EXPOSÉ VII$_A$

ÉTUDE INFINITÉSIMALE DES SCHÉMAS EN GROUPES

par P. GABRIEL

Dans l'exposé II nous nous étions limités à l'étude des invariants différentiels du premier ordre et nous n'avions pas abordé certains phénomènes spéciaux à la caractéristique $p > 0$ ou à la caractéristique 0. Notre objet dans la partie A de cet exposé est de combler cette lacune. **411**

D'ailleurs, l'étude infinitésimale d'ordre quelconque d'un schéma en groupes est reliée à celle du groupe formel associé ; l'objet de la deuxième partie de cet exposé est de présenter les premières définitions et propriétés concernant les groupes formels.

A) Opérateurs différentiels et p-algèbres de Lie (*)

1. Opérateurs différentiels

Dans cette section, ainsi que dans les sections 2 et 3, S désigne un schéma fixé et les produits considérés sont des produits cartésiens dans la catégorie des S-schémas. (1) Si X est un S-schéma, nous notons $p_{X/S}$, p_X ou simplement p le morphisme structural de X dans S.

1.1. Soit $u : Y \to X$ un morphisme de S-schémas et munissons l'image directe $u_*(\mathscr{O}_Y)$ du faisceau structural de Y de la structure de $\mathscr{O}_X$-module induite par u. Le faisceau $\mathscr{H} = \mathscr{H}om_{p_X^{-1}(\mathscr{O}_S)}(\mathscr{O}_X, u_*(\mathscr{O}_Y))$ des homomorphismes de $p_X^{-1}(\mathscr{O}_S)$-modules de $\mathscr{O}_X$ dans $u_*(\mathscr{O}_Y)$ est donc muni naturellement d'une structure de $\mathscr{O}_X$-bimodule : si U est un ouvert de X, f et d des sections de $\mathscr{O}_X$ et $\mathscr{H}$ sur U, fd et df sont respectivement les morphismes $g \mapsto fd(g)$ et $g \mapsto d(fg)$ de $\mathscr{O}_X$ dans $u_*(\mathscr{O}_Y)$. Nous écrirons désormais $(\mathrm{ad}\, f)(d)$ au lieu de $fd - df$. **412**

(*) La partie A du présent exposé n'avait pas été traitée sérieusement dans les exposés oraux.

(1) N.D.E. : En particulier, si X et Y sont deux S-schémas, $X \times_S Y$ est noté simplement $X \times Y$. D'autre part, signalons que pour le contenu des sections 1 et 2, on peut se reporter à [**DG70**], § II.4, n^{os} 5–6, voir aussi [**Ja03**], § I.7.

Définition 1.1.1. — Une S-*déviation d'ordre* $\leqslant n$ est par définition un couple $\mathrm{D} = (u, d)$ formé d'un morphisme de S-schémas $u : \mathrm{Y} \to \mathrm{X}$ et d'un morphisme de $p_{\mathrm{X}}^{-1}(\mathscr{O}_{\mathrm{S}})$-modules $d : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ tel que, pour tout ouvert U de X et toutes les suites de $n+1$ sections $f_0, \ldots, f_n \in \mathscr{O}_{\mathrm{X}}(\mathrm{U})$, on ait dans $\mathrm{Hom}_{p_{\mathrm{U}}^{-1}(\mathscr{O}_{\mathrm{S}})}(\mathscr{O}_{\mathrm{U}}, u_*(\mathscr{O}_{\mathrm{Y}})|_{\mathrm{U}})$ l'égalité :

$$(*_n) \qquad (\mathrm{ad}\, f_0)(\mathrm{ad}\, f_1)\cdots(\mathrm{ad}\, f_n)(d) = 0. \qquad (2)$$

Dans ce cas, nous dirons aussi que d est une S-*déviation de* u *d'ordre* $\leqslant n$. En particulier, une S-déviation de u d'ordre $\leqslant 0$ est un morphisme de $\mathscr{O}_{\mathrm{X}}$-modules de $\mathscr{O}_{\mathrm{X}}$ dans $u_*(\mathscr{O}_{\mathrm{Y}})$, c.-à-d., un élément de $\Gamma(\mathrm{Y}, \mathscr{O}_{\mathrm{Y}})$.

Définition 1.1.2. — Un morphisme de $p^{-1}(\mathscr{O}_{\mathrm{S}})$-modules $d : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ est une S-*déviation de* u si, pour tout point y de Y, il existe un voisinage ouvert U de $u(y)$ dans X et un voisinage ouvert V de y dans Y vérifiant les conditions suivantes :

a) $u(\mathrm{V}) \subset \mathrm{U}$;

b) si $v : \mathrm{V} \to \mathrm{U}$ est le morphisme induit par u, il y a un entier n tel que le morphisme $\mathscr{O}_{\mathrm{U}} \to v_*(\mathscr{O}_{\mathrm{V}})$ induit par d soit une S-déviation de v d'ordre $\leqslant n$. (3)

Si d est une S-déviation de u, nous disons aussi que le couple $\mathrm{D} = (u, d)$ est une S-déviation et il nous arrivera d'écrire $\mathrm{Y} \xrightarrow{\mathrm{D}} \mathrm{X}$ ou $\mathrm{Y} \xrightarrow[u]{d} \mathrm{X}$.

Lorsque d est l'homomorphisme d'algèbres $u^\natural : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ qui correspond au morphisme $u : \mathrm{Y} \to \mathrm{X}$, nous écrirons aussi u au lieu de D.

Remarques 1.1.3. — (4) Soit $\mathrm{Dév}(u)$ (resp. $\mathrm{Dév}^{\leqslant n}(u)$) l'ensemble des S-déviations de u (resp. S-déviations de u d'ordre $\leqslant n$). Il est muni d'une structure naturelle de $\mathscr{O}_{\mathrm{Y}}(\mathrm{Y})$-module : si $\lambda \in \mathscr{O}_{\mathrm{Y}}(\mathrm{Y})$, λd est la déviation qui envoie f sur $\lambda d(f)$, pour toute section f de $\mathscr{O}_{\mathrm{X}}$ sur un ouvert U.

Pour tout ouvert V de Y, posons $\mathscr{D}\acute{e}v(u)(\mathrm{V}) = \mathrm{Dév}(u|_{\mathrm{V}})$, c.-à-d., $\mathscr{D}\acute{e}v(u)(\mathrm{V})$ est l'ensemble des

$$\begin{aligned} d_{\mathrm{V}} \in \mathrm{Hom}_{p^{-1}(\mathscr{O}_{\mathrm{S}})}(\mathscr{O}_{\mathrm{X}}, (u|_{\mathrm{V}})_*(\mathscr{O}_{\mathrm{V}})) &\cong \mathrm{Hom}_{p^{-1}(\mathscr{O}_{\mathrm{S}})}((u|_{\mathrm{V}})^{-1}\mathscr{O}_{\mathrm{X}}, \mathscr{O}_{\mathrm{V}}) \\ &\cong \mathscr{H}om_{p^{-1}(\mathscr{O}_{\mathrm{S}})}(u^{-1}\mathscr{O}_{\mathrm{X}}, \mathscr{O}_{\mathrm{Y}})(\mathrm{V}) \end{aligned}$$

(2) N.D.E. : On voit facilement que ceci équivaut à dire que, pour tout $x \in \mathrm{X}$ et $f_0, \ldots, f_n, g \in \mathscr{O}_{\mathrm{X},x}$, on a $(\mathrm{ad}\, f_0)(\mathrm{ad}\, f_1)\cdots(\mathrm{ad}\, f_n)(d_x)(g) = 0$. D'autre part, rappelons que l'isomorphisme d'adjonction :

$$\theta : \mathrm{Hom}_{p_{\mathrm{X}}^{-1}(\mathscr{O}_{\mathrm{S}})}(\mathscr{O}_{\mathrm{X}}, u_*(\mathscr{O}_{\mathrm{Y}})) \xrightarrow{\sim} \mathrm{Hom}_{p_{\mathrm{Y}}^{-1}(\mathscr{O}_{\mathrm{S}})}(u^{-1}(\mathscr{O}_{\mathrm{X}}), \mathscr{O}_{\mathrm{Y}})$$

associe à tout morphisme de $p_{\mathrm{X}}^{-1}(\mathscr{O}_{\mathrm{S}})$-modules $d : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ le morphisme $d' = \varepsilon \circ u^{-1}(d)$, où ε est le morphisme canonique $u^{-1}u_*(\mathscr{O}_{\mathrm{Y}}) \to \mathscr{O}_{\mathrm{Y}}$. Réciproquement, pour tout $p_{\mathrm{Y}}^{-1}(\mathscr{O}_{\mathrm{S}})$-morphisme $d' : u^{-1}(\mathscr{O}_{\mathrm{X}}) \to \mathscr{O}_{\mathrm{Y}}$, on a $\theta^{-1}(d') = u_*(d') \circ \eta$, où η est le morphisme canonique $\mathscr{O}_{\mathrm{X}} \to u_*u^{-1}(\mathscr{O}_{\mathrm{X}})$. Il en résulte que d vérifie $(*_n)$ si et seulement si d' vérifie :

$$(*'_n) \qquad (\mathrm{ad}\, f_0)\cdots(\mathrm{ad}\, f_n)(d')(g) = 0$$

pour tout ouvert V de Y et $f_0, \ldots, f_n, g \in u^{-1}(\mathscr{O}_{\mathrm{X}})(\mathrm{V})$.

(3) N.D.E. : Si X et u sont *quasi-compacts*, toute S-déviation de u est donc d'ordre $\leqslant n$, pour un certain entier n.

(4) N.D.E. : On a ajouté ces remarques, qui seront utiles dans 1.3, 1.4 et 2.1.

tels que, pour tout ouvert U de X, l'application $d_{\mathrm{V}}(\mathrm{U}) : \mathscr{O}_{\mathrm{X}}(\mathrm{U}) \to \mathscr{O}_{\mathrm{Y}}(u^{-1}(\mathrm{U}) \cap \mathrm{V})$ vérifie $(*_n)$. Ceci définit un préfaisceau de $\mathscr{O}_{\mathrm{Y}}$-modules sur Y, et l'on voit facilement que c'est un *faisceau* (plus précisément, un sous-faisceau de $\mathscr{H}om_{p^{-1}(\mathscr{O}_{\mathrm{S}})}(u^{-1}\mathscr{O}_{\mathrm{X}}, \mathscr{O}_{\mathrm{Y}})$).

1.2. Considérons maintenant deux S-déviations $\mathrm{D} = (u, d)$ et $\mathrm{E} = (v, e)$:

$$\mathrm{Z} \xrightarrow[e]{v} \mathrm{Y} \xrightarrow[d]{u} \mathrm{X} \quad .$$

Lorsque U parcourt les ouverts de X, les applications composées

$$\Gamma(\mathrm{U}, \mathscr{O}_{\mathrm{X}}) \xrightarrow{d(\mathrm{U})} \Gamma(u^{-1}\mathrm{U}, \mathscr{O}_{\mathrm{Y}}) \xrightarrow{e(u^{-1}\mathrm{U})} \Gamma(v^{-1}u^{-1}\mathrm{U}, \mathscr{O}_{\mathrm{Z}})$$

définissent une S-déviation de uv que nous noterons de ; lorsque d est d'ordre $\leqslant m$ et **413**
e d'ordre $\leqslant n$, de est d'ordre $\leqslant m + n$. Nous écrirons aussi

$$(\dagger) \qquad \mathrm{D} \circ \mathrm{E} = (uv, de) \qquad {}^{(5)}$$

et nous dirons que $\mathrm{D} \circ \mathrm{E}$ ou DE est la S-*déviation composée*. Lorsque $d = u^\natural$ (c.-à-d., $\mathrm{D} = u$ avec la convention de 1.1), on dit aussi que DE est *l'image de* E *par* u.

L'application $(\mathrm{D}, \mathrm{E}) \mapsto \mathrm{D} \circ \mathrm{E}$ que nous venons de définir nous permettra désormais de parler de la *catégorie des* S-*déviations*, qui a pour objets les S-schémas, pour morphismes les S-déviations. [6]

Définition 1.2.0. — [7] Soit $w : \mathrm{Z} \to \mathrm{X}$ un S-morphisme. Une S-*dérivation de* w, ou S-*dérivation de* $\mathscr{O}_{\mathrm{X}}$ *dans* $w_*(\mathscr{O}_{\mathrm{Z}})$, est un morphisme de $p^{-1}(\mathscr{O}_{\mathrm{S}})$-modules $d : \mathscr{O}_{\mathrm{X}} \to w_*(\mathscr{O}_{\mathrm{Z}})$ tel que, pour tout ouvert U de X et $f, g \in \mathscr{O}_{\mathrm{X}}(\mathrm{U})$,

$$d(fg) = w^\natural(f)d(g) + w^\natural(g)d(f).$$

Alors, d est une déviation de w d'ordre $\leqslant 1$, qui s'annule sur la section unité de $\mathscr{O}_{\mathrm{X}}$. On notera $\mathrm{Dér}_{\mathrm{S}}(w)$ l'ensemble des S-dérivations de w ; c'est un $\mathscr{O}(\mathrm{Z})$-module.

Avec les notations de 1.2, prenons Y égal à $\mathrm{I}_{\mathrm{Z}} = \operatorname{Spec} \mathscr{O}_{\mathrm{Z}}[t]$, où $t^2 = 0$, et v égal à la section zéro $\tau : \mathrm{Z} \to \mathrm{I}_{\mathrm{Z}}$, définie par le morphisme de $\mathscr{O}_{\mathrm{Z}}$-algèbres $\mathscr{O}_{\mathrm{Z}}[t] \to \mathscr{O}_{\mathrm{Z}}$ qui envoie t sur 0, et prenons e égal au morphisme de $\mathscr{O}_{\mathrm{Z}}$-modules $\sigma : \mathscr{O}_{\mathrm{Z}}[t]$ défini par $\sigma(1) = 0$ et $\sigma(t) = 1$, [8] qu'il est commode de noter ∂_t.

Si $u : \mathrm{I}_{\mathrm{Z}} \to \mathrm{X}$ est un morphisme vérifiant $w = u \circ s$, alors $\sigma \circ u^\natural$ est une S-dérivation de $\mathscr{O}_{\mathrm{X}}$ dans $w_*(\mathscr{O}_{\mathrm{Z}})$. Réciproquement, à toute S-dérivation d on associe le morphisme $u : \mathrm{I}_{\mathrm{Z}} \to \mathrm{X}$ tel que $u = w$ sur les espaces sous-jacents, et

$$u^\natural(f) = w^\natural(f) + d(f)\, t,$$

---

(5) N.D.E. : On prendra garde qu'avec cette notation, de désigne la composée « d suivie de e ».

(6) N.D.E. : Souvent, on ne considère que les S-déviations du morphisme id_{X}, qui forment l'algèbre des S-opérateurs différentiels de X, cf. 1.4 plus bas. Toutefois, le cadre plus général des S-déviations fournit un langage « fonctoriel » commode pour démontrer des énoncés tels que : « si G est un S-groupe, l'algèbre des S-opérateurs différentiels sur G, invariants à gauche, est isomorphe à l'algèbre des S-déviations de la section unité $\varepsilon : \mathrm{S} \to \mathrm{G}$, cf. 2.1 et 2.4 plus loin.

(7) N.D.E. : On a détaillé ce paragraphe, en attribuant à cette définition (resp. au lemme qui suit) le numéro 1.2.0 (resp. 1.2.1).

(8) N.D.E. : On a ajouté ce qui suit, i.e. on a introduit la notation ∂_t.

pour toute section f de $\mathscr{O}_X$ sur un ouvert U. On obtient ainsi :

Lemme 1.2.1. — *Soit* $E = (\tau, \partial_t)$ *la déviation de* $\tau : Z \to I_Z$ *définie plus haut. Pour tout* S*-morphisme* $w : Z \to X$*, l'application* $u \mapsto u \circ E$ *est une bijection entre les* S*-morphismes* $u : I_Z \to X$ *tels que* $u \circ s = w$*, et les* S*-dérivations de* w*.*

1.2.2. — Soit d une S-déviation de $u : Y \to X$. D'une part, d est évidemment une S′-déviation de u pour tout morphisme $s : S \to S'$.

D'autre part, soit $t : T \to S$ un morphisme de but S, et soient $u_T : Y_T \to X_T$ le morphisme déduit de u par changement de base, et $t_Y : Y_T \to Y$ et $t_X : X_T \to X$ les projections canoniques. Il existe alors une T-déviation de u_T et une seule, que nous noterons d_T ou $d \times T$, qui vérifie l'égalité $t_X d_T = d t_Y$, au sens de (†) plus haut, c.-à-d., pour tout ouvert U de X, on a un diagramme commutatif : [9]

$$\begin{array}{ccc} \mathscr{O}(U) & \xrightarrow{t_X^\natural} & \mathscr{O}(U \times T) \\ {\scriptstyle d(U)}\downarrow & & \downarrow{\scriptstyle d_T(U\times T)} \\ \mathscr{O}(u^{-1}U) & \xrightarrow{t_Y^\natural} & \mathscr{O}(u^{-1}U \times T). \end{array}$$

Si l'on pose $D = (u, d)$, on écrira aussi $D_T = (u_T, d_T)$ et nous dirons que d_T *et* D_T *sont déduits de* d *et* D *par changement de base.*

414 ***1.2.3***. — Soient par exemple $u : Y \to X$ et $v : Z \to T$ deux S-morphismes, d et e des S-déviations de u et v. On a un diagramme commutatif

$$\begin{array}{ccc} X \times T & \xleftarrow{u_T} & Y \times T \\ {\scriptstyle v_X}\uparrow & \nwarrow^{u\times v} & \uparrow{\scriptstyle v_Y} \\ X \times Z & \xleftarrow{u_Z} & Y \times Z \end{array}$$

et nous noterons $d \times e$ (*produit de* d *et* e) la S-déviation de $u \times v$ égale à $d_T e_Y = e_X d_Z$ (avec la convention (†) plus haut), c.-à-d., pour tout ouvert U de $X \times T$, si l'on désigne

[9] N.D.E. : Explicitement, si V est un ouvert affine de S et U (resp. U′) un ouvert affine de X (resp. T) au-dessus de V, de sorte que $\mathscr{O}_{X\times T}(U \times U') = \mathscr{O}_X(U) \otimes_{\mathscr{O}_S(V)} \mathscr{O}_T(U')$, alors $d_T(U \times U')$ est la composée :

$$\mathscr{O}_X(U) \otimes_{\mathscr{O}_S(V)} \mathscr{O}_T(U') \xrightarrow{d(U)\otimes \mathrm{id}} \mathscr{O}_Y(u^{-1}U) \otimes_{\mathscr{O}_S(V)} \mathscr{O}_T(U') \longrightarrow \mathscr{O}_{Y\times T}(u^{-1}U \times U').$$

L'auteur a laissé au lecteur le soin de vérifier que d_T est bien définie, et les éditeurs font de même.

par W l'ouvert $v_{\mathrm{Y}}^{-1}u_{\mathrm{T}}^{-1}\mathrm{U} = u_{\mathrm{Z}}^{-1}v_{\mathrm{X}}^{-1}\mathrm{U}$, on a un diagramme commutatif :

$$\begin{array}{ccc} \mathscr{O}(\mathrm{U}) & \xrightarrow{d_{\mathrm{T}}(\mathrm{U})} & \mathscr{O}(u_{\mathrm{T}}^{-1}\mathrm{U}) \\ \Big\downarrow{\scriptstyle e_{\mathrm{X}}(\mathrm{U})} & \searrow^{(d\times e)(\mathrm{U})} & \Big\downarrow{\scriptstyle e_{\mathrm{Y}}(u_{\mathrm{T}}^{-1}\mathrm{U})} \\ \mathscr{O}(v_{\mathrm{X}}^{-1}\mathrm{U}) & \xrightarrow{d_{\mathrm{Z}}(v_{\mathrm{X}}^{-1}\mathrm{U})} & \mathscr{O}(\mathrm{W}). \end{array}$$

Si l'on pose $\mathrm{D} = (u, d)$ et $\mathrm{E} = (v, d)$, nous écrirons aussi $\mathrm{D} \times \mathrm{E} = (u \times v, d \times e)$.

1.3. [(10)] Soit $u : \mathrm{Y} \to \mathrm{X}$ un morphisme de S-schémas. Rappelons que l'isomorphisme d'adjonction :

$$\mathrm{Hom}_{p_{\mathrm{X}}^{-1}(\mathscr{O}_{\mathrm{S}})}(\mathscr{O}_{\mathrm{X}}, u_*(\mathscr{O}_{\mathrm{Y}})) \xrightarrow{\sim} \mathrm{Hom}_{p_{\mathrm{Y}}^{-1}(\mathscr{O}_{\mathrm{S}})}(u^{-1}(\mathscr{O}_{\mathrm{X}}), \mathscr{O}_{\mathrm{Y}})$$

associe à tout morphisme de $p^{-1}(\mathscr{O}_{\mathrm{S}})$-modules $d : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ le morphisme $d' = \varepsilon \circ u^{-1}(d)$, où ε est le morphisme canonique $u^{-1}u_*(\mathscr{O}_{\mathrm{Y}}) \to \mathscr{O}_{\mathrm{Y}}$.

Notons $\mathscr{J}_u$ (resp. $\mathscr{I}_u$) le noyau de l'homomorphisme d'algèbres $u^\natural : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ (resp. $u^{\natural\prime} : u^{-1}(\mathscr{O}_{\mathrm{X}}) \to \mathscr{O}_{\mathrm{Y}}$) et soit $d : \mathscr{O}_{\mathrm{X}} \to u_*(\mathscr{O}_{\mathrm{Y}})$ un morphisme de $p^{-1}(\mathscr{O}_{\mathrm{S}})$-modules. Si U est un ouvert de X et $f_0, \ldots, f_n, g \in \mathscr{O}_{\mathrm{X}}(\mathrm{U})$, on voit facilement par récurrence sur n que la condition $(*_n)$ équivaut à l'égalité suivante (cf. EGA IV_4, 16.8.8.2) :

$$(**_n) \qquad 0 = \sum_{\mathrm{I}\subset[\![0,n]\!]} (-1)^{|\mathrm{I}|}\, u^\natural(f_{[\![0,n]\!]-\mathrm{I}})\, d(f_{\mathrm{I}}g),$$

où f_{I} désigne le produit des f_i, pour $i \in \mathrm{I}$. Il en résulte que si d vérifie $(*_n)$, alors d s'annule sur l'idéal $\mathscr{J}_u^{n+1}$.

Supposons maintenant Y égal à S ; alors $u : \mathrm{S} \to \mathrm{X}$ est une section de $p : \mathrm{X} \to \mathrm{S}$, donc est une immersion (cf. EGA I, 5.3.13). Alors, d'une part, $\varepsilon : u^{-1}u_*\mathscr{O}_{\mathrm{S}} \to \mathscr{O}_{\mathrm{S}}$ est un isomorphisme, de sorte que $u^{-1}(\mathscr{J}_u) = \mathscr{I}_u$. D'autre part, on a un isomorphisme :

$$(\star) \qquad u^{-1}(\mathscr{O}_{\mathrm{X}}) \cong \mathscr{O}_{\mathrm{S}} \oplus \mathscr{I}_u.$$

Supposons que d s'annule sur $\mathscr{J}_u^{n+1}$. Alors $d' = \varepsilon \circ u^{-1}(d)$ s'annule sur $\mathscr{I}_u^{n+1}$ et donc d' vérifie les analogues $(**'_n)$ et $(*'_n)$ de $(**_n)$ et $(*_n)$, lorsque $f_0, \ldots, f_n \in \mathscr{I}_u(u^{-1}(\mathrm{U}))$. De plus, comme $(\mathrm{ad}\, a)(\phi) = 0$, pour tout $a \in \mathscr{O}_{\mathrm{S}}(u^{-1}(\mathrm{U}))$ et tout morphisme de $\mathscr{O}_{u^{-1}(\mathrm{U})}$-modules $\phi : u^{-1}(\mathscr{O}_{\mathrm{U}}) \to \mathscr{O}_{u^{-1}(\mathrm{U})}$, on déduit de $(\star)$ que d' vérifie l'analogue $(*'_n)$ de $(*_n)$. Il en résulte que d vérifie $(*_n)$. Par conséquent, on a obtenu :

Lemme. — *Si $u : \mathrm{S} \to \mathrm{X}$ est une section de $p : \mathrm{X} \to \mathrm{S}$, alors d est une* S*-déviation de u d'ordre $\leqslant n$ si et seulement si d' s'annule sur $\mathscr{I}_u^{n+1}$.*

Cette interprétation peut être généralisée comme suit. Soient $u : \mathrm{Y} \to \mathrm{X}$ un S-morphisme quelconque et Γu le graphe de u, c'est-à-dire le morphisme $\mathrm{Y} \to \mathrm{Y} \times \mathrm{X}$

[(10)] N.D.E. : On a détaillé l'original dans ce paragraphe ; voir aussi la N.D.E. (2) dans 1.1.1.

de composantes id_Y et u. Pour toute S-déviation d de u d'ordre $\leqslant n$, on obtient par composition :

$$Y \xrightarrow{\text{diag.}} Y \times Y \xrightarrow[u_Y]{d_Y} Y \times X$$

une Y-déviation de Γu d'ordre $\leqslant n$ que nous noterons Γd (*le graphe de* d).

Réciproquement, à toute Y-déviation e de Γu on associe la S-déviation composée $e_X = \mathrm{pr}_2 \circ e$:

$$Y \xrightarrow[\Gamma u]{e} Y \times X \xrightarrow{\mathrm{pr}_2} X.$$

On voit aussitôt que $(\Gamma d)_X = d$, et l'égalité $\Gamma e_X = e$ résulte du fait que e est $\mathscr{O}_Y$-linéaire [(11)]. *On obtient ainsi un isomorphisme de* $\mathscr{O}_Y(Y)$*-modules* :

$$\begin{array}{ccc} \{\text{S-déviations de } u \text{ d'ordre} \leqslant n\} & \xrightarrow{\sim} & \{\text{Y-déviations de } \Gamma u \text{ d'ordre} \leqslant n\} \\ d & \mapsto & \Gamma d. \end{array}$$

De plus, on voit facilement que d est une S-dérivation de u si et seulement Γd est une Y-dérivation de Γu.

415 Appelons $\mathscr{I}_{\Gamma u}$ le noyau de l'homomorphisme d'algèbres $(\Gamma u)^{-1}(\mathscr{O}_{Y\times X}) \longrightarrow \mathscr{O}_Y$ qui correspond à Γu. Tenant compte du lemme qui précède, on a obtenu :

Proposition. — *Soient* $u : Y \to X$ *un* S*-morphisme et* $\Gamma u : Y \to Y \times X$ *son graphe. Les* S*-déviations de* u *d'ordre* $\leqslant n$ *s'identifient aux* Y*-déviations de* Γu *d'ordre* $\leqslant n$*, lesquelles sont en bijection avec*

$$\mathrm{Hom}_{\mathscr{O}_Y}\big((\Gamma u)^{-1}(\mathscr{O}_{Y\times X})/\mathscr{I}_{\Gamma u}^{n+1}, \mathscr{O}_Y\big).$$

1.3.1. — [(12)] Revenons au cas où $u : S \to X$ est une section de $p : X \to S$. Alors, l'homomorphisme $\phi : u^{-1}(\mathscr{O}_X) \to \mathscr{O}_S$ admet une section, que nous noterons simplement $g \mapsto g \cdot 1$, de sorte que, avec les notations de 1.3, on a un isomorphisme de $\mathscr{O}_S$-modules :

$$(\star) \qquad u^{-1}(\mathscr{O}_X) \cong \mathscr{O}_S \oplus \mathscr{I}_u,$$

et pour toute section f de $u^{-1}(\mathscr{O}_X)$, $f - \phi(f)\cdot 1$ est une section de $\mathscr{I}_u$.

Soient d une S-déviation de u d'ordre $\leqslant 1$, et d' le $\mathscr{O}_S$-morphisme $u^{-1}(\mathscr{O}_X) \to \mathscr{O}_S$ correspondant à d. Si a, b sont des sections de $u^{-1}(\mathscr{O}_X)$, on a :

$$0 = d'\big((a - \phi(a)\cdot 1)(b - \phi(b)\cdot 1)\big) = d'(ab) - \phi(a)d'(b) - \phi(b)d'(a) + \phi(ab)d'(1).$$

Par conséquent, on voit que d est une S-dérivation de u (cf. 1.2.1 et N.D.E. (2)) si et seulement si $d'(1) = 0$. On obtient donc :

[(11)] N.D.E. : Si λ, f sont des sections locales de $\mathscr{O}_Y$ et $\mathscr{O}_X$, on a $(\Gamma e_X)(\lambda \otimes f) = \lambda \cdot e(1 \otimes g)$, et ceci égale $e(\lambda \otimes g)$ puisque e est $\mathscr{O}_Y$-linéaire.

[(12)] N.D.E. : On a ajouté ce paragraphe.

Lemme. — *Les* S*-dérivations de* u *sont exactement les* S*-déviations de* u *d'ordre* 1 *qui s'annulent sur la section unité de* $\mathscr{O}_X$ *; elles correspondent au* $\mathscr{O}_S(S)$*-module*

$$\mathrm{Hom}_{\mathscr{O}_S}(\mathscr{I}_u/\mathscr{I}_u^2, \mathscr{O}_S),$$

et l'on a un isomorphisme de $\mathscr{O}_S(S)$*-modules* $\mathrm{Dév}^{\leqslant 1}(u) \cong \mathscr{O}_S(S) \oplus \mathrm{Dér}_S(u)$.

Revenant au cas général, on en déduit, avec les notations de 1.3,

Corollaire. — *Soient* $u : Y \to X$ *un* S*-morphisme et* $\Gamma u : Y \to Y \times X$ *son graphe. On a un isomorphisme canonique de* $\mathscr{O}_Y(Y)$*-modules*

$$\mathrm{Dér}_S(u) \cong \mathrm{Dér}_Y(\Gamma u) \cong \mathrm{Hom}_{\mathscr{O}_Y}(\mathscr{I}_{\Gamma u}/\mathscr{I}_{\Gamma u}^2, \mathscr{O}_Y).$$

Définition 1.4. — Soit X un S-schéma. On appelle S-*opérateur différentiel* (resp. S-*opérateur différentiel d'ordre* $\leqslant n$) sur X toute S-déviation (resp. toute S-déviation d'ordre $\leqslant n$) du morphisme identique de X.

D'après 1.1, un S-opérateur différentiel d'ordre $\leqslant n$ est donc un endomorphisme de $p^{-1}(\mathscr{O}_S)$-module de $\mathscr{O}_X$ qui vérifie les égalités $(*_n)$ de 1.1. Nous désignerons par $\mathrm{Dif}^n_{X/S}$ le $\Gamma(\mathscr{O}_S)$-module [13] formé des S-opérateurs différentiels d'ordre $\leqslant n$, par $\mathrm{Dif}_{X/S}$ celui formé de tous les S-opérateurs différentiels.

Comme nous l'avons vu en 1.2, on peut composer les S-déviations de id_X, ce qui munit $\mathrm{Dif}_{X/S}$ d'une structure de $\Gamma(\mathscr{O}_S)$-algèbre ; nous dirons que c'est l'*algèbre des opérateurs différentiels de* X/S.

De même, pour tout ouvert V de X, posons $\mathscr{D}if_{X/S}(V) = \mathrm{Dif}_{V/S} = \mathrm{Dév}(\mathrm{id}_V)$; d'après 1.1.3, ceci définit un *faisceau* de $\mathscr{O}_X$-modules, appelé le *faisceau des* S-*opérateurs différentiels sur* X. [14]

1.4.1. — Comme nous l'avons vu en 1.3, on peut interpréter les opérateurs différentiels de X/S au moyen du graphe du morphisme identique de X, c'est-à-dire du morphisme diagonal $\Delta = \Delta_{X/S}$ de X dans $X \times X$. Traduisons dans le contexte actuel les énoncés de 1.3.

Munissons $\mathscr{O}_{X\times X}$ de la structure de $\mathrm{pr}_1^{-1}(\mathscr{O}_X)$-algèbre définie par pr_1, de sorte que $\Delta^{-1}(\mathscr{O}_{X\times X})$ est muni d'une structure d'algèbre sur $\mathscr{O}_X = \Delta^{-1}\mathrm{pr}_1^{-1}(\mathscr{O}_X)$. Soit $\mathscr{I}_{X/S}$ le noyau de l'homomorphisme

$$\Delta^{-1}(\mathscr{O}_{X\times X}) \longrightarrow \mathscr{O}_X$$

adjoint de l'homomorphisme $\mathscr{O}_{X\times X} \to \Delta_*(\mathscr{O}_X)$, et soit $\mathscr{P}^m_{X/S}$ la $\mathscr{O}_X$-algèbre

$$\Delta^{-1}(\mathscr{O}_{X\times X})/\mathscr{I}^{m+1}_{X/S}.$$

Si V est un ouvert affine de S et U un ouvert affine de X au-dessus de V, et si l'on **416**
pose $k = \Gamma(V, \mathscr{O}_S)$ et $A = \Gamma(U, \mathscr{O}_X)$, on a donc :

$$\Gamma(U, \mathscr{P}^m_{X/S}) = (A \otimes_k A)/I^{m+1},$$

[13] N.D.E. : Dans cet exposé, l'anneau $\Gamma(S, \mathscr{O}_S) = \mathscr{O}_S(S)$ est noté $\Gamma(\mathscr{O}_S)$.

[14] N.D.E. : On a modifié ici l'original, qui mentionnait le faisceau $U \mapsto \mathrm{Dif}_{X_U/U}$, où U parcourt les ouverts de S ; celui-ci est l'image directe de $\mathscr{D}if_{X/S}$ par le morphisme $p_X : X \to S$.

où I est l'idéal engendré par les éléments $a \otimes 1 - 1 \otimes a$, pour $a \in \mathrm{A}$. Ceci étant, *on a* d'après 1.3 *un isomorphisme de* $\mathscr{O}_\mathrm{X}(\mathrm{X})$*-modules* :

$$j_\mathrm{X} : \mathrm{Dif}^m_{\mathrm{X}/\mathrm{S}} \xrightarrow{\sim} \mathrm{Hom}_{\mathscr{O}_\mathrm{X}}(\mathscr{P}^m_{\mathrm{X}/\mathrm{S}}, \mathscr{O}_\mathrm{X})$$

qu'on peut définir comme suit : si d appartient à $\mathrm{Dif}^m_{\mathrm{X}/\mathrm{S}}$ et si c est une section de $\mathscr{P}^m_{\mathrm{X}/\mathrm{S}}$ sur U de la forme $a \otimes b + \mathrm{I}^{m+1}$, on a $j_\mathrm{X}(d)(c) = a \cdot d(b)$. (15)

1.4.2. — Soient d un opérateur différentiel et u une section de X sur S. Nous appelons *valeur de* d *en* u *la* S*-déviation composée*

$$\mathrm{S} \xrightarrow{u} \mathrm{X} \xrightarrow[\mathrm{id}_\mathrm{X}]{d} \mathrm{X}.$$

D'après 1.3 et 1.4.1, si d est un opérateur différentiel d'ordre $\leqslant m$, alors du (resp. d) est associé canoniquement à un morphisme de $\mathscr{O}_\mathrm{S}$-modules $d' : u^{-1}(\mathscr{O}_\mathrm{X})/\mathscr{I}_u^{m+1} \to \mathscr{O}_\mathrm{S}$ (resp. un morphisme de $\mathscr{O}_\mathrm{X}$-modules $d'' : \mathscr{P}^m_{\mathrm{X}/\mathrm{S}} \to \mathscr{O}_\mathrm{X}$).

