Rapport de séminaire : Schémas en groupes plats finis

ptchamitchian

Décembre 2020

1 Introduction

Le but de cette synthèse est de présenter la notion de schémas en groupes, introduite dans les années 60 par Alexandre Grothendieck, et qui généralise la notion de groupes. Les schémas en groupes plats finis y sont les analogues des groupes finis. Ils disposent d'un ordre qui généralise la notion d'ordre d'un groupe, et l'affirmation "$x^n = 1$" dans un groupe fini d'ordre n admet un analogue dans les groupes plats finis commutatifs, qui a été précisé par Pierre Deligne. Quelques exemples simples illustreront le rapport ; on développera un peu en dernière partie l'étude des schémas en groupes d'ordre 2, surtout pour s'apercevoir de la diversité de leurs types.

2 Schémas en groupes : définitions et exemples

2.1 Premières définitions

Pour définir les schémas en groupes, nous allons donner la définition d'objet en groupes dans une catégorie, puis il suffira de se placer dans la catégorie des S-schémas avec S un schéma de base fixé.

Soit donc G un objet dans une catégorie $\mathcal{C}$. On admet (ce qui sera utile pour la suite) que cette catégorie admet un objet terminal S, c'est-à-dire un objet tel que pour tout $G \in \mathcal{C}$, il existe un unique morphisme de G vers S. Donner une multiplication sur G, c'est-à-dire une application $m : G \times G \longrightarrow G$, induit une multiplication sur l'ensemble

$$G(T) := \mathrm{Hom}_{\mathcal{C}}\,(T, G)\ ,$$

pour tout $T \in \mathcal{C}$.

Explicitement, comme $G(T) \times G(T) = (G \times G)(T)$, si $g_1, g_2 \in G(T)$ on a l'égalité $g_1 g_2 = m \circ (g_1, g_2)$, où (g_1, g_2) est l'unique application de $(G \times G)(T)$ telle que pour $i = 1, 2$ on a $pr_i \circ (g_1, g_2) = g_i$ (les pr_i désignant les projections de $G \times G \to G$). Il est donc notamment essentiel que dans notre catégorie la notion de produit fini d'objets soit bien définie. Si on a pour $\mathcal{C}$ la catégorie des

ensembles, cela revient à dire que pour toutes fonctions g_1, g_2 de T dans G, pour tout x dans T, on a $(g_1 g_2)(x) = m(g_1(x), g_2(x))$; si G est un groupe il est facile de voir que $G(T)$ est alors aussi un groupe. On remarque de plus que si l'on dispose d'une application $f : T \to T'$, alors on dispose d'une application induite $f^* : G(T') \to G(T)$ définie par $f^*(g) = g \circ f$ pour tout $g \in G(T')$, et cette application commute avec la multiplication : $f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$ pour tout $g_1, g_2 \in G(T')$. Ainsi, $T \to G(T)$ est un foncteur contravariant de $\mathcal{C}$ dans la catégorie des magmas (c'est-à-dire des ensembles munis d'une opération).

Définition 2.1.1. On dit que G est **un objet en groupes** s'il vient accompagné d'une multiplication $m : G \times G \to G$ qui induit, pour tout $T \in \mathcal{C}$, une structure de groupe sur $G(T)$.

Pour vérifier que $G(T)$ est un groupe pour tout $T \in \mathcal{C}$, on n'aura besoin que de vérifier les trois points suivants.

L'associativité : Le magma $G(T)$ est associatif pour tout $T \in \mathcal{C}$ si et seulement si le diagramme suivant commute :

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mathrm{id} \times m} & G \times G \\ \downarrow{\scriptstyle m \times \mathrm{id}} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array} ,$$

autrement dit quand on a l'égalité $(pr_1 pr_2) pr_3 = pr_1 (pr_2 pr_3)$ dans $G(G \times G \times G)$.

