmentation $m' = m'_G \subset \mathcal{O}(G')$ dans l'idéal d'augmentation, donc envoie $m'^{(p^n)}$ dans $M^{(p^n)}$, qui est 0 dans l'algèbre but. Ainsi un tel morphisme induit un unique $\mathcal{O}(G')/m'^{(p^n)} \to \mathcal{O}(G)/M^{(p^n)}\mathcal{O}(G)$. Ainsi,

$$\mathrm{Hom}(\mathcal{O}(G'), hy(G)^0) \simeq \varprojlim_n \mathrm{Hom}(\mathcal{O}(G')/m'^{p^n}, \mathcal{O}(G)/M^{p^n}\mathcal{O}(G))$$

i.e.

$$\mathrm{Hom}(G, G') \simeq \mathrm{Hom}((hy(G'))^0, (hy(G))^0)$$

Cette flèche se factorise

$$\mathrm{Hom}_{k-group}(G,G') \to \mathrm{Hom}_{Hopf}(hy(G),hy(G')) \to \mathrm{Hom}_{Hopf}((hy(G')^0,hy(G)^0)$$

Montrons que la deuxième flèche est injective. Pour soulager l'écriture, on note à partir de maintenant $A := hy(G)$ et $B := hy(G')$.

Nous allons alors utiliser le fait que B est propre comme algèbre, ou encore (c'est équivalent) propre comme bialgèbre. Rappelons pourquoi c'est vrai : B est construite comme une sous-algèbre de $\mathcal{O}(G')^*$, qui est propre, or toute sous-algèbre d'une algèbre propre est propre, donc B est propre c'est-à-dire que $B \to B^{\circ *}$ est injectif, donc aussi $B \to B^{\circ\circ}$ puisque $B^{\circ\circ} \subset B^{\circ *}$. Maintenant utilisons ceci et le diagramme suivant pour démontrer notre assertion.

$$\begin{array}{ccccc}
\mathrm{Hom}_{Hopf}(A,B) & \longrightarrow & \mathrm{Hom}_{Hopf}(B^\circ,A^\circ) & & \\
\big\downarrow & & \big\downarrow & & \\
 & & \mathrm{Hom}_{\mathrm{Alg}}(B^\circ,A^\circ) & & \\
 & & \big\downarrow & & \\
\mathrm{Hom}_{coalg}(A,B) & \longrightarrow & \mathrm{Hom}_{\mathrm{Alg}}(B^\circ,A^*) & \xrightarrow{(-)^\circ} & \mathrm{Hom}_{coalg}(A^{*\circ},B^{\circ\circ}) \\
 & \searrow & & \nearrow & \\
 & & \varphi & &
\end{array}$$

Il suffit de démontrer que $\varphi : \mathrm{Hom}(A,B) \to \mathrm{Hom}(A^{*\circ},B^{\circ\circ})$ est injectif. Voici ce qu'est cette application : à un morphisme de coalgèbres $u : A \to B$ on associe le morphisme d'algèbres $u^* : B^* \to A^*$, puis sa restriction $u^*_{|B^\circ} : B^\circ \to A^*$, puis le morphisme de coalgèbres $(u^*_{|B^\circ})^\circ : A^{*\circ} \to B^{\circ\circ}$. Pour montrer que φ est injectif soient $u, v : A \to B$ tels que $\varphi(u) = \varphi(v)$:

$$\begin{array}{ccc}
A & \xrightarrow{u,v} & B \\
{\scriptstyle j_A}\big\downarrow & & \big\downarrow{\scriptstyle j_B} \\
A^{*\circ} & \xrightarrow{\varphi(u)=\varphi(v)} & B^{\circ\circ}.
\end{array}$$

De $\varphi(u) = \varphi(v)$ on tire $\varphi(u)j_A = \varphi(v)j_A$, donc $j_B u = j_B v$, donc $u = v$ puisque j_B est injectif.

Ainsi, $\mathrm{Hom}_{k\text{-}group}(G,G') \to \mathrm{Hom}_{k\text{-}\,\mathrm{Hopf}}(A,B)$ est injective.

Montrons maintenant qu'elle est surjective. La deuxième flèche l'est car la composée l'est. Ainsi, La deuxième flèche est une bijection. En considérant son inverse, on obtient que la première flèche est surjective comme composée d'une bijection et d'une surjection.

On a alors démontré que 1) $\implies$ 2). □

5.4.5. Définition. Soit G un groupe localement algébrique. Une sous-algèbre J de $hy(G)$ est dite **algébrique** ou **fermée** s'il existe un sous-schéma en groupes H de G avec $J = hy(H)$. Pour toute sous-algèbre J de $hy(G)$, il existe une unique sous-algèbre fermée que l'on note $A(J)$ de $hy(G)$ qui contient J.

5.4.6. Notation. Nous présentons ici la notation de Sweedler que l'on va utiliser dans la

suite. Si x est un élément d'une coalgèbre (C, Δ, ϵ), l'élément $\Delta(x)$ de $C \otimes C$ est de la forme

$$\Delta(x) = \sum_i x'_i \otimes x''_i.$$

On l'écrit alors

$$\Delta(x) = \sum_{(x)} x_{(1)} \otimes x_{(2)}.$$

5.4.7. Définition. Soit H une algèbre de Hopf, d'antipode S. Soient $x, y \in H$. En adoptant la notation de Sweedler, on note. $[x, y] := \sum_{(x,y)} x_{(1)} y_{(1)} S(x_{(2)}) S(y_{(2)})$. Soient alors K et J deux sous-algèbres de Hopf de H. Alors on note $[K, J]$ la sous-algèbre engendrée par les éléments $[x, y]$.

5.4.8. Proposition.
1) Si J_1 et J_2 sont fermées dans $hy(G)$, alors $[J_1, J_2]$ aussi.
2) On a $[J, J] = [A(J), A(J)]$.

Démonstration. Voir [TA.1]. §0. Proposition 0.3.4. □

5.4.9. Proposition. *Soit G un groupe localement algébrique sur k. Alors*

$$\dim(G) = \dim(hy(G))$$

Démonstration. Voir [DG] II §4 n°1 □

5.5 Algèbre des distributions

On donne enfin un troisième point de vue sur l'hyperalgèbre d'un groupe, afin de mieux la comprendre. On pourra utiliser [JA] Chapitre 7 comme référence pour toute cette section.

Soit X un k-schéma affine. $X = \mathrm{Spec}(A)$. Soit $x \in X(k) = \mathrm{Hom}(\mathrm{Spec}(k), X)$. Soit $I_x \subset A$ l'idéal des fonctions nulles en x, où, pour $f \in A$, on définit $f(x) := x(f)$ où l'on voit x comme un morphisme de k-algèbre $x : A \to k$.

On remarque que comme $x \in X(k)$, on a $\kappa(x) \hookrightarrow k$, mais comme $\kappa(x)$ est un k-espace vectoriel, on identifie $\kappa(x)$ à k.

Par cet identification, pour $f \in A$ et $x \in X(k)$, on a $f(x) = \overline{f_x}$ dans $\kappa(x) = k$.

Ainsi, $(I_x)_x$, où I_x est défini ci-dessus, s'identifie donc à $m_x := \{s_x \in \mathcal{O}_{X_x}, s_x \text{ non inversible}\}$ l'unique idéal maximal de $\mathcal{O}_{X,x}$.

5.5.1. Définition. Une **distribution sur X d'ordre $\leq n$ avec support sur** x est une fonction k-linéaire $\mu : A \to k$ telle que

$$\mu(I_x^{n+1}) = 0$$

Les distribution d'ordre $\leq n$ en x forment un sous-espace vectoriel du dual de A, que l'on note $Dist_n(X, x)$.
On note également $\mathrm{Dist}(X, x) = \bigcup_n Dist_n(X, x)$.

5.5.2. Proposition. *On a un isomorphisme de k-espaces vectoriels $Dist_n(X, x) \simeq (k[X]/(I_x^{n+1}))^*$*

5.5.3. Définition.

Pour un groupe algébrique affine $G = \mathrm{Spec}(A)$ sur k, on note $\mathrm{Dist}(G)$ pour $\mathrm{Dist}(G, e)$, où e est l'élément neutre du groupe. Nous avons vu dans la preuve de la proposition 3.1.7 que e était un point de $G(k)$. Regardons I_x en $x = e \in G$ l'élément neutre. Soit $\tilde{e}$ le morphisme d'anneau $A \to k$ correspondant à e. Alors $I_e = \{a \in A, \tilde{e}(a) = 0\}$, donc $I_e = m$ où m est l'idéal maximal correspondant à l'élément neutre dans $\mathrm{Spec}(A)$.

Quand $\mu, \mu' \in \mathrm{Dist}(G)$, on définit leur composée $\mu.\mu'$ comme étant :

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{(\mu,\mu')} k$$

Ainsi, si G est un groupe algébrique, $\mathrm{Dist}(G)$ est une **algèbre**.

Tout ce que l'on a fait ici est valable pour un schéma en groupes quelconque (remplacer A par $\mathcal{O}_{X,x}$).

On voit donc que notre construction est très similaire à celles faites ci-dessus. Il nous manque juste une structure de plus pour pouvoir les identifier. Nous allons donc donner donner à cette algèbre une structure de coalgèbre :

5.5.4. Définition. Soit X un schéma en groupes sur un schéma $S = \mathrm{Spec}(R)$ et $x \in X$.

On dit que X est **infinitésimalement plat en** x si chaque $\mathcal{O}_X(X)/I_x^{n+1}$ est de présentation finie et plat en tant que R-module.

5.5.5. Remarque. Par définition, si G est un k-schéma en groupes algébrique (où k est un corps), G est infinitésimalement plat en x pour tout x dans G (car présentation finie équivaut à de type fini ici).

Soient deux k-schémas affines $X = \mathrm{Spec}(A)$ et $X' = \mathrm{Spec}(B)$, et $x \in X(k)$ et $x' \in X(k')$. L'idéal d'annulation $I_{(x,x')}$ dans $\mathcal{O}_{X\times X'}(X \times X') = A \otimes B$ est $I_{(x,x')} = I_x \otimes B + A \otimes I_{x'}$.

Si de plus X et X' sont infinitésimalement plats en x et x' respectivement, alors $I_{x,x'}^{n+1}$ peut être identifié à $\sum_{j=0}^{n+1} I_x^j I_{x'}^{n+1-j}$ et donc également à $\bigcap_{j=0}^{n} (A \otimes I_{x'}^{n+1-j} + I_x^{j+1} \otimes B)$.

On obtient alors :

5.5.6. Proposition. *Soient X et X' deux k-schémas en groupes algébriques, infinitésimalement plats en x et x' respectivement.*

Alors, $X \times X'$ l'est en (x, x'), et de plus, on a un isomorphisme :

$$\mathrm{Dist}(X, x) \otimes \mathrm{Dist}(X', x') \simeq \mathrm{Dist}(X \times X', (x, x'))$$

On applique donc cette proposition avec $X = X' = G$, où $G = \mathrm{Spec}(A)$ groupe algébrique sur un corps k, et $x = x'$.

