CLASSIFICATION DES SCHÉMAS EN GROUPES D'ORDRE p (D'APRÈS OORT ET TATE)

YICHAO TIAN

1. Schémas en Groupes d'Ordre Fini

Dans cette section, S désigne un schéma quelconque. On dit qu'un S-schéma T est *d'ordre fini* (resp. *d'ordre m* pour $m \in \mathbb{Z}_{\geq 1}$) si son algèbre $\mathcal{O}_T$ est localement libre de type fini (*resp.*de rang m) en tant que $\mathcal{O}_S$-module.

1.1. Soit $G = \mathrm{Spec}(A)$ un schéma en groupes d'ordre fini sur S. On note

$$s_A : A \to A \otimes_{\mathcal{O}_S} A \quad (resp. \quad t_A : A \otimes_{\mathcal{O}_S} A \to A),$$

les homomorphismes de $\mathcal{O}_S$-algèbres correspondant à la loi de composition $G \times_S G \to G$, (*resp.*au morphisme diagonal $G \to G \times_S G$). Posons $A^\vee = \mathcal{H}om_{\mathcal{O}_S}(A, \mathcal{O}_S)$. C'est un $\mathcal{O}_S$-module localement libre du même rang que celui de A, et on a un isomorphisme canonique

$$(A \otimes_{\mathcal{O}_S} A)^\vee \simeq A^\vee \otimes_{\mathcal{O}_S} A^\vee.$$

On note

$$t_{A^\vee} = (s_A)^\vee : A^\vee \otimes_{\mathcal{O}_S} A^\vee \to A^\vee$$

et

$$s_{A^\vee} = (t_A)^\vee : A^\vee \to A^\vee \otimes_{\mathcal{O}_S} A^\vee$$

les morphismes induits par s_A et t_A. Ceci fait de $A^\vee$ une $\mathcal{O}_S$-algèbre de Hopf associative, coassociative et cocommutative. Pour tout S-schéma T, on a une injection canonique d'ensembles

$$G(T) = \mathrm{Hom}_{\mathcal{O}_S-\mathrm{alg}}(A, \mathcal{O}_T) \longrightarrow \Gamma(S, A^\vee \otimes_{\mathcal{O}_S} \mathcal{O}_T), \tag{1.1.1}$$

dont l'image est le groupe multiplicatif formé par les éléments $g \in \Gamma(S, A^\vee \otimes_{\mathcal{O}_S} \mathcal{O}_T)$ tels que $s_{A_T^\vee}(g) = g \otimes g$, où $s_{A_T^\vee}$ est la comultiplication sur $A^\vee \otimes_{\mathcal{O}_S} \mathcal{O}_T$ induite par $s_{A^\vee}$.

On note que G est commutatif si et seulement si $A^\vee$ est une $\mathcal{O}_S$-algèbre commutative. Si c'est le cas, on pose $G^\vee = \mathrm{Spec}(A^\vee)$. Alors $G^\vee$ est muni de la structure de schéma en groupes induite par la comultiplication $s_{A^\vee}$ sur $A^\vee$, et on l'appelle *dual de Cartier de G*. D'après (1.1.1), le foncteur qui associe à tout S-schéma T le groupe $\mathrm{Hom}_{T-gr}(G \times_S T, \mathbb{G}_{m,T})$ est représentable par G. On en déduit donc un accouplement canonique

$$G \times_S G^\vee \to \mathbb{G}_{m,s} \tag{1.1.2}$$

qui est non-dégénéré et bimultiplicatif.

1.2. Soit $G = \mathrm{Spec}(A)$ un schéma en groupes affine et plat sur S. Pour tout $m \in \mathbb{Z}$, on note $m_G : G \to G$ l'homomorphisme de l'élévation à la m-ème puissance, *i. e.* pour tout S-schéma

T et tout $\xi \in G(T)$, on a $m_G(\xi) = \xi^m$. On note $[m] : A \to A$ l'homomorphisme de O_S-algèbres correspondant. Les relations $(\xi^m)^n = \xi^{mn}$ et $\xi^m \cdot \xi^n = \xi^{m+n}$ correspondent aux identités

$$[m] \circ [n] = [mn] \quad \text{et} \quad t_A \circ ([m] \otimes [n]) \circ s_A = [m+n].$$

On a $[1] = \mathrm{Id}_A$ et $[0] : A \xrightarrow{\epsilon} O_S \xrightarrow{i} A$, où ϵ correspond à la section unité de G et i est le morphisme structural de A. On appelle $I_G = \mathrm{Ker}([0]) = \mathrm{Ker}(\epsilon)$ *idéal d'augmentation* de G.

Théorème 1.3 (Deligne)**.** *Soit G un S-schéma en groupes commutatif d'ordre m. Alors G est annulé par m_G.*

Remarque 1.4. D'après [SGA 3 $\mathrm{VII_A}$ 8.5], si S est réduit, tout S-schéma en groupes d'ordre m est annulé par m_G.

