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 préschéma et les produits considérés sont des produits cartésiens dans la catégorie des S-préschémas [(1)]. Si X est un S-préschéma, 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-préschémas 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**

[(0)] version 1.0 du 18/7/09 ; revoir 1.5, 2.5, 4.1.4 b) et 6.1–2

[(*)] 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-préschémas, $X \times_S Y$ est noté simplement $X \times Y$.

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-préschémas $u : \mathrm{Y} \to \mathrm{X}$ et d'un morphisme de $p^{-1}(\mathscr{O}_\mathrm{S})$-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 $\mathrm{Hom}_{p_\mathrm{U}^{-1}(\mathscr{O}_\mathrm{S})}(\mathscr{O}_\mathrm{U}, u_*(\mathscr{O}_\mathrm{Y})|_\mathrm{U})$:

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

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) $u(\mathrm{V}) \subseteq \mathrm{U}$;

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 $p^{-1}(\mathscr{O}_\mathrm{S})$-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 $p^{-1}(\mathscr{O}_\mathrm{S})$-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 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.

Définition. — 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-préschémas, pour morphismes les S-déviations. [6]

1.2.1. Définition. — [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 $\mathrm{I}_{\mathrm{Z}} = \operatorname{Spec} \mathscr{O}_{\mathrm{Z}}[\mathrm{T}]/(\mathrm{T}^2)$ et v égal à la section nulle s de $\mathrm{I}_{\mathrm{Z}} \to \mathrm{Z}$, définie par l'homomorphisme d'algèbres de $\mathscr{O}_{\mathrm{Z}}[\mathrm{T}]/(\mathrm{T}^2)$ dans $\mathscr{O}_{\mathrm{Z}}$ qui s'annule sur la classe t de T modulo T^2, et prenons e égal au morphisme de $\mathscr{O}_{\mathrm{Z}}$-modules $\sigma : \mathscr{O}_{\mathrm{Z}}[\mathrm{T}]/(\mathrm{T}^2) \to \mathscr{O}_{\mathrm{Z}}$ défini par $\sigma(1) = 0$ et $\sigma(t) = 1$.

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

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

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

---

[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 droite, 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.

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

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

D'autre part, soit $t : \mathrm{T} \to \mathrm{S}$ un morphisme de but S, et soient $u_\mathrm{T} : \mathrm{Y_T} \to \mathrm{X_T}$ le morphisme déduit de u par changement de base, et $t_\mathrm{Y} : \mathrm{Y_T} \to \mathrm{Y}$ et $t_\mathrm{X} : \mathrm{X_T} \to \mathrm{X}$ les projections canoniques. Il existe alors une T-déviation de u_T et une seule, que nous noterons d_T ou $d \times \mathrm{T}$, qui vérifie l'égalité $t_\mathrm{X} d_\mathrm{T} = d t_\mathrm{Y}$, au sens de (†) plus haut, c.-à-d., pour tout ouvert U de X, on a un diagramme commutatif : [8]

$$\begin{array}{ccc} \mathscr{O}(\mathrm{U}) & \xrightarrow{t_\mathrm{X}^\natural} & \mathscr{O}(\mathrm{U} \times \mathrm{T}) \\ {\scriptstyle d(\mathrm{U})}\downarrow & & \downarrow{\scriptstyle d_\mathrm{T}(\mathrm{U}\times\mathrm{T})} \\ \mathscr{O}(u^{-1}\mathrm{U}) & \xrightarrow{t_\mathrm{Y}^\natural} & \mathscr{O}(u^{-1}\mathrm{U} \times \mathrm{T}). \end{array}$$

Si l'on pose $\mathrm{D} = (u, d)$, on écrira aussi $\mathrm{D_T} = (u_\mathrm{T}, d_\mathrm{T})$ et nous dirons que d_T *et* $\mathrm{D_T}$ *sont déduits de* d *et* D *par changement de base.*

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

$$\begin{array}{ccc} \mathrm{X} \times \mathrm{T} & \xleftarrow{u_\mathrm{T}} & \mathrm{Y} \times \mathrm{T} \\ {\scriptstyle v_\mathrm{X}}\uparrow & \nwarrow^{u\times v} & \uparrow{\scriptstyle v_\mathrm{Y}} \\ \mathrm{X} \times \mathrm{Z} & \xleftarrow{u_\mathrm{Z}} & \mathrm{Y} \times \mathrm{Z} \end{array}$$

et nous noterons $d \times e$ (*produit de* d *et* e) la S-déviation de $u \times v$ égale à $d_\mathrm{T} e_\mathrm{Y} = e_\mathrm{X} d_\mathrm{Z}$ (avec la convention (†) plus haut), c.-à-d., pour tout ouvert U de $\mathrm{X} \times \mathrm{T}$, si l'on désigne 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 :

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

---

[8] 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 $\mathscr{O}_{\mathrm{X}\times\mathrm{T}}(\mathrm{U} \times \mathrm{U}') = \mathscr{O}_\mathrm{X}(\mathrm{U}) \otimes_{\mathscr{O}_\mathrm{S}(\mathrm{V})} \mathscr{O}_\mathrm{T}(\mathrm{U}')$, alors $d_\mathrm{T}(\mathrm{U} \times \mathrm{U}')$ est la composée :

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

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

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. [(9)] Soit $u : \mathrm{Y} \to \mathrm{X}$ un morphisme de S-préschémas. 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) :

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

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 $\mathrm{Y} \to \mathrm{Y} \times \mathrm{X}$ de composantes id_{Y} et u. Pour toute S-déviation d de u d'ordre $\leqslant n$, on obtient par composition :

$$\mathrm{Y} \xrightarrow{\mathrm{diag.}} \mathrm{Y} \times \mathrm{Y} \xrightarrow[u_{\mathrm{Y}}]{d_{\mathrm{Y}}} \mathrm{Y} \times \mathrm{X}$$

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 $e_{\mathrm{X}} = \mathrm{pr}_2 \circ e$:

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

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

On voit aussitôt que $(\Gamma d)_{\mathrm{X}} = d$, et l'égalité $\Gamma e_{\mathrm{X}} = e$ résulte du fait que e est $\mathscr{O}_{\mathrm{Y}}$-linéaire [10]. *On obtient ainsi un isomorphisme de* $\mathscr{O}_{\mathrm{Y}}(\mathrm{Y})$*-modules* :

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

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 $(\Gamma u)^{-1}(\mathscr{O}_{\mathrm{Y}\times\mathrm{X}}) \longrightarrow \mathscr{O}_{\mathrm{Y}}$ qui correspond à Γu. Tenant compte du lemme qui précède, on a obtenu :

Proposition. — *Soient* $u : \mathrm{Y} \to \mathrm{X}$ *un* S*-morphisme et* $\Gamma u : \mathrm{Y} \to \mathrm{Y} \times \mathrm{X}$ *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*

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

1.3.1. — [11] Revenons au cas où $u : \mathrm{S} \to \mathrm{X}$ est une section de $p : \mathrm{X} \to \mathrm{S}$. Alors, l'homomorphisme $\phi : u^{-1}(\mathscr{O}_{\mathrm{X}}) \to \mathscr{O}_{\mathrm{S}}$ 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 $\mathscr{O}_{\mathrm{S}}$-modules :

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

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

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

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

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

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

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

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

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

---

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

[11] N.D.E. : On a ajouté ce paragraphe.

1.4. Définition. — Soit X un S-préschéma. 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 [12] 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. [13]

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 :

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

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

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

qu'on peut définir comme suit : si d appartient à $\mathrm{Dif}^m_{X/S}$ et si c est une section de $\mathscr{P}^m_{X/S}$ sur U de la forme $a \otimes b + I^{m+1}$, on a $j_X(d)(c) = a \cdot d(b)$. [14]

---

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

[13] 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 $p_X : X \to S$.

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

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*

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

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 $d'' : \mathscr{P}^m_{\mathrm{X/S}} \to \mathscr{O}_\mathrm{X}$).

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 $u^*(\mathscr{P}^m_{\mathrm{X/S}})$ 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 $\mathrm{I_S} = \mathrm{Spec}\,\mathscr{O}_\mathrm{S}[\mathrm{T}]/(\mathrm{T}^2)$. Soit $s : \mathrm{S} \to \mathrm{I_S}$ la section zéro (II 2.1) et soit σ la déviation canonique de s que nous avons définie en 1.2.1, 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-préschéma. [15] À tout $\mathrm{I_S}$-automorphisme u de $\mathrm{I_S} \times \mathrm{X}$ induisant l'identité sur X est associé par composition un opérateur différentiel D_u de X :

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

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 $\mathrm{I_S} \times \mathrm{X}$ correspondant à l'automorphisme $a + bt \mapsto a + (\mathrm{D}a + b)t$ de $\mathscr{O}_\mathrm{X}[\mathrm{T}]/(\mathrm{T}^2)$.

2. Opérateurs différentiels invariants sur les préschémas en groupes

418 **2.1.** *Soit* G *un* S-*préschéma en groupes* ; nous désignons par ε ou $\varepsilon_\mathrm{G} : \mathrm{S} \to \mathrm{G}$ la section unité de G.

Définition. — Soit U(G) le $\Gamma(\mathscr{O}_\mathrm{S})$-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 $\varepsilon \times \varepsilon : \mathrm{S} \simeq \mathrm{S} \times \mathrm{S} \to \mathrm{G} \times \mathrm{G}$. L'image de $d \times e$ par le morphisme multiplication $m : \mathrm{G} \times \mathrm{G} \to \mathrm{G}$ (cf. 1.2) sera appelé le produit de d et e et sera noté $d \cdot e$.

[15] N.D.E. : revoir ce qui suit, en liaision avec II, 3.12–14 et surtout § avant 3.12.

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.

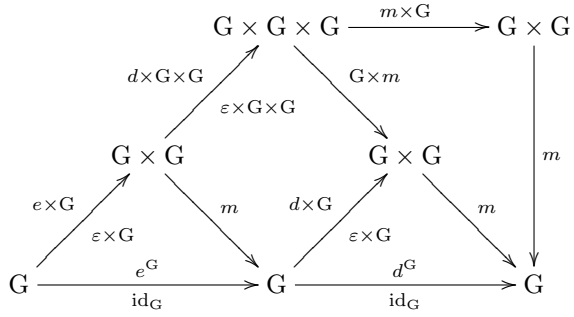
Lorsque T parcourt les préschémas au-dessus de S, l'algèbre infinitésimale $U(G_T)$ du T-groupe $G \times T$ varie évidemment de façon contravariante en T, de sorte que nous pourrons parler du foncteur algèbre infinitésimale.

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. [16]

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 $m \circ (\varepsilon \times \mathrm{id}_G) = \mathrm{id}_G$, c.-à-d., un élément de $\mathrm{Dif}_{G/S}$.

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



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 $e \times G$ et $d \times G \times G$ est $(d \times e) \times G$ (cf. 1.2.2), son image par $m \times G$ est $(d \cdot e) \times G$, et l'image de celle-ci par m est donc égale à $(d \cdot e)^G$.

On obtient ainsi un homomorphisme de $\Gamma(\mathscr{O}_S)$-algèbres, appelé *translation à droite* :

$$U(G) \longrightarrow \mathrm{Dif}_{G/S}\,.$$

[16] N.D.E. : Dans l'original, le faisceau est désigné par « l'Algèbre », la différence avec « l'algèbre » des sections sur un ouvert se faisant par l'usage de la majuscule A.

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

2.3. Nous allons maintenant caractériser les opérateurs différentiels de G sur S de la forme d^G. Soient $g : S \to G$ 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 :

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

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

$$D^g = g_G^{-1} D \, g_G.$$

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

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 :* $D\,m = m(D \times G)$.