On note $\delta_G : G \to G \times G\,;\ x \mapsto (x, x)$. On regarde l'application correspondante sur les anneaux $\phi : A \otimes A \to A$. Le morphisme ϕ envoie $I_{(x,x)}$ dans I_x, et envoie donc $(I_{(x,x)})^{n+1}$ dans $(I_x)^{n+1}$. On obtient alors un morphisme

$$\mathrm{Dist}_n(G, x) \to \mathrm{Dist}_n(G \times G, (x, x)) \simeq \mathrm{Dist}_n(X, x) \otimes \mathrm{Dist}_n(X, x))$$

qui fait de l'algèbre des distributions une coalgèbre.

5.5.7. Proposition. *Grâce à la structure de coalgèbre donnée ci-dessus, on a alors des isomorphismes d'algèbres de Hopf :*

$$B \simeq hy(G) \simeq \mathrm{Dist}(G, e)$$

5.5.8. Exemples.

(1) Regardons l'algèbre des distributions du groupe additif : $\mathbb{G}_a := \mathbb{A}^1 := \mathrm{Spec}(k[T])$. L'élément neutre est $x := 0 : k[T] \to k\,;\, T \mapsto 0$. Alors $I_x = (T)$ et $I_x^n = (T^n)$.

On a $k[T]/(T^{n+1})$ qui est un k-espace vectoriel de dimension $n+1$ et de base $1, T, \ldots, T^n$.

On définit $\gamma_r \in k[T]^*$ par

$$\gamma_r(T^n) = 0 \text{ pour tout } n \neq r \text{ et } \gamma_r(T^r) = 1$$

Alors $Dist_n(\mathbb{G}_a, 0)$ est le k-ev de base $(\gamma_r)_{0 \leq r \leq n}$ et $\mathrm{Dist}(\mathbb{G}_a, 0)$ est le k-ev de base $(\gamma_r)_{r \in \mathbb{N}}$.

Si $car(k) = 0$, alors on a

$$\gamma_r(f) = \frac{1}{r!}\Big(\frac{\partial}{\partial T}\Big)^{(r)} f(0)$$

où $d = \deg(f)$.

(2) On regarde maintenant celle du groupe multiplicatif
$\mathbb{G}_m := \mathrm{Spec}(k[T, T^{-1}]) = k[S, T]/(ST - 1)$.

On regarde toujours au point identité, qui est le noyau de

$$k[T, S]/(TS - 1) \to k$$

$$T, S \mapsto 1.$$

L'idéal que l'on doit considérer est alors $I_x = (T - 1)$.

Une base de $k[T, T^{-1}]$ est donnée par $1, T - 1, \ldots, (T - 1)^n$. Pour décrire l'algèbre des distributions, remarquons que il existe un unique $\partial_n \in \mathrm{Dist}(\mathbb{G}_m)$, avec $\partial_n((I_1)^{n+1}) = 0$ et $\partial_n((T - 1)^k = \partial_{k,n}$ pour tout k plus petit que n.

De plus, comme $T^n = ((T - 1) + 1)^n$, on a $\partial_r(T^n) = \binom{n}{r}$.

6 Lien entre l'hyperalgèbre et la simple connexité d'un groupe

6.1 Les revêtements

6.1.1. Définition. Soit k corps et G, H deux k-schémas en groupes affines connexes. Si $\eta : H \to G$ est un épimorphisme de k-schémas en groupes, dont le noyau est un k-schéma en groupes fini et étale, alors (H, η) est appelée un **revêtement étale** de G.
Si de plus le noyau est d'ordre premier avec $(\max(1, p))$, η est appelé un **p-revêtement étale**.

6.1.2. Exemple. Pour tout groupe G, l'identité de $G \to G$ est un revêtement étale, appelée le revêtement trivial, dont le noyau est $\mathrm{Spec}(k)$.

6.1.3. Exemple.
- Un morphisme $\mathrm{Spec}(l) \to \mathrm{Spec}(k)$ induit par une extension finie et séparable de corps l/k est un revêtement étale, dont le noyau est $\mathrm{Spec}(l)$.
- Sur un corps k, f :$\mathbb{G}_m \to \mathbb{G}_m$ défini par $f(x) = x^n$ où n est un entier premier à $car(k)$, est un revêtement étale, dont le noyau est les racines n-ièmes de l'unité dans k.
- Sur un corps de caractéristique $p > 0$, $f : \mathbb{A}^1 \to \mathbb{A}^1$ définie par $f(x) = x^p - x$ est un revêtement étale, dont le noyau est $\mathrm{Spec}(k[X]/(X^p - X))$.

6.1.4. Définition. Un schéma en groupes G est dit **simplement connexe** (SC) s'il ne possède pas de revêtement étale non isomorphe au revêtement trivial.
Un schéma en groupes G est dit **p-simplement connexe** $(\mathrm{SC})_p$ s'il ne possède pas de p-revêtement étale non trivial.

6.1.5. Exemple. Le groupe additif $\mathbb{G}_a$ sur un corps k de caractéristique positive n'est pas simplement connexe.

En effet, nous avons la suite d'Artin-Schreier suivante :

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \xrightarrow{F_{\mathbb{G}_a} - \mathrm{id}} \mathbb{G}_a \to 0$$

où $F_{\mathbb{G}_a}$ désigne le Frobenius absolu du groupe additif. Cette suite identifie donc $\mathbb{G}_a$ avec un quotient de lui-même, dont le noyau est $\mathbb{Z}/p\mathbb{Z}$ qui est bien fini et étale.

Cependant, le seul revêtement de $\mathbb{G}_a$ étant celui-ci, on peut alors montrer que le groupe additif en caractéristique p positive est p-simplement connexe.

6.1.6. Exemple. Le groupe multiplicatif $\mathbb{G}_m$ n'est pas simplement connexe. En effet nous avons la suite suivante

$$0 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 0$$

expliquée dans l'exemple 6.1.3.

6.1.7. Définition. Un revêtement étale $\psi : H^* \to G$ est appelé un **revêtement universel** de G si le groupe algébrique H est simplement connexe.

6.1.8. Proposition. *Soit G un groupe algébrique sur k et (H^*, ψ) un revêtement universel de G. Alors on a la propriété universelle suivante :*

Pour tout (H, η) revêtement étale de G, il existe un unique morphisme de groupes algébriques $\eta^* : H^* \to H$ avec $\eta \circ \eta^* = \psi$.

$$\begin{array}{ccc} H^* & \xrightarrow{\eta^*} & H \\ & {\scriptstyle\psi}\searrow \quad \swarrow{\scriptstyle\eta} & \\ & G & \end{array}$$

Ainsi, un revêtement universel de G, s'il existe, est unique à isomorphisme près.

6.1.9. Lemme. *Soit Y un schéma en groupes connexe. Les conditions suivantes sont équivalentes ;*
1) Tout revêtement fini étale $f : X \to Y$ possède une section ensembliste
2) Tout revêtement fini étale $f : X \to Y$ possède une section qui est un morphisme de groupe.

6.1.10. Proposition. *Tout quotient d'un groupe simplement connexe G par un sous-groupe distingué connexe H est simplement connexe.*

Démonstration. Soit $P \xrightarrow{\pi} G/H$ un morphisme fini étale, où P est un groupe algébrique. On introduit les notations suivantes :

$$\begin{array}{ccc} P' := P \times_{G/H} G & \xrightarrow{f'} & P \\ \downarrow{\scriptstyle\pi'} & & \downarrow{\scriptstyle\pi} \\ G & \xrightarrow{f} & G/H \end{array}$$

Le fait d'être fini étale est stable par changement de base, donc on a que π' est fini étale. Comme G est simplement connexe, il existe une section : $s' : G \to P'$ telle que $\pi' \circ s' = \mathrm{id}_G$.

On note $Q' := s'(G) \simeq G$. On a $H \subset G$ et donc $H' = s'(H) \subset Q'$. Or, s' est la section d'un morphisme fini étale, et donc elle est ouverte (et fermée), donc $s'(G) = Q'$ est un sous-schéma ouvert de P' (avec la structure de restriction), et de même H' est un sous-schéma ouvert de Q'. Alors $Q = Q'/H'$ est une section (ensembliste, donc de groupes) de π. □

6.1.11. Proposition. *Soit G groupe algébrique affine ou lisse. Alors G connexe implique $[G, G]$ connexe.*

Démonstration. Voir [Mil]. Chapitre 6. §d Corollaire 6.19. □

6.2 Groupes unipotents, semi-simples

6.2.1. Définition. Soit G un schéma en groupes. On appelle **suite de composition de** G un ensemble $(G_i)_{i\in 0,\dots,n}$ de sous-groupes fermés de G tels que $G_0 = G$, $G_n = e$ et pour tout i, G_i est un sous-groupe normal de G_{i-1}.

Si, de plus, pour tout i, $\forall R$ k-algèbre, $\forall x \in G(R)$, $\forall y \in G_i(R)$, on a $x^{-1}y^{-1}xy \in G_{i+1}(R)$, alors on dit que cette suite de composition est **centrale**.

6.2.2. Définition. Soit G un groupe algébrique sur k. On dit que G est **unipotent** si $G \otimes \bar{k}$ est obtenu par un nombre fini d'extensions de sous-groupes de $\mathbb{G}_a$.

6.2.3. Remarque. On vérifie que cette définition ne dépend pas de la clôture algébrique de k choisie.

Voici un théorème qui précise ce que sont les groupes algébriques unipotents :

6.2.4. Théorème. *Pour qu'un groupe algébrique G défini sur un corps k algébriquement clos soit unipotent, il faut et il suffit qu'il possède une suite de composition dont les quotients successifs sont isomorphes à $\mathbb{G}_a$ si $p = 0$, et à l'un des groupes $\mathbb{G}_a$, $\mathbb{Z}/p\mathbb{Z}$, α_p si $p > 0$. (Ces groupes sont appelés les groupes unipotents élémentaires).*

Démonstration. Voir [SGA3.2] Exposé 17 : Groupes algébriques unipotents. Extensions entre groupes unipotents et groupes de type multiplicatif de M. Raynaud. Corollaire 1.7. □

On cite également ce théorème qui nous sera utile plus tard :

6.2.5. Théorème. *Tout groupe algébrique quotient d'un groupe unipotent est unipotent.*

Démonstration. Voir [SGA3.2]. Exposé 17. Proposition 2.2. □

6.2.6. Définition. On suppose que k est un corps parfait et G un groupe algébrique lisse sur k. On appelle **radical unipotent** de G le plus grand sous-groupe normal fermé unipotent connexe lisse de G. On le note G_u.

6.2.7. Définition. Un groupe algébrique lisse G est dit **réductif** si $G_u = (e)$.

6.2.8. Définition. Soit G un groupe algébrique sur k. On dit que G est **résoluble** s'il possède une suite de composition dont les quotients successifs sont commutatifs.

6.2.9. Remarque. En particulier, un groupe unipotent est résoluble.

6.2.10. Définition. On suppose encore que k est parfait et G est un groupe algébrique lisse sur k. On appelle **radical** de G le plus grand sous-groupe fermé normal fermé résoluble connexe lisse de G. On le note $rad(G)$.

6.2.11. Définition. Dans les conditions de la définition ci-dessus, on dit que G est **semi-simple** si $rad(G) = (e)$.

6.2.12. Proposition. *G/G_u est toujours réductif, et $G/rad(G)$ est toujours semi-simple.*

6.2.13. Exemple. GL_n est réductif, et son radical est $\mathbb{G}_m$ = le groupe des matrices d'homothétie. Et on a $\mathrm{GL}_n / \mathbb{G}_m = \mathrm{PGL}_n$ est semi-simple.