Pour montrer le théorème 1.3, on a besoin d'introduire le morphisme trace d'après Deligne. Soient $T = \mathrm{Spec}(B)$ un S-schéma d'ordre n, $f : T \to S$ le morphisme structural. Il existe un unique morphisme Tr_f, appelé *morphisme trace*, qui rend commutatif le diagramme suivant

$$\begin{array}{ccc} G(T) & \hookrightarrow & \Gamma(S, A^\vee \otimes B) \\ {\scriptstyle \mathrm{Tr}_f}\downarrow & & \downarrow{\scriptstyle \mathrm{Nm}} \\ G(S) & \hookrightarrow & \Gamma(S, A^\vee), \end{array}$$

où les flèches horizontales sont définies dans (1.1.1) et Nm désigne l'application norme de $A^\vee$-algèbre $A^\vee \otimes B$. On vérifie facilement que le morphisme Tr_f satisfait aux propriétés suivantes :

(a) Tr_f est un homomorphisme de groupes ;

(b) pour tout $u \in G(S)$, on a $\mathrm{Tr}_f(f^*u) = u^n$, où $f^* = G(f) : G(S) \to G(T)$;

(c) pour tout $t \in \mathrm{Aut}_S(T)$ et $\beta \in G(T)$, on a $\mathrm{Tr}_f(T \xrightarrow{t} T \xrightarrow{\beta} G) = \mathrm{Tr}_f(T \xrightarrow{\beta} G)$.

Démonstration de 1.3. On doit montrer que pour tout S-schéma T et tout $x \in G(T)$, on a $x^m = 1$. Comme on a

$$G(T) = \mathrm{Hom}_{S-sch}(T, G) = \mathrm{Hom}_{T-sch}(T, G \times_S T),$$

quitte à faire un changement de base, on peut supposer $T = S$. Pour tout $x \in G(S)$, on note

$$t_x : G \simeq G \times_S S \xrightarrow{(x, \mathrm{Id}_G)} G \times G \xrightarrow{\mu} G$$

le morphisme de translation par x, où μ est la loi de composition de G. Notons $f : G \to S$ le morphisme structural de G, et $1_G : G \to G$ l'identité de G. Comme $1_G \circ t_x = 1_G \times f^*(x)$, où "$\circ$"signifie le composition et "$\times$" la multiplication dans $G(G)$, on en déduit que

$$\mathrm{Tr}_f(1_G \circ t_x) = \mathrm{Tr}_f(1_G \times f^*(x) = \mathrm{Tr}_f(1_G)\mathrm{Tr}_f(f^*(x)).$$

En utilisant les propriétés (a), (b) et (c) de Tr_f, on obtient $\mathrm{Tr}_f(1_G) = \mathrm{Tr}_f(1_G)x^m$, d'où $x^m = 1$. □

Théorème 1.5. *Soit p un nombre premier. Alors tout S-schéma en groupes d'ordre p est nécessairement commutatif et annulé par p.*

Rappelons d'abord le lemme suivant bien connu.

Lemme 1.6 ([TO] Lemma 1)**.** *Soient k un corps algébriquement clos, $G = \mathrm{Spec}(A)$ un k-groupe d'ordre p. Alors ou bien G est isomorphe au groupe constant $(\mathbb{Z}/p\mathbb{Z})_k$, ou bien k est de caractéristique $p > 0$, et $G \simeq \mu_{p,k}$ ou $G \simeq \alpha_{p,k}$. En particulier, G est commutatif et la k-algèbre A est monogène.*

Démonstration de 1.5. Soit $G = \mathrm{Spec}(A)$ un S-schéma en groupes d'ordre p. D'après le théorème 1.3, il suffit de prouver la commutativité de G, ou de manière équivalente la commutativité de $A^\vee$. Le problème étant local pour S, on peut supposer $S = \mathrm{Spec}(R)$ avec R un anneau local. Si $R \to R'$ est une injection d'anneaux, alors $A^\vee$ s'injecte dans $A^\vee \otimes_R R'$, et la commutativité de $A^\vee \otimes_R R'$ entrainera la commutativité de $A^\vee$. Quitte à élargir R, on peut donc supposer le corps résiduel k de R algébriquement clos. D'après le lemme 1.6, on a $G \otimes k \simeq \alpha_{p,k}, \mu_{p,k}$ ou $(\mathbb{Z}/p\mathbb{Z})_k$. En particulier, l'algèbre $A^\vee \otimes k$ est monogène. On choisit $x \in A^\vee$ tel que $k[\overline{x}] = A^\vee \otimes k$, où $\overline{x} \in A^\vee \otimes k$ est l'image de x. D'après le lemme de Nakayama, on a $A^\vee = R[x]$, ce qui montre que $A^\vee$ est commutative.

□

2. Théorème de Classification d'Oort-Tate

Soient p un nombre premier, $\chi : \mathbb{F}_p \to \mathbb{Z}_p$ le relèvement de Teichmüller, *i. e.* $\chi(0) = 0$ et pour tout $m \in \mathbb{F}_p^\times$, $\chi(m)$ est l'unique $(p-1)$-ème racine de l'unité dans $\mathbb{Z}_p$ telle que $\chi(m) \equiv m \mod p$. On pose

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

où l'intersection est prise dans $\mathbb{Q}_p$. Voici quelques exemples de Λ_p :

$$p = 2, \quad \Lambda_2 = \mathbb{Z};$$
$$p = 3, \quad \Lambda_3 = \mathbb{Z}[1/2];$$
$$p = 5, \quad \Lambda_5 = \mathbb{Z}[i, \frac{1}{2(2+i)}],$$

où $i = \chi(2)$ est l'unique élément de $\mathbb{Z}_5$ tel que $i^2 = -1$ et $i \equiv 2 \mod 5$. Dans la suite, on fixe un nombre premier p, et on note $\Lambda = \Lambda_p$. Sauf mention expresse du contraire, tout schéma considéré sera supposé sur $\mathrm{Spec}(\Lambda)$.

