

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 411
premier ordre et nous n'avons 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. 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 les paragraphes 1, 2 et 3 qui suivent, S désigne un schéma et les produits considérés sont des produits cartésiens dans la catégorie des S -schémas. Si X est un S -schéma, nous notons $p_{X/S}$, p_X ou simplement p le morphisme structural de X dans S .

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

Une S -déviation d'ordre $\leq n$ est par définition un couple $D = (u, d)$ formé d'un morphisme de S -schémas $u : Y \rightarrow X$ et d'un morphisme de $p^{-1}(\mathcal{O}_S)$ -Modules $d : \mathcal{O}_X \rightarrow u_*(\mathcal{O}_Y)$ tel que

$$(*) \quad (ad f_0)(ad f_1) \cdots (ad f_n)d = 0$$

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

pour tout ouvert U de X et toutes les suites de $n+1$ sections $f_0, \dots, f_n$ de $\mathcal{O}_X$ sur U . Si les égalités (*) sont vérifiées, nous dirons aussi que d est une *S-dévi*ation de u d'ordre $\leq n$. En particulier, une S-déviation d'ordre ≤ 0 est un morphisme de $\mathcal{O}_X$ -Modules de $\mathcal{O}_X$ dans $u_*(\mathcal{O}_Y)$.

Un morphisme de $p^{-1}(\mathcal{O}_S)$ -Modules d de $\mathcal{O}_X$ dans $u_*(\mathcal{O}_Y)$ est une *S-dévi*ation 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) $u(V) \subset U$; b) si $v : V \rightarrow U$ est le morphisme induit par u , il y a un entier n tel que le morphisme $\mathcal{O}_U \rightarrow v_*(\mathcal{O}_V)$ induit par d soit une S-déviation d'ordre $\leq n$. Si d est une S-déviation de u , nous disons aussi que le couple $D = (u, d)$ est une S-déviation et il nous arrivera d'écrire $Y \xrightarrow{D} X$ ou $Y \xrightarrow[u]{d} X$. Lorsque d est l'homomorphisme d'algèbres qui définit u , nous écrirons aussi u au lieu de D .

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

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

Lorsque U parcourt les ouverts de X , les applications composées

$$\Gamma(v^{-1}u^{-1}U, \mathcal{O}_Z) \xleftarrow{e(u^{-1}U)} \Gamma(u^{-1}U, \mathcal{O}_Y) \xleftarrow{d(U)} \Gamma(U, \mathcal{O}_X)$$

413 définissent une S-déviation de uv que nous noterons de ; lorsque d est d'ordre $\leq m$ et e d'ordre $\leq n$, de est d'ordre $\leq m+n$. Nous écrirons aussi $D \circ E = (uv, de)$ et nous dirons que $D \circ E$ ou DE est la *S-dévi*ation composée. Lorsque d est l'homomorphisme d'Algèbres définissant u ($D = u$ avec la convention ci-dessus), on dit aussi que DE est l'*image* de E par u .

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

1.2.1. — Supposons par exemple Y égal à $I_Z = \text{Spec } \mathcal{O}_Z[T]/(T^2)$ et v égal à la section définie par l'homomorphisme d'Algèbres de $\mathcal{O}_Z[T]/(T^2)$ dans $\mathcal{O}_Z$ qui s'annule sur la classe t de T modulo T^2 . On peut prendre alors pour e le morphisme de $\mathcal{O}_Z$ -Modules qui s'annule sur la section unité de $\mathcal{O}_Z[T]/(T^2)$ et qui envoie t sur la section unité de $\mathcal{O}_Z$. Si l'on pose $D = u$ et $w = uv$, de est alors simplement une S-déviation de $\mathcal{O}_X$ dans $w_*(\mathcal{O}_Z)$; pour tout S-morphisme $w : Z \rightarrow X$ on obtient ainsi une *correspondance biunivoque* entre les S-déviations de $\mathcal{O}_X$ dans $w_*(\mathcal{O}_Z)$ et les S-déviations de w de la forme $u \circ E$, où u parcourt les morphismes de I_Z dans X prolongeant w .

1.2.2. — Si d est une S-déviation de u , d est évidemment une *S'*-déviation de u pour tout morphisme $s : S \rightarrow S'$. D'autre part, soient $t : T \rightarrow S$ un morphisme de but S , $u_T : Y_T \rightarrow X_T$ le morphisme déduit de u par changement de base et t_Y, t_X les projections canoniques de Y_T, X_T dans Y, X . Il existe alors une *T-dévi*ation de u_T et une seule que nous noterons d_T ou $d \times T$ et qui vérifie l'égalité $t_X d_T = d t_Y$. Si l'on pose $D = (u, d)$, on écrira aussi $D_T = (u_T, d_T)$ et nous dirons que d_T et D_T sont déduits de d et D par *changement de base*.

Soient par exemple $u : Y \rightarrow X$ et $v : Z \rightarrow T$ deux S -morphisms, d et e des S -déviation de u et v . Nous noterons $d \times e$ (*produit de d et e*) la S -déviation de $u \times v$ égale à $d_T \circ e_Y = e_X \circ d_Z$. Si l'on pose $D = (u, d)$ et $E = (v, d)$, nous écrirons aussi $D \times E = (u \times v, d \times e)$. 414

1.3. — Supposons maintenant Y égal à S ; alors $u : S \rightarrow X$ est une section de $p : X \rightarrow S$, c'est-à-dire une immersion; on peut alors donner des S -déviation de u l'interprétation que voici : soient I_u le noyau de l'homomorphisme de $u^{-1}(\mathcal{O}_X)$ dans $\mathcal{O}_S$ qui définit u , d un morphisme de $p^{-1}(\mathcal{O}_S)$ -Modules de $\mathcal{O}_X$ dans $u_*(\mathcal{O}_S)$ et $d' : u^{-1}(\mathcal{O}_X) \rightarrow \mathcal{O}_S$ le morphisme associé canoniquement à d . Alors d est une S -déviation de u d'ordre $\leq n$ si et seulement si d' s'annule sur I_u^{n+1} .

Cette interprétation peut être généralisée comme suit : soient $u : Y \rightarrow X$ un S -morphisme quelconque et Γu le graphe de u , c'est-à-dire le morphisme $Y \rightarrow Y \times X$ de composantes Id_Y et u . Pour toute S -déviation d de u d'ordre $\leq n$, on obtient par composition :

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

une Y -déviation de Γu d'ordre $\leq n$ que nous noterons Γd (*le graphe de d*). On obtient ainsi une bijection $d \mapsto \Gamma d$ de l'ensemble des S -déviation de u d'ordre $\leq n$ sur l'ensemble des Y -déviation de Γu d'ordre $\leq n$. La bijection réciproque associe à une Y -déviation $Y \xrightarrow[\Gamma u]{e} Y \times X$ la S -déviation composée

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

Appelons J le noyau de l'homomorphisme d'Algèbres

$$(\Gamma u)^{-1}(\mathcal{O}_{Y \times X}) \longrightarrow \mathcal{O}_Y$$

qui définit Γu . Tenant compte de ce qui précède, on voit alors que les S -déviation de u d'ordre $\leq n$ correspondent canoniquement aux morphismes de $\mathcal{O}_Y$ -Modules de $(\Gamma u)^{-1}(\mathcal{O}_{Y \times X})$ dans $\mathcal{O}_Y$ qui s'annulent sur J^{n+1} . 415

1.4. — Soit X un S -schéma. On appelle *S -opérateur différentiel* (resp. *S -opérateur différentiel d'ordre $\leq n$*) sur X toute S -déviation (resp. toute S -déviation d'ordre $\leq n$) du morphisme identique de X . D'après 1.1, un S -opérateur différentiel d'ordre $\leq n$ est donc un endomorphisme de $p^{-1}(\mathcal{O}_S)$ -Module de $\mathcal{O}_X$ qui vérifie les égalités $(*)_n$ de 1.1.

Nous désignerons par $\text{Dif}_{X/S}^n$ le $\Gamma(\mathcal{O}_S)$ -module formé des S -opérateurs différentiels d'ordre $\leq n$, par $\text{Dif}_{X/S}$ celui formé de tous les S -opérateurs différentiels. Comme nous l'avons vu en 1.2, on peut composer les S -déviation de Id_X , ce qui munit $\text{Dif}_{X/S}$ d'une structure de $\Gamma(\mathcal{O}_S)$ -algèbre; nous dirons que c'est l'*algèbre des opérateurs différentiels de X/S* . De même, nous noterons $\mathcal{Dif}_{X/S}$ le faisceau $U \mapsto \text{Dif}_{X \times U/U}$, où U parcourt les ouverts de S .

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 $\mathcal{O}_{X \times X}$ de la structure de $\text{pr}_1^{-1}(\mathcal{O}_X)$ -Algèbre définie par pr_1 , de sorte que $\Delta^{-1}(\mathcal{O}_{X \times X})$ est muni d'une structure d'Algèbre sur $\mathcal{O}_X = \Delta^{-1}\text{pr}_1^{-1}(\mathcal{O}_X)$. Soient $I_{X/S}$ le noyau de l'homomorphisme

$$\Delta_{X/S}^a : \Delta^{-1}(\mathcal{O}_{X \times X}) \longrightarrow \mathcal{O}_X$$

définissant Δ et $P_{X/S}^m$ la $\mathcal{O}_X$ -Algèbre $\Delta^{-1}(\mathcal{O}_{X \times X})/I_{X/S}^{m+1}$.