Existence des unités : Les magmas $G(T)$ admettent des unités ε_T préservées par les applications f^* si et seulement si $G(S)$ admet un élément ε tel que l'identité $\pi^*(\varepsilon).\mathrm{id} = \mathrm{id} = \mathrm{id}.\pi^*(\varepsilon)$ est vérifiée dans $G(G)$, où π désigne l'unique morphisme de G vers S. Ceci équivaut à demander que les triangles du diagramme suivant commutent :

$$\begin{array}{ccccc} S \times G = G = G \times S & & \xrightarrow{\mathrm{id} \times \varepsilon} & & G \times G \\ \downarrow{\scriptstyle \varepsilon \times \mathrm{id}} & \searrow & & & \downarrow{\scriptstyle m} \\ G \times G & & \xrightarrow{m} & & G \end{array} .$$

On aura alors $\varepsilon_T = \pi_T^*(\varepsilon)$ pour tout $T \in \mathcal{C}$.

Existence des inverses : L'inversion existe dans chaque $G(T)$ si et seulement si $\mathrm{id} := \mathrm{id}_G$ admet un inverse, noté inv, dans $G(G)$, ce qui revient à demander que le diagramme

$$\begin{array}{ccc} G \times G & \xrightarrow{\mathrm{id} \times \mathrm{inv}} & G \times G \\ {\scriptstyle \Delta}\uparrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\varepsilon \circ \pi} & G \end{array}$$

commute. Ici Δ désigne l'application diagonale, c'est-à dire l'unique application telle que pour $i = 1, 2$ on a l'égalité $pr_i \circ \Delta = \mathrm{id}$. Si g est dans $G(T)$, son inverse est alors $\mathrm{inv} \circ g$.

On dira de plus que G est un objet en groupes commutatifs lorsque tous les $G(T)$ sont commutatifs. Il suffit pour cela que l'on ait $pr_1 pr_2 = pr_2 pr_1$ dans $G(G \times G)$.

Un **morphisme d'objet en groupes** de G dans G' est un morphisme φ de G dans G' tel que les morphismes φ^* induits de $G(T)$ dans $G'(T)$ sont tous des morphismes de groupes. C'est la même chose que de demander que le diagramme suivant commute :

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & G' \times G' \\ \downarrow m & & \downarrow m' \\ G & \xrightarrow{\varphi} & G' \end{array} .$$

En pratique, on n'a pas forcément besoin de définir la multiplication m sur G pour définir un objet en groupes ; en effet il peut être plus facile de donner le foncteur $G(T)$ et de mettre une structure de groupe sur $G(T)$ telle que toutes les applications $f^* : G(T') \to G(T)$ induites par les $f : T \to T'$ soient des morphismes de groupes. Si l'on peut faire cela, il existera alors une unique application $m : G \times G \to G$ qui induit les structures de groupes données sur les $G(T)$: on peut vérifier que $m = pr_1 pr_2$, le membre de droite étant bien défini grâce à la strucure de groupe de $G(G \times G)$. C'est ce que nous allons utiliser pour donner nos premiers exemples. Tout d'abord, montrons ce que ces définitions donnent lorsque on utilise des S-schémas.

Définition 2.1.2. Un **S-schéma en groupes**, ou simplement **schéma en groupes**, est un objet en groupes dans la catégorie des S-schémas.

On considère la catégorie des S-schémas plutôt que celle des schémas, car on a besoin d'un objet terminal (qui sera justement S) et d'un produit dans la catégorie que l'on considère. On se place dans le cas où $S = \mathrm{Spec}(R)$ est un schéma affine. On rappelle maintenant le théorème fondamental suivant :

Théorème 2.1.3. *: Soient $X = \mathrm{Spec}\, A$, $Y = \mathrm{Spec}\, B$ deux schémas affines. L'application*

$$\mathrm{Hom}_{Sch}(X, Y) \longrightarrow \mathrm{Hom}_{Ann}(B, A)$$
$$(f, \theta) \longmapsto \theta_X : B \to A$$

est une bijection.