6.2.14. Remarque. Comme un groupe unipotent est résoluble, le radical unipotent est inclus dans le radical. Ainsi, un groupe semi-simple est en particulier réductif.

Voici une proposition sur les groupes semi-simples que l'on va également utiliser dans la suite :

6.2.15. Proposition. *Un groupe algébrique semi-simple est parfait, i.e. égal à son sous-groupe dérivé.*

Démonstration. Voir [Mil]. Chapitre 21. e) Corollaire 21.50 . □

6.3 Reconstruction des groupes algébriques à partir de leurs noyaux de Frobenius

Soit G un groupe algébrique sur k et $u : \mathcal{O}(G) \to hy(G)^0$ le morphisme construit pour la proposition 5.4.4.

Le but de cette partie est de comprendre et démontrer ce résultat :

6.3.1. Théorème. *Soit $G = \mathrm{Spec}(A)$ un k-groupe algébrique affine et connexe, où k est parfait. Alors :*

G est simplement connexe si et seulement si $u : A \to (hy(G))^0$ est un isomorphisme

Nous allons préciser tout ceci.

6.3.2. Théorème. *Soient G et H deux groupes algébriques affines connexes sur k et $\eta : H \to G$ morphisme de k-groupes algébriques. Alors*

$$(H, \eta) \text{ est un revêtement étale } \Leftrightarrow hy(\eta) : hy(H) \to hy(G) \text{ est un isomorphisme}$$

Démonstration. Voir [TA.1]. §1. Proposition 1.1. □

6.3.3. Théorème. *Soit $G = Spec(A)$ un groupe algébrique affine connexe sur k. On considère ces trois conditions :*
a) G est simplement connexe.
b) Pour tout groupe H localement algébrique sur k, l'application

$$\mathrm{Hom}_{k\text{-}grp}(G, H) \to \mathrm{Hom}_{k\text{-Hopf}}(hy(G), hy(H))$$

$$f \mapsto hy(f)$$

est bijective.
c) L'application canonique $A \to hy(G)^0$ est bijective.

Alors, b) $\implies$ c) $\implies$ a) et si de plus $G/[G, G]$ est fini, alors a) $\implies$ b).

Démonstration. Le b) $\implies$ c) a déjà été prouvé.
Montrons alors que c) $\implies$ a). Soit $\eta : H \to G$ un revêtement étale. Alors, d'après la proposition précédente, $hy(\eta) : hy(H) \simeq hy(G)$. Supposons c) vraie. Alors, comme H est affine, en utilisant la proposition 5.4.4 on a $\mathrm{Hom}(G, H) \simeq \mathrm{Hom}(hy(G), hy(H))$ et donc il existe un unique $\sigma : G \to H$ tel que $hy(\sigma) = hy(\eta)^{-1}$. Or, comme $hy(-)$ est un foncteur, on a $hy(\eta \circ \sigma) = hy(\eta) \circ hy(\sigma) = \mathrm{id}$ et donc comme $\mathrm{Hom}(G, G) \simeq \mathrm{Hom}(hy(G), hy(G))$, on obtient $\eta \circ \sigma = \mathrm{id}$.
De plus, σ est un épimorphisme dans la catégorie des k-groupes algébriques affines : en effet, soit H' un groupe algébrique affine. On veut montrer que $\mathrm{Hom}(H, H') \to \mathrm{Hom}(G, H')$ est injective. Soient f et $g \in \mathrm{Hom}(H, H')$, tels que $f \circ \sigma = g \circ \sigma$. Alors $hy(f) \circ hy(\sigma) = hy(g) \circ hy(\sigma)$ et donc $hy(f) = hy(g)$ et donc $f = g$.
On regarde alors :

$$\mathrm{Hom}(H, H) \to \mathrm{Hom}(G, H)$$

$$\phi \mapsto \phi \circ \sigma$$

On voit alors que $\sigma \circ \eta$ est envoyé sur σ qui est l'image de l'identité, donc par injectivité on a $\sigma \circ \eta = \mathrm{id}$ donc η est une bijection et donc G est simplement connexe. D'où $c) \implies a)$.
Montrons maintenant la deuxième partie du lemme.
On suppose que $G/[G,G]$ est fini et que G est simplement connexe. Soit H un groupe localement algébrique. Soit $w : hy(G) \to hy(H)$ un morphisme entre les deux hyperalgèbres. La composée :

$$\psi : hy(G) \xrightarrow{\Delta} hy(G) \otimes hy(G) \xrightarrow{\mathrm{id} \otimes w} hy(G) \otimes hy(H)$$

est injective. En effet : on considère l'application :

$$hy(G) \otimes hy(H) \xrightarrow{\phi := \mathrm{id} \otimes \epsilon_H} hy(G)$$
$$a \otimes b \mapsto a.\epsilon_H(b)$$

où $\epsilon_H : H \to k$ est la counité.
Alors soit $x \in hy(G)$. On a $\phi \circ \psi(x) = (\mathrm{id} \otimes \epsilon_H) \circ (\mathrm{id} \otimes w)(\Delta(x)) = \mathrm{id} \otimes \epsilon_h(\sum x_{(1)} \otimes w(x_{(2)}))$
$\phi \circ \psi(x) = \sum x_{(1)}.\epsilon_H(w(x_{(2)}) = \sum x_{(1)}.\epsilon_G(x_{(2)}) = (\mathrm{id} \otimes \epsilon_G)(\Delta(x))$.
Enfin, $(\mathrm{id} \otimes \epsilon_G) \circ \Delta = \mathrm{id}_{hy(G)}$ en vertu de ce diagramme commutatif valable dans toute coalgèbre C :

$$\begin{array}{ccccc} C \otimes C & \longrightarrow & C \otimes k & \longrightarrow & C \\ & \nwarrow^{\Delta} & \uparrow{\scriptstyle \simeq} & \nearrow_{\mathrm{id}} & \\ & & C & & \end{array}$$

où l'application $C \otimes C \to C \otimes k$ est donnée par $c \otimes c' \mapsto c \otimes \epsilon_C(c')$, et celle ci $C \otimes k \to C$ par $(c \otimes \lambda) \mapsto \lambda c$. Ainsi $\phi \circ \psi = \mathrm{id}$ et donc ψ est injective.

Maintenant, on pose $R := G \times H$; $J := \mathrm{im}(\psi) \simeq hy(G)$ et $J' := [J, J]$. Par la proposition 5.4.8, J' est fermé dans $hy(G) \otimes hy(H)$. Alors d'après [TA.2] §3.6, il existe un unique sous-schéma fermé connexe G^* de $G \times H$ avec $hy(G^*) = J$. La projection $pr_1 : G^* \to G$, qui est un revêtement étale car $J = hy(G^*) \simeq^{\psi} hy(G)$, donc cette projection est un isomorphisme car G est simplement connexe. Alors, la composée

$$f : G \xrightarrow{(pr_1^{-1})} G^* \xrightarrow{pr_2} H$$

est l'unique antécédent de w, i.e. $w = hy(f)$. □

6.3.4. Théorème. *Soit k un corps parfait de caractéristique $p > 0$. Alors, un groupe algébrique affine sur k est simplement connexe si et seulement si $\mathcal{O}(G) \simeq hy(G)^0$. Dans ce cas, $G/[G,G]$ est fini.*

Démonstration. Par le théorème précédent, il suffit de montrer que $G/[G,G]$ est fini quand G est simplement connexe. Remarquons tout d'abord que l'on peut supposer G lisse. En effet, le théorème 5.1.8 nous dit qu'il existe un entier $n > 0$ tel que G/G_n soit lisse, où G_n est le noyau du n-ième itéré du morphisme de Frobenius relatif.

Soit alors un tel n. On note L le quotient. Soit $\pi_G : G \to L$ le morphisme canonique.

On note $G' := [G, G]$ et $L' := [L, L]$. On veut montrer que π_G passe au quotient et donc peut être défini sur G', et est à valeur dans L'. Soit M sous groupe normal de L tel que L/M soit abélien. On a

$$G \xrightarrow{\pi_G} L \xrightarrow{\pi_L} L/M$$

Comme L/M est abélien, $\pi_L \circ \pi_G$ se factorise par le groupe dérivé : $G/G' \to L/M$. On a alors ce diagramme commutatif :

$$\begin{array}{ccc} G & \longrightarrow & L \\ \downarrow & & \downarrow \\ G/G' & \longrightarrow & L/M \end{array}$$

Donc $\pi_G(G') \subset M$.

Et donc comme M était quelconque, on a $\pi_G(G) \subset L'$. Montrons alors l'inclusion réciproque.

Le morphisme π_G est un épimorphisme dans la catégorie des groupes algébriques. Alors, l'image d'un sous-groupe normal est normal. Ainsi, $\pi_G(G')$ est normal. On a alors ce diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\pi_G} & L \\ \downarrow & & \downarrow \\ G/G' & \longrightarrow & L/\pi_G(G') \end{array}$$

Or, π_G épimorphisme implique que $G/G' \to L/\pi_G(G')$ est un épimorphisme également. Or, G/G' est abélien, et donc $L/\pi_G(G')$ l'est aussi car quotient d'un abélien. Ainsi, $L' \subset \pi_G(G')$ et on obtient ce que l'on veut.

On a donc $G/G' \twoheadrightarrow L/L'$, son noyau est $G_n \cap G'$ qui est fini. Donc

$$L/L' \text{ fini } \Leftrightarrow G/G' \text{ fini.}$$

On suppose alors à partir de maintenant G lisse.

Soit G_u le radical unipotent de G. Le groupe G/G_u est semi-simple, donc parfait par la proposition 6.2.15 : i.e. $G/G_u = [G/G_u, G/G_u]$. Or,

$$1 \to G_u \to G \to G/G_u \to 1$$

est exacte, et donc

$$[G/G_u, G/G_u] = G/G_u = [G, G]G_u/G_u$$

et ainsi, $G = [G, G]G_u$.

On peut alors conclure que $G/[G, G]$ est simplement connexe, unipotent et lisse. En effet :

-La propriété lisse vient de la proposition 4.2.3 qui dit qu'un quotient d'un groupe algébrique lisse est encore lisse.

-Celle d'être unipotent vient de cette propriété : Tout groupe quotient d'un groupe unipotent est unipotent.

Et de ce calcul : on a $G_u/[G,G] \cap G_u = G/[G,G]$.

En effet, on a $G_u \overset{i}{\hookrightarrow} G \overset{\pi}{\to} G/[G,G]$. De plus, $\ker(\pi \circ i) = [G,G] \cap G_u$ car vrai sur le foncteur de point.

Donc le théorème de quotient nous donne :

$$G_u/[G,G] \cap G_u \hookrightarrow G/[G,G]$$

Montrons que cette flèche est également surjective. Soit T un k-schéma, et $x \in (G/[G,G])(T)$. Alors on peut trouver un $T' \overset{f}{\to} T$ fppf et un $y \in G(T')/[G,G](T')$ tel que $x \circ f := x_{|T'} = y$.

Or, comme $G = [G,G]G_u$, alors il existe $T'' \overset{g}{\to} T'$ fppf tel que $y \circ g := y_{|T''} \in [G,G](T'')G_u(T'')/[G,G](T'') = G_u(T'')/[G,G](T'') \cap G_u(T'')$.

et alors $x_{T''} \in G_u(T'')/[G,G](T'') \cap G_u(T'')$.