416 Si V est un ouvert affine de S et U un ouvert affine de X au-dessus de V , l'ensemble des sections de $P_{X/S}^m$ sur U est donc égal à $A \otimes_k A/I^{m+1}$, où l'on a posé $k = \Gamma(V, \mathcal{O}_S)$, $A = \Gamma(U, \mathcal{O}_X)$ et où I est l'idéal engendré par les éléments $a \otimes 1 - 1 \otimes a$, $a \in A$. Ceci étant, on a d'après 1.3 un isomorphisme canonique

$$j_X : \text{Dif}_{X/S}^m \xrightarrow{\sim} \text{Hom}_{\mathcal{O}_X}(P_{X/S}^m, \mathcal{O}_X)$$

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

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*

$$S \xrightarrow{u} X \xrightarrow[\text{id}_X]{d} X.$$

D'après 1.3 et 1.4.1, si d est un opérateur différentiel d'ordre $\leq n$, du et d sont associés canoniquement à des morphismes

$$d' : u^{-1}(\mathcal{O}_X)/I_u^{m+1} \longrightarrow \mathcal{O}_S \quad \text{et} \quad d'' : P_{X/S}^m \longrightarrow \mathcal{O}_X.$$

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

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

est cartésien, ce qui permet d'identifier X à $S \times_X (X \times X)$, u à $S \times_X \Delta$, donc $u^*(P_{X/S}^m)$ à $u^{-1}(\mathcal{O}_X)/I_u^{m+1}$. On identifie ainsi $u^*(d'')$ à un morphisme $u^{-1}(\mathcal{O}_X)/I_u^{m+1} \rightarrow \mathcal{O}_S$, qui n'est autre que d' .

417 **1.5.** — Posons comme d'habitude $I_S = \text{Spec } \mathcal{O}_S[T]/(T^2)$. Soient $s : S \rightarrow I_S$ la section zéro (II 2.1) et σ la déviation canonique de s que nous avons définie en 1.2.1 : la déviation σ est donc l'homomorphisme de $\mathcal{O}_S$ -Modules qui s'annule sur la section unité de $\mathcal{O}_S[T]/(T^2)$ et qui envoie la classe t de T modulo T^2 sur la section unité de $\mathcal{O}_S$.

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

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

D'après II 4.11, l'application $u \mapsto D_u$ est un isomorphisme de l'algèbre de Lie du foncteur en groupes $\underline{\text{Aut}} X$ sur l'algèbre de Lie des $p^{-1}(\mathcal{O}_S)$ -dérivations de $\mathcal{O}_X$. L'isomorphisme réciproque associe à toute dérivation D l'automorphisme de $I_S \times X$ correspondant à l'automorphisme $a + bt \mapsto a + (Da + b)t$ de $\mathcal{O}_S[T]/(T^2)$.

2. Opérateurs différentiels invariants sur les schémas en groupes

418

2.1. — Soit G un S -schéma en groupes. Nous désignons par ε ou $\varepsilon_G : S \rightarrow G$ la section unité de G et par $U(G)$ le $\Gamma(\mathcal{O}_S)$ -module des S -déviation de ε_G (ou S -déviation de l'origine) (cf. 1.1). Si d et e sont deux éléments de $U(G)$, $d \times e$ est une S -déviation de $\varepsilon \times \varepsilon : S \simeq S \times S \rightarrow G \times G$. L'image de $d \times e$ par le morphisme multiplication $m : G \times G \rightarrow G$ (cf. 1.2) sera appelé le produit de d et e et sera noté $d \cdot e$. Le $\Gamma(\mathcal{O}_S)$ -module $U(G)$ se trouve ainsi muni d'une structure de $\Gamma(\mathcal{O}_S)$ -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 schémas au-dessus de S , l'algèbre infinitésimale $U(G_T)$ du T -groupe $G \times T$ varie évidemment de façon contravariante en T , de sorte que nous pourrions parler du foncteur algèbre infinitésimale. En particulier, lorsque T parcourt les ouverts de S , le foncteur $T \mapsto U(G_T)$ est un faisceau d'algèbres que nous noterons $\mathcal{U}(G)$ et que nous appellerons l'algèbre infinitésimale.

L'algèbre $U(G)$ est aussi un foncteur covariant en G : si $u : G \rightarrow H$ 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 $U(u) : U(G) \rightarrow U(H)$ ainsi définie est évidemment un homomorphisme de $\Gamma(\mathcal{O}_S)$ -algèbres. On définit de même un homomorphisme $\mathcal{U}(u)$ de $\mathcal{U}(G)$ dans $\mathcal{U}(H)$.

2.2. — Soient maintenant d une S -déviation de l'origine de G et $d \times G$ la S -déviation de $\varepsilon \times G : G \simeq S \times G \rightarrow G \times G$ obtenue à partir de d par changement de base. L'image de $d \times G$ par le morphisme multiplication $m : G \times G \rightarrow G$ est un opérateur différentiel d^G de G sur S . De plus, l'application $d \mapsto d^G$ est évidemment $\Gamma(\mathcal{O}_S)$ -linéaire et le diagramme « commutatif »

$$\begin{array}{ccccc}
 & & G \times G \times G & \xrightarrow{m \times G} & G \times G \\
 & \nearrow d \times G \times G & & \searrow G \times m & \\
 & G \times G & & G \times G & \\
 \nearrow e \times G & & \searrow m & \nearrow d \times G & \searrow m \\
 G & \xrightarrow{e^G} & G & \xrightarrow{d^G} & G \\
 & \text{Id } G & & \text{Id } G &
 \end{array}$$

montre qu'on a $(d \cdot e)^G = d^G \cdot e^G$: 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 $e \times G$, $d \times G \times G$ et $m \times G$ coïncide avec $(d \cdot e) \times G$; son image par m est donc égale à $(d \cdot e)^G$.

419

On obtient ainsi un homomorphisme, appelé *translation à droite*, de la $\Gamma(\mathcal{O}_S)$ -algèbre $U(G)$ dans $\text{Dif}_{G/S}$. Si $\mathcal{Dif}_{G/S}$ désigne le faisceau $U \mapsto \text{Dif}_{G \times U/U}$ sur S (1.4), on définit de même une « Translation à droite » du faisceau $\mathcal{U}(G)$ dans $\mathcal{Dif}_{G/S}$.

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

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

Pour tout opérateur différentiel D de G sur S , nous notons alors D^g l'opérateur $g_G^{-1} D g_G$ (1.2). Nous disons que D est *invariant à droite* si, pour tout changement de base $t : T \rightarrow S$ et toute section $g : T \rightarrow G \times T$, on a $(D_T)^g = D_T$.

420 **Lemme.** — *Pour tout opérateur différentiel D de G sur S , les assertions suivantes sont équivalentes :*

- (i) D est invariant à droite.
- (ii) Si m est le morphisme multiplication de G , on a $Dm = m(D \times G)$.

(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 $g : S \rightarrow G$. Ceci résulte du diagramme commutatif

$$\begin{array}{ccccc} G & \xleftarrow{m} & G \times G & \xleftarrow{h} & G \\ \downarrow D \text{ Id } G & & \downarrow D \times G \text{ Id } (G \times G) & & \downarrow D \text{ Id } G \\ G & \xleftarrow{m} & G \times G & \xleftarrow{h} & G \end{array},$$

où h est le morphisme

$$G \xrightarrow{\sim} G \times S \xrightarrow{G \times g} G \times G$$

et $m \circ h$ la translation à droite par g .

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

$$\begin{array}{ccccc} G \times G & \xrightarrow{\Delta_{G \times G}} & G \times G & \xrightarrow{\text{pr}_1} & G \\ \downarrow D_G \text{ Id } G \times G & & \downarrow D_G \text{ Id } G \times G & & \downarrow D \text{ Id } G \\ G \times G & \xrightarrow{\Delta_{G \times G}} & G \times G & \xrightarrow{\text{pr}_1} & G \end{array}.$$

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

421 Considérons par exemple un élément d de l'algèbre infinitésimale $U(G)$. Les deux

carrés du diagramme

$$\begin{array}{ccccc}
 G \times G & \xrightarrow[\varepsilon \times G \times G]{d \times G \times G} & G \times G \times G & \xrightarrow{m \times G} & G \times G \\
 \downarrow m & & \downarrow G \times m & & \downarrow m \\
 G & \xrightarrow[\varepsilon \times G]{d \times G} & G \times G & \xrightarrow{m} & G
 \end{array}$$

sont alors commutatifs. Comme on a $m \circ (d \times G) = d^G$ et $(m \times G) \circ (d \times G \times G) = d^G \times G$, on a aussi $d^G \circ m = m \circ (d^G \times G)$. Pour toute S -déviation d de l'origine, d^G est donc 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 $\text{Dif}_{G/S}^G$ de $\text{Dif}_{G/S}$ 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 $S \xrightarrow{\varepsilon} G \xrightarrow[\text{id}_G]{D} G$. L'opérateur différentiel invariant à droite $(D_0)^G$ est alors obtenu par composition :

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

Si D est invariant à droite, on a $Dm = m(D \times G)$, d'où $D = Dm(\varepsilon \times G) = m(D \times G)(\varepsilon \times G) = D_0^G$. 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

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

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

Lorsque S varie, le théorème 2.4 implique évidemment que la Translation à droite $\mathcal{U}(G) \rightarrow \mathcal{Dif}_{G/S}$ est un isomorphisme de $\mathcal{O}_S$ -Algèbres de $\mathcal{U}(G)$ sur la sous-Algèbre $\mathcal{Dif}_{G/S}^G : U \mapsto \text{Dif}_{G_U/U}^G$.

2.4.1. Remarque. — Considérons le diagramme commutatif

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

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

$$\eta' : \eta^{-1}(\mathcal{O}_G) \longrightarrow \mathcal{O}_{G \times G} \quad \text{et} \quad \Delta^{-1}(\eta') : p^{-1}\varepsilon^{-1}(\mathcal{O}_G) \longrightarrow \Delta^{-1}(\mathcal{O}_{G \times G}).$$

Pour tout entier $n \geq 1$, $\Delta^{-1}(\eta')$ définit par passage au quotient un homomorphisme de faisceaux :

$$\eta^n : p^{-1}(p_{G/S}^n) \longrightarrow P_{G/S}^n,$$

où nous avons posé $p_{G/S}^n = \varepsilon^{-1}(\mathcal{O}_G)/I_\varepsilon^{n+1}$ (confer 1.3 et 1.4 pour les notations). Comme le carré formé par les morphismes η , p , pr_1 et p est cartésien, η^n induit un isomorphisme de $p^*(p_{G/S}^n)$ sur $P_{G/S}^n$.