Il est clair qu'on peut construire d' à partir de d'' de la manière suivante : le carré

$$\begin{array}{ccc} \mathrm{X} \simeq \mathrm{S} \times \mathrm{X} & \xrightarrow{u \times \mathrm{X}} & \mathrm{X} \times \mathrm{X} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}_1} \\ \mathrm{S} & \xrightarrow{u} & \mathrm{X} \end{array}$$

est cartésien, ce qui permet d'identifier X à $\mathrm{S} \times_\mathrm{X} (\mathrm{X} \times \mathrm{X})$, u à $\mathrm{S} \times_\mathrm{X} \Delta$, donc $u^*(\mathscr{P}^m_{\mathrm{X}/\mathrm{S}})$ à $u^{-1}(\mathscr{O}_\mathrm{X})/\mathscr{I}_u^{m+1}$. On identifie ainsi $u^*(d'')$ à un morphisme $u^{-1}(\mathscr{O}_\mathrm{X})/\mathscr{I}_u^{m+1} \to \mathscr{O}_\mathrm{S}$, qui n'est autre que d'.

417 **1.5.** Posons comme d'habitude $\mathrm{I}_\mathrm{S} = \mathrm{Spec}\, \mathscr{O}_\mathrm{S}[\mathrm{T}]/(\mathrm{T}^2)$. Soient $\tau : \mathrm{S} \to \mathrm{I}_\mathrm{S}$ la section zéro et σ la déviation canonique de τ que nous avons définie en 1.2.0, i.e. l'homomorphisme de $\mathscr{O}_\mathrm{S}$-modules qui s'annule sur la section unité de $\mathscr{O}_\mathrm{S}[\mathrm{T}]/(\mathrm{T}^2)$ et qui envoie la classe t de T modulo T^2 sur la section unité de $\mathscr{O}_\mathrm{S}$.

Soit X un S-schéma. À tout I_S-automorphisme u de $\mathrm{I}_\mathrm{S} \times \mathrm{X}$ induisant l'identité sur X est associé par composition un opérateur différentiel D_u de X :

$$\mathrm{X} \simeq \mathrm{S} \times \mathrm{X} \xrightarrow{\sigma \times \mathrm{X}} \mathrm{I}_\mathrm{S} \times \mathrm{X} \xrightarrow{u} \mathrm{I}_\mathrm{S} \times \mathrm{X} \xrightarrow{\mathrm{pr}_2} \mathrm{X}.$$

D'après II, 3.14, *l'application* $u \mapsto \mathrm{D}_u$ *est un isomorphisme de la* $\Gamma(\mathscr{O}_\mathrm{S})$*-algèbre de Lie*

$$\mathrm{Lie}(\underline{\mathrm{Aut}}\, \mathrm{X}) := \underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}\, \mathrm{X})(\mathrm{S})$$

sur la $\Gamma(\mathscr{O}_\mathrm{S})$*-algèbre de Lie des* $p^{-1}(\mathscr{O}_\mathrm{S})$*-dérivations de* $\mathscr{O}_\mathrm{X}$. L'isomorphisme réciproque associe à toute dérivation D l'automorphisme de $\mathrm{I}_\mathrm{S} \times \mathrm{X}$ correspondant à l'automorphisme $a + bt \mapsto a + (\mathrm{D}a + b)t$ de $\mathscr{O}_\mathrm{X}[\mathrm{T}]/(\mathrm{T}^2)$.

(15) N.D.E. : Via cet isomorphisme, les X-dérivations de $\Delta_{\mathrm{X}/\mathrm{S}}$ correspondent, d'après 1.3.1, aux S-dérivations de id_X, c.-à-d., aux $p^{-1}(\mathscr{O}_\mathrm{S})$-dérivations de $\mathscr{O}_\mathrm{X}$.

2. Opérateurs différentiels invariants sur les schémas en groupes

418

2.1. *Soit* G *un* S*-schéma en groupes* ; nous désignons par ε ou $\varepsilon_G : S \to G$ la section unité de G.

Définition. — Soit U(G) le $\Gamma(\mathscr{O}_S)$-module des S-déviations de ε_G (ou S-*déviations de l'origine*) (cf. 1.1).

Si d et e sont deux éléments de U(G), $d \times e$ est une S-déviation de $\varepsilon \times \varepsilon : S \simeq S \times S \to G \times G$. L'image de $d \times e$ par le morphisme multiplication $m : G \times G \to G$ (cf. 1.2) sera appelé le produit de d et e et sera noté $d \cdot e$.

Le $\Gamma(\mathscr{O}_S)$-module U(G) se trouve ainsi muni d'une structure de $\Gamma(\mathscr{O}_S)$-algèbre associative qui a ε_G pour élément unité (1.1). Nous dirons que U(G) est *l'algèbre infinitésimale* de G. (16)

Lorsque T parcourt les schémas au-dessus de S, l'algèbre infinitésimale $U(G_T)$ du T-groupe $G \times T$ varie évidemment de façon contravariante en T, de sorte que nous pourrons parler du foncteur algèbre infinitésimale.

Lorsque T parcourt les ouverts de S, on obtient donc un préfaisceau $T \mapsto U(G_T)$ de $\mathscr{O}_S$-algèbres ; de plus, d'après 1.1.3, ceci est un *faisceau*. Nous le noterons $\mathscr{U}(G)$ et nous l'appellerons *le faisceau d'algèbres infinitésimales* de G.

L'algèbre U(G) est aussi un foncteur covariant en G. En effet, si $u : G \to H$ est un homomorphisme de S-groupes et d une S-déviation de ε_G, l'image de d par u est un élément $U(u)(d) = ud$ de U(H). L'application $U(u) : U(G) \to U(H)$ ainsi définie est évidemment un homomorphisme de $\Gamma(\mathscr{O}_S)$-algèbres. On définit de même un homomorphisme $\mathscr{U}(u)$ de $\mathscr{U}(G)$ dans $\mathscr{U}(H)$.

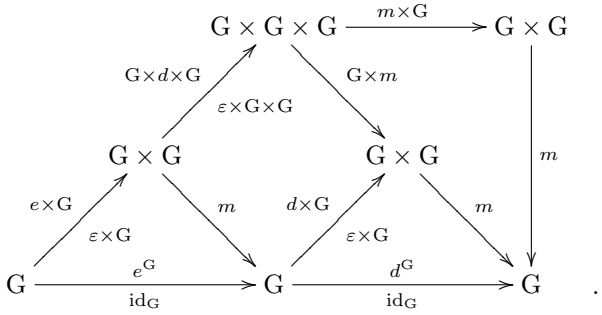
2.2. Soit d un élément de U(G), c.-à-d., une S-déviation de l'origine de G. Considérons la S-déviation $d \times G$ de $\varepsilon \times G : G \simeq S \times G \to G \times G$ obtenue à partir de d par changement de base (1.2.2) ; l'image de $d \times G$ par le morphisme multiplication $m : G \times G \to G$ est une S-déviation de $m \circ (\varepsilon \times \mathrm{id}_G) = \mathrm{id}_G$, i.e. un élément de $\mathrm{Dif}_{G/S}$, qu'on notera d^G.

L'application $d \mapsto d^G$ est évidemment $\Gamma(\mathscr{O}_S)$-linéaire et le diagramme « commutatif » ci-dessous montre qu'on a $(e \cdot d)^G = d^G \cdot e^G$: (17) 419

---

(16) N.D.E. : On dit maintenant « l'algèbre des distributions » (à l'origine) de G, cf. [**DG70**], § II.4, 6.1 et [**Ja03**], I 7.7.

(17) N.D.E. : On a corrigé l'original, en remplaçant dans le diagramme $d \times G \times G$ par $G \times d \times G$, de sorte que la composée sur le côté gauche du triangle est $(e \times d) \times G$, et que l'application $d \mapsto d^G$ est un *anti-isomorphisme* de U(G) sur les opérateurs diférentiels *invariants à droite* (cf. 2.3, 2.4 ci-dessous) ; d'autre part, en définissant ${}^G d$ comme l'image par m de $G \times d$, on obtiendrait de même un *isomorphisme* de U(G) sur les opérateurs diférentiels *invariants à gauche* (cf. [**DG70**], § II.4, Th. 6.5). On a corrigé en conséquence 2.4 et 2.5.



La commutativité des deux triangles du bas résulte en effet de la définition de d^{G} et e^{G} ; d'autre part, la S-déviation composée de $e \times \mathrm{G}$ et $\mathrm{G} \times d \times \mathrm{G}$ est $(e \times d) \times \mathrm{G}$ (cf. 1.2.2), son image par $m \times \mathrm{G}$ est $(e \cdot d) \times \mathrm{G}$, et l'image de celle-ci par m est donc égale à $(e \cdot d)^{\mathrm{G}}$.

On obtient ainsi un anti-homomorphisme $\mathrm{U}(\mathrm{G}) \to \mathrm{Dif}_{\mathrm{G/S}}$ de $\Gamma(\mathscr{O}_{\mathrm{S}})$-algèbres, appelé *translation à droite.* (18)

Si $\mathscr{D}if_{\mathrm{G/S}}$ désigne le faisceau des S-opérateurs différentiels sur G (cf. 1.4) et p le morphisme structural $\mathrm{G} \to \mathrm{S}$, on définit de même une « translation à droite » : $\mathscr{U}(\mathrm{G}) \to p_*(\mathscr{D}if_{\mathrm{G/S}})$.

2.3. Nous allons maintenant caractériser les opérateurs différentiels de G sur S de la forme d^{G}. Soient $g : \mathrm{S} \to \mathrm{G}$ une section du morphisme structural de G et g_{G} la translation à droite de G par g, c'est-à-dire le morphisme composé :

$$g_{\mathrm{G}} : \ \mathrm{G} \simeq \mathrm{G} \times \mathrm{S} \xrightarrow{\mathrm{G}\times g} \mathrm{G} \times \mathrm{G} \xrightarrow{m} \mathrm{G}.$$

Pour tout opérateur différentiel D de G sur S, la composée $g_{\mathrm{G}}^{-1}\mathrm{D}g_{\mathrm{G}}$ (cf. 1.2) est encore une S-déviation de id_{G}, c.-à-d., un élément de $\mathrm{Dif}_{\mathrm{X/S}}$; nous noterons :

$$\mathrm{D}^g = g_{\mathrm{G}}^{-1}\mathrm{D}\, g_{\mathrm{G}}.$$

Nous dirons que D est *invariant à droite* si, pour tout changement de base $t : \mathrm{T} \to \mathrm{S}$ et toute section $g : \mathrm{T} \to \mathrm{G} \times \mathrm{T}$, on a $(\mathrm{D}_{\mathrm{T}})^g = \mathrm{D}_{\mathrm{T}}$.

420 ***Lemme***. — *Pour tout opérateur différentiel* D *de* G *sur* S, *les assertions suivantes sont équivalentes* (où m est le morphisme multiplication de G) *:*

(i) D *est invariant à droite.*

(ii) *Les deux déviations de m suivantes sont égales :* $\mathrm{D}\, m = m(\mathrm{D} \times \mathrm{G})$.

(18) N.D.E. : Il serait préférable de l'appeler *opération à gauche*. En effet, soit par exemple d une S-dérivation de l'origine ; d'après 1.2.1, d est la composée de la S-dérivation $(\tau, \partial_t) : \mathrm{S} \to \mathrm{I}_{\mathrm{S}}$ et d'un morphisme $x : \mathrm{I}_{\mathrm{S}} \to \mathrm{G}$ tel que $x \circ \tau = \varepsilon$ (i.e. $x \in \underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$), et alors d^{G} est la dérivation de $\mathscr{O}_{\mathrm{G}}$ qui envoie une section locale ϕ sur la section $g \mapsto \partial_t \phi(xg)$. De plus, avec cette terminologie, on pourrait dire que : « l'opération à gauche commute aux translations à droite ».

(ii) ⇒ (i) : comme la condition (ii) est stable par changement de base, il suffit de montrer que (ii) entraîne l'égalité $D^g = D$ pour toute section $g : S \to G$. Soit h le morphisme $G \times g : G \simeq G \times S \to G \times G$, de sorte que $m \circ h$ est la translation à droite g_G. L'égalité $D^g = D$ équivaut à l'égalité $g_G \circ D = D \circ g_G$, et celle-ci résulte du diagramme commutatif :

$$\begin{array}{ccccc} G & \xleftarrow{m} & G \times G & \xleftarrow{h} & G \\ {\scriptstyle D}\downarrow{\scriptstyle \mathrm{id}_G} & & {\scriptstyle D\times G}\downarrow{\scriptstyle \mathrm{id}_{(G\times G)}} & & {\scriptstyle D}\downarrow{\scriptstyle \mathrm{id}_G} \\ G & \xleftarrow{m} & G \times G & \xleftarrow{h} & G \end{array} .$$

(i) ⇒ (ii) : prenons en effet pour $t : T \to S$ le morphisme structural $p : G \to S$, pour section $g : T \to G \times T$ le morphisme diagonal $\Delta : G \to G \times G$. La translation à droite

$$\Delta_{G\times G} : G \times G \longrightarrow G \times G$$

est alors le morphisme de $G \times G$ dans $G \times G$ qui a pour composantes m et pr_2. L'égalité $(D_G)^{\Delta} = D_G$ équivaut alors à la commutativité du premier carré du diagramme suivant :

$$\begin{array}{ccccc} G \times G & \xrightarrow{\Delta_{G\times G}} & G \times G & \xrightarrow{\mathrm{pr}_1} & G \\ {\scriptstyle D_G}\downarrow{\scriptstyle \mathrm{id}_{G\times G}} & & {\scriptstyle D_G}\downarrow{\scriptstyle \mathrm{id}_{G\times G}} & & {\scriptstyle D}\downarrow{\scriptstyle \mathrm{id}_G} \\ G \times G & \xrightarrow{\Delta_{G\times G}} & G \times G & \xrightarrow{\mathrm{pr}_1} & G \end{array} .$$

L'égalité (ii) résulte donc de ce que $m = \mathrm{pr}_1 \circ \Delta_{G\times G}$.

Considérons par exemple un élément d de l'algèbre infinitésimale U(G). Les carrés **421**
du diagramme

$$\begin{array}{ccccccc} G \times G & = & S \times G \times G & \xrightarrow[\varepsilon\times G\times G]{d\times G\times G} & G \times G \times G & \xrightarrow{m\times G} & G \times G \\ {\scriptstyle m}\downarrow & & {\scriptstyle S\times m}\downarrow & & {\scriptstyle G\times m}\downarrow & & {\scriptstyle m}\downarrow \\ G & = & S \times G & \xrightarrow[\varepsilon\times G]{d\times G} & G \times G & \xrightarrow{m} & G \end{array}$$

sont alors commutatifs. Comme on a

$$m \circ (d \times G) = d^G \qquad \text{et} \qquad (m \times G) \circ (d \times G \times G) = d^G \times G,$$

on a aussi $d^G \circ m = m \circ (d^G \times G)$. Donc : *pour toute* S*-déviation* d *de l'origine,* d^G *est un opérateur différentiel invariant à droite.*

2.4. Théorème. — (i) *L'application* $d \mapsto d^{\mathrm{G}}$ *est un* anti-isomorphisme [19] *de l'algèbre infinitésimale* $\mathrm{U}(\mathrm{G})$ *sur la sous-algèbre* $\mathrm{Dif}^{\mathrm{G}}_{\mathrm{G/S}}$ *de* $\mathrm{Dif}_{\mathrm{G/S}}$ *formée des opérateurs différentiels invariants à* droite.

(*ii*) *De même, l'application* $d \mapsto {}^{\mathrm{G}}d$ *est un* isomorphisme *de* $\mathrm{U}(\mathrm{G})$ *sur la sous-algèbre de* $\mathrm{Dif}_{\mathrm{G/S}}$ *formée des opérateurs différentiels invariants à* gauche.

Soit en effet D un opérateur différentiel quelconque de G sur S et désignons par D_0 sa *valeur à l'origine*, c'est-à-dire la déviation composée $\mathrm{S} \xrightarrow{\varepsilon} \mathrm{G} \xrightarrow[\mathrm{id_G}]{\mathrm{D}} \mathrm{G}$. L'opérateur différentiel invariant à droite $(\mathrm{D}_0)^{\mathrm{G}}$ est alors obtenu par composition :

$$\mathrm{G} \simeq \mathrm{S} \times \mathrm{G} \xrightarrow{\varepsilon \times \mathrm{G}} \mathrm{G} \times \mathrm{G} \xrightarrow[\mathrm{id_{G \times G}}]{\mathrm{D} \times \mathrm{G}} \mathrm{G} \times \mathrm{G} \xrightarrow{m} \mathrm{G}.$$

Si D est invariant à droite, on a $\mathrm{D}\, m = m(\mathrm{D} \times \mathrm{G})$, d'où

$$\mathrm{D} = \mathrm{D}\, m(\varepsilon \times \mathrm{G}) = m(\mathrm{D} \times \mathrm{G})(\varepsilon \times \mathrm{G}) = (\mathrm{D}_0)^{\mathrm{G}}.$$

En particulier, l'application $d \mapsto d^{\mathrm{G}}$ est surjective.

Réciproquement, soit d une S-déviation de l'origine. On a alors un carré commutatif

$$\begin{array}{ccc} \mathrm{G} \times \mathrm{G} & \xleftarrow{d \times \mathrm{G}} & \mathrm{G} \\ {\scriptstyle \mathrm{G} \times \varepsilon}\uparrow & & \uparrow{\scriptstyle \varepsilon} \\ \mathrm{G} \times \mathrm{S} \simeq \mathrm{G} & \xleftarrow{d} & \mathrm{S} \end{array}$$

422 d'où il résulte que $d = m(\mathrm{G} \times \varepsilon)d = m(d \times \mathrm{G})\varepsilon = (d^{\mathrm{G}})_0$. *A fortiori*, l'application $d \mapsto d^{\mathrm{G}}$ est injective. Ceci prouve le théorème.

Lorsque S varie, le théorème 2.4 implique évidemment que la translation à droite $\mathscr{U}(\mathrm{G}) \to p_*(\mathscr{D}if_{\mathrm{G/S}})$ est un anti-isomorphisme de $\mathscr{O}_{\mathrm{S}}$-algèbres de $\mathscr{U}(\mathrm{G})$ sur le faisceau de $\mathscr{O}_{\mathrm{S}}$-algèbres $p_*(\mathscr{D}if_{\mathrm{G/S}})^{\mathrm{G}}$, qui à tout ouvert U de S associe $\mathrm{Dif}^{\mathrm{G_U}}_{\mathrm{G_U/U}}$.

2.4.1. Remarque. — Considérons le diagramme commutatif

$$\begin{array}{ccc} \mathrm{G} & \xleftarrow{\eta} & \mathrm{G} \times \mathrm{G} \\ {\scriptstyle p}\downarrow\uparrow{\scriptstyle \varepsilon} & & {\scriptstyle \mathrm{pr}_1}\downarrow\uparrow{\scriptstyle \Delta} \\ \mathrm{S} & \xleftarrow{p} & \mathrm{G} \end{array} \quad ,$$

où η désigne le morphisme « $(x, y) \mapsto yx^{-1}$ » [20]. Celui-ci induit des morphismes

$$\eta' : \eta^{-1}(\mathscr{O}_{\mathrm{G}}) \longrightarrow \mathscr{O}_{\mathrm{G \times G}} \qquad \text{et} \qquad \Delta^{-1}(\eta') : p^{-1}\varepsilon^{-1}(\mathscr{O}_{\mathrm{G}}) \longrightarrow \Delta^{-1}(\mathscr{O}_{\mathrm{G \times G}}).$$

[19] N.D.E. : On a corrigé « isomorphisme » en « anti-isomorphisme », et l'on a ajouté l'assertion (ii), cf. la N.D.E. (17).

[20] N.D.E. : c.-à-d., G agit à gauche sur lui-même par translations à droite.

Pour tout entier $n \geqslant 1$, posons $\mathfrak{p}^n_{G/S} = \varepsilon^{-1}(\mathscr{O}_G)/\mathscr{I}_\varepsilon^{n+1}$ (confer 1.3 et 1.4 pour les notations). (21) Comme le carré formé par les morphismes ε, η, Δ et p est cartésien, $\Delta^{-1}(\eta')$ induit un *isomorphisme de $\mathscr{O}_G$-modules* :

$$p^*(\mathfrak{p}^n_{G/S}) \xrightarrow{\sim} \mathscr{P}^n_{G/S}.$$

Les opérateurs différentiels de G sur S d'ordre $\leqslant n$ correspondent donc biunivoquement aux morphismes de $\mathscr{O}_G$-modules $p^*(\mathfrak{p}^n_{G/S}) \longrightarrow \mathscr{O}_G$, c'est-à-dire aux morphismes 423
de $\mathscr{O}_S$-modules

$$\mathfrak{p}^n_{G/S} \longrightarrow p_*(\mathscr{O}_G).$$

Dans cette bijection, les opérateurs différentiels invariants à droite sont associés aux flèches composées

$$\mathfrak{p}^n_{G/S} \longrightarrow \mathscr{O}_S \xrightarrow{\text{can.}} p_*(\mathscr{O}_G).$$

On retrouve ainsi l'isomorphisme du théorème 2.4.

2.5. (22) Soit Lie(G) l'algèbre de Lie de G (23) ; on va définir un morphisme de $\Gamma(\mathscr{O}_S)$-algèbres de Lie $\alpha : \mathrm{Lie}(G) \to U(G)$.

Soient $s : S \to I_S$ la section nulle de $I_S \to S$ et σ la déviation de s définie en 1.2.0. Rappelons (cf. II, 4.1) que Lie(G) est l'ensemble des morphismes $x : I_S \to G$ tels que $x \circ s = \varepsilon_G$. Alors la composée

$$S \xrightarrow[s]{\sigma} I_S \xrightarrow{x} G$$

est une S-déviation de ε_G, i.e. un élément de U(G) ; avec les notations de 1.2 (†), elle est notée σx. De plus, d'après 1.2.1, l'application $\alpha : x \mapsto \sigma x$ est un isomorphisme de $\mathscr{O}_S(S)$-modules de Lie(G) sur le sous-module Dér(ε_G) de U(G) formé des S-dérivations de ε_G. Nous allons voir que α est un morphisme d'algèbres de Lie. (24) Soit

$$\rho' : \quad U(G) \longrightarrow \mathrm{Dif}_{G/S}$$

le morphisme d'algèbres qui à une S-déviation d de ε_G associe l'opérateur différentiel invariant à *gauche* ${}^G d \in \mathrm{Dif}_{G/S}$, cf. 2.2, N.D.E. (17).

Soit $\rho : G \to \underline{\mathrm{Aut}}_S(G)$ l'homomorphisme de foncteurs en groupes qui associe à un S-morphisme $g : T \to G$ la translation *à droite* de G_T par g, i.e. le morphisme :

$$G_T \simeq T \times_T G_T \xrightarrow{G_T \times g} G_T \times_T G_T \xrightarrow{m_T} G_T.$$

Rappelons aussi (cf. 1.5 et II, 3.14) que $\mathrm{Lie}(\underline{\mathrm{Aut}}\, G) = \underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}_S(G)/S)(S)$ s'identifie aux automorphismes infinitésimaux de G, c.-à-d., aux automorphismes de $I_S \times G$

(21) N.D.E. : Dans ce qui suit, on a corrigé l'original, qui référait au carré formé par les morphismes p, p, η, et pr_1, au lieu de ε, η, Δ et p.
(22) N.D.E. : Dans ce paragraphe, on a modifié l'ordre, en commençant par définir l'application $\alpha : \mathrm{Lie}(G) \to U(G)$, et l'on a corrigé l'original, comme indiqué dans la N.D.E. (17).
(23) N.D.E. : Dans cet exposé, si G (resp. X) est un S-schéma en groupes (resp. un S-schéma), l'« algèbre de Lie » Lie(G) (resp. Lie($\underline{\mathrm{Aut}}$ X)) désigne, avec les notations de l'exposé II, $\underline{\mathrm{Lie}}(G/S)(S)$ (resp. $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}_S(X)/S)(S)$) ; c'est une $\Gamma(\mathscr{O}_S)$-algèbre de Lie, d'après II, 4.11 et 3.14.
(24) N.D.E. : Voir aussi II, 4.11.

induisant l'identité sur G. Comme ρ est un monomorphisme, il en est de même du morphisme $\underline{\mathrm{Lie}}(\rho) : \underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S}) \to \underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}_{\mathrm{S}}(\mathrm{G})/\mathrm{S})$ (voir, par exemple, Exp. II, N.D.E. (50)), donc $\mathrm{Lie}(\rho) : \mathrm{Lie}(\mathrm{G}) \to \mathrm{Lie}(\underline{\mathrm{Aut}}\,\mathrm{G})$ est injectif.

D'autre part, d'après 1.5, l'application β qui à tout automorphisme infinitésimal u de G associe l'opérateur différentiel D_u de G :

$$\mathrm{G} \simeq \mathrm{S} \times \mathrm{G} \xrightarrow{\sigma \times \mathrm{G}} \mathrm{I}_{\mathrm{S}} \times \mathrm{G} \xrightarrow{u} \mathrm{I}_{\mathrm{S}} \times \mathrm{G} \xrightarrow{\mathrm{pr}_2} \mathrm{G}$$

est un isomorphisme de $\mathrm{Lie}(\underline{\mathrm{Aut}}\,\mathrm{G})$ sur la sous-algèbre de Lie de $\mathrm{Dif}_{\mathrm{G}/\mathrm{S}}$ formée des $p^{-1}(\mathscr{O}_{\mathrm{S}})$-dérivations de $\mathscr{O}_{\mathrm{G}}$.

Pour tout $x \in \mathrm{Lie}(\mathrm{G})$, on a le carré commutatif suivant qui détermine l'image de x par $\mathrm{Lie}(\rho)$:

$$\begin{array}{ccc} \mathrm{I}_{\mathrm{S}} \times \mathrm{G} & \xrightarrow{\mathrm{Lie}(\rho)(x)} & \mathrm{I}_{\mathrm{S}} \times \mathrm{G} \\ \downarrow{\scriptstyle x \times \mathrm{G}} & & \downarrow{\scriptstyle \mathrm{pr}_2} \\ \mathrm{G} \times \mathrm{G} & \xrightarrow{m} & \mathrm{G} \end{array} .$$

424 Compte-tenu de ce diagramme, l'image de $\mathrm{Lie}(\rho)(x)$ par β est la déviation composée

$$\mathrm{G} \simeq \mathrm{S} \times \mathrm{G} \xrightarrow[s \times \mathrm{G}]{\sigma \times \mathrm{G}} \mathrm{I}_{\mathrm{S}} \times \mathrm{G} \xrightarrow{\mathrm{G} \times x} \mathrm{G} \times \mathrm{G} \xrightarrow{m} \mathrm{G}$$

qui, d'après 2.2 N.D.E. (17), n'est autre que ${}^{\mathrm{G}}(\sigma x) = \rho'(\alpha(x))$. On obtient donc un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Lie}(\mathrm{G}) & \xhookrightarrow{\mathrm{Lie}(\rho)} & \mathrm{Lie}(\underline{\mathrm{Aut}}\,\mathrm{G}) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ \mathrm{U}(\mathrm{G}) & \xhookrightarrow{\rho'} & \mathrm{Dif}_{\mathrm{G}/\mathrm{S}} \end{array}$$

où $\mathrm{Lie}(\rho)$, β et ρ' sont des morphismes d'algèbres de Lie. Comme ρ' est injectif, il en résulte que α est aussi un morphisme d'algèbres de Lie. Par conséquent, on a obtenu :

Proposition. — *α est un isomorphisme de $\mathscr{O}_{\mathrm{S}}(\mathrm{S})$-algèbres de Lie, de* $\mathrm{Lie}(\mathrm{G})$ *dans l'algèbre de Lie des* S*-dérivations de ε_{G}, elle-même isomorphe via* $\mathrm{Lie}(\rho)$ *à l'algèbre de Lie des* S*-dérivations de* G *invariantes à gauche.* [(25)]

3. Coalgèbres et dualité de Cartier

425

[(25)] N.D.E. : Il y a des exemples d'algèbres de Lie $\mathfrak{g}$ sur un anneau A, telles que l'application $\mathfrak{g} \to \mathrm{U}(\mathfrak{g})$ ne soit *pas* injective, cf. [**BLie**], § I.2, Ex. 9. Le résultat ci-dessus montre (puisque α se factorise en $\mathrm{Lie}(\mathrm{G}) \to \mathrm{U}(\mathrm{Lie}(\mathrm{G})) \to \mathrm{U}(\mathrm{G})$) que ceci ne peut se produire pour des algèbres de Lie « algébriques », c.-à-d., de la forme $\mathrm{Lie}(\mathrm{G})$, où G est un A-schéma en groupes.

3.1. Soit S un schéma (ou, plus généralement, un espace annelé). Une $\mathscr{O}_S$-*coalgèbre* [26] est un couple $(\mathscr{U}, \Delta_{\mathscr{U}})$ formé d'un $\mathscr{O}_S$-module $\mathscr{U}$ et d'un morphisme de $\mathscr{O}_S$-modules $\Delta_{\mathscr{U}} : \mathscr{U} \to \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U}$ (dit *morphisme diagonal* ou *comultiplication*) tels que :

(i) $\sigma \circ \Delta_{\mathscr{U}} = \Delta_{\mathscr{U}}$, où $\sigma(a \otimes b) = b \otimes a$.

(ii) Le carré

$$\begin{array}{ccc} \mathscr{U} & \xrightarrow{\Delta_{\mathscr{U}}} & \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} \\ {\scriptstyle \Delta_{\mathscr{U}}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{\mathscr{U}} \otimes \Delta_{\mathscr{U}}} \\ \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} & \xrightarrow{\Delta_{\mathscr{U}} \otimes \mathrm{id}_{\mathscr{U}}} & \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} \end{array}$$

est commutatif.

(iii) Il existe un morphisme de $\mathscr{O}_S$-modules $\varepsilon_{\mathscr{U}} : \mathscr{U} \to \mathscr{O}_S$, dit *augmentation*, tel que les morphismes composés

$$\mathscr{U} \xrightarrow{\Delta_{\mathscr{U}}} \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} \xrightarrow{\mathrm{id}_{\mathscr{U}} \otimes \varepsilon_{\mathscr{U}}} \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{O}_S \simeq \mathscr{U}$$
$$\mathscr{U} \xrightarrow{\Delta_{\mathscr{U}}} \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} \xrightarrow{\varepsilon_U \otimes \mathrm{id}_{\mathscr{U}}} \mathscr{O}_S \otimes_{\mathscr{O}_S} \mathscr{U} \simeq \mathscr{U}$$

soient le morphisme identique de $\mathscr{U}$.

Si $\varepsilon_{\mathscr{U}}$ et $\varepsilon'_{\mathscr{U}}$ sont deux augmentations, on a $\varepsilon_{\mathscr{U}} = (\varepsilon_{\mathscr{U}} \otimes \varepsilon'_{\mathscr{U}}) \circ \Delta_{\mathscr{U}} = \varepsilon'_{\mathscr{U}}$; l'augmentation est donc déterminée de façon unique par (iii).

Si $(\mathscr{U}, \Delta_{\mathscr{U}})$ et $(\mathscr{V}, \Delta_{\mathscr{V}})$ sont deux $\mathscr{O}_S$-coalgèbres, un *morphisme* de la première dans la seconde est un morphisme de $\mathscr{O}_S$-modules $f : \mathscr{U} \to \mathscr{V}$ tel que les diagrammes

$$\begin{array}{ccc} \mathscr{U} & \xrightarrow{f} & \mathscr{V} \\ {\scriptstyle \Delta_{\mathscr{U}}}\downarrow & & \downarrow{\scriptstyle \Delta_{\mathscr{V}}} \\ \mathscr{U} \otimes \mathscr{U} & \xrightarrow{f \otimes f} & \mathscr{V} \otimes \mathscr{V} \end{array} \qquad \text{et} \qquad \begin{array}{ccc} \mathscr{U} & \xrightarrow{f} & \mathscr{V} \\ & {\scriptstyle \varepsilon_{\mathscr{U}}} \searrow \quad \swarrow {\scriptstyle \varepsilon_{\mathscr{V}}} & \\ & \mathscr{O}_S & \end{array}$$

soient commutatifs. Les morphismes de coalgèbres se composent comme les mor- **426**
phismes de $\mathscr{O}_S$-modules de sorte que nous pourrons parler de la catégorie des $\mathscr{O}_S$-coalgèbres.

3.1.0. — [27] Cette catégorie possède des produits finis : l'objet final est le $\mathscr{O}_S$-module $\mathscr{O}_S$, la comultiplication étant l'identité ; le produit de deux coalgèbres $(\mathscr{U}, \Delta_{\mathscr{U}})$ et $(\mathscr{V}, \Delta_{\mathscr{V}})$ est le produit tensoriel $\mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{V}$, la comultiplication étant le morphisme composé

$$\mathscr{U} \otimes \mathscr{V} \xrightarrow{\Delta_{\mathscr{U}} \otimes \Delta_{\mathscr{V}}} \mathscr{U} \otimes \mathscr{U} \otimes \mathscr{V} \otimes \mathscr{V} \xrightarrow{\mathrm{id}_{\mathscr{U}} \otimes \sigma \otimes \mathrm{id}_{\mathscr{V}}} \mathscr{U} \otimes \mathscr{V} \otimes \mathscr{U} \otimes \mathscr{V}$$

[26] N.D.E. : On dit aussi « *cogèbre* », cf. [**BAlg**], III § 11.1. D'autre part, on notera que dans cet exposé (ainsi que dans VII_B), on se place dans la catégorie des coalgèbres *cocommutatives* (c.-à-d., vérifiant la condition (i)), ce qui est crucial pour définir le produit et la notion de coalgèbre en groupes (cf. 3.1.0 et 3.2).