(ii) $\Rightarrow$ (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 :

$$\begin{array}{ccccc}
G & \xleftarrow{m} & G \times G & \xleftarrow{h} & G \\
{\scriptstyle D}\downarrow{\scriptstyle id_G} & & {\scriptstyle D\times G}\downarrow{\scriptstyle id_{(G\times G)}} & & {\scriptstyle D}\downarrow{\scriptstyle id_G} \\
G & \xleftarrow{m} & G \times G & \xleftarrow{h} & G
\end{array} \quad .$$

(i) $\Rightarrow$ (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 :

$$\begin{array}{ccccc}
G \times G & \xrightarrow{\Delta_{G\times G}} & G \times G & \xrightarrow{\mathrm{pr}_1} & G \\
{\scriptstyle D_G}\downarrow{\scriptstyle id_{G\times G}} & & {\scriptstyle D_G}\downarrow{\scriptstyle id_{G\times G}} & & {\scriptstyle D}\downarrow{\scriptstyle id_G} \\
G \times G & \xrightarrow{\Delta_{G\times G}} & G \times G & \xrightarrow{\mathrm{pr}_1} & G
\end{array} \quad .$$

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

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

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

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 $S \xrightarrow{\varepsilon} G \xrightarrow[\mathrm{id}_G]{D} G$. L'opérateur différentiel invariant à droite $(D_0)^G$ est alors obtenu par composition :

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

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

$$D = D\,m(\varepsilon\times G) = m(D\times G)(\varepsilon\times G) = (D_0)^G.$$

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

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

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

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

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

2.4.1. Remarque. — Considérons le diagramme commutatif

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

où η désigne le morphisme « $(x, y) \mapsto yx^{-1}$ » [17]. Celui-ci induit des morphismes

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

Pour tout entier $n \geqslant 1$, posons $\mathfrak{p}^n_{\mathrm{G/S}} = \varepsilon^{-1}(\mathscr{O}_{\mathrm{G}})/\mathscr{I}_\varepsilon^{n+1}$ (confer 1.3 et 1.4 pour les notations). [18] Comme le carré formé par les morphismes ε, η, Δ et p est cartésien, $\Delta^{-1}(\eta')$ induit un *isomorphisme de $\mathscr{O}_{\mathrm{G}}$-modules* :

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

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

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

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

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

On retrouve ainsi l'isomorphisme du théorème 2.4.

2.5. [19] Soit Lie(G) l'algèbre de Lie de G [20] ; on va définir un morphisme de $\Gamma(\mathscr{O}_{\mathrm{S}})$-algèbres de Lie $\alpha : \mathrm{Lie(G)} \to \mathrm{U(G)}$.

Soient $s : \mathrm{S} \to \mathrm{I_S}$ la section nulle de $\mathrm{I_S} \to \mathrm{S}$ et σ la déviation de s définie en 1.2.1. Rappelons (cf. II, 3.8.ter) que Lie(G) est l'ensemble des morphisme $x : \mathrm{I_S} \to \mathrm{G}$ tel que $x \circ s = \varepsilon_{\mathrm{G}}$. Alors la composée

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

est une S-déviation de ε_{G}, i.e. un élément de U(G) ; avec les notations de 1.2 (†), elle notée σx. De plus, d'après 1.2.1, l'application $\alpha : x \mapsto \sigma x$ est un isomorphisme de

---

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

[18] 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.

[19] N.D.E. : Dans ce paragraphe, on a ajouté des détails et modifié l'ordre, en commençant par définir l'application $\alpha : \mathrm{Lie(G)} \to \mathrm{U(G)}$.

[20] N.D.E. : Dans cet exposé, si G (resp. X) est un S-préschéma en groupes (resp. un S-préschéma), l'« algèbre de Lie » Lie(G) (resp. Lie($\underline{\mathrm{Aut}}$ X)) désigne, avec les notations de l'exposé II, $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ (resp. $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}_{\mathrm{S}}(\mathrm{X})/\mathrm{S})(\mathrm{S})$) ; c'est une $\Gamma(\mathscr{O}_{\mathrm{S}})$-algèbre de Lie, d'après II, 4.11 et 3.14.

$\mathscr{O}_S(S)$-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 homomorphisme d'algèbres de Lie. (21) Soit

$$\delta : U(G) \xrightarrow{\sim} \mathrm{Dif}^G_{G/S} \subseteq \mathrm{Dif}_{G/S}$$

la « translation à droite » définie en 2.2, c.-à-d., l'homomorphisme d'algèbres qui à une S-déviation d de ε_G associe l'opérateur différentiel invariant à droite $d^G \in \mathrm{Dif}_{G/S}$.

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

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

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 $I_S \times G$ induisant l'identité sur G. Comme γ est un monomorphisme, il en est de même du morphisme $\underline{\mathrm{Lie}}(\gamma) : \underline{\mathrm{Lie}}(G/S) \to \underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}_S(G)/S)$ (voir, par exemple, Exp. II, N.D.E. (46)), donc $\mathrm{Lie}(\gamma) : \mathrm{Lie}(G) \to \mathrm{Lie}(\underline{\mathrm{Aut}}\, G)$ 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 :

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

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

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

$$\begin{array}{ccc} I_S \times G & \xrightarrow{\mathrm{Lie}(\gamma)(x)} & I_S \times G \\ \downarrow{\scriptstyle x\times G} & & \downarrow{\scriptstyle \mathrm{pr}_2} \\ G \times G & \xrightarrow{m} & G \end{array} .$$

Compte-tenu de ce diagramme, l'image de Lie(γ)(x) par β est la déviation composée **424**

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

qui, d'après 2.2, n'est autre que $(\sigma x)^G$, c.-à-d., $\delta(\alpha(x))$. On obtient donc un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Lie}(G) & \xrightarrow{\mathrm{Lie}(\gamma)} & \mathrm{Lie}(\underline{\mathrm{Aut}}\, G) \\ \alpha\downarrow & & \downarrow\beta \\ U(G) & \xrightarrow{\delta} & \mathrm{Dif}_{G/S} \end{array}$$

où Lie(γ), β et δ sont des morphismes d'algèbres de Lie. Comme δ est injectif, il en résulte que α est aussi un morphisme d'algèbres de Lie. Par conséquent, on a obtenu :

(21) N.D.E. : Voir aussi II, 4.11.

Proposition. — *α est un isomorphisme de $\mathscr{O}_S(S)$-algèbres de Lie de* Lie(G) *dans l'algèbre de Lie des* S*-dérivations de ε_G, elle-même isomorphe* (d'après 2.4) *à l'algèbre de Lie des* S*-dérivations de* G *invariantes à droite.* (22)

3. Coalgèbres et dualité de Cartier

425

3.1. Soit S un préschéma (ou, plus généralement, un espace annelé). Une *$\mathscr{O}_S$-coalgèbre* (23) 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*) tels que :

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

(ii) Le carré

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

soit 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

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

426 soient commutatifs. Les morphismes de coalgèbres se composent comme les mor-

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

(23) N.D.E. : On dit aussi « *cogèbre* », cf. [**BAlg**, III, § 11.1]. D'autre part, dans cet exposé (ainsi que dans VII_B), toutes les coalgèbres considérées sont supposées *cocommutatives*, c.-à-d., vérifient la condition (i) ci-dessous.

phismes de $\mathscr{O}_S$-modules de sorte que nous pourrons parler de la catégorie des $\mathscr{O}_S$-coalgèbres.

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

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

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 $\varepsilon_{\mathscr{U}} \otimes \mathrm{id}_{\mathscr{V}}$.

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 augmentation 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 : **427**

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-préschéma $q : T \to S$, $q^*(\mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U})$ 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 : [24]

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

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, si $\mathscr{A}$ est une $\mathscr{O}_S$-algèbre commutative qui est localement libre de type fini en tant que $\mathscr{O}_S$-module, on a des isomorphismes

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

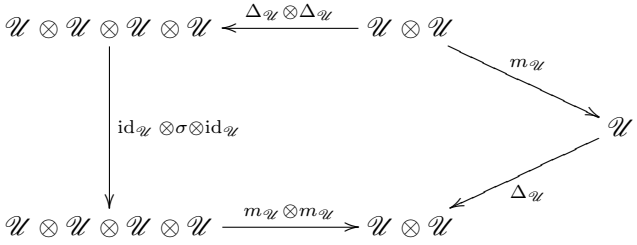
[24] N.D.E. : Pour tout $x \otimes y \in \Gamma(T, \mathscr{U}_T) \otimes_{\mathscr{O}(T)} \Gamma(T, \mathscr{U}_T)$, son image dans $\Gamma(T, \mathscr{U}_T \otimes_{\mathscr{O}_T} \mathscr{U}_T)$ est encore notée $x \otimes y$.

d'où :

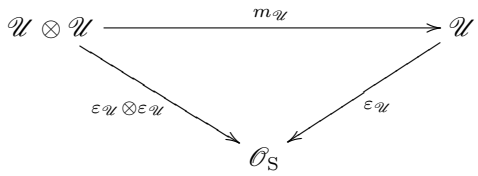
$$\mathrm{Spec}^*\,\mathscr{A}^* \simeq \mathrm{Spec}\,\mathscr{A}\,.$$

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 d'un morphisme de
428 $\mathscr{O}_S$-coalgèbres $m_{\mathscr{U}} : \mathscr{U}\otimes\mathscr{U} \to \mathscr{U}$. Un tel morphisme est un morphisme de $\mathscr{O}_S$-modules rendant commutatifs les diagrammes suivants :

(iv)



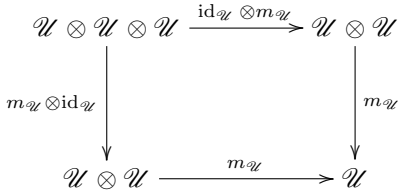
(v)



.

Le morphisme de $\mathscr{O}_S$-coalgèbres $m_{\mathscr{U}}$ doit en outre vérifier les conditions (ii)*, (iii)* et (vi) ci-dessous :

(ii)* Le carré



est commutatif.

(iii)* Il existe un morphisme de $\mathscr{O}_S$-coalgèbres $\eta_{\mathscr{U}} : \mathscr{O}_S \to \mathscr{U}$ tel que les morphismes composés

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

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

soient les morphismes identiques de $\mathscr{U}$.

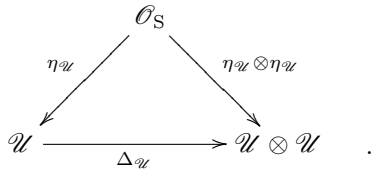
(vi) Il existe un morphisme de $\mathscr{O}_S$-coalgèbres $c_{\mathscr{U}} : \mathscr{U} \to \mathscr{U}$ tel que le morphisme composé

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

429 soit égal à $\eta_{\mathscr{U}} \circ \varepsilon_{\mathscr{U}}$.

3.2.1. — Les morphismes $\eta_{\mathscr{U}}$ et $c_{\mathscr{U}}$ de (iii)* et (vi) sont évidemment uniques. 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 la coalgèbre en groupes opposée [25] ; 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-préschéma 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 $c_{\mathscr{U}}(x)$.

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

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

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

3.2.3. — [26] 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-préschéma. 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

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

[25] N.D.E. : Les éditeurs n'ont pas cherché à comprendre cette assertion pour une catégorie arbitraire.
[26] N.D.E. : On a détaillé ce paragraphe.

et donc

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

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

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

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

c'est-à-dire :

$$\begin{cases} \varepsilon(u_0) = 1, & \Delta u_0 = u_0 \otimes u_0, \qquad (\text{i.e. } u_0 \in \mathrm{G}(\mathrm{T})) \\ \varepsilon(u_i) = 0, & \Delta(u_i) = u_1 \otimes u_0 + u_0 \otimes u_i, \ \text{pour } i = 1, \ldots, r. \end{cases} \tag{2}$$

De plus, le morphisme $\mathrm{G}(\mathrm{I_T}(\mathscr{M})) \to \mathrm{G}(\mathrm{T})$ correspondant à la section nulle de $\mathrm{I_T}(\mathscr{M}) \to \mathrm{T}$ 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 $\mathscr{O}_\mathrm{S}$-module libre de rang fini, le diagramme d'ensembles

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

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

Notons $\operatorname{Prim}\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$ le sous-$\mathscr{O}(\mathrm{T})$-module de $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$ formé des *éléments primitifs*, c.-à-d., des éléments u qui vérifient :

$$\Delta u = u \otimes 1 + 1 \otimes u, \qquad \varepsilon(u) = 0. \tag{27}$$

Comme $(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$ est l'ensemble des éléments de $u_0 + ud \in \mathrm{G}(\mathrm{I_T})$ au-dessus de l'élément unité $u_0 = 1$ de $\mathrm{G}(\mathrm{T})$, on obtient un isomorphisme de $\mathscr{O}(\mathrm{T})$-modules, fonctoriel en T : (28)

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

D'autre part, on déduit de (1) que

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

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 (II, 4.4), et donc G est un bon S-foncteur en groupes (II, 4.6).

Enfin, montrons que G est très bon, c.-à-d., que le « crochet » sur $(\underline{\mathrm{Lie}}\,\mathrm{G})(\mathrm{T})$ est bien un crochet de Lie (cf. II, 4.10).