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

$$p_{G/S}^n \longrightarrow p_*(\mathcal{O}_G).$$

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

$$p_{G/S}^n \longrightarrow \mathcal{O}_S \xrightarrow{\text{can.}} p_*(\mathcal{O}_G).$$

On retrouve ainsi l'isomorphisme du théorème 2.4.

2.5. — Soit $\gamma : G \rightarrow \underline{\text{Aut}} G$ l'homomorphisme de foncteurs en groupes qui associe à un S -morphisme $g : T \rightarrow G$ la translation à gauche de G_T par g , c'est-à-dire le morphisme composé

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

Cet homomorphisme γ définit le diagramme d'ensembles ci-dessous

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

où l'on désigne par β l'application $u \mapsto D_u$ de 1.5, par δ la translation à droite définie en 2.2. Si x est un élément de $\text{Lie } G$, c'est-à-dire un morphisme de I_S dans G tel qu'on ait $xs = \varepsilon_G$ avec les notations de 1.5, on a le carré commutatif suivant qui détermine l'image de x par $\text{Lie } \gamma$:

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

424 D'après 1.5, l'image de $(\text{Lie } \gamma)(x)$ par β est la déviation composée

$$G \simeq S \times G \xrightarrow[\text{Id}]{\sigma \times G} I_S \times G \xrightarrow{x \times G} G \times G \xrightarrow{m} G.$$

D'après 2.2, cette déviation composée n'est autre que $(x\sigma)^G$. En notant α l'application $x \mapsto x\sigma$ de $\text{Lie } G$ dans $U(G)$, on a donc

$$\beta(\text{Lie } \gamma) = \delta\alpha.$$

En particulier, α est un homomorphisme injectif de $\text{Lie } G$ dans l'algèbre de Lie sous-jacente à l'algèbre infinitésimale $U(G)$.

3. Coalgèbres et dualité de Cartier

425

3.1. — Soit S un schéma (ou, plus généralement, un espace annelé). Une $\mathcal{O}_S$ -Coalgèbre est un couple $(\mathcal{U}, \Delta_{\mathcal{U}})$ formé d'un $\mathcal{O}_S$ -Module $\mathcal{U}$ et d'un morphisme de $\mathcal{O}_S$ -Modules $\Delta_{\mathcal{U}} : \mathcal{U} \rightarrow \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U}$ (dit *morphisme diagonal*) tels que :

- (i) $\sigma \circ \Delta_{\mathcal{U}} = \Delta_{\mathcal{U}}$, où $\sigma(a \otimes b) = b \otimes a$.
- (ii) Le carré

$$\begin{array}{ccc} \mathcal{U} & \xrightarrow{\Delta_{\mathcal{U}}} & \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U} \\ \Delta_{\mathcal{U}} \downarrow & & \downarrow \text{id}_{\mathcal{U}} \otimes \Delta_{\mathcal{U}} \\ \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U} & \xrightarrow{\Delta_{\mathcal{U}} \otimes \text{id}_{\mathcal{U}}} & \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U} \end{array}$$

soit commutatif.

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

$$\begin{aligned} \mathcal{U} &\xrightarrow{\Delta_{\mathcal{U}}} \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U} \xrightarrow{\text{id}_{\mathcal{U}} \otimes \varepsilon_{\mathcal{U}}} \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{O}_S \simeq \mathcal{U} \\ \mathcal{U} &\xrightarrow{\Delta_{\mathcal{U}}} \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U} \xrightarrow{\varepsilon_{\mathcal{U}} \otimes \text{id}_{\mathcal{U}}} \mathcal{O}_S \otimes_{\mathcal{O}_S} \mathcal{U} \simeq \mathcal{U} \end{aligned}$$

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

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

Si $(\mathcal{U}, \Delta_{\mathcal{U}})$ et $(\mathcal{V}, \Delta_{\mathcal{V}})$ sont deux $\mathcal{O}_S$ -Coalgèbres, un morphisme de la première dans la seconde est un morphisme de $\mathcal{O}_S$ -Modules $f : \mathcal{U} \rightarrow \mathcal{V}$ tel que les diagrammes

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

soient commutatifs. Les morphismes de Coalgèbres se composent comme les morphismes de $\mathcal{O}_S$ -Modules de sorte que nous pourrions parler de la catégorie des $\mathcal{O}_S$ -Coalgèbres.

426

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

$$\mathcal{U} \otimes \mathcal{V} \xrightarrow{\Delta_{\mathcal{U}} \otimes \Delta_{\mathcal{V}}} \mathcal{U} \otimes \mathcal{U} \otimes \mathcal{V} \otimes \mathcal{V} \xrightarrow{\text{id}_{\mathcal{U}} \otimes \sigma \otimes \text{id}_{\mathcal{V}}} \mathcal{U} \otimes \mathcal{V} \otimes \mathcal{U} \otimes \mathcal{V}$$

où $\sigma(a \otimes b) = b \otimes a$; les projections canoniques de $\mathcal{U} \otimes \mathcal{V}$ sur les facteurs $\mathcal{U}$ et $\mathcal{V}$ sont les morphismes $\text{id}_{\mathcal{U}} \otimes \varepsilon_{\mathcal{V}}$ et $\varepsilon_{\mathcal{U}} \otimes \text{id}_{\mathcal{V}}$.

3.1.1. — Soit $\mathcal{A}$ une $\mathcal{O}_S$ -Algèbre commutative, localement libre et de type fini en tant que $\mathcal{O}_S$ -Module. Si nous posons

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

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

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

427 Ce morphisme diagonal fait évidemment de $\mathcal{A}^*$ une $\mathcal{O}_S$ -Coalgèbre qui a pour augmentation le morphisme transposé du morphisme $\mathcal{O}_S \rightarrow \mathcal{A}$ défini par la section unité de $\mathcal{A}$. De plus, il est clair que *le foncteur $\mathcal{A} \mapsto \mathcal{A}^*$ est une antiéquivalence de la catégorie des $\mathcal{O}_S$ -Algèbres, qui sont localement libres et de type fini en tant que $\mathcal{O}_S$ -Modules, sur la catégorie des $\mathcal{O}_S$ -Coalgèbres localement libres et de type fini en tant que $\mathcal{O}_S$ -Modules.*

3.1.2. — A toute $\mathcal{O}_S$ -Coalgèbre $\mathcal{U}$ est associée canoniquement un S-foncteur $\text{Spec}^* \mathcal{U} : (\mathbf{Sch}/S)^\circ \rightarrow (\mathbf{Ens})$: remarquons en effet que, pour tout S-schéma $q : T \rightarrow S$, $q^*(\mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U})$ s'identifie à $q^*(\mathcal{U}) \otimes_{\mathcal{O}_T} q^*(\mathcal{U})$, de sorte que $q^*(\Delta_{\mathcal{U}})$ fait de $\mathcal{U}_T = q^*(\mathcal{U})$ une $\mathcal{O}_T$ -Coalgèbre ; nous pouvons donc poser par définition et avec un abus de notation évident :

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

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

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

En particulier, si $\mathcal{A}$ est une $\mathcal{O}_S$ -Algèbre commutative qui est localement libre de type fini en tant que $\mathcal{O}_S$ -Module, on a des isomorphismes

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

et

$$\text{Spec}^* \mathcal{A}^* \simeq \text{Spec } \mathcal{A}.$$

428 **3.2.** — Une $\mathcal{O}_S$ -Coalgèbre en groupes, c'est-à-dire un groupe de la catégorie des $\mathcal{O}_S$ -Coalgèbres, consiste en la donnée d'une $\mathcal{O}_S$ -Coalgèbre $(\mathcal{U}, \Delta_{\mathcal{U}})$ et d'un morphisme de $\mathcal{O}_S$ -Coalgèbres $m_{\mathcal{U}} : \mathcal{U} \otimes \mathcal{U} \rightarrow \mathcal{U}$. Un tel morphisme est un morphisme de

$\mathcal{O}_S$ -Modules rendant commutatifs les diagrammes suivants

$$\begin{array}{c}
 \text{(iv)} \quad \begin{array}{ccc}
 \mathcal{U} \otimes \mathcal{U} \otimes \mathcal{U} \otimes \mathcal{U} & \xleftarrow{\Delta_{\mathcal{U}} \otimes \Delta_{\mathcal{U}}} & \mathcal{U} \otimes \mathcal{U} \\
 \downarrow \text{id}_{\mathcal{U}} \otimes \sigma \otimes \text{id}_{\mathcal{U}} & & \searrow m_{\mathcal{U}} \\
 \mathcal{U} \otimes \mathcal{U} \otimes \mathcal{U} \otimes \mathcal{U} & \xrightarrow{m_{\mathcal{U}} \otimes m_{\mathcal{U}}} & \mathcal{U} \otimes \mathcal{U} \\
 & & \swarrow \Delta_{\mathcal{U}} \\
 & & \mathcal{U}
 \end{array} \\
 \\
 \text{(v)} \quad \begin{array}{ccc}
 \mathcal{U} \otimes \mathcal{U} & \xrightarrow{m_{\mathcal{U}}} & \mathcal{U} \\
 \searrow \varepsilon_{\mathcal{U}} \otimes \varepsilon_{\mathcal{U}} & & \swarrow \varepsilon_{\mathcal{U}} \\
 & \mathcal{O}_S &
 \end{array}
 \end{array}$$

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

(ii)* Le carré

$$\begin{array}{ccc}
 \mathcal{U} \otimes \mathcal{U} \otimes \mathcal{U} & \xrightarrow{\text{id}_{\mathcal{U}} \otimes m_{\mathcal{U}}} & \mathcal{U} \otimes \mathcal{U} \\
 \downarrow m_{\mathcal{U}} \otimes \text{id}_{\mathcal{U}} & & \downarrow m_{\mathcal{U}} \\
 \mathcal{U} \otimes \mathcal{U} & \xrightarrow{m_{\mathcal{U}}} & \mathcal{U}
 \end{array}$$

est commutatif.

