الجمهوريـة الجزائـريـة الديمقراطيـة الشعبيـة
République Algérienne Démocratique et Populaire
وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :……

Centre Universitaire
Abd elhafid Boussouf Mila

Institut des sciences et de la technologie **Département de Mathématiques et Informatique**

Mémoire préparé en vue de l'obtention du diplôme de
Master

En: Mathématiques

Spécialité: Mathématiques Fondamentales

Schémas en groupe d'ordre premier

Préparé par : Wissame BENABBAS
Hayette BENHAMMADA

Soutenue devant le jury

Wahida FADEL	**MAA**	**C. U. Abdelhafid Boussouf, Mila**	**Président**
Mohamed KHALFAOUI	**MAA**	**C. U. Abdelhafid Boussouf, Mila**	**Rapporteur**
Monir BOUGUEBINA	**MAA**	**C. U. Abdelhafid Boussouf, Mila**	**Examinateur**

Année universitaire :2022/2023

REMERCIMENTS

Nous tenons à remercier avant tout ALLAH le tout-puissant

de nous avoir donné la volonté, la santé et

le courage pour réaliser ce travail.

Tout d'abord, nos respectueux remerciements à tous aux membres du jury qui

nous ont fait l'honneur de participer à l'évaluation de notre travail,

en l'occurrence le président Mme Wahida FADEL et l'examinateur

Mr Monir BOUGUEBINA qui ont accepté de porter un regard bienveillant sur

notre travail.

Nous remercions chaleureusement notre rapporteur Mr Mohamed KHALFAOUI

qui a supervisé notre travail, pour sa tolérance, son aide précieuse , ses

conseils éclairés dans la direction de notre travail, sa grande disponibilité et son

immense gentillesse .

Sans oublier tous nos enseignants , nos camarades étudiants et administrateurs

du département de mathématiques et notamment nos professeurs de mathématiques fondamentales.

DÉDICACE

C'est avec une joie immense et le cœur ému que je dédie ce mémoire à

Mon cher papa *Karim* qui a été mon ombre durant toutes les années des

études et à mis ma disposition tous les moyens nécessaire

pour que je réussisse.

Ma chère maman *Nadia* qui m'a donné la vie, le symbole de tendresse qui

s'est sacrifiée pour mon bonheur et ma réussite.

Mon frère Nassim , mes sœur Boutheina et Malak pour leur

soutien constant.

Mon binôme * Hayette* pour son soutien moral et pour avoir été formidable tout au long de ce travail pour tous ceux qui m'ont aidé pendant mes études

Wissame

DÉDICACE

Je dédie ce modeste travail :

Mes parents,grâce à leurs tenduragement et leurs grands encouragements et leurs grands sacrifices

Ils ont pu créer le climat aoectueux et propice à la poursuite de mes études.

A mes sœurs, Sanâ, Douâ et mon frère Hamza, Mouad, Farès.

A mon meilleurs ami et mon âme soeur Bouchra

Sans oublier de mentionner ma copine Wissame,

la famille et toute amies et mes collègues.

Tout mes enseignants de département des mathematique et informatique.

Hayette

ملخص

هدفنا في هذه المذكرة هو دراسة مخططات زمر ذات رتبة أولية p لبعض الحلقات الشهيرة، حيث قمنا بتصنيف هذه المخططات بالاعتماد على نظرية التصنيف.

الكلمات المفتاحية: مخططات زمر، فئة، زمر تآلفية، ثنائية كارتي، رتبة أولية.

Résumé

Notre but dans ce mémoire est d'étudier les schémas en groupes d'ordre premier p sur un anneau de base ; et donner une classification de cette schémas en utilisant certaines théorèmes (vecteur de Witt, théorème de classification).

Mots clés : Schéma en groupe, catégorie, groupe affine, dualité de Cartier, ordre premier.

Abstract

Our aim in this is to study groups schemes of prime order p over a base ring, and to give a classification of this scheme using some theorems (Witt vector, classification theorem).

Key words: Group schemes, category, affine group, Cartier duality, prime order.

TABLE DES MATIÈRES

INTRODUCTION

La géométrie algèbrique est principalement née de l'étude des équations polynomiales à coefficients dans les nombres réels. Au xix^e siècle, il est devenu clair (avec les travaux de Jean-Victor Poncelet et Bernhard Riemann) que la géométrie algèbrique était simplifiée si l'on travaillait plutôt avec des variétés complexes, c'est-à-dire sur le corps des nombres complexes, qui a l'avantage d'être algèbriquement clos. Deux problèmes ont graduellement attiré l'attention au début du xx^e siècle, motivés en partie par des problèmes en théorie des nombres : peut-on développer la géométrie algèbrique sur un corps algèbriquement clos quelconque. Qu'en est-t-il sur un corps quelconque ? D'autres méthodes étaient nécessaires, car les outils de la topologie et de l'analyse complexe, utilisés pour étudier les variétés complexes, ne semblaient pas s'appliquer dans ces cadres généraux.

Dans les années 1950, Claude Chevalley, Masayoshi Nagata et Jean-Pierre Serre ont étendu les objets de la géométrie algèbrique en généralisant les anneaux de base considérés, motivés en partie par les conjectures de Weil, qui relient la théorie des nombres à la géométrie algèbrique. Le mot schéma a été utilisé pour la première fois dans le séminaire Chevalley en 1956, où Chevalley s'intéressait aux idées de Zariski. Selon Pierre Cartier, c'est André Martineau qui a suggéré à Serre la possiblité d'utiliser le spectre d'un anneau commutatif arbitraire comme fondement de la géométrie algèbrique. En 1958, Alexandre Grothendieck introduit les schémas, puis étudiés en détail dans son traité Éléments de géométrie algèbrique (rédigé en collaboration avec Jean Dieudonné) suivi du Séminaire de géométrie algèbrique du Bois Marie ; un des objectifs était d'établir le formalisme nécessaire à la démonstration des conjectures de Weil, qui nécessitaient notamment une définition souple de variété définie sur un corps fini.

Notre but est de donner une classification des schémas en groupes commutatifs G d'ordre

premier p sur un schéma de base S. Il existe de nombreux de schémas en groupe d'ordre p. La classification complète, sous hypothèse faible, a été obtenue par Oort et Tate dans [6] et c'est l'objet de ce mémoire.

Dans le premier chapitre nous donnerons quelques préliminaires sur les structures algèbriques, leurs propriétés et quelques définitions utilisées dans le deuxième et le troisième chapitre.

Dans le deuxième chapitre, nous donnerons quelques préliminaires sur les schémas en groupe qui sont fondamentalement une généralisation du concept de groupe dans la théorie des schémas. Nous commençons par la définition d'objet de groupe dans une catégorie générale, puis nous expliquons en détail c'est quoi cet objet dans les catégories des schémas affines, en particulier, nous montrons qu'elle coïncide avec le concept d'algèbre de Hopf dans la catégorie des anneaux, et qu'il existe une manière canonique de passer de l'une à l'autre. On continue avec quelques généralités sur les morphismes de schémas en groupes affines et nous donnons aussi la définition de sous-groupe et de groupe quotient puis il suit une section d'exemples. Nous concluons cet chapitre par une section sur les composants connexes d'un schémas en groupes affines finis et localement libres sur un corps.

Dans le dernier chapitre, nous généralisons le concept de schémas affines : nous n'exigeons plus que G soit de la forme Spec A avec A une algèbre de Hopf, mais nous demandons que G soit un schéma sur S avec un morphisme affine $G \to S$. En particulier lorsque l'on écrira $G = SpecA$, A sera un faisceau quasi cohérent d'algèbres sur le schéma S. On demande aussi que tels schémas en groupes aient une dimension première fixe. On commence par un théorème dû à Deligne [6] qui est l'analogue du théorème de Lagrange pour les groupes. Le théorème de Deligne [6] nous permet aussi de considérer une action de $\mathbb{F}_p$ sur nos schémas en groupes.

Après la preuve que tous les schémas en groupes d'ordre premier doivent être commutatifs, (même si ce n'est pas en général vrai par exemple pour groupe d'ordre p^2) nous arrivons au classement de Tate et Oort.

CHAPITRE 1

PRÉLIMINAIRES

1.1 Structures algèbriques

1.1.1 Groupes

Définition 1.1.1 *[11] Un groupe est un couple formé d'un ensemble G et d'une loi de composition* $(x, y) \mapsto xy$ *sur l'ensemble G. Ces données doivent vérifier les trois conditions :*

i) *L'associativité :* $\forall x, y, z \in G : (xy)z = x(yz)$.

ii) *L'existence d'un élément neutre :* $\exists 1 \in G$ *tel que* $\forall x \in G : x1 = 1x = x$.

iii) *L'existence d'un élément inverse pour tout élément du groupe :*

$\forall x \in G : \exists x^{-1} \in G$ *tel que* $x^{-1}x = xx^{-1} = 1$.

Si $x \cdot y = y \cdot x$ la loi de groupe est commutatif.

Proposition 1.1.1 *[11] Il y a unicité du neutre et de l'inverse.*

1.1.2 Sous-groupes

Définition 1.1.2 *[11] Soit G un groupe. Un sous-groupe de G est une partie* $H \subset G$ *tels que :*

★ $1 \in H$.

★ $\forall (g, h) \in H^2, gh \in H$.

★ $\forall g \in H, g^{-1} \in H$.

Proposition 1.1.2 *Soit* $(G, .)$ *est un groupe non trivial* $(\neq e)$ *et* $H \subseteq G$ *alors* $(H, .)$ *est un sous-groupe de G si et seulement si :*

1) $H \neq \emptyset$.

2) $\forall a, b \in H : a \cdot b \in H$(*H est stable pour* $''\cdot''$).

3) $\forall a \in H, a^{-1} \in H$.

Sous-groupe normale

Définition 1.1.3 *[11] Un sous-groupe H de G est dit distingué (ou normal) si et seulement si pour tout* $h, g \in H \times G$, $ghg^{-1} \in H$.

1.1.3 Groupe de type fini

Les sous-groupes engendré par un sous-ensemble

Soit X≠∅ est un sous-ensemble d'un groupe G, on définit $< X >$ le sous-groupe engendré par X par : $< X >$ l'intersection de tous les sous-groupes de G contenant X donc <X> est le plus petit sous-groupe de G contenant X alors pour $X \subseteq S \leq G \Rightarrow < X > \leq S$, de plus, si X est un sous-groupe de G alors $X =< X >$.

Définition 1.1.4 *Soit* $n \in \mathbb{N}^*$, *un groupe engendré par n éléments* $\{x_1, ..., x_n\}$ *est dit* ≪ *de type fini*≫.

Proposition 1.1.3 *Les éléments de <X> s'écris de la forme :*

$x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, ..., x_k^{\varepsilon_k}, \varepsilon_i = \pm 1$.

Tel que : $x_i \in X$ *et* $k \geq 0$.

Définition 1.1.5 *Un groupe engendré par un seul élément x est dit monotone. De plus, si G fini, on dit que G est cyclique.*

Définition 1.1.6 *[11] L'ordre d'un groupe G est son cardinal.*

Proposition 1.1.4 *Un groupe G à exactement deux sous-groupes 1 et G* $\Leftrightarrow$ *G est cyclique d'ordre premier.*

1.1.4 Groupe quotient

Série de composition

Définition 1.1.7 *[1] Soit G un groupe. On appelle série normale une suite finie de sous-groupes de G, telle que chacun d'eux soit sous-groupe invariant du précédent :*

$$\Sigma : G = G_0 > G_1 > .... > G_i > G_{i+1} > .... > G_n = e.$$

Remarque 1.1.1 **1)** *Les groupes* $\frac{G_i}{G_{i+1}}$ *sont appellés ≪quotients≫ (facteurs) de la suite de composition.*

2) *''n'' est dit la longueur de* Σ.

3) *Si* $\forall i \in \overline{0, n-1}$, $G_i \neq G_{i+1}$ *on dit que la suite est strictement décroissante.*

Une série normale :

$$\Sigma' : G = G_0 > G'_1 > .... > G'_i > G_{i+1} > .... > G'_{n'} = e.$$

est dite subdivision de la série Σ *si les termes de* Σ' *contiennent tous les termes de* Σ *et éventuellement d'autres.*

Une série normale sans répétition telle que toute subdivision ait au moins une répétition, s'appelle une série décomposition.

Groupe résoluble

Définition 1.1.8 *[1] On dit qu'un groupe est résoluble quand les groupes facteurs sont tous d'ordre premier.*

Tout sous-groupe d'un groupe résoluble est lui-même résoluble.

Définition 1.1.9 *[11]*

⋆*Soit G un groupe. On appelle commutateur de* $(a, b) \in G^2$ *et on note* $[a, b]$ *le produit* $ghg^{-1}h^{-1}$.

⋆*Le groupe dérivé de G, noté G' est le sous-groupe engendré par les commutateurs de G.*

Remarque 1.1.2 *G ablien* $\Leftrightarrow \forall a, b \in G, [a, b] = 1$.

Généralement, on défini le sous-groupe dérivée de G d'ordre n : $G^n = \{[a, b], a, b \in G^{n-1}\}$.

Théorème 1.1.3 *Si G est un groupe résoluble, alors tout sous-groupe de G et tout quotient de G est résoluble.*

Théorème 1.1.4 *Un groupe $G \neq (e)$ est résoluble si et seulement s'il contient un sous-groupe normale propre N, tel que N et $\frac{G}{N}$ sont résolubles.*

1.1.5 Groupes nilpotents

1)Notion de suite centrale :

Définition 1.1.10 *Pour un groupe G une suite de composition :*

$\Sigma : G = G_0 \geq G_1 \geq .... \geq G_{n-1} \geq G_n = (e)$ *est dit centrale si* Σ *est une suite normale.*

Définition 1.1.11 *[3] Soit le groupe G, on dit que G est nilpotent si et seulement si G admet une suite centrale.*

1) La longueur de la suite centrale est la classe de nilpotence du groupe G, on la note C.

2) Le groupe nilpotent de classe $C = 0$ est le groupe trivial {e}.

3) Le groupe nilpotent de classe $C = 1$ est le groupe abélien.

1.1.6 Action de groupe

Définition 1.1.12 *[11]*

Une action (ou une opération) (à gauche) d'un groupe G sur un ensemble X est une application :

$$f = \begin{cases} G \times X \to X \\ (g, x) \mapsto gx \end{cases}$$

telle que $\forall x \in X, f(1, x) = x$ *et* $\forall (x, g, h) \in X \times G^2, f(gh, x) = f(g, f(h, x))$.

1.1.7 Anneaux et corps

Anneaux

Définition 1.1.13 *[1] Un anneau est un triplet $(A, +, \cdot)$ formé d'un ensemble A et de deux applications $+, \cdot : A \times A \to A$ appelées respectivement l'addition et la multiplication vérifiant les axiomes suivants :*

1) $(A, +)$ *est un groupe abélien, on note* 0_A *(ou simplement 0) son élément neutre (appelé zéro) et* $(-a)$ *l'inverse d'un élément* $a \in A$.

2) $(A, \cdot)$ *est un monoïde, on note* 1_A *(ou simplement 1) son élément neutre (appelé unité).*

3) *La multiplication est distributive par rapport à l'addition i.e.*

$a\cdot(b+c) = a\cdot b + a\cdot c \; et (b+c)\cdot a = b\cdot a + c\cdot a, a, b, c \in A.$

Un anneau A est dit commutatif si $ab = ba, a, b \in A.$

Définition 1.1.14 *(Idéal) [1] Soit A un anneau (commutatif). Un idéal de A est un sous-ensemble* $I \subset A$ *tel que* $a' - b' \in I, a', b' \in I$ *et* $aa' \in I, a \in A, a' \in I$. *On notera* $\mathcal{I}_A$ *l'ensemble des idéaux de A ; l'inclusion ensembliste* $\subset$ *munit* $\mathcal{I}_A$ *d'un ordre partiel. Pour un idéal* $I \subset A$, *on notera* $V^{tot}(I) \subset \mathcal{I}_A$ *le sous-ensemble des idéaux de A qui contiennent I.*

Lemme 1.1.1 *[1] Soit A un anneau. Les propriétés suivantes sont équivalentes :*

1) *Tout idéal* $I \subset A$ *est de type fini.*

2) *Toute suite d'idéaux de A croissante pour* $\subset$ *est stationnaire à partir d'un certain rang.*

3) *Tout sous-ensemble non vide d'idéaux de A admet un élément maximal pour* $\subset$.

On dit qu'un anneau A qui vérifie les propriétés équivalente du Lemme 1. 1. 1 est noetherien

Définition 1.1.15 *Le spectre d'un anneau A est l'ensemble des idéaux premiers de A, noté 'Spec'.*

L'ensemble des idéaux maximaux de A noté 'Spm' et on dit c'est le spectre maximal de A.

Définition 1.1.16 *(A-module) [1] Soit A un anneau, un A-module (à gauche) est un couple* $((M, +), \cdot)$ *formé d'un groupe abélien* $(M, +)$ *(on notera 0 son élément neutre et* $(-m)$ *l'inverse d'un élément* $m \in M$*) et d'une application* $\cdot : A \times M \to A$ *appelées la multiplication extérieure vérifiant les axiomes suivants :*

1) $a\cdot(m+n) = a\cdot m + a\cdot n, a \in A, m, n \in M.$

2) $(a+b)\cdot m = a\cdot m + b\cdot m, a, b \in A, m \in M.$

3) $(a\cdot b)\cdot m = a\cdot(b\cdot m), a, b \in A, m \in M.$

4) $1\cdot m = m, m \in M.$

Définition 1.1.17 *(Morphisme d'anneaux) [1] Etant donnés deux anneaux A, B, un morphisme d'anneaux est une application* $\phi : A \to B$ *qui induit à la fois un morphisme de groupes* $\phi : (A, +) \to (B, +)$ *et des monoides unitaires* $\phi : (A, \ldots) \to (B, \cdot)$ *i.e qui vérifie :*

1) $\phi(a+b) = \phi(a) + \phi(b), a, b \in A.$

2) $\phi(ab) = \phi(a)\phi(b), a, b \in A$ *et* $\phi(1) = 1$.

Définition 1.1.18 *(A-algèbre) [1] Soit A un anneau commutatif. Une A-algèbre est un couple* (B, ϕ) *où B est un anneau et* $\phi : A \to B$ *est un morphisme d'anneaux tel que* $im(\phi) \subset Z(B)$. *On notera en général* $\phi : A \to B$ *ou simplement (lorsque la donnée de* $\phi : A \to B$ *ne peut prêter à confusion) B la A-algèbre* (B, ϕ). *Etant donnés deux A-algèbres* $\phi_B : A \to B$, $\phi_C : A \to C$, *un morphisme de A-algèbres est un morphisme d'anneaux* $\phi : B \to C$ *tel que* $\phi \circ \phi_B = \phi_C$. *On remarquera que l'application identité* $Id : B \to B$ *est un morphisme de A-algèbres et que si* $\phi : B \to C$ *et* $\psi : C \to D$ *sont des morphismes de A-algèbres alors* $\psi \circ \phi : B \to D$ *est un morphisme de A-algèbres.*

Définition 1.1.19 *(Étale) [9] Un k-algèbre finie A est étale si A est un produit fini* $A = \prod_i k_i$ *pour* $k \subset k_i$ *une extension de corps séparable finie.*

Définition 1.1.20 *(Comultiplication) [5] Une comultiplication sur un k-algèbre A est un homomorphisme de k-algèbre* $\Delta : A \to A \otimes A$.