[27] N.D.E. : On a ajouté la numérotation 3.1.0, pour références ultérieures.

où $\sigma(a\otimes b) = b\otimes a$; les projections canoniques de $\mathscr{U}\otimes\mathscr{V}$ sur les facteurs $\mathscr{U}$ et $\mathscr{V}$ sont les morphismes $\mathrm{id}_{\mathscr{U}}\otimes\varepsilon_{\mathscr{V}}$ et $\varepsilon_{\mathscr{U}}\otimes\mathrm{id}_{\mathscr{V}}$, [28] et le « morphisme diagonal » $\mathscr{U}\to\mathscr{U}\otimes\mathscr{U}$ (correspondant au couple de morphismes $(\mathrm{id}_{\mathscr{U}},\mathrm{id}_{\mathscr{U}})$) n'est autre que la comultiplication $\Delta_{\mathscr{U}}$.

3.1.1. — Soit $\mathscr{A}$ une $\mathscr{O}_S$-algèbre commutative, *localement libre et de type fini* en tant que $\mathscr{O}_S$-module. Si nous posons

$$\mathscr{A}^* = \mathscr{H}om_{\mathscr{O}_S\text{-Mod.}}(\mathscr{A},\mathscr{O}_S),$$

le morphisme canonique φ de $\mathscr{A}^*\otimes_{\mathscr{O}_S}\mathscr{A}^*$ dans $(\mathscr{A}\otimes_{\mathscr{O}_S}\mathscr{A})^*$ est inversible. Si $m : \mathscr{A}\otimes\mathscr{A}\to\mathscr{A}$ est le morphisme définissant la multiplication de $\mathscr{A}$, on obtient par composition un morphisme diagonal

$$\Delta_{\mathscr{A}^*} : \quad \mathscr{A}^* \xrightarrow{m^*} (\mathscr{A}\otimes\mathscr{A})^* \xrightarrow{\varphi^{-1}} \mathscr{A}^*\otimes\mathscr{A}^*.$$

Ce morphisme diagonal fait évidemment de $\mathscr{A}^*$ une $\mathscr{O}_S$-coalgèbre qui a pour aug-
427 mentation le morphisme transposé du morphisme $\mathscr{O}_S\to\mathscr{A}$ défini par la section unité de $\mathscr{A}$. De plus, il est clair que :

Le foncteur $\mathscr{A}\mapsto\mathscr{A}^*$ est une anti-équivalence de la catégorie des $\mathscr{O}_S$-algèbres, qui sont localement libres et de type fini en tant que $\mathscr{O}_S$-modules, sur la catégorie des $\mathscr{O}_S$-coalgèbres localement libres et de type fini en tant que $\mathscr{O}_S$-modules.

3.1.2. — À toute $\mathscr{O}_S$-coalgèbre $\mathscr{U}$ est associée canoniquement un S-foncteur

$$\mathrm{Spec}^*\,\mathscr{U} : (\mathbf{Sch}_{/S})^\circ \longrightarrow (\mathbf{Ens}).$$

Remarquons en effet que, pour tout S-schéma $q : T\to S$, $q^*(\mathscr{U}\otimes_{\mathscr{O}_S}\mathscr{U})$ s'identifie à $q^*(\mathscr{U})\otimes_{\mathscr{O}_T}q^*(\mathscr{U})$, de sorte que $q^*(\Delta_{\mathscr{U}})$ fait de $\mathscr{U}_T = q^*(\mathscr{U})$ une $\mathscr{O}_T$-coalgèbre ; nous pouvons donc poser par définition et avec un abus de notation évident : [29]

$$(\mathrm{Spec}^*\,\mathscr{U})(T) = \{x\in\Gamma(T,\mathscr{U}_T)\mid \varepsilon_{\mathscr{U}_T}(x) = 1 \quad\text{et}\quad \Delta_{\mathscr{U}_T}(x) = x\otimes x\}.$$

Les sections x de $\mathscr{U}_T$ correspondent évidemment aux morphismes de $\mathscr{O}_T$-modules $\xi : \mathscr{O}_T\to\mathscr{U}_T$; les conditions $\varepsilon(x) = 1$ et $\Delta(x) = x\otimes x$ expriment simplement que ξ est un morphisme de coalgèbres. On a donc également :

$$(\mathrm{Spec}^*\,\mathscr{U})(T) = \mathrm{Hom}_{\mathscr{O}_T\text{-coalg.}}(\mathscr{O}_T,\mathscr{U}_T).$$

En particulier, on a la proposition suivante : [30]

---

[28] N.D.E. : On a ajouté ce qui suit. Rappelons aussi que, pour montrer que $\mathscr{U}\otimes\mathscr{V}$ est bien le produit de $\mathscr{U}$ et $\mathscr{V}$ dans la catégorie des $\mathscr{O}_S$-cogèbres cocommutatives, on vérifie que si l'on a une $\mathscr{O}_S$-cogèbre arbitraire $\mathscr{E}$ et des morphismes de cogèbres $f : \mathscr{E}\to\mathscr{U}$ et $g : \mathscr{E}\to\mathscr{V}$, alors tout morphisme de cogèbres $\phi : \mathscr{E}\to\mathscr{U}\otimes\mathscr{V}$ tel que $\mathrm{pr}_{\mathscr{U}}\circ\phi = f$ et $\mathrm{pr}_{\mathscr{V}}\circ\phi = g$ est nécessairement égal à $(f\otimes g)\circ\Delta_{\mathscr{E}}$, et que celui-ci est un morphisme de cogèbres si et seulement si il égale $(g\otimes f)\circ\Delta_{\mathscr{E}}$.

[29] N.D.E. : Pour tout $x\otimes y\in\Gamma(T,\mathscr{U}_T)\otimes_{\mathscr{O}(T)}\Gamma(T,\mathscr{U}_T)$, son image dans $\Gamma(T,\mathscr{U}_T\otimes_{\mathscr{O}_T}\mathscr{U}_T)$ est encore notée $x\otimes y$.

[30] N.D.E. : On a ajouté la numérotation 3.1.2.1, pour références ultérieures. Remarquons d'autre part que le S-foncteur $\mathrm{Spec}^*\,\mathscr{U}$ est un faisceau pour la topologie de Zariski (et même pour la topologie (fpqc) si $\mathscr{U}$ est un $\mathscr{O}_S$-module quasi-cohérent).

Proposition 3.1.2.1. — *Soit $\mathscr{A}$ une $\mathscr{O}_S$-algèbre commutative qui est localement libre de type fini en tant que $\mathscr{O}_S$-module. Alors le* S*-foncteur* $\mathrm{Spec}^*\,\mathscr{A}^*$ *est représenté par* $\mathrm{Spec}\,\mathscr{A}$.

En effet, pour tout S-schéma T, on a des isomorphismes canoniques :

$$(\mathrm{Spec}^*\,\mathscr{A}^*)(T) = \mathrm{Hom}_{\mathscr{O}_T\text{-coalg.}}(\mathscr{O}_T, \mathscr{A}_T^*) \simeq \mathrm{Hom}_{\mathscr{O}_T\text{-alg.}}(\mathscr{A}_T, \mathscr{O}_T) \simeq (\mathrm{Spec}\,A)(T).$$

3.2. Une $\mathscr{O}_S$-*coalgèbre en groupes*, c'est-à-dire un groupe de la catégorie des $\mathscr{O}_S$-coalgèbres, consiste en la donnée d'une $\mathscr{O}_S$-coalgèbre $(\mathscr{U}, \Delta_{\mathscr{U}})$ et de trois morphismes de $\mathscr{O}_S$-coalgèbres $m_{\mathscr{U}} : \mathscr{U} \otimes \mathscr{U} \to \mathscr{U}$, $\eta_{\mathscr{U}} : \mathscr{O}_S \to \mathscr{U}$ et $c_{\mathscr{U}} : \mathscr{U} \to \mathscr{U}$ vérifiant les conditions (ii)*, (iii)* et (vi) ci-dessous ; d'autre part, le fait que $m_{\mathscr{U}}$ soit un morphisme de cogèbres se traduit par la commutativité des diagrammes (iv) et (v) ci-dessous : **428**

(iv)
$$\begin{array}{ccc}
\mathscr{U}\otimes\mathscr{U} & \xrightarrow{m_{\mathscr{U}}} & \mathscr{U} \\
{\scriptstyle \Delta_{\mathscr{U}}\otimes\Delta_{\mathscr{U}}}\downarrow & & \\
\mathscr{U}\otimes\mathscr{U}\otimes\mathscr{U}\otimes\mathscr{U} & & \downarrow{\scriptstyle \Delta_{\mathscr{U}}} \\
{\scriptstyle \mathrm{id}_{\mathscr{U}}\otimes\sigma\otimes\mathrm{id}_{\mathscr{U}}}\downarrow & & \\
\mathscr{U}\otimes\mathscr{U}\otimes\mathscr{U}\otimes\mathscr{U} & \xrightarrow{m_{\mathscr{U}}\otimes m_{\mathscr{U}}} & \mathscr{U}\otimes\mathscr{U}
\end{array}$$

(v)
$$\begin{array}{ccc}
\mathscr{U}\otimes\mathscr{U} & \xrightarrow{m_{\mathscr{U}}} & \mathscr{U} \\
& {\scriptstyle \varepsilon_{\mathscr{U}}\otimes\varepsilon_{\mathscr{U}}}\searrow \quad \swarrow{\scriptstyle \varepsilon_{\mathscr{U}}} & \\
& \mathscr{O}_S &
\end{array}$$

(ii)* Le carré

$$\begin{array}{ccc}
\mathscr{U}\otimes\mathscr{U}\otimes\mathscr{U} & \xrightarrow{\mathrm{id}_{\mathscr{U}}\otimes m_{\mathscr{U}}} & \mathscr{U}\otimes\mathscr{U} \\
{\scriptstyle m_{\mathscr{U}}\otimes\mathrm{id}_{\mathscr{U}}}\downarrow & & \downarrow{\scriptstyle m_{\mathscr{U}}} \\
\mathscr{U}\otimes\mathscr{U} & \xrightarrow{m_{\mathscr{U}}} & \mathscr{U}
\end{array}$$

est commutatif.

(iii)* Les deux composées ci-dessous égalent le morphisme identique de $\mathscr{U}$:

$$\mathscr{U} \simeq \mathscr{U}\otimes\mathscr{O}_S \xrightarrow{\mathrm{id}_{\mathscr{U}}\otimes\eta_{\mathscr{U}}} \mathscr{U}\otimes\mathscr{U} \xrightarrow{m_{\mathscr{U}}} \mathscr{U}$$

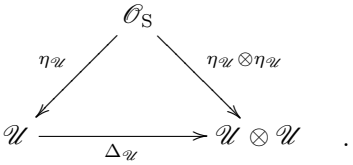
$$\mathscr{U} \simeq \mathscr{O}_S\otimes\mathscr{U} \xrightarrow{\eta_{\mathscr{U}}\otimes\mathrm{id}_{\mathscr{U}}} \mathscr{U}\otimes\mathscr{U} \xrightarrow{m_{\mathscr{U}}} \mathscr{U}.$$

(vi) Le morphisme composé ci-dessous est égal à $\eta_{\mathscr{U}} \circ \varepsilon_{\mathscr{U}}$: **429**

$$\mathscr{U} \xrightarrow{\Delta_{\mathscr{U}}} \mathscr{U}\otimes\mathscr{U} \xrightarrow{c_{\mathscr{U}}\otimes\mathrm{id}_{\mathscr{U}}} \mathscr{U}\otimes\mathscr{U} \xrightarrow{m_{\mathscr{U}}} \mathscr{U}.$$

3.2.1. — Les morphismes $\eta_{\mathscr{U}}$ et $c_{\mathscr{U}}$ sont uniquement déterminés par $m_{\mathscr{U}}$. D'autre part, les conditions (ii)* et (iii)* expriment simplement que $m_{\mathscr{U}}$ fait de $\mathscr{U}$ une $\mathscr{O}_S$-algèbre qui a pour section unité l'image par $\eta_{\mathscr{U}}$ de la section unité de $\mathscr{O}_S$. La condition (iv) exprime aussi que le morphisme diagonal $\Delta_{\mathscr{U}}$ est compatible avec la multiplication ; et en effet, $\Delta_{\mathscr{U}} : \mathscr{U} \to \mathscr{U} \otimes \mathscr{U}$ doit être un homomorphisme de coalgèbres en groupes, ce qui implique également la commutativité du triangle

(v)*



.

D'autre part, comme dans toute catégorie, l'antipodisme $c_{\mathscr{U}}$ est un isomorphisme de $\mathscr{U}$ sur l'objet en groupe « opposé » [31] ; en particulier, $c_{\mathscr{U}}$ induit un isomorphisme d'algèbres de $\mathscr{U}$ sur l'algèbre opposée $\mathscr{U}^\circ$.

3.2.2. — Comme le foncteur $\mathscr{U} \mapsto \mathrm{Spec}^*\,\mathscr{U}$ commute aux produits finis, il transforme une coalgèbre en groupes en un S-foncteur en groupes ; et en effet, pour tout S-schéma T, les éléments $x \in \Gamma(T, \mathscr{U}_T)$ appartenant à $(\mathrm{Spec}^*\,\mathscr{U})(T)$ forment un groupe pour la multiplication de l'algèbre $\Gamma(T, \mathscr{U}_T)$; l'inverse de x n'est autre que $c_{\mathscr{U}}(x)$. D'après 3.1.2.1, on a :

Scholie 3.2.2.1. — [32] Soit $\mathscr{U}$ une $\mathscr{O}_S$-coalgèbre en groupes, finie et localement libre en tant que $\mathscr{O}_S$-module. Alors le S-foncteur en groupes $\mathrm{Spec}^*\,\mathscr{U}$ est représenté par le S-groupe, fini et localement libre, $\mathrm{Spec}\,\mathscr{U}^*$.

Remarque 3.2.2.2. — Soient $\mathscr{L}$ une $\mathscr{O}_S$-algèbre de Lie et $\mathscr{U}(\mathscr{L})$ l'algèbre enveloppante de $\mathscr{L}$, c'est-à-dire le faisceau sur S associé au préfaisceau qui attribue à tout ouvert V l'algèbre enveloppante $U(\Gamma(V, \mathscr{L}))$ de l'algèbre de Lie $\Gamma(V, \mathscr{L})$.

Tout homomorphisme de $\mathscr{L}$ dans l'algèbre de Lie sous-jacente à une $\mathscr{O}_S$-algèbre associative se factorise d'une façon et d'une seule à travers le morphisme canonique
430 de $\mathscr{L}$ dans $\mathscr{U}(\mathscr{L})$; en outre, cette propriété universelle entraîne, outre la fonctorialité de $\mathscr{U}(\mathscr{L})$ en $\mathscr{L}$, que l'algèbre enveloppante d'un produit d'algèbres de Lie s'identifie au produit tensoriel des algèbres enveloppantes.

En particulier, le morphisme diagonal $\delta : \mathscr{L} \to \mathscr{L} \times \mathscr{L}$ induit un homomorphisme d'algèbres $\Delta : \mathscr{U}(\mathscr{L}) \to \mathscr{U}(\mathscr{L} \times \mathscr{L}) \simeq \mathscr{U}(\mathscr{L}) \otimes \mathscr{U}(\mathscr{L})$. Le morphisme nul $\mathscr{L} \to 0$ induit un homomorphisme $\varepsilon : \mathscr{U}(\mathscr{L}) \to \mathscr{U}(0) \simeq \mathscr{O}_S$. L'isomorphisme $x \mapsto -x$ de $\mathscr{L}$ sur l'algèbre de Lie opposée $\mathscr{L}^\circ$ induit un anti-isomorphisme c de l'algèbre $\mathscr{U}(\mathscr{L})$. On vérifie alors facilement que la multiplication m de l'algèbre $\mathscr{U}(\mathscr{L})$ fait de $(\mathscr{U}(\mathscr{L}), \Delta)$ une $\mathscr{O}_S$-coalgèbre en groupes qui a ε pour augmentation et c pour antipodisme. [33]

---

[31] N.D.E. : i.e. muni de la multiplication $m'_{\mathscr{U}} = m_{\mathscr{U}} \circ \sigma$

[32] N.D.E. : On a ajouté ce scholie, implicite dans l'original.

[33] N.D.E. : Le S-foncteur en groupes $\mathrm{Spec}^*\,\mathscr{U}(\mathscr{L})$ n'est pas représentable en général, mais on verra plus loin (5.5) que si S est un schéma de caractéristique p, si $\mathscr{L}$ est finie localement libre sur $\mathscr{O}_S$ et si $\mathscr{U}_p(\mathscr{L})$ est son *algèbre enveloppante restreinte* (cf. 5.3), alors $\mathrm{Spec}^*\,\mathscr{U}_p(\mathscr{L})$ est représenté par un S-groupe fini et localement libre.

3.2.3. — [(34)] Soit $\mathscr{U}$ une $\mathscr{O}_S$-coalgèbre en groupes. On va voir que le S-foncteur en groupes $G = \mathrm{Spec}^* \mathscr{U}$ est *très bon*, au sens de II, 4.6 et 4.10.

Soit $\mathscr{M}$ un $\mathscr{O}_S$-module libre de rang r, et soit $T \to S$ un S-schéma. Comme $I_T(\mathscr{M}) = \mathrm{Spec}(\mathscr{O}_T \oplus \mathscr{M}_T)$, de sorte que $\pi : I_T(\mathscr{M}) \to T$ est affine, on a

$$\pi_*(\mathscr{U}_{I_T(\mathscr{M})}) = \mathscr{U}_T \otimes_{\mathscr{O}_T} \pi_*(\mathscr{O}_{I_T(\mathscr{M})}) = \mathscr{U}_T \otimes_{\mathscr{O}_T} (\mathscr{O}_T \oplus \mathscr{M}_T),$$

et donc

$$\Gamma(I_T(\mathscr{M}), \mathscr{U}_{I_T(\mathscr{M})}) \simeq \Gamma(T, \mathscr{U}_T) \otimes_{\mathscr{O}(T)} \big(\mathscr{O}(T) \oplus \Gamma(T, \mathscr{M}_T)\big). \tag{1}$$

Soit $(d_1, \dots, d_r)$ une base de $\mathscr{M}$. Alors, un élément $u_0 + \sum_i u_i d_i$ de $\Gamma(I_T(\mathscr{M}), \mathscr{U}_{I_T(\mathscr{M})})$ appartient à $G(I_T(\mathscr{M}))$ si et seulement si l'on a :

$$1 = \varepsilon(u_0 + \sum_i u_i d_i) = \varepsilon(u_0) + \sum_i \varepsilon(u_i) d_i \ ,$$

et

$$(u_0 + \sum_i u_i d_i) \otimes (u_0 + \sum_i u_i d_i) = \Delta(u_0 + \sum_i u_i d_i) = \Delta(u_0) + \sum_i \Delta(u_i) d_i \ ,$$

c'est-à-dire :

$$\begin{cases} \varepsilon(u_0) = 1, & \Delta u_0 = u_0 \otimes u_0, \qquad (\text{i.e. } u_0 \in G(T)) \\ \varepsilon(u_i) = 0, & \Delta(u_i) = u_i \otimes u_0 + u_0 \otimes u_i, \ \text{ pour } i = 1, \dots, r. \end{cases} \tag{2}$$

De plus, le morphisme $G(I_T(\mathscr{M})) \to G(T)$ correspondant à la section nulle de $I_T(\mathscr{M}) \to T$ est donné par : $u_0 + \sum_i u_i d_i \mapsto u_0$. De ceci, combiné avec (1) et (2), on déduit que, si $\mathscr{N}$ est un second $\mathscr{O}_S$-module libre de rang fini, le diagramme d'ensembles

$$\begin{array}{ccc} G(I_T(\mathscr{M} \oplus \mathscr{N})) & \longrightarrow & G(I_T(\mathscr{N})) \\ \downarrow & & \downarrow \\ G(I_T(\mathscr{M})) & \longrightarrow & G(T) \end{array}$$

est cartésien, i.e. G vérifie la condition (E) de II, 3.5.

Notons $\mathrm{Prim}\,\Gamma(T, \mathscr{U}_T)$ le sous-$\mathscr{O}(T)$-module de $\Gamma(T, \mathscr{U}_T)$ formé des *éléments primitifs*, c.-à-d., des éléments u qui vérifient (avec l'abus de notation signalé en 3.1.2) :

$$\Delta u = u \otimes 1 + 1 \otimes u, \qquad \varepsilon(u) = 0. \qquad [(35)]$$

Comme $(\underline{\mathrm{Lie}}\, G)(T)$ est l'ensemble des éléments de $u_0 + ud \in G(I_T)$ au-dessus de l'élément unité $u_0 = 1$ de $G(T)$, on obtient un isomorphisme de $\mathscr{O}(T)$-modules, fonctoriel en T : [(36)]

$$(\underline{\mathrm{Lie}}\, G)(T) \simeq \mathrm{Prim}\,\Gamma(T, \mathscr{U}_T).$$

D'autre part, on déduit de (1) que

$$\mathrm{Prim}\,\Gamma(I_T(\mathscr{M}), \mathscr{U}_{I_T(\mathscr{M})}) \simeq \mathrm{Prim}\,\Gamma(T, \mathscr{U}_T) \otimes_{\mathscr{O}(T)} \mathscr{O}(I_T(\mathscr{M})),$$

[(34)] N.D.E. : On a détaillé ce paragraphe.

[(35)] N.D.E. : Notons que la seconde condition est conséquence de la première, car celle-ci entraîne que $u = (\mathrm{id} \otimes \varepsilon)\Delta(u) = u + \varepsilon(u)$, d'où $\varepsilon(u) = 0$.

[(36)] N.D.E. : La structure de $\mathbf{O}_S$-module sur $\underline{\mathrm{Lie}}\, G$ est définie dans II, Prop. 3.6.

et il en résulte que le morphisme naturel de $\mathscr{O}(\mathrm{I_T}(\mathscr{M}))$-modules :

$$(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T}) \otimes_{\mathscr{O}(\mathrm{T})} \mathscr{O}(\mathrm{I_T}(\mathscr{M})) \longrightarrow (\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{I_T}(\mathscr{M}))$$

est un isomorphisme, i.e. $\underline{\mathrm{Lie}}\,\mathrm{G}$ est un bon $\mathbf{O}_\mathrm{S}$-module (cf. II, Déf. 4.4).

Donc G est un bon S-foncteur en groupes (cf. II, Déf. 4.6), et d'après II, 4.7.2, $\underline{\mathrm{Lie}}\,\mathrm{G}$ est muni d'un « crochet de Lie » $\mathbf{O}_\mathrm{S}$-bilinéaire et vérifiant l'identité de Jacobi. Reste à montrer que G est très bon, i.e. que le « crochet » sur $(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$ vérifie bien $[u,u]=0$ pour tout $u \in (\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$ (cf. II, 4.10).

Soient u, v deux éléments de $(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$, c.-à-d., deux éléments primitifs de $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$. Posons $\mathrm{I} = \mathrm{Spec}\,\mathscr{O}_\mathrm{S}[d]/(d^2)$ et $\mathrm{I}' = \mathrm{Spec}\,\mathscr{O}_\mathrm{S}[d']/(d'^2)$. Comme la loi de composition de $\mathrm{G}(\mathrm{I}\times\mathrm{I}')$ est induite par la multiplication de l'algèbre $\mathscr{U}_{\mathrm{I}\times\mathrm{I}'}$, on a dans $\mathrm{G}(\mathrm{I}\times\mathrm{I}')$ l'égalité :

$$\begin{aligned}(1+ud)(1+vd')(1+ud)^{-1}(1+vd')^{-1} &= (1+ud)(1+vd')(1-ud)(1-vd)\\ &= 1+(uv-vu)dd'\end{aligned}$$

431 D'après la description du crochet $[u,v]$ donnée avant la Prop. 4.8 de l'Exp. II, on obtient que

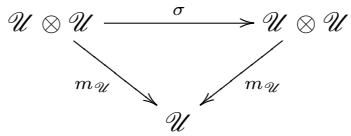
$$[u,v] = uv - vu,$$

où le terme de droite est le commutateur de u et v dans l'algèbre $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$, d'où $[u,u]=0$. On a donc obtenu la proposition suivante : [37]

Proposition. — *Soit $\mathscr{U}$ une $\mathscr{O}_\mathrm{S}$-coalgèbre en groupes. Le* S*-foncteur en groupes* $\mathrm{G} = \mathrm{Spec}^*\,\mathscr{U}$ *est très bon, et l'on a un isomorphisme* $\underline{\mathrm{Lie}}\,\mathrm{G} \simeq \mathrm{Prim}\,\mathbf{W}(\mathscr{U})$ *de* $\mathbf{O}_\mathrm{S}$*-algèbres de Lie, où* $\mathrm{Prim}\,\mathbf{W}(\mathscr{U})$ *désigne le foncteur qui à tout* $\mathrm{T}\to\mathrm{S}$ *associe la* $\mathscr{O}(\mathrm{T})$*-algèbre de Lie formée des éléments primitifs de* $\mathbf{W}(\mathscr{U})(\mathrm{T}) = \Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$.

3.3. Supposons enfin que $\mathscr{U}$ soit une $\mathscr{O}_\mathrm{S}$*-coalgèbre en groupes commutatifs*, c'est-à-dire que le triangle

(i)*



soit commutatif, ou encore que $m_\mathscr{U}$ fasse de $\mathscr{U}$ une $\mathscr{O}_\mathrm{S}$-algèbre commutative. Les conditions (i), (ii), (iii), (iv), (v), (vi), (i)*, (ii)*, (iii)* et (v)* signifient alors aussi que $\mathscr{U}$ est un cogroupe dans la catégorie des $\mathscr{O}_\mathrm{S}$-algèbres commutatives. Donc, si de plus $\mathscr{U}$ est un $\mathscr{O}_\mathrm{S}$-module *quasi-cohérent*, alors le S-schéma affine $\mathrm{Spec}\,\mathscr{U}$ est un S-schéma en groupes commutatifs.

Dans ce cas, puisque le morphisme diagonal Δ' de $\mathscr{O}_\mathrm{S}[\mathrm{T},\mathrm{T}^{-1}]$ envoie T sur $\mathrm{T}\otimes\mathrm{T}$, les morphismes de S-groupes de $\mathrm{Spec}\,\mathscr{U}$ dans $\mathbb{G}_{m,\mathrm{S}}$ (I 4.3.2) correspondent bijectivement aux morphismes de $\mathscr{O}_\mathrm{S}$-algèbres unitaires

$$\varphi : \mathscr{O}_\mathrm{S}[\mathrm{T},\mathrm{T}^{-1}] \longrightarrow \mathscr{U}$$

[37] N.D.E. : On a ajouté cette proposition, qui résume la discussion précédente.

tels que $(\varphi \otimes \varphi) \circ \Delta' = \Delta_{\mathscr{U}} \circ \varphi$ (dans ce cas, $\varepsilon_{\mathscr{U}} \circ \varphi$ est l'élément neutre de $\mathbb{G}_{m,\mathrm{S}}(\mathrm{S})$, i.e. l'augmentation ε'). Un tel morphisme φ est déterminé par l'image $\varphi(\mathrm{T})$, qui doit être un élément inversible x de $\mathscr{U}$ vérifiant $\Delta_{\mathscr{U}} x = x \otimes x$ et $\varepsilon_{\mathscr{U}}(x) = \varepsilon'(\mathrm{T}) = 1$. On a donc :

$$\mathrm{Hom}_{\text{S-gr.}}(\mathrm{Spec}\,\mathscr{U}, \mathbb{G}_{m,\mathrm{S}}) \simeq (\mathrm{Spec}^*\,\mathscr{U})(\mathrm{S})$$

et comme cette formule reste valable après tout changement de base, ceci donne : **432**

$$\mathrm{Spec}^*\,\mathscr{U} \simeq \underline{\mathrm{Hom}}_{\text{S-gr.}}(\mathrm{Spec}\,\mathscr{U}, \mathbb{G}_{m,\mathrm{S}}).$$

On a donc obtenu la

Proposition 3.3.0. — *Si $\mathscr{U}$ est une $\mathscr{O}_{\mathrm{S}}$-coalgèbre en groupes* commutatifs, quasi-cohérente *comme $\mathscr{O}_{\mathrm{S}}$-module, alors le* S-*schéma affine* $\mathrm{G} = \mathrm{Spec}\,\mathscr{U}$ *est un* S-*schéma en groupes commutatifs, et l'on a un isomorphisme de* S-*foncteurs en groupes* $\mathrm{Spec}^*\,\mathscr{U} \simeq \underline{\mathrm{Hom}}_{\text{S-gr.}}(\mathrm{G}, \mathbb{G}_{m,\mathrm{S}})$.

Si l'on suppose de plus que $\mathscr{U}$ est un $\mathscr{O}_{\mathrm{S}}$-module localement libre de type fini alors, d'après 3.1.2.1, le S-foncteur en groupes $\mathrm{Spec}^*\,\mathscr{U}$ est représenté par $\mathrm{Spec}\,\mathscr{U}^*$. On obtient donc la

Proposition 3.3.1 (Dualité de Cartier). — *Le foncteur*

$$\mathscr{A}(\mathrm{G}) \mapsto \mathscr{A}(\mathrm{G})^* = \mathscr{H}om_{\mathscr{O}_{\mathrm{S}}\text{-Mod.}}(\mathscr{A}(\mathrm{G}), \mathscr{O}_{\mathrm{S}})$$

induit une dualité (*) *de la catégorie des* S-*schémas en groupes commutatifs, finis et localement libres ; elle associe à* G *le* S-*groupe* $\underline{\mathrm{Hom}}_{\text{S-gr.}}(\mathrm{G}, \mathbb{G}_{m,\mathrm{S}})$.

4. « Frobeniuseries »

433

Soient p un nombre premier fixé et $(\mathbf{Sch}_{/\mathbb{F}_p})$ la catégorie des schémas de caractéristique p, c'est-à-dire des schémas au-dessus du corps premier $\mathbb{F}_p$. Suivant les conventions générales de ce séminaire, nous identifions $(\mathbf{Sch}_{/\mathbb{F}_p})$ à une sous-catégorie de $\widehat{(\mathbf{Sch}_{/\mathbb{F}_p})}$ au moyen du foncteur $\mathbf{h}$ de I 1.1. Nous profitons de même de l'isomorphisme de $\mathrm{Hom}(\mathbf{h}_{\mathrm{X}}, \mathrm{F})$ sur $\mathrm{F}(\mathrm{X})$ défini en I 1.1 pour identifier ces deux ensembles chaque fois que X est un $\mathbb{F}_p$-schéma et F un objet de $\widehat{(\mathbf{Sch}_{/\mathbb{F}_p})}$.

Notations 4.0. — (39) Si T est un $\mathbb{F}_p$-schéma, un T-foncteur est un morphisme $q : \mathrm{F} \to \mathrm{T}$ de $\widehat{(\mathbf{Sch}_{/\mathbb{F}_p})}$ qui a T pour but ; pour tout T-schéma $r : \mathrm{X} \to \mathrm{T}$, l'ensemble des T-morphismes $\mathrm{X} \to \mathrm{F}$, i.e. des $\mathbb{F}_p$-morphismes $s : \mathrm{X} \to \mathrm{F}$ tels que $q \circ s = r$, sera alors noté $q(r)$, $q(\mathrm{X/T})$, $\mathrm{F}(r)$ ou $\mathrm{F}(\mathrm{X/T})$ (ou même $\mathrm{F}(\mathrm{X})$ lorsqu'aucune confusion ne sera possible avec $\mathrm{Hom}(\mathbf{h}_{\mathrm{X}}, \mathrm{F})$).

(*) Une dualité d'une catégorie $\mathscr{C}$ est un couple (D, φ) formé d'un foncteur contravariant D de $\mathscr{C}$ dans $\mathscr{C}$ et d'un isomorphisme fonctoriel $\varphi : \mathrm{Id}_{\mathscr{C}} \to \mathrm{DD}$ tel que les isomorphismes $\varphi\mathrm{D} : \mathrm{D} \to \mathrm{DDD}$ et $\mathrm{D}\varphi^{-1} : \mathrm{DDD} \to \mathrm{D}$ soient réciproques l'un de l'autre. (38)

(38) N.D.E. : On a corrigé $\mathrm{D}\varphi$ en $\mathrm{D}\varphi^{-1}$.

(39) N.D.E. : On a ajouté la numérotation 4.0, pour références ultérieures.

4.1. Pour tout schéma S de caractéristique p, nous notons fr(S), ou simplement fr, l'endomorphisme de S qui induit l'identité sur l'espace topologique sous-jacent à S et qui associe x^p à une section x de $\mathscr{O}_S$ sur un ouvert U.

Alors l'application fr : S $\mapsto$ fr(S) est un *endomorphisme du foncteur identique* de $(\mathbf{Sch}_{/\mathbb{F}_p})$, [40] ce qui implique les résultats suivants. Soit E un $\mathbb{F}_p$-foncteur, c'est-à-dire un objet de $(\widehat{\mathbf{Sch}_{/\mathbb{F}_p}})$; l'application qui associe à tout $\mathbb{F}_p$-schéma S l'endomorphisme E(fr(S)) de E(S), est un endomorphisme fonctoriel de E que nous noterons fr(E) ou fr ; cette notation est compatible avec l'identification de $(\mathbf{Sch}_{/\mathbb{F}_p})$ à une sous-catégorie de $(\widehat{\mathbf{Sch}_{/\mathbb{F}_p}})$. De plus, l'application E $\mapsto$ fr(E) est un *endomorphisme du foncteur identique* de $(\widehat{\mathbf{Sch}_{/\mathbb{F}_p}})$ (que nous noterons encore fr). [41]

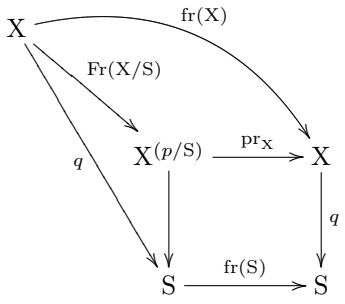
Pour tout $\mathbb{F}_p$-schéma S et tout S-foncteur q : X $\to$ S, nous notons $X^{(p/S)}$ ou $X^{(p)}$ l'image réciproque de X par le changement de base fr(S) :

$$\begin{array}{ccc} X^{(p/S)} & \xrightarrow{pr_X} & X \\ \downarrow & & \downarrow q \\ S & \xrightarrow{fr(S)} & S \end{array} .$$

Le carré commutatif

$$\begin{array}{ccc} X & \xrightarrow{fr(X)} & X \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q} \\ S & \xrightarrow{fr(S)} & S \end{array}$$

434 induit alors un S-morphisme noté Fr(X/S) (ou simplement Fr) de X dans $X^{(p/S)}$ tel que fr(X) = $pr_X \circ Fr(X/S)$:



[40] N.D.E. : i.e. pour tout morphisme de $\mathbb{F}_p$-schémas f : Y $\to$ X, le diagramme ci-dessous est commutatif :

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ {\scriptstyle fr(Y)}\downarrow & & \downarrow{\scriptstyle fr(X)} \\ Y & \xrightarrow{f} & X. \end{array}$$

[41] N.D.E. : On dit que fr(X) est le morphisme de Frobenius « absolu » de X, pour le distinguer du morphisme de Frobenius « relatif » Fr(X/S) introduit plus bas.