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

$$\begin{aligned}
 \mathcal{U} &\simeq \mathcal{U} \otimes \mathcal{O}_S \xrightarrow{\text{id}_{\mathcal{U}} \otimes \eta_{\mathcal{U}}} \mathcal{U} \otimes \mathcal{U} \xrightarrow{m_{\mathcal{U}}} \mathcal{U} \\
 \text{et } \mathcal{U} &\simeq \mathcal{O}_S \otimes \mathcal{U} \xrightarrow{\eta_{\mathcal{U}} \otimes \text{id}_{\mathcal{U}}} \mathcal{U} \otimes \mathcal{U} \xrightarrow{m_{\mathcal{U}}} \mathcal{U}
 \end{aligned}$$

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

(vi) Il existe un morphisme de $\mathcal{O}_S$ -Coalgèbres $c_{\mathcal{U}} : \mathcal{U} \rightarrow \mathcal{U}$ tel que le morphisme composé

$$\mathcal{U} \xrightarrow{\Delta_{\mathcal{U}}} \mathcal{U} \otimes \mathcal{U} \xrightarrow{c_{\mathcal{U}} \otimes \text{id}_{\mathcal{U}}} \mathcal{U} \otimes \mathcal{U} \xrightarrow{m_{\mathcal{U}}} \mathcal{U}$$

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

3.2.1. — Les morphismes $\eta_{\mathcal{U}}$ et $c_{\mathcal{U}}$ de (iii)* et (vi) sont évidemment uniques. Les conditions (ii)* et (iii)* expriment simplement que $m_{\mathcal{U}}$ fait de $\mathcal{U}$ une $\mathcal{O}_S$ -algèbre qui a pour section unité l'image par $\eta_{\mathcal{U}}$ de la section unité de $\mathcal{O}_S$. La condition (iv) exprime aussi que le morphisme diagonal $\Delta_{\mathcal{U}}$ est compatible avec la multiplication ; et en effet,

$\Delta_{\mathcal{U}} : \mathcal{U} \rightarrow \mathcal{U} \otimes \mathcal{U}$ doit être un homomorphisme de Coalgèbres en groupes, ce qui implique également la commutativité du triangle

$$(v)^* \quad \begin{array}{ccc} & \mathcal{O}_S & \\ \eta_{\mathcal{U}} \swarrow & & \searrow \eta_{\mathcal{U}} \otimes \eta_{\mathcal{U}} \\ \mathcal{U} & \xrightarrow{\Delta_{\mathcal{U}}} & \mathcal{U} \otimes \mathcal{U} \end{array} .$$

D'autre part, comme dans toute catégorie, l'antipodisme $c_{\mathcal{U}}$ est un isomorphisme de $\mathcal{U}$ sur la Coalgèbre en groupes opposée; en particulier, $c_{\mathcal{U}}$ induit un isomorphisme d'algèbres de $\mathcal{U}$ sur l'algèbre opposée $\mathcal{U}^\circ$.

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

Soient par exemple $\mathfrak{g}$ une $\mathcal{O}_S$ -Algèbre de Lie et $\mathcal{U}(\mathfrak{g})$ 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 $\Gamma(V, \mathfrak{g})$.

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

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

3.2.3. — Soit $\mathcal{U}$ une $\mathcal{O}_S$ -Coalgèbre en groupes. On vérifie facilement que $G = \text{Spec}^* \mathcal{U}$ est un bon S-groupe (II 4.6). Comme on a

$$\Gamma(I_S, \mathcal{U}_{I_S}) \simeq \Gamma(S, \mathcal{U}) \oplus d\Gamma(S, \mathcal{U}),$$

un élément $u_0 + du_1$ de $\Gamma(I_S, \mathcal{U}_{I_S})$ appartient à $(\text{Spec}^* \mathcal{U})(I_S)$ si et seulement si l'on a

$$\Delta(u_0 + du_1) = (u_0 + du_1) \otimes (u_0 + du_1) \quad \text{et} \quad \varepsilon(u_0 + du_1) = 1,$$

d'où $\Delta u_0 + d\Delta u_1 = u_0 \otimes u_0 + (u_1 \otimes u_0 + u_0 \otimes u_1)d$ et $\varepsilon(u_0) + d\varepsilon(u_1) = 1$ c'est-à-dire $\Delta u_0 = u_0 \otimes u_0$, $u_1 = u_1 \otimes u_0 + u_0 \otimes u_1$ et $\varepsilon(u_0) = 1$, $\varepsilon(u_1) = 0$.

En particulier, $(\text{Lie } G)(T)$ est l'ensemble des éléments primitifs de $\Gamma(T, \mathcal{U}_T)$, c'est-à-dire des éléments u tels qu'on ait $\Delta u = u \otimes 1 + 1 \otimes u$ (avec l'abus de notation évident déjà signalé).

La structure de $\Gamma(T, \mathcal{O}_T)$ -module de $(\text{Lie } G)(T)$ est évidemment induite par celle de $\Gamma(T, \mathcal{U}_T)$. D'autre part, considérons deux éléments primitifs u et v de $(\text{Lie } G)(S)$

et posons $I = \operatorname{Spec} \mathcal{O}_S[d]/(d^2)$ et $I' = \operatorname{Spec} \mathcal{O}_S[d']/(d'^2)$. Comme la loi de composition de $G(I \times I')$ est induite par la multiplication de l'Algèbre $\mathcal{U}_{I \times I'}$, on a

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

D'où l'égalité $[u, v] = uv - vu$, qui prouve que G est très bon (II 4.10).

431

3.3. — Supposons enfin que $\mathcal{U}$ soit une $\mathcal{O}_S$ -Coalgèbre en groupes commutatifs, c'est-à-dire que le triangle

$$(i)^* \quad \begin{array}{ccc} \mathcal{U} \otimes \mathcal{U} & \xrightarrow{\sigma} & \mathcal{U} \otimes \mathcal{U} \\ & \searrow m_{\mathcal{U}} \quad \swarrow m_{\mathcal{U}} & \\ & \mathcal{U} & \end{array}$$

soit commutatif, ou encore que $m_{\mathcal{U}}$ fasse de $\mathcal{U}$ une $\mathcal{O}_S$ -Algèbre commutative. Les conditions (i), (ii), (iii), (iv), (v), (vi), (i)*, (ii)*, (iii)* et (v)* signifient alors aussi que $\mathcal{U}$ est un cogroupe dans la catégorie des $\mathcal{O}_S$ -Algèbres commutatives. En particulier, si de plus $\mathcal{U}$ est un $\mathcal{O}_S$ -Module quasi-cohérent, $\operatorname{Spec} \mathcal{U}$ est un S -schéma en groupes commutatifs.

Un homomorphisme de S -groupes de $\operatorname{Spec} \mathcal{U}$ dans $\mathbb{G}_{m,S}$ (I 4.3.2) est alors induit par un homomorphisme de $\mathcal{O}_S$ -Algèbres unitaires

$$\varphi : \mathcal{O}_S[T, T^{-1}] \longrightarrow \mathcal{U}$$

tel que $(\varphi \otimes \varphi) \circ \Delta' = \Delta_U \circ \varphi$ (le morphisme diagonal Δ' de $\mathcal{O}_S[T, T^{-1}]$ envoie T sur $T \otimes T$). Un tel homomorphisme φ est déterminé par l'image $\varphi(T)$ qui doit être un élément inversible x de $\mathcal{U}$ tel que $\Delta_{\mathcal{U}} x = x \otimes x$; comme φ commute alors nécessairement avec l'augmentation, on a $\varepsilon_{\mathcal{U}} x = 1$ (l'augmentation de $\mathcal{O}_S[T, T^{-1}]$ envoie T sur 1). On a donc

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

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

432

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

pour toute $\mathcal{O}_S$ -Coalgèbre en groupes commutatifs quasi-cohérente $\mathcal{U}$.

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

$$\operatorname{Spec}^* \mathcal{U} \simeq \operatorname{Spec} \mathcal{U}^*.$$

Le foncteur $\mathcal{U} \mapsto \mathcal{U}^* = \mathcal{H}om_{\mathcal{O}_S\text{-Mod.}}(\mathcal{U}, \mathcal{O}_S)$ induit donc une dualité (*) de la catégorie des S -schémas en groupes commutatifs qui sont finis localement libres sur S (c'est la *dualité de CARTIER*). D'après 3.3, cette dualité associe $\underline{\operatorname{Hom}}_{S\text{-gr.}}(G, \mathbb{G}_{m,S})$ à un S -groupe G .

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

433

4. « Frobeniusseries »

Soient p un nombre premier fixé et $(\mathbf{Sch}/\mathbb{F}_p)$ la catégorie des schémas de caractéristique p , c'est-à-dire des schémas au-dessus du corps premier $\mathbb{F}_p$. Suivant les conventions générales de ce séminaire, nous identifions $(\mathbf{Sch}/\mathbb{F}_p)$ à une sous-catégorie de $(\widehat{\mathbf{Sch}}/\mathbb{F}_p)$ au moyen du foncteur $\mathbf{h}$ de I 1.1. Nous profitons de même de l'isomorphisme de $\mathrm{Hom}(\mathbf{h}_X, \mathbf{F})$ sur $\mathbf{F}(X)$ défini en I 1.1 pour identifier ces deux ensembles chaque fois que X est un $\mathbb{F}_p$ -schéma et $\mathbf{F}$ un objet de $(\widehat{\mathbf{Sch}}/\mathbb{F}_p)$. Si T est un $\mathbb{F}_p$ -schéma, un T -foncteur est un morphisme $q : \mathbf{F} \rightarrow T$ de $(\widehat{\mathbf{Sch}}/\mathbb{F}_p)$ qui a T pour but ; pour tout T -schéma $r : X \rightarrow T$, l'ensemble des morphismes $s : X \rightarrow \mathbf{F}$ tels que $q \circ s = r$ sera alors noté $q(r)$, $q(X/T)$, $\mathbf{F}(r)$ ou $\mathbf{F}(X/T)$ (ou même $\mathbf{F}(X)$ lorsqu'aucune confusion ne sera possible avec $\mathrm{Hom}(\mathbf{h}_X, \mathbf{F})$).