-Et enfin, d'après la proposition 6.1.10, on sait que tout quotient d'un groupe simplement connexe par un groupe connexe est simplement connexe. Il nous suffit alors de démontrer que $[G,G]$ est connexe dans notre cas. Mais la proposition 6.1.11 nous dit que si G est lisse et connexe, alors $[G,G]$ est connexe.

On a vu alors que $G/[G,G]$ est unipotent. Il est donc extension successive de copies du groupe additif $\mathbb{G}_a$. Le but est de montrer que sa dimension est nulle. Supposons le contraire, c'est-à-dire supposons qu'il y ait au moins une copie de $\mathbb{G}_a$ dans l'extension, et on note $n > 0$ la dimension de $G/[G,G]$.
On a donc des suites exactes suivantes :
$G_1 := \mathbb{G}_a$
$1 \to G_1 \to G_2 \to \mathbb{G}_a \to 1$
$1 \to G_2 \to G_3 \to \mathbb{G}_a \to 1$
$1 \to G_{n-1} \to G_n \to \mathbb{G}_a \to 1$
avec $G_n := G/[G,G]$.

Or, G_n simplement connexe implique que G_{n-1} simplement connexe (comme quotient de G_n). Par récurrence, ceci implique que G_1 est simplement connexe.
Comme $G_1 = \mathbb{G}_a$, la suite exacte d'Artin-Schreier que l'on a expliquée dans l'exemple 6.1.5 donne une contradiction.
Ainsi, $n = 0$ et donc $G = [G,G]$. □

6.3.5. Exemple. Reprenons l'exemple du groupe multiplicatif $\mathbb{G}_m = \mathrm{Spec}(k[x,x^{-1}])$. On a vu qu'il n'était pas simplement connexe. On note $B = hy(G)$. On note $A = k[x,x^{-1}]$. On va montrer que $B^0 = B^* \not\simeq A$. Il suffit alors de montrer (en gardant les notations de 5.3.6), que $w^* : B^* \to (B \otimes B)^*$ a son image dans $B^* \otimes B^*$. Calculons alors B^*. On voudrait se mettre au voisinage de $x = 1$ car c'est en ce point que sont centrés les noyaux de Frobenius. On pose alors :

$$\phi : k[x,x^{-1}] \to k[z,(z+1)^{-1}]$$

$$x \mapsto z+1$$

On note $\Delta : k[x,x^{-1}] \to A' := k[x_1,x_1^{-1}] \otimes k[x_2,x_2^{-1}]$, $x \mapsto x_1 \otimes x_2$ la comultiplication de $k[x,x^{-1}]$, et $\Delta' : k[z,(z+1)^{-1}] \to k[z_1,(z_1+1)^{-1}] \otimes k[z_2,(z_2+1)^{-1}]$ celle de $k[z,(z+1)^{-1}]$.

Nous voulons que ϕ soit un morphisme d'algèbre de Hopf. En particulier, on veut que ϕ

respecte la comultiplication, i.e. : $(\phi \otimes \phi) \circ \Delta = \Delta' \circ \phi$, ce qui donne :

$$\begin{aligned}(\phi \otimes \phi)(\Delta(x)) = (\phi \otimes \phi)(x_1 \otimes x_2) = \phi(x_1) \otimes \phi(x_2) = ((z_1 + 1) \otimes (z_2 + 1)) \\ = 1 \otimes 1 + z_1 \otimes 1 + 1 \otimes z_2 + z_1 \otimes z_2 \\ = \Delta'(z + 1) \\ = \Delta'(z) + \Delta'(1) \\ = \Delta'(z) + 1 \otimes 1\end{aligned}$$

On voit alors apparaître la comultiplication de notre nouvelle algèbre de Hopf doit alors être définie ainsi : $\Delta'(z) = z_1 \otimes 1 + 1 \otimes z_2 + z_1 \otimes z_2$.

Par ailleurs, si on garde M pour la notation du noyau de Frobenius, on a
$M = (x - 1) = (z)$ et donc $M^{(p^n)} = (z^{p^n})$ d'où

$$B^* = \varprojlim A'/M^{(p^n)} = \varprojlim k[z, (z + 1)^{-1}]/(z^{p^n}) = k[[z]].$$

On peut alors trouver le morphisme $w : B^* \to (B \otimes B)^*$ par passage à la limite, qui est donné par

$$w : B^* \to (B \otimes B)^*$$

$$z \mapsto z_1 \otimes 1 + 1 \otimes z_2 + z_1 \otimes z_2$$

On voit bien que ce morphisme est à valeur dans $B^* \otimes B^*$, ce que l'on voulait démontrer.

Ainsi, $B^0 = B^* = k[[x]] \not\simeq A = k[x, x^{-1}]$, ce qui, grâce au théorème, permet de voir d'une autre manière que le groupe multiplicatif n'est pas simplement connexe.

Annexes

Rappels de théorie des catégories utiles pour la suite

Voici une nouvelle section, qui a pour but de définir les notions catégoriques générales dont on aura besoin. Dans la catégorie des ensembles, ces limites existent toujours et se décrivent explicitement. Ces notions sont donc rappelées ici. On se place dans l'ensemble de ce document sur des catégories petites.

6.3.6. Définition. Pour tout couple de morphismes $f, g : X \rightrightarrows Y$, un **coégalisateur** de f et de g est un morphisme $\alpha : Y \to Coeg(f, g)$ tel que les deux propriétés suivantes soient satisfaites :
(a) $\alpha \circ f = \alpha \circ g$
(b) Pour tout $\beta : Y \to Z$ tel que $\beta \circ f = \beta \circ g$, il existe un unique morphisme $\phi : Z \to Coeg(f, g)$ avec $\phi \circ \alpha = \beta$.

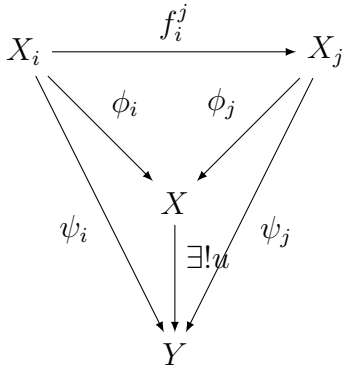
6.3.7. Définition. Soit $(I, \leq)$ un ensemble partiellement ordonné. Il est appellé **ensemble ordonné filtrant** ssi pour tout $(i, j) \in I$, $k \in I$ tel que $i \leq k$ et $j \leq k$.

Limite inductive

6.3.8. Définition. Soit $(I, \leq)$ un ensemble ordonné filtrant et $\mathcal{C}$ une catégorie. On appelle **système inductif** d'objets de $\mathcal{C}$, indexé par I, la donnée d'une famille $(X_i)_{i\in I}$ d'objets de $\mathcal{C}$ et de morphismes : $f_i^j : X_i \to X_j$ pour tout $i \leq j$, vérifiant :
1) $\forall i \in I, f_i^i = \mathrm{id}_{X_i}$
2) $\forall (i, j, k)$, $i \leq j \leq k$, on a $f_j^k \circ f_i^j = f_i^k$

6.3.9. Définition. Soit $\left((X_i)_{i\in I}, f_i^j\right)$ un système inductif dans une catégorie $\mathcal{C}$. On appelle, lorsqu'elle existe la **limite inductive** de ce système, notée $X = \varinjlim X_i$ un objet de $\mathcal{C}$ muni de morphismes $\Phi_i : X_i \to X$ vérifiant les relations de comptabilité : $\phi_i = \phi_j \circ f_i^j$ pour tout $i \leq j$.

De plus, on a la propriété universelle suivante :



6.3.10. Proposition. *La limite inductive d'ensembles existe, et vaut :* $\bigsqcup_{i\in I} X_i$ *modulo la relation d'équivalence :*

$$(i, x_i) \sim (j, x_j) \exists k \in I, i \leq k, j \leq k \text{ tel que } f_i^k(x_i) = f_j^k(y_j).$$

Démonstration. Pour tout $i \in I$, et $x_i \in X_i$, on note $\overline{(i, x_i)}$ la classe d'équivalence de (i, x_i) et on définit $\phi(x_i) = \overline{(i, x_i)}$.
ϕ est bien définie, et vérifions que l'on a : $\forall i \leq j \ \phi_i = \phi_j \circ f_i^j$:
Soit $x_i \in X_i$. Alors :

$$\phi_i(x_i) = \overline{(i, x_i)}$$
$$\phi_j \circ f_i^j(x_i) = \overline{(j, f_i^j(x_i))}.$$

Il existe $k \in I$ tel que $i \leq k$ et $j \leq k$, et on a $f_i^k(x_i) = f_j^k(f_i^j(x_i))$.
Donc $\overline{(i, x_i)} = \overline{(j, f_i^j(x_i))}$.
Il ne reste plus qu'à vérifier la propriété universelle :
Avec les notations précédentes, soit Y un ensemble et $\psi_i : X_i \to Y$ tel que $\psi_i = \psi_j \circ f_i^j$. Cherchons l'application u de la définition.
On défini

$$u : X \to Y$$
$$\overline{(i, x_i)} \mapsto \psi_i(x_i).$$

Vérifions que u est bien définie :
Soit $\overline{(j, x_j)} \in X$ tel que $\overline{(j, x_j)} = \overline{(i, x_i)}$. Alors, il existe $k \in I$, $i \leq k$ et $j \leq k$ et tel que $f_i^k(x_i) = f_j^k(y_j)$ Alors :

$$u(\overline{(i, x_i)}) = \psi_i(x_i)$$
$$u(\overline{(i, x_i)}) = \psi_k \circ f_i^k(x_i)$$
$$u(\overline{(i, x_i)}) = \psi_k \circ f_j^k(y_j)$$
$$u(\overline{(i, x_i)}) = \psi_j(y_j)$$
$$u(\overline{(i, x_i)}) = u(\overline{(j, y_j)}).$$

Donc u est bien défini. Vérifions qu'elle fait commuter le diagramme :
Par la définition de u, pour tout $x_i \in X_i$, $u \circ \phi_i(x_i) = \psi_i(x_i)$, et pour tout $y_j \in X_j$, $u \circ \phi_j(y_j) = \psi_j(y_j)$ donc le diagramme est commutatif.
Montrons maintenant l'unicité.
Soit u' une autre application respectant les mêmes contraintes. Pour tout $\overline{(i, x_i)} \in X$, pour que le diagramme soit commutatif, il faudrait que

$$u'(\overline{(i, x_i)}) = \psi_i(x_i)$$

d'où l'unicité. □

En utilisant ce que l'on vient de faire, on va prouver que la limite inductive dans la catégorie des espaces vectoriels existe.