2.1. Soient S un Λ-schéma, $G = \mathrm{Spec}(A)$ un schéma en groupes d'ordre p sur S, $I \subset A$ l'idéal d'augmentation de G. Alors l'algèbre $\mathcal{O}_S[\mathbb{F}_p^\times]$ agit naturellement sur A et préserve I. Pour tout $i \in \mathbb{Z}$, on pose

$$e_i = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^{-i}(m)[m] \in \mathcal{O}_S[\mathbb{F}_p^\times]$$

et $I_i = e_i I$. On note que e_i et I_i ne dépendent que de la classe $i \mod (p-1)$.

Lemme 2.2. *Sous les hypothèses précédentes, on a une décomposition de $\mathcal{O}_S$-modules*

$$I = \bigoplus_{i=1}^{p-1} I_i. \tag{2.2.1}$$

Pour chaque $i \in \mathbb{Z}$, I_i est un faisceau inversible sur S, et pour tout ouvert U de S, on a

$$\Gamma(U, I_i) = \{f \in \Gamma(U, I); \quad [m](f) = \chi^i(m) f \text{ pour tout } m \in \mathbb{F}_p.\} \tag{2.2.2}$$

En plus, on a $I_iI_j \subset I_{i+j}$ pour tout $i, j \in \mathbb{Z}$, et $I_i = I_1^i$ pour $1 \leq i \leq p-1$.

Démonstration. On a des égalités dans $\mathcal{O}_S[\mathbb{F}_p^\times]$:

$$1 = e_1 + \cdots + e_{p-1};$$
$$e_ie_j = \begin{cases} 0 & \text{si } i \neq j, \\ e_i & \text{si } i = j; \end{cases}$$
$$[m]e_i = \chi^i(m)e_i.$$

On en déduit immédiatement l'existence de la décomposition (2.2.1) et la caractéristaion (2.2.2) de I_i. Le fait que $I_iI_j \subset I_{i+j}$ résulte de (2.2.2). Il reste à montrer que les I_i sont inversibles et que $I_i = I_1^i$ pour $1 \leq i \leq p-1$. Étant facteur direct de I, les I_i sont localement libres de rang fini sur S. Désignant par r_i le rang de I_i, on a donc $r_1 + \cdots + r_{p-1} = p-1$. Comme la décomposition (2.2.1) commute à tout changement de base, on se ramène à traiter le cas où S est le spectre d'un corps algébriquement clos k sur Λ. Il suffit de trouver une section f_1 de I_1 telle que $f_1^i \neq 0$ pour $1 \leq i \leq p-1$. D'après le lemme 1.6, il y a trois cas à distinguer :

(a) $G = (\mathbb{Z}/p\mathbb{Z})_k$. Dans cette situation, l'algèbre A de G consiste en les fonctions sur $\mathbb{F}_p$ à valeur dans k. L'action de $\mathbb{F}_p$ sur A est donnée par $([m] \cdot f)(n) = f(mn)$ pour tout $f \in A$ et $m, n \in \mathbb{F}_p$. On peut prendre alors $f_1 = \chi$.

(b) $G = \alpha_{p,k}$. Alors on a $A = k[t]/t^p$ avec $s_A(t) = t \otimes 1 + 1 \otimes t$ et $[m](t) = mt$. Comme k est de caractéristique p, on a $\chi(m) = m$ dans k, et donc on peut prendre $f_1 = t$.

(c) $G = \mu_{p,k}$. On a $A = k[t]/((1+t)^p - 1)$ avec $s_A(t) = 1 \otimes t + t \otimes 1 + t \otimes t$, et donc $[m](t) \equiv mt \mod t^2$. Posons $f_1 = e_1(t)$. Alors on a $f_1^i \equiv t^i \mod t^{i+1}$ pour tout $1 \leq i \leq p-1$; en particulier, $f_1^i \neq 0$ pour $1 \leq i \leq p-1$. □

De la description (2.2.2) de I_i, on déduit aisément le corollaire suivant.

Corollaire 2.3. *Soient $\varphi : G \to H$ un homomorphisme de S-schémas en groupes d'ordre p, I_G et I_H les idéaux d'augmentation de G et de H. Alors l'homomorphisme $\varphi^* : I_H \to I_G$ de $\mathcal{O}_S$-modules induit par φ envoie $I_{H,i}$ dans $I_{G,i}$ pour tout $1 \leq i \leq p-1$.*

Exemple 2.4. Soit $\mu_p = \mathrm{Spec}(B)$ le schéma en groupes multiplicatif d'ordre p sur Λ. On va expliciter la décompostion (2.2.1) pour μ_p. On a alors $B = \Lambda[z]/(z^p - 1)$ avec $s_B(z) = z \otimes z$ et $[m](z) = z^m$ pour tout $m \in \mathbb{F}_p$. L'idéal d'augmentation I_B de μ_p est $B(z-1)$, et il a $(z^m - 1)$ avec $m \in \mathbb{F}_p^\times$ pour sa base sur Λ :

$$I_B = \Lambda(z-1) + \cdots + \Lambda(z^{p-1} - 1).$$

Pour tout $i \in \mathbb{Z}$, posons

$$y_i = (p-1)e_i(1-z) = \sum_{m \in \mathbb{F}_p} \chi^{-i}(m)(1 - z^m) \tag{2.4.1}$$
$$= \begin{cases} p - \sum_{m \in \mathbb{F}_p} z^m & \text{si } i \equiv 0 \mod (p-1); \\ -\sum_{m \in \mathbb{F}_p} \chi^{-i}(m) z^m & \text{sinon.} \end{cases}$$