Définition 1.1.21 *(Élément nilpotent) [1] On dit qu'un élément* $a \in A$ *est nilpotent s'il existe un entier* $n \geq 1$ *tel que* $a^n = 0$ *et, si* $a \neq 0$, *on dit que le plus petit entier* $n \geq 1$ *tel que* $a^{n-1} \neq 0$ *et* $a^n = 0$ *est l'indice de nilpotence de a (on dit parfois que 0 est d'indice de nilpotence 1). On note* $\mathcal{N}_A \subset A$ *l'ensemble des éléments nilpotents de A.*

Corps et idéaux maximaux

Définition 1.1.22 *[1] Le singleton* $\{0\}$ *et A sont des ideaux de A. En général, un anneau contient beaucoup d'idéaux. L'ensemble des idéaux et leur 'position' dans l'anneau mesure la complexité de celui-ci. En ce sens, les anneaux les plus simples sont les corps.*

Produit tensoriel

Définition 1.1.23 *Le produit tensoriel est le produit de chaque composante d'un tenseur par chaque composante d'un autre tenseur.*

k-algèbres affines

Définition 1.1.24 *[5] Une k-algèbre affine est une k-algèbre de type fini A telle que* $k^{al} \otimes_k A$ *soit réduite. Si A est affine, alors* $K \otimes_k A$ *est réduit pour tout corps K contenant k ; en particulier, A lui-même est réduit. Lorsque k est parfait, toute k-algèbre réduite de type fini est une k-algèbre affine. Le produit tenseur de deux k-algèbres affines est à nouveau une k-algèbre affine.*

Définition 1.1.25 *Soit R un anneau commutatif.*

L'anneau R[[X]] des séries formelles sur R en une indéterminée X est le groupe abélien $(R^{\mathbb{N}}, +)$ *des suites à valeurs dans R, muni d'une certaine loi interne de multiplication.*

CHAPITRE 2

SCHÉMA EN GROUPE

2.1 Préliminaires sur le schéma en groupe

2.1.1 Objets de groupe dans une catégorie

Définition 2.1.1 *(Catégorie) [8]*

Une catégorie C peut être décrite comme étant la donnée d'une "classe" d'objets telle qu'à chaque couple ordonné A, B d'objets de C soit associé un ensemble, noté $Hom(A, B)$ ou $Hom_C(A, B)$. Pour deux couples d'objets distincts (A, B) et (A', B'), les ensembles $Hom(A, B)$ et $Hom(A', B')$ sont supposés disjoints. Les éléments de $Hom(A, B)$ sont les morphismes de A vers B. On écrit $f : A \to B$ si $f \in Hom(A, B)$; l'objet A, appelé source de f, est noté $S(f)$; l'objet B, appelé but de f, est noté $B(f)$. D'autre part, il existe une loi de composition entre les morphismes de telle sorte que si f et g sont deux morphismes et si $B(f) = S(g)$, il existe un morphisme unique de $S(f)$ vers $B(g)$, noté gf. Cette loi de composition est assujettie aux axiomes suivants :

- ⋆ *Elle est associative : c'est-à-dire si $f : A \to B$, $g : B \to C$, $h : C \to D$, alors $h(gf) = (hf)g$.*
- ⋆ *Pour tout objet A, il existe un morphisme, dit morphisme identité ou identique : $1_A : A \to A$, tel que si $f : A \to B$ et $g : C \to A$, alors $f1_A = f$ et $1_A g = g$.*

L'unicité, pour chaque objet, du morphisme identique, résulte de l'associativité.

Dans la définition, le mot "classe" est pris au sens de la théorie des ensembles de Gödel-Bernays [7] ; cette théorie permet de former la classe de tous les ensembles ; on évite ainsi les difficultés qu'il y aurait à parler de "l'ensemble de tous les ensembles". Si la classe des objets de C est un ensemble, on dit que C est une petite catégorie.

Définition 2.1.2 *(Objet initial. Objet final. Objet nul) [8]*

Un objet O_1 d'une catégorie $\mathcal{C}$ est dit initial si, pour tout objet A de $\mathcal{C}$, il existe un morphisme et un seul $O_1 \to A$. Si O_1 est initial, le seul morphisme $O_1 \to O_1$ est l'identité, et deux objets initiaux de $\mathcal{C}$ sont équivalents.
Dualement, un objet O_2 de $\mathcal{C}$ est dit final si, pour chaque objet A de $\mathcal{C}$, il existe un morphisme et un seul : $A \to O_2$.
Un objet O de $\mathcal{C}$ est dit objet nul s'il est à la fois initial et final. On identifiera, s'il en existe, les objets nuls à un seul et même objet de $\mathcal{C}$.

Foncteurs

Définition 2.1.3 *(Foncteur covariant) [8]*

Soient $\mathcal{C}$ et $\mathcal{C}'$ deux catégories. Un foncteur covariant F de $\mathcal{C}$ dans $\mathcal{C}'$ est constitué par la donnée :

1) *D'une application, notée F, de $Ob(\mathcal{C})$ dans $Ob(\mathcal{C}')$.*

2) *Pour tout couple d'objets X, Y de $\mathcal{C}$ et tout morphisme $f : X \to Y$, d'un morphisme $F(f) : F(X) \to F(Y)$;*
de telle sorte que :

- ⋆ *Si $X \in Ob(\mathcal{C})$, on ait $F(1_X) = 1_{F(X)}$.*
- ⋆ *Si X, Y et $Z \in Ob(\mathcal{C})$ et si $X \xrightarrow{f} Y \xrightarrow{g} Z$ dans $\mathcal{C}$, alors $F(g)F(f) = F(gf)$.*

Définition 2.1.4 *(Foncteur contravariant) [8]*

Soient $\mathcal{C}$ et $\mathcal{C}'$ deux catégories. Un foncteur contravariant de $\mathcal{C}$ dans $\mathcal{C}'$ est un foncteur covariant de la catégorie $\mathcal{C}^\circ$ dans $\mathcal{C}'$.

Définition 2.1.5 *(Foncteur représentable) [8]*

La catégorie Ens des ensembles a pour objets tous les ensembles et pour morphismes toutes les applications avec la composition habituelle.
Un foncteur F d'une catégorie $\mathcal{C}$ dans la catégorie Ens est dit représentable s'il existe un objet X de $\mathcal{C}$ tel que F soit isomorphe au foncteur $Hom(X, .)$. Un tel objet X est appelé un représentant de F. Si Φ est un isomorphisme de F vers $Hom(X, .)$, le couple (X, Φ) est appelé une représentation de F.

Soit $\mathcal{C}$ une catégorie à produits finis arbitraires.

Définition 2.1.6 *[5] Un objet de groupe dans $\mathcal{C}$ est un foncteur représentable G de $\mathcal{C}$ dans un ensemble associé à une transformation naturelle $\mu : G \times G \to G$ telle que pour tout R-algèbres S :*

$$\mu(S) : G(S) \times G(S) \to G(S)$$

est un structure de groupe sur G(S).

Dans la suite, nous voulons montrer que les propriétés du groupe de G(S) passent sur G qui peut être considère dans un certain cas comme un groupe.

Soit $F : \mathcal{C} \to$ ensemble un foncteur contravariant, A un objet de $\mathcal{C}$ et définir $h_A = \hom_{\mathcal{C}}(-, A)$. D'aprés le lemme de Yoneda [1], donner une transformation naturelle $h_A \to F$ est le même que donné un élément de F(A). Plus précisément une transformation naturelle $T : h_A \to F$ définit un élément :

$$a_T = T_A(Id_A).$$

de F(A). Inversement, un élément a de F(A) définit une application :

$$h_A(R) \to F(R).$$

$$f \mapsto F(f)(a).$$

Pour chaque $R \in \mathcal{C}$. L'application est naturelle dans R et donc cette famille des applications est une transformation naturelle.

Lemme 2.1.1 *[5] L'application $T \to a_T$ et $a \to T_a$ sont des bijections inverses $Nat(h_A, F) \cong F(A)$ naturel dans A et F.*

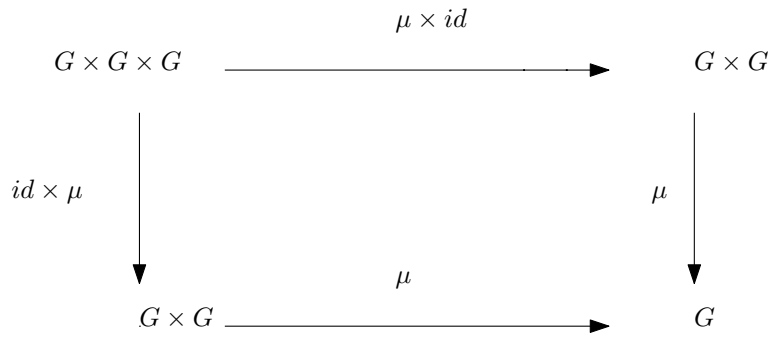
Remarque 2.1.1 *On prend $F = h_B$, dans ce cas on a $\hom(h_A, h_B) \cong \hom(A, B)$. En particulier si G est un objet de $\mathcal{C}$, donner une application $G \times G \to G$ est la même chose que donner une application $h_{G\times G} \cong h_G \times h_G \to h_G$. Il est donc facile de voir que l'ancienne définition de groupe affine coïncide avec cette nouvelle.*

Définition 2.1.7 *[10] Un objet de groupe dans un catégorie $\mathcal{C}$ est une paire constituée d'un objet $G \in Ob(\mathcal{C})$ et un morphisme $\mu : G \times G \to G$ tel que pour tout objet $Z \in Ob(\mathcal{C})$, l'application évidente $G(Z) \times G(Z) \to G(Z)$ définit un groupe où $G(Z) = \hom(Z, G)$.*

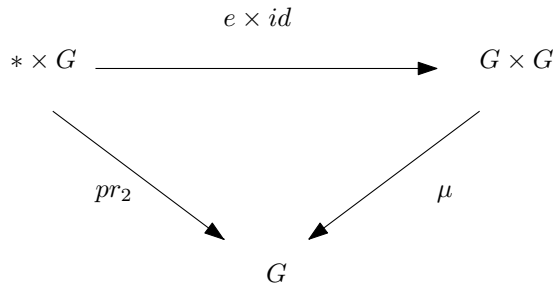
Donc dans la remarque précédente nous avons vu substantiellement que le produit de$h_G(Z)$ passe à une application produit $G \times G \to G$. Il est donc naturel de penser que ce passage se produit aussi pour toutes les autres propriétés concernant le produit.

Proposition 2.1.1 *[10] Un objet G et un morphisme $\mu : G \times G \to G$ définir un objet de groupe si et seulement si les propriétés suivantes sont vérifiées :*

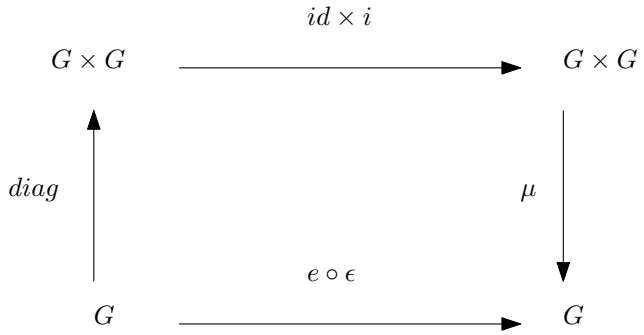
1)Associativité *: Le diagramme suivant est commutatif :*



2)Élément d'identité *: Il existe un morphisme* $e : * \to G$ *où* $*$ *est l'objet final de C, tel que le diagramme suivant commute :*



3)Élément inverse *: il existe un morphisme* $i : G \to G$ *tel que le diagramme suivant commute :*



où ϵ *est le morphisme final.*

Preuve. La partie « si » suit en prenant des points de valeur Z. Pour la partie « seulement si» :

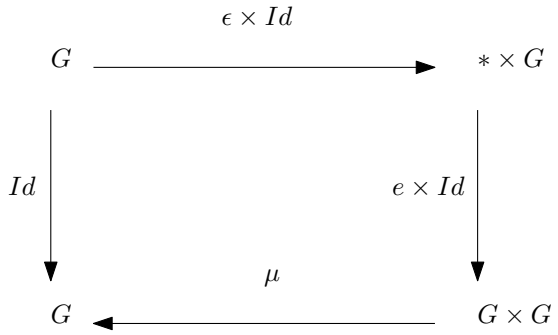
1)Associativité : Prenez $Z = G \times G \times G$ et appliquez l'associativité dans G(Z). En détail prendre p_1 , p_2 , p_3 $G \times G \times G \to G$. Maintenant

$$(p_1 * p_2) * p_3 = \mu(\mu(p_1, p_2), p_3) = \mu(\mu \times id).$$

$$p_1 * (p_2 * p_3) = \mu(p_1, \mu(p_2, p_3)) = \mu(id \times \mu).$$

Nous concluons en utilisant l'associativité du produit.

2)Élément d'identité : Le morphisme $e : * \to G$ est défini comme l'élément d'identité de $G(*)$. Pour toute Z considérons l'application $G(*) \to G(Z)$ défini en composant un morphisme $* \to G$ avec l'unique morphisme $Z \to *$. En particulier en prenant Z = G et en se rappelant que l'application $\epsilon \times Id : G \to * \times G$ est un isomorphisme on obtient

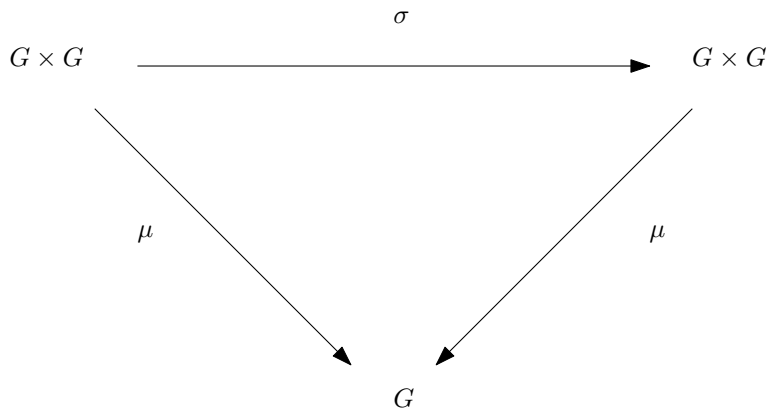


3)Élément inverse Le morphisme $i : G \to G$ est défini comme l'inverse dans le groupe G(G) de l'élément $Id \in G(G)$. Le reste est analogue au précédent.

■

Définition 2.1.8 *Un objet de groupe G est dit commutatif si pour tout objet $Z \in Ob(C)$, $G(Z)$ est un groupe commutatif.*

Lemme 2.1.2 *Un objet de groupe est commutatif si et seulement si le diagramme suivant est commutatif :*



où σ est le morphisme qui échange les deux facteurs.

Preuve. Soit $Z = G \times G$ et on applique la commutativité dans G(Z) à $Id \in (G \times G)(Z)$. En détail : prendre p_1 et p_2 les projections $G \times G \to G$. Maintenant $p_1 * p_2 = \mu \circ (p_1, p_2) = \mu \circ Id = \mu$ et $p_2 * p_1 = \mu \circ (p_2, p_1) = \mu \circ \sigma$. Par la commutativité il s'ensuit que $\mu = \mu \circ \sigma$. ■

2.1.2 Schémas de groupe affine

Soit Ann la catégorie des anneaux noethériens commutatifs avec unité, à partir de maintenant tous les anneaux sont censé être dans Ann. Soit R , $A \in Ann$, on associer un morphisme $R \to A$, alors A est appelé un R-algèbre unitaire. De manière équivalente A est un R-module avec deux morphismes de R-modules $e : R \to A$ et $\mu : A \otimes_R A \to A$ tel que μ soit associatif et commutatif et e induit une unité.

On note la catégorie des R-algèbres unitaires par $R-Alg$ et on a donc une anti-équivalence

$$R - Alg \longleftrightarrow \text{aff.R-Sch.}$$

où aff.R-Sch désigne la catégorie des schémas affines sur *Spec R*. L'objet $* = Spec\ R$ est un objet dans aff.R-Sch.

Définition 2.1.9 *[10] Soit A un anneau unitaire. Un schéma en groupe commutatif affine sur Spec A est un objet de groupe commutatif dans la catégorie des schémas affines sur Spec A.*

Les morphismes associés à l'objet de groupe G correspondent aux homomorphismes suivants de Modules R :

1. $e : R \to A$ *et* $\mu : A \otimes_R A \to A$ *qui sont l'application de la structure de la A-algèbre A.*

2. $\epsilon : A \to R$ *appelé la counité, correspond au morphisme* $* \to G$.

3. $m : A \to A \otimes_R A$, *appelée la comultiplication, correspond à l'application* $\mu : G \times G \to G$.

4. $i : A \to A$, *correspond au morphisme* $G \to G$ *transmit un élément à son inverse.*

En particulier, les axiomes d'un schéma en groupe affine commutatif se traduisent par ceux-ci :

1. μ *est associatif et m est coassociatif :*

$$\mu \circ (Id \otimes \mu) = \mu \circ (\mu \otimes Id).$$

$$(m \otimes Id) \circ m = (Id \otimes m) \circ m.$$

2. μ *est commutatif et m est cocommutatif :*

$$\mu \circ \sigma = \mu.$$

$$\sigma \circ m = m.$$

3. *e est unité pour* μ *et compte pour m :*

$$\mu \circ (e(1) \otimes Id) = Id.$$

$$(\epsilon \otimes Id) \circ m = 1 \otimes Id.$$

4. *m est un morphisme d'anneaux unitaires (préserve le produit et l'unité) :*

$$m \circ \mu = (\mu \otimes \mu) \circ (Id \otimes \sigma \otimes Id) \circ (m \otimes m).$$

$$m(e(1)) = e(1) \otimes e(1).$$

5. *ϵ est le morphisme des anneaux unitaires :*

$$\epsilon \circ \mu = \epsilon \circ \epsilon.$$

$$\epsilon \circ e = Id.$$

6. *i est un morphisme d'anneaux unitaires :*

$$i \circ \mu = \mu \circ (i \otimes i).$$

$$i \circ e = e.$$

7. *i est coinverse pour m :*

$$e \circ \epsilon = \mu \circ (Id \otimes i) \circ m.$$

Définition 2.1.10 *[10] Un A-module A avec des applications μ, ϵ, e, m et i satisfaisant les axiomes ci-dessus est appelé une algèbre A-Hopf cocommutative.*

Nous avons vu que donner un schéma en groupes affine G sur R revient à donner une algèbre de A-Hopf A. En particulier on montre qu'il existe un choix canonique pour A qui s'appelle l'anneau de coordonnées de G et noté $\boldsymbol{O}(G)$.

Soit A^1 le foncteur transmit une A-algèbre S à son ensemble,

$$A^1 : Alg_R \to ensemble.$$

Soit $G : Alg_R \to Grp$ un foncteur, et soit $G_0 = (oubli) \circ G$ le foncteur sous-jacent.

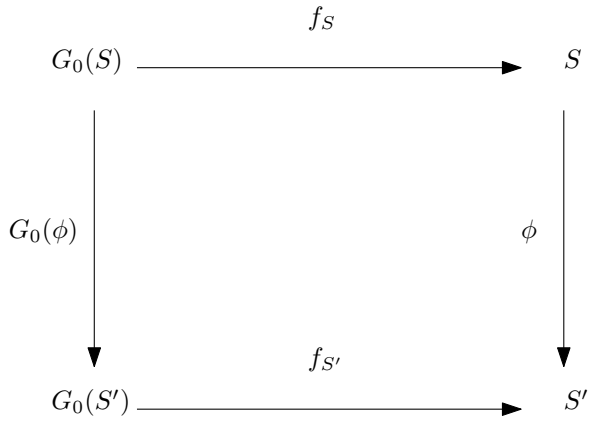
Définissons A comme l'ensemble des transformations naturelles de G_0 à A^1

$$A = Nat(G_0, A^1).$$

Ainsi un élément f de A est une famille d'applications d'ensembles

$$f_S : G_0(S) \to S.$$

tel que, pour tout morphisme de R-algèbres $\phi : S \to S'$, le diagramme



commute. Pour $f, f' \in A$ et $g \in G_0(S)$, définir

$$(f \pm f')_S(g) = f_S(g) \pm f'_S(g).$$

$$(f f')_S(g) = f_S(g) f'_S(g).$$

Avec ces opérations, A devient un anneau commutatif, et même une A-algèbre car chaque $c \in A$ définit une transformation naturelle

$$c_S : G_0(S) \to S.$$

$$c_S(g) = c \text{ pour tout } g \in G_0(S).$$

Un élément $g \in G_0(S)$ définit un morphisme $f_S \to f_S(g)$ où $f_S(g) : A \to S$ des A-algèbres. De cette manière, on obtient une transformation naturelle $\alpha : G_0 \to h^A$ de foncteurs à valeurs ensemblistes.

Remarque 2.1.2 *Dans ce qui suit, pour les groupes affines, nous entendons les schémas en groupes affines.*

Proposition 2.1.2 *[5] Le foncteur G est un groupe affine si et seulement si α est un isomorphisme.*

Preuve. Si α est un isomorphisme, alors certainement G_0 est représentable (et donc G est un

groupe affine). Inversement, supposons que $G_0 = h^B$. Alors

$$A = Nat(G_0, A^1) = Nat(h^B, A^1) \cong A^1(B) = B.$$

Ainsi A ≅ B comme ensemble mais il n'est pas difficile de montrer que c'est un isomorphisme de A-algèbres. Dénoter avec $y : A \cong B$ l'isomorphisme. Le point principal est que dans ce cas, le lemme de Yoneda [1] nous dit $Nat(h^B, A^1)$ sont les « évaluations ». Donc par exemple on vérifie que l'isomorphisme préserve les produits : soient $a, b \in A = Nat(h^B, A^1)$ et $a_1, b_1 \in B$ leur image par l'isomorphisme. Fixons ensuite une A-algèbre S et soit $g \in h^B(S)$:

$$ab(g) = a(g) * b(g) = g(a_1) * g(b_1) = g(a_1 b_1).$$

ce qui implique que $a_1 b_1$ est l'image de ab par l'isomorphisme.