---

(27) N.D.E. : Puisque $u = (\mathrm{id} \otimes \varepsilon)\Delta(u) = u + \varepsilon(u)$, la deuxième condition est en fait conséquence de la première.

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

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 :

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

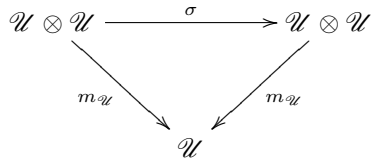
D'après la description du crochet $[u, v]$ donnée avant la Prop. 4.8 de l'Exp. II, on **431**
obtient que

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

où le terme de droite est le commutateur de u et v dans l'algèbre $\Gamma(\mathrm{T}, \mathscr{U}_\mathrm{T})$. Ceci prouve que G est très bon.

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. En particulier : *si de plus $\mathscr{U}$ est un $\mathscr{O}_\mathrm{S}$-module quasi-cohérent, le* S*-préschéma affine* $\mathrm{Spec}\,\mathscr{U}$ *est un* S*-préschéma en groupes commutatifs.*

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

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

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 homomorphisme 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 :

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

Comme cette formule reste valable après tout changement de base, on a finalement : **432**

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

pour toute $\mathscr{O}_\mathrm{S}$*-coalgèbre en groupes commutatifs quasi-cohérente* $\mathscr{U}$*.*

3.3.1. — Si l'on suppose de plus que $\mathscr{U}$ est un $\mathscr{O}_\mathrm{S}$-module localement libre de type fini, $\mathrm{Spec}^*\,\mathscr{U}$ est également représentable et l'on a (cf. 3.1.2) :

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

Le foncteur $\mathscr{U} \mapsto \mathscr{U}^* = \mathscr{H}om_{\mathscr{O}_S\text{-Mod.}}(\mathscr{U}, \mathscr{O}_S)$ induit donc une dualité [(*)] de la catégorie des S-préschémas en groupes commutatifs finis et localement libres sur S (c'est la *dualité de Cartier*). D'après 3.3, cette dualité associe à un tel S-groupe G le S-groupe $\underline{\mathrm{Hom}}_{\text{S-gr.}}(G, \mathbb{G}_{m,S})$.

4. « Frobeniuseries »

433

Soient p un nombre premier fixé et $(\mathbf{Sch}_{/\mathbb{F}_p})$ la catégorie des préschémas de caractéristique p, c'est-à-dire des préschémas 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 $\mathrm{Hom}(\mathbf{h}_X, F)$ sur $F(X)$ défini en I 1.1 pour identifier ces deux ensembles chaque fois que X est un $\mathbb{F}_p$-préschéma et F un objet de $(\widehat{\mathbf{Sch}_{/\mathbb{F}_p}})$.

4.0. Notations. — [(30)] Si T est un $\mathbb{F}_p$-préschéma, un T-foncteur est un morphisme $q : F \to T$ de $(\widehat{\mathbf{Sch}_{/\mathbb{F}_p}})$ qui a T pour but ; pour tout T-préschéma $r : X \to T$, l'ensemble des T-morphismes $X \to F$, i.e. des $\mathbb{F}_p$-morphismes $s : X \to F$ tels que $q \circ s = r$, sera alors noté $q(r)$, $q(X/T)$, $F(r)$ ou $F(X/T)$ (ou même $F(X)$ lorsqu'aucune confusion ne sera possible avec $\mathrm{Hom}(\mathbf{h}_X, F)$).

4.1. Pour tout préschéma 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 ↦ fr(S) est un *endomorphisme du foncteur identique* de $(\mathbf{Sch}_{/\mathbb{F}_p})$ [(31)], 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 $\mathbb{F}_p$-préschéma 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 ↦ fr(E) est un *endomorphisme du foncteur identique* de $(\widehat{\mathbf{Sch}_{/\mathbb{F}_p}})$ (que nous noterons encore fr).

(*) 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 $\varphi : \mathrm{Id}_{\mathscr{C}} \to DD$ tel que les isomorphismes $\varphi D : D \to DDD$ et $D\varphi^{-1} : DDD \to D$ soient réciproques l'un de l'autre. [(29)]

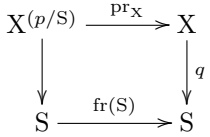
(29) N.D.E. : On a corrigé $D\varphi$ en $D\varphi^{-1}$.

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

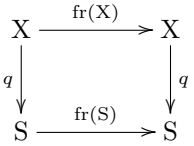
(31) N.D.E. : c.-à-d., pour tout morphisme de $\mathbb{F}_p$-préschémas $f : Y \to X$, le diagramme ci-dessous est commutatif :

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

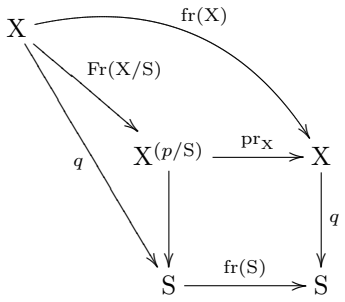
Pour tout $\mathbb{F}_p$-préschéma S et tout S-foncteur $q : X \to S$, nous notons $X^{(p/S)}$ ou $X^{(p)}$ l'image réciproque de X par le changement de base fr(S) :



Le carré commutatif

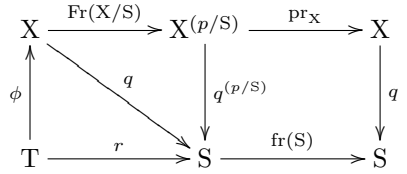


induit alors un S-morphisme noté Fr(X/S) (ou simplement Fr) de X dans $X^{(p/S)}$ tel **434**
que $\mathrm{fr}(X) = \mathrm{pr}_X \circ \mathrm{Fr}(X/S)$:



Nous dirons que 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.

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



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

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

caractérisée par la commutativité du carré suivant :

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

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

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

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

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

$$\mathrm{X}_\mathrm{T}^{(p/\mathrm{T})} \xrightarrow{\sim} (\mathrm{X}^{(p/\mathrm{S})})_\mathrm{T}.$$

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

En particulier, si S est le spectre du corps premier $\mathbb{F}_p$, $\mathrm{X}^{(p/\mathrm{S})}$ est égal à X et Fr(X/S) à fr(X). Par conséquent, $\mathrm{X}_\mathrm{T}^{(p/\mathrm{T})}$ s'identifie à X_T et $\mathrm{Fr}(\mathrm{X}_\mathrm{T}/\mathrm{T})$ à $\mathrm{fr}(\mathrm{X})_\mathrm{T}$. Soient par exemple E un ensemble et E_T le T-préschéma constant de type E ; on a alors $\mathrm{E}_\mathrm{T}^{(p/\mathrm{T})} \simeq \mathrm{E}_\mathrm{T}$ et $\mathrm{Fr}(\mathrm{E}_\mathrm{T}/\mathrm{T}) \simeq \mathrm{id}_{\mathrm{E}_\mathrm{T}}$.

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

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

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

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

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

Par exemple, lorsque T est le préschéma I_R des nombres duaux sur un S-préschéma R, $\mathrm{fr}(\mathrm{I}_\mathrm{R})$ se factorise comme suit :

$$\mathrm{I}_\mathrm{R} \xrightarrow{\mathrm{can.}} \mathrm{R} \xrightarrow{\mathrm{fr}(\mathrm{R})} \mathrm{R} \xrightarrow{s} \mathrm{I}_\mathrm{R},$$

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

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

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

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

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

On notera que $\mathrm{Fr}(\mathrm{X}^{(p)}/\mathrm{S})$ coïncide avec $\mathrm{Fr}(\mathrm{X}/\mathrm{S})^{(p)}$, c.-à-d., le diagramme suivant est commutatif :

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

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

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

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

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

4.1.4. — Voici quelques exemples.

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

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

b) Considérons maintenant un préschéma 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). De plus, d'après 4.1 (†) , l'application **437**

$\mathrm{Fr}(\mathbf{W}(\mathscr{E}))(q)$ est déterminée pour tout S-préschéma T par le triangle commutatif

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

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

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

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

c) On verrait de même que, pour toute $\mathscr{O}_\mathrm{S}$-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 $\mathscr{O}_\mathrm{S}$, on a donc

$$\mathscr{A}^{(p)} = \mathscr{A} \otimes_\pi \mathscr{O}_\mathrm{S} \qquad (33)$$

et il est clair que $\mathrm{Fr}((\mathrm{Spec}\,\mathscr{A})/\mathrm{S})$ est induit par l'homomorphisme $a \otimes_\pi x \mapsto a^p x$ de $\mathscr{A} \otimes_\pi \mathscr{O}_\mathrm{S}$ dans $\mathscr{A}$.

Pour tout $\mathscr{O}_\mathrm{S}$-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 $\mathscr{O}_\mathrm{S}$-module $\mathscr{E}$.

438 **d)** Soient $\mathscr{U}$ une $\mathscr{O}_\mathrm{S}$-coalgèbre (3.1) et T un préschéma de caractéristique p. Si $\mathscr{U}^{(p/\mathrm{S})}$ 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-préschéma 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.

---

(33) N.D.E. : $\mathscr{A} \otimes_\pi \mathscr{O}_\mathrm{S}$ désigne la $\mathscr{O}_\mathrm{S}$-algèbre obtenue par l'extension des scalaires $\pi : \mathscr{O}_\mathrm{S} \to \mathscr{O}_\mathrm{S}$, c.-à-d., on a : $ax \otimes_\pi 1 = a \otimes_\pi x^p$, et $x \cdot (a \otimes_\pi 1) = a \otimes_\pi x$.

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

Nous désignons alors par $U^p(X)$ le sous-préschéma 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 $U^p(X)$ 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 $U^p(X) = X_S^p$.

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

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

Considérons maintenant le morphisme diagonal δ de X dans $U^p(X)$. La restriction de δ à l'ouvert U ci-dessus est définie par l'homomorphisme d'algèbres

$$\eta : \bigotimes_R^p A \longrightarrow A, \qquad a_1 \otimes \cdots \otimes a_p \mapsto a_1 a_2 \cdots a_p.$$

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

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

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

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

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

De plus, si $i(X)$ désigne l'inclusion de $X^{[p/S]}$ dans $V^p(X)$, nous venons de voir que $q'(X) \circ \delta$ se factorise à travers $X^{[p/S]}$, d'où un morphisme $F^{[p]}(X/S) : X \to X^{[p/S]}$: [34]

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

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

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

4.2.1. — Les préschémas $\mathrm{X}^{[p/\mathrm{S}]}$ et $\mathrm{X}^{(p/\mathrm{S})}$ sont évidemment reliés : soient V un ouvert
440 affine de S d'anneau affine R et U un ouvert affine de X au-dessus de V ; soit A 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

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

définit un homomorphisme de R-algèbres de $\mathrm{A} \otimes_\pi \mathrm{R}$ dans $\Sigma^p \mathrm{A}/\mathrm{N}(\bigotimes_{\mathrm{R}}^{p} \mathrm{A})$; cet homomorphisme induit un morphisme

$$\varphi(\mathrm{U}) : \mathrm{U}^{[p/\mathrm{S}]} \longrightarrow \mathrm{U}^{(p/\mathrm{S})} \qquad \text{tel que} \quad \varphi(\mathrm{U}) \circ \mathrm{F}^{[p]}(\mathrm{U}/\mathrm{S}) = \mathrm{Fr}(\mathrm{U}/\mathrm{S}).$$

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

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

Par exemple, si X est le sous-préschéma de S défini par un idéal quasi-cohérent $\mathscr{I}$, $\mathrm{F}^{[p]}(\mathrm{X}/\mathrm{S})$ s'identifie au morphisme identique de X, de sorte que $\varphi(\mathrm{X})$ est l'immersion canonique de $\mathrm{Spec}(\mathscr{O}_{\mathrm{S}}/\mathscr{I})$ dans $\mathrm{Spec}(\mathscr{O}_{\mathrm{S}}/\mathscr{I}^{\{p\}})$. On voit ainsi que $\varphi(\mathrm{X})$ n'est pas un isomorphisme en général.