Comme

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

pour tout $m \in \mathbb{F}_p^\times$, On en déduit pour tout $i \in \mathbb{Z}$

$$\begin{aligned} s_B(y_i) - 1 \otimes y_i - y_i \otimes 1 & \\ &= \sum_{m \in \mathbb{F}_p^\times} \chi^{-i}(m)((1 \otimes 1 - z^m \otimes z^m) - 1 \otimes (1 - z^m) - (1 - z^m) \otimes 1) \\ &= - \sum_{m \in \mathbb{F}_p^\times} \chi^{-i}(m)[(1 - z^m) \otimes (1 - z^m)] \\ &= -\frac{1}{(p-1)^2} \sum_{m \in \mathbb{F}_p^\times} \chi^{-i}(m) \sum_{j=1}^{p-1} \sum_{k=1}^{p-1} \chi^j(m)\chi^k(m) y_j \otimes y_k \\ &= -\frac{1}{p-1} \sum_{j+k \equiv i \mod (p-1)} y_j \otimes y_k, \end{aligned}$$

et donc

$$s_B(y_i) = y_i \otimes 1 + 1 \otimes y_i + \frac{1}{1-p} \sum_{j=1}^{p-1} y_j \otimes y_{i-j}. \tag{2.4.2}$$

On a alors $I_i = \Lambda y_i$ pour tout $1 \leq i \leq p-1$, et $I_B = \Lambda y_1 + \cdots + \Lambda y_{p-1}$. Posons $y = y_1$. Comme $I_1^i \subset I_i$ pour tout $i \in \mathbb{Z}$, il existe des éléments $w_1 = 1, w_2, \cdots, w_i, \cdots \in \Lambda$ tels que $y_i = w_i y^i$.

Proposition 2.5. (i) *Les nombres w_i pour $1 \leq i \leq p-1$ sont inversibles dans Λ et on a $w_i \equiv i!$ mod p.*

(ii) *On a $w_p = p w_{p-1}$.*

(iii) *Posons $y = y_1$. Alors on a $B = \Lambda[y]/(y^p - w_p y)$ avec*

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

$$[m](y) = \chi(m) y \quad \textit{pour tout } m \in \mathbb{F}_p$$

et

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

On renvoie le lecture à [TO, p.9] pour une preuve complète de cette proposition. Indiquons ici comment démontrer (ii), ce qui fait le lien avec les sommes de Gauss. On fixe un plongement $\sigma : \Lambda \to \mathbb{C}$ dans le corps des nombres complexes. On l'étend en un homomorphisme $\varphi : B \to \mathbb{C}$ en posant $\varphi(z) = \zeta$, une p-ème racine primitive de l'unité. Notons $\eta_i = \varphi(y_i)$ pour tout $i \in \mathbb{Z}$. D'après (2.4.1), on a

$$\eta_i = \begin{cases} p & \text{si } i \equiv 0 \mod p-1 \\ -\sum_{m \in \mathbb{F}_p} \chi^{-i}(m) \zeta^m & \text{si } i \not\equiv 0 \mod p-1. \end{cases}$$

On remarque que η_i ne dépend que de la classe $i \mod (p-1)$, et que si $i \not\equiv 0 \mod (p-1)$, η_i est une somme de Gauss. Il résulte donc de la relation $y_1^i = w_i y_i$ que $w_i = \eta_1^i/\eta_i$. Donc on a $w_p = \eta_1^p/\eta_p = \eta_1^{p-1} = w_{p-1}\eta_{p-1} = pw_{p-1}$, ce qui montre (ii) de la proposition 2.5. En plus, d'après les propriétés des sommes de Gauss, on a $|\eta_i|_{\mathbb{C}} = p^{1/2}$ pour $i \not\equiv 0 \mod (p-1)$. On en déduit que

$$|\sigma(w_i)|_{\mathbb{C}} = \begin{cases} p^{\frac{i-1}{2}} & \text{si} \quad 1 \leq i \leq p-2; \\ p^{\frac{p-3}{2}} & \text{si} \quad i = p-1; \\ p^{\frac{p-1}{2}} & \text{si} \quad i = p. \end{cases}$$

On remarque aussi que les valeurs absolues archimédiennes des w_i ne dépendent pas du plongement $\sigma : \Lambda \to \mathbb{C}$ choisi.

2.6. Revenons à la situation générale. Soient S un schéma sur Λ, $G = \mathrm{Spec}(A)$ un schéma en groupes d'ordre p sur S, $I = \bigoplus_{i=1}^{p-1} I_i$ la décomposition (2.2.1) de l'idéal d'augmentation de G. Soient

$$\mathbf{S}[I_1] = \bigoplus_{i=0}^{\infty} I_1^{\otimes n}$$

l'algèbre symétrique engendrée par I_1 sur $\mathcal{O}_S$, $\psi : \mathbf{S}[I_1] \to A$ l'homomorphisme induit par l'inclusion $I_1 \subset A$. D'après le lemme 2.2, ψ est surjectif et son noyau est l'idéal engendré par $(a-1)\otimes I_1^{\otimes p}$, où