Nous dirons que $\mathrm{Fr}(X/S)$ est *le morphisme de Frobenius de* X *relativement à* S ; il est clair que l'application $\mathrm{Fr} : X \mapsto \mathrm{Fr}(X/S)$ est un homomorphisme fonctoriel.

(42) Soit $r : T \to S$ un S-schéma. Pour tout $\phi \in X(r) = \mathrm{Hom}_S(T, X)$ (cf. 4.0), on a un diagramme commutatif :

$$\begin{array}{ccccc} X & \xrightarrow{\mathrm{Fr}(X/S)} & X^{(p/S)} & \xrightarrow{\mathrm{pr}_X} & X \\ {\scriptstyle\phi}\uparrow & \searrow^{q} & \downarrow{\scriptstyle q^{(p/S)}} & & \downarrow{\scriptstyle q} \\ T & \xrightarrow{r} & S & \xrightarrow{\mathrm{fr}(S)} & S \end{array} .$$

D'après la définition de $X^{(p/S)}$ comme produit fibré, pr_X induit une bijection :

$$X^{(p/S)}(r) = \mathrm{Hom}_S(T, X^{(p/S)}) \xrightarrow{\sim} \mathrm{Hom}_S(T, X) = X(\mathrm{fr}(S) \circ r).$$

D'autre part, $r \circ \mathrm{fr}(T) = \mathrm{fr}(S) \circ r$, puisque fr est un endomorphisme du foncteur identique. Il en résulte que l'application $\mathrm{Fr}(X/S)(r) : X(r) \to X^{(p/S)}(r)$ peut être caractérisée par la commutativité du carré suivant :

$$(\dagger) \qquad \begin{array}{ccc} X(r) & \xrightarrow{\mathrm{Fr}(X/S)(r)} & X^{(p/S)}(r) \\ {\scriptstyle X(\mathrm{fr}(T))}\downarrow & & \downarrow\wr \\ X(r \circ \mathrm{fr}(T)) & = & X(\mathrm{fr}(S) \circ r). \end{array}$$

Par exemple, si X est le sous-schéma de S défini par un idéal quasi-cohérent $\mathscr{I}$, alors $X^{(p)}$ est le sous-schéma de S défini par l'idéal $\mathscr{I}^{\{p\}}$ engendré par les puissances p-ièmes des sections de $\mathscr{I}$; en outre, $\mathrm{Fr}(X/S)$ est alors l'immersion canonique de $\mathrm{Spec}(\mathscr{O}_X/\mathscr{I})$ dans $\mathrm{Spec}(\mathscr{O}/\mathscr{I}^{\{p\}})$.

4.1.1. — (43) Soient $t : T \to S$ un changement de base et $X_T = X \underset{q,t}{\times} T$. Considérons l'image réciproque de X_T par $\mathrm{fr}(T)$:

$$\begin{array}{ccccc} (X_T)^{(p/T)} & \longrightarrow & X_T & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle q} \\ T & \xrightarrow{\mathrm{fr}(T)} & T & \xrightarrow{t} & S \end{array} .$$

Comme $t \circ \mathrm{fr}(T) = \mathrm{fr}(S) \circ t$, alors $(X_T)^{(p/T)}$ s'identifie à l'image réciproque de $X^{(p/S)}$ **435** par t ; autrement dit, on a un isomorphisme canonique :

$$X_T^{(p/T)} \xrightarrow{\sim} (X^{(p/S)})_T .$$

Il est clair que, dans cette identification, $\mathrm{Fr}(X_T/T)$ s'identifie à l'image réciproque $\mathrm{Fr}(X/S)_T$ de $\mathrm{Fr}(X/S)$.

(42) N.D.E. : On a détaillé l'original dans ce qui suit.
(43) N.D.E. : On a détaillé l'original dans ce qui suit.

4.1.1.1. — En particulier, si S est le spectre du corps premier $\mathbb{F}_p$, $X^{(p/S)}$ est égal à X et $\mathrm{Fr}(X/S)$ à $\mathrm{fr}(X)$. Par conséquent, $X_T^{(p/T)}$ s'identifie à X_T et $\mathrm{Fr}(X_T/T)$ à $\mathrm{fr}(X)_T$.

Par exemple, si E est un ensemble et E_T le T-schéma constant de type E, on a $E_T^{(p/T)} \simeq E_T$ et $\mathrm{Fr}(E_T/T) \simeq \mathrm{id}_{E_T}$.

4.1.2. — Le foncteur $X \mapsto X^{(p/S)}$ commute évidemment aux produits ; il transforme donc un S-groupe G en un S-groupe $G^{(p/S)}$; de plus, comme Fr est un homomorphisme fonctoriel, alors

$$\mathrm{Fr}(G/S) : \quad G \longrightarrow G^{(p/S)}$$

est un homomorphisme de S-groupes. Nous noterons ${}_{\mathrm{Fr}}G$ son noyau.

Si $r : T \to S$ est un schéma au-dessus de S, il résulte du diagramme (†) de 4.1 que la valeur de ${}_{\mathrm{Fr}}G$ en r est le noyau de l'homomorphisme

$$G(\mathrm{fr}(T)) : \ G(r) \longrightarrow G(r \circ \mathrm{fr}(T)).$$

Or, lorsque T est le schéma I_R des nombres duaux sur un S-schéma R, $\mathrm{fr}(I_R)$ se factorise comme suit :

$$I_R \xrightarrow{\text{can.}} R \xrightarrow{\mathrm{fr}(R)} R \xrightarrow{s} I_R,$$

où s est la section nulle. Il en résulte que $({}_{\mathrm{Fr}}G)(I_R)$ contient le noyau $\underline{\mathrm{Lie}}(G/S)(R)$ du morphisme $G(s) : G(I_R) \to G(R)$, et qu'on a donc : $\underline{\mathrm{Lie}}(G/S) = \underline{\mathrm{Lie}}({}_{\mathrm{Fr}}G/S)$.

4.1.3. — Plus généralement, pour tout S-foncteur X, nous définissons le S-foncteur $X^{(p^n)}$ par récurrence sur n à l'aide des formules :

$$X^{(p)} = X^{(p/S)} \qquad \text{et} \qquad X^{(p^n)} = (X^{(p^{n-1})})^{(p)}.$$

436 De même, $\mathrm{Fr}^n(X/S)$ ou Fr^n désignent l'homomorphisme fonctoriel composé

$$X \xrightarrow{\mathrm{Fr}(X/S)} X^{(p)} \xrightarrow{\mathrm{Fr}(X^{(p)}/S)} X^{(p^2)} \longrightarrow \cdots \longrightarrow X^{(p^{n-1})} \xrightarrow{\mathrm{Fr}(X^{(p^{n-1})}/S)} X^{(p^n)}.$$

On notera que, d'après 4.1.1, $\mathrm{Fr}(X^{(p)}/S)$ coïncide avec $\mathrm{Fr}(X/S)^{(p)}$, i.e. le diagramme suivant est commutatif :

$$\begin{array}{ccc} X^{(p)} & \longrightarrow & X \\ \downarrow{\scriptstyle \mathrm{Fr}(X^{(p)}/S)} & & \downarrow{\scriptstyle \mathrm{Fr}(X/S)} \\ X^{(p^2)} & \longrightarrow & X^{(p)} \end{array} .$$

Si G est un S-foncteur en groupes, $G^{(p^n)}$ en est un également et $\mathrm{Fr}^n(G/S)$ est un homomorphisme de S-foncteurs en groupes.

Définition. — Nous noterons ${}_{\mathrm{Fr}^n}G$ le noyau de $\mathrm{Fr}^n(G/S)$ et nous dirons que G *est de hauteur* $\leqslant n$ si $\mathrm{Fr}^n(G/S)$ est nul, c'est-à-dire si ${}_{\mathrm{Fr}^n}G = G$.

Lemme. — *Le sous-foncteur en groupes* ${}_{\mathrm{Fr}^n}G$ *de* G *est* caractéristique*, c.-à-d., pour tout* S*-schéma* T*, tout endomorphisme* ϕ *du* T*-foncteur en groupes* G_T *induit un endomorphisme de* $({}_{\mathrm{Fr}^n}G)_T$.

En effet, comme la construction de $G^{(p^n)}$ et de $\mathrm{Fr}^n(G/S)$ commute aux changements de base d'après 4.1.1, on peut supposer $T = S$; dans ce cas, l'assertion résulte de ce que $\mathrm{Fr}^n(G/S)$ est un homomorphisme fonctoriel.

4.1.4. — Voici quelques exemples.

a) Considérons d'abord un groupe abélien « abstrait » M et le groupe diagonalisable $G = D_S(M)$ de type M (I 4.4) : pour tout S-schéma T, G(T) est donc le groupe abélien $\mathrm{Hom}_{(\mathrm{Ab})}(M, \Gamma(T, \mathscr{O}_T)^\times)$. Comme G est l'image réciproque du groupe diagonalisable D(M) sur $\mathbb{F}_p$, $G^{(p)}$ s'identifie à G et $\mathrm{Fr}(G/S)(T)$ s'identifie à l'endomorphisme $x \mapsto x^p$ de G(T) (4.1.1). En particulier, lorsque M est égal à $\mathbb{Z}$, on a $D_S(M) = \mathbb{G}_{m,S}$, de sorte que :

> *$\mathrm{Fr}\mathbb{G}_{m,S}$ est le* S*-groupe $\boldsymbol{\mu}_{p,S}$ qui associe à tout* S*-schéma* T *le groupe des racines p-ièmes de l'unité dans* $\Gamma(T, \mathscr{O}_T)^*$.

b) Considérons maintenant un schéma S de caractéristique p et un faisceau de modules $\mathscr{E}$ sur S. D'après I 4.6.2, on a un isomorphisme canonique

$$\mathbf{W}(\mathscr{E})^{(p)} \simeq \mathbf{W}(\mathscr{E}^{(p)}),$$

où $\mathscr{E}^{(p)}$ est l'image réciproque de $\mathscr{E}$ par fr(S). Pour tout S-schéma $\pi : T \to S$ l'appli- **437**
cation $\mathrm{Fr}(\mathbf{W}(\mathscr{E}))(\pi)$ est déterminée, d'après 4.1 (†), par le triangle commutatif

$$\begin{array}{ccc} \Gamma(T, \pi^* \mathrm{fr}(S)^* \mathscr{E}) & \xrightarrow[\text{can.}]{\sim} & \Gamma(T, \mathrm{fr}(T)^* \pi^* \mathscr{E}) \\ & {\scriptstyle \mathrm{Fr}(\mathbf{W}(\mathscr{E})/S)(\pi)} \nwarrow \quad \nearrow {\scriptstyle f'} & \\ & \Gamma(T, \pi^* \mathscr{E}) & \end{array} ,$$

où f' est l'application induite par fr(T).

En particulier, si $\mathscr{E}$ est égal à $\mathscr{O}_S$, $\mathbf{W}(\mathscr{E})$ s'identifie au groupe additif $\mathbb{G}_{a,S}$. Dans ce cas, on a $\mathscr{E}^{(p)} = \mathscr{E} = \mathscr{O}_S$ et le morphisme de Frobenius $\mathrm{Fr}(\mathbb{G}_{a,S}/S)$ applique $x \in \Gamma(T, \mathscr{O}_T)$ sur x^p. Donc :

> *$\mathrm{Fr}\mathbb{G}_{a,S}$ est le* S*-groupe $\boldsymbol{\alpha}_{p,S}$ qui associe à tout* S*-schéma* T *le groupe :* $\{x \in \Gamma(T, \mathscr{O}_T) \mid x^p = 0\}$.

c) On verrait de même que, pour toute $\mathscr{O}_S$-algèbre quasi-cohérente $\mathscr{A}$, $(\mathrm{Spec}\,\mathscr{A})^{(p)}$ s'identifie au spectre $\mathrm{Spec}\,\mathscr{A}^{(p)}$ de l'image réciproque de $\mathscr{A}$ par fr(S). Si π désigne l'endomorphisme $x \mapsto x^p$ du faisceau d'anneaux $\mathscr{O}_S$, on a donc

$$\mathscr{A}^{(p)} = \mathscr{A} \otimes_\pi \mathscr{O}_S \qquad (44)$$

et $\mathrm{Fr}((\mathrm{Spec}\,\mathscr{A})/S)$ est induit par le morphisme de $\mathscr{O}_S$-algèbres $\mathscr{A} \otimes_\pi \mathscr{O}_S \to \mathscr{A}$ défini par $a \otimes_\pi x \mapsto a^p x$.

(44) N.D.E. : $\mathscr{A} \otimes_\pi \mathscr{O}_S$ désigne la $\mathscr{O}_S$-algèbre obtenue par l'extension des scalaires $\pi : \mathscr{O}_S \to \mathscr{O}_S$, i.e. on a : $ax \otimes_\pi 1 = a \otimes_\pi x^p$, et $x \cdot (a \otimes_\pi 1) = a \otimes_\pi x$.

Pour tout $\mathscr{O}_S$-module quasi-cohérent $\mathscr{E}$ enfin, on a des isomorphismes canoniques

$$\mathbb{V}(\mathscr{E})^{(p)} \simeq \mathbb{V}(\mathscr{E}^{(p)}) \qquad \text{et} \qquad \mathcal{S}(\mathscr{E})^{(p)} \simeq \mathcal{S}(\mathscr{E}^{(p)}),$$

où $\mathcal{S}(\mathscr{E})$ désigne l'algèbre symétrique du $\mathscr{O}_S$-module $\mathscr{E}$.

438 **d)** Soient $\mathscr{U}$ une $\mathscr{O}_S$-coalgèbre (3.1) et T un schéma de caractéristique p. Si $\mathscr{U}^{(p/S)}$ ou $\mathscr{U}^{(p)}$ désignent l'image réciproque de la coalgèbre $\mathscr{U}$ par fr(S), on a comme en b) un isomorphisme canonique :

$$(\mathrm{Spec}^*\,\mathscr{U})^{(p)} \simeq \mathrm{Spec}^*\,\mathscr{U}^{(p)}.$$

Si $\mathscr{U}$ est une coalgèbre en groupes, la valeur de ${}_{\mathrm{Fr}}(\mathrm{Spec}^*\,\mathscr{U})$, i.e. du noyau du morphisme de Frobenius $\mathrm{Spec}^*\,\mathscr{U} \to (\mathrm{Spec}^*\,\mathscr{U})^{(p)}$, pour un S-schéma T est donc l'ensemble des éléments γ de

$$(\mathrm{Spec}^*\,\mathscr{U})(\mathrm{T}) = \{x \in \Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T}) \mid \varepsilon_{\mathscr{U}_\mathrm{T}}(x) = 1, \quad \Delta_{\mathscr{U}_\mathrm{T}} x = x \otimes x\}$$

tels que l'image dans $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T} \otimes_{\mathrm{fr}(\mathrm{T})} \mathscr{O}_\mathrm{T})$ de l'élément $\gamma \otimes_{\mathrm{fr}(\mathrm{T})} 1$ de $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T}) \otimes_{\mathrm{fr}(\mathrm{T})} \mathscr{O}(\mathrm{T})$ soit égale à 1.

4.2. [45] Nous allons maintenant nous occuper d'une construction voisine de la précédente : soient S un schéma de caractéristique p, X un S-schéma et X_S^p le produit dans la catégorie $(\mathbf{Sch}_{/\mathrm{S}})$ de p exemplaires de X.

Nous désignons alors par $\mathrm{U}^p(\mathrm{X})$ le sous-schéma ouvert de X_S^p qui est la réunion des produits U_S^p, lorsque U parcourt les ouverts affines de X. Un point x de X_S^p appartient donc à $\mathrm{U}^p(\mathrm{X})$ si et seulement si les projections $\mathrm{pr}_i\, x$ de x sur les facteurs de X_S^p appartiennent à un même ouvert affine de X. Par exemple, si toute partie finie de X est contenue dans un ouvert affine, on a $\mathrm{U}^p(\mathrm{X}) = \mathrm{X}_\mathrm{S}^p$.

Le groupe symétrique $\mathscr{S}_p$ d'ordre p opère sur X_S^p par permutation des facteurs et laisse stable l'ouvert $\mathrm{U}^p(\mathrm{X})$. Nous appellerons *produit symétrique p-uple de* X et nous noterons $\Sigma^p\mathrm{X}$ le quotient de X_S^p par $\mathscr{S}_p$ dans la catégorie des espaces annelés. Soit $q(\mathrm{X})$, ou simplement q, la projection canonique $\mathrm{X}_\mathrm{S}^p \to \Sigma^p\mathrm{X}$

Alors, q applique $\mathrm{U}^p(\mathrm{X})$ sur un ouvert $\mathrm{V}^p(\mathrm{X})$ du produit symétrique, qu'on peut décrire comme suit (cf. V 4.1). Le faisceau structural de $\Sigma^p\mathrm{X}$ induit sur $\mathrm{V}^p(\mathrm{X})$ une structure de schéma ; le morphisme $q'(\mathrm{X}) : \mathrm{U}^p(\mathrm{X}) \to \mathrm{V}^p(\mathrm{X})$ induit par $q(\mathrm{X})$ est affine et même entier ; lorsque U parcourt les ouverts affines de X qui se projettent dans un
439 ouvert affine variable V de S, les $\Sigma^p\mathrm{U}$ forment un recouvrement affine de $\mathrm{V}^p(\mathrm{X})$; si R désigne l'algèbre affine de V et A celle de U, $\Sigma^p\mathrm{U}$ a pour algèbre affine la sous-algèbre $\Sigma^p\mathrm{A}$ de $\bigotimes_\mathrm{R}^p \mathrm{A}$ formée des tenseurs symétriques.

Considérons maintenant le morphisme diagonal δ de X dans $\mathrm{U}^p(\mathrm{X})$. Si $\mathrm{V} = \mathrm{Spec}\,\mathrm{R}$ est un ouvert affine de S et $\mathrm{U} = \mathrm{Spec}\,\mathrm{A}$ un ouvert affine de X au-dessus de V, la restriction de δ à U est définie par le morphisme d'algèbres

$$\eta : \bigotimes_\mathrm{R}^p \mathrm{A} \longrightarrow \mathrm{A}, \qquad a_1 \otimes \cdots \otimes a_p \mapsto a_1 a_2 \cdots a_p.$$

[45] N.D.E. : Pour le contenu des n$^{\mathrm{os}}$ 4.2 et 4.3, on peut aussi se reporter à [**DG70**], § IV.3, n$^{\mathrm{os}}$ 4–6.

On a donc, si N est l'opérateur de symétrisation :

$$\eta\big(\mathrm{N}(a_1 \otimes \cdots \otimes a_p)\big) = \eta\Big(\sum_{\sigma \in \mathscr{S}_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}\Big) = p!\, a_1 \cdots a_p = 0.$$

Autrement dit, η s'annule sur le sous-espace $\mathrm{N}(\bigotimes^p_{\mathrm{R}} \mathrm{A})$ de $\Sigma^p\mathrm{A}$ formé des tenseurs symétrisés. De plus, si f est un tenseur symétrique, on a évidemment $\mathrm{N}(fa) = f\mathrm{N}(a)$, ce qui montre que $\mathrm{N}(\bigotimes^p_{\mathrm{R}} \mathrm{A})$ est un idéal de $\Sigma^p\mathrm{A}$. Nous noterons désormais

$$\mathrm{U}^{[p/\mathrm{S}]} = \mathrm{Spec}\,\Big(\Sigma^p\mathrm{A}/\mathrm{N}(\textstyle\bigotimes^p_{\mathrm{R}} \mathrm{A})\Big);$$

c'est un sous-schéma fermé de $\Sigma^p(\mathrm{U}) = \mathrm{V}^p(\mathrm{U})$. La réunion des $\mathrm{U}^{[p/\mathrm{S}]}$, lorsque U parcourt les ouverts affines de X qui se projettent dans un ouvert affine variable V de S, est un sous-schéma fermé de $\mathrm{V}^p(\mathrm{X})$, noté $\mathrm{X}^{[p/\mathrm{S}]}$.

De plus, si $i(\mathrm{X})$ désigne l'inclusion de $\mathrm{X}^{[p/\mathrm{S}]}$ dans $\mathrm{V}^p(\mathrm{X})$, nous venons de voir que $q'(\mathrm{X}) \circ \delta$ se factorise à travers $\mathrm{X}^{[p/\mathrm{S}]}$, d'où un morphisme $\mathrm{F}^{[p]}(\mathrm{X/S}) : \mathrm{X} \to \mathrm{X}^{[p/\mathrm{S}]}$: (46)

$$\begin{array}{ccccc}
\mathrm{X}^p_{\mathrm{S}} & \supset & \mathrm{U}^p(\mathrm{X}) & \xleftarrow{\delta(\mathrm{X})} & \mathrm{X} \\
\Big\downarrow{\scriptstyle q(\mathrm{X})} & & \Big\downarrow{\scriptstyle q'(\mathrm{X})} & & \Big\downarrow{\scriptstyle \mathrm{F}^{[p]}(\mathrm{X/S})} \\
\Sigma^p(\mathrm{X}) & \supset & \mathrm{V}^p(\mathrm{X}) & \xleftarrow{i(\mathrm{X})} & \mathrm{X}^{[p/\mathrm{S}]}
\end{array} .$$

Il est clair que $\mathrm{X}^{[p/\mathrm{S}]}$ est fonctoriel en X et que l'application $\mathrm{F}^{[p]} : \mathrm{X} \mapsto \mathrm{F}^{[p]}(\mathrm{X/S})$ est un homomorphisme fonctoriel.

4.2.1. — Les schémas $\mathrm{X}^{[p/\mathrm{S}]}$ et $\mathrm{X}^{(p/\mathrm{S})}$ sont évidemment reliés : soient V un ouvert affine de S d'anneau affine R et U un ouvert affine de X au-dessus de V ; soit A **440**
l'algèbre affine de U. Si π désigne l'endomorphisme $x \mapsto x^p$ de R, alors $\mathrm{U}^{(p/\mathrm{S})}$ a $\mathrm{A} \otimes_\pi \mathrm{R}$ pour algèbre affine. On vérifie en outre que l'application

$$a \otimes_\pi \lambda \mapsto \Big(\lambda a \otimes \cdots \otimes a \qquad \mathrm{mod}\ \mathrm{N}(\textstyle\bigotimes^p_{\mathrm{R}} \mathrm{A})\Big)$$

définit un morphisme de R-algèbres de $\mathrm{A} \otimes_\pi \mathrm{R}$ dans $\Sigma^p\mathrm{A}/\mathrm{N}(\bigotimes^p_{\mathrm{R}} \mathrm{A})$, et celui-ci induit un morphisme $\varphi(\mathrm{U}) : \mathrm{U}^{[p/\mathrm{S}]} \to \mathrm{U}^{(p/\mathrm{S})}$ tel que $\varphi(\mathrm{U}) \circ \mathrm{F}^{[p]}(\mathrm{U/S}) = \mathrm{Fr}(\mathrm{U/S})$.

« Recollant les morceaux », on obtient alors un triangle commutatif

$$\begin{array}{ccc}
 & \mathrm{X} & \\
{\scriptstyle \mathrm{F}^{[p]}(\mathrm{X/S})}\swarrow & & \searrow{\scriptstyle \mathrm{Fr}(\mathrm{X/S})} \\
\mathrm{X}^{[p/\mathrm{S}]} & \xrightarrow{\varphi(\mathrm{X})} & \mathrm{X}^{(p/\mathrm{S})}
\end{array} .$$

Par exemple, si X est le sous-schéma de S défini par un idéal quasi-cohérent $\mathscr{I}$, $\mathrm{F}^{[p]}(\mathrm{X/S})$ s'identifie au morphisme identique de X, de sorte que $\varphi(\mathrm{X})$ est l'immersion

(46) N.D.E. : Dans l'original, ce morphisme (resp. le morphisme de Frobenius relatif) était noté $\underline{\mathrm{F}}'$ (resp. $\underline{\mathrm{F}}$).

canonique de $\mathrm{Spec}(\mathscr{O}_S/\mathscr{I})$ dans $\mathrm{Spec}(\mathscr{O}_S/\mathscr{I}^{\{p\}})$. On voit ainsi que $\varphi(X)$ n'est pas un isomorphisme en général.

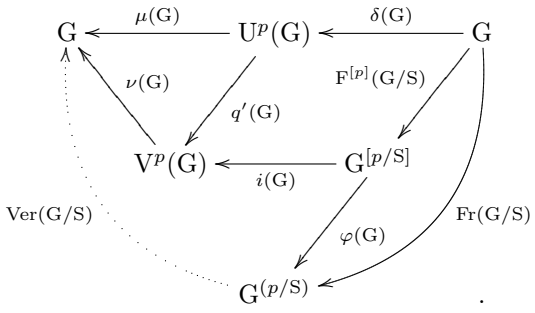
Toutefois, lorsque M est un R-module libre, il est clair que l'application

$$M \otimes_\pi R \longrightarrow \Sigma^p M/N(\bigotimes_R^p M), \qquad m \otimes_\pi \lambda \mapsto \Big(\lambda m \otimes \cdots \otimes m \qquad \mathrm{mod}\ N(\bigotimes_R^p M)\Big)$$

est bijective ; cette application reste donc bijective lorsque M est R-plat, parce que tout module plat est une limite inductive filtrante de modules libres (Lazard $^{(*)}$ $^{(47)}$). Il s'ensuit que

$\varphi(X) : X^{[p/S]} \to X^{(p/S)}$ est un isomorphisme si X *est un* S*-schéma plat.*

4.3. Considérons enfin un S-*schéma en groupes abéliens* G. Alors, le morphisme composé $\mu(G) : U^p(G) \hookrightarrow G_S^p \to G$, qui est défini par la multiplication, se factorise à travers $V^p(G)$, i.e. il existe un morphisme $\nu(G) : V^p(G) \to G$ tel que $\nu(G) \circ q'(G) = \mu(G)$, de sorte qu'on a le diagramme commutatif suivant :



441 *Lorsque* G *est* S*-plat*, $\varphi(G)$ est un isomorphisme et l'on peut définir un morphisme (dit *Verschiebung*)

$$\mathrm{Ver}(G/S) : \quad G^{(p/S)} \longrightarrow G$$

à l'aide de la formule $\mathrm{Ver}(G/S) = \nu(G) \circ i(G) \circ \varphi(G)^{-1}$. Lorsque G parcourt les S-schémas plats en groupes abéliens, l'application $\mathrm{Ver} : G \mapsto \mathrm{Ver}(G/S)$ est évidemment un homomorphisme fonctoriel ; par conséquent, Ver(G/S) est un *homomorphisme de groupes*. Pour tout S-schéma T enfin, l'application composée

$$G(T) \xrightarrow{\delta(G)(T)} U^p(G)(T) \xrightarrow{\mu(G)(T)} G(T)$$

applique $x \in G(T)$ sur $p \cdot x$. Nous pouvons écrire $p \cdot \mathrm{id}_G$ au lieu de $\mu(G) \circ \delta(G)$, obtenant ainsi la formule classique :

$$(*) \qquad \mathrm{Ver}(G/S) \circ \mathrm{Fr}(G/S) = p \cdot \mathrm{id}_G\,.$$

$^{(*)}$D. Lazard, C. R. Acad. Sc. Paris **258**, 1964, p. 6313-6316.

$^{(47)}$N.D.E. : Voir aussi : D. Lazard, Bull. Soc. Math. France **97** (1969), 81-128, ou : [**BAlg**], X § 1.6, Th. 1.

Exemples 4.3.1. — (a) Lorsque G est un S-schéma constant en groupes abéliens, nous savons que $\mathrm{Fr}(G/S)$ s'identifie au morphisme identique de G (cf. 4.1.1.1). On a donc $\mathrm{Ver}(G/S) = p\,\mathrm{id}_G$.

(b) Lorsque G est le S-groupe diagonalisable de type M, $\mathrm{Fr}(G/S)$ est égal à $p\,\mathrm{id}_G$ d'après 4.1.4 (a) ; on voit alors facilement que $\mathrm{Ver}(G/S)$ est le morphisme identique de G.

(c) Lorsque $\mathscr{E}$ est un $\mathscr{O}_S$-module plat et que G est le S-groupe $\mathbb{V}(\mathscr{E})$, le morphisme **442**
$\mathrm{Ver}(G/S)$ est nul ainsi que $p\cdot\mathrm{id}_G$. On verra dans l'exposé VII_B qu'un groupe algébrique commutatif G sur un corps k est « unipotent » si et seulement si l'homomorphisme composé

$$G^{(p^n)} \xrightarrow{\mathrm{Ver}(G^{(p^{n-1})}/S)} G^{(p^{n-1})} \longrightarrow \cdots \longrightarrow G^{(p)} \xrightarrow{\mathrm{Ver}(G/S)} G$$

est nul pour un certain n (on a posé $G^{(p^n)} = (G^{(p^{n-1})})^{(p)}$, cf. 4.1.3). [48]

4.3.2. — Comme l'application $\mathrm{Ver} : G \mapsto \mathrm{Ver}(G/S)$ est un homomorphisme fonctoriel lorsque G parcourt les S-*schémas plats en groupes commutatifs*, le carré

$$\begin{array}{ccc} G^{(p)} & \xrightarrow{\mathrm{Ver}(G/S)} & G \\ {\scriptstyle \mathrm{Fr}(G/S)^{(p)}}\downarrow & & \downarrow{\scriptstyle \mathrm{Fr}(G/S)} \\ G^{(p^2)} & \xrightarrow{\mathrm{Ver}(G^{(p)}/S)} & G^{(p)} \end{array}$$

est commutatif, où $\mathrm{Fr}(G/S)^{(p)}$ désigne l'image réciproque de $\mathrm{Fr}(G/S)$ par le changement de base fr(S). D'après 4.1.1, on a $\mathrm{Fr}(G/S)^{(p)} = \mathrm{Fr}(G^{(p)}/S)$ donc, d'après 4.3 $(*)$ appliqué à $G^{(p)}$, on obtient :

$$(**) \qquad \mathrm{Fr}(G/S)\circ\mathrm{Ver}(G/S) = \mathrm{Ver}(G^{(p)}/S)\circ\mathrm{Fr}(G^{(p)}/S) = p\cdot\mathrm{id}_{G^{(p)}}\,.$$

4.3.3. — Supposons enfin que G soit un S-*groupe commutatif, fini et localement libre* ; soient $\mathscr{A}$ la $\mathscr{O}_S$-algèbre affine de G et π l'endomorphisme du faisceau d'anneaux $\mathscr{O}_S$ qui envoie une section x de $\mathscr{O}_S$ sur x^p.

[49] On désigne par $\Sigma^p\mathscr{A}$ la sous-algèbre de $\bigotimes^p_{\mathscr{O}_S}\mathscr{A}$ formée des sections invariantes **443**
sous l'action du groupe symétrique, par $i(\mathscr{A})$ l'inclusion de $\Sigma^p\mathscr{A}$ dans le produit tensoriel. Soit $\Delta^p(\mathscr{A}) : \mathscr{A} \to \bigotimes^p_{\mathscr{O}_S}\mathscr{A}$ le morphisme obtenu en itérant le morphisme diagonal de la coalgèbre $\mathscr{A}$ (il correspond au morphisme de multiplication de $U^p(G) = G^p_S$ vers G) ; d'après le début du paragraphe 4.3, $\Delta^p(\mathscr{A})$ se factorise à travers $\Sigma^p\mathscr{A}$, c.-à-d., induit un morphisme

$$a(\mathscr{A}) : \mathscr{A} \longrightarrow \Sigma^p\mathscr{A}$$

tel que $i(\mathscr{A})\circ a(\mathscr{A}) = \Delta^p(\mathscr{A})$.

---

[48] N.D.E. : Ceci ne figurant pas explicitement dans VII_B, on renvoie à [**DG70**], § IV.3, Prop. 4.11.
[49] N.D.E. : On a modifié l'ordre, en introduisant d'abord les objets intervenant dans le diagramme qui va suivre.

D'autre part, soient $\mathcal{S}^p(\mathscr{A})$ la composante de degré p de l'algèbre symétrique de $\mathscr{A}$ et $q(\mathscr{A}) : \bigotimes^p_{\mathscr{O}_S} \mathscr{A} \to \mathcal{S}^p(\mathscr{A})$ la projection canonique. La multiplication $m^p(\mathscr{A}) : \bigotimes^p_{\mathscr{O}_S} \mathscr{A} \to \mathscr{A}$ se factorise à travers $\mathcal{S}^p(\mathscr{A})$, c.-à-d., induit une application

$$b(\mathscr{A}) : \mathcal{S}^p(\mathscr{A}) \longrightarrow \mathscr{A}$$

telle que $b(\mathscr{A}) \circ q(\mathscr{A}) = m^p(\mathscr{A})$.

Comme $\Sigma^p\mathscr{A}$ est l'algèbre affine de $\mathrm{V}^p(\mathscr{A})$ alors, d'après le début de 4.3 à nouveau, le morphisme composé $i(\mathrm{G}) \circ \varphi(\mathrm{G})^{-1}$ induit un homomorphisme d'algèbres

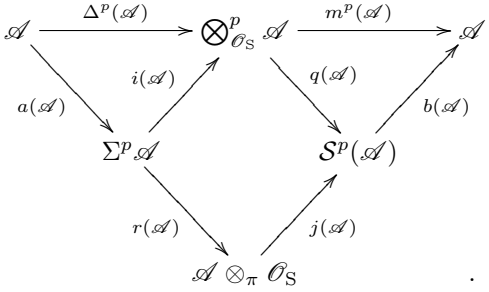
$$r(\mathscr{A}) : \ \Sigma^p\mathscr{A} \longrightarrow \mathscr{A} \otimes_\pi \mathscr{O}_S \quad ;$$

cet homomorphisme s'annule sur les sections de la forme

$$\sum_{\sigma \in \mathscr{S}_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}$$

et envoie $a \otimes \cdots \otimes a$ sur $a \otimes_\pi 1$. De même, $j(\mathscr{A})$ est le morphisme de $\mathscr{O}_S$-modules $a \otimes_\pi 1 \mapsto q(a \otimes \cdots \otimes a)$. On obtient donc le diagramme commutatif :

$(\mathscr{A})$



.