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

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

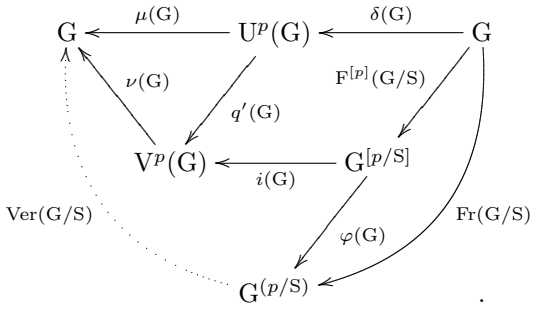
est bijective ; cette application reste donc bijective lorsque M est R-plat, parce que tout module plat est une limite inductive filtrante de modules libres (Lazard [(*)] [(35)]). Il s'ensuit que

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

[(*)] D. Lazard, C. R. Acad. Sc. Paris **258**, 1964, p. 6313-6316.

[(35)] N.D.E. : Voir aussi : D. Lazard, Bull. Soc. Math. France **97** (1969), 81-128, ou : N. Bourbaki, *Algèbre*, Chap. 10, § 1.6, Th. 1.

4.3. Considérons enfin un S-*préschéma en groupes abéliens* G. Alors, le morphisme composé $\mu(G) : U^p(G) \xrightarrow{\text{incl.}} G_S^p \to G$, qui est défini par la multiplication, se factorise à travers $V^p(G)$, de sorte qu'on a le diagramme commutatif suivant :



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

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

à l'aide de la formule $\mathrm{Ver}(G/S) = \nu(G) \circ i(G) \circ \varphi(G)^{-1}$. Lorsque G parcourt les S-préschémas plats en groupes abéliens, l'application 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-préschéma 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 $\mu(G) \cdot \delta(G)$, obtenant ainsi la formule classique

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

4.3.1. — Par exemple, lorsque G est un S-préschéma constant en groupes abéliens, nous savons que Fr(G/S) s'identifie au morphisme identique de G (4.1.1). On a donc $\mathrm{Ver}(G/S) = p\,\mathrm{id}_G$.

Lorsque G est le S-groupe diagonalisable de type M, Fr(G/S) est égal à $p\,\mathrm{id}_G$ d'après 4.1.2 ; on voit facilement que Ver(G/S) est le morphisme identique de G.

Lorsque $\mathscr{E}$ est un $\mathscr{O}_S$-module plat et que G est le S-groupe $\mathbb{V}(\mathscr{E})$, le morphisme **442**
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 $G^{(p^n)} = (G^{(p^{n-1})})^{(p)}$).

4.3.2. — Comme l'application Ver : G ↦ Ver(G/S) est un homomorphisme fonctoriel lorsque G parcourt les S-*préschémas plats en groupes commutatifs*, le carré

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

est commutatif (où $\mathrm{Fr}(\mathrm{G/S})^{(p)}$ désigne l'image réciproque de Fr(G/S) par le changement de base fr(S)). Comme il résulte directement des définitions que $\mathrm{Fr}(\mathrm{G/S})^{(p)}$ est égal à $\mathrm{Fr}(\mathrm{G}^{(p)}/\mathrm{S})$ [(36)], on a aussi

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

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

443 [(37)] On désigne par $\Sigma^p\mathscr{A}$ la sous-algèbre de $\bigotimes^p_{\mathscr{O}_\mathrm{S}} \mathscr{A}$ formée des sections invariantes sous l'action du groupe symétrique, par $i(\mathscr{A})$ l'inclusion de $\Sigma^p\mathscr{A}$ dans le produit tensoriel. Soit $\Delta^p(\mathscr{A}) : \mathscr{A} \to \bigotimes^p_{\mathscr{O}_\mathrm{S}} \mathscr{A}$ le morphisme obtenu en itérant le morphisme diagonal de la coalgèbre $\mathscr{A}$ (il correspond au morphisme de multiplication de $\mathrm{U}^p(\mathrm{G}) = \mathrm{G}^p_\mathrm{S}$ 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 $i(\mathscr{A}) \circ a(\mathscr{A}) = \Delta^p(\mathscr{A})$.

D'autre part, soient $\mathcal{S}^p(\mathscr{A})$ la composante de degré p de l'algèbre symétrique de $\mathscr{A}$ et $q(\mathscr{A}) : \bigotimes^p_{\mathscr{O}_\mathrm{S}} \mathscr{A} \to \mathcal{S}^p(\mathscr{A})$ la projection canonique. La multiplication $m^p(\mathscr{A}) : \bigotimes^p_{\mathscr{O}_\mathrm{S}} \mathscr{A} \to \mathscr{A}$ 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

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

cet homomorphisme s'annule sur les sections de la forme

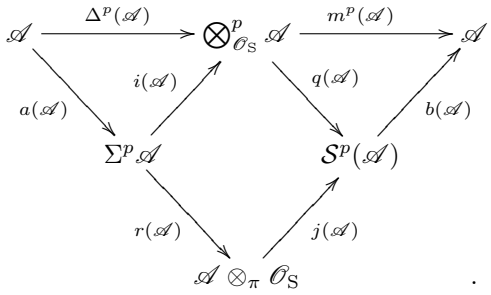
$$\sum_{\sigma \in \mathscr{S}_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}$$

[(36)] N.D.E. : Voir 4.1.3.

[(37)] N.D.E. : On a modifié l'ordre, en introduisant d'abord les objets intervenant dans le diagramme qui va suivre.

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.*

5. p-algèbres de Lie

444

Rappelons d'abord quelques résultats du Séminaire Sophus Lie. [38]

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 on a, notant N l'opérateur de symétrisation (cf. 4.2) :

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

[38] 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).

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, $i_1,\dots,i_r$ les suites strictement croissantes d'entiers de l'intervalle $[1,p-1]$ et où $j_1,\dots,j_s$ désigne la suite strictement croissante dont les valeurs sont les entiers de $[1,p-1]$ différents de $i_1,\dots,i_r$. 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

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

445 où ρ parcourt les permutations de $p-1$ lettres. L'égalité, dans $\mathbb{F}_p[x]$,

$$(x-1)^p = x^p - 1 = (x-1)(x^{p-1}+\cdots+1),$$

d'où $(x-1)^{p-1} = x^{p-1}+\cdots+1$, montre d'autre part que $(-1)^s\binom{p-1}{s}$ est égal à 1 en caractéristique p, ce qui prouve $(*)$. (39)

En particulier, 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

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

(40) Or, d'après $(*)$, on a :

$$\mathrm{N}(\underbrace{x_0,\dots,x_0}_{r},\underbrace{x_1,\dots,x_1}_{p-r}) = r!(p-1-r)!\sum_{t}\big[x_{t(1)}\big[x_{t(2)}\big[\cdots\big[x_{t(p-1)},x_1\big]\cdots\big]\big]\big]$$

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* :

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

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

(39) N.D.E. : On peut aussi utiliser l'égalité $\binom{p-1}{r} = \frac{p-r}{r}\binom{p-1}{r-1}$ pour conclure que $\binom{p-1}{r} = (-1)^r$ en caractéristique p.

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

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

où t parcourt les applications $[1, p-1] \to \{0, 1\}$ prenant r fois la valeur 0 ($x_0, x_1 \in \mathfrak{g}$). **446**

Par exemple, si A est une R-algèbre associative, nous avons vu en 5.1 qu'on obtenait une p-algèbre de Lie $\mathrm{A}_{\mathrm{Lie}}$ 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 préschéma de caractéristique $p > 0$ et X un S-préschéma. 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 composés 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 structure de *p-algèbre de Lie sur $\mathscr{R}$* si, pour tout ouvert U, $\Gamma(\mathrm{U}, \mathfrak{g})$ est muni d'une structure **447**
de p-algèbre de Lie sur $\Gamma(\mathrm{U}, \mathscr{R})$ et si les restrictions sont des homomorphismes.

5.3. Nous nous intéressons maintenant au foncteur adjoint à gauche du foncteur $\mathrm{A} \mapsto \mathrm{A}_{\mathrm{Lie}}$ de 5.2. Soient $\mathfrak{g}$ une p-algèbre de Lie sur l'anneau R de caractéristique p, $\mathrm{U}(\mathfrak{g})$ l'algèbre enveloppante de l'algèbre de Lie sous-jacente à $\mathfrak{g}$ (cf. Bourbaki, Groupes et algèbres de Lie, Chap. I, § 2) et $i_{\mathfrak{g}}$ (ou simplement i) l'application canonique $\mathfrak{g} \to \mathrm{U}(\mathfrak{g})$.

Soit A une R-algèbre associative unitaire. On sait que, pour tout homomorphisme d'algèbres de Lie $\phi : \mathfrak{g} \to \mathrm{A}_{\mathrm{Lie}}$ il existe un unique homomorphisme de R-algèbres unitaires $\psi : \mathrm{U}(\mathfrak{g}) \to \mathrm{A}$ 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 $\mathfrak{g}$. Par conséquent, si $\mathrm{U}_p^{\mathrm{R}}(\mathfrak{g})$ ou $\mathrm{U}_p(\mathfrak{g})$ désigne le quotient de $\mathrm{U}(\mathfrak{g})$ par l'idéal bilatère engendré par les éléments $i(x)^p - i(x^{(p)})$, et si $j_{\mathfrak{g}}$ (ou simplement j) est l'application $\mathfrak{g} \to \mathrm{U}_p(\mathfrak{g})$ composée de $i : \mathfrak{g} \to \mathrm{U}(\mathfrak{g})$ et de l'application canonique $\mathrm{U}(\mathfrak{g}) \to \mathrm{U}_p(\mathfrak{g})$, on voit que pour tout homomorphisme de p-algèbres de Lie $\phi : \mathfrak{g} \to \mathrm{A}_{\mathrm{Lie}}$, il existe un unique homomorphisme d'algèbres unitaires $\psi : \mathrm{U}_p(\mathfrak{g}) \to \mathrm{A}$ tel que $\psi \circ j = \phi$.

On dit que $\mathrm{U}_p(\mathfrak{g})$ est *l'algèbre enveloppante restreinte de* $\mathfrak{g}$.

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) :

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

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

D'autre part, il est clair que $\beta(\lambda x) = \lambda^p \beta(x)$, pour $\lambda \in \mathrm{R}$, 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. — [(41)] Soit $\mathfrak{g}$ une R-algèbre de Lie dont le R-module sous-jacent est libre de base (x_α). Dans ce cas, d'après le théorème de Poincaré-Birkhoff-Witt (cf. Bourbaki, *Groupes et algèbres de Lie*, I, § 2.7), on peut identifier $\mathfrak{g}$ à un sous-module de $\mathrm{U}(\mathfrak{g})$ au moyen de i.

Proposition. — *Les structures de p-algèbre de Lie sur $\mathfrak{g}$ correspondent biunivoquement aux familles (y_α) de $\mathfrak{g}$ telles que* $\operatorname{ad} y_\alpha = (\operatorname{ad} x_\alpha)^p$.

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 p-structure.

Réciproquement, 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 $\pi : \mathrm{R} \to \mathrm{R}$. [(42)]

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

[(42)] 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 $x \in \mathfrak{g}$, $r \in \mathrm{R}$.

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 :

$$x^{(p)} = \sum \lambda_\alpha^p \, y_\alpha + z$$

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).

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

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

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. Bourbaki, *Groupes et algèbres de Lie*, 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 $\mathrm{U}_p(\mathfrak{g}) = \mathrm{U}(\mathfrak{g})/\mathrm{J}$. C.Q.F.D.

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
450 de caractéristique p, pour q_0 l'homomorphisme $\lambda \otimes x \mapsto \lambda x$ ($\mathfrak{g}$ est libre sur $\mathbb{F}_p$!). Le 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 $\mathrm{R}' \otimes_\mathrm{R} q_1$ est manifestement un homomorphisme de p-algèbres de Lie, le noyau de $\mathrm{R}' \otimes_\mathrm{R} q_0$ est un p-idéal, de sorte que l'opération puissance p-ième symbolique de $\mathrm{R}' \otimes_\mathrm{R} \mathrm{L}_0$ induit par passage au quotient une application de $\mathrm{R}' \otimes_\mathrm{R} \mathfrak{g}$ dans $\mathrm{R}' \otimes_\mathrm{R} \mathfrak{g}$ (utiliser

la formule (ii) de 5.2.) ; cette dernière munit $\mathrm{R}' \otimes_{\mathrm{R}} \mathfrak{g}$ de la structure de p-algèbre de Lie cherchée.