6.3.11. Définition. Supposons que les X_i soient des k-espaces vectoriels et les f_i^j soient des applications linéaires. Définissons une structure d'espace vectoriel sur la limite inductive des ensembles sous-jacents au X_i. Soit $x = \overline{(i, x_i)}$ et $y = \overline{(j, y_j)}$ dans X, et $\lambda \in k$. Soit $k \in I$ tel que $i \leq k$ et $j \leq k$. Alors : $x = \phi_i(x_i) = \phi_k \circ f_i^k(x_i)$
$y = \phi_j(y_j) = \phi_k \circ f_j^k(y_j)$
Alors on pose :

$$x + y := \phi_k(f_i^k(x_i) + f_j^k(y_j))$$

et

$$\lambda x = \phi_i(\lambda x_i).$$

6.3.12. Proposition. *Ces deux opérations sont bien définies et font de X un espace vectoriel.*

Démonstration. Montrons que la loi "+" ne dépend pas du choix de k. Soit $l \in I$ tel que $i \leq l$ et $j \leq l$. On peut supposer $k \leq l$. Avec les mêmes notations :

$$\phi_l(f_i^l(x_i) + f_j^l(y_j)) = \phi_l(f_k^l \circ f_i^k(x_i) + f_k^l \circ f_j^k(y_j))$$
$$\phi_l(f_i^l(x_i) + f_j^l(y_j)) = \phi_l \circ f_k^l(f_i^k(x_i) + f_j^k(y_j)) \text{ car} f_k^l \text{ est linéaire}$$
$$\phi_l(f_i^l(x_i) + f_j^l(y_j)) = \phi_k(f_i^k(x_i) + f_j^k(y_j)).$$

De même on vérifie que la multiplication par un scalaire est bien définie.
On vérifie enfin facilement que X muni de ces opérations est un espace vectoriel. □

6.3.13. Proposition. *Pour tout $i \in I$, $\phi_i : X_i \to X$ est linéaire.*

Démonstration. Soient $\lambda \in k$ et $(x_i, y_i) \in X_i^2$. On a :
$\phi_i(\lambda x_i + y_i) = \overline{(i, \lambda x_i + y_i)}$
$= \overline{(i, \lambda x_i)} + \overline{(i, y_i)}$ par définition
$\lambda\overline{(i, x_i)} + \overline{(i, y_i)}$
$= \lambda\phi_i(x_i) + \phi_i(y_i)$. □

De même, on prouve que

6.3.14. Proposition. *L'application u définie plus haut est linéaire.*

Et on arrive alors à :

6.3.15. Corollaire. *La limite inductive d'espace vectoriel existe.*

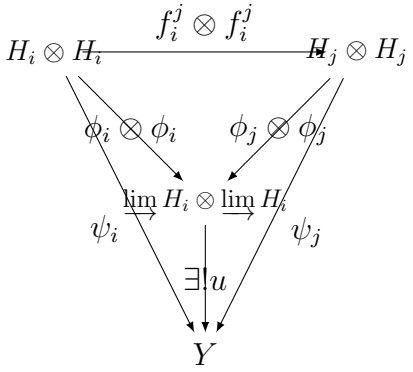
On peut maintenant montrer quelques propriétés :

6.3.16. Proposition. *On se place dans la catégorie des R-modules avec R un anneau commutatif. La limite inductive commute avec le produit tensoriel :*

$$\varinjlim(H_i \otimes H_i) \simeq (\varinjlim H_i) \otimes (\varinjlim H_i).$$

Démonstration. On prend donc $(H_i)_{i\in I}$ un système inductif, et on note H sa limite. On note $f_i^j : H_i \to H_j$ et $\phi_i : H_i \to H$.

On va montrer que $\varinjlim H_i \otimes \varinjlim H_i$ vérifie la propriété universelle de $\varinjlim(H_i \otimes H_i)$.
Alors on pose :



On veut alors trouver l'application u.

pour $x, y \in \varinjlim H_i$, alors $x = \overline{(l, x_l)}$ et $y = \overline{(m, y_m)}$. Soit $k \in I$ tel que $l \leq k$ et $m \leq k$. On définit alors $u(x \otimes y) = \psi_k(f_l^k(x_l) \otimes f_m^k(y_m)$. Cette application est bien définie.
On vérifie que cette définition ne dépend pas du choix de k : soit $n \geq k$. Alors, $\overline{(l, x_l)} = \overline{(n, f_l^n(x_l))}$ et $\overline{(m, y_m)} = \overline{(n, f_m^n(y_m))}$ et donc $u(x \otimes y) = u(\overline{(n, f_l^n(x_l))} \otimes \overline{(n, f_m^n(y_m))} = \psi_n(f_n^n(f_l^n(x_l)) \otimes f_n^n(f_m^n(y_m)) = \psi_n(f_l^n(x_l) \otimes f_m^n(y_m))$.
Montrons que u fait commuter le diagramme :
Soit $a \otimes b \in H_j \otimes H_j$. Alors $u(\phi_j(a) \otimes \phi_j(b)) = \psi_j(a \otimes b)$ car on peut prendre $k = j$ et $f_j^j = \mathrm{id}$.
Il nous reste alors à montrer l'unicité : Soit u' un autre morphisme faisant commuter le diagramme. Soient $x, y \in \varinjlim H_i$. Alors :

$$u'(x \otimes y) = u'(\overline{(l, x_l)} \otimes \overline{(m, y_m)})$$

Soit alors k majorant de l et m.

$$u'(x \otimes y) = u'(\overline{(k, f_l^k(x_l))} \otimes \overline{(k, f_m^k(y_m))}$$

$$u'(x \otimes y) = \psi_k(f_l^k(x_l) \otimes f_m^k(y_m))$$
$$= u(x \otimes y).$$

Alors on vient de prouver que

$$\varinjlim(H_i \otimes H_i) \simeq (\varinjlim H_i) \otimes (\varinjlim H_i).$$

□

6.3.17. Corollaire. *On peut construire la limite inductive d'algèbres de Hopf en rajoutant les structures necessaires sur celle dans la catégorie des espaces vectoriels.*

Démonstration. Pour tout i on a :
-(Multiplication) : $H_i \otimes H_i \to H_i \to H$ et donc on a une map : $\varinjlim(H_i \otimes H_i) = H \otimes H \to H$.
-(Co-multiplication) :$H_i \to H_i \otimes H_i \to H \otimes H$ et donc on a $H \to H \otimes H$.
-(Antipode) : $H_i \to H$ implique $H \to H$
et idem pour unité et counité. □

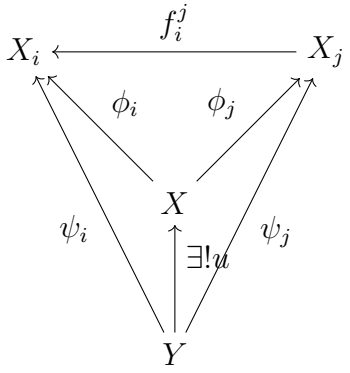
Limite projective

6.3.18. Définition. Soit $(I, \leq)$ un ensemble ordonné filtrant et $\mathcal{C}$ une catégorie. On appelle **système projectif** d'objets de $\mathcal{C}$, indexé par I, la donnée d'une famille $(X_i)_{i \in I}$ d'objets de $\mathcal{C}$ et de morphismes : $f_i^j : X_j \to X_i$ pour tout $i \leq j$, vérifiant :
1) $\forall i \in I, f_i^i = \mathrm{id}_{X_i}$
2) $\forall (i, j, k)$, $i \leq j \leq k$, on a $f_i^j \circ f_j^k = f_i^k$.

6.3.19. Définition. Soit $\left((X_i)_{i \in I}, f_i^j\right)$ un système projectif dans une catégorie $\mathcal{C}$. On appelle, lorsqu'elle existe la **limite projective** de ce système, notée $X = \varprojlim X_i$ un objet de

$\mathcal{C}$ muni de morphismes $\pi_i : X \to X_i$ vérifiant les relations de comptabilité : $\pi_i = f_i^j \circ \pi_j$ pour tout $i \leq j$.

De plus, on a la propriété universelle suivante :



6.3.20. Proposition. *La limite projective d'ensemble existe, et vaut :*

$$X = \varprojlim X_i = \left\{(a_i)_{i\in I} \in_{i\in I} X_i \ / \ \forall i \leq j \in I \ , \ a_i = f_i^j(a_j)\right\}.$$

Notons $a = (a_i)_{i\in I}$. Pour tout $i \in I$ on définit $\pi_i(a) = a_i$.
De plus, si chaque X_i soient des espaces vectoriels et chaque f_i^j soient linéaires, alors on peut munir X d'une structure d'espace vectoriel en définissant l'addition et la multiplication par un scalaire point par point, et on obtient la limite projective dans la catégorie des espaces vectoriels.

On a vu plus haut que la limite inductive commutait avec le produit tensoriel. Ce n'est pas le cas avec la limite projective, en voici la preuve :

6.3.21. Contre-exemple. La limite projective par contre ne commute pas forcément avec le produit tensoriel : En effet :
On considère le système projectif suivant : Soit p un nombre premier. Pour tout $n \in \mathbb{N}$, on définit :

$$\begin{gathered}\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \\ \overline{x} \mapsto \overline{x}.\end{gathered}$$

Ceci définit un système projectif d'anneaux, et on note sa limite $\mathbb{Z}_p$: l'anneau des entiers p-adic. $\mathbb{Z}_p$ est non nul : En effet on a une description : $\mathbb{Z}_p = \{(a_n)_{n\in\mathbb{N}} \in_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \mid \forall n, a_n \equiv a_{n+1} \ [p^n]\}$ et alors on a un morphisme naturel de $\mathbb{Z}$ dans $\mathbb{Z}^p$: $a \mapsto (a, \ldots, a, \ldots$ qui est injectif car 0 est le seul divisible par toutes les puissances de p.
Cependant, on a pour tout $n \in \mathbb{N}$

$$\mathbb{Z}/p^n\mathbb{Z} \otimes \mathbb{Q} = 0$$

donc la limite projective est nulle, mais :

$$\mathbb{Z}_p \otimes \mathbb{Q} = \mathbb{Q}_p$$

où $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$ (Car si A anneau intègre et M A-module, alors $S^{-1}M \simeq M \otimes_A S^{-1}A$ pour toute partie multiplicative S de A) qui est non nul.

C'est pour cela qu'il est en général plus difficile de définir une limite projective d'algèbres de Hopf.

Rappels d'algèbre commutative utiles pour la suite

Comme le titre de la section l'indique, nous donnons ici les définitions et résultats classiques d'algèbre commutative, utiles pour ce que l'on va étudier ensuite dans la théorie des groupes algébriques. Dans toute cette section, les algèbres considérées seront associatives et unitaires.

Produit tensoriel d'algèbres

La première partie de ces révisions est consacrée au produit tensoriel. En effet, il nous sera tout le temps utile, comme par exemple à travers l'anneau des fonctions d'un k-schéma algébrique produit.

Dans cette section, A est un anneau commutatif unitaire.

6.3.22. Définition. Soient N, M, et R deux A-modules. Soit $u : M \to N$ un morphisme de A-modules.
On note

$$u \otimes \mathrm{id}_R : M \otimes R \to N \otimes R \ ,$$
$$x \otimes r \mapsto u(x) \otimes r.$$

6.3.23. Remarque. De manière générale, u injective n'implique pas $u \otimes \mathrm{id}_R$ injective : en effet, le fait de tensoriser ne consiste pas seulement à raisonner composante par composante (il y a un produit direct pour ça) puisque les scalaires de l'anneau considéré peuvent se balader par linéarité d'une composante à l'autre et ainsi tuer des éléments qui étaient non nuls au départ.

6.3.24. Définition. Les A-modules R qui vérifient
«u injective» implique «$u \otimes \mathrm{id}_R$ injective» pour tout A-modules M, N et tout morphisme de A-module $u : M \to N$.
sont appelés des A-modules **plats**.