4.1. — Pour tout schéma S de caractéristique p , nous notons $\mathrm{fr}(S)$ ou 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 $\mathcal{O}_S$ sur un ouvert U . Alors l'application $\mathrm{fr} : S \mapsto \mathrm{fr}(S)$ est un endomorphisme du foncteur identique de $(\mathbf{Sch}/\mathbb{F}_p)$, ce qui implique les résultats suivants : soit E un $\mathbb{F}_p$ -foncteur, c'est-à-dire un objet de $(\widehat{\mathbf{Sch}}/\mathbb{F}_p)$; l'application qui associe à tout $\mathbb{F}_p$ -schéma S l'endomorphisme $E(\mathrm{fr}(S))$ de $E(S)$, est un endomorphisme fonctoriel de E que nous noterons $\mathrm{fr}(E)$ ou fr ; cette notation est compatible avec l'identification de $(\mathbf{Sch}/\mathbb{F}_p)$ à une sous-catégorie de $(\widehat{\mathbf{Sch}}/\mathbb{F}_p)$; de plus, l'application $E \mapsto \mathrm{fr}(E)$ est un endomorphisme du foncteur identique de $(\widehat{\mathbf{Sch}}/\mathbb{F}_p)$ (que nous noterons encore fr).

Pour tout schéma S de caractéristique p et tout S -foncteur $q : X \rightarrow S$, nous notons $X^{(p/S)}$ ou $X^{(p)}$ l'image réciproque $S \times_{\mathrm{fr}, q} X$ de X par le changement de base $\mathrm{fr}(S)$. Le carré commutatif

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

434 induit alors un S -morphisme $\mathrm{Fr}(X/S)$ ou Fr de X dans $X^{(p/S)}$ tel que $\mathrm{fr}(X) = \mathrm{pr}_2 \circ \mathrm{Fr}(X/S)$. Nous dirons que $\mathrm{Fr}(X/S)$ est le *morphisme de Frobenius de X relativement à S* ; il est clair que l'application $\mathrm{Fr} : X \mapsto \mathrm{Fr}(X/S)$ est un homomorphisme fonctoriel.

D'après les définitions, pour tout S -schéma $K : T \rightarrow S$, l'application $\mathrm{Fr}(X/S)(K)$ peut donc être caractérisée par la commutativité du triangle

$$\begin{array}{ccc} X^{(p/S)}(K) & \xrightarrow{\sim} & X(\mathrm{fr}(S) \circ K) = X(K \circ \mathrm{fr}(T)) \\ \mathrm{Fr}(X/S)(K) \swarrow & & \searrow X(\mathrm{fr}(T)) \\ & X(K) & \end{array} \quad .$$

(†)

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

4.1.1. — Considérons maintenant un changement de base $t : T \rightarrow S$. Comme le carré

$$\begin{array}{ccc} T & \xrightarrow{\text{fr}(T)} & T \\ t \downarrow & & \downarrow t \\ S & \xrightarrow{\text{fr}(S)} & S \end{array}$$

est commutatif, l'image réciproque de $X \times T$ par $\text{fr}(T)$ s'identifie à l'image réciproque 435

de $X \times S$ par t ; autrement dit, on a un isomorphisme canonique de $X_T^{(p/T)}$ sur $(X^{(p/S)})_T$. Il est clair que, dans cette identification, $\text{Fr}(X_T/T)$ s'identifie à l'image réciproque $\text{Fr}(X/S)_T$ de $\text{Fr}(X/S)$.

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

4.1.2. — Le foncteur $X \mapsto X^{(p/S)}$ commute évidemment aux produits; il transforme donc un S -groupe G en un S -groupe $G^{(p/S)}$; de plus, comme Fr est un homomorphisme fonctoriel, $\text{Fr}(G/S)$ est un homomorphisme de S -groupes. Nous noterons $_{\text{Fr}}G$ le noyau de cet homomorphisme : si $q : T \rightarrow S$ est un schéma au-dessus de S , il résulte de 4.1 que la valeur de $_{\text{Fr}}G$ en q est le noyau de l'homomorphisme $G(\text{fr}(T)) : G(q) \rightarrow G(q \circ \text{fr}(T))$. Par exemple, lorsque T est le schéma I_R des nombres duals sur un S -schéma R , $\text{fr}(I_R)$ se factorise comme suit

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

Ceci montre que $(_{\text{Fr}}G)(I_R)$ contient le noyau du morphisme $G(I_R) \rightarrow G(R)$ et qu'on a $\text{Lie } G/S = \text{Lie } (_{\text{Fr}}G/S)$.

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

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

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

$$X \xrightarrow{\text{Fr}(X/S)} X^{(p)} \xrightarrow{\text{Fr}(X^{(p)}/S)} X^{(p^2)} \dots X^{(p^{n-1})} \xrightarrow{\text{Fr}(X^{(p^{n-1})}/S)} X^{(p^n)}.$$

Si G est un S -foncteur en groupes, $G^{(p^n)}$ en est un également et $\text{Fr}^n(G/S)$ est un homomorphisme de S -foncteurs en groupes. Nous noterons $_{\text{Fr}^n}G$ le noyau de $\text{Fr}^n(G/S)$ et nous dirons que G est de hauteur $\leq n$ si $\text{Fr}^n(G/S)$ est nul, c'est-à-dire si $_{\text{Fr}^n}G = G$.

Le sous-foncteur en groupes ${}_{\mathrm{Fr}^n}G$ de G est caractéristique, en ce sens que, pour tout S -schéma T , tout endomorphisme f du T -foncteur en groupes G_T induit un endomorphisme de $({}_{\mathrm{Fr}^n}G)_T$: en effet, comme la construction de $G^{(p^n)}$ et de $\mathrm{Fr}^n(G/S)$ commute aux changements de base d'après 4.1.1, on peut supposer $T = S$; dans ce cas, l'assertion résulte de ce que $\mathrm{Fr}^n(G/S)$ est un homomorphisme fonctoriel.

On notera enfin que $F(X^{(p)}/S)$ coïncide avec $F(X/S)^{(p)}$.

4.1.4. — Voici quelques exemples :

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

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

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

437 où $E^{(p)}$ est l'image réciproque de E par $\mathrm{fr}(S)$. De plus, d'après 4.1, l'application $\mathrm{Fr}(\mathbf{W}(E))(q)$ est déterminée pour tout S -schéma T par le triangle commutatif

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

où f' est l'application induite par $\mathrm{fr}(T)$.

En particulier, si E est égal à $\mathcal{O}_S$, $\mathbf{W}(E)$ s'identifie au groupe additif $\mathbb{G}_{a,S}$. Dans ce cas, on a $E^{(p)} = E = \mathcal{O}_S$ et le morphisme de Frobenius $\mathrm{Fr}(\mathbb{G}_{a,S}/S)$ applique $x \in \Gamma(T, \mathcal{O}_T)$ sur x^p . Le noyau $\alpha_{p,S}$ du morphisme de Frobenius de $\mathbb{G}_{a,S}$ associe donc à tout S -schéma T l'ensemble des sections x de $\mathcal{O}_T$ telles que $x^p = 0$.

c) On verrait de même que, pour toute $\mathcal{O}_S$ -Algèbre quasi-cohérente $\mathcal{A}$, $(\mathrm{Spec} \mathcal{A})^{(p)}$ s'identifie au spectre $\mathrm{Spec} \mathcal{A}^{(p)}$ de l'image réciproque de $\mathcal{A}$ par $\mathrm{fr}(S)$. Si π désigne l'endomorphisme $x \mapsto x^p$ du faisceau d'anneaux $\mathcal{O}_S$, on a donc $\mathcal{A}^{(p)} = \mathcal{A} \otimes_\pi \mathcal{O}_S$ et il est clair que $\mathrm{Fr}((\mathrm{Spec} \mathcal{A})/S)$ est induit par l'homomorphisme $a \otimes_\pi x \mapsto a^p x$ de $\mathcal{A} \otimes_\pi \mathcal{O}_S$ dans $\mathcal{A}$.

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

$$\mathbf{V}(E)^{(p)} \simeq \mathbf{V}(E^{(p)}) \quad \text{et} \quad \mathcal{S}(E)^{(p)} \simeq \mathcal{S}(E^{(p)}),$$

où $\mathcal{S}(E)$ désigne l'Algèbre symétrique du $\mathcal{O}_S$ -Module E .