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

$$\mathrm{R}' \otimes_{\mathrm{R}} j_{\mathfrak{g}} : \quad \mathrm{R}' \otimes_{\mathrm{R}} \mathfrak{g} \longrightarrow \mathrm{R}' \otimes_{\mathrm{R}} \mathrm{U}_p(\mathfrak{g}),$$

d'où un homomorphisme

$$h : \mathrm{U}_p(\mathrm{R}' \otimes_{\mathrm{R}} \mathfrak{g}) \longrightarrow \mathrm{R}' \otimes_{\mathrm{R}} \mathrm{U}_p(\mathfrak{g})$$

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

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

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

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

a) Si $\mathfrak{h} = 0$, $\mathrm{U}_p(\mathfrak{h})$ s'identifie à l'anneau de base et $\mathrm{U}_p(\phi)$ est un homomorphisme d'algèbres $\varepsilon_{\mathfrak{g}} : \mathrm{U}_p(\mathfrak{g}) \to \mathrm{R}$ 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 $\mathrm{U}_p(\mathfrak{g}^\circ)$ à l'algèbre opposée à $\mathrm{U}_p(\mathfrak{g})$. De plus, l'isomorphisme $x \mapsto -x$ de $\mathfrak{g}$ sur $\mathfrak{g}^\circ$ induit un isomorphisme $c_{\mathfrak{g}}$ de $\mathrm{U}_p(\mathfrak{g})$ sur $\mathrm{U}_p(\mathfrak{g}^\circ) \simeq \mathrm{U}_p(\mathfrak{g})^\circ$. On dit que $c_{\mathfrak{g}}$ est l'*antipodisme* de $\mathrm{U}_p(\mathfrak{g})$.

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 symbolique étant définis par les formules

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

Si $h_1 : \mathfrak{f} \to \mathfrak{k}$ et $h_2 : \mathfrak{g} \to \mathfrak{k}$ sont deux homomorphismes de p-algèbres de Lie **452**
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 $\varphi : \mathrm{U}_p(\mathfrak{g}\times\mathfrak{g}) \xrightarrow{\sim} \mathrm{U}_p(\mathfrak{g})\otimes\mathrm{U}_p(\mathfrak{g})$.

On voit 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* (3.2) qui a $\varepsilon_{\mathfrak{g}}$ pour augmentation et $c_{\mathfrak{g}}$ pour antipodisme.

5.4.1. — De même, soient S un préschéma de caractéristique p et $\mathscr{G}$ une $\mathscr{O}_{\mathrm{S}}$-p-algèbre de Lie. Lorsque V parcourt les ouverts de S, les structures de coalgèbres en groupes définies précédemment sur les ensembles $\mathrm{U}_p(\Gamma(\mathrm{V},\mathscr{G}))$ induisent sur le faisceau associé, i.e. sur l'algèbre enveloppante restreinte $\mathscr{U}_p(\mathscr{G})$, une structure de $\mathscr{O}_{\mathrm{S}}$-p-coalgèbre en groupes. D'après 5.3.1, le S-foncteur en groupes correspondant $\mathrm{Spec}^*\,\mathscr{U}_p(\mathscr{G})$ associe à tout S-préschéma T l'ensemble des $x\in\Gamma(\mathrm{T},\mathscr{U}_p(\mathscr{G}\otimes_{\mathscr{O}_{\mathrm{S}}}\mathscr{O}_{\mathrm{T}}))$ tels que

$$\varepsilon(x)=1 \qquad \text{et} \qquad \Delta x = x\otimes x.$$

Ici, ε et Δ désignent l'augmentation et le morphisme diagonal de $\mathscr{U}_p(\mathscr{G}\otimes_{\mathscr{O}_{\mathrm{S}}}\mathscr{O}_{\mathrm{T}})$; par abus de notation, on a encore noté $x\otimes x$ l'image dans $\Gamma(\mathrm{T},\mathscr{U}_p(\mathscr{G}_{\mathrm{T}})\otimes_{\mathscr{O}_{\mathrm{T}}}\mathscr{U}_p(\mathscr{G}_{\mathrm{T}}))$ de l'élément $x\otimes x$ de $\Gamma(\mathrm{T},\mathscr{U}_p(\mathscr{G}_{\mathrm{T}}))\otimes_{\mathscr{O}(\mathrm{T})}\Gamma(\mathrm{T},\mathscr{U}_p(\mathscr{G}_{\mathrm{T}}))$.

D'après 5.3.3 et 3.1.2, on obtient :

Proposition. — *Lorsque $\mathscr{G}$ est localement libre de type fini en tant que $\mathscr{O}_{\mathrm{S}}$-module,* $\mathrm{Spec}^*\,\mathscr{U}_p(\mathscr{G})$ *est représentable par un* S-*préschéma fini et localement libre.*

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

453

Soit S un préschéma de caractéristique $p>0$. Au paragraphe 5.4.1 nous avons associé à toute $\mathscr{O}_{\mathrm{S}}$-p-algèbre de Lie quasi-cohérente $\mathscr{G}$ un S-foncteur en groupes $\mathrm{Spec}^*\,\mathscr{U}_p(\mathscr{G})$. Nous allons voir maintenant que, pour tout S-préschéma en groupes G, la $\mathscr{O}_{\mathrm{S}}$-algèbre de Lie $\mathscr{L}ie(\mathrm{G}/\mathrm{S})$ définie en II 4.11 est munie naturellement d'une structure de $\mathscr{O}_{\mathrm{S}}$-p-algèbre de Lie.

6.1. Identifions tout d'abord $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ et $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}\,\mathrm{G/S})(\mathrm{S})$ respectivement à des sous-algèbres de Lie de $\mathrm{U}(\mathrm{G})$ et $\mathrm{Dif}_{\mathrm{G/S}}$ au moyen des injections α et β de 2.5 ; $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}\,\mathrm{G/S})(\mathrm{S})$ 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 $\mathrm{Dif}_{\mathrm{G/S}}$.

D'autre part, d'après II 4.1.4 [(43)], l'image de $\mathrm{L} = \underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ par la translation à droite $r : \mathrm{U}(\mathrm{G}) \to \mathrm{Dif}_{\mathrm{G/S}}$ (cf. 2.2) est formée des dérivations invariantes à droite. Si x appartient à L, $r(x)^p$ n'est autre que $r(x^p)$ d'après 2.2. Comme $r(x)^p$ est encore une dérivation, on voit que x^p appartient à $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$. Donc : [(44)]

$\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ *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-préschémas 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 $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ et $\underline{\mathrm{Lie}}(\mathrm{H/S})(\mathrm{S})$ 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 $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{S})$ dans $\underline{\mathrm{Lie}}(\mathrm{G/S})(\mathrm{T})$, qui est induite par s, est un homomorphisme de p-algèbres de Lie. On peut traduire cela en disant que le foncteur $\underline{\mathrm{Lie}}(\mathrm{G/S})$ est muni d'une structure de $\mathbf{O}_{\mathrm{S}}$-p-algèbre de Lie. En particulier, lorsque T parcourt les ouverts de S, on voit que **454**
le faisceau $\mathscr{L}ie(\mathrm{G/S})$ 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-préschéma en groupes G.

Soit D une dérivation de G à l'origine, c'est-à-dire la déviation de l'origine obtenue en composant la déviation canonique $\delta : \mathrm{S} \to \mathrm{I}_{\mathrm{S}}$ de 1.5 [(45)] avec un prolongement x à I_{S} de la section unité $\varepsilon : \mathrm{S} \to \mathrm{G}$. 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 $\mathscr{O}_{\mathrm{S}}[d_1, \ldots, d_p]/(d_1^2, \ldots, d_p^2)$, la déviation $\delta \times \cdots \times \delta$ est définie par un morphisme de $\mathscr{O}_{\mathrm{S}}$-modules

$$\mathscr{O}_{\mathrm{S}}[d_1, \ldots, d_p]/(d_1^2, \ldots, d_p^2) \longrightarrow \mathscr{O}_{\mathrm{S}}$$

qui applique le monôme $d_1 d_2 \cdots d_p$ sur 1 et les autres monômes $d_{i_1} \cdots d_{i_r}$ sur 0 ($r < p$). 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 l'image

[(43)] N.D.E. : voir aussi 2.5.

[(44)] N.D.E. : Voir aussi 6.2 pour une autre démonstration.

[(45)] N.D.E. : En 1.5, elle était notée σ ; ici, la lettre σ est réservée pour les polynômes symétriques élémentaires σ_i qui apparaissent un peu plus loin.

de $x \in \mathrm{G}(\mathrm{I}_\mathrm{S}^p)$ par $\mathrm{G}(\mathrm{pr}_i)$, le morphisme composé $m^{(p)} \circ (x \times \cdots \times x)$ n'est autre que le produit $x_1 x_2 \dots x_p$. Par conséquent, D^p est aussi la déviation composée suivante

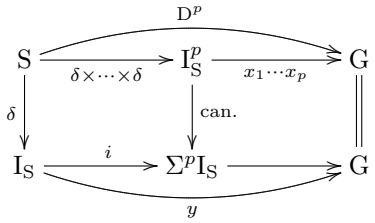
$$\mathrm{S} \xrightarrow{\delta \times \cdots \times \delta} \mathrm{I}_\mathrm{S} \times \cdots \times \mathrm{I}_\mathrm{S} \xrightarrow{x_1 x_2 \dots x_p} \mathrm{G}.$$

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

Le produit symétrique $\Sigma^p \mathrm{I}_\mathrm{S}$ a pour algèbre affine une sous-algèbre $\mathscr{A}$ de

$$\mathscr{O}_\mathrm{S}[d_1, \dots, d_p]/(d_1^2, \dots, d_p^2)$$

qui a pour base sur $\mathscr{O}_\mathrm{S}$ les fonctions symétriques élémentaires $1 = \sigma_0, \sigma_1, \dots, \sigma_p$ de $d_1, \dots, d_p$. Nous désignons par q l'homomorphisme de $\mathscr{A}$ dans $\mathscr{O}_\mathrm{S}[d]/(d^2)$ qui annule $\sigma_1, \dots, \sigma_{p-1}$ et envoie σ_p sur d, par i l'immersion fermée de I_S dans $\Sigma^p \mathrm{I}_\mathrm{S}$ qui est associée à q. On a alors un diagramme commutatif :



qui montre que D^p est de la forme $y \circ \delta$. C.Q.F.D.

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

$$\mu : \mathrm{I}_\mathrm{S}^p \times \mathscr{S}_p \longrightarrow \mathrm{I}_\mathrm{S}^p$$

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 $\mathrm{I}_\mathrm{S}^p \times \tau$ a $\mathrm{pr}_{\tau(j)}$ pour j-ième composante). Ceci étant, nous disons que :

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

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

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

$$\mathrm{X}(\mathrm{T} \times \Sigma^p \mathrm{I}_\mathrm{S}) \longrightarrow \mathrm{X}(\mathrm{T} \times \mathrm{I}_\mathrm{S}^p) \rightrightarrows \mathrm{X}(\mathrm{T} \times \mathrm{I}_\mathrm{S}^p \times \mathscr{S}_p).$$

(les deux flèches parallèles sont $\mathrm{X}(\mathrm{id}_\mathrm{T} \times \pi)$ et $\mathrm{X}(\mathrm{id}_\mathrm{T} \times \mu)$).

Tout S-préschéma vérifie (F) ; si $\mathscr{F}$ est un $\mathscr{O}_\mathrm{S}$-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, $\underline{\mathrm{Hom}}_\mathrm{S}(\mathrm{X}, \mathrm{Y})$ 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 $\Sigma^p \mathrm{I_S}$:

$$\begin{array}{ccc} \mathrm{I_S^p} & \xrightarrow{x_1 \cdots x_p} & \mathrm{X} \\ & {\scriptstyle \mathrm{can.}} \searrow \quad \nearrow {\scriptstyle \Sigma^p(x)} & \\ & \Sigma^p \mathrm{I_S} & \end{array}$$

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.

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 : **457**

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-préschéma T, on a donc

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

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

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

de la forme $m \mapsto 1 + d\,\xi(m)$, où $\xi \in \mathrm{Hom_{(Ab)}}(\mathrm{M}, \mathscr{O}(\mathrm{S}))$. 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 $\Gamma(\mathrm{S}, \mathscr{O}_\mathrm{S} + d\mathscr{O}_\mathrm{S})$ 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 $\mathrm{Hom_{(Ab)}}(\mathrm{M}, \mathscr{O}(\mathrm{S})^*)$ comme en 5.1, la puissance p-ième symbolique associe à ξ l'homomorphisme $\xi^{(p)} : m \mapsto \xi(m)^p$.

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 $\mathbf{W}(\mathscr{F})(\mathrm{I_S} \to \mathrm{S})$. **458**

On sait 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' [46] 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 l'algèbre de Lie de $\mathbf{W}(\mathscr{F})$ est nulle.