6.3.25. Remarque. Par contre, on a toujours la conservation des surjections, pour tout A-module et tout idéal A. C'est l'objet de la prochaine proposition.

6.3.26. Proposition. *Soit A un anneau, R un A-module et soit $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ une suite exacte de A-modules.*
Alors la suite suivante est également exacte : $M' \otimes R \xrightarrow{u \otimes \mathrm{id}_R} M \otimes R \xrightarrow{v \otimes \mathrm{id}_R} M'' \to 0$.

Démonstration. Une remarque tout d'abord : dire que la suite de modules $A \xrightarrow{u} B \xrightarrow{v} C \to 0$ est exacte équivaut à dire :

$$\mathrm{im}(u) \subset \ker(v)$$

et

$$\overline{v} : B/\mathrm{im}(u) \to C$$

est un isomorphisme.

En effet, si la suite est exacte alors on a les deux affirmations trivialement, et réciproquement on a $\mathrm{im}(v) = \mathrm{im}(\overline{v}) = C$ donc v surjective, et soit $m \in \ker(v)$, alors $v(m) = 0$ i.e. $\overline{v}(\overline{m}) = 0$ i.e. $\overline{m} = \overline{0}$ i.e. $m \in \mathrm{im}(u)$. D'où l'équivalence.

On a $(v \otimes \mathrm{id}) \circ (u \otimes \mathrm{id}) = (v \circ u \otimes \mathrm{id}) = 0 \otimes \mathrm{id} = 0$ donc $\mathrm{im}(u \otimes \mathrm{id}) \subset \ker(v \otimes \mathrm{id})$.
On regarde ensuite l'application :

$$f : \big(M \otimes R\big)/\big(\mathrm{im}(v \otimes \mathrm{id})\big) \to M'' \otimes R$$
$$\overline{m \otimes r} \mapsto v(m) \otimes r$$

On veut un inverse pour f.

Remarquons déjà que si m_1 et m_2 ont la même image par v, alors pour tout $r \in A$, $m_1 \otimes r$ et $m_2 \otimes r$ ont la même classe dans $M \otimes R/\,\mathrm{im}(v \otimes \mathrm{id})$: En effet : $v(m_1 - m_2) = 0$ i.e. $m_1 - m_2 \in \ker(v) = \mathrm{im}(u)$ donc il existe $m' \in M'$ tel que $m_1 - m_2 = u(m')$ et donc $m_1 \otimes r - m_1 \otimes r = (m_1 - m_2) \otimes r = u(m') \otimes r = (u \otimes \mathrm{id})(m' \otimes r)$.

Donc, l'application

$$\Phi : \mathrm{im}(v) \times R \to M \otimes R/\,\mathrm{im}(v \otimes \mathrm{id})$$
$$v(m) \otimes r \mapsto \overline{m \otimes r}$$

est bien définie, bilinéaire d'où (par propriété universelle du produit tensoriel et car $\mathrm{im}(v) = M''$), on a une application linéaire $\overline{\Phi}$:

$$\overline{\Phi} : M'' \otimes R \to M \otimes R/\,\mathrm{im}(v \otimes \mathrm{id})$$

$$m'' \otimes r \mapsto \Phi(m'', r)$$

On a bien $(f \circ \overline{\Phi})(m'' \otimes r) = f \circ \Phi(m'', r) = f(\overline{m \otimes r}) = m'' \otimes r$ où $v(m) = m''$, et $(\Phi \circ f)(\overline{m \otimes r}) = \Phi(v(m \otimes r) = \overline{m \otimes r}$, d'où l'inverse recherchée. □

6.3.27. Corollaire. *(Produit tensoriel de deux suites exactes) :*
Soient

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$

et

$$N' \xrightarrow{s} N \xrightarrow{t} N'' \to 0$$

deux suites exactes de A-modules. Alors $v \otimes t : M \otimes N \to M'' \otimes N''$ est sujective et de noyau

$$\ker(v \otimes t) = \ker(v \otimes \mathrm{id}_N) + \ker(\mathrm{id}_M \otimes t) = \mathrm{im}(u \otimes \mathrm{id}_N) + \mathrm{im}(\mathrm{id}_M \otimes s)$$

Démonstration. D'après la proposition précédente, $v \otimes \mathrm{id}_{N'}$ et $\mathrm{id}_M \otimes t$ sont surjectives, donc leur composée $v \otimes t$ l'est aussi.

On peut toujours écrire $v \otimes t = [v \otimes \mathrm{id}_{N'}] \circ [\mathrm{id}_M \otimes t]$ ou encore $v \otimes t = [\mathrm{id}_{M''} \otimes t] \circ [v \otimes \mathrm{id}_N]$ d'où les inclusions : $\ker(v \otimes \mathrm{id}_N) \subset \ker(v \otimes t)$ et $\ker(\mathrm{id}_M \otimes t) \subset \ker(v \otimes t)$, donc la somme est bien incluse dans $\ker(v \otimes t)$. Montrons alors l'inclusion réciproque.

Soit alors $z \in \ker(v \otimes t)$ dans $M \otimes N$. On a : $0 = [v \otimes t](z) = [v \otimes \mathrm{id}_{N''}] \otimes [\mathrm{id}_M \otimes t](z)$.
Donc, d'après la proposition précédente, $[\mathrm{id}_M \otimes t](z) \in \ker(v \otimes \mathrm{id}_{N''}) = \mathrm{im}(u \otimes \mathrm{id}_{N''})$.
et alors $[\mathrm{id}_M \otimes t](z) = [u \otimes \mathrm{id}_{N''}](y)$ pour $y \in M' \otimes N''$. Or, toujours d'après la proposition précédente, $\mathrm{id}_{M'} \otimes t$ est surjective de $M' \otimes N$ dans $M' \otimes N''$ et donc y est atteint par un $x \in M' \otimes N$. On a alors :
$[\mathrm{id}_M \otimes t](z) = [u \otimes \mathrm{id}_{N''}](y) = [u \otimes \mathrm{id}_{N''}] \circ [\mathrm{id}_{M'} \otimes t](x) = [u \otimes t](x) = [\mathrm{id}_M \otimes t] \circ [u \otimes \mathrm{id}_N](x)$.
D'où :

$[\mathrm{id}_M \otimes t]\big(z - [u \otimes \mathrm{id}_N](x)\big) = 0$ $z - [u \otimes \mathrm{id}_N](x) \in \ker(\mathrm{id}_M \otimes t) = \mathrm{im}(\mathrm{id}_M \otimes s)$.
Donc $z \in \mathrm{im}(u \otimes \mathrm{id}_N) + \mathrm{im}(\mathrm{id}_M \otimes s)$

D'où la seconde inclusion.

□

6.3.28. Corollaire. *Si M' est un sous-module de M et N' est un sous-module de N, alors on a un isomorphisme canonique :*

$$M/M' \otimes N/N' \simeq M \otimes N/(i \otimes \mathrm{id})(M' \otimes N) + (\mathrm{id} \otimes j)(M \otimes N'))$$

$$\overline{m} \otimes \overline{n} \mapsto \overline{m \otimes n}.$$

Démonstration. Les suites

$$M' \overset{i}{\hookrightarrow} M \twoheadrightarrow^{\pi_1} M/M' \to 0$$

et

$$N' \overset{j}{\hookrightarrow} N \twoheadrightarrow^{\pi_2} N/N' \to 0$$

sont exactes, donc on peut appliquer la proposition qui précède :

$$M/M' \otimes N/N' = \mathrm{im}(\pi_1 \otimes \pi_2) \simeq M \otimes N/\ker(\pi_1 \otimes \pi_2)$$

$$\simeq M \otimes N/(\mathrm{im}(i \otimes \mathrm{id}_N) + \mathrm{im}(\mathrm{id}_M \otimes i)) \simeq M \otimes N/(M' \otimes N + M \otimes N')$$

□

Voyons maintenant les propriétés sympathiques que donne l'hypothèse de platitude.

6.3.29. Proposition. *Soient M un A-module plat, et N_1, N_2 deux sous-modules d'un A-module N. Alors :*

$$(N_1 \cap N_2) \otimes M = (N_1 \otimes M) \cap (N_2 \otimes M)$$

Démonstration. Soit

$$\Phi : N \to N/N_1 \oplus N/N_2$$

$$x \mapsto (\overline{x}, \overline{x}).$$

Alors, on a cette suite exacte :

$$0 \to N_1 \cap N_2 \to N \to N/N_1 \oplus N/N_2 \to 0.$$

Donc celle-ci également par platitude :

$$0 \to (N_1 \cap N_2) \otimes M \to N \otimes M \to (N/N_1 \oplus N/N_2) \otimes M \to 0.$$

C'est-à-dire

$$0 \to (N_1 \cap N_2) \otimes M \to N \otimes M \to (N \otimes M/(N_1 \otimes M)) \oplus (N \otimes M/(N_2 \otimes M)) \to 0.$$

Ce qui donne exactement ce que l'on veut. □

Jusqu'ici, nous n'avons parlé que de produit tensoriel de modules. Notre objectif est de définir un produit tensoriel d'algèbre. Pour ceci, on définit tout simplement une structure d'algèbre sur le produit tensoriel de deux algèbres.

6.3.30. Définition. Soient A et B deux algèbres. On définit une structure d'algèbre sur $A \otimes B$ de cette manière : pour tout $a, a' \in A$ et $b, b' \in B$, on pose :

$$(a \otimes b).(a' \otimes b') := aa' \otimes bb'.$$

Et on étend ensuite cette relations par bilinéarité. Son unité est $1 \otimes 1$.

On définit deux applications $i_A : A \to A \otimes B$ et $i_B : B \to A \otimes B$ par $i_A(a) = a \otimes 1$ et $i_B(b) = 1 \otimes b$.

Le produit tensoriel d'algèbres vérifie cette propriété universelle :

6.3.31. Proposition. *Soit $f : A \to C$ et $g : B \to C$ deux morphismes d'algèbres, tels que pour tout $(a, b) \in A \times B$, la relation $f(a)g(b) = g(b)f(a)$ est vérifiée dans C. Alors, il existe un unique morphisme d'algèbres $f \otimes g : A \otimes B \to C$ tel que $(f \otimes g) \circ i_A = f$ et $(f \otimes g) \circ i_B = g$.*

On est en train de dire que $\mathrm{Hom}_{\mathrm{Alg}}(A \otimes B, C)$ est le sous-ensemble de $\mathrm{Hom}_{\mathrm{Alg}}(A, C) \times \mathrm{Hom}_{\mathrm{Alg}}(B, C)$ consistant des paires (f, g) de morphismes dont les images commutent dans C.