Le composé $r(\mathscr{A}) \circ a(\mathscr{A})$ est associé au morphisme Verschiebung Ver(G/S), tandis que $b(\mathscr{A}) \circ j(\mathscr{A})$ est associé au morphisme de Frobenius Fr(G/S).

Le diagramme commutatif $(\mathscr{A})$ ci-dessus est autodual ; soit en effet D le foncteur qui associe à tout $\mathscr{O}_S$-module $\mathscr{M}$ le $\mathscr{O}_S$-module dual $\mathscr{H}om_{\mathscr{O}_S}(\mathscr{M}, \mathscr{O}_S)$; il est clair que l'image du diagramme $(\mathscr{A})$ par le foncteur D n'est autre que le diagramme $(\mathrm{D}\mathscr{A})$, les morphismes $\mathrm{D}r(\mathscr{A})$, $\mathrm{D}a(\mathscr{A})$, $\mathrm{D}j(\mathscr{A})$ et $\mathrm{D}b(\mathscr{A})$ s'identifiant respectivement à $j(\mathrm{D}\mathscr{A})$, $b(\mathrm{D}\mathscr{A})$, $r(\mathrm{D}\mathscr{A})$ et $a(\mathrm{D}\mathscr{A})$. D'après 3.3.1, on voit donc que :

> *Dans la catégorie des* S*-groupes commutatifs, finis et localement libres, la dualité de Cartier échange morphisme de Frobenius et Verschiebung.* (50)

5. p-algèbres de Lie

444

Rappelons d'abord quelques résultats du Séminaire Sophus Lie. (51)

(50) N.D.E. : Voir aussi [**DG70**], § IV.3, 4.9.

(51) N.D.E. : cf. P. Cartier, *Exemples d'hyperalgèbres*, Sém. Sophus Lie 1955/56, Exp. 3 (accessible sur le site Numdam : http://www.numdam.org).

5.1. Soient p un nombre premier, R un anneau commutatif de caractéristique p et A une R-algèbre associative, mais non nécessairement commutative. Si a et b sont deux éléments de A, nous posons $[a,b] = ab - ba$ et $ab = \mathrm{L}_a(b) = \mathrm{R}_b(a)$. On a alors :

$$(\operatorname{ad} x^p)(y) = [x^p, y] = (\mathrm{L}_x^p - \mathrm{R}_x^p)(y) = (\mathrm{L}_x - \mathrm{R}_x)^p(y) = (\operatorname{ad} x)^p(y)$$

d'où la *première formule de Jacobson* :

$$\text{(i)} \qquad \operatorname{ad}(x^p) = (\operatorname{ad} x)^p.$$

Si $a_1, \ldots, a_p$ sont p éléments arbitraires de A alors, notant N l'opérateur de symétrisation (cf. 4.2), on a les égalités :

$$(*) \qquad \mathrm{N}(a_1 \otimes \cdots \otimes a_p) = \sum_\sigma a_{\sigma(1)} \cdots a_{\sigma(p)} = \sum_\tau [a_{\tau(1)}[a_{\tau(2)}[\cdots[a_{\tau(p-1)}, a_p]\cdots]]]$$

où σ parcourt les permutations de p lettres et τ celles de $(p-1)$ lettres. En effet, le dernier terme vaut

$$\sum_\tau \sum_{r=0}^{p-1} \sum_{i_1 < \cdots < i_r} (-1)^s \, a_{\tau(i_1)} \, a_{\tau(i_2)} \cdots a_{\tau(i_r)} \, a_p \, a_{\tau(j_s)} \cdots a_{\tau(j_1)}$$

où τ parcourt les permutations de $p-1$ lettres, $i_1, \ldots, i_r$ les suites strictement croissantes d'entiers de l'intervalle $[1, p-1]$ et où $j_1, \ldots, j_s$ désigne la suite strictement croissante dont les valeurs sont les entiers de $[1, p-1]$ différents de $i_1, \ldots, i_r$. Pour une valeur fixée de r, la somme des termes $(-1)^s \, a_{\tau(i_1)} \cdots a_{\tau(i_r)} \, a_p \, a_{\tau(j_s)} \cdots a_{\tau(j_1)}$ vaut évidemment

$$(-1)^s \binom{p-1}{s} \sum_\rho a_{\rho(1)} \cdots a_{\rho(r)} \, a_p \, a_{\rho(r+1)} \cdots a_{\rho(p-1)}$$

où ρ parcourt les permutations de $p-1$ lettres. Or $(-1)^s \binom{p-1}{s} = 1$ dans $\mathbb{F}_p$, puisque **445**
dans $\mathbb{F}_p[x]$ (x une indéterminée) on a : $(x-1)^p = x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$ et donc $(x-1)^{p-1} = x^{p-1} + \cdots + 1$. Ceci prouve $(*)$.

D'autre part, si x_0 et x_1 sont deux éléments de A, on a

$$(x_0 + x_1)^p = x_0^p + x_1^p + \sum x_{z(1)} x_{z(2)} \cdots x_{z(p)},$$

où z parcourt les applications non constantes de $[1, p]$ dans $\{0, 1\}$. On en tire

$$(x_0 + x_1)^p = x_0^p + x_1^p + \sum_{0<r<p} \frac{1}{r!(p-r)!} \, \mathrm{N}(\underbrace{x_0, \ldots, x_0}_{r}, \underbrace{x_1, \ldots, x_1}_{p-r}).$$

(52) Or, d'après $(*)$, on a :

$$\mathrm{N}(\underbrace{x_0, \ldots, x_0}_{r}, \underbrace{x_1, \ldots, x_1}_{p-r}) = r!(p-1-r)! \sum_t \left[x_{t(1)}\left[x_{t(2)}\left[\cdots\left[x_{t(p-1)}, x_1\right]\cdots\right]\right]\right]$$

(52) N.D.E. : On a inséré l'explication qui suit, tirée de [**DG70**], § II.7, 3.2.

où t parcourt les applications $[1, p-1] \to \{0,1\}$ prenant r fois la valeur 0. On en déduit la *deuxième formule de Jacobson* :

$$\text{(ii)} \qquad (x_0+x_1)^p = x_0^p + x_1^p - \sum_{0<r<p} \sum_t \frac{1}{r} \left[x_{t(1)}\left[x_{t(2)}\left[\cdots\left[x_{t(p-1)}, x_1\right]\cdots\right]\right]\right]$$

où t parcourt les applications $[1, p-1] \to \{0,1\}$ prenant r fois la valeur 0.

5.2. Soit maintenant $\mathfrak{g}$ une R-algèbre de Lie. On dit qu'une application $x \mapsto x^{(p)}$ de $\mathfrak{g}$ dans $\mathfrak{g}$ fait de $\mathfrak{g}$ une *p-algèbre de Lie* sur R si les conditions suivantes sont vérifiées :

(0) $(\lambda x)^{(p)} = \lambda^p \cdot x^{(p)}$, pour $\lambda \in \mathrm{R}$, $x \in \mathfrak{g}$

(i) $\operatorname{ad} x^{(p)} = (\operatorname{ad} x)^p$, pour $x \in \mathfrak{g}$

(ii) $(x_0+x_1)^{(p)} = x_0^{(p)} + x_1^{(p)} - \sum_{0<r<p} \sum_t \frac{1}{r} \left[x_{t(1)}\left[x_{t(2)}\left[\cdots\left[x_{t(p-1)}, x_1\right]\cdots\right]\right]\right]$

446 où t parcourt les applications $[1, p-1] \to \{0,1\}$ prenant r fois la valeur 0 ($x_0, x_1 \in \mathfrak{g}$). L'application $x \mapsto x^{(p)}$ sera alors appelée « puissance p-ième symbolique ».

Par exemple, si A est une R-algèbre associative, nous avons vu en 5.1 qu'on obtenait une p-algèbre de Lie, qu'on notera $\mathrm{A}_{\mathrm{Lie}}$, en prenant le R-module sous-jacent à A et en posant, pour $x, y \in \mathrm{A}$,

$$[x,y] = xy - yx \qquad \text{et} \qquad x^{(p)} = x^p.$$

Nous dirons que $\mathrm{A}_{\mathrm{Lie}}$ est la *p-algèbre de Lie sous-jacente à* A.

Dans la suite nous considèrerons surtout des sous-p-algèbres de Lie de p-algèbres de la forme $\mathrm{A}_{\mathrm{Lie}}$; en voici un exemple : soient S un schéma de caractéristique $p > 0$ et X un S-schéma. On rappelle qu'une dérivation de X sur S est un endomorphisme D du faisceau en groupes abéliens $\mathscr{O}_{\mathrm{X}}$ tel que

$$\mathrm{D}(\lambda \cdot s) = \lambda \cdot \mathrm{D}(s) \qquad \text{et} \qquad \mathrm{D}(st) = (\mathrm{D}s)t + s(\mathrm{D}t)$$

lorsque λ et s, t parcourent les sections de $\mathscr{O}_{\mathrm{S}}$ et de $\mathscr{O}_{\mathrm{X}}$ sur des ouverts tels que les formules aient un sens. La formule de Leibniz

$$\mathrm{D}^n(st) = \sum_{i=0}^{n} \binom{n}{i} (\mathrm{D}^i s)(\mathrm{D}^{n-i} t)$$

montre que D^p est encore une dérivation de X sur S, compte-tenu de l'égalité $\binom{p}{i} \equiv 0 \pmod{p}$ pour $i \neq 0, p$. Il s'ensuit que :

> *L'algèbre* $\mathrm{Dér}_{\mathrm{X/S}}$ *des dérivations de* X *sur* S *est une p-sous-algèbre de Lie de la* $\Gamma(\mathrm{S}, \mathscr{O}_{\mathrm{S}})$*-algèbre des opérateurs différentiels de* X *sur* S.

5.2.1. — Si $\mathfrak{g}$ et $\mathfrak{h}$ sont deux p-algèbres de Lie, un homomorphisme $h : \mathfrak{g} \to \mathfrak{h}$ est une application R-linéaire de $\mathfrak{g}$ dans $\mathfrak{h}$ telle que $h([x,y]) = [h(x), h(y)]$ et $h(x^{(p)}) = h(x)^{(p)}$ si x, $y \in \mathfrak{g}$. L'application composée de deux homomorphismes est encore un homomorphisme, de sorte que nous pourrons parler de la catégorie des p-algèbres de Lie sur R.

Si $(\mathrm{X}, \mathscr{R})$ est un espace annelé, nous dirons qu'un $\mathscr{R}$-module $\mathfrak{g}$ est muni d'une struc-
447 ture de *p-algèbre de Lie sur* $\mathscr{R}$ si, pour tout ouvert U, $\Gamma(\mathrm{U}, \mathfrak{g})$ est muni d'une structure

de p-algèbre de Lie sur $\Gamma(U, \mathscr{R})$ et si les restrictions sont des homomorphismes.

5.3. Nous nous intéressons maintenant au foncteur adjoint à gauche du foncteur $A \mapsto A_{Lie}$ de 5.2. Soient $\mathfrak{g}$ une p-algèbre de Lie sur l'anneau R de caractéristique p, $U(\mathfrak{g})$ l'algèbre enveloppante de l'algèbre de Lie sous-jacente à $\mathfrak{g}$ (cf. [**BLie**], I § 2.1) et $i_{\mathfrak{g}}$ (ou simplement i) l'application canonique $\mathfrak{g} \to U(\mathfrak{g})$.

Soit A une R-algèbre associative unitaire. On sait que, pour tout homomorphisme d'algèbres de Lie $\phi : \mathfrak{g} \to A_{Lie}$ il existe un unique homomorphisme de R-algèbres unitaires $\psi : U(\mathfrak{g}) \to A$ tel que $\psi \circ i = \phi$. En outre, ϕ est un homomorphisme de p-algèbres de Lie si et seulement si ψ s'annule sur les éléments $i(x)^p - i(x^{(p)})$, lorsque x parcourt $\mathfrak{g}$.

Définition. — On note $U_p^R(\mathfrak{g})$ ou simplement $U_p(\mathfrak{g})$ le quotient de $U(\mathfrak{g})$ par l'idéal bilatère engendré par les éléments $i(x)^p - i(x^{(p)})$, et $j_{\mathfrak{g}}$ (ou simplement j) l'application $\mathfrak{g} \to U_p(\mathfrak{g})$ composée de $i : \mathfrak{g} \to U(\mathfrak{g})$ et de l'application canonique $U(\mathfrak{g}) \to U_p(\mathfrak{g})$. On dit que $U_p(\mathfrak{g})$ est *l'algèbre enveloppante restreinte de* $\mathfrak{g}$.

D'après ce qui précède, on a la

Proposition. — *Pour toute* R*-algèbre associative unitaire et tout morphisme de p-algèbres de Lie $\phi : \mathfrak{g} \to A_{Lie}$, il existe un unique homomorphisme d'algèbres unitaires $\psi : U_p(\mathfrak{g}) \to A$ tel que $\psi \circ j = \phi$. En d'autres termes, le foncteur $\mathfrak{g} \mapsto U_p(\mathfrak{g})$ est adjoint à gauche du foncteur d'oubli $A \mapsto A_{Lie}$.*

5.3.1. — Avec les notations de 5.3, posons maintenant $\beta(x) = i(x)^p - i(x^{(p)})$. Pour tout élément y de $\mathfrak{g}$, on a, d'après 5.1 (i) et 5.2 (i) :

$$\begin{aligned}\beta(x)i(y) &= i(y)\beta(x) + [\beta(x), i(y)] \\ &= i(y)\beta(x) + (\operatorname{ad} i(x))^p\, i(y) - i((\operatorname{ad} x)^p\, y) \\ &= i(y)\beta(x),\end{aligned}$$

de sorte que $\beta(x)$ appartient au centre de $U(\mathfrak{g})$; en particulier, l'idéal à gauche en- **448**
gendré par les éléments $\beta(x)$ est déjà bilatère.

D'autre part, il est clair que $\beta(\lambda x) = \lambda^p \beta(x)$, pour $\lambda \in R$, et il résulte de 5.1 (ii) et 5.2 (ii) que, pour $x, y \in \mathfrak{g}$,

$$\beta(x + y) = \beta(x) + \beta(y).$$

En particulier, si (x_α) est une famille de générateurs du R-module $\mathfrak{g}$, l'idéal à gauche engendré par les éléments $\beta(x)$ est déjà engendré par les $\beta(x_\alpha)$.

5.3.2. Proposition. — [(53)] *Soit $\mathfrak{g}$ une* R*-algèbre de Lie dont le* R*-module sous-jacent est libre de base (x_α). Alors les structures de p-algèbre de Lie sur $\mathfrak{g}$ correspondent biunivoquement aux familles (y_α) de $\mathfrak{g}$ telles que* $\operatorname{ad} y_\alpha = (\operatorname{ad} x_\alpha)^p$.

(53) N.D.E. : Dans ce paragraphe, on a modifié l'ordre, énonçant d'abord le résultat, puis détaillant la démonstration.

En effet, si $\mathfrak{g}$ est munie d'une structure de p-algèbre de Lie $x \mapsto x^{(p)}$, alors d'après 5.2 (i) et (0), (ii), les $y_\alpha = x_\alpha^{(p)}$ vérifient $\operatorname{ad} y_\alpha = (\operatorname{ad} x_\alpha)^p$, et déterminent la structure de p-algèbre de Lie.

Prouvons la réciproque. Comme $\mathfrak{g}$ est un R-module libre, l'application canonique $i : \mathfrak{g} \to \mathrm{U}(\mathfrak{g})$ est injective, d'après le théorème de Poincaré-Birkhoff-Witt (cf. [**BLie**], I § 2.7), donc on peut identifier $\mathfrak{g}$ à un sous-R-module de $\mathrm{U}(\mathfrak{g})$. Supposons que (y_α) soit une famille d'éléments de $\mathfrak{g}$ tels que $\operatorname{ad} y_\alpha = (\operatorname{ad} x_\alpha)^p$. Soit π l'application $r \mapsto r^p$ de R dans R, et soit $\mathfrak{g} \otimes_\pi \mathrm{R}$ la R-algèbre de Lie obtenue par l'extension des scalaires $\pi : \mathrm{R} \to \mathrm{R}$. (54)

Il existe alors une application R-linéaire γ de $\mathfrak{g} \otimes_\pi \mathrm{R}$ dans $\mathrm{U}(\mathfrak{g})$ qui envoie $x_\alpha \otimes_\pi 1$ sur $x_\alpha^p - y_\alpha$; de plus, comme on a, pour tout $x \in \mathfrak{g}$,

$$(\operatorname{ad} x_\alpha^p)(x) = (\operatorname{ad} x_\alpha)^p(x) = (\operatorname{ad} y_\alpha)(x),$$

γ applique $\mathfrak{g} \otimes_\pi \mathrm{R}$ dans le centre de $\mathrm{U}(\mathfrak{g})$. Posons, pour tout $x \in \mathfrak{g}$:

$$x^{(p)} = x^p - \gamma(x \otimes_\pi 1).$$

Alors, pour tout α, on a $x_\alpha^{(p)} = y_\alpha$. Si $x = \sum \lambda_\alpha x_\alpha$, on déduit de 5.1 (ii) (en procédant par récurrence sur le nombre d'indices α tels que $\lambda_\alpha \neq 0$), que

$$x^p - \sum_\alpha \lambda_\alpha^p \, x_\alpha^p \in \mathfrak{g};$$

désignant par z cet élément, on a alors $x^{(p)} = \sum \lambda_\alpha^p \, y_\alpha + z$ et donc $x^{(p)} \in \mathfrak{g}$.

Il est clair que l'application $x \mapsto x^{(p)}$ vérifie $(\lambda x)^{(p)} = \lambda^p \, x^{(p)}$. De plus, comme $\gamma(x \otimes_\pi 1)$ est central, alors $\operatorname{ad} x^{(p)} = \operatorname{ad} x^p$ et donc, d'après la première formule de Jacobson (5.1 (i)), on a

$$\operatorname{ad} x^{(p)} = (\operatorname{ad} x)^p.$$

Enfin, d'après la deuxième formule de Jacobson (5.1 (ii)), l'application $x \mapsto x^{(p)}$ vérifie la condition (ii) de 5.2. Elle fait donc de $\mathfrak{g}$ une p-algèbre de Lie. Ceci prouve la proposition.

5.3.3. Proposition. — *Soit $\mathfrak{g}$ une p-algèbre de Lie sur* R *dont le module sous-jacent est libre de base (x_α). Alors l'application $j : \mathfrak{g} \to \mathrm{U}_p(\mathfrak{g})$ est injective et, si l'on pose $z_\alpha = j(x_\alpha)$, alors $\mathrm{U}_p(\mathfrak{g})$ a pour base les monômes*

$$\prod_\alpha z^{n_\alpha} \qquad \text{où} \quad 0 \leqslant n_\alpha < p,$$

(les n_α sont supposés nuls hormis un nombre fini d'entre eux ; on suppose la base totalement ordonnée et les produits effectués dans l'ordre croissant).

449 En effet, identifions $\mathfrak{g}$ à un sous-module de l'algèbre enveloppante $\mathrm{U}(\mathfrak{g})$ au moyen de l'application canonique i. Pour toute famille $n = (n_\alpha)$ d'entiers naturels, nuls hormis un nombre fini d'entre eux, posons

$$|n| = \sum_\alpha n_\alpha \qquad \text{et} \qquad x^n = \prod_\alpha x_\alpha^{n_\alpha}.$$

(54) N.D.E. : c.-à-d., $xr \otimes_\pi 1 = x \otimes_\pi r^p$ et $r \cdot (x \otimes_\pi 1) = x \otimes_\pi r$, pour $x \in \mathfrak{g}$, $r \in \mathrm{R}$.

Écrivant $n_\alpha = m_\alpha + p\ell_\alpha$, avec $0 \leqslant m_\alpha < p$, posons aussi

$$\mathrm{T}_n = \prod_\alpha x^{m_\alpha}\, \beta(x_\alpha)^{\ell_\alpha}$$

où $\beta(x) = x^p - x^{(p)}$ est l'application $\mathfrak{g} \to \mathrm{U}(\mathfrak{g})$ définie en 5.3.1.

Pour tout $r \in \mathbb{N}$, notons U^r le sous-R-module de $\mathrm{U}(\mathfrak{g})$ engendré par les x^n tels que $|n| \leqslant r$. Comme l'anneau gradué $\bigoplus_r \mathrm{U}^r/\mathrm{U}^{r-1}$ est commutatif (cf. [**BLie**], I § 2.6), on voit que, pour tout n :

$$\mathrm{T}_n - \prod_\alpha x^{n_\alpha} \in \mathrm{U}^{|n|-1}.$$

Pour tout $s \in \mathbb{N}$, les x^n tels que $|n| = s$ forment, d'après le théorème de Poincaré-Birkhoff-Witt (*loc. cit.*, § 2.7), une base de $\mathrm{U}^s/\mathrm{U}^{s-1}$, et donc il en est de même pour les T_n tels que $|n| = s$.

Donc, lorsque $s = |n|$ varie, les T_n forment une base de $\mathrm{U}(\mathfrak{g})$. Or le noyau J de l'application canonique $\mathrm{U}(\mathfrak{g}) \to \mathrm{U}_p(\mathfrak{g})$ est l'idéal à gauche de $\mathrm{U}(\mathfrak{g})$ engendré par les éléments centraux $\beta(x_\alpha)$ (5.3.1). Par conséquent, les T_n tels que $\ell = (\ell_\alpha) \neq 0$ forment une base de J, et les T_n tels que $n_\alpha < p$ pour tout α, forment une base de $\mathrm{U}_p(\mathfrak{g}) = \mathrm{U}(\mathfrak{g})/\mathrm{J}$.

5.3.3 bis. — Soient $\mathfrak{g}$ une p-algèbre de Lie sur R et $f : \mathrm{R} \to \mathrm{R}'$ une extension de l'anneau de base. Je dis qu'*il existe sur le* R'*-module* $\mathrm{R}' \otimes_\mathrm{R} \mathfrak{g}$ *une structure de p-algèbre de Lie et une seule telle que*

$$(*) \qquad [\lambda \otimes x, \mu \otimes y] = \lambda\mu \otimes [x, y] \qquad \text{et} \qquad (\lambda \otimes x)^{(p)} = \lambda^p \otimes x^{(p)}.$$

Il en résultera, en particulier, que le foncteur $\mathfrak{g} \mapsto \mathrm{R}' \otimes_\mathrm{R} \mathfrak{g}$ est adjoint à gauche au foncteur « restriction des scalaires de R' à R ».

L'unicité de la structure de p-algèbre de Lie définie par $(*)$ étant claire, prouvons l'existence. Lorsque $\mathfrak{g}$ est libre de base (x_α) il existe d'après 5.3.2 une et une seule structure de p-algèbre de Lie sur l'algèbre de Lie $\mathrm{R}' \otimes_\mathrm{R} \mathfrak{g}$ telle que

$$(1 \otimes x_\alpha)^{(p)} = 1 \otimes x_\alpha^{(p)};$$

cette structure est celle que nous cherchons.

Lorsque $\mathfrak{g}$ est une p-algèbre de Lie arbitraire, il existe une p-algèbre de Lie libre (en tant que R-module) L_0 et un homomorphisme surjectif $q_0 : \mathrm{L}_0 \to \mathfrak{g}$; il suffit par exemple de prendre pour L_0 la p-algèbre de Lie $\mathrm{R} \otimes_{\mathbb{F}_p} \mathfrak{g}$, où $\mathbb{F}_p$ désigne le corps premier de caractéristique p, pour q_0 l'homomorphisme $\lambda \otimes x \mapsto \lambda x$ ($\mathfrak{g}$ est libre sur $\mathbb{F}_p$!). Le **450**
noyau de q_0 est alors un p-idéal de L_0, c'est-à-dire un idéal de l'algèbre de Lie L_0 qui est stable par l'endomorphisme $x \mapsto x^{(p)}$; il y a donc également une p-algèbre de Lie libre (en tant que R-module) L_1 et un homomorphisme $q_1 : \mathrm{L}_1 \to \mathrm{L}_0$ dont l'image est $\operatorname{Ker} q_0$, d'où la suite exacte :

$$\mathrm{L}_1 \xrightarrow{q_1} \mathrm{L}_0 \xrightarrow{q_0} \mathfrak{g} \longrightarrow 0.$$

On en déduit une suite exacte de R'-algèbres de Lie

$$\mathrm{R}' \otimes_\mathrm{R} \mathrm{L}_1 \xrightarrow{\mathrm{R}' \otimes_\mathrm{R} q_1} \mathrm{R}' \otimes_\mathrm{R} \mathrm{L}_0 \xrightarrow{\mathrm{R}' \otimes_\mathrm{R} q_0} \mathrm{R}' \otimes_\mathrm{R} \mathfrak{g} \longrightarrow 0.$$

Comme $R' \otimes_R q_1$ est manifestement un homomorphisme de p-algèbres de Lie, le noyau de $R' \otimes_R q_0$ est un p-idéal, de sorte que l'opération puissance p-ième symbolique de $R' \otimes_R L_0$ induit par passage au quotient une application de $R' \otimes_R \mathfrak{g}$ dans $R' \otimes_R \mathfrak{g}$ (utiliser la formule (ii) de 5.2.) ; cette dernière munit $R' \otimes_R \mathfrak{g}$ de la structure de p-algèbre de Lie cherchée.

5.3.4. — L'application canonique $j_{\mathfrak{g}} : \mathfrak{g} \to U_p(\mathfrak{g})$ induit, pour toute extension $R \to R'$ de l'anneau de base, un homomorphisme

$$R' \otimes_R j_{\mathfrak{g}} : \quad R' \otimes_R \mathfrak{g} \longrightarrow R' \otimes_R U_p(\mathfrak{g}),$$

d'où un homomorphisme

$$h : U_p(R' \otimes_R \mathfrak{g}) \longrightarrow R' \otimes_R U_p(\mathfrak{g})$$

tel que $h \circ j_{R' \otimes \mathfrak{g}} = R' \otimes_R j_{\mathfrak{g}}$. Il résulte évidemment des propriétés universelles de $R' \otimes_R \mathfrak{g}$ et de l'algèbre enveloppante restreinte que h est un *isomorphisme*, ce qui nous permettra *d'identifier* $U_p(R' \otimes_R \mathfrak{g})$ à $R' \otimes_R U_p(\mathfrak{g})$.

En particulier, si r est un élément de R et si R' est l'anneau localisé R_r, on voit que
451 $\mathfrak{g}_r = R_r \otimes_R \mathfrak{g}$ est muni canoniquement d'une structure de p-algèbre de Lie sur R_r, de sorte que le faisceau $\widetilde{\mathfrak{g}}$ sur $\operatorname{Spec} R$ est une p-algèbre de Lie quasi-cohérente sur $\operatorname{Spec} R$. De plus, l'algèbre enveloppante restreinte $U_p^{R_r}(\mathfrak{g}_r)$ s'identifie à $U_p^R(\mathfrak{g})_r$ de sorte que le faisceau associé au préfaisceau $V \mapsto U_p(\Gamma(V, \mathfrak{g}))$ est quasi-cohérent.

Définition. — Plus généralement, si S est un schéma de caractéristique p et $\mathscr{G}$ une p-algèbre de Lie quasi-cohérente sur $\mathscr{O}_S$, le faisceau associé au préfaisceau $V \mapsto U_p(\Gamma(V, \mathscr{G}))$ est quasi-cohérent ; il sera noté $\mathscr{U}_p(\mathscr{G})$ et appelé *l'algèbre enveloppante restreinte de* $\mathscr{G}$. Si V est affine, $U_p(\Gamma(V, \mathscr{G}))$ s'identifie à $\Gamma(V, \mathscr{U}_p(\mathscr{G}))$.

5.4. Le caractère universel de $U_p(\mathfrak{g})$ entraîne que $U_p(\mathfrak{g})$ est fonctoriel en $\mathfrak{g}$: tout homomorphisme de p-algèbres de Lie $\phi : \mathfrak{g} \to \mathfrak{h}$ induit un homomorphisme d'algèbres unitaires $U_p(\phi)$ et un seul tel que $j_{\mathfrak{h}} \circ \phi = U_p(\phi) \circ j_{\mathfrak{g}}$. Voici quelques exemples :

a) Si $\mathfrak{h} = 0$, $U_p(\mathfrak{h})$ s'identifie à l'anneau de base et $U_p(\phi)$ est un homomorphisme d'algèbres $\varepsilon_{\mathfrak{g}} : U_p(\mathfrak{g}) \to R$ appelé *augmentation*.

b) Prenons maintenant pour $\mathfrak{h}$ l'algèbre $\mathfrak{g}^\circ$ opposée à $\mathfrak{g}$, i.e. $\mathfrak{g}^\circ$ a même module sous-jacent que $\mathfrak{g}$, même puissance p-ième symbolique, le crochet de deux éléments dans $\mathfrak{g}^\circ$ étant l'opposé du crochet dans $\mathfrak{g}$. Il est clair que nous pouvons identifier $U_p(\mathfrak{g}^\circ)$ à l'algèbre opposée à $U_p(\mathfrak{g})$. De plus, l'isomorphisme $x \mapsto -x$ de $\mathfrak{g}$ sur $\mathfrak{g}^\circ$ induit un isomorphisme $c_{\mathfrak{g}}$ de $U_p(\mathfrak{g})$ sur $U_p(\mathfrak{g}^\circ) \simeq U_p(\mathfrak{g})^\circ$. On dit que $c_{\mathfrak{g}}$ est l'*antipodisme* de $U_p(\mathfrak{g})$.

c) Soient enfin $\mathfrak{f}$ et $\mathfrak{g}$ deux p-algèbres de Lie et $\mathfrak{h}$ la *p-algèbre de Lie produit* $\mathfrak{f} \times \mathfrak{g}$ qui a pour R-module sous-jacent le produit direct $\mathfrak{f} \times \mathfrak{g}$, le crochet et la puissance p-ième symbolique étant définis par les formules

$$\big[(x, y), (x', y')\big] = ([x, x'], [y, y']) \qquad \text{et} \qquad (x, y)^{(p)} = (x^{(p)}, y^{(p)}).$$

452 Si $h_1 : \mathfrak{f} \to \mathfrak{k}$ et $h_2 : \mathfrak{g} \to \mathfrak{k}$ sont deux homomorphismes de p-algèbres de Lie tels que $[h_1(x), h_2(y)] = 0$ pour tout x de $\mathfrak{f}$ et tout y de $\mathfrak{g}$, l'application $h_1 + h_2 : (x, y) \to h_1(x) + h_2(y)$ est un homomorphisme de p-algèbres de Lie ; réciproquement, tout homomorphisme de $\mathfrak{f} \times \mathfrak{g}$ dans $\mathfrak{k}$ est de ce type, ce qui permet de caractériser $\mathfrak{f} \times \mathfrak{g}$ comme solution d'un problème universel. Par exemple, les applications

$$h_1 : x \mapsto i_{\mathfrak{f}}(x) \otimes 1 \qquad \text{et} \qquad h_2 : y \mapsto 1 \otimes i_{\mathfrak{g}}(y)$$

induisent un homomorphisme $h_1 + h_2$ de $\mathfrak{f} \times \mathfrak{g}$ dans la p-algèbre de Lie sous-jacente à $\mathrm{U}_p(\mathfrak{f}) \otimes \mathrm{U}_p(\mathfrak{g})$. Il résulte des caractères universels de $\mathfrak{f} \times \mathfrak{g}$ et des algèbres enveloppantes restreintes que $h_1 + h_2$ se prolonge en un isomorphisme :

$$\varphi : \mathrm{U}_p(\mathfrak{f} \times \mathfrak{g}) \xrightarrow{\sim} \mathrm{U}_p(\mathfrak{f}) \otimes \mathrm{U}_p(\mathfrak{g}).$$

Définition. — Si $\mathfrak{f} = \mathfrak{g}$, l'application diagonale $\delta : x \mapsto (x, x)$ de $\mathfrak{g}$ dans $\mathfrak{g} \times \mathfrak{g}$ induit un homomorphisme de $\mathrm{U}_p(\mathfrak{g})$ dans $\mathrm{U}_p(\mathfrak{g} \times \mathfrak{g})$. Nous noterons $\Delta_{\mathfrak{g}}$ le composé de cet homomorphisme avec l'isomorphisme $\varphi : \mathrm{U}_p(\mathfrak{g} \times \mathfrak{g}) \xrightarrow{\sim} \mathrm{U}_p(\mathfrak{g}) \otimes \mathrm{U}_p(\mathfrak{g})$. [55]

On voit alors facilement que $\Delta_{\mathfrak{g}}$ et la multiplication de l'algèbre $\mathrm{U}_p(\mathfrak{g})$ font de $\mathrm{U}_p(\mathfrak{g})$ *une* R-*coalgèbre en groupes* (cf. 3.2) qui a $\varepsilon_{\mathfrak{g}}$ pour augmentation et $c_{\mathfrak{g}}$ pour antipodisme.

5.5. [56] Soit maintenant S un schéma de caractéristique p. D'abord, si $\mathscr{U}$ est une $\mathscr{O}_{\mathrm{S}}$-coalgèbre en groupes et G le S-foncteur en groupes $\mathrm{Spec}^*\,\mathscr{U}$, on a vu (3.2.3) que, pour tout $\mathrm{T} \to \mathrm{S}$, $(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$ est la sous-algèbre de Lie de $\Gamma(\mathrm{T}, \mathscr{U}_{\mathrm{T}})$ formée des éléments primitifs. Or, si x est un tel élément, on a $\Delta(x^p) = x^p \otimes 1 + 1 \otimes x^p$ (puisque $\binom{p}{i} = 0 \bmod p$ pour $0 < i < p$), i.e. x^p est encore un élément primitif. Il en résulte, d'après 5.1 et 5.2, que l'application $x \mapsto x^p$ munit $(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$ d'une structure de $\mathscr{O}(\mathrm{T})$-p-algèbre de Lie.

Soit maintenant $\mathscr{L}$ une $\mathscr{O}_{\mathrm{S}}$-p-algèbre de Lie, quasi-cohérente sur $\mathscr{O}_{\mathrm{S}}$. Lorsque V parcourt les ouverts de S, les structures de coalgèbres en groupes définies précédemment sur les ensembles $\mathrm{U}_p(\Gamma(\mathrm{V}, \mathscr{L}))$ induisent sur le faisceau associé, i.e. sur l'algèbre enveloppante restreinte $\mathscr{U}_p(\mathscr{L})$, une structure de $\mathscr{O}_{\mathrm{S}}$-coalgèbre en groupes. De plus, pour tout S-schéma T, on a un isomorphisme $\mathscr{U}_p(\mathscr{L}_{\mathrm{T}}) \xrightarrow{\sim} \mathscr{U}_p(\mathscr{L})_{\mathrm{T}}$.