6.4.3. — Soient X un S-préschéma, 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 6.1, D peut être identifié à un I_S-automorphisme x de $\mathrm{X}_{\mathrm{I}_\mathrm{S}}$ 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 $f \mapsto f + (\mathrm{D}_{\mathrm{I}_\mathrm{S}^p} f)d$ 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

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

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

Le coefficient de σ_p est $\mathrm{D}_{\mathrm{I}_\mathrm{S}^p}^p$, ce qui signifie que la bijection $\mathrm{D} \mapsto x$ de $\mathrm{Dér}_\mathrm{S}(\mathscr{O}_\mathrm{X})$ sur $\mathrm{Lie}(\underline{\mathrm{Aut}}_\mathrm{S}\, \mathrm{X})$ est 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 $\mathscr{F}$, la bijection décrite en II 4.5 est un isomorphisme de p-algèbres de Lie :

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

De même, si $\mathscr{U}$ est une $\mathscr{O}_\mathrm{S}$-coalgèbre en groupes quasi-cohérente, et si G est le foncteur en groupes $\mathrm{Spec}^*\, \mathscr{U}$, on voit facilement que l'injection canonique de $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ dans $\Gamma(\mathrm{S}, \mathscr{U})$, qui identifie $\underline{\mathrm{Lie}}(\mathrm{G}/\mathrm{S})(\mathrm{S})$ à l'ensemble des éléments primitifs de $\Gamma(\mathrm{S}, \mathscr{U})$, est compatible avec la puissance p-ième.

7. Groupes radiciels de hauteur 1

460

Soit S un préschéma 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 que le S-foncteur en groupes

$$\mathrm{G}_p(\mathscr{L}) = \mathrm{Spec}^*\, \mathscr{U}_p(\mathscr{L})$$

[46] N.D.E. : on a corrigé x en y'. D'autre part, préciser le « on sait ».

est représentable par un S-préschéma fini, localement libre (5.4.1). Nous allons voir que ce S-préschéma est solution d'un problème universel et nous allons caractériser les S-préschémas en groupes de la forme $\mathrm{Spec}^*\,\mathscr{U}_p(\mathscr{L})$.

7.1. Considérons d'abord une $\mathscr{O}_S$-p-algèbre de Lie quasi-cohérente $\mathscr{L}$. Lorsque V parcourt les ouverts de S, les applications $j : \Gamma(V,\mathscr{L}) \to U_p(\Gamma(V,\mathscr{L}))$ de 5.3 définissent un morphisme $\mathscr{L} \to \mathscr{U}_p(\mathscr{L})$, que nous noterons encore j.

D'autre part, d'après 3.2.3, la $\mathscr{O}_S$-algèbre de Lie du S-foncteur en groupes $G_p(\mathscr{L})$ est le noyau du morphisme

$$\Delta - \tau_1 - \tau_2 : \quad \mathscr{U}_p(\mathscr{L}) \longrightarrow \mathscr{U}_p(\mathscr{L}) \otimes_{\mathscr{O}_S} \mathscr{U}_p(\mathscr{L}),$$

où Δ désigne le morphisme diagonal et où τ_1 et τ_2 sont les morphismes $x \mapsto x \otimes 1$ et $x \mapsto 1 \otimes x$. Il est clair que l'image de j est contenue dans le noyau $\mathscr{L}ie\, G_p(\mathscr{L})$ de $\Delta - \tau_1 - \tau_2$; c'est pourquoi nous noterons

$$j_{\mathscr{L}} : \mathscr{L} \longrightarrow \mathscr{L}ie\, G_p(\mathscr{L})$$

le morphisme de $\mathscr{O}_S$-p-algèbres de Lie qui est induit par j (cf. 6.4.4).

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

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

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

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

est bijective dans chacun des cas suivants :

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

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

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

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

Lemme. — *Si $\mathscr{L}$ est une $\mathscr{O}_S$-p-algèbre finie localement libre, le* S*-groupe $G_p(\mathscr{L})$ est annulé par le morphisme de Frobenius de $G_p(\mathscr{L})$ relativement à* S.

Soient en effet $\mathscr{U}$ l'algèbre enveloppante restreinte de $\mathscr{L}$ et posons $\mathscr{A} = \mathscr{U}^* = \mathscr{H}om_{\mathscr{O}_S}(\mathscr{U}, \mathscr{O}_S)$. Alors $\mathscr{A}$ est l'algèbre affine de $G_p(\mathscr{L})$. De plus, si $\mathscr{J}$ est l'idéal d'augmentation de $\mathscr{U}$, c'est-à-dire l'idéal engendré par l'image de $j_{\mathscr{L}} : \mathscr{L} \to \mathscr{U}$, nous notons $\mathscr{I}$ l'orthogonal de $\mathscr{J}$ dans $\mathscr{A}$. On a donc $\mathscr{A}/\mathscr{I} \simeq \mathscr{O}_S$ et l'idéal $\mathscr{I}$ définit la section unité de $G_p(\mathscr{L})$.

Si π est l'endomorphisme $x \mapsto x^p$ de $\mathscr{O}_S$, nous devons montrer que le morphisme $\Phi : a \otimes_\pi x \mapsto a^p x$ de $\mathscr{A} \otimes_\pi \mathscr{O}_S$ dans $\mathscr{A}$ s'annule sur $\mathscr{I} \otimes_\pi \mathscr{O}_S$. Or Φ n'est autre que le composé suivant

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

462 où $b(\mathscr{A})$ et $j(\mathscr{A})$ sont définis comme en 4.3.3. Comme le $\mathscr{O}_S$-module dual de $\mathcal{S}^p\mathscr{A}$ n'est autre que le 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 le transposé Φ^* de Φ est le morphisme composé suivant :

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

où $a(\mathscr{U})$ est induit par le morphisme $(\Delta \otimes \mathscr{U} \otimes \cdots \otimes \mathscr{U}) \cdots (\Delta \otimes \mathscr{U})\Delta$ de $\mathscr{U}$ dans $\bigotimes^p \mathscr{U}$ (Δ est le morphisme diagonal de $\mathscr{U}$) ; de même, $r(\mathscr{U})$ 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 reste maintenant à montrer que Φ^* annule l'idéal d'augmentation $\mathscr{J}$. Comme Φ^* est un homomorphisme d'algèbres, il suffit de voir que Φ^* s'annule sur l'image de $j_{\mathscr{L}}$. Ceci résulte de la formule $\Delta s = s \otimes 1 + 1 \otimes s$, lorsque $s \in \operatorname{Im} j_{\mathscr{L}}$.

7.2.1. — Posons $G_p = G_p(\mathscr{L})$. Nous allons d'abord prouver l'assertion (ii) du théorème 7.2 en conservant les notations ci-dessus. Comme tout élément de $\mathscr{I}$ a une puissance p-ième nulle et que $\mathscr{I}$ est un $\mathscr{O}_S$-module de type fini, $\mathscr{I}$ est localement nilpotent. On a donc $(G_p)_{\text{réd}} = S_{\text{réd}}$. Or les homomorphismes h de G_p dans $\underline{\mathrm{Aut}}\, X$ correspondent biunivoquement aux opérations à gauche $h' : G_p \times X \to X$ de G_p sur X. Pour une telle opération, si ε est la section unité de G_p, le morphisme composé

$$X \simeq S \times X \xrightarrow{\varepsilon \times X} G_p \times X \xrightarrow{h'} X$$

doit être l'identité. Comme $(G_p \times X)_{\text{réd}}$ s'identifie à $X_{\text{réd}}$, on voit que h' doit induire l'identité sur les préschémas réduits associés. En particulier, h' induit une opération de G_p sur tous les ouverts de X, de sorte qu'on se ramène facilement au cas où S et X sont affines, ou plus généralement au cas où X est affine au-dessus de S. Dans ce dernier cas, on applique le lemme suivant :

463 ***Lemme***. — *Soient* X *un* S*-préschéma affine d'algèbre* $\mathscr{C}$ *et* G_p *un* S*-préschéma en groupes fini localement libre d'algèbre* $\mathscr{A}$. *Si nous posons* $\mathscr{U} = \mathscr{A}^* = \mathscr{H}om_{\mathscr{O}_S}(\mathscr{A}, \mathscr{O}_S)$, *les opérations de* G_p *à gauche sur* X *correspondent biunivoquement aux représentations de l'algèbre* $\mathscr{U}$ *dans le* $\mathscr{O}_S$*-module* $\mathscr{C}$ *telles qu'on ait*

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

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

Dans ces formules, u désigne une section quelconque de $\mathscr{U}$ sur un ouvert affine V, 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 $\mathscr{U}$. Une opération h' de G à gauche sur X est définie par un homomorphisme d'algèbres $\lambda : \mathscr{C} \to \mathscr{A} \otimes_{\mathscr{O}_S} \mathscr{C}$. Nous noterons μ 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 $\mathscr{O}_S$. 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 λ est un homomorphisme d'algèbres unitaires définissant une opération de G_p sur X si et seulement si μ satisfait aux conditions du lemme.

Il est d'ailleurs 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 du lemme précédent forment une sous-algèbre de $\mathscr{U}$. Dans le cas particulier qui nous intéresse, ces conditions sont donc satisfaites pour toutes les sections u, si elles sont vraies pour les sections u de $\mathrm{Im}\, j_{\mathscr{L}}$. Si u est une section de $\mathrm{Im}\, j_{\mathscr{L}}$, ces conditions signifient que $u(1_{\mathscr{C}}) = 0$ et que $u(xy) = u(x)y + xu(y)$. Tout homomorphisme h de $G_p = G_p(\mathscr{L})$ dans $\underline{\mathrm{Aut}}\, X$ définit donc un **464**
homomorphisme H de $\mathscr{U}$ dans $\mathrm{Hom}_{\mathscr{O}_S}(\mathscr{C}, \mathscr{C})$ qui envoie $\mathrm{Im}\, j_{\mathscr{L}}$ dans l'ensemble des $\mathscr{O}_S$-dérivations de $\mathscr{C}$. L'application $H \circ j_{\mathscr{L}}$ est un homomorphisme de p-algèbres de Lie de $\mathscr{L}$ dans le faisceau $\mathrm{Dér}_{X/S}$ des $\mathscr{O}_S$-dérivations de $\mathscr{C}$. De plus, l'application $h \mapsto H \circ j_{\mathscr{L}}$ est évidemment bijective ; il resterait à vérifier qu'en identifiant $\mathrm{Dér}_{X/S}$ à $\underline{\mathrm{Lie}}(\underline{\mathrm{Aut}}\, X/S)$ comme en 2.5 [47], on identifie l'application $h \mapsto H \circ j_{\mathscr{L}}$ à celle du théorème 7.2.

7.2.2. — Montrons maintenant comment l'assertion (i) du théorème 7.2 résulte de (ii). Si T est un S-préschéma 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 $(r_x^T)^{-1} f r_x^T$; de cette façon G opère à gauche sur le S-foncteur $\underline{\mathrm{Aut}}\, G$, donc aussi sur les foncteurs $T \mapsto \mathrm{Hom}_{T\text{-Gr.}}(G_p(\mathscr{L}_T), \underline{\mathrm{Aut}}\, X_T)$ et $T \mapsto \mathrm{Hom}_p(\mathscr{L}_T, \mathscr{L}ie(\underline{\mathrm{Aut}}\, X_T/T))$. D'autre part, l'homomorphisme ℓ induit des carrés commutatifs

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

Les images des deux flèches verticales sont les sous-foncteurs formés des invariants sous l'action du S-groupe G. Comme la deuxième flèche horizontale est inversible d'après 7.2.1 et qu'elle est compatible avec l'action de G, la première flèche horizontale est aussi inversible.

7.2.3. — Considérons enfin le cas de $\underline{\mathrm{Aut}}_{\mathbf{O}_S\text{-mod.}}\, \mathbf{W}(\mathscr{F})$ (le cas de $\mathbf{W}(\mathscr{F})$ est ana- **465**
logue). Posons $G_p = G_p(\mathscr{L})$. Un homomorphisme de G_p dans $\underline{\mathrm{Aut}}_{\mathbf{O}_S\text{-mod.}}\, \mathbf{W}(\mathscr{F})$ est un homomorphisme multiplicatif de G_p dans $\underline{\mathrm{End}}_{\mathbf{O}_S\text{-mod}}\, \mathbf{W}(\mathscr{F})$ qui est compatible avec les sections unités de G_p et de $\underline{\mathrm{End}}_{\mathbf{O}_S\text{-mod.}}\, \mathbf{W}(\mathscr{F})$. Or un morphisme de S-foncteurs $h : G_p \to \underline{\mathrm{End}}_{\mathbf{O}_S\text{-mod.}}\, \mathbf{W}(\mathscr{F})$ est par définition un endomorphisme de

[47] N.D.E. : Voir II 3.14 et la N.D.E. qui s'y trouve.