En particulier, si C est commutative, on a

$$\mathrm{Hom}_{\mathrm{Alg}}(A \otimes B, C) \simeq \mathrm{Hom}_{\mathrm{Alg}}(A, C) \times \mathrm{Hom}_{\mathrm{Alg}}(B, C)$$

Démonstration. Tout élément de $A \otimes B$ est une somme finie d'éléments de la forme $a \otimes b$. Alors, si $f \otimes g$ existe, elle doit être de la forme

$$(f \otimes g)(a \otimes b) = (f \otimes g)(i_A(a))(f \otimes g)(i_B(b)) = f(a)g(b).$$

Ce qui prouve l'unicité. Pour l'existence, on montre que la formule ci-dessus donne bien un morphisme d'algèbres. On utilise pour cela l'hypothèse de commutativité :
$(f \otimes g)(a \otimes b)(f \otimes g)(a' \otimes b') = f(a)g(b)f(a')g(b')$
$(f \otimes g)(a \otimes b)(f \otimes g)(a' \otimes b') = f(a)f(a')g(b)g(b')$
$(f \otimes g)(a \otimes b)(f \otimes g)(a' \otimes b') = f(aa')g(bb')$. □

Anneaux, corps, modules et algèbre linéaire

La théorie des schémas est étroitement liée à la théorie des anneaux via une équivalence de catégories. Ainsi, plusieurs définitions du monde des schémas nécessitent du vocabulaire et des propriétés de la théorie des anneaux. Nous résumons ce dont nous avons besoin dans cette section.

6.3.32. Définition. Soit A un anneau et M un A-module.

On dit que M est un A-module **de présentation finie** si il existe $n, m \in \mathbb{N}$ et une suite exacte :

$$A^m \to A^n \to M \to 0.$$

Autrement dit, M est de présentation finie s'il est quotient de A^n par un sous-module de type fini.

6.3.33. Proposition. *Un module de présentation finie est en particulier de type fini. La réciproque est vraie lorsque A est noethérien.*

Démonstration. Un module de présentation finie est de type fini car quotient d'un module de type fini par un sous-module.
On suppose maintenant l'anneau de base noethérien. Alors dans ce cas tout sous-module d'un A-module de type fini est aussi de type fini. Soit alors M un A-module de type fini. Alors $M \simeq A/N$ avec N sous module de A^n, donc de type fini également. □

Cette définition nous sera utile lorsque l'on parlera de morphisme de schémas localement de présentation finie, et de topologie fppf.

Nous continuons ces bases d'algèbre commutative avec un lemme important : Le lemme de Nakayama.

6.3.34. Lemme. *(Nakayama) : Soit A anneau et M un A-module de type fini, I un idéal de A et N un sous-A-module de M tel que $M \subset IM + N$. Alors, il existe un élément a de I tel que $(1+a)M \subset N$.*

Pour le prouver, nous avons d'abords besoin d'un résultat d'algèbre linéaire :

6.3.35. Proposition. *(Cayley-Hamilton) : Soit $I \subset A$ un idéal et $\phi : M \to IM$ un morphisme de A-modules, où M est de type fini, $M = \langle x_1, \ldots, x_n \rangle$. Alors, ϕ satisfait l'identité :*

$$\phi^n = a_1\phi^{n-1} + \cdots + a_n = 0 \in End(M)$$

où chaque $a_j \in I^j$.

Démonstration. On écrit $\phi(x_i) = \sum_{j=1}^{n} a_{i,j}x_j$, avec les $a_{i,j} \in A$. On écrit la matrice $(\phi\,\mathrm{id}_n - (a_{i,j}))$ de taille (n,n) à coefficients dans l'anneau $A[\phi]$. Cette matrice agit sur M^n, avec $(\phi\,\mathrm{id}_n - (a_{i,j}))(x_1, \ldots, x_n) (0)$.
On a la transposée de la comatrice : $(\phi\,\mathrm{id}_n - (a_{i,j}))^*$ avec

$$(\phi\,\mathrm{id}_n - (a_{i,j}))^*(\phi\,\mathrm{id}_n - (a_{i,j})) = det((\phi\,\mathrm{id}_n - (a_{i,j}))\,\mathrm{id}_n\,.$$

Alors, $\det((\phi\,\mathrm{id}_n - (a_{i,j}))$ annule $(x_1, \ldots, x_n)$ et donc annule tout élément de M. Or le déterminant en question est de la forme demandée. □

6.3.36. Corollaire. *Soit M un A-module de type fini et I idéal de A tel que $M \subset IM$. Alors il existe $a \in I$, tel que $(1+a)M = 0$.*

Démonstration. On applique la proposition précédente avec $\phi : x \mapsto x$. □

6.3.37. Corollaire. *Soit $I \subset A$ un idéal contenu dans tous les idéaux maximaux de A (c'est-à-dire dans le radical de Jacobson), et si M est un A-module de type fini avec $M = IM$, alors $M = (0)$.*

Démonstration. On applique Cayley-Hamilton avec $\phi = \mathrm{id}$. Cayley-Hamilton nous donne l'existence d'un $a \in I$ tel que pour tout $x \in M$, $(1+a)x = 0$. Mais $(1+a)$ est inversible car I est contenu dans tous les idéaux maximaux de A. Donc $M = (0)$. □

Démonstration. (Du cas général). Le A-module $N' = M/N$ est de type fini et vérifie $N' \subset IN'$. On applique alors le premier corollaire : il existe $a \in I$ tel que $(1+a)N' = (1+a)M/N = (0)$, i.e. on a $(1+a)M \subset N$. □

Nous continuons avec la définition d'un anneau régulier, qui va donc nous servir pour définir ce qu'est un schéma régulier. Ici, le lemme de Nakayama va déjà nous servir, pour prouver qu'un anneau régulier est réduit.

6.3.38. Définition. Un anneau local noethérien A est dit **régulier** si le cardinal minimal d'une partie génératrice de son idéal maximal m est égal à sa dimension de Krull.
Un anneau A noethérien est dit **régulier** si la localisation en chacun de ses idéaux premiers est régulier.

6.3.39. Proposition. *Un anneau local A de corps résiduel k est régulier ssi* $\dim_k(m/m^2) = \dim_{Krull}(A)$.

Démonstration. Cela revient à montrer que m/m^2 est engendré par d éléments ssi m est engendré par d éléments. Si m est engendré par d élément, alors le quotient aussi (prendre les classes de ces éléments).
Réciproquement supposons que m/m^2 est engendré par d éléments, $\overline{x_1}, \ldots, \overline{x_d}$. Soit $x \in m$. Alors $\exists a_1, \ldots, a_d \in A$, $\overline{x} = \sum a_i \overline{x_i}$. Alors $x - \sum a_i x_i \in m^2$. Soit alors $n =< x_1, \ldots, x_d > \subset m$. Alors $\overline{m/n = m.m/n}$: En effet : une inclusion évidente, et dans l'autre sens, si $x \in m$, alors $\overline{x} = \overline{x - \sum a_i x_i}$ dans le quotient par n, mais $x - \sum a_i x_i \in m^2$ i.e. $\overline{x} \in m.m/n$. Par le lemme de Nakayama, on a $m/n = 0$. □

Notre but est de montrer qu'un anneau régulier est réduit. On va montrer qu'un anneau régulier est intègre. Pour cela, on a besoin de plusieurs lemmes.

6.3.40. Proposition. *Soit A un anneau. Tout idéal premier contient un idéal premier minimal.*

Démonstration. Soit I un idéal premier d'un anneau R et $\mathcal{P}$ l'ensemble des idéaux premiers de R contenus dans I. On ordonne partiellement P via $Q' \leq Q$ ssi $Q \subset Q'$ pour $Q', Q \in P$.. On peut utiliser le lemme de Zorn à condition de montrer que toute chaîne dans P admet une borne supérieure. Soit donc $\mathcal{C}$ une telle chaîne. L'ensemble $Q := \cap_{C \in \mathcal{C}} C$ est un idéal de R inclus dans I. Montrons que c'est un idéal premier : Soit donc $x, y \in R$ tels que $xy \in Q$ mais $x \notin Q$. Alors $x \notin P'$ pour un certain idéal $P' \in \mathcal{C}$. Remarquons que P' étant premier et $xy \in Q \subset P'$, on a $y \in P'$. Pour tout $P'' \in \mathcal{C}$, on a soit $''P \subset P'$, soit $P' \subset P''$. Dans le premier cas on a $x \notin P''$ donc $y \in P''$. Dans le second cas on a $y \in P' \subset P''$ donc on a à nouveau $y \in P''$. Or, P'' étant quelconque dans $\mathcal{C}$, on conclut $y \in Q$ et donc Q est bien un idéal premier.
Il est clair que $Q \in P$ est une borne supérieure pour $\mathcal{C}$. Le lemme de Zorn s'applique et fournit un élément maximal dans P et cet élément est un idéal premier minimal de R. □

6.3.41. Proposition. *Dans un anneau noethérien R, il y a un nombre fini d'idéaux premiers minimaux.*

Démonstration. Nous allons montrer qu'il existe des idéaux premiers $P_1, \ldots, P_n$ de R tels que
$P_1 P_2 \ldots P_n = 0$. Supposons qu'aucun produit d'idéaux premiers de R ne soit nul.
Soit Z l'ensemble des idéaux de R qui ne contiennent pas un produit fini d'idéaux premiers. L'idéal nul étant dans Z, on a $Z \neq \emptyset$.
L'hypothèse de noethérianité montre qu'il existe un élément maximal $M \in Z$. Aucun produit fini d'idéaux premiers n'est contenu dans M (car $M \in Z$) mais tout idéal non nul contenant M contient un produit fini d'idéaux premiers (maximalité de M dans Z). En particulier M lui-même n'est pas premier donc il existe des idéaux I, J de R tels que $(I+M)(J+M) \subset M$ et $M \subsetneq I+M$, $M \subsetneq J+M$. La maximalité de M montre qu'il existe des idéaux premiers $P_1, \ldots, P_n$ et $Q_1, \ldots, Q_l$ tels que $P_1 \ldots P_n \subset I+M$ et $Q_{1l} \subset J+M$. On conclut que $P_1 \ldots P_n Q_{1l} \subset M$ ce qui contredit $M \in Z$.
Donc, il existe $P_1, \ldots, P_n$ des idéaux premiers de produit nul. Soit maintenant Q un idéal premier minimal. Alors Q contient le produit $P_1 \ldots P_n$, donc Q contient l'un des P_i, donc $P_i = Q$. Ainsi il y a au plus n idéaux premiers minimaux. □

6.3.42. Lemme. *(D'évitement des idéaux premiers)*
Soit A un anneau commutatif. Soit I un idéal de A contenu dans la réunion d'un nombre fini d'idéaux premiers $P_1, \ldots, P_n$. Alors I est contenu dans l'un des P_i.