Clairement y induit un autre isomorphisme

$$h^B \to h^A.$$

qui pour une A-algèbre fixe S fonctionne comme

$$g \to g \circ y.$$

si $g \in h^B(S)$. On veut montrer que cet isomorphisme est α. On a

$$\alpha_S : h^B(S) \to h^A(S).$$

$$g \to (a \to a(g)).$$

mais $a(g) = g(b)$ où b = y(a) et donc αet notre isomorphisme coïncident.

Ainsi, pour un groupe affine G, $\mathcal{O}(G) := Hom(G, A^1)$ est un anneau de coordonnées canoniques. Nous savons déjà comment les applications μ, m, ϵ, e, i fonctionne sur cet anneau (c'est-à-dire qu'ils doivent satisfaire tous les axiomes précédents de Hopf-algebras), mais il est aussi intéressant de comprendre leur comportement lorsque A est définit comme $\mathcal{O}(G) = Hom(G, A^1)$.

Si $f_1 \in \mathcal{O}(G)$ et $f_2 \in \mathcal{O}(G)$, alors $f_1 \otimes f_2$ définit une fonction $(f_1 \otimes f_2)_S : G(S) \times G(S) \to S$ selon la règle :

$$(f_1 \times f_2)_S(a, b) = (f_1)_S(a) * (f_2)_S(b).$$

Pour $f \in \mathcal{O}(G)$, $m(f)$ est l'unique élément de $\mathcal{O}(G) \otimes \mathcal{O}(G)$ tel que :

$$(m(f))_S(a,b) = f_S(ab) \text{ pour toute A-algèbre S et } a,b \in G(S).$$

et $\epsilon(f)$ est l'élément $f(1_G)$ de R, de plus i(f) est l'unique élément de $\mathcal{O}(G)$ tel que :

$$(if)_S(a) = f_S(a^{-1}) \text{ pour tout S et tout } a \in G(S).$$

De plus on a :

$$f_S(a^{-1}) = i(a)(f_S) = (a \circ i)(f_S) = (a)(i(f_S)) = (if_S)(a).$$

■

2.1.3 Sous-groupes ;morphismes injectifs

Définition 2.1.11 *[10] Un homomorphisme de groupes affines $\phi : G \to H$ sur Spec S est un morphisme dans aff.S-Sch tel que le morphisme induit $G(Z) \to H(Z)$ est un homomorphisme de groupes pour tout $Z \in$ aff.S-Sch.*

Remarque 2.1.3 *Il existe une définition analogue de l'homomorphisme de groupe affine énoncée en termes des algèbres de S−Hopf ; un morphisme d'algèbres de S−Hopf est une application linéaire S qui "commute" avec les applications μ, m, ϵ, e, i.*

Proposition 2.1.3 *[5] Un morphisme de groupes affines $u : H \to G$ est un isomorphisme si et seulement si :*

1. *L'application $u(R) : H(R) \to G(R)$ est injective pour toutes les S-algèbres R.*
2. *Le morphisme $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ est fidèlement plat.*

Lorsque S est un corps 2) peut être remplacé par : le morphisme $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ est injectif. ***Preuve.*** *Voir la proposition 1. 1 page 87 de [5].* ■

Définition 2.1.12 *[1] Soit $u : H \to G$ un morphisme de groupes affines sur S.*

1. *On dit que u est un monomorphisme si $u(R) : H(R) \to G(R)$ est injectif pour toutes les S-algèbres R.*
2. *On dit que u est une immersion fermée si l'application $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ est surjectif.*

Proposition 2.1.4 *[5] Si $u : H \to G$ est une immersion fermée, alors c'est un monomorphisme. L'inverse est vrai lorsque S est un corps.*

Preuve. Si $u^\natural$ est surjectif, alors deux morphismes quelconques $\mathcal{O}(H) \to R$ qui devient égal lorsqu'il est composé avec $u^\natural$ doit déjà être égal, mais cela signifie que $H(R) \to G(R)$ est injectif.

Supposons maintenant que S soit un corps et que u(R) soit injectif pour tout R. Le morphisme $u^\natural$ se factorise en morphisme des algèbres de Hopf

$$\mathcal{O}(G) \twoheadrightarrow u^\natural(\mathcal{O}(G)) \hookrightarrow \mathcal{O}(H).$$

Soit H' le groupe affine dont l'algèbre de Hopf est $u^\natural(\mathcal{O}(G))$. Alors u se factorise en

$$H \to H' \to g.$$

et l'injectivité de u(R) implique que $H(R) \to H'(R)$ est injective pour toutes les S-algèbres R.

Parce que $\mathcal{O}(H') \to \mathcal{O}(H)$ est injective, la proposition précédente montre que l'application $H \to H'$ est un isomorphisme. ■

Définition 2.1.13 *Un sous-groupe fermé affine H d'un groupe affine G est un foncteur aff.S-Sch→ Groupes tel que :*

1. *H_0 est un sous-foncteur de G_0.*
2. *H(R) est un sous-groupe de G(R) pour toutes les S-algèbres R.*
3. *H est représentable par un quotient de $\mathcal{O}(G)$.*

Définition 2.1.14 *Soit A une algèbre de Hopf. Un idéal I de A est dit idéal de Hopf si :*

1. $m(I) \subseteq I \otimes A + A \otimes I$.
2. $\epsilon(I) = 0$.
3. $i(I) \subseteq I$.

Remarque 2.1.4 *En particulier, le noyau de tout morphisme d'algèbres de Hopf est un idéal de Hopf.*

Proposition 2.1.5 *[5] Les sous-groupes fermés affines d'un groupe affine G en bijection naturel avec les idéaux de Hopf sur $\mathcal{O}(G)$.*

Preuve. Soit H un sous-groupe fermé affine de G et soit $i : H \to G$ l'injection canonique.

Nous avons maintenant l'application relative entre les algèbres

$$Hom(G, A^1) = \mathcal{O}(G) \to \mathcal{O}(H) = Hom(H, A^1).$$

et ainsi

$$f \to (g \to f(i(g))).$$

$$I(H) = \{f \in \mathcal{O}(G) | f(h) = 0 \text{ pour tout } h \in H(R) \text{ et toutes les } S - \text{algbres } R\}.$$

est un idéal de Hopf car est le noyau de $\mathcal{O}(G) \to \mathcal{O}(H)$. Inversement si I est un idéal de Hopf en $\mathcal{O}(G)$, alors le foncteur

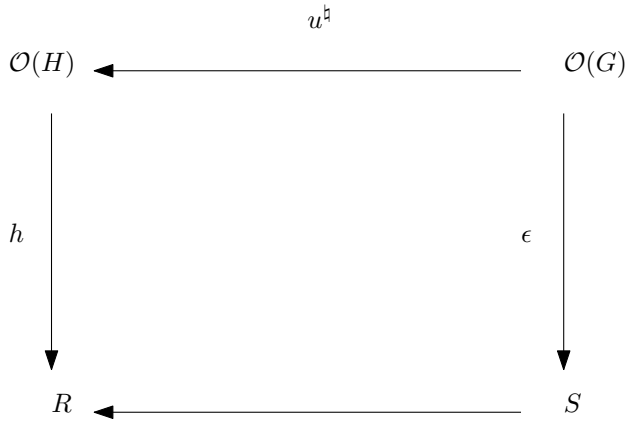
$$R \rightsquigarrow \{g \in G(R) | f(g) = 0 \text{ pour tout } f \in I\}.$$

est un sous-groupe affine de G (il est représenté par $\mathcal{O}(G)/I$). Ces applications sont l'inverse l'une de l'autre. ■

Définition 2.1.15 *[5] Le noyau d'un homomorphisme $u : H \to G$ des groupes affines est le foncteur*

$$R \rightsquigarrow N(R) := Ker(u(R) : H(R) \to G(R)).$$

Soit $\epsilon : \mathcal{O}(G) \to S$ l'élément d'identité de G(S). Alors un élément $h : \mathcal{O}(H) \to R$ de H(R) existe dans N(R) si et seulement si son composé avec $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ se factorise par ϵ :



Soit I_G le noyau de ϵ (l'idéal d'augmentation), et soit $I_G\mathcal{O}(H)$ l'idéal engendré par son image en $\mathcal{O}(H)$. Alors les éléments de N(R) correspondent aux morphismes $\mathcal{O}(H) \to R$ qui sont nuls sur $I_G\mathcal{O}(H)$, c'est-à-dire :

$$N(R) = Hom_{S-alg}(\mathcal{O}(H)/I_G\mathcal{O}(H), R).$$

Proposition 2.1.6 *[5] Pour tout morphisme $H \to G$ de groupes affines, il existe un sous-groupe affine N de H (appelé noyau du morphisme) tel que :*

$$N(R) = Ker(H(R) \to G(R)).$$

pour tout R ; son anneau de coordonnées est $\mathcal{O}(H)/I_G\mathcal{O}(H)$.

Corollaire 2.1.1 *En particulier une application entre groupes affines* $H \to G$ *est un monomorphisme si et seulement si le noyau est trivial.*

2.1.4 Groupes quotients ; homomorphismes surjectifs

Qu'est-ce que cela signifie pour un morphisme de groupes affines $G \to Q$ être surjectif ? On pourrait deviner que cela signifie que $G(R) \to Q(R)$ est surjectif pour tout R, mais cette condition est trop stricte.

Définition 2.1.16 *[5] Un morphisme* $G \to Q$ *des groupes affines est dit surjectif (et Q est appelé un quotient de G) si le morphisme* $\mathcal{O}(Q) \to \mathcal{O}(G)$ *est fidèlement plat. Un homomorphisme surjectif est aussi appelé "application quotient ".*

Proposition 2.1.7 *Un morphisme de groupes affines qui est à la fois une immersion fermée et surjectif est un isomorphisme.*

Preuve. Une application fidèlement plate est injective. Par conséquent, l'application sur les anneaux de coordonnées est à la fois surjective et injectif, et est donc un isomorphisme. ■

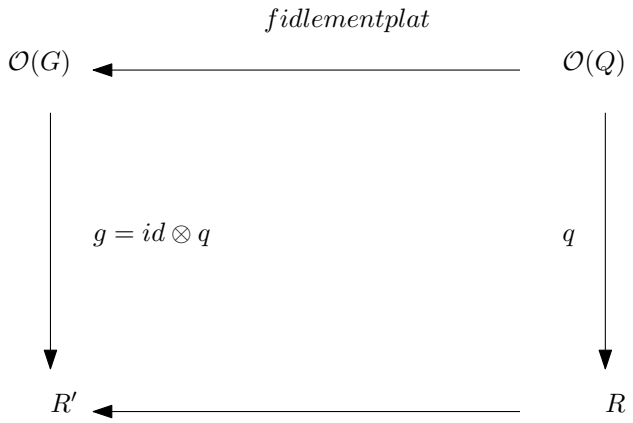
Théorème 2.1.5 *[5] Soit k un corps. Les conditions suivantes sur un morphisme* $G \to Q$ *sont équivalents :*

1. $G \to Q$ *est surjectif.*
2. $\mathcal{O}(Q) \to \mathcal{O}(G)$ *est injectif.*
3. *Pour toute k-algèbre Retq* $\in Q(R)$*, il existe une R-algèbre fidèlement plate R' et un* $g \in G(R')$ *application à l'image de q dans Q(R').*

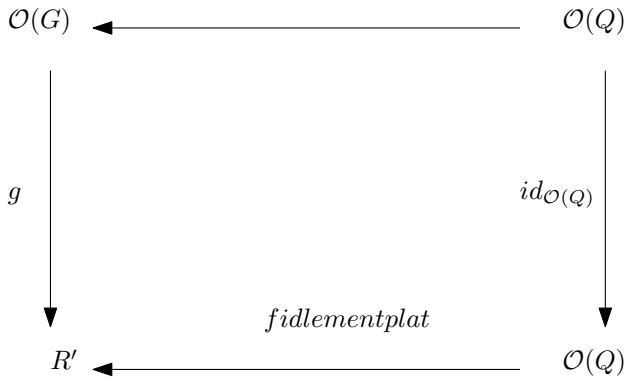
Preuve.

⋆ 1) ⇒ 3) : soit $q \in Q(R)$ un morphisme $\mathcal{O}(Q) \to R$, et on considère $R' = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} R$

Alors R' est une R-algèbre fidèlement plate car $\mathcal{O}(G)$ est une $\mathcal{O}(Q)$-algèbre fidèlement plate. La commutativité du carré signifie que $g \in G(R')$ correspond à l'image q' de q dans Q(R').



⋆ 3) ⇒ 2) : considérons l'élément $id_{O(Q)} \in Q(O(Q))$. Par hypothèse il existe un $g \in G(R')$, avec R' fidèlement plat sur $O(Q)$, tel que g et $id_{O(Q)}$ correspondent au même élément de Q(R') tel que le diagramme commute



Mais l'application $O(Q) \to R'$ est injectif parce qu'il est fidèlement plat, et donc aussi l'application $O(Q) \to O(G)$ est injectif.

⋆ 2) ⇒ 1) on utilise le fait : pour toute algèbre de Hopf $A \subset B$ sur un corps k, B est fidèlement plat sur A.

■

Corollaire 2.1.2 *[5] Tout morphisme $H \to G$ de groupes affines sur un corps vérifie*

$$H \to H' \to G.$$

avec $H \to H'$ surjectif et $H' \to G$ une immersion fermée.

Preuve.

Le morphisme $O(G) \to O(H)$ se divise en

$$O(G) \twoheadrightarrow B \hookrightarrow O(H).$$

où B est l'image de l'application $O(G) \to O(H)$. B est une algèbre de Hopf et donc on peut considérons le groupe affine H' = Spec B. Alors la première application implique que $H' \to G$ est une immersion fermée, et par la proposition précédente l'injectivité de la seconde application implique que $H \to H'$ est surjectif.

Le groupe affine H' du corollaire est appelé l'image du morphisme $H \to G$. ■

2.1.5 Exemples

Désormais, nous devons supposer autres hypothèses sur les groupes affines.
Soit $S \in Anneaux$.

Définition 2.1.17 *[5] Un groupe affine G sur S est fini (resp. fini et localement libre) si $O(G)$ est de type fini (resp. de type fini et projectif) comme S-module.*

Un groupe affine G sur S est fini et localement libre si et seulement si $O(G)$ satisfait les conditions équivalentes suivantes :

1. *$O(G)$ est de type fini et projectif et un S-module.*
2. *$O(G)$ est de type fini comme un S-module et $O(G)_m$est un S_m − module libre pour tout idéal maximal m de S.*
3. *Il existe une famille finie $(f_i)_{i\in I}$ engendrant l'idéal S et telle que, pour tout $i \in I$, le S_{f_i} − module $O(G)_{f_i}$ est libre de rang fini ;*
4. *$O(G)$ est de type fini et plat comme un S-module ;*
5. *(S intègre) $O(G)$ est de type fini et $dim_{S(p)}(O(G) \otimes_S S(p))$ est le même pour tout idéaux premiers p de S (ici S(p) est le corps des fractions de S / p).*

En général, si G est fini et localement libre, la fonction

$$m \to dim_{S(m)} O(G) \otimes S(m) : Spm(S) \to \mathbb{N}.$$

est localement constante. On l'appelle l'ordre de G sur S.

Notons en particulier que si G = Spec A est fini, alors A est localement libre $\Longleftrightarrow$A est projectif en tant que A-module$\Longleftrightarrow$ A est plat comme A-module $\Longleftrightarrow$ G est fini et localement libre.

Lorsque S est un corps un groupe affine G sur S est fini si et seulement si $dim_S O(G)$ est fini (et $dim_S O(G)$ est alors l'ordre de G sur S).

A partir de maintenant tous les schémas en groupes sont supposés affines, commutatifs, finis et localement libres même si nous les appellerons uniquement « groupes affines ».

Dualité de Cartier

Définition 2.1.18 *[10] $G^\vee$ est appelé le dual de Cartier de G.*

L'un des premiers exemples de groupe affine est le schéma en groupe multiplicatif $\mathbb{G}_m$; on l'appelle le groupe multiplicatif parce que

$$\mathbb{G}_m(S) = Hom_{R-alg}(R[X, X^{-1}], S) \cong Hom_{R-alg}(R[X, Y]/(XY - 1), S) \cong \{a \in S | a \text{ est inversible}\}.$$

est la partie multiplicative de la R-algèbre S. Notons en particulier que l'on définit les applications $m(X) = X \otimes X$, $\epsilon(f) = f(1, 1)$ et i qui intervertit X et X^{-1}. Donc le produit des éléments de $\mathbb{G}_m(S)$ coïncide avec le de S.

Pour une R-algèbre S, soit $\underline{Hom}(G, \mathbb{G}_m)(S)$ l'ensemble des morphismes de $u : G_S \to \mathbb{G}_{m,S}$ de groupes affines sur S. Cela devient un groupe sous la multiplication

$$(u_1 * u_2)(g) = u_1(g) * u_2(g), \ g \in G(S').$$

S′ une S-algébre.

De cette façon

$$S \rightsquigarrow \underline{Hom}(G, \mathbb{G}_m)(S).$$

devient un foncteur $Alg_R \to$ Groupe.

Lemme 2.1.3 *Soit R un anneau noethérien. A et M deux R-modules où A est de type fini et M est projectif. Alors*

$$Hom_R(A, M) \cong Hom_R(A, R) \otimes M.$$

Preuve. On sait qu'un module projectif a une "base duale" c'est-à-dire qu'il existe un ensemble I et $m_i \in M$ et$f_i \in Hom(M, R)$ avec $i \in I$ tel que pour tout $m \in M$, $f_i(m)$ est seulement non nul pour un nombre fini de i et $m = \sum f_i(m)m_i$.

On constate maintenant que les applications

$$Hom_R(A, R) \otimes M \to Hom_R(A, M).$$

$$\sum h_k \otimes x_k \to \sum h_k x_k.$$

et

$$Hom_R(A, M) \to Hom_R(A, R) \otimes M.$$

$$g \to \sum f_i \circ g \otimes m_i.$$

sont l'un l'inverse de l'autre. Notez que A est de type fini et qu'il n'y a donc qu'un nombre fini de f_i qui sont non nuls sur l'image de g et donc la dernière somme est sur un indice fini ■

Corollaire 2.1.3 *Soit A une algèbre R-Hopf de type fini et projective. Alors*

$$(A \otimes A)^\vee \cong A^\vee \otimes A^\vee.$$

Preuve.

$$A^\vee \otimes A^\vee = Hom_R(A,R) \otimes A^\vee \cong Hom_R(A, Hom_R(A,R)) \cong Hom_R(A \otimes A, R) = (A \otimes A)^\vee .$$

Soit $A^\vee := Hom_{R-lin}(A,R)$ son R-dual ; puisque A est plat et R est noethérien, A est projectif et $(A \otimes_R A)^\vee = A^\vee \otimes_R A^\vee$ et nous pouvons définir $e^\vee$, $m^\vee$, $\mu^\vee$, $\epsilon^\vee$et $i^\vee$comme le R-dual de e, m, μ, ϵ et i. ces applications satisfont l'axiome de l'algèbre de Hopf, et $G^\vee := Spec(A^\vee)$ est un groupe affine sur Spec R aussi. ■

Théorème 2.1.6 *[5] Il existe un isomorphisme canonique*

$$G^\vee \cong \underline{Hom}(G, \mathbb{G}_m).$$

des foncteurs $Alg_R \to Groupe$.