Ainsi, lorsqu'on veut donner un morphisme de schémas affines, il suffit en fait de donner un morphisme d'anneaux, et lorsqu'on veut donner un morphisme de S-schémas, un morphisme de R-algèbres. De plus, si $G = \mathrm{Spec}\, A$ est un S-schéma, alors $G \times G = \mathrm{Spec}(A \otimes_R A)$. De ces remarques on déduit que donner une structure de schéma en groupes à G revient à donner des morphismes de R-algèbres

$$\widetilde{m} : A \to A \otimes_R A, \qquad \widetilde{\varepsilon} : A \to R, \qquad \widetilde{\mathrm{inv}} : A \to A,$$

qui correspondent aux morphismes m, ε et inv que l'on a vus plus haut, et qui font commuter les diagrammes suivants :

$$\begin{array}{ccc} A\otimes A\otimes A & \xleftarrow{\mathrm{id}\times\widetilde{m}} & A\otimes A \\ \uparrow{\scriptstyle \widetilde{m}\times\mathrm{id}} & & \uparrow{\scriptstyle \widetilde{m}} \\ A\otimes A & \xleftarrow{\widetilde{m}} & A \end{array} \quad , \quad \begin{array}{ccccc} R\otimes A = A = A\otimes R & & \xleftarrow[\mathrm{id}\times\widetilde{\varepsilon}]{} & & A\otimes A \\ \uparrow{\scriptstyle \widetilde{\varepsilon}\times\mathrm{id}} & \nwarrow & & & \uparrow{\scriptstyle \widetilde{m}} \\ A\otimes A & & \xleftarrow[\widetilde{m}]{} & & A \end{array}$$

$$\text{et} \quad \begin{array}{ccc} A\otimes A & \xleftarrow{\mathrm{id}\times\widetilde{\mathrm{inv}}} & A\otimes A \\ \widetilde{\Delta}\downarrow & & \uparrow{\scriptstyle \widetilde{m}} \\ A & \xleftarrow{\widetilde{\varepsilon}\circ\widetilde{\pi}} & A \end{array} \quad .$$

On appelle $\widetilde{m}$ la comultiplication, $\widetilde{\varepsilon}$ la counité et $\widetilde{\mathrm{inv}}$ l'antipode.

La définition de la diagonale donne notamment que $\widetilde{\Delta}$ est l'application induite sur $A\otimes_R A$ par la multiplication sur A. La commutativité de G est équivalente à la cocommutativité de A, c'est-à-dire à la commutativité du diagramme suivant :

$$\begin{array}{ccccc} A\otimes_R A & & \xleftarrow[\varphi]{} & & A\otimes_R A \\ & \nwarrow_{\widetilde{m}} & & \nearrow_{\widetilde{m}} & \\ & & A & & \end{array} \quad ,$$

où $\varphi(x\otimes y) = y\otimes x$.

2.2 Exemples

On rappelle que pour définir un schéma en groupes G il peut être commode de donner à tous les $G(T)$ une structure de groupe de manière fonctorielle. De plus, si on a au départ $G = \mathrm{Spec}\, A$ on peut ne considérer que les morphismes de T dans G avec T également affine. Ceci nous permet de définir les deux schémas en groupes suivants.

Le groupe additif G_a

On pose $G_a = \mathrm{Spec}\, R[X]$, et pour tout $T = \mathrm{Spec}\, B$ avec B une algèbre commutative on a $G_a(T) = \mathrm{Hom}_{R-alg}(R[X], B) = B$, via l'identification $f \mapsto f(X)$. On a donc une structure de groupe sur $G_a(T)$. Pour retrouver la comultiplication sur G_a, l'antipode et la counité, il suffit de se servir des projections de G_a dans $G_a \times_S G_a$, soit explicitement

$$\widetilde{pr_1}(u) = u\otimes 1, \qquad \widetilde{pr_2}(u) = 1\otimes u\ ,$$

d'où

$$\widetilde{m}(u) = u\otimes 1 + 1\otimes u, \quad \widetilde{\varepsilon}(u) = 0, \quad \widetilde{\mathrm{inv}}(u) = -u\ .$$