Notons $\mathrm{Prim}\,\mathscr{U}_p(\mathscr{L})$ le sous-préfaisceau de $\mathscr{U}_p(\mathscr{L})$ associant à tout ouvert V l'ensemble des éléments primitifs de $\mathscr{U}_p(\mathscr{L})(\mathrm{V})$; on voit facilement que c'est un *faisceau*. Lorsque V parcourt les ouverts de S, les applications composées

$$\Gamma(\mathrm{V}, \mathscr{L}) \xrightarrow{j} \mathrm{Prim}\,\mathrm{U}_p(\Gamma(\mathrm{V}, \mathscr{L})) \longrightarrow \mathrm{Prim}\,\mathscr{U}_p(\mathscr{L})(\mathrm{V})$$

---

[55] N.D.E. : i.e. $\Delta_{\mathfrak{g}}(x) = x \otimes 1 + 1 \otimes x$ pour tout $x \in \mathfrak{g}$; en particulier, la comultiplication $\Delta_{\mathfrak{g}}$ est bien cocommutative ...

[56] N.D.E. : On a transformé le § 5.4.1 de l'original en ce § 5.5 : d'une part, la proposition 5.5.1 réunit les résultats de la Section 5 et la proposition 3.2.3 et contient le lemme 7.3 de l'original ; d'autre part, la démonstration de 5.5.3 (ii) reprend, en la détaillant, celle de l'implication (i) ⇒ (ii) dans le théorème 7.4 plus bas.

définissent un morphisme $\mathscr{L} \to \operatorname{Prim} \mathscr{U}_p(\mathscr{L})$, que nous noterons encore j ou $j_{\mathscr{L}}$, et celui définit encore un morphisme de $\mathbf{O}_S$-p-algèbres de Lie $\mathbf{W}(\mathscr{L}) \to \operatorname{Prim} \mathbf{W}(\mathscr{U}_p(\mathscr{L}))$ (cf. 3.2.3).

Proposition 5.5.1. — *Soit $\mathscr{L}$ une $\mathscr{O}_S$-p-algèbre de Lie, localement libre comme $\mathscr{O}_S$-module. Alors $j_{\mathscr{L}}$ induit un isomorphisme de $\mathbf{O}_S$-p-algèbres de Lie :*

$$\mathbf{W}(\mathscr{L}) \xrightarrow{\sim} \operatorname{Prim} \mathbf{W}(\mathscr{U}_p(\mathscr{L})).$$

Démonstration. Soit T un S-schéma ; compte-tenu de l'identification $\mathscr{U}_p(\mathscr{L}_T) = \mathscr{U}_p(\mathscr{L})_T$, il s'agit de montrer que l'application $\Gamma(T, \mathscr{L}_T) \to \operatorname{Prim} \Gamma(T, \mathscr{U}_p(\mathscr{L}_T))$ est bijective. Remplaçant S par T, on est ramené au cas où T = S, et il suffit alors de montrer que le morphisme de faisceaux $j_{\mathscr{L}} : \mathscr{L} \to \operatorname{Prim} \mathscr{U}_p(\mathscr{L})$ est un isomorphisme. Cette question étant locale sur S, nous pouvons supposer que S est affine d'anneau R et que $\mathscr{L}$ est le faisceau associé à une R-p-algèbre de Lie L de base (x_α). Comme en 5.3.3, notons z_α l'image de x_α dans $U = U_p(L)$ et, pour toute famille $n = (n_\alpha)$ d'entiers compris entre 0 et $p-1$, nuls hormis un nombre fini d'entre eux, notons $z^{(n)}$ le produit

$$\prod_\alpha \frac{z_\alpha^{n_\alpha}}{n_\alpha!}$$

(on suppose la base (x_α) totalement ordonnée et les produits effectués dans l'ordre croissant).

Comme $\Delta(z_\alpha) = z_\alpha \otimes 1 + 1 \otimes z_\alpha$, on voit facilement que

$$\Delta(z^{(n)}) = \sum_r z^{(n-r)} \otimes z^{(r)}$$

la somme étant prise sur l'ensemble (fini !) des r tels que $0 \leqslant r_\alpha \leqslant n_\alpha$ pour tout α. Comme les $z^{(n)}$ (resp. les $z^{(n)} \otimes z^{(m)}$) forment une base de U (resp. de $U \otimes U$), on en déduit qu'un élément u de U vérifie $\Delta(u) = u \otimes 1 + 1 \otimes u$ si et seulement si u est combinaison linéaire des z_α. Ceci prouve 5.5.1.

Remarque 5.5.2. — Rappelons (cf. 3.2.2 et 3.2.3), que le S-foncteur en groupes $G = \operatorname{Spec}^* \mathscr{U}_p(\mathscr{L})$ est très bon et que $\underline{\mathrm{Lie}}(G) = \operatorname{Prim} \mathbf{W}(\mathscr{U}_p(\mathscr{L}))$. La proposition précédente signifie donc que $j_{\mathscr{L}}$ induit un isomorphisme $\mathbf{W}(\mathscr{L}) \xrightarrow{\sim} \underline{\mathrm{Lie}}(G)$.

Si l'on suppose de plus que $\mathscr{L}$ est un $\mathscr{O}_S$-module localement libre de rang fini, alors $\mathscr{U}_p(\mathscr{L})$ est finie localement libre sur $\mathscr{O}_S$, d'après 5.3.3, donc $\operatorname{Spec}^* \mathscr{U}_p(\mathscr{L})$ est représenté par le S-groupe $G_p(\mathscr{L}) = \operatorname{Spec} \mathscr{U}_p(\mathscr{L})^*$ (cf. 3.2.2.1), et l'on obtient la proposition plus précise suivante :

Proposition 5.5.3. — *Soit $\mathscr{L}$ une $\mathscr{O}_S$-p-algèbre de Lie, localement libre de rang fini comme $\mathscr{O}_S$-module, soit $\mathscr{A} = \mathscr{U}_p(\mathscr{L})^*$ et soit $G = G_p(\mathscr{L})$ le S-groupe affine $\operatorname{Spec} \mathscr{A}$.*

(i) *$j_{\mathscr{L}}$ induit un isomorphisme $\mathbf{W}(\mathscr{L}) \xrightarrow{\sim} \underline{\mathrm{Lie}}(G)$ de $\mathbf{O}_S$-p-algèbres de Lie.*

(ii) *Soient $\mathscr{I}$ l'idéal d'augmentation de $\mathscr{A}$ et $\omega_G = \mathscr{I}/\mathscr{I}^2$* (cf. II, 4.11.4). *Alors ω_G s'identifie à $\mathscr{L}^* = \mathscr{H}om_{\mathscr{O}_S}(\mathscr{L}, \mathscr{O}_S)$, donc est un $\mathscr{O}_S$-module localement libre de rang fini* (*et l'on a $\omega^*_{G/S} = \mathscr{L}$*).

Démonstration. (i) découlant de 5.5.2, prouvons (ii). Notons $\eta_{\mathscr{U}}$ et $\varepsilon_{\mathscr{U}}$ la section unité et l'augmentation de $\mathscr{U} = \mathscr{U}_p(\mathscr{L})$, $\eta_{\mathscr{A}}$ et $\varepsilon_{\mathscr{A}}$ celles de $\mathscr{A}$, et $\mathscr{J} = \operatorname{Ker}\varepsilon_{\mathscr{U}}$. Alors on a :

$$\mathscr{U} = \eta_{\mathscr{U}}(\mathscr{O}_S) \oplus \mathscr{J}. \tag{1}$$

Soit δ le morphisme défini par le diagramme ci-dessous, où τ et π désignent l'inclusion et la projection déduites de la décomposition (1) :

$$\begin{array}{ccc} \mathscr{J} & \xrightarrow{\delta} & \mathscr{J}\otimes\mathscr{J} \\ {\scriptstyle\tau}\downarrow & & \uparrow{\scriptstyle\pi} \\ \mathscr{U} & \xrightarrow{\Delta} & \mathscr{U}\otimes\mathscr{U} \end{array}$$

alors on a une suite exacte :

$$0 \longrightarrow \mathscr{L}^* \xrightarrow{j_{\mathscr{L}}} \mathscr{J} \xrightarrow{\delta} \mathscr{J}\otimes\mathscr{J}. \tag{$*$}$$

De plus, d'après 5.3.3, le $\mathscr{O}_S$-module $\mathscr{J}/\mathscr{L}$ est localement libre et, d'après 5.5.1, la suite $(*)$ reste exacte après tout changement de base. Donc, d'après [**BAC**], II § 3, prop. 6, δ induit un isomorphisme de $\mathscr{J}/\mathscr{L}$ sur un sous-module $\mathscr{Q}$ localement facteur direct de $\mathscr{J}\otimes\mathscr{J}$. Il en résulte que $(*)$ donne par dualité la suite exacte :

$$0 \longleftarrow \mathscr{L} \xleftarrow{{}^t j_{\mathscr{L}}} \mathscr{I} \xleftarrow{{}^t\delta} \mathscr{I}\otimes\mathscr{I}. \tag{$**$}$$

Or la décomposition (1) correspond par dualité à la décomposition :

$$\mathscr{A} = \eta_{\mathscr{A}}(\mathscr{O}_S) \oplus \mathscr{I} \tag{2}$$

et la transposée de Δ est la multiplication $m_{\mathscr{A}} : \mathscr{A}\otimes\mathscr{A} \to \mathscr{A}$. Comme $\mathscr{I}$ est un idéal de $\mathscr{A}$, $m_{\mathscr{A}}$ envoie $\mathscr{I}\otimes\mathscr{I}$ dans $\mathscr{I}$; plus précisément, compte-tenu de la décomposition (2), on a un carré commutatif

$$\begin{array}{ccc} \mathscr{I} & \xleftarrow{m'} & \mathscr{I}\otimes\mathscr{I} \\ {\scriptstyle{}^t\tau}\uparrow & & \downarrow{\scriptstyle{}^t\pi} \\ \mathscr{A} & \xleftarrow{m_{\mathscr{A}}} & \mathscr{A}\otimes\mathscr{A} \end{array}$$

qui montre que la restriction m' de $m_{\mathscr{A}}$ à $\mathscr{I}\otimes\mathscr{I}$ est la transposée de δ. La suite exacte $(**)$ donne alors $\mathscr{I}/\mathscr{I}^2 \simeq \mathscr{L}^*$, et la proposition en découle.

6. p-algèbre de Lie d'un S-schéma en groupes

453

Soit S un schéma de caractéristique $p > 0$. Au paragraphe 5.5 nous avons associé à toute $\mathscr{O}_S$-p-algèbre de Lie quasi-cohérente $\mathscr{L}$ un S-foncteur en groupes $\mathrm{G}_p(\mathscr{L}) = \operatorname{Spec}^* \mathscr{U}_p(\mathscr{L})$. Nous allons voir maintenant que, pour tout S-schéma en groupes G, la $\mathbf{O}_S$-algèbre de Lie $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})$ définie en II 4.11 est munie naturellement d'une structure de $\mathbf{O}_S$-p-algèbre de Lie.

6.1. Identifions tout d'abord $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ et $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}\,\mathrm{G}/\mathrm{S})(\mathrm{S})$ respectivement à des sous-algèbres de Lie de $\mathrm{U}(\mathrm{G})$ et $\mathrm{Dif}_{\mathrm{G}/\mathrm{S}}$ au moyen des injections α et β de 2.5 ; $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}\,\mathrm{G}/\mathrm{S})(\mathrm{S})$ est donc identifiée à la $\Gamma(\mathscr{O}_{\mathrm{S}})$-algèbre de Lie des S-dérivations de $\mathscr{O}_{\mathrm{G}}$. D'après 5.2, cette dernière est une sous-p-algèbre de Lie de $\mathrm{Dif}_{\mathrm{G}/\mathrm{S}}$.

D'autre part, l'image de $\mathrm{L} = \underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ par le morphisme injectif d'algèbres $\ell : \mathrm{U}(\mathrm{G}) \to \mathrm{Dif}_{\mathrm{G}/\mathrm{S}}$, $d \mapsto {}^{\mathrm{G}}d$ est formée des dérivations invariantes à gauche (cf. 2.2, N.D.E. (17), 2.4 et 2.5). Si x appartient à L, $\ell(x)^p$ n'est autre que $\ell(x^p)$, d'après *loc. cit.* Comme $\ell(x)^p$ est encore une dérivation, on voit que x^p appartient à $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$. Donc : [57]

$\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ *est une sous-p-algèbre de Lie de l'algèbre infinitésimale* $\mathrm{U}(\mathrm{G})$.

6.1.1. — Soit $\phi : \mathrm{G} \to \mathrm{H}$ un homomorphisme de S-schémas en groupes. Il est clair que les homomorphismes $\underline{\mathrm{Lie}}(\phi/\mathrm{S})(\mathrm{S})$ et $\mathrm{U}(\phi)$ sont compatibles avec les identifications de $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ et $\underline{\mathrm{Lie}}(\mathrm{H}/\mathrm{S})(\mathrm{S})$ à des sous-p-algèbres de Lie de $\mathrm{U}(\mathrm{G})$ et $\mathrm{U}(\mathrm{H})$. Comme $\mathrm{U}(\phi)$ est un homomorphisme d'algèbres, on voit donc que $\underline{\mathrm{Lie}}(\phi/\mathrm{S})(\mathrm{S})$ est un homomorphisme de p-algèbres de Lie.

De même, si $s : \mathrm{T} \to \mathrm{S}$ est un changement de base, l'application de $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ dans $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{T})$, qui est induite par s, est un homomorphisme de p-algèbres de Lie. On peut traduire cela en disant que le foncteur $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})$ est muni d'une structure de
454 $\mathbf{O}_{\mathrm{S}}$-p-algèbre de Lie. En particulier, lorsque T parcourt les ouverts de S, on voit que le faisceau $\mathscr{L}ie(\mathrm{G}/\mathrm{S})$ est muni d'une structure de $\mathscr{O}_{\mathrm{S}}$-p-algèbre de Lie.

6.2. Suivant une idée de Demazure, nous allons maintenant généraliser ce qui précède à certains S-foncteurs en groupes non nécessairement représentables. Pour cela, nous allons d'abord donner une autre définition de la puissance p-ième symbolique dans l'algèbre de Lie d'un S-schéma en groupes G.

Soit D une dérivation de G à l'origine ; [58] d'après 1.2.1, D est la composée de la S-dérivation $\delta = (\tau, \partial_t)$ de la section zéro $\tau : \mathrm{S} \to \mathrm{I}_{\mathrm{S}}$, et d'un morphisme $x : \mathrm{I}_{\mathrm{S}} \to \mathrm{G}$ tel que $x \circ \tau = \varepsilon$ (i.e. $x \in \underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$). D'après la définition que nous avons donnée en 2.1, D^p est la déviation composée suivante :

$$\mathrm{S} \simeq \underbrace{\mathrm{S} \times \mathrm{S} \times \cdots \times \mathrm{S}}_{p} \xrightarrow{\delta \times \cdots \times \delta} \mathrm{I}_{\mathrm{S}} \times \cdots \times \mathrm{I}_{\mathrm{S}} \xrightarrow{x \times \cdots \times x} \mathrm{G} \times \cdots \times \mathrm{G} \xrightarrow{m^{(p)}} \mathrm{G}$$

où $m^{(p)}$ est le morphisme induit par la multiplication $m : \mathrm{G} \times \mathrm{G} \to \mathrm{G}$. Comme $\mathrm{I}_{\mathrm{S}} \times \cdots \times \mathrm{I}_{\mathrm{S}}$ est affine sur S et a pour algèbre affine $\mathscr{B} = \mathscr{O}_{\mathrm{S}}[d_1, \ldots, d_p]/(d_1^2, \ldots, d_p^2)$, la déviation $\delta \times \cdots \times \delta$ est définie par le morphisme de $\mathscr{O}_{\mathrm{S}}$-modules

$$\phi : \quad \mathscr{B} \longrightarrow \mathscr{O}_{\mathrm{S}}$$

qui envoie sur 1 le monôme $d_1 d_2 \cdots d_p$, et sur 0 les autres monômes $d_{i_1} \cdots d_{i_r}$, pour $0 \leqslant r < p$. D'autre part, si pr_i désigne la projection de $\mathrm{I}_{\mathrm{S}}^p$ sur le i-ième facteur et si x_i est

[57] N.D.E. : On peut aussi montrer directement (sans l'intermédiaire de $\mathrm{Dif}_{\mathrm{G}/\mathrm{S}}$) que l'algèbre de Lie des dérivations de G à l'origine (isomorphe à $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ d'après 2.5) est stable par l'élévation à la puissance p dans $\mathrm{U}(\mathrm{G})$: ceci est fait en 6.2 ci-dessous.

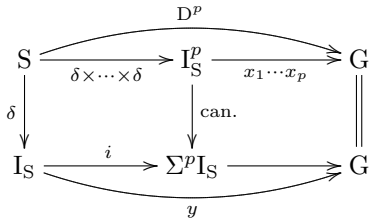
[58] N.D.E. : On a détaillé l'original dans ce qui suit.

l'image dans $G(I_S^p)$ de x par $G(\mathrm{pr}_i)$, alors le morphisme composé $m^{(p)} \circ (x \times \cdots \times x)$ n'est autre que le produit $x_1 x_2 \cdots x_p$. Par conséquent, D^p est aussi la déviation composée suivante :

$$S \xrightarrow{\delta \times \cdots \times \delta} I_S \times \cdots \times I_S \xrightarrow{x_1 x_2 \cdots x_p} G.$$

Cette description nous permet de redémontrer que D^p est une dérivation de G à **455** l'origine. En effet, comme G est un très bon groupe (II 4.11), les images $G(\mathrm{pr}_1)(x)$ et $G(\mathrm{pr}_2)(x)$ de x dans $G(I_S \times I_S)$ commutent entre elles. Il s'ensuit que les éléments x_i de $G(I_S^p)$ commutent deux à deux et donc, pour toute permutation γ des facteurs de I_S^p, on a $(x_1 \cdots x_p) \circ \gamma = x_1 \cdots x_p$; il s'ensuit que $x_1 \cdots x_p$ se factorise à travers la projection canonique de I_S^p dans le produit symétrique $\Sigma^p I_S$ (cf. 4.2).

Le produit symétrique $\Sigma^p I_S$ a pour algèbre affine la sous-algèbre $\mathscr{A}$ de $\mathscr{B}$ qui a pour base sur $\mathscr{O}_S$ les fonctions symétriques élémentaires $1 = \sigma_0, \sigma_1, \ldots, \sigma_p$ de $d_1, \ldots, d_p$. Notons κ l'inclusion $\mathscr{A} \hookrightarrow \mathscr{B}$ et π le morphisme de $\mathscr{O}_S$-algèbres $\mathscr{A} \to \mathscr{O}_S[t]/(t^2)$ qui annule $\sigma_1, \ldots, \sigma_{p-1}$ et envoie σ_p sur t ; alors on a $\phi \circ \kappa = \partial_t \circ \pi$ (on rappelle que $\partial_t : \mathscr{O}_S[t]/(t^2) \to \mathscr{O}_S$ est le morphisme de $\mathscr{O}_S$-modules qui annule 1 et envoie t sur 1). Par conséquent, notant i l'immersion fermée $I_S \hookrightarrow \Sigma^p I_S$ définie par π, on a un diagramme commutatif :



qui montre que D^p est de la forme $y \circ \delta$, donc est bien une dérivation de G à l'origine.

6.3. Soient $\mathscr{S}_p$ le groupe symétrique d'ordre p et $I_S^p \times \mathscr{S}_p$ la somme directe d'une famille d'exemplaires de I_S^p indexés par $\mathscr{S}_p$. Nous notons $\pi : I_S^p \times \mathscr{S}_p \to I_S^p$ la projection canonique et

$$\mu : I_S^p \times \mathscr{S}_p \longrightarrow I_S^p$$

le morphisme définissant l'opération de $\mathscr{S}_p$ sur I_S^p (c.-à-d., si τ est un élément de $\mathscr{S}_p$, la restriction de μ à $I_S^p \times \tau$ a $\mathrm{pr}_{\tau(j)}$ pour j-ième composante). Ceci étant, nous posons la définition suivante :

Définition. — Un foncteur $X : (\mathbf{Sch}_{/S})^\circ \to (\mathbf{Ens})$ vérifie la condition (F) si : **456**

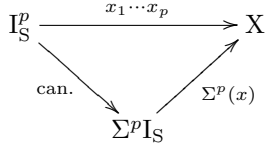
a) X transforme les sommes directes finies en produits directs,

b) pour tout S-schéma T, la suite ci-dessous est exacte :

$$X(T \times \Sigma^p I_S) \longrightarrow X(T \times I_S^p) \underset{X(\mathrm{id}_T \times \mu)}{\overset{X(\mathrm{id}_T \times \pi)}{\rightrightarrows}} X(T \times I_S^p \times \mathscr{S}_p).$$

Tout S-schéma vérifie (F) ; si $\mathscr{F}$ est un $\mathscr{O}_S$-module, $\mathbf{W}(\mathscr{F})$ vérifie (F) ; toute limite projective de foncteurs vérifiant (F), vérifie aussi (F) ; si Y vérifie (F) et si X est un S-foncteur quelconque, $\underline{\mathrm{Hom}}_S(X, Y)$ vérifie (F).

Soit X *un très bon groupe* (II 4.10) *vérifiant la condition* (F). Désignant par $x : \mathrm{I_S} \to \mathrm{X}$ un morphisme qui prolonge la section unité de X et reprenant les notations de 6.2, on voit comme ci-dessus que $x_1 \cdots x_p : \mathrm{I_S^p} \to \mathrm{X}$ se factorise à travers $\Sigma^p \mathrm{I_S}$:



et définit par composition un morphisme

$$x^{(p)} : \mathrm{I_S} \xrightarrow{i} \Sigma^p \mathrm{I_S} \xrightarrow{\Sigma^p(x)} \mathrm{X}$$

que nous appellerons la *puissance p-ième symbolique de x.*

L'endomorphisme $x \mapsto x^{(p)}$ de $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ est évidemment compatible avec les changements de base et est fonctoriel en G. Il serait intéressant de savoir pour quels G cet endomorphisme fait de $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ une p-algèbre de Lie.

457 **6.4.** La dernière définition de la puissance p-ième symbolique, que nous venons de donner, est particulièrement bien adaptée au calcul. Voici quelques exemples :

6.4.1. — Soient M un groupe abélien « abstrait » et $\mathrm{D_S(M)}$ le S-groupe diagonalisable de type M (I 4.4.2). Pour tout S-schéma T, on a donc

$$\mathrm{D_S(M)(T)} = \mathrm{Hom_{(Ab)}(M, \mathscr{O}(T)^\times)}.$$

Soit x un élément de $\underline{\mathrm{Lie}}(\mathrm{D_S(M)/S})(\mathrm{S})$, c'est-à-dire un homomorphisme de groupes abéliens

$$\mathrm{M} \xrightarrow{x} \Gamma(\mathrm{S}, \mathscr{O}_\mathrm{S} + d\mathscr{O}_\mathrm{S})^\times$$

de la forme $m \mapsto 1 + d\,\xi(m)$, où $\xi \in \mathrm{Hom_{(Ab)}(M, \mathscr{O}(S))}$. Avec les notations de 6.2 et 6.3, le produit $x_1 \cdots x_p$ associe à un élément m de M l'expression

$$(1 + d_1\,\xi(m)) \cdots (1 + d_p\,\xi(m))$$

c'est-à-dire $1 + \sigma_1\,\xi(m) + \sigma_2\,\xi(m)^2 + \cdots + \sigma_p\,\xi(m)^p$.

Cette expression appartient bien à $\mathscr{O}(\Sigma^p \mathrm{I_S})$. Projetant ceci dans $\mathscr{O}(\mathrm{S})[d]/(d^2)$ en annulant $\sigma_1, \ldots, \sigma_{p-1}$ et en envoyant σ_p sur d, on voit que $x^{(p)}$ est l'homomorphisme de M dans $\Gamma(\mathrm{S}, \mathscr{O}_\mathrm{S} + d\mathscr{O}_\mathrm{S})^\times$ suivant :

$$m \mapsto 1 + d\,\xi(m)^p.$$

En résumé, si l'on identifie $\underline{\mathrm{Lie}}(\mathrm{D_S(M)/S})(\mathrm{S})$ à $\mathrm{Hom_{(Ab)}(M, \mathscr{O}(S))}$ comme en II 5.1, la puissance p-ième symbolique associe à ξ l'homomorphisme $\xi^{(p)} : m \mapsto \xi(m)^p$.

458 ***6.4.2***. — Soient $\mathscr{F}$ un $\mathscr{O}_\mathrm{S}$-module et G le S-foncteur en groupes abéliens $\mathbf{W}(\mathscr{F})$ (cf. I, 4.6). Soient y un élément de $\mathbf{W}(\mathscr{F})(\mathrm{S}) = \Gamma(\mathrm{S}, \mathscr{F})$ et y' son image dans $\mathbf{W}(\mathscr{F})(\mathrm{I_S})$ par $\mathbf{W}(\mathscr{F})(\mathrm{I_S} \to \mathrm{S})$.

On sait (cf. II, 4.4.2 et 4.5.1) que l'application $y \mapsto d\,y'$ est un isomorphisme de $\mathscr{O}(\mathrm{S})$-modules de $\mathbf{W}(\mathscr{F})(\mathrm{S})$ sur $\underline{\mathrm{Lie}}(\mathbf{W}(\mathscr{F})/\mathrm{S})(\mathrm{S})$. Si l'on pose $x = d\,y'$, la quantité x_i

de 6.2 n'est autre que $d_i\, y''$, où y'' désigne l'image canonique de y' [59] dans $\mathbf{W}(\mathscr{F})(\mathrm{I}_{\mathrm{S}}^p)$. Par conséquent le produit $x_1 \cdots x_p$ est égal ici à

$$x_1 + \cdots + x_p = (d_1 + \cdots + d_p)y'' = \sigma_1 y''$$

et appartient à $\mathbf{W}(\mathscr{F})(\Sigma^p \mathrm{I}_{\mathrm{S}})$. Comme l'homomorphisme $\mathscr{O}(\Sigma^p \mathrm{I}_{\mathrm{S}}) \to \mathscr{O}(\mathrm{I}_{\mathrm{S}})$, qui définit le morphisme i de 6.1, annule σ_1, on voit que $x^{(p)}$ est nul. Donc :

Pour tout $\mathscr{O}_{\mathrm{S}}$-module $\mathscr{F}$, l'opération $x \mapsto x^{(p)}$ dans $\underline{\mathrm{Lie}}\, \mathbf{W}(\mathscr{F})$ est nulle.

6.4.3. — Soient X un S-schéma, G le S-foncteur en groupes $\underline{\mathrm{Aut}}_{\mathrm{S}}\, \mathrm{X}$ et D une S-dérivation du faisceau structural $\mathscr{O}_{\mathrm{X}}$. D'après 1.5, D peut être identifié à un I_{S}-automorphisme x de $\mathrm{X}_{\mathrm{I}_{\mathrm{S}}}$, induisant l'identité sur X, qu'on peut décrire comme suit. Si f est une section de $\mathscr{O}_{\mathrm{S}}[d]/(d^2)$ de la forme $a + bd$, posons $\mathrm{D}_{\mathrm{I}_{\mathrm{S}}} f = \mathrm{D}a + (\mathrm{D}b)d$; autrement dit, $\mathrm{D}_{\mathrm{I}_{\mathrm{S}}}$ est déduit de D par le changement de base $\mathrm{I}_{\mathrm{S}} \to \mathrm{S}$; alors l'automorphisme en question de $\mathrm{X}_{\mathrm{I}_{\mathrm{S}}}$ est associé à l'endomorphisme $f \mapsto f + (\mathrm{D}_{\mathrm{I}_{\mathrm{S}}} f)d = a + (\mathrm{D}(a) + b)d$ de $\mathscr{O}_{\mathrm{S}}[d]/(d^2)$.

De même, soit $\mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p}$ l'opérateur différentiel de $\mathrm{X}_{\mathrm{I}_{\mathrm{S}}^p}$ déduit de D par le changement de base $\mathrm{I}_{\mathrm{S}}^p \to \mathrm{S}$. Avec les notations de 6.2, l'automorphisme x_i de $\mathrm{X}_{\mathrm{I}_{\mathrm{S}}^p}$ est alors associé à l'endomorphisme $f \mapsto f + (\mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p} f)d_i$ de $\mathscr{O}_{\mathrm{S}}[d_1, \ldots, d_p]/(d_1^2, \ldots, d_p^2)$. Le produit $x_1 \cdots x_p$ est donc associé à l'endomorphisme

$$(1 + d_1 \mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p})(1 + d_2 \mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p}) \cdots (1 + d_p \mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p})$$

c'est-à-dire, à $1 + \sigma_1\, \mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p} + \sigma_2\, \mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p}^2 + \cdots + \sigma_p\, \mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p}^p$. **459**

Le coefficient de σ_p est $\mathrm{D}_{\mathrm{I}_{\mathrm{S}}^p}^p$, ce qui signifie que l'isomorphisme d'algèbres de Lie $\mathrm{Dér}_{\mathrm{S}}(\mathscr{O}_{\mathrm{X}}) \xrightarrow{\sim} \mathrm{Lie}(\underline{\mathrm{Aut}}_{\mathrm{S}}\, \mathrm{X})$, $\mathrm{D} \mapsto x$ (cf. 1.5), est aussi un isomorphisme de p-algèbres de Lie.

6.4.4. — En utilisant la même méthode, on voit que, pour tout $\mathscr{O}_{\mathrm{S}}$-module $\mathscr{F}$, l'isomorphisme

$$\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}_{\mathbf{O}_{\mathrm{S}}\text{-mod.}}\, \mathbf{W}(\mathscr{F})/\mathrm{S})(\mathrm{S}) \xrightarrow{\sim} (\underline{\mathrm{End}}_{\mathbf{O}_{\mathrm{S}}\text{-mod.}}\, \mathbf{W}(\mathscr{F}))(\mathrm{S}).$$

d'algèbres de Lie (cf. II 4.8) est aussi un isomorphisme de p-algèbres de Lie.

6.4.5. — [60] Soient $\mathscr{U}$ une $\mathscr{O}_{\mathrm{S}}$-coalgèbre en groupes et G le S-foncteur en groupes $\mathrm{Spec}^*\, \mathscr{U}$, supposons que G soit *représentable*. Dans ce cas, pour tout $\mathrm{T} \to \mathrm{S}$, on a défini en 5.5 et 6.1.1 deux structures de p-algèbre de Lie sur $\mathrm{L}(\mathrm{T}) = \underline{\mathrm{Lie}}(\mathrm{G})(\mathrm{T})$. Comme on a un diagramme commutatif

$$\begin{array}{ccc} \mathrm{L}(\mathrm{T}) & \xrightarrow{\tau} & \Gamma(\mathrm{T}, \mathscr{U}_{\mathrm{T}}) \\ \downarrow{\scriptstyle \alpha} & \searrow^{i} & \uparrow{\scriptstyle \psi} \\ \mathrm{U}(\mathrm{G}_{\mathrm{T}}) & \xleftarrow{\phi} & \mathrm{U}(\mathrm{L}(\mathrm{T})) \end{array}$$

[59] N.D.E. : on a corrigé x en y'.

[60] N.D.E. : On a ajouté la numérotation 6.4.5, et détaillé l'original.

où U(L(T)) est l'algèbre enveloppante de L(T) et ϕ, ψ les morphismes d'algèbres induits par α, τ, on voit que les deux structures de p-algèbres de Lie coïncident : si on identifie $x \in \mathrm{L(T)}$ à son image dans $\mathrm{U(G_T)}$ (resp. $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$), alors $x^{(p)}$ est l'image de l'élément x^p de U(L(T)) par ϕ (resp. ψ).

7. Groupes radiciels de hauteur 1

460

(61) Soit S un schéma de caractéristique $p > 0$. Nous dirons qu'une $\mathscr{O}_\mathrm{S}$-algèbre $\mathscr{A}$ (resp. une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie $\mathscr{L}$) est *finie localement libre* si le $\mathscr{O}_\mathrm{S}$-module sous-jacent à $\mathscr{A}$ (resp. $\mathscr{L}$) est localement libre et de type fini. Si $\mathscr{L}$ est une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie finie localement libre, nous savons (cf. 5.5.2) que le S-foncteur en groupes $\mathrm{Spec}^*\, \mathscr{U}_p(\mathscr{L})$ est représenté par un S-schéma en groupes $\mathrm{G}_p(\mathscr{L})$, fini et localement libre . Nous allons voir que ce S-schéma en groupes est solution d'un problème universel (7.2) et nous allons caractériser les S-schémas en groupes de la forme $\mathrm{G}_p(\mathscr{L})$ (7.4).

Définition 7.0. — (62) Soit $\mathrm{H} = \mathrm{Spec}\, \mathscr{A}$ un S-schéma en groupes fini localement libre. On dit que H est *infinitésimal* si la section unité $\varepsilon_\mathrm{H} : \mathrm{S} \to \mathrm{H}$ est un homéomorphisme, ce qui équivaut à dire que l'idéal d'augmentation de $\mathscr{A}$ est localement nilpotent.

7.1. (63) Soit $\mathscr{L}$ une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie finie localement libre et soit $\mathrm{G}_p(\mathscr{L})$ le S-groupe affine $\mathrm{Spec}\, \mathscr{U}_p(\mathscr{L})$. D'après 5.5, on sait que $\mathscr{L}$ s'identifie à $\mathscr{L}ie\, \mathrm{G}_p(\mathscr{L})$.

Considérons maintenant un très bon S-foncteur en groupes G vérifiant la condition (F) de 6.3 et soit $\phi : \mathrm{G}_p(\mathscr{L}) \to \mathrm{G}$ un morphisme de S-foncteurs en groupes. D'après 6.3, le morphisme de $\mathscr{O}_\mathrm{S}$-algèbres de Lie $\mathscr{L}ie\, \phi : \mathscr{L}ie\, \mathrm{G}_p(\mathscr{L}) \to \mathscr{L}ie\, \mathrm{G}$ est compatible
461 avec la puissance p-ième symbolique. Si nous notons $\mathrm{Hom}_p(\mathscr{L}, \mathscr{L}ie\, \mathrm{G})$ l'ensemble des morphismes de $\mathscr{O}_\mathrm{S}$-algèbres de Lie, qui sont compatibles avec la puissance p-ième symbolique, on a donc une application

$$\mathscr{L}ie : \mathrm{Hom}_{\text{S-Gr.}}(\mathrm{G}_p(\mathscr{L}), \mathrm{G}) \longrightarrow \mathrm{Hom}_p(\mathscr{L}, \mathscr{L}ie\, \mathrm{G}), \qquad \phi \mapsto \mathscr{L}ie\, \phi.$$

7.2. Théorème. — *Si $\mathscr{L}$ est une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie finie localement libre, l'application*

$$\mathrm{Hom}_{\text{S-gr.}}(\mathrm{G}_p(\mathscr{L}), \mathrm{G}) \longrightarrow \mathrm{Hom}_p(\mathscr{L}, \mathscr{L}ie\, \mathrm{G})$$

est bijective dans chacun des cas suivants :

(i) G *est un* S*-schéma en groupes ;*

(ii) G *est de la forme* $\underline{\mathrm{Aut}}_\mathrm{S}\, \mathrm{X}$*, où* X *est un* S*-schéma ;*

(iii) G *est de l'une des formes* $\mathbf{W}(\mathscr{F})$ *ou* $\underline{\mathrm{Aut}}_{\mathbf{O}_\mathrm{S}\text{-mod}}\, \mathbf{W}(\mathscr{F})$*, où* $\mathscr{F}$ *désigne un* $\mathscr{O}_\mathrm{S}$*-module quasi-cohérent.*

La démonstration du théorème s'appuie sur le lemme suivant :

---

(61) N.D.E. : Pour les résultats de cette section, on peut aussi se reporter à [**DG70**], § II.7, n$^{\text{os}}$ 3-4.
(62) N.D.E. : On a ajouté cette définition (cf. [**DG70**], § II.4, 7.1), qui sera utilisée en 7.2.1.
(63) N.D.E. : On a simplifié l'original, en tenant compte des ajouts faits en 5.5.