Preuve. Soit S une R-algèbre. Nous avons

$$G(S) = Hom_{R-alg}(\mathcal{O}(G), S) = Hom_{S-alg}(\mathcal{O}(G)_S, S) \hookrightarrow Hom_{S-lin}(\mathcal{O}(G)_S, S) = \mathcal{O}(G^\vee)_S.$$

Si on prend $f \in Hom_{S-alg}(\mathcal{O}(G)_S, S) \hookrightarrow Hom_{S-lin}(\mathcal{O}(G)_S, S)$ alors $m^\vee(f) = f \otimes f$ car

$$m^\vee(f)(a \otimes b) = f(\mu(a \otimes b)) = f(ab) = f(a)f(b) = (f \otimes f)(a \otimes b) \text{ avec } a\ , b \in \mathcal{O}(G)_S.$$

D'autre part $Hom(G_S^\vee, \mathbb{G}_{m,S}) = Hom_{S-alg}(S[X, X^{-1}], \mathcal{O}(G^\vee)_S)$ est aussi constitué des éléments de $\mathcal{O}(G^\vee)_S$ tel que $m^\vee(g) = g \otimes g$. En effet si on prend $f \in Hom_{S-alg}(S[X, X^{-1}], \mathcal{O}(G^\vee)_S)$, alors

$$m^\vee(f(X)) = (f \otimes f)(m(X)) = (f \otimes f)(X \otimes X) = f(X) \otimes f(X).$$

Ainsi

$$G(S) \cong \underline{Hom}(G^\vee, \mathbb{G}_m)(S).$$

Cet isomorphisme est naturel dans S, et nous avons montré que $G \cong \underline{Hom}(G^\vee, \mathbb{G}_m)$. Pour obtenir le isomorphisme, remplacez G par $G^\vee$ et utilisez que $(G^\vee)^\vee \cong G$. ■

Exemples

1. μ_n. Pour un entier $1 \leq n$,

$$\mu_n(S) = \{s \in S | s^n = 1\} \cong Hom_{R-alg}(R[X]/(X^n - 1), S).$$

est un sous-groupe de $\mathbb{G}_m$.

2. Schémas en groupe constants. On commence par composant Γun groupe abélien fini, et on définit l'anneau des fonctions

$$R^\Gamma := \{f : \Gamma \to R | f \textit{ est une application d'ensembles}\}.$$

dont l'addition et la multiplication sont définies par composant, et dont 0 et 1 sont les applications constantes de valeur 0, respectivement 1. La comultplication $m : R^\Gamma \to R^\Gamma \otimes_R R^\Gamma \cong R^{\Gamma \times \Gamma}$ est donné par la formule $m(f)(\gamma, \gamma') = f(\gamma + \gamma')$, le co-unité $\epsilon : R^\Gamma \to R$ par $\epsilon(f) = f(0)$, et la coinverse $i : R^\Gamma \to R^\Gamma$ par $i(f)(\gamma) = f(-\gamma)$.

Observons ensuite que les éléments suivants $\{e_\gamma\}_\gamma \in \Gamma$ constituent une base canonique du R-module R^Γ libre :

$$e_\gamma(\gamma') = \begin{cases} 1 & si \quad \gamma = \gamma' \\ 0 & sinon \end{cases}$$

On vérifie que μ, ϵ, e, m, et i sont donnés par :

$$\mu(e_\gamma \otimes e_{\gamma'}) = \begin{cases} e_\gamma & si \quad \gamma = \gamma' \\ 0 & sinon \end{cases}$$

$$\epsilon(e_\gamma) = \begin{cases} 1 & si \quad \gamma = 0 \\ 0 & sinon \end{cases}$$

$$e(1) = \left(\sum_{\gamma \in \Gamma} e_\gamma \right).$$

$$m(e_\gamma) = \sum_{\gamma' \in \Gamma} e_{\gamma'} \otimes e_{\gamma - \gamma'}.$$

$$i(e_\gamma) = e_{-\gamma}.$$

Maintenant, pour calculer le dual de Cartier, nous pouvons utiliser la base caractérisée par

$$\hat{e}_\gamma(e_{\gamma'}) = \begin{cases} 1 & si \quad \gamma = \gamma' \\ 0 & sinon \end{cases}$$

Les applications duales sont données par les formules

$$m^\vee(\hat{e}_\gamma) = \hat{e}_{\ \gamma} \otimes \hat{e}_\gamma.$$

$$e^\vee(1) = \hat{e}_0.$$

$$\epsilon^\vee(\hat{\epsilon}_\gamma) = 1$$

$$\mu^\vee(\hat{e}_\gamma \otimes \hat{e}_{\gamma'}) = \hat{e}_{\gamma+\gamma'}.$$

$$i^\vee(\hat{e}_\gamma) = \hat{e}_{-\gamma}.$$

La démonstration de ces formules découle directement de la définition, nous démontrons la dernière pour donner un exemple.

$$i^\vee(\hat{e}_\gamma)(e_{\gamma'}) = (\hat{e}_\gamma \circ i)(e_{\gamma'}) = \hat{e}_\gamma(e_{-\gamma'}) = \begin{cases} 1 & si \quad \gamma = -\gamma' \\ 0 & sinon \end{cases}$$

et on conclut par la définition de e_γ.

En particulier, les formules pour $\mu^\vee$ et $e^\vee$ montrent que $(R^\Gamma)^\vee$ est isomorphe au groupe anneau $R[\Gamma]$ comme une R-algèbre, telle que $\epsilon^\vee$ corresponde à l'application d'augmentation usuelle $R[\Gamma] \to R$.

Par exemple si $\Gamma := \mathbb{Z}/n\mathbb{Z}$, alors $(R^\Gamma)^\vee \cong \mu_n$.

3. α_p. En caractéristique $p \neq 0$ on a $(a+b)^p = a^p + b^p$; donc, pour toute R-algèbre S sur un anneau de caractéristique p, on peut définir

$$\alpha_p(S) = \{s \in S | s^p = 0\} \cong Hom_{R-alg}(R[T]/T^p, S).$$

En fonction de la base $\{T^i\}_{0 \leq i < p}$ toutes les applications sont données par les formules

$$\mu(T^i \otimes T^j) = \begin{cases} T^{i+j} & si \quad i + j < p \\ 0 & sinon \end{cases}$$

$$e(1) = T^0.$$

$$m(T^i) = \left(\sum_{0 \le j \le i} (C_j^i) T^i \otimes T^{i-j} \right).$$

$$i(T^i) = (-1)^i T^i.$$

Soit $\{u_i\}$ la base duale de $A^\vee$. Puis on vérifie que l'application R-linéaire $\phi : A^\vee \to A$ transmit u_i à $T^i/i!$ est un isomorphisme des algèbres de Hopf. Par exemple, nous prouvons que cette application préserve des produits ; il est immédiat de vérifier que

$$u_i u_j = (C_i^{i+j}) u_{i+j}.$$

$$\phi(u_i u_j) = (C_i^{i+j}) u_{i+j} \phi(u_{i+j}) = (C_i^{i+j}) u_{i+j} \frac{T^{i+j}}{(i+j)!} = \frac{T^i}{i!} \frac{T^j}{j!} = \phi(u_i)\phi(u_j).$$

2.2 Les composants connexes d'un groupe affine

Rappelons qu'un espace topologique X est connexe s'il n'est pas la réunion de deux ouverts non vides disjoints sous-ensembles. Cela revient à dire qu'en dehors de X lui-même et de l'ensemble vide, il n'y a pas de sous-ensemble de X qui est à la fois ouvert et fermé. Pour chaque point x de X, la réunion des sous-ensembles connexes de X contenant x est à nouveau connexe, et c'est donc le plus grand sous-ensemble connexe contenant x - on l'appelle le connexe composante de x. L'ensemble des composantes connexes des points de X est une partition de X par sous-ensembles fermés.

Notons $\pi_0(X)$ l'ensemble des composantes connexes de X. Dans un groupe topologique G, la composante connexe de l'élément neutre est un sous-groupe normal fermé connexe G^0 de G, appelé composant neutre (ou identité) de G. Par conséquent, le quotient $\pi_0(G) = G/G^0$ est un groupe topologique séparé. Dans la suite, k est un corps.

2.2.1 Idempotents et composants connexes

Soit A un anneau commutatif et $e_1, \cdots, e_n$ un ensemble de n éléments idempotents et orthogonaux. Si cet ensemble est complet, ce qui signifie que $e_1 + ... + e_n = 1$, alors Ae_i devient un anneau avec l'addition et multiplication induite par celle de A (mais avec l'élément d'identité e_i) et $A = Ae_1 \times ... \times Ae_n$.

Inversement si $A = A_1 \times ... \times A_n$ alors les éléments $e_1 = (1, 0, 0, ...), ... e_n = (0, ..., 0, 1)$ forment un ensemble complet des idempotents orthogonaux.

Lemme 2.2.1 *[5] L'espace Spec A est discontinu si et seulement si A contient un idempotent non trivial.*

Preuve. Voir Lemme 1. 1 page 204 de [5]. ■

Proposition 2.2.1 *[5] Soit $\{e_1, ..., e_n\}$ un ensemble complet d'idempotents orthogonaux dans A. Alors*

$$SpecA = D(e_1) \sqcup ... \sqcup D(e_n).$$

est une décomposition de Spec A en une union disjointe de sous-ensembles ouverts.

Remarque 2.2.1 *Rappelons qu'un anneau A est dit de Jacobson si tout idéal premier est une intersection d'idéaux maximaux, et que toute algèbre de type fini sur un corps est de Jacobson. Dans un anneau de Jacobson, le nilradical est une intersection d'idéaux maximaux. Lorsque A est Jacobson, "l'idéal premier" peut être remplacé par "l'idéal maximal" et "Spec" par "Spm" dans la discussion ci-dessus. En particulier, pour un anneau de Jacobson A, il existe des correspondances naturelles entre*

1. *les décompositions de Spm A en une union finie disjointe de sous-espaces ouverts.*

2. *les décompositions de A en produits directs finis d'anneaux.*

3. *les ensembles complets d'idempotents orthogonaux dans A.*

Considérons maintenant un anneau $A = k[X_1, ..., X_n]/I$. Si k est un corps algèbriquement clos,

$$SpmA \cong \text{l'ensemble nul de I dans } k^n.$$

comme espace topologique, et donc Spm A est connexe si et seulement si l'ensemble nul de I dans k^n est connexe.

Définition 2.2.1 *[5] Une algèbre A sur un corps k est diagonalisable si elle est isomorphe à l'algèbre produit k^n pour un certain n, et elle est étale si $L \otimes A$ est diagonalisable pour un corps L contenant k.*

Remarque 2.2.2 *Soit k un corps, et soit A une k-algèbre finie. Pour tout ensemble fini S d'idéaux maximaux dans A, le théorème des restes chinois [2] montre que l'application $A \to (\prod_{m \in S}) A/m$ est surjectif de noyau $(\cap_{m \in S} m)$ En particulier $|S| \leq |A : k|$, et donc A n'a qu'un nombre fini d'idéaux maximaux. Si S est l'ensemble de tous les idéaux maximaux de A, alors $(\cap_{m \in S} m)$ est le nilradical N de A et donc A/N est un produit fini de corps. Où N est l'ensemble des éléments nilpotents défini par $N = Nil(A) = \{x \in A | \exists n \in \mathbb{N}^*, x^n = 0_A\}$.*

Proposition 2.2.2 *[5] Les conditions suivantes sur une k-algèbre finie A sont équivalentes :*

1. *A est étale.*

2. *$L \otimes A$ est réduit (c'est-à-dire qu'il n'a pas d'éléments nilpotents non nuls) pour tout corps L contenant k.*

3. *A est un produit d'extensions de corps séparables de k.*

Preuve.

⋆ 1) ⇒ 2) : soit L un corps contenant k. Par hypothèse, il existe un corps L' contenant k tel que $L' \otimes A$ est diagonalisable. Soit L'' un corps qui contient L et L', alors $L'' \otimes A$ est diagonalisable et l'application $L \otimes A \to L'' \otimes A$ défini par l'inclusion $L \to L''$ est injectif, donc $L \otimes A$ est réduit.

⋆**)** 2) ⇒ 3) : supposons que $L \otimes A$ est réduit, alors A est également réduit car A est contenu dans $L \otimes A$. Ce fait et la remarque ci-dessus nous disent que A est un produit fini des corps, soit k' un de ces corps. Si k' n'est pas séparable sur k, alors k de caractéristique $p \neq 0$ et il existe un élément $u \in k'$ dont le polynôme minimum est de la forme $f(X^p)$ avec $f \in k[X]$. Soit L un corps contenant k tel que tous les les coefficients de f sont les puissances p dans L. Alors

$$L \otimes k[u] \cong L \otimes (k[X]/f(X^p)) \cong L[X]/f(X^p).$$

qui ne se réduit pas car $f(X^p) = f(X)^p$ est une p-ième puissance dans L[X]. Donc $L \otimes A$ n'est pas réduit.

⋆ 3) ⇒ 1) : supposons que A lui-même est une extension de corps séparable de k. A partir du théorème de l'élément primitif, nous sachez que A = k[u] pour un certain u. Comme k[u] est séparable sur k, le polynôme minimum f(X) de u est séparable, ce qui signifie que

$$f(X) = \prod (X - u_i), u_i \neq u_j \; pour \; i \neq j,$$

dans un corps de séparation L pour f. Maintenant

$$L \otimes A \cong L \otimes k[X]/(f) \cong L[X]/(f).$$

et d'après le théorème des restes chinois [2]

$$L[X]/(f) \cong \prod L[X]/(X - u_i) \cong L \times L \times ... \times L.$$

■

Corollaire 2.2.1 *[5] Soit k^{sep} une clôture séparable de k. Une k-algèbre A est étale si et seulement si $k^{sep} \otimes A$ est diagonalisable.*

Preuve. La preuve que 3) ⇒ 2) montre que $L \otimes A$ est diagonalisable si certains polynômes séparables se décomposent en L. Mais par définition, tous les polynômes séparables se décomposent en k^{sep}. ■

Remarque 2.2.3 *Les produits finis, les produits tensoriels et les quotients de k-algèbres diagonalisables (resp. étales) sont diagonalisable (resp. étale).*

Corollaire 2.2.2 *[5] Le composé de tout ensemble fini de sous-algèbres étales d'une k-algèbre est étale.*

Preuve. Soit A_i des sous-algèbres étales de B. Alors $A_1 \times A_2 \times \cdots A_n$ est l'image de l'application

$$a_1 \otimes \cdots \otimes a_n \to a_1 * \cdots * a_n.$$

et est donc un quotient de $A_1 \otimes \cdots \otimes A_n$. ■

Proposition 2.2.3 *[5] Si A est étale sur k, alors k' ⊗ A est étale sur k' pour tout corps k' contenant k.*

Preuve. Soit L tel que $A \otimes L \cong L^m$, et soit L' un corps contenant L et k'. Alors

$$L' \otimes_{k'} (k' \otimes A) \cong L' \otimes A \cong L' \otimes_L L \otimes A \cong L' \otimes_L L^m \cong (L')^m.$$

■

Lemme 2.2.2 *[5] Soit A une algèbre de type fini sur un corps séparablement clos k. Le nombre de composantes connexes de Spm A est égal au plus grand degré d'une k-sous-algèbre étale de A (et les deux sont fini).*

Preuve. car *Spm A* est noethérien, c'est une union finie disjointe de ses composantes connexes, chacune de qui est ouvert. ■

Soit E une k-sous-algèbre étale de A. Comme k est séparablement clos, E est un produit de copies de k. Une décomposition de E correspond à un ensemble complet $(e_i)_{1 \le i \le m}$ d'idempotents orthogonaux dans E, et $m = [E : k]$. Inversement, un ensemble complet $(e_i)_{1 \le i \le m}$ d'idempotents orthogonaux dans A définit une étale k-sous-algèbre de A de degré $m : \sum k e_i$

Lemme 2.2.3 *[5] Soit A une k-algèbre de type fini. Supposons que k est algèbriquement clos, et soit K un corps algèbriquement clos contenant k. Si Spm A est connexe, Spm A_K l'est aussi.*

Preuve. Supposons $A = k[X_1, ..., X_n]/a$, de sorte que $A_K = K[X_1, ..., X_n]/b$ où b est l'idéal engendré par a. Par hypothèse, l'ensemble nul $V(a)$ dans k^n est connexe, et il appartient à l'ensemble $V(b)$ dans K^n. Comme la clôture d'un ensemble connexe est connexe, on veut montrer que V (b) est contenu dans la clôture de V (a) dans K^n. Choisissons une base $(ai)_{i\in I}$ de K sur k, soit $f \in K[X_1, ..., X_n]$ un polynôme nul sur V (a) et on veut montrer qu'il est nul sur V (b). Écrire

$$f = \sum a_i f_i, f_i \in k[X_1, ..., X_n].$$

Comme f est nul sur $V(a)$, il en va de même pour chaque f_i. Par le Nullstellensatz fort, certaine puissance de f_i appartient à $a \subset b$ donc chaque f_i est nul sur V (b) et donc f est nul sur $V(b)$. ■

Soit A une k-algèbre de type fini. Une k-sous-algèbre étale de A donnera une k^{al}-sous-algèbre étale de même degré de $A_{k^{al}}$, et donc son degré est borné par le nombre de composantes connexes de Spm $A_{k^{al}}$. Le composé de deux sous-algèbres étales de A est étale, et il existe donc une plus grande k-sous-algèbre étale $\pi_0(A)$ de A, contenant toutes les autres sous-algèbres.

Soit K un corps contenant k. Alors $K \otimes \pi_0(A)$ est une K-sous-algèbre étale de $K \otimes A$. Il faudra savoir que c'est la plus grande sous-algèbre étale.

Proposition 2.2.4 *[5] Soit A une k-algèbre de type fini, et soit K un corps contenant k. Alors*

$$K \otimes \pi_0(A) = \pi_0(K \otimes A).$$

Preuve. Voir la proposition 2. 1 page 206 de [5]. ■

Corollaire 2.2.3 *[5] Soit A une k-algèbre de type fini. Le degré* $[\pi_0(A) : k]$ *est égal au nombre des composantes connexes de Spm*$(k^{al} \otimes A)$.

Preuve.

$$[\pi_0(A) : k] = [k^{al} \otimes \pi_0(A) : k^{al}] = [\pi_0(k^{al} \otimes A) : k^{al}].$$

■

Proposition 2.2.5 *[5] Soient A et A′ des k-algèbres de type fini. Alors*

$$\pi_0(A \otimes A') = \pi_0(A) \otimes \pi_0(A').$$

Preuve. Voir la proposition 2. 3 page 207 de [5]. ■

2.2.2 Groupes affines

Soit G un groupe affine d'anneau de coordonnées $A = \mathcal{O}(G)$. L'application $m : A \to A \otimes A$ est un morphisme de k-algèbre et envoie donc $\pi_0(A)$ dans $\pi_0(A \otimes A) = \pi_0(A) \otimes \pi_0(A)$; de même $i : A \to A$, transmit $\pi_0(A)$ dans $\pi_0(A)$ et on peut se restreindre sur $\pi_0(A)$, donc $\pi_0(A)$ devient une sous-algèbre de Hopf de A. En détails. Supposons $\phi : A \to B$ est un morphisme d'algèbres de Hopf, alors on veut montrer qu'on peut restreindre $\phi : \pi_0(A) \to \pi_0(B)$. En particulier nous montrerons que l'image de $\pi_0(A)$ est une algèbre ètale. Premièrement $\pi_0(A) = \prod_{i=1}^{n} k_i$ où k_i sont des extensions séparables de k ; en particulier il existe $e_1, ..., e_n$ un ensemble complet d'idempotents. Clairement $\phi(e_1), ..., \phi(e_n)$ est encore un ensemble complet d'idempotents ce qui implique que $\phi(\pi_0(A)) = \prod_{i=1}^{n}(\phi(\pi_0(A))\phi(e_i)) = \prod_{i=1}^{n} \phi(k_i)$. Donc pour conclure il suffit de prouver que $\phi(k_i)$ reste une extension de corps séparable pour tout i. En utilisant la multiplicativité de ϕ on voit que $\phi(k_i)$ est un corps qui implique que $\phi_{|k_i}$ est injectif. Il s'ensuit un élément $\phi(j) \in \phi(k_i)$, son polynôme minimal sur k est le même que celui de j et donc il ne peut pas avoir plusieurs racines dans $\phi(k_i)$.

Définition 2.2.2 *[5] Soit G un groupe algèbrique sur un corps k.*

1. *Le groupe de composante connexe $\pi_0(G)$ de G est le groupe affine quotient correspondant à $\pi_0(\mathcal{O}(G))$.*
2. *La composante identité G° de G est le noyau du morphisme $G \to \pi_0(G)$.*

Proposition 2.2.6 *[5] Les quatre conditions suivantes sur un groupe affine G sont équivalentes :*

1. *le groupe affine étale $\pi_0(G)$ est trivial.*
2. *l'espace topologique Spm ($\mathcal{O}(G)$) est connexe.*
3. *l'espace topologique Spm ($\mathcal{O}(G)$) est irréductible.*
4. *l'anneau $\mathcal{O}(G)/N$ est intégre.*

Preuve.