Le groupe multiplicatif G_m

Cette fois-ci on pose $G_m = \operatorname{Spec} R[u, u^{-1}]$, et de même que précédemment on a $G_m(B) = B^*$, via l'identification $f \in \operatorname{Hom}_{R-alg}(R[u, u^{-1}], B) \mapsto f(u)$. Ici on a donc

$$\widetilde{m}(u) = u \otimes u, \quad \widetilde{\varepsilon}(u) = 1, \quad \widetilde{\text{inv}}(u) = u^{-1} .$$

Un schéma en groupes diagonalisables est la donnée, pour X un groupe abélien ordinaire, de $D(X) := \operatorname{Spec} R[X]$, où $R[X]$ désigne l'algèbre engendrée par X. Ainsi, si $T = \operatorname{Spec} B$, on a

$$[D(X)](T) = \operatorname{Hom}_{R-Alg}(R[X], B) = \operatorname{Hom}_{Ab}(X, B^*) ,$$

car la donnée d'un morphisme partant de $R[X]$ se rapporte à la donnée des images des éléments de X, et la structure d'algèbre de $R[X]$ induit la structure de groupe de X. Quand X est abélien fini d'ordre n, ce shéma en groupes est dit plat fini et son ordre est n - nous allons préciser tout ceci. On a notamment, pour tout $x \in X$,

$$\widetilde{m}(x) = x \otimes x, \quad \widetilde{\varepsilon}(x) = 1, \quad \widetilde{\text{inv}}(u) = x^{-1} ,$$

de façon analogue à ce qui se passe dans le groupe multiplicatif.

On mentionne enfin le comportement des schémas en groupes lors d'un changement de base :

Proposition 2.2.1. *Soit G un S-schéma en groupes et T un S-schéma. On note $G_T := G \times_S T$ et si V est un T-schéma, alors il est aussi un S-schéma et on a*

$$G_S(V) = G_T(V),$$

et donc G_T est également un schéma en groupes.

On utilise cette propriété dans la section suivante afin de se ramener, dans les démonstrations, au cas où les schémas considérés sont tous affines.

3 Ordre d'un groupe et théorème principal

Le théorème qui fait le résultat essentiel de ce rapport nécessite d'introduire la définition d'ordre d'un schéma en groupes, que nous donnons maintenant.

Définition 3.0.1. 1. Soit S un schéma de base localement noethérien. Un S-schéma X est dit **plat fini** s'il est localement libre, c'est-à-dire que l'on peut écrire $S = \bigcup S_i$ avec $S_i = \operatorname{Spec}(R_i)$ tel que X_{S_i} est de la forme $\operatorname{Spec}(A_i)$ pour tout i, et que les morphismes structuraux $\operatorname{Spec}(A_i) \to \operatorname{Spec}(R_i)$ munissent chaque A_i d'une structure de R_i-module libre de type fini.

2. Le rang des A_i, localement constant sur S que l'on va supposer connexe, est une constante r appelée **ordre** du schéma X.

Remarquons, en reprenant les mêmes notations, que si G est un schéma en groupes, alors $G_{\operatorname{Spec} R_i} = \operatorname{Spec} A_i$ est aussi un schéma en groupes. Comme annoncé à la fin de la section précédente, cela nous permet de nous ramener quasiment toujours au cas où nos schémas d'ordre fini sont affines.