$\mathbf{W}(\mathscr{O}_{\mathrm{G}_p} \otimes_{\mathscr{O}_\mathrm{S}} \mathscr{F})$; d'après I 4.6.2 (ii), un tel endomorphisme est induit par un endomorphisme de $\mathscr{O}_{\mathrm{G}_p} \otimes_{\mathscr{O}_\mathrm{S}} \mathscr{F}$, c'est-à-dire par un endomorphisme $\mathscr{A}$-linéaire du faisceau $\mathscr{A} \otimes_{\mathscr{O}_\mathrm{S}} \mathscr{F}$, où $\mathscr{A}$ est la $\mathscr{O}_\mathrm{S}$-algèbre affine de G_p. Un tel endomorphisme est de la forme $a \otimes x \mapsto a\lambda(x)$, où λ est un morphisme de $\mathscr{O}_\mathrm{S}$-modules de $\mathscr{F}$ dans $\mathscr{A} \otimes_{\mathscr{O}_\mathrm{S}} \mathscr{F}$. Si l'on pose $\mu = (\gamma \otimes \mathscr{F})(\mathscr{U} \otimes \lambda)$ comme en 7.2.1, h est finalement déterminé par $\mu : \mathscr{U} \otimes_{\mathscr{O}_\mathrm{S}} \mathscr{F} \to \mathscr{F}$. Les hypothèses faites sur h se traduisent en disant que μ définit une structure de $\mathscr{U}$-module sur $\mathscr{F}$. Une telle structure de module est définie par un homomorphisme de p-algèbres de Lie de $\mathscr{L}$ dans $\mathscr{E}nd_{\mathscr{O}_\mathrm{S}}(\mathscr{F})$, [48] qui égale $\mathscr{L}ie(\underline{\mathrm{Aut}}_{\mathbf{O}_\mathrm{S}\text{-mod.}} \mathbf{W}(\mathscr{F}))$.

7.3. Lemme. — *Si $\mathscr{L}$ est une $\mathscr{O}_\mathrm{S}$-p-algèbre de Lie finie localement libre, le morphisme $j_{\mathscr{L}} : \mathscr{L} \to \mathscr{L}ie\,\mathrm{G}_p(\mathscr{L})$ de* 7.1 *est inversible.*

Le problème est en effet local sur S. Nous pouvons donc supposer que S est affine d'anneau R et que $\mathscr{L}$ est le faisceau associé à une R-p-algèbre de Lie de base $x_1, \ldots, x_r$. Nous pouvons alors utiliser les notations de 5.3.3 et poser $z^n = \prod_i z^{n_i}$ pour tout r-uplet $(n_1, \ldots, n_r)$ formés d'entiers naturels tels que $0 \leqslant n_i < p$. Posant en outre $n! = \prod_i (n_i)!$ et munissant le monoïde $\mathbb{N}^r$ de l'ordre produit, on voit facilement que

$$\Delta\left(\frac{z^n}{n!}\right) = \sum \frac{z^m}{m!} \otimes \frac{z^{n-m}}{(n-m)!}$$

466 la somme étant étendue à tous les m de $\mathbb{N}^r$ tels que $0 \leqslant m \leqslant n$ (Δ est le morphisme diagonal de $\mathscr{U}$). Comme les z^n forment une base de $\mathscr{U}_p(\mathfrak{g})$, il est clair qu'on a $\Delta x = x \otimes 1 + 1 \otimes x$ si et seulement si x est combinaison linéaire de $z_1, \ldots, z_r$. C.Q.F.D.

7.4. Pour terminer l'exposé, nous allons donner une caractérisation des S-préschémas 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-préschéma 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 $\mathrm{U}(\mathrm{G})$ (cf. 2.5) s'identifie d'après 1.3 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 $\mathscr{I}^2$. [49] 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 l'exposé II. Nous poserons d'ailleurs $\omega_{\mathrm{G}/\mathrm{S}} = \mathscr{I}/\mathscr{I}^2$ comme dans l'exposé II, de sorte que le faisceau $\mathscr{L}ie(\mathrm{G}/\mathrm{S})$ s'identifie à $\mathscr{H}om_{\mathscr{O}_\mathrm{S}}(\omega_{\mathrm{G}/\mathrm{S}}, \mathscr{O}_\mathrm{S})$.

Théorème. — *Si* G *est un préschéma en groupes sur un préschéma* 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* G *soit isomorphe à* $\mathrm{G}_p(\mathscr{L})$.

[48] N.D.E. : détailler ce point...
[49] N.D.E. : cf. 1.3.1, 2.4 et 2.5.

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

(iii) G *est localement de présentation finie sur* S, *de hauteur* $\leqslant 1$ (4.1.3) *et* $\omega_{G/S}$ *est localement libre* (*).

7.4.1. — L'implication (ii) ⇒ (iii) étant claire, montrons d'abord que (i) entraîne (ii). **467**
Nous considérons pour cela la suite exacte

$$(*) \qquad 0 \longrightarrow \mathscr{L} \xrightarrow{j_{\mathscr{L}}} \mathscr{J} \xrightarrow{\delta} \mathscr{J} \otimes_{\mathscr{O}_S} \mathscr{J},$$

où $\mathscr{J}$ est l'idéal d'augmentation de $\mathscr{U} = \mathscr{U}_p(\mathscr{L})$ et où δ est le morphisme induit par $\Delta - \mathrm{in}_1 - \mathrm{in}_2$. Si q est la projection de $\mathscr{U}$ sur $\mathscr{J}$ qui s'annule sur la section unité de $\mathscr{U}$, alors δ peut être caractérisé par le carré commutatif

$$\begin{array}{ccc} \mathscr{U} & \xrightarrow{\Delta} & \mathscr{U} \otimes_{\mathscr{O}_S} \mathscr{U} \\ \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle q \otimes q} \\ \mathscr{J} & \xrightarrow{\delta} & \mathscr{J} \otimes_{\mathscr{O}_S} \mathscr{J} \end{array} .$$

De plus, la suite (∗) reste exacte après tout changement de base ; par conséquent (Bourbaki, Alg. Comm. II § 3, prop. 6), la suite (∗) se scinde et donne par dualité une suite exacte

$$\mathscr{I} \otimes_{\mathscr{O}_S} \mathscr{I} \xrightarrow{m} \mathscr{I} \longrightarrow \mathscr{H}om_{\mathscr{O}_S}(\mathscr{L}, \mathscr{O}_S) \longrightarrow 0,$$

où $\mathscr{I}$ désigne l'idéal d'augmentation de l'algèbre affine $\mathscr{A}$ de $G_p(\mathscr{L})$ et où m est induit par la multiplication de $\mathscr{A}$. Ceci montre que $\omega_{G/S}$ *est le dual de* $\mathscr{L}$, donc est fini localement libre.

Supposons maintenant S affine. Il y a alors une section $\sigma : \omega_{G/S} \to \mathscr{I}$ de la projection canonique de $\mathscr{I}$ sur $\mathscr{I}/\mathscr{I}^2$; une telle section induit (lemme 7.2) un homomorphisme d'algèbres

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

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 h induit un épimorphisme des gradués associés. Donc h est un épimorphisme de $\mathscr{O}_S$-modules localement libres de même rang ; donc h est un isomorphisme.

7.4.2. — Montrons enfin que (iii) entraine (i). Comme le morphisme de Frobenius **468**
annule G, il est clair que la section unité de G induit un homéomorphisme de l'espace topologique sous-jacent à S sur l'espace sous-jacent à G. Nous pouvons donc identifier S au sous-préschéma fermé de G défini par un certain idéal $\mathscr{I}$ de $\mathscr{O}_G$. Comme G est localement de présentation finie sur S et que toute section de $\mathscr{I}$ a une puissance

(*) La condition sur $\omega_{G/S}$ 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.

p-ième nulle, $\mathscr{I}$ est localement nilpotent et G est affine sur S (EGA I, 5.1.9), donc fini sur S.

Soit donc $\mathscr{A}$ la $\mathscr{O}_S$-algèbre affine de G ; posons $\mathscr{L} = \mathscr{L}ie(G/S)$, $\mathscr{A}_p = \mathscr{U}_p(\mathscr{L})^*$ et soit $G_p = G_p(\mathscr{L})$ le spectre de $\mathscr{A}_p$. D'après le théorème 7.2, l'application identique de $\mathscr{L}$ correspond à un homomorphisme de groupes $h : G_p(\mathscr{L}) \to G$, donc à un homomorphisme de $\mathscr{O}_S$-algèbres $\phi : \mathscr{A} \to \mathscr{A}_p$. Il s'agit de montrer que ϕ, qui induit par définition un isomorphisme de $\omega_{G/S}$ sur $\omega_{G_p/S}$, 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 canonique de $\mathscr{I}$ sur $\omega_{G/S}$. Comme toute section de $\mathscr{I}$ a une puissance p-ième nulle, τ induit un homomorphisme de $\mathscr{O}_S$-algèbres

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

Il est clair que ψ est un épimorphisme de $\mathscr{O}_S$-modules (cf. 7.4.1). D'autre part, nous avons vu en 7.4.1 que $\phi\psi$ est un isomorphisme. Il en va donc de même pour ϕ. C.Q.F.D.

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-préschéma en groupes est *algébrique* si le préschéma sous-jacent est de type fini sur k.

Dans ce cas, d'après le théorème 7.2, on obtient :

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

D'après 7.3 et le théorème 7.4.1, on obtient :

Théorème 8.1.2. — *Le foncteur $G_p : \mathscr{L} \mapsto G_p(\mathscr{L})$ induit une équivalence de la catégorie des k-p-algèbres de Lie de dimension finie, sur celle des k-groupes algébriques de hauteur $\leqslant 1$.*

Alors, comme G_p est un foncteur adjoint à gauche, *il commute aux limites inductives*. De plus, comme l'inclusion de la catégorie des k-groupes algébriques de hauteur $\leqslant 1$ dans celle de tous les k-groupes algébriques commute manifestement aux limites projectives finies, on obtient le

Corollaire 8.1.3. — *Le foncteur G_p est exact : si $i : \mathscr{L}_0 \to \mathscr{L}_1$ et $q : \mathscr{L}_1 \to \mathscr{L}_2$ sont des homomorphismes de k-p-algèbres de Lie et si la suite*

$$0 \longrightarrow \mathscr{L}_0 \xrightarrow{\ i\ } \mathscr{L}_1 \xrightarrow{\ q\ } \mathscr{L}_2 \longrightarrow 0$$

formée par les espaces vectoriels sous-jacents, est exacte, alors $G_p(i)$ est un isomorphisme de $G_p(\mathscr{L}_0)$ sur le noyau de $G_p(q)$; l'image de $G_p(i)$ est donc un sous-groupe distingué de $G_p(\mathscr{L}_1)$ et $G_p(q)$ induit un isomorphisme du quotient de $G_p(\mathscr{L}_1)$ par ce sous-groupe distingué sur $G_p(\mathscr{L}_2)$.

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

$$1 \longrightarrow \mathrm{G}' \xrightarrow{v} \mathrm{G} \xrightarrow{u} \mathrm{G}'' \longrightarrow 1$$

et les assertions suivantes :

(i) *Le morphisme u est lisse.*

(ii) *G' est lisse.*

(iii) *Pour tout entier $n > 0$, la suite ci-dessous, induite par v et u,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 ${}_{\mathrm{Fr}}u : {}_{\mathrm{Fr}}\mathrm{G} \to {}_{\mathrm{Fr}}\mathrm{G}''$ est un épimorphisme.*

(v) *Le morphisme $\mathscr{L}ie(u) : \mathscr{L}ie(\mathrm{G}) \to \mathscr{L}ie(\mathrm{G}'')$ est surjectif* (II 4.11).

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 l'exposé VI_B (1.3) : rappelons en effet que (i) entraîne (ii) d'après SGA 1, II 1.3 ; d'autre part (ii) signifie que u est lisse à l'origine (SGA 1, II 2.1 ; u est plat parce que épimorphique), donc partout.