⋆ 2) ⇒ 1) : $\pi_0(\mathcal{O}(G))$ n'a pas d'idempotents non triviaux et c'est donc un corps. L'existence de $\epsilon : \mathcal{O}(G) \to k$ implique que $\pi_0(\mathcal{O}(G)) = k$.

⋆ 3) ⇒ 2) : trivial.

⋆ 3) ⇔ 4) : $Spm(A)$ est irréductible si et seulement si le nilradical de A est premier.

⋆ 1) ⇒ 4) : Si $\pi_0(G)$ est trivial, $\pi_0(G_{k^{al}})$ l'est aussi. Soit $Spm(\mathcal{O}(G_{k^{al}}))$ comme union de ses composants irréductibles. Par définition, aucune composante irréductible n'est contenue dans la réunion du reste. Par conséquent, il existe un point qui se trouve exactement dans une composante irréductible. Par homogénéité, tous les points ont cette propriété et donc les composantes irréductibles sont disjointes. Comme $Spm(\mathcal{O}(G_{k^{al}}))$ est connexe, il ne doit y avoir qu'une seule composante irréductible, donc Spm $\mathcal{O}(G_{k^{al}})$ est irréductible. Soit N' le nilradical de $\mathcal{O}(G_{k^{al}})$; l'implication 3) ⇒ 4) nous dit que $\mathcal{O}(G_{k^{al}}))/N'$ est intégre. L'application canonique $\mathcal{O}(G) \to k^{al} \otimes \mathcal{O}(G) \cong \mathcal{O}(G_{k^{al}})$ est injectif : cela nous dit que l'image inverse de N' est contenue dans N et l'autre inclusion découle de la multiplicativité de l'application. Il reste donc injectif après quotients par les nilradicaux respectifs, et donc $\mathcal{O}(G)/N$ est intégre.

■

Définition 2.2.3 *[5] Un groupe affine est connexe s'il satisfait les conditions équivalentes de la proposition.*

Proposition 2.2.7 *[5] Les fibres de l'application Spm $G \to Spm\pi_0(G)$ sont les composantes connexes de l'espace topologique Spm G.*

Preuve. Les composantes connexes de Spm G et les points de Spm $\pi_0(G)$ sont tous deux indexés par les éléments d'un ensemble complet maximal d'idempotents orthogonaux. ■

Proposition 2.2.8 *[5] Tout morphisme de G vers un groupe affine étale se factorise uniquement par $G \to \pi_0(G)$.*

Preuve. Soit $G \to H$ un morphisme de G vers un groupe affine étale H. L'image de $\mathcal{O}(H)$ est une algèbre étale et donc elle est contenue dans $\pi_0(\mathcal{O}(G)) = \mathcal{O}(\pi_0 G)$. ■

Proposition 2.2.9 *[5] Le sous-groupe G° de G est connexe.*

Preuve. Le morphisme des k-algèbres : $\mathcal{O}(\pi_0(G)) \to k$ décompose $\mathcal{O}(\pi_o(G))$ en un produit direct

$$\mathcal{O}(\pi_0(G)) = k \times B.$$

où B est l'idéal d'augmentation de $\mathcal{O}(\pi_0(G))$. Soit $e = (1, 0)$.

$$\mathcal{O}(G) = e\mathcal{O}(G) \times (1 - e)\mathcal{O}(G).$$

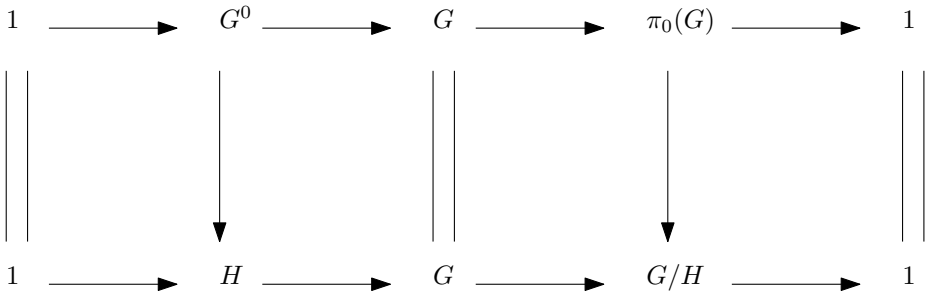
avec

$$e\mathcal{O}(G) \cong \mathcal{O}(G)/(1-e)\mathcal{O}(G) = \mathcal{O}(G^\circ).$$

Maintenant $k = \pi_0(e\mathcal{O}(G)) \cong \pi_0(\mathcal{O}(G^\circ))$. Donc $\pi_0(G^\circ) = 1$ ce qui implique que G° est connexe. ■

Proposition 2.2.10 *[5] Le sous-groupe G° est l'unique sous-groupe affine normal connexe de G tel que G/G° est étale.*

Preuve. Nous n'avons qu'à prouver l'unicité. Supposons que H soit un second sous-groupe affine normal de G. Si G / H est étale, alors le morphisme $G \to G/H$ passe par $\pi_0(G)$, et on obtient ainsi un diagramme commutatif



avec des lignes exactes ; notez que la deuxième ligne est exacte car H est un sous-groupe affine de G et G/H est le conoyau de la première application. Le diagramme similaire avec chaque $*$ remplacé par $*(R)$ donne, pour chaque k-algèbre R, une suite

$$1 \to G^\circ(R) \to H(R) \to \pi_0(G)(R).$$

Vérifions que la suite est exact, la première application est injective car $G^\circ(R)$ est contenu dans le noyau de l'application $G(R) \to G/H(R)$ qui est H(R). L'exactitude au milieu découle du fait que l'application $H(R) \to \pi_0(G)(R)$ est la restriction à H(R) de l'application $G(R) \to \pi_0(G)(R)$; le noyau de cette dernière application est $G^\circ(R)$ qui est contenu dans H(R) et donc c'est aussi le noyau de l'application $H(R) \to \pi_0(G)(R)$.

Puisque c'est fonctoriel dans R et que nous sommes sur un corps, la proposition 2. 1. 4 nous dit qu'une immersion fermée peut être vérifié sur des « points » ; donc la suite des groupes affines

$$1 \to G^\circ \to H \to \pi_0(G).$$

est exacte, donc G° est le noyau de $H \to \pi_0(G)$. Cette application se factorise par $\pi_0(H)$ et donc si $\pi_0(H) = 1$, son noyau est H : donc $G^\circ \cong H$. ■

Remarque 2.2.4 *Cette proposition affirme que pour tout groupe affine G il existe une suite exacte unique*

$$1 \to G^\circ \to G \to \pi_0(G) \to 1.$$

tel que G° est connexe et $\pi_0(G)$ est étale. C'est ce qu'on appelle la suite exacte connexe - étale.

Proposition 2.2.11 *[5] Pour toute extension de corps $k' \supset k$*

$$\pi_0(G_{k'}) \cong \pi_0(G)_{k'}(G_{k'})^\circ \cong (G^\circ)_{k'}.$$

En particulier G est connexe si et seulement si $G_{k'}$ est connexe.

Preuve. Prenez la suite exacte

$$1 \to G^\circ \to G \to \pi_0(G) \to 1.$$

En appliquant $\_\_ \otimes k'$ aux algèbres on obtient

$$1 \to (G^\circ)_{k'} \to G_{k'} \to \pi_0(G)_{k'}.$$

Rappelons que la proposition 2. 2. 4 dit que $\pi_0(G)_{k'} = \pi_0(G_{k'})$ et donc nous concluons que $(G^\circ)_{k'}$ est le noyau de $G_{k'} \to \pi_0(G_{k'})$ et donc $(G^\circ)_{k'} = (G_{k'})^\circ$. ■

Proposition 2.2.12 *[10] Pour tout corps k de caractéristique $p > 0$, les groupes affines $(\mathbb{Z}/p\mathbb{Z})_k$, $\mu_{p,k}$ et $\alpha_{p,k}$ sont deux à deux non isomorphes.*

Preuve. Le premier est étale, tandis que $\mu_{p,k}$ et $\alpha_{p,k}$ sont réduites. Maintenant la dualité de Cartier de $\mu_{p,k}$ et $\alpha_{p,k}$ sont respectivement $\mathbb{Z}/p\mathbb{Z}_k$ et $\alpha_{p,k}$ qui ne sont pas isomorphes. Donc $\alpha_{p,k}$ et $\mu_{p,k}$ ne sont pas isomorphe aussi. ■

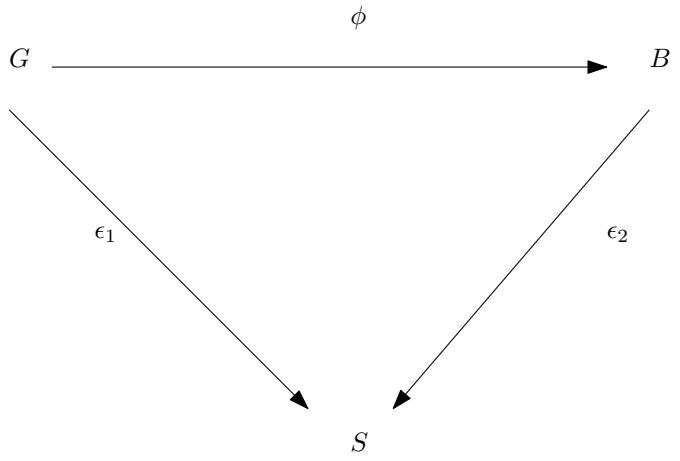
CHAPITRE 3

UNE CLASSIFICATION DES SCHÉMAS EN GROUPE D'ORDRE PREMIER

3.1 Deux théorèmes généraux

Jusqu'à présent, nous avons étudié l'objet de groupe dans la catégorie des schémas en groupe affine. Nous voulons maintenant étendre cette notion à la catégorie des schémas en groupe ; comme nous le verrons la notion d'algèbre de Hopf être remplacé par le faisceau quasi cohérent d'algèbres de Hopf. Comment passer de l'un à l'autre ? Soient $S = (S, \mathcal{O}_S)$ un schéma et A un faisceau quasi-cohérent d'O_S-algèbres ; nous voulons définir un schéma qui est en quelque sorte l'analogue de Spec A quand A était une algèbre.

On observe d'abord que pour chaque sous-ensemble affine U ⊂ S on a une application $\mathcal{O}_S(U) \to A(U)$ et une associée $f : Spec(A(U)) \to Spec(\mathcal{O}_S(U)) = U$. Donc l'idée est de définir Spec A et un morphisme $\epsilon : SpecA \to S$ comme l'unique schéma tel que $\epsilon^{-1}(U) = Spec(A(U))$ pour tout ouvert affine $U \subset S$. Il est possible de vérifier que Spec A est un collage approprié des schémas affines $Spec(A(U))$ et l'application ϵ l'extension des applications f. Donc le point principal est que nous avons construit un schéma Spec A avec un morphisme affine
ϵ : Spec A →S (affine signifie que pour chaque $U \subset S$ affine, $\epsilon^{-1}(U)$ est affine). Pour voir l'importance de cette propriété, prenons deux schémas en groupes G et B sur S et un S-morphisme $\phi : G \to B$. Le diagramme suivant commute



En particulier $\phi_{|\epsilon^{-1}(U)} : \epsilon_1^{-1}(U) \to \epsilon_2^{-1}(U)$ qui signifie que recouvrant G et B par des ouvertures de telle forme, on peut déterminer complètement le comportement de ϕ en l'étudiant localement sur des schémas affines.

Notez que si S est un schéma affine, alors Spec A l'est aussi et coïncide avec $Spec(A(S))$. Désormais nous écrirons Spec A bien que nous parlions de schémas pas nécessairement affines ; il sera clair d'après le contexte si A est une algèbre ou un faisceau d'algèbres.

Rappelons que tous les schémas en groupes sont supposés commutatifs, finis et localement libres. Soit $G \to S$ un schéma en groupe S. Pour chaque entier $m \in \mathbb{Z}$ on note

$$m_G : G \to G.$$

le morphisme obtenu en élevant à la puissance m tous les éléments du foncteur de groupe G. Supposons $G = Spec(A)$, alors on utilise $[m] : A \to A$ pour le morphisme $\mathcal{O}_S$-algèbre correspondant. En particulier soit $n \in \mathbb{Z}$, R une $\mathcal{O}_S$-algèbre, $u \in G(R)$ et $a \in A$; on a la relation suivante

$$n_G(u)(a) = u([n]a).$$

Les "lois des exposants" $(\xi^n)^m = \xi^{nm}$ et $(\xi^m)(\xi^n) = \xi^{n+m}$ reviennent aux identités

$$[m][n] = [mn]\mu_A \circ ([m] \otimes [n]) \circ m_A = [m + n].$$

De plus $[1] = id_A$ et $[0] = e \circ \epsilon$.

Théorème 3.1.1 *[6] Un groupe S commutatif d'ordre m est annulé par m (c'est-à-dire $m_G = 0_G$).*

Remarque 3.1.2 *Nous savons par la théorie des groupes que si G est un groupe commutatif fini d'ordre m, alors l'ordre de chaque élément divise m. Nous pouvons le prouver en montrant que si*

$x \in G$, alors

$$\prod_{y\in G} y = \prod_{y\in G} xy = (\prod_{y\in G} y)x^m.$$

et donc $x^m = 1$. On ne peut pas appliquer ces égalités dans le cas où G est un schéma en groupe car en général G(R) n'a pas un nombre fini d'éléments, où R est un S-schéma en groupes, et donc $\prod_{y\in G(R)} y$ n'a pas de sens. Il faut donc de trouver un objet qui peut substituer $\prod_{y\in G(R)} y$; un bon point de départ est d'analyser ce qui se passe pour les schémas en groupe affine constants.

On rappelle que le groupe constant C associé à un groupe fini G d'ordre m a $A := \mathcal{O}(C) = \prod_{g\in G} R$. Considérons la $A^\vee$-algèbre libre $A^\vee \otimes A$; à chaque élément $g \in A^\vee \otimes A$ on peut associer sa norme $\mathcal{N}(g)$ qui est le déterminant associé à la matrice de l'application linéaire

$$A^\vee \otimes A \to A^\vee \otimes A.$$

$$a \to g * a.$$

En notant par $\{e_i\}$ et $\{e_i'\}$ respectivement la base et la base duale, prenons $Id_A \in G(A)$ qui peut être écrit comme

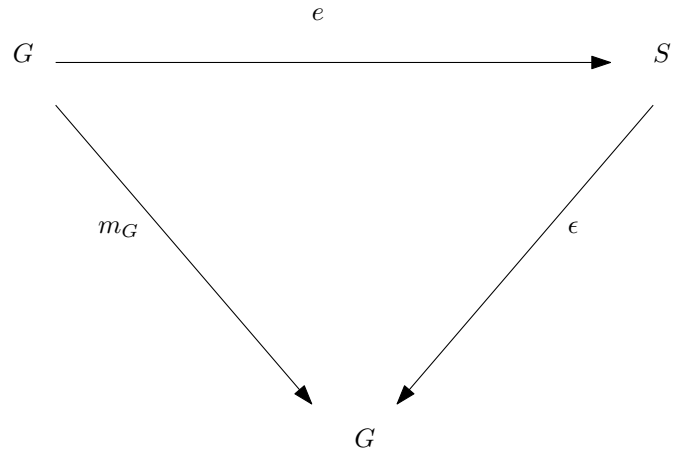
$$\sum_{i=1}^{m} e_i' \otimes e_i.$$

comme un élément de $A^\vee \otimes A$. On veut calculer $\mathcal{N}(Id_A)$. Soit $1 \otimes e_i$ un élément générique de la base de $A^\vee \otimes A$ sur $A^\vee$,

$$(Id_A)(1 \otimes e_j) = e_j' \otimes e_j.$$

et donc la matrice associée à la multiplication de Id_A est $(e_1', ..., e_m') * Id$ ce qui implique que $\mathcal{N}(Id_A) = \prod_{i=1}^m e_i'$ est inversible ; donc nous suggère que la norme est le bon objet à considérer.

Remarque 3.1.3 *Il s'agit essentiellement de prouver la commutativité des éléments suivants*



Mais on rappelle que G est un collage de schémas affines de la forme Spec$(A(U))$ *où* A *est un faisceau quasi-cohérent d'*$\mathcal{O}_S$*-algèbres et* $U \subset S$ *affine ouvert. On peut donc prouver la commutativité du diagramme dans chaque schéma affine Spec(A(U)) et on peut donc supposer S affine.*

On peut aussi supposer que $\mathcal{O}_S = R$ *est un anneau local ; en fait prenons* $a \in A$ *et supposons que* $([m]a - \epsilon \circ e(a)) \neq 0$ *dans* A *mais* $([m]a - \epsilon \circ e(a)) = 0$ *dans* $A \otimes R_p$ *pour chaque p nombres premiers de R. Considérons alors l'annulateur de* $([m]a - \epsilon \circ e(a))$ *qui est un idéal propre de R et considérons un idéal maximal m qui le contient. Alors* $([m]a - \epsilon \circ e(a)) \neq 0$ *dans* $A \otimes R_m$ *; absurde.*

Preuve. Donc en conclusion nous nous sommes réduits à prouver qu'un S-schéma commutatif plat fini $G = Spec$A d'ordre m est annulé par m_G. Soit $R = \mathcal{O}_S$, R est local ce qui implique que A est libre. Nous devrait prouver que pour toute R-algèbre B, chaque élément de G(B) a un ordre divisant m. Mais notons que si $A = \mathcal{O}(G)$, alors

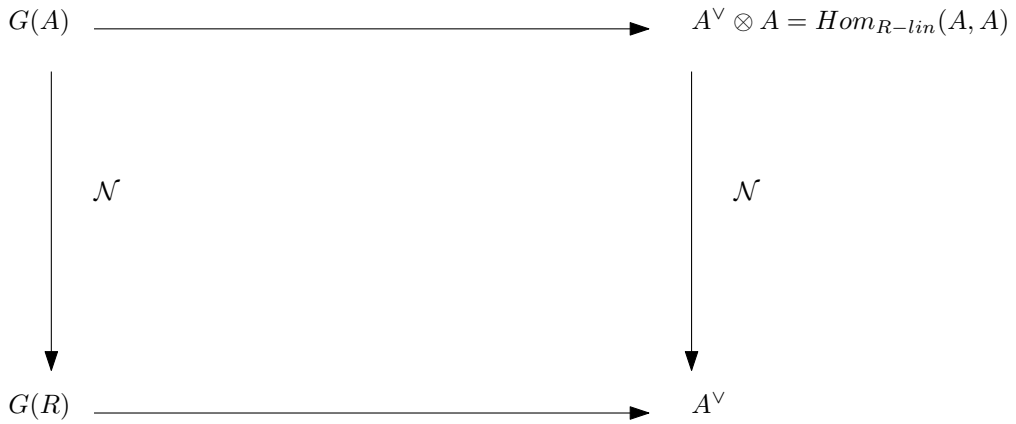
$$G(B) = Hom_R(A, B) = Hom_B(A \otimes B, B).$$

et donc on peut se ramener au cas $B = R$ et vérifier que pour tout $u \in G(R)$, $u^m = 1$. ■

Lemme 3.1.1 *[9] Soit S une R-algèbre finie et libre. Alors on a une application*

$$G(R) \to G(S) \xrightarrow{\mathcal{N}} G(R).$$

Fondamentalement, le lemme nous dit que le diagramme suivant commute



montrant que la norme « préserve » les éléments inversibles.

Soit $u \in G(R) \hookrightarrow A^\vee$ *et considérons la multiplication par* $u, m_u : A^\vee \otimes A \to A^\vee \otimes A$. *D'abord c'est un automorphisme de* $A^\vee$*-algèbres car* $u \in G(R)$ *et donc il est inversible aussi dans* $A^\vee$ *en observant que les produit dans G(R) coïncident avec le produit de G(R) dans* $A^\vee$. *On note aussi que l'application* $e : R \to A$ *est injective puisque A est libre et donc u peut être vu comme un élément*

de $G(A)$ et de $A^\vee \otimes A$; en particulier $\mathcal{N}(u) = u^m$ (dans ce cas on note u au lieu de $u * 1_{A^\vee \otimes A}$), car $u \in A^\vee$ et donc la matrice associée à la multiplication est $u * Id$. De plus si $a \in A^\vee \otimes A$, alors $\mathcal{N}(u*a) = \mathcal{N}(m_u(a)) = \mathcal{N}(a)$; la dernière égalité s'ensuit car m_u est un isomorphisme et l'application des normes est indépendante du choix d'un base.