Supposons maintenant que l'on dispose d'un S-schéma en groupes G plat fini. On suppose également que $G = \operatorname{Spec} A$ et $S = \operatorname{Spec} R$. Comme $G(G)$ est muni d'une structure de groupe, on peut considérer pour tout $n \in \mathbb{Z}$ la mise à la puissance n dans G, c'est-à-dire la fonction

$$n_G := (\mathrm{id}_G)^n.$$

On peut remarquer que si $g \in G(T)$ pour un certain S-schéma T, alors $g^*(n_G) = g^n$: on aurait pu définir n_G en disant que c'est la fonction de G dans G correspondant à la mise à la puissance n dans tous les $G(T)$, et utiliser le lemme de Yoneda. Les propriétés suivantes sont immédiates :

$$n_G.m_G = (n+m)_G \ \text{ et } \ n_G \circ m_G = (n.m)_G \ , \text{ pour tous } n, m \in \mathbb{Z} \ .$$

Les morphismes sur G correspondent à des morphismes de R-algèbres sur A. On note $\widetilde{n_G}$ le morphisme correspondant à n_G. On a alors

$$t_A \circ (\widetilde{n_G} \otimes \widetilde{m_G}) \circ \widetilde{m} = \widetilde{(n+m)_G} \text{ et } \widetilde{n_G} \circ \widetilde{m_G} = \widetilde{(m.n)_G} \ .$$

On utilise notamment l'identité $n_G.m_G = m \circ (n_g, m_G) \circ \Delta$ où (n_g, m_G) désigne l'unique fonciton de $G \times G$ dans G telle que $pr_1 \circ (n_g, m_G) = n_G$ et $pr_2 \circ (n_g, m_G) = m_G$, et Δ désigne la diagonale de G dans $G \times G$. On notera également que $\widetilde{0}_G = i \circ \varepsilon$ (l'analogue de la fonction constante sur les groupes).

Nous pouvons maintenant énoncer le théorème principal de ce rapport.

Théorème 3.0.2. *(P.Deligne) Soit G un schéma en groupes commutatif plat fini d'ordre n. Alors la mise à la puissance n "tue" tous les éléments du groupe, c'est-à-dire $\widetilde{n}_G = \widetilde{0}_G$.*

Pour prouver ce théorème, penchons nous tout d'abord sur la notion de schéma en groupes dual.

3.1 Dualité de Cartier

Supposons que $G = \operatorname{Spec} A$ est un schéma en groupes sur $S = \operatorname{Spec} R$. On dispose des applications suivantes :

$$s_A : A \otimes_R A \to A \ \text{ et } \ \widetilde{m_A} : A \to A \otimes_R A,$$

la multiplication et la comultiplication dans A qui correspondent respectivement à Δ et m la diagonale et la structure de groupe de G. Si on suppose maintenant

que G est plat fini, et donc que A est un module libre de type fini sur R, alors on peut considérer le dual de A en tant que R module :

$$A' := \mathrm{Hom}_{R-Mod}(A, R).$$

Comme A est libre de type fini, il en est de même pour A', et notamment on a $A' \otimes A' \simeq (A \otimes A)'$. Ceci permet de considérer les transposées des applications définies plus haut, et on a

$$s_{A'} := (m_A)' : A' \otimes_R A' \to A' \text{ et } \widetilde{m'_A} := (s_A)' : A' \to A' \otimes_R A',$$

qui font de A' une algèbre de Hopf au même titre que A. De plus, si A est commutative alors A' est cocommutative, et si A est cocommutative alors A' est commutative ; ainsi, A' est commutative si et seulement si G est un schéma en groupes commutatifs. Le schéma en groupes $\mathrm{Spec}\, A'$ défini par l'algèbre de Hopf A' est appelé dual de Cartier de G, et est noté G'.

Remarquons que l'on a l'injection suivante :

$$G(S) = \mathrm{Hom}_{R-Alg}(A, R) \hookrightarrow \mathrm{Hom}_{R-Mod}(A, R) = A' ,$$

qui nous sera utile par la suite.