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

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

Si $\mathcal{U}$ est une Coalgèbre en groupes, la valeur de $_{\mathrm{Fr}}(\mathrm{Spec}^* \mathcal{U})$ pour un S -schéma T est donc l'ensemble des éléments γ de $\Gamma(T, \mathcal{U}_T)$ tels que

$$\mathrm{varepsilon}_{\mathcal{U}_T}(x) = 1, \quad \Delta_{\mathcal{U}_T} x = x \otimes x, \quad \text{et} \quad \gamma \circ \mathrm{times}_{\mathrm{Fr}(T)} 1 = 1.$$

4.2. — Nous allons maintenant nous occuper d'une construction voisine de la précédente : soient S un schéma de caractéristique p , X un S -schéma et X_S^p le produit dans la catégorie $(\mathbf{Sch}/_S)$ de p exemplaires de X . Nous désignons alors par $U^p(X)$ le sous-schéma ouvert de X_S^p qui est la réunion des produits U_S^p , lorsque U parcourt les ouverts affines de X . Un point x de X_S^p appartient donc à $U^p(X)$ 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 $\mathcal{S}_p$ 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 -uplé de X et nous noterons $\Sigma^p X$ le quotient de X_S^p par $\mathcal{S}_p$ dans la catégorie de tous les espaces annelés. La projection canonique $q : X_S^p \rightarrow \Sigma^p X$ 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 schéma ; le morphisme $q' : U^p(X) \rightarrow V^p(X)$ induit par q 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 $V^p(X)$; si k 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 $\bigotimes_k^p A$ formée des tenseurs symétriques. 439

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 $\eta : a_1 \otimes \cdots \otimes a_p \mapsto a_1 \cdot a_2 \cdots a_p$ de $\bigotimes_k^p A$ dans A . On a donc, si N est l'opérateur de symétrisation

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

Autrement dit, η s'annule sur le sous-espace $N(\bigotimes_k^p A)$ 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 $N(\bigotimes_k^p A)$ est un idéal de $\Sigma^p A$.

Nous noterons désormais $U^{[p/S]}$ le spectre premier de l'algèbre $\Sigma^p A / N(\bigotimes_k^p A)$. Ce spectre est un sous-schéma fermé de $\Sigma^p(U) = V^p(U)$ et la réunion des $U^{[p/S]}$ est un sous-schéma fermé $X^{[p/S]}$ de $V^p(X)$.

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

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

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

440 **4.2.1.** — Les schémas $X^{[p/S]}$ et $X^{(p/S)}$ sont évidemment reliés : soient V un ouvert affine de S d'anneau affine k 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 k , $X^{(p/S)}$ a alors $k_\pi \otimes A$ pour algèbre affine. On vérifie en outre que l'application $\lambda \otimes a \mapsto (\lambda a \otimes \cdots \otimes a \pmod{N(\otimes^p A)})$ définit un homomorphisme de k -algèbres de $A \otimes_\pi k$ dans $\Sigma^p A / N(\otimes^p A)$; cet homomorphisme induit un morphisme $\varphi(U) : U^{[p/S]} \rightarrow U^{(p/S)}$ tel que $\varphi(U) \circ F'(U/S) = F(U/S)$.

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

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

Par exemple, si X est le sous-schéma de S défini par un Idéal quasi-cohérent $\mathcal{I}$, $F^{[p]}(X/S)$ s'identifie au morphisme identique de X , de sorte que $\varphi(X)$ est l'immersion canonique de $\text{Spec}(\mathcal{O}_S/\mathcal{I})$ dans $\text{Spec}(\mathcal{O}_S/\mathcal{I}^{[p]})$. On voit ainsi que $\varphi(X)$ n'est pas un isomorphisme en général. Toutefois, lorsque M est un k -module libre, il est clair que l'application $\lambda \otimes m \mapsto (\lambda m \otimes \cdots \otimes m \pmod{N(\otimes_k^p M)})$ de $k_\pi \otimes M$ dans $\Sigma^p M / N(\otimes_k^p M)$ est bijective ; cette application reste donc bijective lorsque M est k -plat, parce que tout module plat est une limite inductive filtrante de modules libres (LAZARD ^(*)). Il s'ensuit que $\varphi(X) : X^{[p/S]} \rightarrow X^{(p/S)}$ est un isomorphisme lorsque X est un S -schéma plat.

4.3. — Considérons enfin un S -schéma en groupes abéliens G . Alors, le morphisme composé $\mu(G) : U^p(G) \xrightarrow{\text{incl.}} G_S^p \rightarrow G$, qui est défini par la multiplication, se factorise

(*)D. LAZARD GR. Acad. Sc. Paris 258, 1964, p. 6313-6316.

à travers $V^p(G)$, de sorte qu'on a le diagramme commutatif suivant :

$$\begin{array}{ccccc}
 G & \xleftarrow{\mu(G)} & U^p(G) & \xleftarrow{\delta(G)} & G \\
 \downarrow \nu(G) & & \downarrow q'(G) & & \downarrow F^{[p]}(G/S) \\
 & & V^p(G) & \xleftarrow{i(G)} & G^{[p/S]} \\
 \downarrow \text{Ver}(G/S) & & & & \downarrow \varphi(G) \\
 & & & & G^{(p/S)}
 \end{array}$$

. Fr(G/S)

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

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

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

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

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

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

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

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

Lorsque E est un $\mathcal{O}_S$ -Module plat et que G est le S -groupe $\mathbb{V}(\mathcal{E})$, le morphisme 442
 $\text{Ver}(G/S)$ est nul ainsi que $p \cdot \text{id}_G$. 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

$$G^{(p^n)} \xrightarrow{\text{Ver}(G^{(p^{n-1})}/S)} G^{(p^{n-1})} \dots G^{(p)} \xrightarrow{\text{Ver}(G/S)} G$$

est nul pour un certain n (on a posé $G^{(p^n)} = (G^{(p^{n-1})})^{(p)}$).

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

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

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

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

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

$$\begin{array}{ccccc} \mathcal{A} & \xrightarrow{\Delta^p(\mathcal{A})} & \bigotimes_{\mathcal{O}_S}^p \mathcal{A} & \xrightarrow{m^p(\mathcal{A})} & \mathcal{A} \\ & \searrow a(\mathcal{A}) & \nearrow i(\mathcal{A}) & \searrow q(\mathcal{A}) & \nearrow b(\mathcal{A}) \\ & & \Sigma^p \mathcal{A} & & \mathcal{S}^p(\mathcal{A}) \\ & & \searrow r(\mathcal{A}) & \nearrow j(\mathcal{A}) & \\ & & \mathcal{A} \otimes_{\pi} \mathcal{O}_S & & \end{array}.$$

($\mathcal{A}$)

443 où les différentes lettres ont les significations suivantes : $m^p(A)$ est induit par la multiplication de A ; le morphisme $\Delta^p(A)$ est associé au morphisme $\mu(G)$ dont il est question plus haut (il est donc défini par le morphisme diagonal de la Coalgèbre A) ; on désigne par $\Sigma^p A$ la sous-Algèbre de $\bigotimes_{\mathcal{O}_S}^p A$ formée des sections invariantes sous l'action du groupe symétrique, par $i(A)$ l'inclusion de $\Sigma^p A$ dans le produit tensoriel ; de même, $\mathcal{S}^p(A)$ est la composante de degré p de l'algèbre symétrique de A et $q(A)$ est la projection canonique. Comme $\Sigma^p A$ est l'algèbre affine de $V^p(A)$ avec les notations ci-dessus, le morphisme composé $i(G) \circ \varphi(G)^{-1}$ induit un homomorphisme d'Algèbres $r(A)$; cet homomorphisme s'annule sur les sections de la forme

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

et envoie $x \otimes \cdots \otimes x$ sur $1 \otimes x$. De même, $j(A)$ est le morphisme de $\mathcal{O}_S$ -Modules $1 \otimes x \mapsto q(x \otimes \cdots \otimes x)$. Le composé $r(A) \circ a(A)$ est donc associé au morphisme Verschiebung $\text{Ver}(G/S)$, tandis que $b(A) \circ j(A)$ est associé au morphisme de Frobenius $\text{Fr}(G/S)$ ($a(A)$ et $b(A)$ sont tels que $i(A) \circ a(A) = \Delta^p(A)$ et $b(A) \circ q(A) = m^p(A)$).

Le diagramme commutatif (A) ci-dessus est autodual ; soit en effet D le foncteur qui associe à tout $\mathcal{O}_S$ -Module M le $\mathcal{O}_S$ -Module dual $\mathcal{H}om_{\mathcal{O}_S}(M, \mathcal{O}_S)$; il est clair que l'image de (A) par le foncteur D n'est autre que le diagramme (DA), les morphismes $Dr(A)$, $Da(A)$, $Dj(A)$ et $Db(A)$ s'identifiant respectivement à $j(DA)$, $b(DA)$, $r(DA)$ et $a(DA)$. On voit donc que *la dualité de Cartier (3.3.1) échange morphisme de Frobenius et Verschiebung.*

5. p -Algèbres de Lie

444

Rappelons d'abord quelques résultats du Séminaire Sophus Lie :

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 $ab = L_a(b) = R_b(a)$. On a alors :

$$(\operatorname{ad} x^p)(y) = [x^p, y] = (L_x^p - R_x^p)(y) = (L_x - R_x)^p(y) = (\operatorname{ad} x)^p(y)$$

d'où la *première formule de Jacobson*

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

De même, si $a_1, \dots, a_p$ sont p éléments arbitraires de A on a (confer 4.2) :

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

où σ parcourt les permutations de p lettres et τ celles de $(p-1)$ lettres. Le deuxième membre vaut en effet

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

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 $(-1)^s a_{\tau(i_1)} \dots a_{\tau(i_r)} a_p a_{\tau(j_s)} \dots a_{\tau(j_1)}$ vaut évidemment

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

où ρ parcourt les permutations de $p-1$ lettres. Les égalités

445

$$(x-1)^p = x^p - 1 = (x-1)(x^{p-1} + \dots + 1) \quad \text{et} \quad (x-1)^{p-1} = x^{p-1} + \dots + 1$$

montrent d'autre part que $(-1)^s \binom{p-1}{s}$ est égal à 1 en caractéristique p , ce qui prouve (*).

En particulier, si x_0 et x_1 sont deux éléments de A , on a

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

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

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

d'où la *deuxième formule de Jacobson*

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

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

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

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

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

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

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

Par exemple, si A est une R -algèbre, nous avons vu en 5.1 qu'on obtenait une p -algèbre de Lie $A_{\mathfrak{g}}$ en prenant le R -module sous-jacent à A et en posant

$$[x, y] = xy - yx \quad , \quad x^{(p)} = x^p \quad , \quad x, y \in A$$

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

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

$$D(\lambda \cdot s) = \lambda \cdot D(s) \quad \text{et} \quad D(s \cdot t) = (Ds)t + s(Dt)$$

lorsque λ parcourt les sections de $\mathcal{O}_S$, s et t les sections de $\mathcal{O}_X$ sur des ouverts tels que les formules aient un sens. La formule de Leibniz

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

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 $\text{Dér}_{X/S}$ des dérivations de X sur S est une p -sous-algèbre de Lie de l'algèbre sur $\Gamma(S, \mathcal{O}_S)$ des opérateurs différentiels de X sur S .