Prenons enfin $Id_A \in G(A) \hookrightarrow A^\vee \otimes A$.

$$\mathcal{N}(Id_A) = \mathcal{N}(m_u(Id_A)) = \mathcal{N}(u * Id_A) = \mathcal{N}(u)\mathcal{N}(Id_A) = u^m \mathcal{N}(Id_A).$$

Mais $\mathcal{N}(Id_A) \in G(R)$ est inversible, donc $u^m = 1$.

Preuve. On continue la preuve du lemme.

S est fini et libre sur R et donc aussi $A^\vee \otimes S$ est fini et libre comme $A^\vee$-algèbre. On a donc une application norme $\mathcal{N} : A^\vee \otimes S \to A^\vee$ qui envoie un élément s$\in A^\vee \otimes S$à l'élément $\mathcal{N}(s)$ qui est le déterminant de la matrice de l'application $A^\vee$-linéaire $A^\vee \otimes S \to A^\vee \otimes S$ qui prend $x \in A^\vee \otimes S$ en sx. Nous prétendons que cette norme induit une application $G(S) \to G(R)$ tel que le diagramme suivant commute :

où les applications horizontales sont les inclusions, en effet

$$G(R) \subset Hom_{R-lin}(A, R) = A^\vee.$$

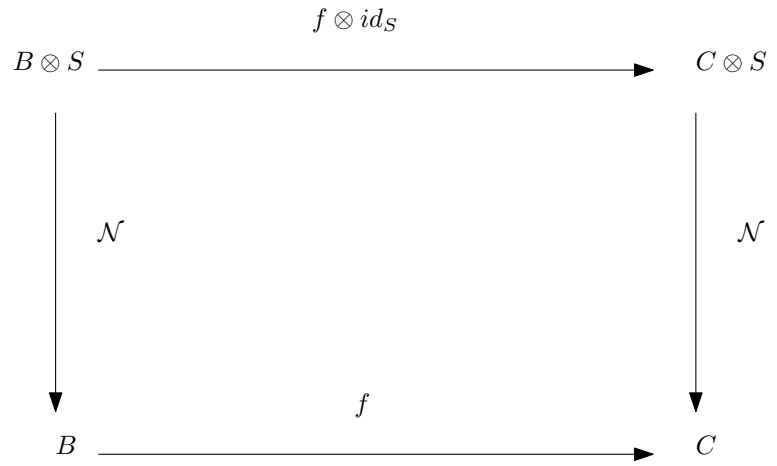
et

$$G(S) \subset Hom_{R-lin}(A\ , S) = Hom_{S-lin}(A \otimes S\ , S) = (A \otimes S)^\vee \cong A^\vee \otimes S\ .$$

■

Pour prouver cette affirmation, nous devons prouver une remarque générale suivante

Lemme 3.1.2 *Soit S une R-algèbre finie et libre, B et C deux R-algèbres. Si $f : B \to C$ est un homomorphisme de R-algèbres, alors*



est commutatif.

Preuve. Soit e_i une base de S sur R, de sorte que $\{1 \otimes e_i\}$ soit une B-base pour $B \otimes S$ et une C-base pour $C \otimes S$.

Si $\alpha \in B \otimes S$,

$$\alpha * (1 \otimes e_i) = \sum_j \mu_{i,j}(1 \otimes e_j) = \sum_j (\mu_{i,j} \otimes e_j).$$

pour $\mu_{i,j} \in B$ et donc $\mathcal{N}(\alpha) = det(\mu_{i,j})$.

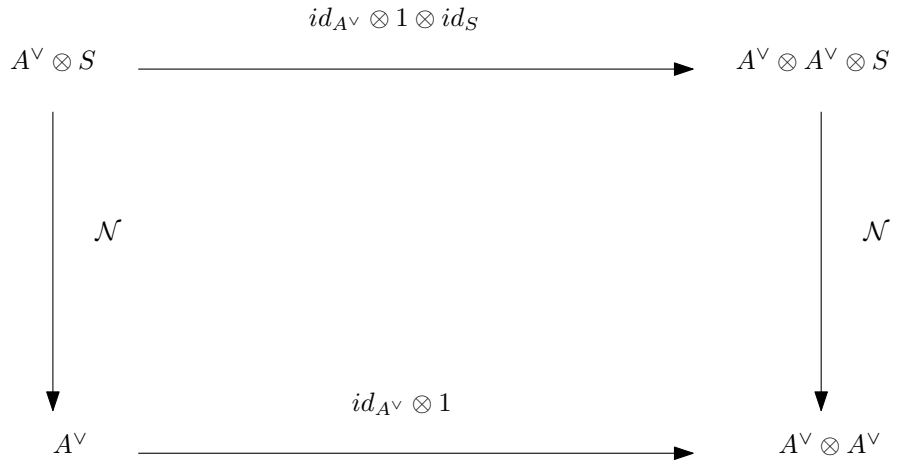
Donc $\mathcal{N}(f \otimes id_S(\alpha))$:

$(f \otimes id_S)(\alpha) * (1 \otimes e_i) = f \otimes id_S(\alpha) * f \otimes id_S(1 \otimes e_i) = f \otimes id_S(\alpha * (1 \otimes e_i)) = \sum_j (f(\mu_{i,j}) \otimes e_j) = \sum_j f(\mu_{i,j})(1 \otimes e_j)$

et $\mathcal{N}(f \otimes id_S(\alpha)) = det(f(\mu_{i,j}) = f(\mathcal{N}(\alpha))$.

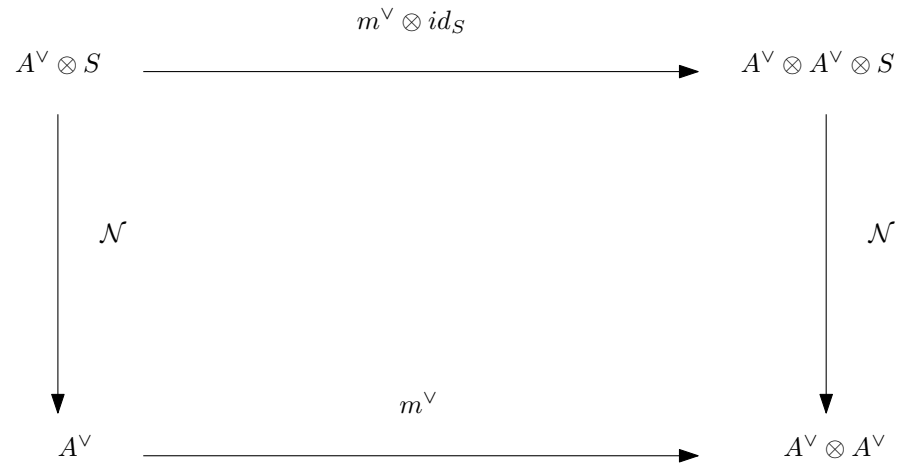
En revenant au lemme, nous devons prouver que si $f \in G(S)$ alors $\mathcal{N}(f) \in G(R)$ ce qui équivaut à prouver que $m^\vee(\mathcal{N}(f)) = \mathcal{N}(f) \otimes \mathcal{N}(f)$. Nous appliquons la remarque à

1.



qui nous dit que si $f \in A^\vee \otimes S$, alors $\mathcal{N}(f) \otimes 1 = \mathcal{N}(f \otimes 1)$;

2.



Remarquons d'abord que $m^\vee \otimes id_S$ est égal à la comultiplication de $A^\vee \otimes S = (A \otimes S)^\vee$; et donc la commutativité du diagramme nous dit que $\mathcal{N}(m^\vee(f)) = m^\vee(\mathcal{N}(f))$.

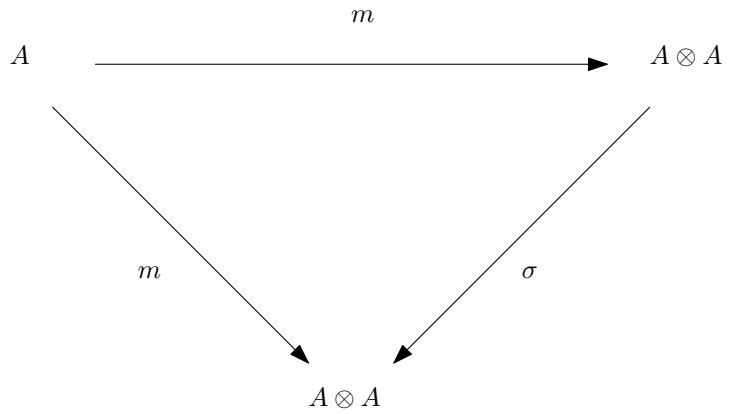
Maintenant si $f \in G(S)$, alors $m^\vee(f) = f \otimes f$. Ainsi $m^\vee(\mathcal{N}(f)) = \mathcal{N}(m^\vee(f)) = \mathcal{N}(f \otimes f) = \mathcal{N}(1 \otimes f)\mathcal{N}(f \otimes 1) = (\mathcal{N}(f) \otimes 1)(1 \otimes \mathcal{N}(f)) = \mathcal{N}(f) \otimes \mathcal{N}(f)$.

Ceci prouve le lemme. ■

Théorème 3.1.4 *[6] Un schéma en groupe S d'ordre p est commutatif et annulé par p.*

Preuve. Par le théorème de Deligne[6], il suffit de prouver la commutativité. On peut supposer que l'on est dans le cas $S = Spec$R où R est un anneau local avec corps de classe résiduel algèbriquement clos. ■

Remarque 3.1.5 *Dans ce cas également, nous devons essentiellement prouver que 2 morphismes coïncident, c'est-à-dire*



où σ change les facteurs. On peut donc se réduire au cas R affine et local. Mais pourquoi peut-on supposer que R a un corps résiduel algèbriquement clos ?

Définition 3.1.1 *Soit (R, m, k) un anneau local où m est l'unique idéal maximal de R et k est le corps résiduel.*

1. *On dit que R est hensélien si pour tout polynôme unitaire $f \in R[X]$ et toute racine $a_0 \in k$ de $\tilde{f}$ (la réduction modulo m de f) tel que $\tilde{f}'(a_0) \neq 0$ il existe un $a \in R$ tel que $f(a) = 0$ et $a_0 = \tilde{a}$.*

2. *On dit que R est strictement hensélien si R est hensélien et que son corps résiduel est séparable algèbriquement clos*

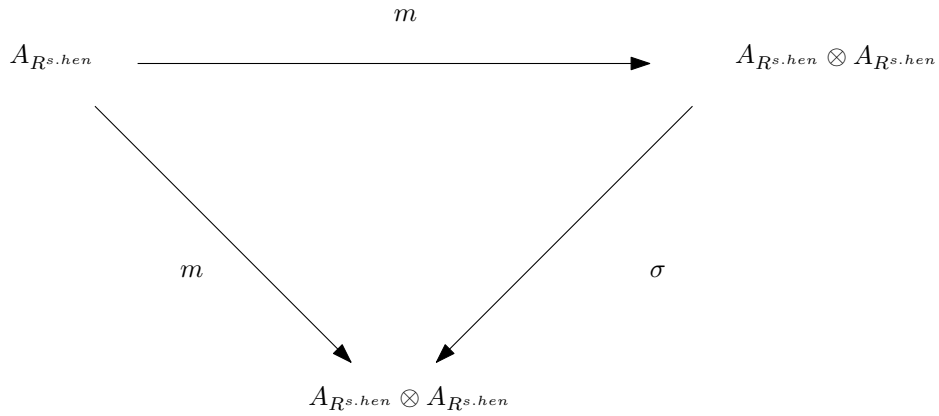
D'aprés le résultat de Nagata pour chaque anneau local R il existe un anneau hensélien R^{hen} et un anneau strictement hensélien $R^{s.hen}$ tels que

$$R \hookrightarrow R^{hen} \hookrightarrow R^{s.hen} .$$

Maintenant, nous savons que A sur R est plat (parce que c'est libre), et donc l'application

$$A \hookrightarrow A \otimes R^{s.hen}.$$

est injectif. Cela signifie que la commutativité du diagramme ci-dessus est impliquée par la commutativité de



Par définition $R^{s.hen}$ est un anneau local avec corps résiduel algèbriquement clos, et ainsi nous concluons.

Lemme 3.1.3 *[6] Soit k un corps algèbriquement clos, et supposons que G = Spec A est un schéma en k-groupe d'ordre premier p. Alors soit G est le schéma en groupe constant, ou le caractéristique de k est p et $G = \mu_{p,k}$ ou $G = \alpha_{p,k}$. En particulier G est commutatif et la k-algèbre A est engendrée par un seul élément.*

Preuve. *On rappelle que l'ordre de G est le produit de l'ordre de G^0 et G/G^0. Puisque G est d'ordre premier, soit il est connexe, soit sa composante connexe est Spec k. Dans le dernier cas $G = \pi^0(G) = Spec(k^{\otimes p})$ car k est algèbriquement clos et donc G est le schéma en groupes constants ; car il n'y a qu'un seul groupe d'ordre p, $G = Z/pZ$. Notez que si nous supposons que $car(k) = 0$, alors $\mu_{p,k}$ est également représenté par $k^{\otimes p}$.*

On peut donc penser que $\mu_{p,k} \neq (Z/pZ)_k$ *car ils ont des multiplications différentes ; en effet, nous verrons qu'ils ont le même et donc dans ce cas, ils sont isomorphes. Notez également que dans le cas* $car(k) = p$ *la situation est complètement différente car* $\mu_{p,k} = Spec(k[X]/(X-1)^p)$ *et donc il est connexe.*

Supposons maintenant que G est connexe. On sait que G possède un nombre fini d'idéaux maximaux et donc un seul idéal maximal ; donc $A = \mathcal{O}(G)$ *est Artinien[1] (car de type fini sur un corps) et local. Nous sommes sur un corps et donc l'idéal d'augmentation I est maximal ; du fait qu'il n'y a qu'un seul idéal maximal, il coïncide avec l'idéal de Jacobson qui est nilpotent (car on est dans un anneau artinien). Maintenant, le lemme de Nakayama [9] déclare que pour un A-module de type fini M, si J est un idéal contenu dans le radical de Jacobson de A, alors* $JM = M$ *implique que* $M = 0$*. Appliquer le lemme à* $J = M = I$ *(notez que I est de type fini car c'est un sous-espace vectoriel de A) on voit que* $I/I^2 \neq 0$*.*

I/I^2 *n'est pas 0 donc il existe une k-dérivation* $d : A \to k$*. En raison de la linéarité de la k-dérivation, d appartient à* $I^\vee \subset A^\vee$ *et* $m_{A^\vee}(d) = d \otimes 1 + 1 \otimes d \in A^\vee \otimes A^\vee$*. Donc k[d] est une sous-bialgèbre de* $A^\vee$*et on ont un morphisme surjectif* $(A^\vee)^\vee = A \to (k[d])^\vee$ *; comme l'ordre de G est premier, alors l'ordre de k[d] est p et donc* $k[d] = A^\vee$*. Maintenant* $G^\vee$ *doit être étale ou connexe. Dans le premier cas* $G = \mu_{p,k}$ *; G est connexe, il n'a qu'un idéal maximal et donc k doit avoir de caractéristique p telle que* $x^p - 1 = (x-1)^p$*. Si* $G^\vee$ *est connexe,* $I^\vee$ *est nilpotent et aussi* $d \in I^\vee$ *il l'est. Comme k[d] est de rang p,* $d^{p-1} \neq 0$ *et* $d^p = 0$ *et en se rappelant que* $m_{A^\vee}(d) = d \otimes 1 + 1 \otimes d$ *on conclut que* $G^\vee = \alpha_{p,k} = G$*. Enfin, comme* $m_{A^\vee}$ *est un morphisme,* $p = 0$ *dans k et donc* $p = car(k)$*.*

Nous pouvons maintenant conclure la preuve du théorème. Notons par ˜ *la réduction modulo l'unique idéal maximal m de R.* $\tilde{G}$*est commutatif par le lemme précédent ; maintenant on veut appliquer le lemme au dual* $(\tilde{G})^\vee = Spec((\tilde{A})^\vee)$*. Noter que*

$$\tilde{A}^\vee = Hom_{R-lin}(A, R) \otimes R/m$$

$$= Hom_{R-lin}(A, R/m)$$

$$= Hom_{R-lin}(A, Hom_{R/m-lin}(R/m, R/m))$$

$$= Hom_{R/m-lin}(A \otimes R/m, R/m)$$

$$= (\tilde{A})^\vee.$$

On se souvient que le lemme nous donne un élément qui engendre l'algèbre ; l'égalité $(\tilde{A}^\vee) = (\tilde{A})^\vee$

implique que cet élément est de la forme $\tilde{x}$ avec $x \in A^\vee$. Maintenant

$$\tilde{R}[x] = k[\tilde{x}] = \tilde{A}^\vee.$$

Une généralisation du lemme de Nakayama dit que si un R-module de type fini M est tel que $M/IM = 0$ pour un idéal $I \subset R$, alors il existe $r \in R$ tel que $r - 1 \in I$ et $rM = 0$. On peut appliquer ce résultat à $A^\vee R[x]$ et $I = m$; on en déduit que $r(A^\vee/R[x]) = 0$ mais r est inversible et donc $A^\vee = R[x]$.

En rappelant que pour chaque R-algèbre S, G(S) est constitué des éléments inversibles de $A^\vee \otimes S$, le fait que $A^\vee$ soit commutatif implique que G est commutatif. ■

Définition 3.1.2 *[5] Un groupe affine G est dit produit semi-direct de ses sous-groupes affines N et Q, noté $G = N \rtimes Q$, si N est normal dans G et l'application*

$$N(S) \times Q(S) \to G(S).$$

$$(n, q) \to nq.$$

est une bijection d'ensembles pour toutes R-algèbres S.

Remarque 3.1.6 *Contrairement à la théorie des groupes, il existe un schéma en groupes de rang p qui agit de manière non-triviale sur un autre schéma en groupes de rang p, à savoir μ_p et α_p. Il existe donc des schémas en groupes de rang p^2 qui ne sont pas commutatifs. Par exemple soit R une $\mathbb{F}_p$-algèbre, et définissons $A = R[\tau, \sigma]$, avec $\tau^p = 1$, $\sigma^p = 0$, $m(\tau) = \tau \otimes \tau$ et $m(\sigma) = \tau \otimes \sigma + \sigma \otimes 1$.*

Le R-schéma en groupes $G = Spec(A)$ est isomorphe au produit semi-direct du schéma en sous-groupes normal défini par $\tau = 1$, qui est isomorphe à $\alpha_{p,R}$, et du schéma en sous-groupes défini par $\sigma = 0$, qui est isomorphe à $\mu_{p,R}$. En prenant $\psi \in \alpha_{p,R}(S)$ et $\phi \in \mu_{p,R}(S)$ on note que

$$\psi * \phi(\sigma) = (\psi \otimes \phi)(\tau \otimes \sigma + \sigma \otimes 1) = \psi(\sigma).$$

$$\psi * \phi(\tau) = (\psi \otimes \phi)(\tau \otimes \tau) = \phi(\tau).$$

et donc l'application ci-dessus $N(S) \times Q(S) \to G(S)$ est une bijection. Pour conclure on prouve que $\alpha_{p,R}$ est un sous-groupe normal choisissant $\psi' \in \alpha_{p,R}(S)$ tel que $\phi * \psi' = \psi * \phi$.

$$\phi * \psi'(\tau) = \phi(\tau).$$

$$\phi * \psi'(\sigma) = \phi(\tau)\psi'(\sigma).$$

et donc il suffit de prendre ψ' tel que

$$\psi'(\sigma) = (\phi(\tau))^{-1}\psi(\sigma).$$

Remarque 3.1.7 *Le théorème déjà démontré a une autre conséquence importante. On sait que pour chaque schéma en groupes $G = Spec(A)$ d'ordre p et chaque S-algèbre R, les éléments de G(R) sont les éléments inversibles de $A_R^\vee$ c'est-à-dire*

$$G(R) = Hom(G_R^\vee, G_{m,R}).$$

Mais maintenant nous connaissons l'information supplémentaire que chaque élément de G(R) est annulé par p, et donc

$$G(R) = Hom(G_R^\vee, \mu_{m,R}).$$

Autrement dit le couple de Cartier

$$G \times G^\vee \to G_{m,S}.$$

facteurs passant par $\mu_{p,S}$.