Mentionnons au passage le théorème suivant - que nous n'utiliserons pas, mais qui explique l'interêt du dual de Cartier :

Théorème 3.1.1. *Le dual de Cartier G' représente le foncteur* $\mathrm{Hom}(G, G_m)$ *qui à T un S-schéma associe* $\mathrm{Hom}_{Gr-sch/T}(G_T, G_{m,T})$ *l'ensemble des morphismes de schéma en groupes sur T de G_T dans $G_{m,T}$.*

3.2 Démonstration du théorème 3.0.2

Pour démontrer ce théorème, on utilise la notion de trace : soit G un S-schéma en groupes plat fini d'ordre n, avec toujours la convention $G = \mathrm{Spec}\, A$ et $S = \mathrm{Spec}\, R$. Considérons également $T = \mathrm{Spec}\, B$ un S-schéma d'ordre r de morphisme structural $f : T \to S$. On dispose alors de l'application suivante :

$$G(T) \hookrightarrow Hom_{R-mod}(A, B) = B \otimes A' \xrightarrow{N} A' ,$$

où N désigne la norme : si $g \in B \otimes A'$, on peut considérer R_x la multiplication par x de $B \otimes A'$ dans $B \otimes A'$. Cette application est un morphisme de R-modules, et comme A' est commutatif on peut en considérer le déterminant ; par définition, il s'agit de $N(x)$. Soit donc $a \in A$, et fixons $(e_1, \cdots, e_r)$ une base de B sur R. On remarque alors qu'une base de $B \otimes A'$ sur A' est $(e_1 \otimes 1_R, \cdots, e_r \otimes 1_R)$ (par 1_R on désigne la fonction constante de A dans R de valeur 1_R, d'où l'abus de notation). Si on écrit $g = \sum g_i.(e_i \otimes 1_R)$ avec $g_i \in A'$ on obtient

$$N(R_g) = \det_{(e_i \otimes 1_R)}(\sum g_i.(e_1.e_i) \otimes 1_R, \cdots, \sum g_i.(e_r.e_i) \otimes 1_R) .$$

Si on évalue en l'élément a on trouve alors

$$N(R_g)(a) = \det_{(e_i)}(\sum g_i(a).(e_1.e_i), \cdots, \sum g_i(a).(e_r.e_i)) \ ,$$

qui est la norme de l'élément $g(a) \in B$, soit

$$N(R_g)(a) = N(R_{g(a)}).$$

Le premier terme est une norme sur $B \otimes A'$ évaluée en a, le deuxième est une norme sur B comme R- algèbre, évaluée en $g(a)$. A partir de là, on peut montrer que $N(R_g)$ est un morphisme d'algèbres : si $a, b \in A$ alors

$$N(g)(ab)) = N(g(ab)) = N(g(a)g(b)) = N(g(a))N(g(b)) = N(g)(a)N(g)(b)$$

et

$$N(g)(1_A) = N(g)(1_A) = 1_B \ ,$$

car la norme est multiplicative, envoie 1 sur 1, et g est un morphisme d'algèbres.

Ainsi, il existe une fonction nommée trace de f, notée Tr_f, qui envoie $g \in \mathrm{Hom}_{R-alg}(A, B)$ sur $N(g) \in \mathrm{Hom}_{R-alg}(A, R)$. Si $u \in G(S)$, on a alors $\mathrm{Tr}_f(f^*u) = u^r$ (l'application R_{f^*u} est une homothétie de rapport u). Enfin, la norme est un invariant d'automorphismes d'algèbres. Donc si $\tau : T \to T$ est un automorphisme de S-schémas, alors pour tout $g \in G(T)$ on a $\mathrm{Tr}_f(g \circ \tau) = \mathrm{Tr}_f(g)$.

Maintenant que la trace est introduite, nous pouvons passer à la démonstration proprement dite du théorème.

Démonstration. Soit $G = \mathrm{Spec}\, A$ un S-schéma en groupes d'ordre n. Pour prouver que $\widetilde{n_G} = \widetilde{0_G}$ il suffit de prouver que tout élément de $G(T)$ est d'ordre divisant n, pour tout S-schéma T. De plus, comme

$$G(T) \simeq \mathrm{Hom}_{T-Sch}(T, T \times_T G) \ ,$$

il est suffisant de prouver que les éléments de $G(S)$ sont d'ordre divisant n. Soit donc $u \in G(S)$, et notons f le morphisme de structure de $G = \mathrm{Spec}\, A$ sur S. Considérons la translation t_u par u :

$$t_u = m \circ (\mathrm{id}, u) : G = G \times_S S \overset{(\mathrm{id}_G, u)}{\longrightarrow} G \times G \overset{m}{\longrightarrow} G.$$