De même, l'équivalence de (iv) et (v) résulte de l'équivalence définie en 8.1 entre la catégorie des k-groupes algébriques de hauteur $\leqslant 1$ et celle des p-algèbres de Lie de dimension finie sur k.

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

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

dont les deux lignes sont exactes : comme $\mathrm{Fr}^n(\mathrm{G}'/k)$ est un épimorphisme d'après le corollaire 8.3.1 ci-dessous, u 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).

Enfin, lorsque G est lisse sur k, $\mathrm{Fr}(\mathrm{G}/k)$ est un épimorphisme. Si, de plus, ${}_{\mathrm{Fr}}u$ 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 (8.3.1 ci-dessous).

8.3. Proposition. — *Si* G *est un groupe algébrique 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 $n \geqslant n_0$.*

Comme la construction de ${}_{\mathrm{G}/\mathrm{Fr}^n}\mathrm{G}$ commute à l'extension du corps de base (4.1.1 **471**
et VI_A, 4.7), nous pouvons supposer k parfait (SGA II 5.5). Dans ce cas, $\mathrm{G}_{\mathrm{réd}}$ est un sous-groupe algébrique de G (VI_A 0.2) et l'on a le diagramme commutatif et exact suivant, où l'on a posé $\mathrm{H} = \mathrm{G}_{\mathrm{réd}}\backslash\mathrm{G}$:

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

Or H est le spectre d'une k-algèbre finie, locale, de corps résiduel k ($\mathrm{VI_B}$). Par conséquent, il existe un entier n_0 tel que $\mathrm{Fr}^n(\mathrm{H}/k)$ se factorise à travers l'unique section de $\operatorname{Spec} k$ dans $\mathrm{H}^{(p^n)}$, lorsque $n \geqslant n_0$. Il s'ensuit que, pour $n \geqslant n_0$, $\mathrm{Fr}^n(\mathrm{G}/k)$ se factorise à travers $\mathrm{G}_{\text{réd}}^{(p^n)}$; l'homomorphisme $h : \mathrm{G}/_{\mathrm{Fr}^n}\mathrm{G} \to \mathrm{G}_{\text{réd}}^{(p^n)}$, qui est défini par cette factorisation, est un monomorphisme ($\mathrm{VI_A}$ 5.4) et induit un homéomorphisme des espaces topologiques sous-jacents ; c'est donc un isomorphisme ($\mathrm{VI_B}$, $\mathrm{G}_{\text{réd}}^{(p^n)}$ est réduit [(50)]). Comme $\mathrm{G}_{\text{réd}}^{(p^n)}$ est lisse sur k ($\mathrm{VI_A}$, 1.3.1), $\mathrm{G}/_{\mathrm{Fr}^n}\mathrm{G}$ est lisse sur k, lorsque $n \geqslant n_0$.

8.3.1. Corollaire. — *Soit n un entier $\geqslant 1$. Alors* G *est lisse sur k si et seulement si* $\mathrm{Fr}^n(\mathrm{G}/k)$ *est un épimorphisme.*

Si G est lisse sur k, G est réduit et $\mathrm{Fr}^n(\mathrm{G}/k)$ est surjectif, donc est un épimorphisme [(51)]. Réciproquement, comme $\mathrm{Fr}^n(\mathrm{G}/k)^{(p^n)}$ coïncide avec $\mathrm{Fr}^n(\mathrm{G}^{(p^n)}/k)$ (confer 4.1.3), alors $\mathrm{Fr}^{nm}(\mathrm{G}/k)$ est un épimorphisme pour tout m si $\mathrm{Fr}^n(\mathrm{G}/k)$ en est un. On a alors $\mathrm{G}/_{\mathrm{Fr}^{nm}}\mathrm{G} \simeq \mathrm{G}^{(p^{nm})}$. Donc, d'après la proposition 8.3, $\mathrm{G}^{(p^{nm})}$ est lisse sur k pour m grand, donc G l'est aussi [(52)].

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
472 la caractéristique de k. De plus, si G est un préschéma en groupes sur k, nous notons $n_{\mathrm{G}} : \mathrm{G} \to \mathrm{G}$ le morphisme de k-préschémas qui applique un élément x de $\mathrm{G}(\mathrm{T})$ sur $x^n \in \mathrm{G}(\mathrm{T})$, lorsque T est un k-préschéma.

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 à l'origine.*

Soient en effet A l'anneau local de G à l'origine et I l'idéal maximal de A. D'après II 3.9, 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 I/I^2. Si k est de caractéristique 0, G est lisse sur k ($\mathrm{VI_B}$ 1.6.1 ; voir aussi $\mathrm{VII_B}$ § 3) ; donc A est régulier et n induit un automorphisme du gradué associé à A, donc aussi un automorphisme du complété $\widehat{\mathrm{A}}$ de A.

[(50)] N.D.E. : préciser ce point et vérifier la réf. à $\mathrm{VI_A}$ 5.4

[(51)] N.D.E. : préciser ce point...

[(52)] N.D.E. : voir, par exemple, EGA IV_4, 17.7.1.

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

Si G est de hauteur $\leqslant r$ et si nous supposons notre assertion démontrée pour les groupes de hauteur $\leqslant r-1$, soient B, A et C les algèbres affines de ${}_{Fr}G$, G et $G_{Fr} = {}_{Fr}G\backslash G$. Appelons n_B, n_A et n_C les morphismes de B, A et C qui sont induits par $n_{{}_{Fr}G}$, n_G et $n_{G_{Fr}}$. Comme n_C est un isomorphisme d'après l'hypothèse de récurrence et que A est plat sur C (VI_A 3.2), n_A est une bijection si et seulement si $n_A \otimes_C (C/\mathfrak{r})$ en est une ($\mathfrak{r}$ désigne le radical de C) ; or $n_A \otimes_C (C/\mathfrak{r})$ n'est autre que n_B !

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 ${}_{Fr^r}G$; ces schémas sont affines sur k et ont pour algèbres les quotients de l'algèbre locale A par l'idéal $I^{\{p^r\}}$ engendré par les puissances p^r-ièmes des éléments de I. Comme **473**
n_G définit des automorphismes des algèbres $A/I^{\{p^r\}}$, on voit par passage à la limite projective, que n induit un automorphisme de $\widehat{A}$.

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 (confer 8.4).

Soit H un sous-groupe distingué de G de rang m sur k. Avec les notations de VI_A, 3.2 [(53)], le carré

$$\begin{array}{ccc} H \times G & \xrightarrow{\lambda} & G \\ {\scriptstyle pr_2}\downarrow & & \downarrow{\scriptstyle can.} \\ G & \xrightarrow{can.} & H \setminus G \end{array}$$

est cartésien. Comme $G \to H\backslash G$ est fidèlement plat, quasi-compact (VI_A 3.2), et que pr_2 est localement libre de rang m, il résulte de EGA IV 2.5.2, que $G \to H\backslash G$ est localement libre de rang m. On a donc $rg_k(H\backslash G) \times rg_k H = rg_k G$.

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-préschéma T ; il est donc clair que n_G est nul si m_H et $(nm^{-1})_{H\backslash G}$ le sont. Si H est la composante connexe de l'origine de G, alors $H\backslash G$ est étale (VI_B), de sorte qu'on peut supposer G étale sur k ou connexe.

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 (I 4.1), et l'énoncé est classique.

Si G est connexe et non nul, la caractéristique p de k est nécessairement > 0 (VI_B ; **474**
VII_B § 3) ; les sous-groupes ${}_{Fr^n}G$ forment alors une suite de composition de G, dont les quotients sont de hauteur $\leqslant 1$.

(53) N.D.E. : le morphisme λ est induit par la multiplication de G.

Ceci nous ramène au cas où G est de hauteur $\leqslant 1$: soient alors A l'algèbre affine de G et L son algèbre de Lie ; si $\dim_k \mathrm{L} = r$, le rang de G sur k est p^r (5.3.3) ; nous allons donc étudier le morphisme $p_{\mathrm{G}} : \mathrm{G} \to \mathrm{G}$ défini par l'élévation à la puissance $p^{\text{ième}}$.

Ce morphisme p_{G} définit des endomorphismes p_{A} et p_{U} de A et de l'algèbre enveloppante restreinte $\mathrm{U} = \mathrm{U}_p(\mathrm{L})$ de L. L'application p_{U} se décompose comme suit

$$\mathrm{U} \xrightarrow{\Delta^p_{\mathrm{U}}} \bigotimes^p_k \mathrm{U} \xrightarrow{m^p_{\mathrm{U}}} \mathrm{U},$$

où Δ^p_{U} désigne l'homomorphisme d'algèbres qui applique $x \in \mathrm{L} \subset \mathrm{U}$ sur

$$x \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes x \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes x,$$

tandis que m^p_{U} est l'application linéaire qui envoie $u_1 \otimes u_2 \otimes \cdots \otimes u_p$ sur le produit $u_1 u_2 \cdots u_p$.

Soit t un entier $\geqslant 1$. Si $x_1, x_2, \ldots, x_t$ sont t éléments de $\mathrm{L} \subset \mathrm{U}$, on a donc

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

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 $\{1, 2, \ldots, t\}$ dans $\{1, 2, \ldots, p\}$. Une telle application définit un préordre sur $\{1, 2, \ldots, t\}$ tel qu'on ait $i \preceq j$ si et seulement si $h(i) \leqslant h(j)$; de plus, on a

$$m^p_{\mathrm{U}}(x_h) = m^p_{\mathrm{U}}(x_\ell) \qquad \text{si } h \text{ et } \ell \text{ définissent le même préordre,}$$

de sorte que nous pouvons écrire $m^p_{\mathrm{U}}(x_h) = x_{\mathfrak{o}}$, où $\mathfrak{o}$ est le préordre défini par h. On a par conséquent

$$p_{\mathrm{U}}(x_1 x_2 \cdots x_t) = \sum_{\mathfrak{o}} \binom{p}{s(\mathfrak{o})} x_{\mathfrak{o}},$$

où $\mathfrak{o}$ parcourt les relations de préordre sur $\{1, \ldots, t\}$ telles que l'ensemble ordonné associé ait au plus p éléments, et où $s(\mathfrak{o})$ est le cardinal de l'ensemble ordonné associé à $\mathfrak{o}$.

475 Lorsque $t < p$, tous les termes $\binom{p}{s(\mathfrak{o})}$, sont nuls, de sorte que $p_{\mathrm{U}}(x_1 \cdots x_t) = 0$. Autrement dit, p_{U} s'annule sur le sous-espace vectoriel U^+_{p-1} de U, qui est engendré par les produits $x_1 \cdots x_t$, avec $1 \leqslant t < p$, $x_i \in \mathrm{L}$. Or, il résulte facilement de 7.3 que l'isomorphisme canonique du dual U^* sur A, qui est décrit en 7.4, identifie l'orthogonal de U^+_{p-1} à $\mathrm{I}^p_{\mathrm{A}}$ (I_{A} = idéal d'augmentation de A ; confer aussi $\mathrm{VII}_{\mathrm{B}}$ 1.3.6 et 4.3). L'isomorphisme de U^* sur A, permet aussi d'identifier p_{A} à l'application transposée de p_{U}, de sorte que l'application composée

$$\mathrm{I}_{\mathrm{A}} \xrightarrow{p_{\mathrm{A}}} \mathrm{I}_{\mathrm{A}} \xrightarrow{\text{can.}} \mathrm{I}_{\mathrm{A}}/\mathrm{I}^p_{\mathrm{A}}$$

est nulle. Donc p_{A} applique I_{A} dans $\mathrm{I}^p_{\mathrm{A}}$ et $(p_{\mathrm{A}})^t$ applique I_{A} dans $\mathrm{I}^{pt}_{\mathrm{A}}$, pour tout entier $t \geqslant 1$, en particulier pour $t = r = \dim_k \mathrm{L}$. Comme $\mathrm{I}^{r(p-1)+1}\mathrm{A}$ est nul d'après le théorème 7.4, l'inégalité $p^r > r(p-1)$ montre que p^r_{A} annule I_{A}. C.Q.F.D.

Bibliographie

[BAlg] N. Bourbaki, *Algèbre*, Chap. I-III, Hermann, 1974.

[DG70] M. Demazure, P. Gabriel, *Groupes algébriques*, Masson & North-Holland, 1970.

[TO70] J. Tate, F. Oort, *Groups schemes of prime order*, Ann. scient. Éc. Norm. Sup. **3** (1970), 1-21.