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

est l'élément correspondant à l'homomorphisme $I_1^{\otimes p} \to I_1$ induit par la multiplication dans A. Soient $G^\vee = \mathrm{Spec}(A^\vee)$ le dual de G, $I^\vee$ l'idéal d'augmentation, $I_i^\vee \subset I^\vee$ et $a' \in \Gamma(S, (I_1^\vee)^{\otimes(1-p)})$ les données analogues pour $G^\vee$. Comme G et $G^\vee$ sont annulés par p, l'accouplement canonique (1.1.2) se factorise par l'inclusion $\mu_{p,S} \to \mathbb{G}_{m,S}$, *i. e.* on a un accouplement canonique et non-dégénéré

$$\Phi : G \times G^\vee \to \mu_{p,S},$$

qui correspond à un homomorphisme de $\mathcal{O}_S$-algèbres

$$\varphi = \Phi^* : B_S = \mathcal{O}_S \otimes_\Lambda B \simeq \mathcal{O}_S[y]/(y^p - w_p y) \longrightarrow A \otimes A^\vee.$$

Lemme 2.7. *Sous les hypothèses précédentes, $\varphi(y)$ engendre $I_1 \otimes I_1^\vee$ partout. En plus, si on identifie $I_1^\vee$ à I_1^{-1} et $\varphi(y)$ à la section identité de $\mathcal{O}_S$, alors on a $a \otimes a' = w_p \,\mathrm{Id}_{\mathcal{O}_S}$.*

Démonstration. Comme l'accouplement Φ est bimultiplicatif, on a pour tout $m, n \in \mathbb{Z}$ un diagramme commutatif

$$\begin{array}{ccc} G \times G^\vee & \xrightarrow{(m_G, n_{G^\vee})} & G \times G^\vee \\ \Big\downarrow{\scriptstyle \Phi} & & \Big\downarrow{\scriptstyle \Phi} \\ \mu_{p,S} & \xrightarrow{(mn)_{\mu_{p,S}}} & \mu_{p,S}. \end{array}$$

Donc on a $([m] \otimes [n])\varphi(y) = \varphi([mn](y)) = \chi(m)\chi(n)\varphi(y)$ pour tout $m, n \in \mathbb{Z}$. D'après le lemme 2.2, on en déduit que $\varphi(y) \in \Gamma(S, I_1 \otimes I_1^\vee)$. Comme Φ est non-dégénéré et commute à tout changement de base, on a $\varphi(y) \otimes \kappa(s)$ pour tout point $s \in S$, *i. e.* $\varphi(y)$ engendre le faisceau inversible $I_1 \otimes I_1^\vee$

partout. Par conséquent, $\varphi(y)^{\otimes p}$ engendre $I_1^{\otimes p} \otimes (I_1^\vee)^{\otimes p}$ partout. Mais d'après la définition de a et a', on a

$$\varphi(y)^p = \varphi(y)^{\otimes p} a \otimes a' = \varphi(y^p) = w_p \varphi(y).$$

Donc si on identifie $I_1^\vee$ à I_1^{-1} et $\varphi(y)$ à la section identité de $\mathcal{O}_S$, on a $a \otimes a' = w_p \operatorname{Id}_{\mathcal{O}_S}$. □

2.8. Soient S un schéma sur $\Lambda = \Lambda_p$, $\mathbf{Gr}_S(p)$ la catégorie des schémas en groupes d'ordre p sur S. Notons encore $\mathbf{C}_S$ la catégorie dont les objets sont des triples (L, a, b), où L est un faisceau inversible sur S, $a \in \Gamma(S, L^{\otimes(p-1)})$ et $b \in \Gamma(S, L^{\otimes(1-p)})$ avec $a \otimes b = w_p \operatorname{Id}_{\mathcal{O}_S}$, et que les morphismes d'un objet (L_1, a_1, b_1) dans un autre (L_2, a_2, b_2) sont des morphismes $\varphi : L_1 \to L_2$ de $\mathcal{O}_S$-modules tels que $\varphi^{\otimes(p-1)}(a_1) = a_2$ et $(\varphi^\vee)^{\otimes(p-1)}(b_2) = b_1$, où $\varphi^\vee : L_2^{-1} \to L_1^{-1}$ est le morphisme induit par φ en appliquant le foncteur $\mathcal{H}om_{\mathcal{O}_S}(\_, \mathcal{O}_S)$.

Théorème 2.9 (Oort-Tate)**.** *Le foncteur qui associe à tout objet $G \in \mathbf{Gr}_S(p)$ le triple $(I_1^\vee, a, a')$ induit une équivalence de catégories entre $\mathbf{Gr}_S(p)$ et $\mathbf{C}_S$.*

Démonstration. On construit un quasi-inverse du foncteur $G \mapsto (I_1^\vee, a, a')$ comme suit. Soit (L, a, b) un objet dans $\mathbf{C}_S$. Posons

$$A = \mathbf{S}[L^{-1}]/((a-1) \otimes L^{\otimes(-p)}),$$

où $\mathbf{S}(L^{-1})$ est l'algèbre symétrique engendrée par L^{-1} sur $\mathcal{O}_S$, et de même

$$A^\vee = \mathbf{S}[L]/((b-1) \otimes L^{\otimes p}).$$

Alors $G = \operatorname{Spec}(A)$ et $G^\vee = \operatorname{Spec}(A^\vee)$ sont des schémas d'ordre p sur S. On va munir des structures de schémas en groupes sur G et $G^\vee$ comme suit. On définit un homomorphisme de $\mathcal{O}_S$-algèbres $\mathcal{O}_S[y] \to A \otimes A^\vee$ en posant $y \mapsto \operatorname{Id}_{\mathcal{O}_S} \in \Gamma(S, L^{-1} \otimes L)$. Comme $a \otimes a' = w_p \operatorname{Id}_{\mathcal{O}_S}$, le noyau de cet homomorphisme est engendré par $(y^p - w_p y)$, on obtient un morphisme de $\mathcal{O}_S$-algèbres

$$\varphi : B = \mathcal{O}_S[y]/(y^p - w_p y) \to A \otimes A^\vee.$$

Soit T un S-schéma.À tout point $f \in \operatorname{Hom}_{\mathcal{O}_S-alg}(A, \mathcal{O}_T)$ de G à valeur dans T, on associe l'homomorphisme composé

$$B \xrightarrow{\varphi} A \otimes A^\vee \xrightarrow{f \otimes id} \mathcal{O}_T \otimes A^\vee.$$