3.2 Une classification

3.2.1 Vecteurs de Witt

Soit p un entier premier, $(X_0, \cdots, X_n, \cdots)$ une suite d'indéterminées, et considérons les polynômes suivants appelés " polynômes de Witt " :

$$W_0 = X_0$$

$$W_1 = X_0^p + pX_1$$

$$\cdots$$

$$W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$$

$$\cdots$$

Théorème 3.2.1 *Pour tout $\phi \in \mathbb{Z}[X, Y]$, il existe une unique suite $(\phi_0, \phi_1, ..., \phi_n, ...)$ d'éléments de $\mathbb{Z}[X_0, ..., X_n, ..., Y_0, ..., Y_n, ...]$ tel que*

$$W_m(\phi_0, ..., \phi_n, ...) = \phi(W_m(X_0, ...), W_m(Y_0, ...)).$$

avec $m = 0, 1, ...$

En particulier on note $S_0, ..., S_n, ...(resp.P_0, ..., P_n, ...)$ les polynômes $\phi_0, ..., \phi_n, ...$ associé à

$$\phi(X, Y) = X + Y.$$

$$(resp.\phi(X, Y) = XY).$$

Soit maintenant A un anneau commutatif, on note $A^{\mathbb{N}}$ l'ensemble $\{(a_0, ..., a_n, ...)$ *tel que* $a_i \in A\}$.

Étant donné a et $b \in A^{\mathbb{N}}$ on peut définir

$$a + b = (S_0(a, b), ..., S_n(a, b), ...).$$

$$a * b = (P_0(a, b), ..., P_n(a, b), ...).$$

Théorème 3.2.2 *Avec les deux opérations définies ci-dessus, A^N devient un anneau unitaire commutatif appelé l'anneau des vecteurs de Witt à coefficients dans A ; il est noté $W(A)$.*

Remarque 3.2.3 *Notons que l'application*

$$W_* : W(A) \to A^{\mathbb{N}}.$$

$$a = (a_0, ..., a_n, ...) \to (W_0(a), ..., W_n(a), ...).$$

est un morphisme.

Remarque 3.2.4 *Remarquons que les polynômes ϕ_i ne font intervenir que des variables d'indice $\leq i$; on en déduit que les vecteurs $(a_0, ..., a_{n-1})$ forment un anneau que l'on note $W_n(A)$. On a $W_1(A) = A$ et $W(A)$ est la limite projective des anneaux $W_n(A)$ lorsque $n \to \infty$. Si $x \in A$, on définie l'application*

$$\chi : A \to W(A).$$

$$\chi(x) = (x, 0, ..., 0, ...).$$

la composition de χ avec W_* induit une application de A dans $A^{\mathbb{N}}$ qui envoie x vers $(x, x^p, ..., x^{p^n}, ...)$.

En particulier

$$\chi(xy) = \chi(x)\chi(y).$$

Théorème 3.2.5 *$W(\mathbb{F}_p) = \mathbb{Z}_p$ et$W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.*

Remarque 3.2.6 *Prenant $A = \mathbb{F}_p$, on obtient une application multiplicative*

$$\mathbb{F}_p \to W(\mathbb{F}_p) = \mathbb{Z}_p.$$

qui est un inverse à droite de l'application évidente $\mathbb{Z}_p \to \mathbb{F}_p$. On observe aussi que $\chi(0) = 0$ et grâce au lemme de Hensel, pour $m \in \mathbb{F}_p^*$, $\chi(m)$ est l'unique $(p-1)-$ racine de l'unité dans $\mathbb{Z}_p$ dont le reste (mod p) est m.

La restriction de χ à $\mathbb{F}_p^*$ est un générateur du groupe $Hom(\mathbb{F}_p^*, \mathbb{Z}_p^*)$.

3.2.2 Un théorème de classification

Fixons un nombre premier p et supposons que notre schéma fondamental S est sur $Spec(\lambda_p)$ où

$$\lambda_p = \mathbb{Z}[\chi(\mathbb{F}_p), \frac{1}{p(p-1)}] \cap \mathbb{Z}_p.$$

On écrira désormais $\lambda = \lambda_p$.

À la fin de cette section, nous donnerons un théorème qui classe tout schéma en groupes G d'ordre premier p sur S.

Pour avoir aussi une idée pratique de ce qui se passe nous allons procéder en alternant la théorie et l'exemple de base d'un schéma en groupes affines d'ordre 2 sur un corps.

Soit $G = Spec(A)$ un S-schéma en groupes d'ordre p.Par le théorème 3. 1. 1 nous savons que $\mathbb{F}_p^*$ agit sur G, et nous pouvons donc considérer A et I comme un faisceau de modules sur l'algèbre de groupe $\mathcal{O}_S[\mathbb{F}_p^*]$.

Pour chaque $i \in \mathbb{Z}$, soit $I_i = e_i I$ où e_i est l'opérateur $\mathcal{O}_S$-linéaire

$$e_i = \frac{1}{p-1} \sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m)[m].$$

Puisque χ est d'ordre $p-1$, e_i et I_i ne dépendent que de i $mod(p-1)$.

Lemme 3.2.1 *[6] On a $I = \sum_{i=1,\dots,p-1} I_i$ (somme directe). Pour chaque i, I_i est un O_S-module inversible, composé des sections locales de A tel que : $[m]f = \chi^i(m)f$ pour tout $m \in \mathbb{F}_p$. On a $I_iI_j \subset I_{i+j}$ pour tout i et j et $I_1^i = I_i$ pour $1 \leq i \leq p-1$.*

Preuve. Tout d'abord les opérateurs e_i sont des idempotents orthogonaux et leur somme est 1, donc I est la somme directe des I_i pour $1 \leq i \leq p-1$. On note alors que e_i vérifie $[m]e_i = \chi^i(m)e_i$ pour $m \in \mathbb{F}_p^*$ et donc I_i est constitué des sections locales f de I tel que : $[m]f = \chi^i(m)f$ pour tout $m \in \mathbb{F}_p^*$ ou de manière équivalente des sections locales $f \in A$ tel que : $[m]f = \chi^i(m)f$ pour tout $m \in \mathbb{F}_p^*$. Cela découle du fait que $\chi(0) = 0$ et $[0] = e \circ \epsilon$ donc l'égalité $e \circ \epsilon(f) = 0$ implique que $f \in I$.

Prenons maintenant $f \in I_i$ et $g \in I_j$; en utilisant le fait que $[m]fg = [m]f[m]g$ on en déduit que

$$[m]fg = [m]f[m]g = \chi^i(m)f\chi^i(m)g = \chi^{i+j}(m)fg.$$

et donc $I_iI_j \subset I_{i+j}$.

Nous savons que A est un faisceau localement libre, donc nous en déduisons que I et I_i sont également des O_S-modules localement libres ; en particulier puisque I est de rang $p-1$, les I_i sont de rang r_i avec $r_1 + \dots + r_{p-1} = p-1$.

Pour prouver que $r_i = 1$ pour chaque i et que $I_1^i = I_i$ pour $1 \leq i \leq p-1$ il suffit d'estimer le cas $S = Spec(k)$, avec k un corps algèbriquement clos. On peut se ramener au cas affine sur $S = SpecR$.

Il s'agit ici de calculer le rang de I_i qui est la dimension de $I_i \otimes R(p)$ (où R(p) désigne le corps des fractions de R/p) ; cette dimension reste la même si on la calcule sur une extension algèbriquement clos de $R(p)$. Enfin on veut exposer dans ce cas une section $f_1 \in I_1$ tel que : $f_1^i \neq 0$ (ce qui revient à demander que $f_1^i \notin k$ car $\epsilon(k) = k$ et $\epsilon(I) = 0$) pour $1 \leq i \leq p-1$; alors $kf_1^i \subset I_i$ implique $1 \leq r_i$, mais $r_i \leq 1$ et donc $r_i = 1$ et $kf_1^i = I_i$. D'après le lemme 3. 1. 3, il n'y a que trois cas à considérer, à savoir $G \cong (\mathbb{Z}/p\mathbb{Z})_k$, $\alpha_{p,k}$ ou $\mu_{p,k}$ et les 2 derniers uniquement pour $car(k) = p$, auquel cas $\chi(m) = m$. Si $G \cong (\mathbb{Z}/p\mathbb{Z})_k$, alors A est l'algèbre des fonctions de $\mathbb{F}_p$ à valeurs dans k et $([m]f)(n) = f(mn)$ pour $f \in A$ et $m, n \in \mathbb{F}_p$. χ est un bon choix, en effet, $\chi^i \neq 0$ car c'est un générateur de $Hom(\mathbb{F}_p^*, \mathbb{Z}_p^*)$ et il appartient à I_1 car

$$([m]\chi)(n) = \chi(mn) = \chi(m)\chi(n).$$

Si $G = \alpha_{p,k}$ (resp. $\mu_{p,k}$), alors $A = k[t]$ avec $t^p = 0$ et $m(t) = t \otimes 1 + 1 \otimes t$ et donc $[m]t = mt$ (resp. $s(1+t) = (1+t) \otimes (1+t)$ et donc $[m](1+t) = (1+t)^m - 1$). En utilisant le fait que dans les deux

cas

$$[m]t \equiv mt \equiv \chi(m)t(mod\ t^2).$$

en particulier $e_1 t \equiv t \not\equiv 0(mod\ t^2)$, et on peut donc prendre $f_1 = e_1 t$. ■

Ce lemme nous montre que la structure en modules d'un schéma en groupes finis d'ordre premier est complètement déterminée par un module inversible.

Exemple $\mu_{p,\lambda}$. Dans cette section nous voulons réécrire l'algèbre et la structure de groupe de $\mu_{p,\lambda}$. Nous introduirons également quelques notations nécessaires à notre objectif principal : la classification.

Soit $\mu_{p,\lambda} = Spec(B)$ avec $B = \lambda[z]$ et $z^p = 1$. La comultiplication dans B est donnée par $m(z) = z \otimes z$ et donc $[m]z = z^m$ pour tout $m \in \mathbb{F}_p$. On se rappelle que $\epsilon(z) = 1$ donc l'idéal d'augmentation est $J = B(z-1)$ et il a une λ-base constituée des éléments $z^m - 1$ pour $m \in \mathbb{F}_p^*$:

$$B(z-1) = \lambda(z-1) + ... + \lambda(z^{p-1} - 1).$$

Maintenant pour chaque $i \in \mathbb{Z}$ on pose

$$y_i = (p-1)e_i(1-z) = \sum_{m\in\mathbb{F}_p^*} \chi^{-i}(m)(1-z^m) = \begin{cases} p - \sum_{m\in\mathbb{F}_p} & si \quad i \equiv 0 mod(p-1) \\ -\sum_{m\in\mathbb{F}_p^*} \chi^{-i}(m) z^m & si \quad i \not\equiv 0 mod(p-1) \end{cases}$$

Notons que y_i ne dépend que de i$mod(p-1)$. Alors

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m) y_i$$

Pour $m \in \mathbb{F}_p^*$ et

$$m(y_i) - y_i \otimes 1 - 1 \otimes y_i = \sum_{m\in\mathbb{F}_p^*} \chi^{-i}(m)((1-z^m) \otimes (1-z^m))$$

$$\frac{-1}{(p-1)^2} \sum_{m\in\mathbb{F}_p^*} \chi^{-i}(m) \sum_{j=1}^{p-1} \sum_{k=1}^{p-1} \chi^j(m)\chi^k(m) y_i \otimes y_k$$

$$= \frac{-1}{p-1} \sum_{j+k\equiv i(p-1)} y_j \otimes y_k$$

Par conséquent, la comultiplication fonctionne comme

$$m(y_i) = y_i \otimes 1 + 1 \otimes y_i + \frac{1}{1-p} \sum_{j=1}^{p-1} y_i \otimes y_{i-j}.$$

Noter que

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m) y_i.$$

implique que

$$J = \lambda y_1 + ... + \lambda y_{p-1}.$$

et donc $J_i = \lambda y_i$ pour chaque $i \in \mathbb{Z}$ en fait $\lambda y_i \subset J_i$ car $y_i \in J_i$ et l'égalité s'ensuit car les λy_i avec $1 \leq i \leq p-1$ engendrent complètement J. Posons $y = y_1$ on peut de définir une suite d'éléments $w_1 = 1, w_2$, dans λ par $y^i = w_i y_i$.

Notez que c'est une bonne définition car dans ce cas les I_i sont des λ-modules libres et il n'y a donc qu'un seul choix possible pour w_i.

Proposition 3.2.1 *[6] Les éléments w_i sont inversibles pour $1 \leq i \leq p-1$, et $w_p = pw_{p-1}$. Nous avons $B = \lambda[y]$, avec $y^p = w_p y_p$, et*

1. $m(y) = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$.

2. $[m]y = \chi(m)y$ *pour* $m \in \mathbb{F}_p$.

3. $w_i \equiv i!(mod p)$ *pour* $1 \leq i \leq p-1$.

4. $z = 1 + \frac{1}{1-p}(y + \frac{y^2}{w_2} + ... + \frac{y^{p-1}}{w_{p-1}})$.

Preuve. Par Lemme 3. 2. 1, nous savons que

$$\lambda y^i = (\lambda y)^i = (J_1)^i = J_i = \lambda y_i.$$

donc les w_i sont inversibles pour $1 \leq i \leq p-1$. On a $(z-1)^p \equiv 0(mod\ p)$, donc $y^p \equiv 0(mod\ p)$; de plus

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m) y_i.$$

et le fait que $\frac{1}{1-p} \equiv 1(mod\ p)$ on en déduit que

$$z \equiv 1 + y + \frac{y^2}{w_2} + ... + \frac{y^{p-1}}{w_{p-1}}(mod\ p).$$

Pour prouver que $w_i \equiv i!(mod\ p)$ il suffit de comparer les coefficients de $y^i \otimes y$, $1 \leq i < p-1$ de

$$m(z) = (1 + y + ... + \frac{y^{p-1}}{w_{p-1}}) \otimes (1 + y + ... + \frac{y^{p-1}}{w_{p-1}}) \equiv 1 + m(y) + ... + \frac{(m(y))^{p-1}}{w_{p-1}}(mod\ p).$$

ce qui nous donne $w^{i+1} \equiv (i+1)w_i$ et en se rappelant que $w_1 = 1$ on conclut.

La dernière chose à prouver est que $w_p = pw_{p-1}$. Choisissez un plongement $\lambda \to K$ où K est un corps avec une primitive racine d'ordre p d'unité ζ et étend le plongement à $\lambda[z]$ en envoyant z vers ζ ; le corps peut être par exemple une clôture algèbrique de $\mathbb{Q}_p \supset \mathbb{Z}_p \supset \lambda$. Soit $y_i \to \eta_i$ et renommez $\eta = \eta_1$. Utilisant le fait que

$$y_{p-1} = p - \sum_{m \in \mathbb{F}_p} z^m.$$

on observe que $\eta_{p-1} = p \neq 0$ et comme aussi $w_{p-1} \neq 0$, on conclut que $\eta \neq 0$. On obtient donc

$$pw_{p-1} = \eta_{p-1}w_{p-1} = \eta^{p-1} = \frac{\eta^p}{\eta} = w_p.$$

car on plonge λ dans K, alors $pw_{p-1} = w_p$ aussi dans λ. ■

Lemme 3.2.2 *[6] Le $w_i \in \lambda$ peut être calculé à partir de $w_1 = 1$ et des relations suivantes :*

$$\frac{w_{i+j}}{w_i w_j} = \begin{cases} p & si \quad i \equiv 0 \quad ou \quad j \equiv 0 \\ (-1)^i & si \quad i \not\equiv 0, j \not\equiv 0 \quad mais \quad i+j \equiv 0 \\ (-1)^{i+j+1}\mathcal{J}(-i,-j) & si \quad i \not\equiv 0, j \not\equiv 0 \quad et \quad i+j \not\equiv 0 \end{cases}$$

où les congruences sont mod$(p-1)$, et où $\mathcal{J}$ désigne les sommes de Jacobi

$$\mathcal{J}(i,j) = \sum_{m+n=-1, m,n \in \mathbb{F}_p^*} \chi^i(m)\chi^j(n).$$

Preuve. Choisissez un plongement $\lambda \to K$ comme dans la preuve précédente ; alors

$$\frac{w_{i+j}}{w_i w_j} = \frac{\eta_i \eta_j}{\eta_{i+j}}.$$

car

$$w_{i+j}\eta_{i+j} = \eta^{i+j} = \eta^i \eta^j = w_i \eta_i w_j \eta_j.$$

Voyons le premier cas : supposons que $i \equiv 0$, alors $\eta_i = p$ et $\eta_{i+j} = \eta_j$, donc

$$\frac{w_{i+j}}{w_i w_j} = \frac{\eta_i \eta_j}{\eta_{i+j}} = \frac{p\eta_j}{\eta_j} = p.$$

Supposons maintenant $i \not\equiv 0$ et $j \not\equiv 0 (mod(p-1))$; alors $p \neq 2$ et $\chi(-1) = -1$; soient l, m, n parcourir dans $\mathbb{F}_p$, nous avons

$$\eta_i \eta_j = (\textstyle\sum_{m \neq 0} \chi^{-i}(\mathrm{m})\zeta^m)(\sum_{n \neq 0} \chi^{-j}(\mathrm{n})\zeta^n)$$

$$=\sum_{mn\neq 0}\chi^{-i}(\mathrm{m})\chi^{-j}(\mathrm{n})\zeta^{i+j}$$
$$=\sum_{l}\zeta^{l}\sum_{m+n=l,mn\neq 0}\chi^{-i}(\mathrm{m})\chi^{-j}(\mathrm{n})$$
$$=\sum_{n\neq 0}\chi^{-i}(-\mathrm{n})\chi^{-j}(\mathrm{n})+\sum_{l\neq 0}\sum_{m+n=-1,mn\neq 0}\zeta^{l}\chi^{-i}(-\mathrm{lm})\chi^{-j}(-\mathrm{ln})$$
$$= (-1)^{i}\sum_{n\neq 0}\chi^{-(i+j)}(n) + (-1)^{(i+j)}\sum_{l\neq 0}\zeta^{l}\chi^{-(i+j)}(l) * \sum_{m+n=-1,mn\neq 0}\chi^{-i}(m)\chi^{-j}(n) =$$
$$\begin{cases}(-1)^{i+j+1}\eta_{i+j}\mathcal{J}(-i,-j) & si \quad i+j\not\equiv 0\\ (-1)^{i}(p-1)-\sum_{m+n=-1,mn\neq 0}\chi^{i}(\frac{n}{m}) & si \quad i+j\equiv 0\end{cases}$$

Prenons maintenant notre exemple de schéma en groupe d'ordre 2 sur un corps k. Nous aimerions trouver une paire d'"objets" qui, en quelque sorte, le définissent. La structure du module est $k\oplus k$ grâce au Lemme 3. 2. 1. Donc, les deux paramètres que nous trouvons doivent concerner la structure de l'algèbre et la structure du groupe. Considérons d'abord $a \in k$ tel que $x^2 = ax$ où x est un générateur de I. En utilisant le fait que $Id = \mu\circ(Id\otimes\epsilon)\circ m = \mu\circ(\epsilon\circ Id)\circ m$ il est immédiat de vérifier que $m(x) = x\otimes 1+1\otimes x-c(x\otimes x)$. Donc (a, c) pourraient être les bons objets. Or on affirme que $ac = 2$. On remarque que $m(x)^2 = m(x^2) = am(x)$ et donc en comparant les coefficients de $x \otimes x$ dans l'écriture de $m(x)^2$ et de $am(x)$ on obtenir $ac = a^2c^2 + +2 - 4ac$ ce qui implique $(ac - 1)(ac - 2) = 0$. Or l'inverse de 1 est 1 et donc $\epsilon \circ i = \epsilon$ et donc $i(x) \in I$ et $i(x) = \beta x$ (avec $\beta \in k$ et $\beta^2 = 1$ car $\beta \circ \beta = id$). On observe aussi que $x \otimes 1 + 1 \otimes \beta x - c\beta x \otimes x$ devient 0 sous multiplication et donc $1 + \beta = ac\beta$. En multipliant par β on obtient $ac = \beta + 1$, et donc $ac - 1$ est inversible. En se souvenant que $(ac - 1)(ac - 2) = 0$ on en déduit que $ac = 2$ et donc $\beta = 1$.

Voyons d'abord comment généraliser cette idée sur des schémas en groupes affines sur un anneau local. Soit G un S- groupe d'ordre p avec $A = \mathcal{O}_G$.