5.2.1. — Si $\mathfrak{g}$ et $\mathfrak{h}$ sont deux p -algèbres de Lie, un homomorphisme $h : \mathfrak{g} \rightarrow \mathfrak{h}$ est une application R -linéaire de $\mathfrak{g}$ dans $\mathfrak{h}$ telle que $h([x, y]) = [h(x), h(y)]$ et $h(x^{(p)}) = h(x)^{(p)}$ si $x, y \in \mathfrak{g}$. L'application composée de deux homomorphismes est encore un homomorphisme, de sorte que nous pourrions parler de la catégorie des p -algèbres de Lie sur R . De même, si $(X, \mathcal{R})$ est un espace annelé, nous dirons qu'un $\mathcal{R}$ -Module $\mathfrak{g}$ est muni d'une structure de p -Algèbre de Lie sur $\mathcal{R}$ si, pour tout ouvert U , $\Gamma(U, \mathfrak{g})$

est muni d'une structure de p -algèbre de Lie sur $\Gamma(U, \mathcal{R})$ et si les restrictions sont des homomorphismes.

5.3. — Nous nous intéressons maintenant au foncteur adjoint à gauche du foncteur $A \mapsto A_{\mathfrak{g}}$ de 5.2 : soient $\mathfrak{g}$ une p -algèbre de Lie sur l'anneau R de caractéristique p , $U(\mathfrak{g})$ l'algèbre enveloppante de l'algèbre de Lie sous-jacente à $\mathfrak{g}$ (cf. Bourbaki, algèbre de Lie, § 2) et $i_{\mathfrak{g}}$ ou $i : \mathfrak{g} \rightarrow U(\mathfrak{g})$ l'application canonique. On sait que tout homomorphisme d'algèbres de Lie h de $\mathfrak{g}$ dans l'algèbre de Lie sous-jacente à une R -algèbre unitaire A , se prolonge d'une manière et d'une seule en un homomorphisme de R -algèbres unitaires g de $U(\mathfrak{g})$ dans A ($gi = h$). En outre, h est un homomorphisme de p -algèbres de Lie si et seulement si g s'annule sur les éléments $i(x)^p - i(x^{(p)})$, lorsque x parcourt $\mathfrak{g}$. Par conséquent, si $U_p^R(\mathfrak{g})$ ou $U_p(\mathfrak{g})$ désigne le quotient de $U(\mathfrak{g})$ par l'idéal bilatère engendré par les éléments $i(x)^p - i(x^{(p)})$, et si $j_{\mathfrak{g}}$ ou $j : \mathfrak{g} \rightarrow U_p(\mathfrak{g})$ est l'application composée de $i : \mathfrak{g} \rightarrow U(\mathfrak{g})$ et de l'application canonique de $U(\mathfrak{g})$ dans $U_p(\mathfrak{g})$, on voit que tout homomorphisme de p -algèbres de Lie de $\mathfrak{g}$ dans $A_{\mathfrak{g}}$ se prolonge d'une manière et d'une seule en un homomorphisme d'algèbres unitaires $g : U_p(\mathfrak{g}) \rightarrow A$ ($gj = h$).

On dit que $U_p(\mathfrak{g})$ est l'algèbre enveloppante restreinte de $\mathfrak{g}$.

5.3.1. — Avec les notations de 5.3, posons maintenant $\underline{p}(x) = i(x)^p - i(x^{(p)})$. Pour tout élément y de $\mathfrak{g}$, on a

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

de sorte que $\underline{p}(x)$ appartient au centre de $U(\mathfrak{g})$; en particulier, l'idéal à gauche engendré par les éléments $\underline{p}(x)$ est déjà bilatère. De plus, on a $\underline{p}(\lambda x) = \lambda^p \underline{p}(x)$ et $\underline{p}(x + y) = \underline{p}(x) + \underline{p}(y)$, si $\lambda \in R$ et $x, y \in \mathfrak{g}$; en particulier, si (x_{α}) est une famille de générateurs du R -module $\mathfrak{g}$, l'idéal à gauche engendré par les éléments $\underline{p}(x)$ est déjà engendré par les $\underline{p}(x_{\alpha})$. 448

5.3.2. — Lorsque $\mathfrak{g}$ est une R -algèbre de Lie dont le R -module sous-jacent est libre de base (x_{α}) , on peut définir comme suit une structure de p -algèbre de Lie sur $\mathfrak{g}$: identifions $\mathfrak{g}$ à un sous-module de $U(\mathfrak{g})$ au moyen de i (Bourbaki, Alg. de Lie, I, § 2.7) et soit π l'application $r \mapsto r^p$ de R dans R . Si (y_{α}) est une famille quelconque d'éléments de $\mathfrak{g}$ tels que $\text{ad } y_{\alpha} = (\text{ad } x_{\alpha})^p$, il existe alors une application R -linéaire $\underline{q}$ de $R \otimes_{\pi} \mathfrak{g}$ dans $U(\mathfrak{g})$ qui envoie $1 \otimes x_{\alpha}$ sur $x_{\alpha}^p - y_{\alpha}$; de plus, comme on a

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

pour tout $x \in \mathfrak{g}$, $\underline{q}$ applique $\mathfrak{g}^{(p)}$ dans le centre de $U(\mathfrak{g})$.

Posant alors $x^{\{p\}} = x^p - \underline{q}(1 \otimes x)$ pour tout $x \in \mathfrak{g}$, on vérifie sans peine que $x^{\{p\}}$ appartient à $\mathfrak{g}$ et que l'application $x \mapsto x^{\{p\}}$ fait de $\mathfrak{g}$ une p -algèbre de Lie. Autrement dit, si (x_{α}) est une base du module sous-jacent à une algèbre de Lie $\mathfrak{g}$ sur R , les structures de p -algèbre de Lie sur $\mathfrak{g}$ correspondent biunivoquement aux familles (y_{α}) de $\mathfrak{g}$ telles que $\text{ad } y_{\alpha} = (\text{ad } x_{\alpha})^p$.

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 $j : \mathfrak{g} \rightarrow U_p(\mathfrak{g})$ est injective et, si l'on pose $z_\alpha = j(x_\alpha)$, $U_p(\mathfrak{g})$ a pour base les monômes $\prod_\alpha z_\alpha^{n_\alpha}$ ($0 \leq n_\alpha < p$; les n_α sont supposés nuls hormis un nombre fini d'entre eux; on suppose la base totalement ordonnée et les produits effectués dans l'ordre croissant).

449 Soit en effet $n = (n_\alpha)$ une famille d'entiers naturels qui sont nuls hormis un nombre fini d'entre eux. Identifions $\mathfrak{g}$ à un sous-module de l'algèbre enveloppante $U(\mathfrak{g})$ au moyen de l'application canonique i ; posons $|n| = \sum_\alpha n_\alpha$, $x^n = \prod_\alpha x_\alpha^{n_\alpha}$ et soit U^r le sous-module de $U(\mathfrak{g})$ qui est engendré par les x^n tels que $|n| \leq r$. Posons enfin $s = |n|$, $n_\alpha = m_\alpha + p\ell_\alpha$, avec $0 \leq m_\alpha < p$, et $Tn = \prod_\alpha x_\alpha^{m_\alpha} \underline{p}(x_\alpha)^{\ell_\alpha}$ (confer 5.3.1). Il est clair que $Tn - \prod_\alpha x_\alpha^{n_\alpha}$ appartient à U^{s-1} . D'après le théorème de Poincaré-Birkhoff-Witt, les Tn tels que $|n| = s$ forment donc une base de U^s modulo U^{s-1} . Lorsque $s = |n|$ varie, les Tn forment une base de $U(\mathfrak{g})$. Or le noyau J de l'application canonique de $U(\mathfrak{g})$ dans $U_p(\mathfrak{g})$ est l'idéal à gauche de $U(\mathfrak{g})$ qui est engendré par les éléments centraux $\underline{p}(x_\alpha)$ (5.3.1); par conséquent, les Tn tels que $\ell = (\ell_\alpha) \neq 0$ forment une base de J ; les Tn , tels que $n_\alpha < p$ pour tout α , forment une base de $U(\mathfrak{g})$ modulo J , cqfd

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

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

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

L'unicité de la structure de p -algèbre de Lie de $R' \otimes_R \mathfrak{g}$ étant claire, prouvons l'existence : lorsque $\mathfrak{g}$ est libre de base (x_α) il existe d'après 5.3.1 une et une seule structure de p -algèbre de Lie sur l'algèbre de Lie $R' \otimes_R \mathfrak{g}$ telle que $(1 \otimes x_\alpha)^{(p)} = 1 \otimes (x_\alpha^{(p)})$; cette structure est celle que nous cherchons.