Ceci définit un morphisme d'ensembles

$$\Theta_T : G(T) \longrightarrow \mu_p(G \times_S T).$$

Il est facile de voir que Θ_T est toujours injectif. En plus, on prétend que $G(T)$ s'identifie à un sous-ensemble de $\mu_p(G \times_S T)$ stable par la loi de composition ; c'est-à-dire on peut munir $G(T)$ d'une unique structure de sous-groupe de $\mu_p(G^\vee \times_S T)$, et ceci fera G d'un schéma en groupes d'ordre p sur S et donnera donc un quasi-inverse du foncteur $G \mapsto (I_1^\vee, a, a')$. Pour conclure, il suffit donc de montrer qu'il exsite un unique morphisme coproduit $s_A : A \to A \otimes A^\vee$ tel que l'homomorphisme $\varphi_{A^\vee} : A^\vee[y]/(y^p - w_p y) \to A \otimes A^\vee$ induit par φ par linéraliser sur $A^\vee$ soit un morphisme d'algèbres de Hopf sur $A^\vee$. Grâce à l'injectivité de Θ_T, un tel s_A, s'il existe, est forcément unique. Il suffit alors de prouver son existence localement pour S.

Supposons L libre sur $\mathcal{O}_S$, $x \in \Gamma(S, L^{-1})$ qui induit un isomorphisme $\mathcal{O}_S \simeq L^{-1}$, et posons $x' = x^{-1} \in \Gamma(S, L)$. Donc on a

$$A = \mathcal{O}_S[x]/(x^p - ax) \quad \text{et} \quad A^\vee = \mathcal{O}_S[x']/(x'^p - a'x').$$

L'homomorphisme $\varphi : B = \mathcal{O}_S[y]/(y^p - w_p y) \to A \otimes A^\vee$ est donné par $\varphi(y) = x \otimes x'$. Soit $\varphi_{A^\vee} : B \otimes_{\mathcal{O}_S} A^\vee = A^\vee[y]/(y^p - w_p y) \to A \otimes A^\vee$ le linéralisé de φ sur $A^\vee$. Le morphisme $s_A : A \to A \otimes A$ à chercher doit satisfaire à l'équation

$$\varphi_{A^\vee}(s_{B_{A^\vee}}(y)) = s_{A_{A^\vee}}(\varphi(y)),$$

où $\varphi_{A^\vee}$, $s_{B_{A^\vee}}$ et $s_{A_{A^\vee}}$ sont respectivement les morphismes induits par φ, s_B et s_A par extension de scalaire à $A^\vee$. Le terme à droite est $s_{A_{A^\vee}}(x \otimes x') = s_A(x) \otimes x'$, et d'après la proposition 2.5(iii), on a

$$\begin{aligned}
\varphi_{A^\vee}(s_{B_{A^\vee}}(y)) &= \varphi_{A^\vee}(1 \otimes y + y \otimes 1 + \frac{1}{1-p}\sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}) \\
&= (1 \otimes x + x \otimes 1) \otimes x' + \frac{1}{1-p}\sum_{i=1}^{p-1} \frac{x^i \otimes x^{p-i}}{w_i w_{p-i}} \otimes x'^p \\
&= (1 \otimes x + x \otimes 1 + \frac{b}{1-p}\sum_{i=1}^{p-1} \frac{x^i \otimes x^{p-i}}{w_i w_{p-i}}) \otimes x'.
\end{aligned}$$

Dans la troisième égalité, on a utilisé la relation $x'^p = bx'$. On en déduit donc

$$s_A(x) = 1 \otimes x + x \otimes 1 + \frac{b}{1-p}\sum_{i=1}^{p-1} \frac{x^i \otimes x^{p-i}}{w_i w_{p-i}}. \tag{2.9.1}$$

Ceci montre l'existence de s_A, et termine donc la démonstration. □

Remarque 2.10. (i) Dans la suite, on notera $G^L_{a,b}$ le S-schéma en groupes d'ordre p construit dans la démonstration de 2.9 à partir d'un objet (L, a, b) de $\mathbf{C}_S$. Lorsque L^{-1} est libre sur $\mathcal{O}_S$ et trivialisé par une section $x \in \Gamma(S, L^{-1})$, on a

$$G^L_{a,b} = \mathrm{Spec}(\mathcal{O}_S[x]/(x^p - ax))$$

avec le morphisme coproduit s_A donné par (2.9.1), et l'action de $\mathbb{F}_p$ donnée par $[m](x) = \chi(m)x$ pour tout $m \in \mathbb{F}_p$.