Démonstration. Par récurrence sur n. Si $n = 1$ on n'a rien à faire.
On suppose le lemme vrai jusqu'à $n-1$. Soit I un idéal de A inclus dans $P_1 \cap \cdots \cap P_n$ avec P_i idéaux premiers. Par hypothèse de récurrence, pour tout $k \leq n$, il existe x_k dans I et n'appartenant pas à la réunion des autres P_i. On a alors $x_k \in P_k$. Considérons l'élément $x = x_n + x_1 x_2 \ldots x_{n-1}$ de I. On a $x_n \in P_n$ et $x_1 x_2 \ldots x_{n-1} \notin P_n$ (car P_n est premier) donc $x \notin P_n$ et, pour tout $k < n$, $x_n \notin P_k$ et $x_1 x_2 \ldots x_{n-1} \in P_k$ donc $x \notin P_k$. Ainsi, x n'appartient à aucun P_i. Cette contradiction termine la démonstration. □

6.3.43. Corollaire. *Un anneau régulier est réduit.*

Démonstration. Soit A un anneau régulier. Tout localisé de A est régulier. Or A est réduit si et seulement si A_p est réduit pour tout $p \in \mathrm{Spec}(A)$. On peut donc supposer A local, d'idéal maximal m. On va montrer que A est en fait intègre. On fait une récurrence sur la dimension de Krull de l'anneau A.
(I) : Si A est de dimension 0 alors par hypothèse l'idéal maximal est réduit à l'idéal nul et donc A est un corps donc réduit.
(H) : On suppose la propriété vraie pour tout anneau de dimension $d-1$. Soit alors A un anneau de dimension $d > 0$. Alors, par le lemme de Nakayama, $m^2 \neq m$ (sinon $m = 0$, impossible). De plus, l'ensemble des idéaux premiers minimaux de A est fini (car A est noethérien).
Maintenant, supposons que m soit contenu dans l'union de m^2 et des idéaux premiers minimaux. Alors, m est contenu dans un idéal premier minimal, i.e. A a une dimension de Krull nulle : impossible.
Donc, il existe $x \in m$ tel que $x \notin m^2 \cup_{i=1}^{p} p_i$ avec p_i idéal minimal.
Soit $S = A/(x)$ et $N = mS$. Alors N est l'unique idéal maximal de S. Or, $\dim(S) < \dim(A)$, on a même $\dim(S) = d-1$ Maintenant N/N^2 est l'image propre d'un morphismme de m/m^2 donc il peut être engendré par $(d-1)$ éléments. Par le lemme de Nakayama, N peut aussi être engendré par $(d-1)$ éléments.

Donc S est un anneau local régulier de dimension $d-1$. Par hypothèse de récurence, il est donc intègre. Donc (x) est premier. Mais comme x n'est dans aucun idéal premier minimal, il existe un idéal premier minimal Q contenu strictement dans (x).
Soit $y \in Q$. On peut écrire $y = ax$ avec $a \in A$. Mais comme $x \notin Q$ et Q premier, avec $a \in Q$. Alors $Q = xQ$. Le lemme de Nakayama nous donne alors que $Q = 0$ et donc A est intègre. □

Un autre type d'anneau utile pour la suite est le suivant :

6.3.44. Définition. On dit qu'un anneau A est un anneau **artinien** si c'est un A-module artinien, autrement dit, si toute suite décroissante d'idéaux de A est stationnaire. Cela équivaut à dire que tout ensemble non vide d'idéaux de A admet un élément minimal (pour la relation d'inclusion).

6.3.45. Exemple. -Tout anneau fini est artinien.
-Tout corps est artinien.
-$\mathbb{Z}$ ne l'est pas :

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 2^2\mathbb{Z} \supsetneq 2^3\mathbb{Z} \supsetneq \dots$$

est une suite décroissante d'idéaux non stationnaire.

6.3.46. Proposition. *Un anneau commutatif est artinien si et seulement si il est noethérien et de dimension de Krull nulle.*

Algèbres étales sur un corps

Nous avons besoin de définir la notion d'algèbre étale pour comprendre ce qu'est un schéma étale (disons sur un corps), ce qui permettra alors de parler de revêtement étale et donc de groupe simplement connexe.

6.3.47. Définition. Un corps k est **séparablement clos** si toute extension finie séparable de k est triviale, c'est-à-dire égale à k.

Une **clôture séparable**, notée k^{sep} de k est une extension algébrique séparable (non nécessairement finie) qui est séparablement close. Cela revient à dire que si L est une extension algébrique séparable de k contenant k^{sep}, alors $L = k^{sep}$.

6.3.48. Exemple. Un corps algébriquement clos est sa propre clôture séparable.

6.3.49. Définition. Une k-algèbre A est dite **diagonalisable** ssi $\exists n \in \mathbb{N}, A \simeq k^n$ (isomorphisme d'algèbre).
On dit que A est **étale** si $A \otimes_k k'$ est diagonalisable, en tant que k'-algèbre pour une extension k' de k.

6.3.50. Remarque. Une k-algèbre étale est toujours un k-espace vectoriel de dimension finie : en effet si $(e_i)_{i\in I}$ est une base de A en tant que k-espace vectoriel, alors $(e_i \otimes 1)_{i\in I}$ est une base de $A \otimes_k k'$ sur k'.

La propriété d'être étale est invariante par changement de base :

6.3.51. Proposition. *Si A est étale sur k, alors $k' \otimes_k A$ est étale sur k', pour tout corps k' contenant k.*

Démonstration. Soit L tel que $L \otimes_k A \simeq L^m$. Soit L' un corps contenant k' et L (prendre par exemple le quotient de $k' \otimes L$ par un idéal maximal). Alors on a :

$$L' \otimes_{k'} (k' \otimes_k A) \simeq L' \otimes_k A \simeq L' \otimes_L L \otimes_k A \simeq L' \otimes_L L^m \simeq L'^m.$$

□

Nous donnons maintenant une caractérisation des algèbres étales. Le c) est par exemple utile pour mieux visualiser cette notion.

6.3.52. Proposition. *Soit A une k-algèbre finie.*
Les assertions suivantes sont équivalentes :
a) A étale
b) $k' \otimes_k A$ est réduit pour tout corps k' contenant k
c) A est le produit fini de corps, extensions séparables de k.

Démonstration. $a) \Rightarrow b)$ Soit L un corps contenant k. Par hypothèse, il existe L' corps contenant k tel que $A \otimes k'$ soit diagonalisable. Soit L'' un corps contenant L' et L (prendre par exemple le quotient de $L' \otimes L''$ par un idéal maximal). Alors $L'' \otimes_k A = L'' \otimes_{k'} k' \otimes_k A$ est diagonalisable, et l'application $L' \otimes_k A \to L'' \otimes A$, provenant de l'inclusion $L \subset L''$ est injective. Ainsi, $L \otimes_k A$ est réduit.
$b) \Rightarrow c)$ Soit S un ensemble d'idéaux maximaux de A. Grâce au théorème des restes chinois, on a un application surjective $A \to \prod_{M \in S} A/M$ avec noyau $\cap_{M \in S} M$. Or, d'après le lemme de Zariski, A/m est une extension finie de k, pour tout idéal maximal m. Ainsi, A a un nombre fini d'idéaux maximaux. Si on prend pour S l'ensemble de tous les idéaux maximaux de A, leur intersection est le nilradical N de A, et donc A/N est un produit fini de corps. De plus, l'application : $A \to L \otimes_k A$, $a \mapsto 1 \otimes a$ est injective. Ainsi, si $L \otimes_k A$ est réduit, alors A l'est aussi, et donc, d'après ce que l'on vient de dire, A est produit d'un nombre fini de corps. Soit k' un facteur de A. Si k' n'est pas une extension séparable de k, alors k est de caractéristique $p > 0$ et il existe $u \in k'$, dont le polynôme minimal est de la forme $f(X^p)$, avec $f \in k[X]$. Soit L un corps contenant k et tel que tous les coefficients de f sont des puissances $p - ieme$ d'éléments de L. Alors

$$L \otimes_k k[u] \simeq L \otimes_k (k[X]/f(X^p)) \simeq L[X]/(f(X^p))$$

ui n'est pas réduit car $f(X^p)$ est une puissance p-ieme dans $L[X]$. Alors $L \otimes_k A$ n'est pas réduit.
$c) \Rightarrow a)$ On peut supposer que A est une extension séparable de k. D'après le théorème de l'élément primitif ($k \subset A$ finie et séparable), il existe $u \in A$, tel que $A = k[u]$. On appelle f le polynôme minimal (séparable !) de u. On a alors $f(X) = \prod (X - u_i)$, avec $u_i \neq u_j, i \neq j$, dans une extension l de k. Alors

$$L \otimes_k A \simeq L \otimes_k k[X]/(f) \simeq L[X]/(f)$$

et, grâce au théorème chinois, on a $L[X]/(f) \simeq \prod_i L[X]/(X - u_i) \simeq \prod_i L$, et ainsi A est étale. □

6.3.53. Corollaire. *Une k-algèbre A est étale ssi $k^{sep} \otimes_k A$ est diagonalisable.*

Démonstration. Dans la preuve de $c) \Rightarrow a)$, on voit que $L \otimes_k A$ diagonalisable si un certain polynôme se scinde dans L. Par définition, tous les polynômes séparables se scindent dans k^{sep}. □

6.3.54. Exemple. Pour tout corps k, k^n est une k-algèbre étale.

6.3.55. Proposition. *Pour tout corps k, $k[X]/(f)$ est étale ssi f est séparable.*

Démonstration. On écrit $f = \prod f_i^{m_i}$ la décomposition de f en facteurs irréductibles. Alors avec le théorème chinois, $k[X]/(f) = \prod k[x]/f_i^{m_i}$. Or, $k[x]/f_i^{m_i}$ est un corps ssi $m_i = 1$, et est séparable ssi f_i l'est. Donc $k[X]/(f)$ étale ssi f séparable. □

Références

[DG] M. Demazure et P. Gabriel, *Groupes algébriques. Tome I : Géométrie algébrique, généralités, groupes commutatifs*, Masson Cie, Éditeur, Paris ; North-Holland Publishing Co., Amsterdam, 1970.

[DU] A. Ducros, *Introduction à la théorie des schémas*. Polycopié issu de deux cours du master Mathématiques fondamentales de l'UPMC. Lien ici.

[EGA1] A.Grothendieck, *Éléments de géométrie algébrique*. I. Le langage des schémas. Publications mathématiques, n°4. 1960.

[GW] U. Görtz, T. Wedhorn, *Algebraic geometry I. Schemes with examples and exercises*, Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010.

[HR] R.G. Heyneman D.E. Radford, *Reflexivity and coalgebras of finite type*. Journal of algebra. 28, 215-246 (1974).

[JA] J.C. Jantzen, *Representations of algebraic groups*. Mathematical Surveys and Monographs, (2003) Vol. 107. American Mathematical Society, Providence, RI, second edition.

[MIL] J. Milne, *Algebraic groups. The theory of group schemes of finite type over a field*, Cambridge Studies in Advanced Mathematics, 170. Cambridge University Press, Cambridge, 2017.

[RAY] M. Raynaud, *Passage au quotient par une relation d'équivalence plate*, Proc. Conf. Local Fields (Driebergen, 1966) pp. 78–85 Springer, 1967.

[RO] M. Romagny, *Géométrie algébrique 2*. Polycopié issu de cours du master Mathématiques à l'UPMC. 2011-2012. Lien ici.

[SGA3.1] *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie 1962–64. A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre. Revised and annotated edition of the 1970 French original. Edited by Philippe Gille and Patrick Polo. Documents Mathématiques 7, Société Mathématique de France, 2011.

[SGA3.2] *Schémas en groupes (SGA 3). Tome II. Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics 152, Springer-Verlag, 1970.

[SU.1] J. Sullivan, *Simply connected groups, the hyperalgebra, and Verma's conjecture*, Amer. J. Math. 100 (1978), no. 5, 1015–1019.

[SU.2] J. Sullivan, *Representations of the hyperalgebra of an algebraic group*, Amer. J. Math. 100 (1978), pp. 643-652.

[SW] M.E. Sweedler, *Hopf algebras*. Mathematics Lecture Note Series. W. A. Benjamin, (1969) Inc., New York and Amsterdam.

[TA.1] M. Takeuchi, *On coverings and hyperalgebras of affine algebraic groups*, Trans. Amer. Math. Soc. 211 (1975), 249–275.

[TA.2] M. Takeuchi, *Tangent coalgebras and hyperalgebras*, I, Japan. J. Math (1974).