Lemme. — *Si $\mathscr{L}$ est une $\mathscr{O}_S$-p-algèbre de Lie finie localement libre, le* S*-groupe* $G = G_p(\mathscr{L})$ *est annulé par le morphisme de Frobenius* $\mathrm{Fr} : G \to G^{(p)}$. *En particulier,* G *est infinitésimal.*

(64) Soient en effet $\mathscr{U}$ l'algèbre enveloppante restreinte de $\mathscr{L}$, $\mathscr{A} = \mathscr{U}^*$ l'algèbre affine de G, et $\mathscr{I} = \mathrm{Ker}\,\varepsilon_{\mathscr{A}}$ l'idéal d'augmentation de $\mathscr{A}$. On a

$$\mathscr{A} = \mathscr{I} \oplus \eta_{\mathscr{A}}(\mathscr{O}_S)\,, \tag{1}$$

où $\eta_{\mathscr{A}}$ désigne la section unité de $\mathscr{A}$, et comme $\varepsilon_{\mathscr{A}}$ (resp. $\eta_{\mathscr{A}}$) est la transposée de $\eta_{\mathscr{U}}$ (resp. $\varepsilon_{\mathscr{U}}$), cette décomposition correspond par dualité à la décomposition

$$\mathscr{U} = \mathscr{J} \oplus \eta_{\mathscr{U}}(\mathscr{O}_S)\,, \tag{2}$$

où $\mathscr{J}$ est l'idéal d'augmentation de $\mathscr{U}$; on a donc $\mathscr{J} = \mathscr{I}^*$.

Notons π l'endomorphisme $x \mapsto x^p$ de $\mathscr{O}_S$. Nous devons montrer que le morphisme $\mathrm{Fr} : G \to G^{(p)}$ se factorise à travers la section unité de $G^{(p)}$, ce qui équivaut à dire (cf. 4.1.4 (c)) que le morphisme $\Phi : a \otimes_\pi x \mapsto a^p\, x$ de $\mathscr{I} \otimes_\pi \mathscr{O}_S$ dans $\mathscr{A}$ est nul. Comme $\mathscr{A}$ est fini localement libre sur $\mathscr{O}_S$, il suffit de voir que le morphisme transposé ${}^t\Phi$ est nul.

Or Φ n'est autre que le composé suivant

$$\mathscr{I} \otimes_\pi \mathscr{O}_S \xrightarrow{\tau} \mathscr{A} \otimes_\pi \mathscr{O}_S \xrightarrow{j(\mathscr{A})} \mathcal{S}^p\mathscr{A} \xrightarrow{b(\mathscr{A})} \mathscr{A}\ ,$$

où τ est déduit de l'inclusion $\mathscr{I} \hookrightarrow \mathscr{A}$, et $b(\mathscr{A})$ et $j(\mathscr{A})$ sont définis comme en 4.3.3 (i.e. $b(\mathscr{A})$ est induit par la multiplication de $\mathscr{A}$ et $j(\mathscr{A})$ envoie $a \otimes_\pi 1$ sur l'image de $a \otimes \cdots \otimes a$ dans $\mathcal{S}^p\mathscr{A}$). Comme le $\mathscr{O}_S$-module dual de $\mathcal{S}^p\mathscr{A}$ n'est autre que le **462**
sous-module $\Sigma^p\mathscr{U}$ de $\bigotimes^p \mathscr{U}$ formé des sections invariantes sous l'action du groupe symétrique d'ordre p, on voit que ${}^t\Phi$ est le morphisme composé suivant :

$$\mathscr{U} \xrightarrow{a(\mathscr{U})} \Sigma^p\mathscr{U} \xrightarrow{r(\mathscr{U})} \mathscr{U} \otimes_\pi \mathscr{O}_S \xrightarrow{q} \mathscr{J} \otimes_\pi \mathscr{O}_S\ ,$$

où q est déduit de la projection $\mathscr{U} \to \mathscr{J}$ de noyau $\eta_{\mathscr{U}}(\mathscr{O}_S)$, $a(\mathscr{U})$ est induit par la comultiplication de $\mathscr{U}$ et $r(\mathscr{U})$ s'annule sur les tenseurs symétrisés et applique une section $x \otimes \cdots \otimes x$ sur $x \otimes_\pi 1$ (confer 4.3.3).

Il est clair que ${}^t\Phi \circ \eta_{\mathscr{U}} = 0$ et donc, d'après (2), il reste à voir que ${}^t\Phi$ annule l'idéal d'augmentation $\mathscr{J}$. Comme ${}^t\Phi$ est un morphisme d'algèbres et comme l'idéal $\mathscr{J}$ est engendré par $\mathscr{L}$ (identifiée à son image dans $\mathscr{U}$), il suffit de voir que ${}^t\Phi(x) = 0$ pour toute section x de $\mathscr{L}$. Or $-a(\mathscr{U})(x) = (p-1)!\; a(\mathscr{U})(x)$ est le symétrisé de $x \otimes 1 \otimes \cdots \otimes 1$, donc son image par $r(\mathscr{U})$ est nulle. Ceci prouve la première assertion du lemme.

La seconde en découle. En effet, comme toute section locale de $\mathscr{I}$ est de puissance p-ième nulle et comme $\mathscr{I}$ est un $\mathscr{O}_S$-module de type fini, $\mathscr{I}$ est localement nilpotent (explicitement, si V est un ouvert affine de S tel que $I = \Gamma(V, \mathscr{I})$ soit engendré par r éléments, alors $I^{r(p-1)+1} = 0$), d'où $G_{\text{réd}} = S_{\text{réd}}$ et donc la section unité $\varepsilon_G : S \to G$ est un homéomorphisme.

(64) N.D.E. : On a détaillé l'original dans ce qui suit. Pour une autre démonstration, voir [**DG70**], §II.7, 3.9.

7.2.1. — [(65)] Nous allons d'abord prouver l'assertion (ii) du théorème 7.2. Soit $\pi : X \to S$ un S-schéma. Considérons d'abord un S-groupe infinitésimal H arbitraire. Les morphismes ϕ de H dans $\underline{\mathrm{Aut}}\, X$ correspondent bijectivement aux opérations à gauche $\mu : H \times X \to X$ de H sur X. Pour une telle opération, si ε est la section unité de H, le morphisme composé

$$X \simeq S \times X \xrightarrow{\varepsilon \times X} H \times X \xrightarrow{\mu} X$$

doit être l'identité. Comme $(H \times X)_{\text{réd}}$ s'identifie à $X_{\text{réd}}$, on voit que μ doit induire l'identité sur les schémas réduits associés. En particulier, μ induit une opération de H sur chaque ouvert de X, et l'on obtient donc, pour tout ouvert U de X, affine sur S, un morphisme d'algèbres associatives unitaires :

$$\mathscr{A}(U) \longrightarrow \mathscr{A}(H) \otimes \mathscr{A}(U)$$

faisant de $\mathscr{A}(U)$ un $\mathscr{A}(H)$-comodule à gauche, ceci de façon que les applications de restrictions $\mathscr{A}(U) \to \mathscr{A}(U')$, pour $U' \subset U$, soient des morphismes de comodules. Réciproquement, toute donnée de ce type provient d'une unique action à gauche $\mu : H \times X \to X$. D'autre part, on a le lemme suivant :

463 ***Lemme***. — *Soient* $X = \mathrm{Spec}\,\mathscr{C}$ *un* S*-schéma affine,* $H = \mathrm{Spec}\,\mathscr{A}$ *un* S*-groupe infinitésimal, et* $\mathscr{U} = \mathscr{A}^* = \mathscr{H}om_{\mathscr{O}_S}(\mathscr{A}, \mathscr{O}_S)$. *Les opérations à gauche de* H *sur* X *correspondent bijectivement aux représentations de l'algèbre* $\mathscr{U}$ *dans le* $\mathscr{O}_S$*-module* $\mathscr{C}$ *telles qu'on ait :*

$$\text{(a)} \qquad u(1_{\mathscr{C}}) = \varepsilon(u) \cdot 1_{\mathscr{C}}$$

$$\text{(b)} \qquad u(xy) = \sum_i v_i(x) w_i(y) \quad si \quad \Delta u = \sum_i v_i \otimes w_i.$$

(Dans les formules ci-dessus, u désigne une section quelconque de $\mathscr{U}$ sur un ouvert affine V de S, x et y des sections de $\mathscr{C}$ sur V ; on désigne par $1_{\mathscr{C}}$ la section unité de $\mathscr{C}$, par ε et Δ l'augmentation et le morphisme diagonal de $\mathscr{U}$.) En effet, une opération à gauche μ de H sur X est définie par un morphisme d'algèbres associatives unitaires :

$$\lambda : \mathscr{C} \longrightarrow \mathscr{A} \otimes \mathscr{C}$$

faisant de $\mathscr{C}$ un $\mathscr{A}$-comodule à gauche. Nous noterons α le morphisme composé

$$\mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{C} \xrightarrow{\mathscr{U} \otimes \lambda} \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{A} \otimes_{\mathscr{O}_S} \mathscr{C} \xrightarrow{\gamma \otimes \mathscr{C}} \mathscr{O}_S \otimes_{\mathscr{O}_S} \mathscr{C} \simeq \mathscr{C}$$

où γ est la « contraction » de $\mathscr{A}^* \otimes_{\mathscr{O}_S} \mathscr{A}$ dans $\mathscr{O}_S$. Comme $\mathscr{A}$ est finie localement libre sur $\mathscr{O}_S$, on sait que l'application $\lambda \mapsto (\gamma \otimes \mathscr{C})(\mathscr{U} \otimes \lambda)$ est une bijection de $\mathrm{Hom}_{\mathscr{O}_S}(\mathscr{C}, \mathscr{A} \otimes \mathscr{C})$ sur $\mathrm{Hom}_{\mathscr{O}_S}(\mathscr{U} \otimes \mathscr{C}, \mathscr{C})$. De plus, on voit facilement que la condition que λ définisse une structure de $\mathscr{A}$-comodule à gauche (resp. soit un morphisme d'algèbres associatives unitaires) équivaut, par dualité, à la condition que α soit une représentation de $\mathscr{U}$ dans $\mathscr{C}$ (resp. que α vérifie les conditions (a) et (b)). Ceci prouve le lemme.

(65) N.D.E. : On a détaillé l'original dans ce qui suit.

De plus, il est clair que, pour toute représentation de $\mathscr{U}$ dans le $\mathscr{O}_S$-module $\mathscr{C}$, les sections u de $\mathscr{U}$ qui vérifient les conditions (a) et (b) du lemme forment une sous-algèbre de $\mathscr{U}$.

Dans le cas particulier $H = G_p(\mathscr{L})$ qui nous intéresse, ces conditions seront donc satisfaites pour toutes les sections u de $\mathscr{U} = \mathscr{U}_p(\mathscr{L})$, si elles sont vraies pour les sections u de $\mathscr{L}$ (en identifiant $\mathscr{L}$ à son image dans $\mathscr{U}_p(\mathscr{L})$). Or, si u est une section de $\mathscr{L}$, les conditions (a) et (b) signifient simplement que $u(1_{\mathscr{C}}) = 0$ et que $u(xy) = u(x)y + xu(y)$, i.e. que $\alpha(u)$ est une $\mathscr{O}_S$-dérivation de $\mathscr{C} = \mathscr{A}(X)$. L'assertion (ii) de 7.2 en découle. En effet, tout morphisme ϕ de $G_p = G_p(\mathscr{L})$ dans $\underline{\mathrm{Aut}}\, X$ définit **464**
un morphisme de p-algèbres de Lie $\mathscr{L}ie\,\phi$ de $\mathscr{L} = \mathscr{L}ie\, G_p$ dans $\pi_*(\mathscr{D}ér_{\mathscr{O}_S}\mathscr{O}_X)$, et réciproquement toute donnée de ce type provient, d'après ce qui précède, d'une unique action $\mu : G \times X \to X$.

7.2.2. — Montrons maintenant comment l'assertion (i) du théorème 7.2 résulte de (ii). Soit G un S-schéma en groupes. Si T est un S-schéma et x un élément de G(T), nous notons ℓ_x^T (resp. r_x^T) la translation à gauche (resp. à droite) de G_T qui est définie par x. Les applications $\ell^T : x \mapsto \ell_x^T$ déterminent donc un homomorphisme ℓ de G dans $\underline{\mathrm{Aut}}\, G$. Soit d'autre part f un T-automorphisme de G_T ; on définit alors xf comme étant égal à $(r_x^T)^{-1} f r_x^T$, i.e. pour tout $T' \to T$ et $g \in G(T')$, $(xf)(g) = f(gx)x^{-1}$. De cette façon G opère à gauche sur le S-foncteur en groupes $\underline{\mathrm{Aut}}\, G$, donc aussi sur les foncteurs $T \mapsto \mathrm{Hom}_{T\text{-Gr.}}(G_p(\mathscr{L}_T), \underline{\mathrm{Aut}}\, G_T)$ et $T \mapsto \mathrm{Hom}_p(\mathscr{L}_T, \mathscr{L}ie(\underline{\mathrm{Aut}}\, G_T/T))$. D'autre part, le morphisme $\ell_T : G_T \to \underline{\mathrm{Aut}}\, G_T$ identifie G_T au groupe des automorphismes du T-schéma G_T commutant aux translations à droite, et le morphisme dérivé $\mathscr{L}ie(\ell_T)$ identifie $\mathscr{L}ie\, G_T$ à la p-algèbre de Lie des $\mathscr{O}_T$-dérivations de $\mathscr{O}_{G_T}$ commutant aux translations à droite (cf. II, 4.11.1) ; ils induisent donc des carrés commutatifs

$$\begin{array}{ccc} \mathrm{Hom}_{T\text{-Gr.}}(G_p(\mathscr{L}_T), G_T) & \xrightarrow{\mathscr{L}ie} & \mathrm{Hom}_p(\mathscr{L}_T, \mathscr{L}ie(G_T/T)) \\ \Big\downarrow{\scriptstyle \ell_T} & & \Big\downarrow{\scriptstyle \mathscr{L}ie\,\ell_T} \\ \mathrm{Hom}_{T\text{-Gr.}}(G_p(\mathscr{L}_T), \underline{\mathrm{Aut}}\, G_T) & \xrightarrow{\mathscr{L}ie} & \mathrm{Hom}_p(\mathscr{L}_T, \mathscr{L}ie(\underline{\mathrm{Aut}}\, G_T/T)). \end{array}$$

Les images des deux flèches verticales sont les sous-foncteurs formés des invariants sous l'action du S-groupe G. Comme la flèche horizontale du bas est inversible d'après 7.2.1 et qu'elle est compatible avec l'action de G, la flèche horizontale du haut est aussi inversible. Ceci prouve 7.2 (i).

7.2.3. — Considérons maintenant le cas où $G = \underline{\mathrm{Aut}}_{\mathbf{O}_S\text{-mod.}}\, \mathbf{W}(\mathscr{F})$. [(66)] Posons $\mathscr{U} =$ **465**
$\mathscr{U}_p(\mathscr{L})$, $\mathscr{A} = \mathscr{U}^*$ et $H = G_p(\mathscr{L}) = \mathrm{Spec}\,\mathscr{A}$. Comme H est affine sur S alors, d'après VI_B 11.6.1, un morphisme de S-groupes de H dans $\underline{\mathrm{Aut}}_{\mathbf{O}_S\text{-mod.}}\, \mathbf{W}(\mathscr{F})$ est la même chose qu'une structure de $\mathscr{A}$-comodule à droite

$$\mu : \mathscr{F} \longrightarrow \mathscr{F} \otimes \mathscr{A}.$$

[(66)] N.D.E. : Dans ce qui suit, on a détaillé (et simplifié) l'original, en tenant compte de VI_B, 11.6.1.

De plus, comme $\mathscr{A}$ est finie localement libre sur $\mathscr{O}_S$, ceci équivaut à la donnée d'une représentation

$$\alpha : \mathscr{U} \longrightarrow \mathscr{E}nd_{\mathscr{O}_S}(\mathscr{F})$$

de $\mathscr{U}$ dans $\mathscr{F}$. Enfin, d'après la propriété universelle de $\mathscr{U} = \mathscr{U}_p(\mathscr{L})$, se donner un tel morphisme α équivaut à se donner sa restriction ρ à $\mathscr{L}$ (identifiée à son image dans $\mathscr{U}$), qui est un morphisme de p-algèbres de Lie de $\mathscr{L}$ dans $\mathscr{E}nd_{\mathscr{O}_S}(\mathscr{F})$.

(67) Enfin, considérons le cas où $G = \mathbf{W}(\mathscr{F})$, en gardant les notations précédentes. D'abord, se donner un morphisme de S-foncteurs $\phi : H \to \mathbf{W}(\mathscr{F})$ équivaut à se donner un élément θ de $\Gamma(H, \mathscr{F} \otimes \mathscr{O}_H)$, et comme H est fini localement libre sur S, on a :

$$\Gamma(H, \mathscr{F} \otimes \mathscr{O}_H) = \Gamma(S, \mathscr{F} \otimes \mathscr{A}) = \mathrm{Hom}_{\mathscr{O}_S}(\mathscr{U}, \mathscr{F}).$$

La condition que ϕ soit un morphisme de groupes se traduit alors par le fait que θ, considéré comme morphisme de $\mathscr{O}_S$-modules $\mathscr{U} \to \mathscr{F}$, s'annule sur $1_{\mathscr{U}}$ et sur $\mathscr{J} / \mathscr{J}^2$, où $\mathscr{J}$ est l'idéal d'augmentation de $\mathscr{U}$, d'où

$$\mathrm{Hom}_{S\text{-gr.}}(H, \mathbf{W}(\mathscr{F})) = \mathrm{Hom}_{\mathscr{O}_S}(\mathscr{J} / \mathscr{J}^2, \mathscr{F}). \tag{1}$$

D'autre part, considérons le faisceau quasi-cohérent $[\mathscr{L}, \mathscr{L}]$, image du morphisme $\mathscr{L} \otimes \mathscr{L} \to \mathscr{L}$, $x \otimes y \mapsto [x, y]$; pour tout ouvert affine V de S, on a $[\mathscr{L}, \mathscr{L}](V) = [\mathscr{L}(V), \mathscr{L}(V)]$. Alors on a une suite exacte

$$0 \longrightarrow [\mathscr{L}, \mathscr{L}] \longrightarrow \mathscr{L} \xrightarrow{\pi} \mathscr{J} / \mathscr{J}^2 \longrightarrow 0\ , \tag{†}$$

où π est la composée de l'inclusion $\mathscr{L} \hookrightarrow \mathscr{J}$ et de la projection $\mathscr{J} \to \mathscr{J} / \mathscr{J}^2$. En effet, la question étant locale sur S, on peut supposer que S est affine d'anneau R et que $L = \mathscr{L}(S)$ est libre de base $(x_1, \ldots, x_r)$. Identifiant L à son image dans $U = U_p(L)$, soit K le sous-R-module de U somme directe de $[L, L]$ et du sous-module de base les monômes $x_1^{n_1} \cdots x_r^{n_r}$ tels que $n_1 + \cdots + n_r \geqslant 2$; on vérifie alors que K est un idéal bilatère de U. Comme K est contenu dans J^2 (où J est l'idéal d'augmentation de U) et contient tous les produits $x_i x_j$ (qui engendrent J^2), on en déduit que $K = J^2$, d'où $J^2 \cap L = [L, L]$ et l'on a la suite exacte (†).

D'autre part, on sait d'après 6.4.2 que $\underline{\mathrm{Lie}}\, \mathbf{W}(\mathscr{F})$ n'est autre que $\mathbf{W}(\mathscr{F})$, le crochet de Lie et la puissance p-ième symbolique étant nuls. De ceci et de ce qui précède on déduit que

$$\mathrm{Hom}_p(\mathscr{L}, \mathscr{F}) = \mathrm{Hom}_{\mathscr{O}_S}(\mathscr{L}/[\mathscr{L}, \mathscr{L}], \mathscr{F}) = \mathrm{Hom}_{\mathscr{O}_S}(\mathscr{J} / \mathscr{J}^2, \mathscr{F}) \tag{2}$$

et ceci, combiné avec (1), achève la démonstration du théorème 7.2.

7.3. Lemme. — *Si $\mathscr{L}$ est une $\mathscr{O}_S$-p-algèbre de Lie finie localement libre, le morphisme*
466 *$j_{\mathscr{L}} : \mathscr{L} \to \mathscr{L}ie\, G_p(\mathscr{L})$ de* 5.5 *est inversible.*

(68) Pour la démonstration, voir 5.5.1.

(67) N.D.E. : On a ajouté ce qui suit. (L'original indiquait « le cas de $\mathbf{W}(\mathscr{F})$ est analogue »).

(68) N.D.E. : Pour ne pas modifier la numérotation, on a conservé l'énoncé 7.3, bien qu'on l'ait inclus, avec sa démonstration, dans 5.5.1.

7.4. Pour terminer cette section, nous allons donner une caractérisation des S-schémas en groupes de la forme $\mathrm{G}_p(\mathscr{L})$, où $\mathscr{L}$ est une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie finie localement libre.

Soient G un S-schéma en groupes, ε_G la section unité et $\mathscr{I}'$ le noyau du morphisme $\varepsilon_\mathrm{G}^{-1}(\mathscr{O}_\mathrm{G}) \to \mathscr{O}_\mathrm{S}$ correspondant à ε_G. L'image de $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ dans $\mathrm{U}(\mathrm{G})$ s'identifie, d'après 2.5 et 1.3.1, aux morphismes de $\mathscr{O}_\mathrm{S}$-modules de $\varepsilon_\mathrm{G}^{-1}(\mathscr{O}_\mathrm{G})$ dans $\mathscr{O}_\mathrm{S}$ qui s'annulent sur la section unité de $\varepsilon_\mathrm{G}^{-1}(\mathscr{O}_\mathrm{G})$ et sur $\mathscr{I}'^2$. On retrouve ainsi l'isomorphisme canonique de $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ sur $\mathrm{Hom}_{\mathscr{O}_\mathrm{S}}(\mathscr{I}'/\mathscr{I}'^2, \mathscr{O}_\mathrm{S})$ de II, 3.3 et 4.11.4. [(69)] Nous poserons $\omega_{\mathrm{G}/\mathrm{S}} = \mathscr{I}'/\mathscr{I}'^2$ comme dans *loc. cit.*, de sorte que le faisceau $\mathscr{L}ie(\mathrm{G}/\mathrm{S})$ s'identifie à $\omega_{\mathrm{G}/\mathrm{S}}^* = \mathscr{H}om_{\mathscr{O}_\mathrm{S}}(\omega_{\mathrm{G}/\mathrm{S}}, \mathscr{O}_\mathrm{S})$. [(70)] De plus, si $\mathrm{G} = \mathrm{G}_p(\mathscr{L})$, où $\mathscr{L}$ est une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie finie localement libre, on a vu en 5.5.3 que $\omega_{\mathrm{G}/\mathrm{S}} = \mathscr{L}^*$.

Théorème. — *Si* G *est un schéma en groupes sur un schéma* S *de caractéristique* $p > 0$*, les assertions suivantes sont équivalentes :*

(i) *Il existe une* $\mathscr{O}_\mathrm{S}$*-*p*-algèbre de Lie finie localement libre* $\mathscr{L}$ *telle que* $\mathrm{G} \simeq \mathrm{G}_p(\mathscr{L})$.

(i′) *La* $\mathscr{O}_\mathrm{S}$*-*p*-algèbre de Lie* $\mathscr{L}ie(\mathrm{G})$ *est finie localement libre et* $\mathrm{G} \simeq \mathrm{G}_p(\mathscr{L}ie(\mathrm{G}))$.

(ii) G *est affine sur* S*,* $\omega_{\mathrm{G}/\mathrm{S}}$ *est un* $\mathscr{O}_\mathrm{S}$*-module localement libre de type fini et l'algèbre affine de* G *est localement isomorphe au quotient de l'algèbre symétrique* $\mathscr{S}_{\mathscr{O}_\mathrm{S}}(\omega_{\mathrm{G}/\mathrm{S}})$ *par l'idéal engendré par les puissances* p*-ièmes des sections de* $\omega_{\mathrm{G}/\mathrm{S}}$.

(iii) G *est localement de présentation finie sur* S*, de hauteur* $\leqslant 1$*, et* $\omega_{\mathrm{G}/\mathrm{S}}$ *est localement libre.*

(iii′) G *est localement de type fini sur* S*, de hauteur* $\leqslant 1$*, et* $\omega_{\mathrm{G}/\mathrm{S}}$ *est localement libre.*

(iv) G *est localement de présentation finie et* plat *sur* S*, de hauteur* $\leqslant 1$. [(71)]

7.4.1. — L'équivalence (i) $\Leftrightarrow$ (i′) résulte de 5.5.3 (i), les implications (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iii′) sont claires, et l'on a (i) $\Rightarrow$ (iv) puisque $\mathrm{G}_p(\mathscr{L})$ est fini localement libre et de hauteur $\leqslant 1$, d'après 5.5.2 et le lemme 7.2. Montrons que (i) entraîne (ii). Notons $\mathscr{I}$ l'idéal d'augmentation de $\mathscr{A} = \mathscr{U}_p(\mathscr{L})^*$. On a déjà vu en 5.5.3 (ii) que $\omega_{\mathrm{G}/\mathrm{S}} = \mathscr{I}/\mathscr{I}^2$ s'identifie à $\mathscr{L}^*$, donc est fini localement libre. **467**

(69) N.D.E. : Si G est affine sur S et si $\mathscr{I}$ désigne l'idéal d'augmentation de $\mathscr{A}(\mathrm{G})$, alors $\mathscr{I}'/\mathscr{I}'^2$ s'identifie à $\varepsilon_\mathrm{G}^*(\mathscr{I}/\mathscr{I}^2)$, cf. *loc. cit.*

(70) N.D.E. : On a ajouté la phrase qui suit.

(71) N.D.E. : On ajouté, d'une part, l'assertion (i′), implicite dans l'original, et d'autre part, les assertions (iii′) et (iv), signalées par O. Gabber ; l'assertion (iv) reprend une note de bas de page de l'original, qui indiquait : « La condition sur $\omega_{\mathrm{G}/\mathrm{S}}$ est en fait inutile, comme on voit aisément en se ramenant au cas où S est local de corps résiduel k, et en appliquant le théorème au cas du groupe G_k ». Comme signalé par Gabber, ceci est inexact sans hypothèse de platitude : si A est un anneau local artinien de caractéristique $p > 0$ et J un idéal propre non nul de A, soit H le sous-groupe $\mathrm{Spec}\,\mathrm{A}[x]/(x^p, \mathrm{J}x)$ de $\boldsymbol{\alpha}_{p,\,\mathrm{A}}$ (i.e. pour toute A-algèbre R, $\mathrm{H}(\mathrm{R}) = \{x \in \mathrm{R} \mid x^p = 0 \text{ et } \mathrm{J}x = 0\}$), alors H n'est pas plat sur A donc n'est pas de la forme $\mathrm{G}_p(\mathscr{L})$, où $\mathscr{L}$ est une p-algèbre de Lie libre de rang fini sur A.

Supposons maintenant S *affine*. Il y a alors une section $\sigma : \omega_{G/S} \to \mathscr{I}$ de la projection $\mathscr{I} \to \mathscr{I}/\mathscr{I}^2$; elle induit un morphisme d'algèbres $\sigma' : \mathcal{S}_{\mathscr{O}_S}(\omega_{G/S}) \to \mathscr{A}$ et, d'après le lemme 7.2, σ' se factorise en un morphisme

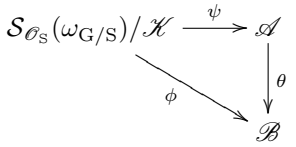
$$\phi : \mathcal{S}_{\mathscr{O}_S}(\omega_{G/S})/\mathscr{K} \longrightarrow \mathscr{A},$$

où $\mathscr{K}$ désigne l'idéal engendré par les puissances p-ièmes de sections de $\omega_{G/S}$. Si l'on filtre $\mathscr{A}$ (resp. $\mathcal{S}_{\mathscr{O}_S}(\omega_{G/S})/\mathscr{K}$) par les puissances de $\mathscr{I}$ (resp. de l'idéal engendré par $\omega_{G/S}$), il est clair que ϕ induit un épimorphisme des gradués associés. Donc ϕ est un épimorphisme de $\mathscr{O}_S$-modules localement libres de même rang (cf. 5.3.3) ; donc ϕ est un isomorphisme. Ceci prouve que (i) ⇒ (ii).

468 ***7.4.2***. — Supposons maintenant G de hauteur $\leqslant 1$ et localement de présentation finie sur S. [72] Comme le morphisme de Frobenius $\mathrm{Fr} : G \to G^{(p)}$ est entier et se factorise par la section unité de $G^{(p)}$, alors G est entier (donc affine) sur S. Soit alors $\mathscr{A} = \mathscr{A}(G)$, comme G est supposé localement de présentation finie sur S, il en résulte que G est fini et de présentation finie sur S, donc que $\mathscr{A}(G)$ est un $\mathscr{O}_S$-module de présentation finie (cf. EGA IV_1, 1.4.7). Soit $\mathscr{I}$ l'idéal d'augmentation de $\mathscr{A}$; comme $\mathscr{A} = \eta_{\mathscr{A}}(\mathscr{O}_S) \oplus \mathscr{I}$ (où $\eta_{\mathscr{A}}$ est la section unité de $\mathscr{A}$), $\mathscr{I}$ est un $\mathscr{O}_S$-module de présentation finie, et il en est donc de même de $\omega_G = \mathscr{I}/\mathscr{I}^2$. Lorsqu'on suppose G de hauteur $\leqslant 1$ et localement de type fini sur S, on obtient de même que $\mathscr{A}(G)$, $\mathscr{I}$ et $\omega_G = \mathscr{I}/\mathscr{I}^2$ sont des $\mathscr{O}_S$-modules de type fini.

Donc, sous l'hypothèse (iii′) on obtient que $\omega_{G/S}$ est fini localement libre sur $\mathscr{O}_S$, ainsi que $\mathscr{L} = \mathscr{L}ie(G/S) = \omega^*_{G/S}$. Soient alors $\mathscr{B} = \mathscr{U}_p(\mathscr{L})^*$ et $H = G_p(\mathscr{L}) = \operatorname{Spec}\mathscr{B}$. D'après le théorème 7.2, l'application identique de $\mathscr{L}$ correspond à un morphisme de groupes de $H = G_p(\mathscr{L})$ vers G, donc à un morphisme de $\mathscr{O}_S$-algèbres $\theta : \mathscr{A} \to \mathscr{B}$. Il s'agit de montrer que θ, qui induit par définition un isomorphisme de $\omega_{G/S}$ sur $\omega_{H/S}$, est un isomorphisme.

Pour cela, on peut se restreindre au cas où S est affine. Il y a alors une section τ de la projection $\mathscr{I} \to \omega_{G/S}$; elle induit un morphisme d'algèbres $\tau' : \mathcal{S}_{\mathscr{O}_S}(\omega_{G/S}) \to \mathscr{A}$ et comme toute section locale de $\mathscr{I}$ est de puissance p-ième nulle (puisque $\mathrm{Fr} : G \to G^{(p)}$ se factorise par la section unité de $G^{(p)}$), τ' induit un morphisme de $\mathscr{O}_S$-algèbres ψ qui s'incrit dans le diagramme commutatif ci-dessous :



où $\mathscr{K}$ est l'idéal engendré par les puissances p-ièmes de sections de $\omega_{G/S}$. D'une part, on montre comme en 7.4.1 que ψ est un épimorphisme de $\mathscr{O}_S$-modules. D'autre part, nous avons vu en 7.4.1 que $\phi = \theta \circ \psi$ est un isomorphisme. Il en va donc de même pour θ. Ceci prouve que (iii′) ⇒ (i).

[72] N.D.E. : On a détaillé (et simplifié) l'original dans ce qui suit.

7.4.3. — [73] Montrons enfin que (iv) entraine (iii). Il suffit de montrer que $\omega_{G/S}$ est localement libre, donc on peut supposer S affine d'anneau R. Comme remarqué au début de 7.4.2, l'hypothèse (iv) entraîne alors que $G = \operatorname{Spec} A$, pour une R-algèbre A qui est un R-module de présentation finie, ainsi que $\omega_{G/A} = I/I^2$ (où I est l'idéal d'augmentation de A). Comme on suppose de plus G plat sur S, alors A est un R-module fini localement libre (cf. [**BAC**] II, § 5.2, Th. 1 et cor. 2) et, d'après *loc. cit.*, pour montrer que $\omega_{G/A}$ est localement libre de rang fini, il suffit de montrer que $(\omega_{G/A})_{\mathfrak{m}}$ est plat pour tout idéal maximal $\mathfrak{m}$ de R. Donc on peut supposer R local, et A libre de rang $n+1$, donc I libre de rang n. Soient $\mathfrak{m}$ l'idéal maximal de R et $k = R/\mathfrak{m}$.