(ii) Pour tout objet (L, a, b), le dual de Cartier de $G^L_{a,b}$ est $G^{L^{-1}}_{b,a}$. Si L^{-1} admet une trivialisation $x \in \Gamma(S, L^{-1})$ de sorte que $G^L_{a,b} = \mathrm{Spec}(\mathcal{O}_S[x]/(x^p - ax))$, alors on a $G^{L^{-1}}_{b,a} = \mathrm{Spec}(\mathcal{O}_S[x']/(x'^p - bx'))$ avec $x' = x^{-1} \in \Gamma(S, L)$ et l'accouplement canonique de Cartier

$$\Phi : G^L_{a,b} \times_S G^{L^{-1}}_{b,a} \to \mu_p = \mathrm{Spec}(\mathcal{O}_S[z]/(z^p - 1))$$

est donné par

$$\Phi^*(z) = 1 + \frac{1}{1-p}\sum_{i=1}^{p-1} \frac{(x \otimes x')^i}{w_i}.$$

(iii) Supposons S de caractéristique p. Alors les nombres universels $w_i = i!$ pour $1 \le i \le p-1$ (2.5). Soit (L, a, b) un objet de $\mathbf{C}_S$. On a alors $a \otimes b = 0$. Notons $(G^L_{a,b})^{(p)}$ l'image réciproque de $G^L_{a,b}$ par le Frobenius absolu de S. Alors on a un isomorphisme canonique $(G^L_{a,b})^{(p)} \simeq G^{L^{\otimes p}}_{a^{\otimes p}, b^{\otimes p}}$, et l'homomorphisme Frobenius $F : G^L_{a,b} \to G^{L^{\otimes p}}_{a^{\otimes p}, b^{\otimes p}}$ et le Verschiebung $V : G^{L^{\otimes p}}_{a^{\otimes p}, b^{\otimes p}} \to G^L_{a,b}$

correspondent respectivement à $F_L : L \to L^{\otimes p}$ donné par $x \mapsto a \otimes x$ et à $V_L : L^{\otimes p} \to L$ donné par $x' \mapsto b \otimes x'$.

3. Le Cas sur un Trait

3.1. Soient R un anneau noethérien local et complet de corps résiduel de caractéristique p, $S = \mathrm{Spec}(R)$. Tout module projectif de rang 1 sur R est isomorphe à R. Un objet de la catégorie $\mathbf{C}_S$ est donc donné par un couple $(a, c) \in R \times R$ avec $ac = p \in R$. Notons G_c^a le schéma en groupes $G^R_{a,cw_{p-1}}$ sur R (2.10(i)). Un morphisme $f : G_{c_1}^{a_1} \to G_{c_2}^{a_2}$ de tels schémas en groupes est donné par un élément $u \in R$ tel que $a_2 = a_1 u^{p-1}$ et $c_1 = c_2 u^{p-1}$, et f est un isomorphisme si et seulement si u est inversible dans R.

3.2. Soit R un anneau de valuation discrète complet de corps résiduel de caractéristique p. D'après le théorème 2.9, tout schéma en groupes d'ordre p sur R s'écrit de la forme G_c^a avec $ac = p \in R$. Distinguons deux cas suivant la caractéristique de R :

Cas 1. *R est d'égale caractéristique*. La relation $ac = p = 0$ implique donc ou bien $a = 0$, ou bien $c = 0$. Les schémas en groupes d'ordre p sur R sont donc classifiés en trois classes suivantes :

(i) $a = c = 0$. Alors on a $G_0^0 \simeq \alpha_{p,R}$, le groupe constant additif d'ordre p sur R. Les homomorphismes de Frobenius et Verschiebung de $\alpha_{p,R}$ sont tous nuls, et le dual de Cartier de $\alpha_{p,R}$ est lui-même.

(ii) $a = 0$ et $c \neq 0$. Dans ce cas là, on a $G_c^0 \simeq \mathrm{Spec}(R[X]/X^p)$ avec la comultiplication donnée par

$$s(X) = 1 \otimes X + X \otimes 1 + \frac{c}{1-p} \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} (X^i \otimes X^{p-i}).$$

Le morphisme de Frobenius de G_c^0 est nul, et son morphisme Verschiebung

$$V : G_{c^p}^0 \simeq (G_{c^p}^0) \to G_c^0$$

est donné par $V^*(X) = cX$.

(iii) $c = 0$ et $a \neq 0$. On a alors $G_0^a \simeq \mathrm{Spec}(R[X]/(X^p - aX))$ avec la comultiplication $s(X) = 1 \otimes X + X \otimes 1$. Le morphisme Verschiebung de G_0^a est nul, et son morphisme de Frobenius $F : G_0^a \to G_0^{a^p} \simeq (G_0^a)^{(p)}$ est donné par $F^*(X) = aX$.

On remarque aussi qu'il existe pas de morphismes non-trivaux entre les schémas en groupes de type différents. Pour qu'il exisite un morphisme non-trivial $f : G_{c_1}^0 \to G_{c_2}^0$ (*resp.*$g : G_0^{a_1} \to G_0^{a_2}$), il faut et il suffit qu'il existe $u \in R\backslash\{0\}$ tel que $c_1 = c_2 u^{p-1}$ (*resp.*$a_2 = a_1 u^{p-1}$). Soit $v : R \to \mathbb{Z}_{\geq 0}$ une valuation sur R. Donc si $v(c_2) \leq v(c_1)$ (*resp.*$v(a_2) \geq v(a_1)$), il existe une extension finie et modérément ramifiée R' sur R, telle qu'il existe un morphisme $f : G_{c_1}^0 \to G_{c_2}^0$ (*resp.*$g : G_0^{a_1} \to G_0^{a_2}$) défini sur R'.