Supposons maintenant que $\mathcal{O}_S$ est un anneau local et complet. Lemme 3. 2. 1 nous dit que I_i est libre de rang 1 sur $\mathcal{O}_S$ et donc si x est un générateur de I_1 alors

$$A = \mathcal{O}_S \oplus \mathcal{O}_S x \oplus \mathcal{O}_S x^2 \oplus ... \oplus \mathcal{O}_S x^{p-1}.$$

En particulier du fait que $I_iI_j \subseteq I_{i+j}$ pour tout $i, j \in N$ on voit qu'il existe $a \in \mathcal{O}_S$ tel que :

$$x^p = ax.$$

et soit $a^\vee$ l'analogue dans $A^\vee$. Dans ce cas nous avons considéré un autre représentant de la multiplication de groupe par rapport à l'exemple précédent ; mais nous verrons qu'ils sont fondamentalement les mêmes. ■

Remarque 3.2.7 *Supposons que M soit un autre S-groupe isomorphe à G. Alors $B = \mathcal{O}_M \cong A$. On a si J est l'idéal d'augmentation de B, alors l'isomorphisme envoie J dans I et J_1 dans I_1. En particulier*

un générateur de J_1 est envoyé dans un générateur de I_1 et est donc de la forme $y = ux$ où $u \in \mathcal{O}_S$ est un élément inversible et x est un générateur de I_1. Alors

$$y^p = u^p x^p = u^p ax = au^{p-1}y.$$

et ainsi à chaque classe isomorphe de groupes on peut assigner la classe d'équivalence de la multiplication où $[a_1] = [a_2] \iff a_1 = u^{p-1}a_2$ pour certains $u \in \mathcal{O}_S$ inversibles.

Rappelons maintenant que nous avons prouvé que

$$G \times G^\vee \to G_{m,S}.$$

factors through $\mu_{p,S}$. Cela revient à dire qu'on a un morphisme

$$\phi : \mathcal{O}_S \otimes_\lambda \lambda[y] = \mathcal{O}_S[y] \to A \otimes A^\vee.$$

Le Lemme suivant est la version affine et locale du Lemme 3. 2. 4 donc nous l'énonçons et reportons la preuve dans le cas général.

Lemme 3.2.3 *L'image $\phi(y) = x \otimes x'$ est un générateur de $I_1 \otimes I_1^\vee$ et $aa^\vee = w_p$ avec a (resp. $a^\vee$) tel que : $x^p = ax$ ($resp. x'^p = a^\vee x'$).*

Nous continuons maintenant notre discussion sur le S-groupe G où S est un schéma général sur Spec(λ). Soit

$$S_{\mathcal{O}_S}[I_1] = \mathcal{O}_S \oplus I_1 \oplus I_1^{\otimes 2} \oplus ...$$

notons l'algèbre symétrique engendrée par I_1 sur $\mathcal{O}_S$; notez que dans ce cas il existe des modules inversibles qui ne sont pas triviaux. On sait que le morphisme $\mathcal{S}_{\mathcal{O}_S}[I_1] \to A$ induit par l'inclusion est surjectif, et que son noyau est l'idéal engendré par $(a-1) \otimes I_1^{\otimes p}$, où

$$a \in \Gamma(S, I_1^{\otimes(1-p)}) = Hom_{\mathcal{O}_S}(I_1^{\otimes p}, I_1).$$

est l'élément correspondant au morphisme $I_1^{\otimes p} \to I_1$ induit par la multiplication dans A ; nous insistons sur le fait que la présence de modules inversibles non triviaux nous interdit de voir a comme un élément de $\mathcal{O}_S$.

Soit $G^\vee = Spec(A^\vee)$ le dual de Cartier de G et soit $I^\vee$, $I_i^\vee$ et $a^\vee$ les analogues pour $G^\vee$ de I, I_i et a pour G. Notez que la notation est cohérente car $(I_A)^\vee = I_{A^\vee}$ et $(I_i)^\vee = (e_i I_A)^\vee = (I^\vee)_i$.

Lemme 3.2.4 *[6] L'image $\phi(y)$ de y est une section génératrice de $I_1 \otimes I_1^\vee$; si on l'utilise pour identifier*

$I_1^\vee$ *avec* $I_l^{\otimes(-1)}$, *alors* $a \otimes a^\vee = w_p 1_{O_S}$.

Preuve. L'application Cartier pairing $(\zeta, \zeta') \to < \zeta, \zeta' >$ satisfait

$$< \zeta^m, (\zeta')^n > = < \zeta , \zeta' >^{mn} .$$

Donc, pour tout $m, n \in \mathbb{F}_p$

$$([m] \otimes [n])\phi(y) = \phi([mn]y) = \phi(\chi(mn)y) = \chi(m)\chi(n)\phi(y).$$

donc $\phi(y) \in \Gamma(S, I_1 \otimes I_1^\vee)$. On a $\phi(y)$ ne s'annule en aucun point $s \in S$, en effet, si $\phi(y) = 0$ alors l'application Cartier pairing sur la fibre $G_s \times G_s^\vee \to G_{m,s}$ est dégenérate ; c'est impossible et l'idée que $G = Hom(G^\vee, G_m)$, et donc si $< \zeta, \zeta^\vee >= \zeta(\zeta^\vee) = 0$ pour tout $\zeta^\vee \in G^\vee$ alors $\zeta = 0$.

Puisque ϕ est un morphisme d'algèbres,

$$w_p\phi(y) = (\phi(y))^p = (\phi(y))^{\otimes_p} \otimes a \otimes a^\vee.$$

et cela montre que $a \otimes a^\vee = w_p$ si on identifie $I_1 \otimes I_1^\vee$ avec O_S de telle sorte que $\phi(y) = 1$.

Enfin, nous sommes prêts à exposer le théorème principal, mais nous voulons d'abord donner une idée de ce qui se passe en utilisant notre exemple.

La partie la plus intéressante du théorème est lorsqu'il explique comment construire un schéma en groupes à partir d'un module inversible et d'une factorisation de p.

Notons qu'un groupe générique d'ordre 2 a une structure d'algèbre et de groupe très similaire à celle de $\mu_{2,k}$. En effet nous avons vu que $\mu_{2,k}$ est engendré par un élément y tel que :

$$y^2 = 2y \; et \; m(y) = y \otimes 1 + 1 \otimes y - y \otimes y.$$

En particulier si on essaie de déformer le générateur en le multipliant par un élément inversible $Y = u^{-1}y$ avec $u \in k$ alors

$$Y^2 = 2u^{-1}Y \; et \; m(Y) = Y \otimes 1 + 1 \otimes Y - uY \otimes Y.$$

Donc, en prenant $u = 2/a = b$, nous obtenons le schéma en groupe souhaité. ■

Théorème 3.2.8 *[6] Pour tout schéma S sur Spec*(λ)*, l'application*

$$G \to (I_1^\vee, a, a^\vee).$$

discuté ci-dessus donne une bijection entre les classes d'isomorphismes des S-groupes d'ordre p et les classes d'isomorphismes des triplets (L, a, b) *consistant en un* $\mathcal{O}_S$*-module inversible* L*, une section* $a \in \Gamma(S, L^{\otimes(p-1)})$*, et une section* $b \in \Gamma(S, L^{\otimes(1-p)})$*, telle que* $a \otimes b = w_p 1_{\mathcal{O}_S}$.

Preuve. On prouve d'abord l'injectivité de l'application ; à partir d'un triplet $(I^\vee, a, a^\vee)$ on peut reconstruire la structure de S-schéma de G et $G^\vee$ (d'abord sans la structure de S-groupe) avec le morphisme de Cartier $G \times G^\vee \to \mu_{p,S}$. En effet A est le quotient de l'algèbre symétrique $S_{\mathcal{O}_S}[(I_1^\vee)^{\otimes(-1)}]$ par un idéal déterminé par a, $A^\vee$ est le quotient de $S_{\mathcal{O}_S}[I_1^\vee]$ par un idéal déterminé par $a^\vee$, et le morphisme $\phi : B[y] \to A \otimes A^\vee$ est déterminé par $\phi(y) = 1 \in (I_1^\vee)^{\otimes(-1)} \otimes I_1^\vee = \mathcal{O}_S$. Mais le morphisme de Cartier détermine la structure de groupe de G et $G^\vee$car il donne pour chaque S-schéma T une application

$$G(T) \hookrightarrow Hom_{T-schemas}(G_T^\vee, \mu_{p,T}).$$

qui identifie G(T) comme un sous-groupe de $\mu_p(G_T^\vee)$. La loi de composition ainsi induite sur le foncteur $T \to G(T)$ détermine la loi de composition dans G.

Maintenant, nous devons montrer que tout triplet (L, a, b) provient d'un schéma en groupe. Le problème est local sur la base S, on peut donc supposer S=Spec R où R est un anneau local, $L = R$ et a, b peut être considéré comme élément de R tel que $ab = w_p * 1_R$.

Soit F le corps des fractions de λ, et soit U une indéterminée. On sait que $\mu_{p,F(U)}$ est égal à $Spec(A)$ où

$$A = F(U)[y] \; et \; y^p = w_p y.$$

avec

$$m(y) = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{1}{w_i w_{p-i}} y^i \otimes y^{p-i}.$$

et

$$[m]y = \chi(m)y \; .$$

Soit $Y = U^{-1}y \in A$. Alors

$$A = F(U)[Y], \; Y^p = w_p U^{1-p} Y.$$

et

$$m(Y) = Y \otimes 1 + 1 \otimes Y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{U^{p-1}}{w_i w_{p-i}} Y^i \otimes Y^{p-i}.$$

et $[m]Y = \chi(m)Y$. Soit

$$R_0 = \lambda[w_p U^{1-p}, U^{p-1}] \subset F(U).$$

et

$$C = R_0[Y] \subset A.$$

A partir des formules ci-dessus, on voit que C est libre de rang p sur R_0 et que $m(C) \subset C \otimes_{R_0} C$. Aussi $[-1]C \subset C$. On définit donc un R_0-groupe G d'ordre p par $G = Spec(C)$ avec la multiplication induite par m. On a

$$R_0 \cong \lambda[X_1, X_2]/(X_1X_2 - w_p).$$

Ainsi le triplet (R, a, b) détermine un morphisme d'λ-algèbres $h : R_0 \to R$ tel que $h(w_pU^{1-p}) = a$ et $h(U^{p-1}) = b$, et alors il résulte des formules explicites de la structure de G que le triplet (R, a, b) vient de G_R déduit de G par l'extension de base via h. ■

Nous énonçons maintenant le théorème dans le cas local.

Théorème 3.2.9 *Pour tout schéma S sur $Spec(\lambda)$, l'application $G \to (a, c)$ où $c = a^\vee/w_{p-1}$ donne une bijection entre les classes d'isomorphisme des S-groupes d'ordre p et les classes d'équivalence de factorisation $p = ac$ où 2 factorisations $p = a_1c_1$ et $p = a_2c_2$ sont équivalentes s'il existe un élément inversible $u \in \mathcal{O}_S$ tel que : $a_2 = u^{p-1}a_1$ et $c_2 = u^{1-p}c_1$.*

3.2.3 Exemples

Dans cette section, nous allons essayer de classer tous les schémas en groupe d'ordre p sur les anneaux de base suivants ; on sait que grâce au théorème 3. 2. 5 ce problème est équivalent à trouver les classes d'équivalence des factorisations de p.

1. $\mathbb{F}_p$.

Proposition 3.2.2 *Les schémas en groupe d'ordre p sur $\mathbb{F}_p$ sont de la forme (0, 0), (0, a) ou (a, 0) avec $a \in \mathbb{F}_p$ différent de zéro.*

Preuve. (0, 0), (0, a) ou (a, 0) avec $a \in \mathbb{F}_p$ différent de zéro sont toutes les factorisations possibles de p dans $\mathbb{F}_p$.

Nous n'avons donc qu'à montrer qu'ils ne sont pas équivalents. Fixant $a \in \mathbb{F}_p$ non nul, clairement les couples (a, 0), (0, 0) et (0, a) ne sont pas équivalents.

Il reste à prouver que si a, b sont non nuls et différents l'un de l'autre alors (a, 0) et (b, 0) ne sont pas équivalents (ou ce qui revient au même que (0, a) et (0, b) ne sont pas équivalents). Supposons qu'ils sont, alors il existe une unité $u \in \mathbb{F}_p$ telle que $a * u^{p-1} = b$; mais $u^{p-1} = 1$ ce qui implique que $a = b$; absurde. ■

En particulier les couples $(0,0),(0,1),(1,0)$ représentent respectivement $\alpha_{p,\mathbb{F}_p}$, $\mu_{p,\mathbb{F}_p}$ *et* $(\mathbb{Z}/p\mathbb{Z})_{\mathbb{F}_p}$.

2. k algèbriquement clos.

Proposition 3.2.3 *Soit k un corps algèbriquement clos sur λ_p. Si k est de caractéristique 0, alors il n'existe qu'un seul schéma en groupes d'ordre p. Si k est de caractéristique p, alors les seuls schémas en groupe d'ordre p sont $\alpha_{p,k}$, $\mu_{p,k}$ et $(\mathbb{Z}/p\mathbb{Z})_k$.*

Nous observons que nous connaissons déjà ce résultat grâce au Lemme 3. 1. 3 ; voyons une preuve plus facile.

Preuve. Si $car(k) = 0$, alors p est inversible et donc chacun de ses facteurs aussi. Notons que deux factorisations distinctes sont de la forme (a, b), $(a * u, b * u^{-1})$. Nous devons essentiellement prouver que u admet un $(p-1)$ ième racine. Mais dans un corps algèbriquement clos chaque polynôme a racine en particulier $x^{p-1} - u$; cela implique qu'il n'existe qu'un seul groupe.

Si $car(k) = p$, les factorisations possibles sont (0, 0), (0, z) et (z, 0) où z est une unité ; mais pour la même raison qu'avant les factorisations (0, z), (0 , z′) sont équivalents (et aussi dans le cas dual (z, 0), (z′, 0)) ce qui implique que les schémas en groupe sont représentés par (0, 0), (1, 0) et (0, 1) qui correspondent respectivement à $\alpha_{p,k}$, $(\mathbb{Z}p\mathbb{Z})_k$ et $\mu_{p,k}$. ■

3. $\mathbb{Z}_p$

Théorème 3.2.10 (Lemme de Hensel) *Soit R un anneau complet par rapport à l'idéal m, et soit $f(x) \in R[x]$ un polynôme. Si a est une racine approchée de f au sens où*

$$f(a) = 0 (mod\, f'(a)^2 m).$$

alors il y a une racine b de f près de a en sens que

$$f(b) = 0 \text{ et } b = a (mod\, f'(a) m).$$

Si f′(a) est un diviseur non nul dans R, alors b est unique.

Remarquons tout d'abord que $\mathbb{Z}_p$ est un domaine de caractéristique 0 ce qui implique qu'un groupe affine est totalement déterminé par sa structure algèbrique. Évidemment, toute factorisation de p doit être de la forme $(p * s^{-1}, s)$ ou $(s, p * s^{-1})$ où s est une unité.

Lemme 3.2.5 *Soit $z \in \mathbb{Z}_p$ une unité. L'équation $x^{p-1} = z$ admet des solutions dans $\mathbb{Z}_p$ si et seulement si $z = 1$ dans $\mathbb{Z}/p\mathbb{Z}$.*

Preuve. Supposons que l'équation admet une solution y. z est une unité et donc $z \neq 0 \in \mathbb{Z}/p\mathbb{Z}$ ce qui implique que $y \neq 0 \in \mathbb{Z}/p\mathbb{Z}$. Mais $y \in \mathbb{Z}/p\mathbb{Z}$ est une unité et le résultat découle du petit théorème de Fermat.

Si $z = 1$ dans $\mathbb{Z}/p\mathbb{Z}$ alors l'équation a une solution dans $\mathbb{Z}/p\mathbb{Z}$, mais d'après le lemme de Hensel il y a une solution aussi dans $\mathbb{Z}_p$ ■

Corollaire 3.2.1 *Pour chaque $1 \leq i \leq p-1$ choisir $a_i \in \mathbb{Z}_p$ tel que $a_i = i$ dans $\mathbb{Z}/p\mathbb{Z}$. Les schémas en groupes d'ordre p sur $\mathbb{Z}_p$ sont de la forme $(a_i, p * a_i^{-1})$ ou $(p * a_i^{-1}, a_i)$.*

Preuve. On a chaque $1 \leq i < j \leq p-1$ il y a aucun élément inversible $u \in \mathbb{Z}_p$ tel que $a_i * u^{p-1} = p * a_j^{-1}$; donc pour tout $1 \leq i < j \leq p-1$ les couples $(a_i, p * a_i^{-1})$ et $(p * a_j^{-1} a_j)$ ne sont pas équivalents.

On veut maintenant montrer que deux couples de la forme $(a, p * a^{-1})$ et $(b, p * b^{-1})$ avec a et b des unités, sont équivalentes si et seulement si $a = b$ dans $\mathbb{Z}/p\mathbb{Z}$. $(a, p * a^{-1})$ est équivalent à $(b, p * b^{-1}) \iff$ il existe u unité telle que $a * u^{p-1} = b \iff u^{p-1} = b * a^{-1} \iff$ $b * a^{-1} = 1$ dans $\mathbb{Z}/p\mathbb{Z}$ grâce au lemme 3. 2. 5 on a $a = b$ dans $\mathbb{Z}/p\mathbb{Z}$ ■

4. k[[t]]

Proposition 3.2.4 *Si k de caractéristique 0, alors chaque schéma en groupe d'ordre p sur k[[t]] est obtenu à partir d'un schéma en groupe unique sur k.*

Preuve. Rappelons qu'un élément de k[[t]] est une unité si et seulement si son terme constant est différent de zéro. Toute factorisation de p est aussi ici de la forme $(u, p * u^{-1})$ où u est une unité ; note que nous avons considéré aussi les factorisations de la forme $(p * u^{-1}, u)$ car p est inversible. Notre problème se réduit à trouver si l'équation $x^{p-1} = u$ a des solutions ou non. Le lemme de Hensel simplifie le problème en indiquant que l'équation a une solution dans k[[t]] si et seulement si elle a une solution dans k. Ceci permet en particulier de conclure que les schémas en groupes d'ordre p sur k[[t]] sont en bijection avec ceux sur k. ■

Proposition 3.2.5 *Si k de caractéristique p, alors chaque schéma en groupes d'ordre p sur k[[t]] est de la forme $(t^m a, 0)$ ou $(0, t^m a)$ avec $m \in \mathbb{N}$ pour tout a tel que (a, 0) désigne schémas en groupes distincts d'ordre p sur k.*

Preuve. Supposons que $car(k) = p$. Toute factorisation de p nule est de la forme (0, 0), (0, a) ou (a, 0) pour tout $a \in k[[t]]$ différent de zéro. Pour a fixé les couples (0, 0), (0, a) et (a, 0) ne sont pas équivalents, donc notre problème est de comprendre si (a,

0) et (b, 0) peuvent être équivalent pour un élément $b \neq 0 \in k[[t]]$ (on peut énoncer de façon analogue le problème dual avec (0, a) et (0, b)). On veut donc étudier si l'équation $ax^{p-1} = b$ a une solution ou non dans l'ensemble des unités de k[[t]]. La structure dvr de k[[t]] implique que $a = t^n * u$ et $b = t^m * v$ pour m et n uniques où u, v sont des unités ; cela signifie que si $m \neq n$ il n'y a aucune chance que notre équation ait une solution et donc a et b représentent deux schémas en groupe différents. Supposons $n = m$; dans ce cas, nous devons vérifier si $x^{p-1} = u/v$ a une solution qui peut être vérifiée sur k grâce au lemme de Hensel. ■

BIBLIOGRAPHIE

[1] Anna CADORET, *ALGEBRE ET THÉORIE DE GALOIS*, SORBONNE UNIVERSITÉ(2019),`https://webusers.imj-prg.fr/~anna.cadoret`.

[2] C. Ding, D. Pei et A. Salomaa, *Chinese Remainder Theorem*, World Scientific

[3] Derek J. S. Robinson, *A Course in the Theory of Groups*, 2 nd ed Springer-Verlag New York, 1996

[4] Hideyuki Matsumura, *Commutative algebra*, W. A. Benjamin, Inc., 1970

[5] James S. Milne, *Basic theory of affine group schemes*, 2012.

[6] John. Tate and Frans. Oort, *Group schemes of prime order*, Annales scientifiques de l'E. N. S. , 1970.

[7] Mac. Lane(Saunders), *Categorical algebra*, ENS Ker Lann

[8] Marie-Paule. Brameret, Michel. Enguehard and Guy Renault, *Étude élémentaire des catégories*

[9] René. Schoof, *Introduction to finite group schemes*, 2000.

[10] Richard. Pink, *Finite group schemes*, 2004.

[11] Théo PIERRON, *Theorie des groupes*, ENS Ker Lann.