Notons I_k l'idéal d'augmentation de A_k et r la dimension de $\omega_{G_k/k} = I_k/I_k^2$. Soit $(e_1, \dots, e_n)$ une base de I_k telle que $(e_{r+1}, \dots, e_n)$ soit une base de I_k^2, et soient $x_1, \dots, x_n$ des éléments de I relevant les e_i. D'après le lemme de Nakayama, $(x_1, \dots, x_n)$ est une base de I sur R. Soit N le sous-R-module de I de base $(x_1, \dots, x_r)$ et soit B le quotient de l'algèbre symétrique de N par l'idéal engendré par les éléments x^p, pour $x \in N$. Comme tout élément de I est de puissance p-ième nulle, on obtient un morphisme de R-algèbres

$$\psi : \quad B \longrightarrow A.$$

D'après 7.4.2, $\psi \otimes k$ est un isomorphisme. Il en résulte que $\operatorname{Coker} \psi = 0$ et que, notant $K = \operatorname{Ker} \psi$, le morphisme $\tau : K \otimes k \to B \otimes k$ est nul. Mais puisque ψ est surjectif et que A est plat sur R, alors τ est aussi injectif, d'où $K \otimes k = 0$. D'autre part, comme A est un R-module de présentation finie, K est un R-module de type fini (cf. [**BAC**] I, § 2.8, Lemme 9), d'où $K = 0$ d'après Nakayama. Donc ψ est un isomorphisme de R-algèbres, et comme $\psi^{-1}(I)$ contient l'idéal d'augmentation J de B, il en résulte que $\psi^{-1}(I) = J$, et donc ψ^{-1} induit un isomorphisme de R-modules de I/I^2 sur $J/J^2 = N$. Ceci prouve que $\omega_{G/S}$ est fini localement libre, d'où l'implication (iv) $\Rightarrow$ (iii). Ceci achève la démonstration du théorème 7.4.

Remarque 7.5. — [74] Il résulte évidemment des théorèmes 7.2 et 7.4 que les foncteurs $G \mapsto \mathscr{L}ie(G)$ et $\mathscr{L} \mapsto G_p(\mathscr{L})$ induisent des équivalences, quasi-inverses l'une de l'autre, entre la catégorie des S-groupes localement de présentation finie et plats, de hauteur $\leqslant 1$, et la sous-catégorie pleine de celle des $\mathscr{O}_S$-p-algèbres de Lie, formée des $\mathscr{O}_S$-p-algèbres de Lie finies localement libres.

8. Cas d'un corps de base

469

8.1. Résumons maintenant les résultats obtenus dans le cas où S *est le spectre d'un corps k de caractéristique* $p > 0$. Disons alors qu'un k-schéma en groupes est *algébrique* si le schéma sous-jacent est de type fini sur k. Dans ce cas, d'après le théorème 7.2, on obtient : [75]

[73] N.D.E. : On a ajouté ce paragraphe pour démontrer que (iv) $\Rightarrow$ (iii), cf. la N.D.E. (71).
[74] N.D.E. : On a ajouté cette remarque.
[75] N.D.E. : On a ajouté la numérotation 8.1.1 à 8.1.3, pour mettre en évidence les résultats qui y sont énoncés.

Théorème 8.1.1. — *Le foncteur* G_p*, qui associe à toute p-algèbre de Lie* $\mathscr{L}$ *de dimension finie sur k le k-groupe* $\mathrm{G}_p(\mathscr{L})$*, est adjoint à gauche au foncteur qui à tout k-groupe algébrique* G *associe* Lie(G)*.*

Combinant ceci avec le théorème 7.4, on obtient :

Théorème 8.1.2. — *Les foncteurs* $\mathrm{G}_p : \mathscr{L} \mapsto \mathrm{G}_p(\mathscr{L})$ *et* $\mathrm{G} \mapsto \mathscr{L}ie(\mathrm{G})$ *induisent des* équivalences*, quasi-inverses l'une de l'autre, entre la catégorie des p-algèbres de Lie de dimension finie sur k, et celle des k-groupes algébriques de hauteur* $\leqslant 1$*.*

Alors, comme G_p est un foncteur adjoint à gauche, *il commute aux limites inductives*, [(76)] donc en particulier à la formation des conoyaux. D'autre part, si l'on a deux morphismes $\phi : \mathrm{G} \to \mathrm{H}$ et $\phi' : \mathrm{G}' \to \mathrm{H}$ entre k-groupes algébriques de hauteur $\leqslant 1$, alors le produit fibré $\mathrm{G} \times_{\mathrm{H}} \mathrm{G}'$ est encore un k-groupe algébrique de hauteur $\leqslant 1$ (car le morphisme $\mathrm{Fr} : \mathrm{G} \to \mathrm{G}^{(p)}$ commute au produits fibrés). Donc l'inclusion de la catégorie des k-groupes algébriques de hauteur $\leqslant 1$ dans celle de tous les k-groupes algébriques commute aux produits fibrés, donc en particulier à la formation des noyaux. On en déduit le :

Corollaire 8.1.3. — *Le foncteur* G_p *est* exact*, au sens suivant. Si* $\pi : \mathscr{L}_1 \to \mathscr{L}_2$ *est un morphisme surjectif entre p-algèbres de Lie de dimension finie sur k et si i est l'inclusion de* $\mathscr{L}_0 = \operatorname{Ker} \pi$ *dans* $\mathscr{L}_1$*, on a une suite exacte de k-groupes algébriques :*

$$1 \longrightarrow \mathrm{G}_p(\mathscr{L}_0) \xrightarrow{\mathrm{G}_p(i)} \mathrm{G}_p(\mathscr{L}_1) \xrightarrow{\mathrm{G}_p(\pi)} \mathrm{G}_p(\mathscr{L}_2) \longrightarrow 1\ . \qquad (77)$$

En effet, d'après ce qui précède, $\mathrm{G}_p(i)$ induit un isomorphisme de $\mathrm{G}_p(\mathscr{L}_0)$ sur $\operatorname{Ker}(\mathrm{G}_p(\pi))$ (ce noyau étant le même dans la catégorie de tous les k-groupes algébriques H ou dans celle des H de hauteur $\leqslant 1$), et $\mathrm{G}_p(\pi) : \mathrm{G}_p(\mathscr{L}_1) \to \mathrm{G}_p(\mathscr{L}_2)$ identifie $\mathrm{G}_p(\mathscr{L}_2)$ au quotient de $\mathrm{G}_p(\mathscr{L}_1)$ par $\mathrm{G}_p(\mathscr{L}_0)$ dans la catégories des k-groupes algébriques.

Remarque 8.1.4. — [(78)] Soient $\phi : \mathrm{G} \to \mathrm{H}$ un morphisme de k-groupes et $\mathrm{K} = \operatorname{Ker}(\phi)$. On suppose ϕ couvrant pour la topologie (fpqc) (ceci sera le cas, en particulier, si ϕ est couvrant pour une topologie moins fine, par exemple la topologie (fppf)). Alors, d'une part, ϕ est un K-torseur au-dessus de H (cf. IV 5.1.7.1). D'autre part, (cf. IV 6.3.1) il existe un recouvrement de H par des ouverts affines S_i, et pour chaque i un morphisme affine fidèlement plat $\mathrm{T}_i \to \mathrm{S}_i$ se factorisant par ϕ. Alors $\mathrm{G} \times_{\mathrm{H}} \mathrm{T}_i$ est T_i-isomorphe à $\mathrm{K} \times \mathrm{T}_i$, donc fidèlement plat sur T_i, et donc, par descente (fpqc), $\mathrm{G} \times_{\mathrm{H}} \mathrm{S}_i \to \mathrm{S}_i$ est fidèlement plat, de sorte que ϕ est fidèlement plat.

Réciproquement, si ϕ est fidèlement plat et quasi-compact (resp. et localement de présentation finie), il est couvrant pour la topologie (fpqc) (resp. (fppf)), cf. IV 6.3.1. Rappelons enfin qu'un morphisme de faisceaux est couvrant si et seulement si c'est un

---

[(76)] N.D.E. : On a détaillé ce qui suit, ainsi que la démonstration du corollaire ci-dessous.

[(77)] N.D.E. : De plus, d'après VI_A, 3.2, $\mathrm{G}_p(\mathscr{L}_2)$ représente le faisceau (fppf) quotient de $\mathrm{G}_p(\mathscr{L}_1)$ par $\mathrm{G}_p(\mathscr{L}_0)$.

[(78)] N.D.E. : On a ajouté cette remarque, signalée par O. Gabber, qui sera utile en 8.3.1.

épimorphisme, cf. IV 4.4.3. On obtient donc, en particulier, qu'un morphisme quasi-compact de k-groupes est fidèlement plat si et seulement si c'est un épimorphisme de faisceaux (fpqc).

8.2. Proposition. — *Considérons une suite exacte* [79] *de groupes algébriques sur un corps k de caractéristique $p > 0$*

$$1 \longrightarrow \mathrm{G}' \xrightarrow{\tau} \mathrm{G} \xrightarrow{\pi} \mathrm{G}'' \longrightarrow 1$$

et les assertions suivantes :

(i) *Le morphisme π est lisse.*

(ii) G' *est lisse.*

(iii) *Pour tout entier $n > 0$, la suite ci-dessous, induite par τ et π, est exacte :* **470**

$$1 \longrightarrow {}_{\mathrm{Fr}^n}\mathrm{G}' \longrightarrow {}_{\mathrm{Fr}^n}\mathrm{G} \longrightarrow {}_{\mathrm{Fr}^n}\mathrm{G}'' \longrightarrow 1.$$

(iv) *Le morphisme* ${}_{\mathrm{Fr}}\pi : {}_{\mathrm{Fr}}\mathrm{G} \to {}_{\mathrm{Fr}}\mathrm{G}''$ *est un épimorphisme de faisceaux* (fppf).

(v) *Le morphisme* $\mathrm{Lie}(\pi) : \mathrm{Lie}(\mathrm{G}) \to \mathrm{Lie}(\mathrm{G}'')$ *est surjectif.*

Alors on a les implications (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Leftrightarrow$ (v) *et toutes les assertions sont équivalentes lorsque* G *est lisse sur k.*

En effet, (i) équivaut à (ii) d'après VI_B 9.2 (vii), et il est clair que (iii) implique (iv). D'autre part, l'équivalence de (iv) et (v) résulte de 8.1.3.

L'implication (ii) $\Rightarrow$ (iii) résulte du diagramme :

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{G}' & \xrightarrow{\tau} & \mathrm{G} & \xrightarrow{\pi} & \mathrm{G}'' & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{Fr}^n(\mathrm{G}'/k)} & & \downarrow{\scriptstyle \mathrm{Fr}^n(\mathrm{G}/k)} & & \downarrow{\scriptstyle \mathrm{Fr}^n(\mathrm{G}''/k)} & & \\
1 & \longrightarrow & \mathrm{G}'^{(p^n)} & \xrightarrow[\tau^{(p^n)}]{} & \mathrm{G}^{(p^n)} & \xrightarrow[\pi^{(p^n)}]{} & \mathrm{G}''^{(p^n)} & \longrightarrow & 1
\end{array}$$

dont les deux lignes sont exactes : comme $\mathrm{Fr}^n(\mathrm{G}'/k)$ est un épimorphisme de faisceaux (fppf) d'après le corollaire 8.3.1 ci-dessous, π induit un épimorphisme de ${}_{\mathrm{Fr}^n}\mathrm{G}$ sur ${}_{\mathrm{Fr}^n}\mathrm{G}''$ (généraliser le lemme du serpent aux faisceaux en groupes non nécessairement commutatifs).

De même, lorsque G est lisse sur k, $\mathrm{Fr}(\mathrm{G}/k)$ est un épimorphisme, donc si de plus ${}_{\mathrm{Fr}}\pi$ est un épimorphisme, le même lemme du serpent appliqué au diagramme ci-dessus pour $n = 1$ montre que $\mathrm{Fr}(\mathrm{G}'/k)$ est un épimorphisme, donc que G' est lisse sur k, d'après 8.3.1 ci-dessous.

8.3. Proposition. — *Si* G *est un groupe localement de type fini* [80] *sur un corps k de caractéristique $p > 0$, il existe un entier n_0 tel que* $\mathrm{G}/({}_{\mathrm{Fr}^n}\mathrm{G})$ *soit lisse sur k pour $n \geqslant n_0$.*

---

[79] N.D.E. : i.e. π est fidèlement plat et i est un isomorphisme de G' sur $\mathrm{Ker}\,\pi$, de sorte que G'' représente le faisceau (fppf) quotient de G par G', cf. VI_A, 3.2 et 5.2.

[80] N.D.E. : On a remplacé « algébrique » par « localement de type fini ».

471 Comme la construction de $G/({}_{Fr^n}G)$ commute à l'extension du corps de base (4.1.1 et VI_A, 3.3.2), nous pouvons supposer k parfait. Dans ce cas, $G_{réd}$ est un k-groupe localement de type fini (cf. VI_A 0.2) et l'on a le diagramme commutatif et exact suivant, où l'on a noté H le k-schéma $G_{réd}\backslash G$:

$$\begin{array}{ccccccc} 1 & \longrightarrow & G_{réd} & \longrightarrow & G & \longrightarrow & H \\ & & \downarrow{\scriptstyle Fr^n(G_{réd}/k)} & & \downarrow{\scriptstyle Fr^n(G/k)} & & \downarrow{\scriptstyle Fr^n(H/k)} \\ 1 & \longrightarrow & G_{réd}^{(p^n)} & \longrightarrow & G^{(p^n)} & \longrightarrow & H^{(p^n)} \end{array} .$$

Or H est le spectre d'une k-algèbre finie, locale, de corps résiduel k (cf. VI_A, 5.6.1). Par conséquent, il existe un entier n_0 tel que, pour tout $n \geqslant n_0$, $Fr^n(H/k)$ se factorise à travers la section « unité » de $H^{(p^n)}$. Il s'ensuit que, pour $n \geqslant n_0$, $Fr^n(G/k)$ se factorise à travers $G_{réd}^{(p^n)}$ et donc, d'après VI_A, 5.4.1, on a un diagramme commutatif

$$\begin{array}{ccc} G & \xrightarrow{Fr^n(G/k)} & G_{réd}^{(p^n)} \\ {\scriptstyle \pi}\downarrow & \nearrow_{i} & \\ G/({}_{Fr^n}G) & & \end{array}$$

où i est une immersion fermée (et π est la projection canonique). Comme, de plus, i induit un homéomorphisme des espaces topologiques sous-jacents, c'est donc un isomorphisme. Comme k est parfait, $G_{réd}^{(p^n)}$ est lisse sur k (VI_A, 1.3.1), et donc $G/({}_{Fr^n}G)$ est lisse sur k, pour tout $n \geqslant n_0$.

8.3.1. Corollaire. — *Soit* G *un groupe localement de type fini* [80] *sur un corps* k *de caractéristique* $p > 0$ *et soit* n *un entier* $\geqslant 1$. [81] *Les conditions suivantes sont équivalentes :*

(i) G *est lisse sur* k.

(ii) $Fr^n(G/k) : G \to G^{(p^n)}$ *est un épimorphisme de faisceaux* (fppf).

(iii) $Fr^n(G/k) : G \to G^{(p^n)}$ *est fidèlement plat.*

D'abord, comme G est localement de type fini sur k, $Fr^n(G/k)$ est de présentation finie, donc l'équivalence de (ii) et (iii) découle de 8.1.4. Supposons G lisse sur k, donc G réduit. Alors, comme $Fr^n(G/k)$ est surjectif, il est fidèlement plat (cf. VI_A, 6.2 ou VI_B, 1.3).

Réciproquement, supposons $Fr^n(G/k)$ fidèlement plat. Comme $Fr^n(G^{(p^n)}/k)$ est déduit de $Fr^n(G/k)$ par changement de base (cf. 4.1.3), il est donc aussi fidèlement plat, ainsi que le composé :

$$Fr^{2n}(G/k) : \quad G \longrightarrow G^{(p^n)} \longrightarrow G^{(p^{2n})}.$$

[81] N.D.E. : On a explicité l'équivalence entre (ii) et (iii) et l'on a détaillé la démonstration.

On obtient ainsi que, pour tout $m \in \mathbb{N}$, $\mathrm{Fr}^{mn}(\mathrm{G}/k) : \mathrm{G} \to \mathrm{G}^{(p^{mn})}$ est fidèlement plat, donc induit un isomorphisme $\mathrm{G}/({}_{\mathrm{Fr}^{mn}}\mathrm{G}) \simeq \mathrm{G}^{(p^{mn})}$ (cf. VI_A, 5.4.1). Or, d'après la proposition 8.3, $\mathrm{G}^{(p^{mn})}$ est lisse sur k pour m grand, donc G l'est aussi, par descente (fpqc) (cf. EGA IV_4, 17.7.1).

8.4. Dans les deux énoncés qui terminent cet exposé, nous revenons au cas d'un corps k de caractéristique quelconque.

Lorsque k est de caractéristique 0 (resp. $p > 0$), soit n un entier $\geqslant 1$ (resp. un entier $\geqslant 1$ et premier à p) ; dans les deux cas, nous disons simplement que n est premier à la caractéristique de k. De plus, si G est un schéma en groupes sur k, nous notons **472**
$n_\mathrm{G} : \mathrm{G} \to \mathrm{G}$ le morphisme de k-schémas qui applique un élément x de $\mathrm{G}(\mathrm{T})$ sur $x^n \in \mathrm{G}(\mathrm{T})$, lorsque T est un k-schéma.

Proposition. — *Soient* G *un groupe algébrique sur un corps k et n un entier premier à la caractéristique de k. Alors $n_\mathrm{G} : \mathrm{G} \to \mathrm{G}$ est un morphisme étale.*

(82) D'après VI_B 1.3, il suffit de montrer que n_G est étale à l'origine. Soient A l'anneau local de G à l'origine et I l'idéal maximal de A. D'après II 3.9.4, l'application $\mathrm{Lie}(n_\mathrm{G}) : \mathrm{Lie}(\mathrm{G}) \to \mathrm{Lie}(\mathrm{G})$, qui est induite par n_G, est l'homothétie de rapport n. C'est donc un isomorphisme ainsi que l'endomorphisme induit par n_G sur $\mathrm{I}/\mathrm{I}^2 = \mathrm{Lie}(\mathrm{G})^*$. Si k est de caractéristique 0, G est lisse sur k (VI_B 1.6.1, voir aussi VII_B 3.3.1), donc le morphisme canonique $\mathcal{S}(\mathrm{I}/\mathrm{I}^2) \to \mathrm{gr}_\mathrm{I}(\mathrm{A})$ est un isomorphisme, où $\mathrm{gr}_\mathrm{I}(\mathrm{A})$ désigne le gradué associé à la filtration I-adique. Il en résulte que n_G induit un automorphisme de $\mathrm{gr}_\mathrm{I}(\mathrm{A})$, donc aussi du complété $\widehat{\mathrm{A}}$ de A, donc n_G est étale à l'origine (cf. EGA IV_4, 17.6.3).

Si la caractéristique est $p > 0$ et si G est de hauteur $\leqslant 1$, alors A est isomorphe au quotient de l'algèbre symétrique de $\omega_{\mathrm{G}/k} = \mathrm{I}/\mathrm{I}^2$ par l'idéal engendré par les puissances p-ièmes des éléments de $\omega_{\mathrm{G}/k}$ (cf. 7.4) ; on peut appliquer alors le « même » raisonnement qu'en caractéristique 0, et l'on obtient que n_G induit un automorphisme de A.

Si G est de hauteur $\leqslant r$ et si nous supposons notre assertion démontrée pour les groupes de hauteur $\leqslant r-1$, notons B, A et A′ les algèbres affines de ${}_{\mathrm{Fr}}\mathrm{G}$, G et $\mathrm{G}' = {}_{\mathrm{Fr}}\mathrm{G}\backslash\mathrm{G}$, et n_B, n_A et $n_{\mathrm{A}'}$ les endomorphismes de B, A et A′ qui sont induits par $n_{{}_{\mathrm{Fr}}\mathrm{G}}$, n_G et $n_{\mathrm{G}'}$. (83) Soit $\mathrm{I}' = \mathrm{I} \cap \mathrm{A}$ l'idéal maximal de A′, comme on a un carré cartésien

$$\begin{array}{ccc} {}_{\mathrm{Fr}}\mathrm{G} & \longrightarrow & \mathrm{G} \\ \downarrow & & \downarrow \\ e & \longrightarrow & \mathrm{G}' \end{array}$$

on a $\mathrm{B} = \mathrm{A}/\mathrm{I}'\mathrm{A}$. Observons que $n_{\mathrm{A}'}$ (resp. n_B) n'est autre que l'endomorphisme induit par n_A sur A′ (resp. sur B). D'après VI_A 3.2, A est un A′-module fidèlement

(82) N.D.E. : On a changé dans l'énoncé « étale à l'origine » en « étale », et l'on a ajouté la phrase qui suit.
(83) N.D.E. : On a détaillé l'original dans ce qui suit.

plat, et comme A' est un anneau local artinien (G' étant un k-groupe algébrique de hauteur $\leqslant r-1$), il en résulte que A est un A'-module libre. Comme la restriction de n_A à A' est $n_{A'}$, qui est un isomorphisme d'après l'hypothèse de récurrence, il résulte du lemme de Nakayama que n_A sera un automorphisme si l'endomorphisme qu'il induit sur $A/I'A$ en est un. Or cet endomorphisme n'est autre que n_B, qui est un automorphisme puisque B est de hauteur $\leqslant 1$. Donc n_A est un automorphisme.

Enfin, lorsque G est un groupe algébrique quelconque sur un corps de caractéristique $p>0$, ce qui précède montre que n_G induit des automorphismes des k-schémas ${}_{\mathrm{Fr}^r}G$; ces schémas sont affines sur k et ont pour algèbres les quotients de l'algèbre lo-
473 cale A par l'idéal $I^{\{p^r\}}$ engendré par les puissances p^r-ièmes des éléments de I. Comme n_G définit des automorphismes des algèbres $A/I^{\{p^r\}}$, on voit par passage à la limite projective, que n_G induit un automorphisme de $\widehat{A}$, donc n_G est étale à l'origine (EGA IV_4, 17.6.3).

8.5. Proposition. — *Soit* G *un groupe algébrique fini, de rang n sur le corps k. Alors* $n_G : G \to G$ *est le morphisme nul de* G.

Signalons tout de suite le corollaire suivant, obtenu en combinant 8.4 et 8.5 : [(84)]

Corollaire 8.5.1. — *Soit* G *un groupe algébrique fini, de rang n sur le corps k. Si n est premier à la caractéristique de k, alors* G *est étale sur k.*

Démontrons maintenant 8.5. Soit H un sous-groupe distingué de G de rang m sur k. Notons $\lambda : H \times G \to G$ le morphisme induit par la multiplication de G. Alors, avec les notations de VI_A 3.2, on a un carré cartésien :

$$\begin{array}{ccc} H \times G & \xrightarrow{\lambda} & G \\ {\scriptstyle \mathrm{pr}_2}\downarrow & & \downarrow{\scriptstyle \pi} \\ G & \xrightarrow{\pi} & H\backslash G \end{array}$$

Comme $\pi : G \to H\backslash G$ est fidèlement plat, quasi-compact (VI_A 3.2), et que pr_2 est localement libre de rang m, il résulte de EGA IV_2, 2.5.2, que $G \to H\backslash G$ est localement libre de rang m. Notant $r = rg_k(H\backslash G)$, on a donc $n = \mathrm{rg}_k(G) = r\,m$.

D'un autre côté, on a une suite exacte de groupes « abstraits »

$$1 \longrightarrow H(T) \longrightarrow G(T) \longrightarrow (H\backslash G)(T)$$

quel que soit le k-schéma T ; il est donc clair que n_G est nul si m_H et $r_{H\backslash G}$ le sont. Si l'on prend pour H la composante neutre G^0 de G, alors $G^0\backslash G$ est étale (cf. VI_A 5.5.1), de sorte qu'on peut supposer G étale sur k ou bien infinitésimal (cf. 7.0).

Si G est étale, on se ramène, par extension du corps de base, au cas où k est algébriquement clos. Dans ce cas, G est un groupe constant (cf. I 4.1), et l'énoncé est classique.

474 Si G est infinitésimal et non nul, k est nécessairement de caractéristique $p>0$

(84) N.D.E. : On a ajouté ce corollaire, indiqué implicitement dans l'original par : « (confer 8.4) ». Pour une autre démonstration du corollaire, n'utilisant pas 8.5, voir par exemple [**TO70**], Lemma 5.

(cf. $\mathrm{VI_B}$ 1.6.1 ou $\mathrm{VII_B}$ 3.3.1) ; les sous-groupes ${}_{\mathrm{Fr}^n}\mathrm{G}$ forment alors une suite de composition de G, dont les quotients sont de hauteur $\leqslant 1$.

Ceci nous ramène au cas où G est de hauteur $\leqslant 1$. Soient alors A (resp. L) l'algèbre affine (resp. l'algèbre de Lie) de G et $\mathrm{U} = \mathrm{U}_p(\mathrm{L})$. D'après 7.4, on a $\mathrm{G} = \mathrm{G}_p(\mathrm{L})$ d'où $\mathrm{A} = \mathrm{U}^*$; donc si $\dim_k \mathrm{L} = r$, le rang de G sur k est p^r (cf. 5.3.3). Nous allons donc étudier le morphisme $p_{\mathrm{G}} : \mathrm{G} \to \mathrm{G}$ défini par l'élévation à la puissance p ; il induit un endomorphisme p_{A} de A et, par dualité, un endomorphisme p_{U} de U.

Soit I l'idéal d'augmentation de A, nous allons montrer que $p_{\mathrm{A}}(\mathrm{I}) \subset \mathrm{I}^p$. Supposant ceci établi, on aura donc $p_{\mathrm{A}}^r(\mathrm{I}) \subset \mathrm{I}^{p^r}$. D'autre part, on sait que $\mathrm{I}^{r(p-1)+1} = 0$ (puisque I est engendré par r éléments de puissance p-ième nulle). Comme $p^r > r(p-1)$, il en résulte que $p_{\mathrm{A}}^r(\mathrm{I}) = 0$, donc p_{G}^r est le morphisme nul. Il reste donc à montrer l'assertion :

$$(*) \qquad p_{\mathrm{A}}(\mathrm{I}) \subset \mathrm{I}^p.$$

Pour tout entier $s \geqslant 1$, on notera $m_{\mathrm{A}}^{s-1} : \mathrm{A}^{\otimes s} \to \mathrm{A}$ (resp. $\Delta_{\mathrm{U}}^s : \mathrm{U} \to \mathrm{U}^{\otimes s}$) l'application induite par la multiplication m_{A} de A (resp. la comultiplication Δ_{U} de U). Alors p_{A} est égal au composé suivant :

$$\mathrm{A} \xrightarrow{\Delta_{\mathrm{A}}^{p-1}} \mathrm{A}^{\otimes p} \xrightarrow{m_{\mathrm{A}}^{p-1}} \mathrm{A} \ ,$$

et comme la transposée de m_{A} (resp. Δ_{A}) est Δ_{U} (resp. m_{U}), l'endomorphisme $p_{\mathrm{U}} = {}^t p_{\mathrm{A}}$ de U est le composé ci-dessous :

$$\mathrm{U} \xrightarrow{\Delta_{\mathrm{U}}^{p-1}} \mathrm{U}^{\otimes p} \xrightarrow{m_{\mathrm{U}}^{p-1}} \mathrm{U} \ .$$

(85) Soit J l'idéal d'augmentation de U, on a $\mathrm{U} = k1_{\mathrm{U}} \oplus \mathrm{J}$ et l'on notera π la projection $\mathrm{U} \to \mathrm{J}$ de noyau $k1_{\mathrm{U}}$. Pour tout entier $s \geqslant 1$, notons $(\mathrm{I}^s)^\perp$ l'orthogonal de I^s dans $\mathrm{A}^* = \mathrm{U}$, i.e. $(\mathrm{I}^s)^\perp$ est l'ensemble des $u \in \mathrm{U}$ tels que le composé ci-dessous soit nul :

$$\mathrm{I}^{\otimes s} \xrightarrow{m_{\mathrm{A}}^{s-1}} \mathrm{I} \xrightarrow{u} k \ .$$

Comme la transposée de m_{A} est Δ_{U}, on voit que $(\mathrm{I}^s)^\perp$ est le sous-espace vectoriel P_{s-1} formé des $u \in \mathrm{U}$ tels que $\Delta_{\mathrm{U}}^{s-1}(u)$ s'annule sur $\mathrm{I}^{\otimes s}$, i.e. notant $\overline{\Delta_{\mathrm{U}}^{s-1}}$ la composée de $\Delta_{\mathrm{U}}^{s-1}$ et de la projection $\pi^{\otimes s} : \mathrm{U}^{\otimes s} \to \mathrm{J}^{\otimes s}$, on obtient que

$$(\mathrm{I}^s)^\perp = \mathrm{P}_{s-1} = \operatorname{Ker} \overline{\Delta_{\mathrm{U}}^{s-1}}$$

(voir aussi $\mathrm{VII_B}$, 1.3.6). Donc, pour montrer l'assertion $(*)$, il faut montrer que l'application transposée $p_{\mathrm{U}} = {}^t p_{\mathrm{A}}$ applique P_{p-1} dans $\mathrm{I}^\perp = k1_{\mathrm{U}}$. Comme $p_{\mathrm{U}}(1_{\mathrm{U}}) = 1_{\mathrm{U}}$, il suffit de montrer l'assertion ci-dessous, où P_{p-1}^+ désigne $\mathrm{J} \cap \mathrm{P}_{p-1}$:

$$(**) \qquad p_{\mathrm{U}}(\mathrm{P}_{p-1}^+) = 0.$$

(85) N.D.E. : On a détaillé l'original dans le paragraphe ce qui suit.

D'autre part, on montre facilement, par récurrence sur s, que P_{s-1}^{+} est le sous-espace vectoriel de U engendré par les produits $x_1 \cdots x_t$, avec $1 \leqslant t \leqslant s-1$ et $x_i \in \mathrm{L}$ (cf. $\mathrm{VII_B}$ 4.3). Or, si $x_1, x_2, \ldots, x_t$ sont des éléments de L, on a :

$$p_{\mathrm{U}}(x_1 x_2 \cdots x_t) = m_{\mathrm{U}}^{p-1}\left(\prod_{j=1}^{t}\sum_{i=1}^{p} 1 \otimes \cdots \otimes \overset{i}{\underset{\downarrow}{x_j}} \otimes \cdots \otimes 1\right).$$

Il est clair que l'expression $\prod_j \sum_i 1 \otimes \cdots \otimes x_j \otimes \cdots \otimes 1$ est une somme de p^t termes x_h indexés par les applications h de $\{1, \ldots, t\}$ dans $\{1, \ldots, p\}$. [86] Une telle application h définit une *partition ordonnée* $\mathfrak{p}_h$ de $\{1, \ldots, t\}$ en au plus p parts. En effet, notons $i_1 < \cdots < i_r$ les éléments de l'image de h et, pour $s = 1, \ldots, r$, posons $\mathrm{I}_s = h^{-1}(i_s)$ et $x_{\mathrm{I}_s} = \prod_{j \in \mathrm{I}_s} x_j$, le produit étant pris dans l'ordre croissant. Alors h correspond au p-tenseur

$$1 \otimes \cdots \otimes x_{\mathrm{I}_1} \otimes \cdots \otimes x_{\mathrm{I}_r} \otimes \cdots \otimes 1$$

(où chaque x_{I_s} est à la place i_s), et son image par m_{U}^{p} est le produit :

$$x_{\mathrm{I}_1} \otimes \cdots \otimes x_{\mathrm{I}_r}$$

qui ne dépend que de la partition ordonnée $\mathfrak{p} = (\mathrm{I}_1, \ldots, \mathrm{I}_r)$, et qu'on notera $x_{\mathfrak{p}}$. Pour $\mathfrak{p}$ fixé, $x_{\mathfrak{p}}$ est obtenu pour tous les choix de $i_1 < \cdots < i_r$ dans $\{1, \ldots, p\}$, et l'on obtient donc l'égalité

$$p_{\mathrm{U}}(x_1 x_2 \cdots x_t) = \sum_{\mathfrak{p}} \binom{p}{n(\mathfrak{p})} x_{\mathfrak{p}},$$

où $\mathfrak{p}$ parcourt l'ensemble des partitions ordonnées de $\{1, \ldots, t\}$ en au plus p parts, et où $n(\mathfrak{p})$ désigne le nombre de parts de $\mathfrak{p}$. (On a $1 \leqslant n(\mathfrak{p}) \leqslant \min(t, p)$.)

475 Lorsque $t < p$, tous les termes $\binom{p}{n(\mathfrak{p})}$ sont donc nuls, de sorte que $p_{\mathrm{U}}(x_1 \cdots x_t) = 0$. Donc p_{U} s'annule sur P_{p-1}^{+}, ce qui prouve l'assertion $(**)$, et donc $(*)$, et achève la démonstration de 8.5.

Corollaire 8.5.2. — [87] *Soient* S *un schéma* réduit *et* G *un* S*-groupe fini localement libre de rang* n. *Alors* $n_{\mathrm{G}} : \mathrm{G} \to \mathrm{G}$ *est le morphisme nul de* G.

En effet, soit S' la somme des $\operatorname{Spec} \mathscr{O}_{\mathrm{S},\eta}$, pour η parcourant les points maximaux de S. Comme S est réduit, le morphisme $\mathrm{S}' \to \mathrm{S}$ est schématiquement dominant, et il en est de même du morphisme $f : \mathrm{G}_{\mathrm{S}'} \to \mathrm{G}$, puisque G est fini localement libre sur S (cf. EGA IV_3, 11.10.5). Comme $\mathrm{G} \to \mathrm{S}$ affine, donc séparé, le lieu de coïncidence de n_{G} et du morphisme nul est un sous-schéma fermé de G, or il majore f d'après 8.5, donc égale G, i.e. n_{G} est le morphisme nul.

Remarque 8.5.3. — Signalons aussi que, d'après un théorème de P. Deligne (voir [**TO70**], p. 4), si G est un S-groupe *commutatif* fini localement libre de rang n sur une base S arbitraire, alors $n_{\mathrm{G}} = 0$.

---

[86] N.D.E. : On a détaillé l'original dans ce qui suit, en remplaçant la notion de préordre par la notion équivalente de partition ordonnée.

[87] N.D.E. : On a ajouté ce corollaire, signalé dans l'Exp. VIII, Remarque 7.3.1.

Bibliographie

[BAlg] N. Bourbaki, *Algèbre*, Chap. I-III, Hermann, 1974, Chap. X, Masson, 1980.

[BAC] N. Bourbaki, *Algèbre commutative*, Chap. I-IV, Masson, 1985.

[BLie] N. Bourbaki, *Groupes et algèbres de Lie*, Chap. I, Hermann, 1971.

[DG70] M. Demazure, P. Gabriel, *Groupes algébriques*, Masson & North-Holland, 1970.

[Ja03] J. C. Jantzen, *Representations of algebraic groups*, Academic Press 1987 ; 2nd edition, Amer. Math. Soc., 2003.

[TO70] J. Tate, F. Oort, *Groups schemes of prime order*, Ann. scient. Éc. Norm. Sup. **3** (1970), 1-21.