Cas 2. *R est d'inégales caractéristiques*. Soient v la valuation sur R normailisée par $v(R) = \mathbb{Z}_{\geq 0} \cup \{+\infty\}$, $e = v(p)$ l'indice de ramification absolu de R. Les schémas en groupes d'ordre p sur R sont de la forme G_c^a, où $a, c \in R$ avec $ac = p$. En particulier, on a $v(a) \leq e$.

Soient $G_{c_1}^{a_1}$ et $G_{c_2}^{a_2}$ deux schémas en groupes d'ordre p sur R. La donnée d'un homomorphisme non-trivial $f : G_{c_1}^{a_1} \to G_{c_2}^{a_2}$ de schémas en groupes est équivalente à la donnée d'un élément $u \in R$

non-nul tel que $a_2 = a_1 u^{p-1}$. Supposons un tel u non-nul existe. Si $v(u) = 0$, f est un isomorphisme sur R ; si $v(u) > 0$, on a forcément

$$e \geq v(a_2) = (p-1)v(u) + v(a_1) \geq p-1,$$

et la restriction de f aux fibres génériques est un isomorphisme tandis que sa restriction aux fibres spéciales est est nulle. En particulier, le noyau de f au sens de faisceaux fppf sur R n'est pas représentable par un schéma en groupes fini plat sur R.

Remarque 3.3. L'exemple précédent montre que, lorsque $e \geq p-1$, la catégorie des schémas en groupes finis plats sur R n'est pas abélienne et le foncteur "fibre générique" n'est pas pleinement fidèle. En revanche, Raynaud a montré que si $e < p-1$ le foncteur fibre générique induit une équivalence de catégories entre la catégorie des schémas en groupes sur R, annulés par une puissance de p, et la catégorie analogue sur le corps des fractions de R [Ray, 3.3.3 et 3.3.6].

Signalons enfin une autre description des schémas en groupes d'ordre p sur R dans le cas d'inégales caractéristiques. D'après [SOS], pour tout $\lambda \in R$ avec $0 \leq v(\lambda) \leq e/(p-1)$, on pose

$$P(\lambda) = \frac{(1+\lambda T)^p - 1}{\lambda^p}.$$

C'est un polynôme à coefficients dans R. On pose $G_\lambda = \mathrm{Spec}(R[T]/P_\lambda(T))$, et on le munit d'une structure de schéma en groupes sur R en posant la comultiplication

$$s(T) = 1 \otimes T + T \otimes 1 + \lambda T \otimes T$$

et le coinverse $T \mapsto (-T)/(1+\lambda T)$. Suivant Raynaud, on appelle G_λ *groupe de congruence de niveau* λ. Pour tout λ avec $0 \leq v(\lambda) \leq e/(p-1)$, on définit un morphisme $\theta_\lambda : G_\lambda \to \mu_p = \mathrm{Spec}(R[X]/X^p - 1)$ donné par $X \mapsto 1 + \lambda T$. Si $v(\lambda) = 0$, c'est un isomorphisme. D'après la classification précédente, il existe $a(\lambda), c(\lambda) \in R$ avec $a(\lambda)c(\lambda) = p$ tels que $G_\lambda \simeq G_{c(\lambda)}^{a(\lambda)}$. En effet, on peux prendre

$$a(\lambda) = \frac{p w_{p-1}}{(\lambda(1-p))^{p-1}} \quad \text{et} \quad c(\lambda) = \frac{(\lambda(1-p))^{p-1}}{w_{p-1}}.$$

Bien que les choix des $a(\lambda), c(\lambda)$ ne soient pas uniques, les valuations $v(a(\lambda)) = e - (p-1)v(\lambda)$ et $v(c(\lambda)) = (p-1)v(\lambda)$ sont uniquement déterminées par $v(\lambda)$. Réciproquement, étant donné $a, c \in R$ avec $ac = p$, il existe une extension finie et modérément ramifiée R' de R et $\lambda \in R'$ tel que $G_\lambda \simeq G_c^a$ sur R'. L'avantage des groupes de congruence est que pour tout $\lambda, \lambda' \in R$, avec $0 \leq v(\lambda), v(\nu) \leq e/(p-1)$, il existe des homomorphismes non-triviaux G_ν dans G_λ si et seulement si $v(\lambda) \leq v(\nu)$. En effet, si $v(\lambda) > v(\nu)$, on a $v(a(\lambda)) > v(a(\nu))$ donc il n'existe pas de morphismes non-triviaux de G_ν dans G_λ par la discussion plus haute ; si $v(\lambda) \leq v(\nu)$, on a un morphisme naturel $\theta_{\nu,\lambda} : G_\nu \to G_\lambda$, donné par $\theta^*_{\lambda',\lambda}(T) = \frac{\lambda'}{\lambda} T$, qui vérifie $\theta_\nu = \theta_{\nu,\lambda} \circ \theta_\lambda$. En particulier, si $v(\lambda) = v(\nu)$, on a $G_\nu \simeq G_\lambda$.

Références

[Ray] M. Raynaud, Schémas en groupes de type $(p, \cdots, p)$, *Bulletin de la S.M.F.*, tome 102 (1974), 241-280.

[SOS] T. Sekiguchi, F. Oort and N. Suwa, On the deformation of Artin-Schreier to Kummer, *Ann. Sci. de l'É.N.S.* 4^e série, tome 22, No.3 (1989), 345-375.

[TO] J. Tate et F. Oort, Group scheme of prime order, *Ann. Sci. de l'È.N.S. 4^e série*, tome 3, n° 1 (1970), 1-21.