Il est clair que t_u est un autormophisme d'inverse $t_{u^{-1}}$; ainsi des remarques faites plus haut on déduit

$$\mathrm{Tr}_f(\mathrm{id}_G) = \mathrm{Tr}_f(\mathrm{id} \circ t_u) \ .$$

Par définition de t_u, on a $\mathrm{id}_G \circ t_u = \mathrm{id}_G \,.f^*u$ (le deuxième terme est un produit dans $G(G)$) et donc

$$\mathrm{Tr}_f(\mathrm{id}_G) = \mathrm{Tr}_f(\mathrm{id} \circ t_u) = \mathrm{Tr}_f(\mathrm{id}_G).\,\mathrm{Tr}_f(f^*u) = \mathrm{Tr}_f(\mathrm{id}_G).u^n \ ,$$

d'où $u^n = \varepsilon$, ce qui prouve le théorème. □

.

Comme discuté lorsqu'on a donné la définition de l'ordre, la démonstration dans le cas affine donne la démonstration pour tout schéma plat fini. On remarquera que dans l'exemple de $D(X)$, où X est un groupe abélien d'ordre n, la mise à la puissance m dans $D(X)$ correspond à un morphisme de $R[X]$ dans lui même, qui notamment envoie tout élement $x \in X$ sur x^m. Ainsi ce théorème généralise bien le théorème déjà connu sur les groupes (abéliens).

4 Schéma en groupes d'ordre 2

Dans cette dernière section, nous montrons une illustration du théorème dans le cas d'un ordre égal à 2.

Supposons que $G = \operatorname{Spec} A$ est un S-schéma d'ordre 2, avec $S = \operatorname{Spec} R$. Cela signifie que A est une R-algèbre libre de rang 2. Pour l'instant, on suppose seulement que G admet une multiplication associative et une unité, donc que l'on a une comultiplication $\widetilde{m}$ et une counité sur A

$$\widetilde{\varepsilon} : A \to R \, ,$$

dont on peux considérer le noyau I, appelé **idéal d'augmentation**. On se restreint au cas où I est lui même un module libre de rang 1 sur R. Appelons x un générateur de I sur R. On a alors $A = R \oplus Rx$ (si $y \in A$ on a $y = \varepsilon(y).1_A + (y - \varepsilon(y).1_A)$, et donc la multiplication sur A est entièrement déterminée par $a \in R$ tel que $x^2 = ax$. De plus, $A \otimes A = R \oplus R(x \otimes 1) \oplus R(1 \otimes x) \oplus R(x \otimes x)$.

Remarquons que

$$\widetilde{m}(x) - x \otimes 1 - 1 \otimes x \in R(x \otimes x) \, ,$$

car

$$(\widetilde{\varepsilon} \times \mathrm{id})(\widetilde{m}(x) - x \otimes 1 - 1 \otimes x) = \otimes x - 0 \otimes 1 - 1 \otimes x = 0 \, ,$$

et de même que

$$(\mathrm{id} \times \widetilde{\varepsilon})(\widetilde{m}(x) - x \otimes 1 - 1 \otimes x) = 0 \, ,$$

et les noyaux de $(\mathrm{id} \times \widetilde{\varepsilon})$ et de $(\widetilde{\varepsilon} \times \mathrm{id})$ s'intersectent en $I \otimes I$.
Ainsi, $\widetilde{m}(x) = x \otimes 1 - 1 \otimes x + b(x \otimes x)$ pour un certain $b \in R$, et comme $\widetilde{m}(1) = 1$, la comultiplication sur A est entièrement déterminée par ce scalaire b.

Pour que $\widetilde{m}$ soit un morphisme d'algèbres, il faut notamment que

$$\widetilde{m}(x^2) = (\widetilde{m}(x))^2$$

ce qui devient

$$a(x \otimes 1 + 1 \otimes x + b(x \otimes x)) = (x \otimes 1 + 1 \otimes x + b(x \otimes x))^2$$

puis

$$a(x \otimes 1 + 1 \otimes x + b(x \otimes x)) = (ax \otimes 1 + 1 \otimes ax + a^2 b^2 (x \otimes x)) + (2 + 2ab + 2ab)(x \otimes x),$$

soit $(1+ab)(2+ab)=0$ dans R. Cette condition est en fait suffisante.

On pose maintenant $e_1 = ab+2$ et $e_2 + -ab-1$. Ces deux éléments de R sont idempotents, et de somme égale à 1. Ainsi on peut écrire $S = S_1 \bigsqcup S_2$ (en prenant les ouverts standards associés respectivement à e_2 et e_1), et on peut alors considérer G_{S_1} et G_{S_2}, c'est-à-dire se ramener au deux cas disjoints suivants : G est un S-schéma avec soit $ab+2=0$ dans R, soit $ab=-1$ dans R.

Si $T = \operatorname{Spec} B$, alors si $f \in G(T) = \operatorname{Hom}_{R-Alg}(A,B)$ on peut poser $y = f(x)$ et donc $y^2 = ay$. La loi de composition sur $G(B)$ est donc celle qui, à toute paire d'éléments de B (y,z) tels que $y^2 = ay$, $z^2 = ay$, associe

$$y * z = y + z + byz.$$

On a donc, si $y*y = (2+ab)y = 0)$ dans le premier cas et $y*y = (2+ab)y = y$ dans le deuxième. Ainsi, pour que G soit un schéma en groupes il faut se placer dans le cas $ab+2=0$. On remarque d'ailleurs que le théorème de P.Deligne est vérifié puisque $y*y=0$.

A tout couple (a,b) de R^2 vérifiant $ab=-2$ on peut donc associer le S-schéma en groupes $G_{a,b}$. La condition $G_{a,b} \simeq G_{\alpha,\beta}$ est équivalente à la condition "il existe u inversible dans R tel que $a = u\alpha$ et $b = u^{-1}\beta$", comme on peut le vérifier en considérant un isomorphisme de $G_{a,b}$ dans $G_{\alpha,\beta}$ et regarder l'image de x qui génère l'idéal d'augmentation associé à $G_{a,b}$ dans l'anneau correspondant à $G_{\alpha,\beta}$ (il suffit ensuite de regarder l'image de x^2 pour conclure facilement).

Ainsi, si 2 est inversible dans R tous les $G_{a,b}$ sont isomorphes, et si R est un anneau intègre de caractérique 2, alors les seuls $G_{a,b}$ sont de la forme $G_{a,0}$, $G_{0,a}$ ou $G_{0,0}$ avec a qui ne divise pas 0 dans R.

5 Conclusion

La dernière partie, sans aller très loin, montre néanmoins que contrairement au cas des groupes ordinaires, on peut trouver énormément de schémas en groupes d'ordre 2 - ne serait-ce que grâce à la multitude de schémas de base possibles. Par exemple, il est prouvé qu'il y a 18 schémas en groupes d'ordre 2 non isomorphes (cf. [1]) sur $\operatorname{Spec}(\mathbb{Z}_2[2^{1/17}])$. La classification des schémas en groupes d'ordre p pour p premier est réalisée dans [2]. Remarquons enfin que nous n'avons pas développé dans ce rapport certaines autres notions de base, comme celles de noyau et de conoyau de morphisme de schémas en groupes, ou de quotient.

Pour toutes les définitions de base, voir [1]. La démonstration du théorème de P.Deligne est rapportée dans [2].

Bibliographie

[1] John Tate ; Frans Oort. *Group schemes of prime order.* Ann. Sci. ÉcoleNorm. Sup. (4) 3, 1970.

[2] John Tate. *Finite flat group schemes.* dans "Modular forms and Fermat's last theorem", Spinger, 1997.