450 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 $q_0 : L_0 \rightarrow \mathfrak{g}$; il suffit par exemple de prendre pour L_0 la p -algèbre de Lie $R \otimes_{\mathbb{F}_p} \mathfrak{g}$, où $\mathbb{F}_p$ désigne le corps premier de caractéristique p , pour q_0 l'homomorphisme $\lambda \otimes x \mapsto \lambda \cdot x$ ($\mathfrak{g}$ 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 pour 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 $q_1 : L_1 \rightarrow L_0$ dont l'image est $\text{Ker } q_0$:

$$L_1 \xrightarrow{q_1} L_0 \xrightarrow{q_0} \mathfrak{g} \longrightarrow 0.$$

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

$$R' \otimes_R L_1 \xrightarrow{R' \otimes_R q_1} R' \otimes_R L_0 \xrightarrow{R' \otimes_R q_0} R' \otimes_R \mathfrak{g} \longrightarrow 0.$$

Comme $R' \otimes_R q_1$ est manifestement un homomorphisme de p -algèbres de Lie, le noyau de $R' \otimes_R q_0$ est un p -idéal, de sorte que l'opération puissance p -ième symbolique de $R' \otimes_R L_0$ induit par passage au quotient une application de $R' \otimes_R \mathfrak{g}$ dans $R' \otimes_R \mathfrak{g}$

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

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

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

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

En particulier, si r est un élément de R et si R' est l'anneau localisé R_r , on voit que $\mathfrak{g}_r \simeq R_r \otimes_R \mathfrak{g}$ est muni canoniquement d'une structure de p -algèbre de Lie sur R_r , de sorte que le faisceau $\tilde{\mathfrak{g}}$ sur $\text{Spec } R$ est une p -Algèbre de Lie quasi-cohérente sur $\text{Spec } R$. De plus, l'algèbre enveloppante restreinte $U_p^{R_r}(\mathfrak{g}_r)$ s'identifie à $U_p^R(\mathfrak{g})_r$ de sorte que le faisceau associé au préfaisceau $V \mapsto U_p(\Gamma(V, \tilde{\mathfrak{g}}))$ est quasi-cohérent. Plus généralement, si S est un schéma de caractéristique p et $\mathcal{G}$ une p -Algèbre de Lie quasi-cohérente sur $\mathcal{O}_S$, le faisceau associé au préfaisceau $V \mapsto U_p(\Gamma(V, \mathcal{G}))$ est quasi-cohérent ; il sera noté $\mathcal{U}_p(\mathcal{G})$ et appelé *l'Algèbre enveloppante restreinte de $\mathcal{G}$* . Si V est affine, $U_p(\Gamma(V, \mathcal{G}))$ s'identifie à l'ensemble des sections de $\mathcal{U}_p(\mathcal{G})$ sur V . 451

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

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

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

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

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

Si $h_1 : \mathfrak{f} \rightarrow \mathfrak{k}$ et $h_2 : \mathfrak{g} \rightarrow \mathfrak{k}$ sont deux homomorphismes de p -algèbres de Lie tels que $[h_1(x), h_2(y)] = 0$ pour tout x de $\mathfrak{f}$ et tout y de $\mathfrak{g}$, l'application $h_1 + h_2 : (x, y) \rightarrow h_1(x) + h_2(y)$ 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 $h_1 : x \mapsto i_{\mathfrak{f}}(x) \otimes 1$ et $h_2 : y \mapsto 1 \otimes i_{\mathfrak{g}}(y)$ induisent un homomorphisme $h_1 + h_2$ de $\mathfrak{f} \times \mathfrak{g}$ dans la p -algèbre de Lie sous-jacente à $U_p(\mathfrak{f}) \otimes U_p(\mathfrak{g})$. Il résulte des caractères universels de $\mathfrak{f} \times \mathfrak{g}$ et des 452

algèbres enveloppantes restreintes que $h_1 + h_2$ se prolonge en un isomorphisme φ de $U_p(\mathfrak{f} \times \mathfrak{g})$ sur le produit tensoriel $U_p(\mathfrak{f}) \otimes U_p(\mathfrak{g})$.

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 $U_p(\mathfrak{g})$ dans $U_p(\mathfrak{g} \times \mathfrak{g})$. Nous noterons $\Delta_{\mathfrak{g}}$ le composé de cet homomorphisme avec φ ; on voit facilement que $\Delta_{\mathfrak{g}}$ et la multiplication de l'algèbre $U_p(\mathfrak{g})$ font de $U_p(\mathfrak{g})$ 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 schéma de caractéristique p et $\mathcal{G}$ une $\mathcal{O}_S$ - p -Algèbre de Lie. Lorsque V parcourt les ouverts de S , les structures de coalgèbres en groupes définies précédemment sur les ensembles $U_p(\Gamma(V, \mathcal{G}))$ induisent sur l'algèbre enveloppante restreinte $\mathcal{U}_p(\mathcal{G})$ une structure de $\mathcal{O}_S$ - p -Coalgèbre en groupes. D'après 5.3.1, le S -foncteur en groupes correspondant $\text{Spec}^* \mathcal{U}_p(\mathcal{G})$ associe à tout S -schéma T l'ensemble des sections x de $\mathcal{U}_p(\mathcal{G} \otimes_{\mathcal{O}_S} \mathcal{O}_T)$ telles que

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

Ici ε désigne l'augmentation de $\mathcal{U}_p(\mathcal{G} \otimes_{\mathcal{O}_S} \mathcal{O}_T)$, Δ le morphisme diagonal, et $x \otimes x$ l'image canonique de (x, x) dans $\Gamma(T, \mathcal{U}_p(\mathcal{G}_T) \otimes_{\mathcal{O}_T} \mathcal{U}_p(\mathcal{G}_T))$.

Lorsque $\mathcal{G}$ est localement libre de type fini en tant que $\mathcal{O}_S$ -Module, $\text{Spec}^* \mathcal{U}_p(\mathcal{G})$ est représentable par un S -schéma fini, localement libre (5.3.3 et 3.1.2).

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

453

Soit S un schéma de caractéristique $p > 0$. Au paragraphe 5 nous avons associé à toute $\mathcal{O}_S$ - p -Algèbre de Lie quasi-cohérente $\mathcal{G}$ un S -foncteur en groupes $\text{Spec}^* \mathcal{U}_p(\mathcal{G})$. Nous allons voir maintenant que, pour tout S -schéma en groupes G , l'Algèbre de Lie $\underline{\text{Lie}}(G/S)$ définie en II 4.11 est munie naturellement d'une structure de $\mathbf{O}_S$ - p -algèbre de Lie.

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

D'autre part, d'après II 4.1.4, l'image de $L = \underline{\text{Lie}}(G/S)(S)$ par la translation à droite $r : U(G) \rightarrow \text{Dif}_{G/S}$ 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 $\underline{\text{Lie}}(G/S)(S)$, qui est donc une sous- p -algèbre de Lie de l'algèbre infinitésimale $U(G)$.

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

De même, si $s : T \rightarrow S$ est un changement de base, l'application de $\underline{\text{Lie}}(G/S)(S)$ dans $\underline{\text{Lie}}(G/S)(T)$, qui est induite par s , est un homomorphisme de p -algèbres de Lie.

On peut traduire cela en disant que le foncteur $\underline{\text{Lie}}(G/S)$ est muni d'une structure de $\mathbf{O}_S$ - p -algèbre de Lie. En particulier, lorsque T parcourt les ouverts de S , on voit que le faisceau $\mathcal{L}ie(G/S)$ est muni d'une structure de $\mathcal{O}_S$ - p -algèbre de Lie. 454

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

Soit D une dérivation de G à l'origine, c'est-à-dire la déviation de l'origine obtenue en composant la déviation canonique $\delta : S \rightarrow I_S$ de 1.5 avec un prolongement x à I_S de la section unité $\varepsilon : S \rightarrow G$. D'après la définition que nous avons donnée en 2.1, D^p est la déviation composée suivante

$$S \simeq \underbrace{S \times S \times \cdots \times S}_p \xrightarrow{\delta \times \cdots \times \delta} I_S \times \cdots \times I_S \xrightarrow{x \times \cdots \times x} G \times \cdots \times G \xrightarrow{m^{(p)}} G$$

où $m^{(p)}$ est le morphisme induit par la multiplication $m : G \times G \rightarrow G$. Comme $I_S \times \cdots \times I_S$ est affine sur S et a pour Algèbre affine $\mathcal{O}_S[d_1, \dots, d_p]/(d_1^2, \dots, d_p^2)$, la déviation $\delta \times \cdots \times \delta$ est définie par un morphisme de $\mathcal{O}_S$ -Modules

$$\mathcal{O}_S[d_1, \dots, d_p]/(d_1^2, \dots, d_p^2) \longrightarrow \mathcal{O}_S$$

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 I_S^p sur le i -ième facteur et si x_i est l'image de x dans $G(I_S^p)$ par $G(\text{pr}_i)$, le morphisme composé $m^{(p)} \circ (x \times \cdots \times x)$ n'est autre que le produit $x_1 x_2 \cdots x_p$. Par conséquent, D^p est aussi la déviation composée suivante

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

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

Le produit symétrique $\Sigma^p I_S$ a pour Algèbre affine une sous-Algèbre A de $\mathcal{O}_S[d_1, \dots, d_p]/(d_1^2, \dots, d_p^2)$ qui a pour base sur $\mathcal{O}_S$ 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 A dans $\mathcal{O}_S[d]/(d^2)$ qui annule $\sigma_1, \dots, \sigma_{p-1}$ et envoie σ_p sur d , par i l'immersion fermée de I_S dans $\Sigma^p I_S$ qui est associée à q . On a alors un diagramme commutatif :

$$\begin{array}{ccccc} & & D^p & & \\ & \curvearrowright & & \curvearrowright & \\ S & \xrightarrow{\delta \times \cdots \times \delta} & I_S^p & \xrightarrow{x_1 \cdots x_p} & G \\ \delta \downarrow & & \downarrow \text{can.} & & \parallel \\ I_S & \xrightarrow{i} & \Sigma^p I_S & \xrightarrow{\quad} & G \\ & \curvearrowright & & \curvearrowright & \\ & & y & & \end{array}$$

qui montre que D^p est de la forme $y \circ \delta$, cqfd

6.3. — Soient $\mathcal{S}_p$ le groupe symétrique d'ordre p et $I_S^p \times \mathcal{S}_p$ la somme directe d'une famille d'exemplaires de I_S^p indexés par $\mathcal{S}_p$. Nous notons $\pi : I_S^p \times \mathcal{S}_p \rightarrow I_S^p$ la projection canonique et $k : I_S^p \times \mathcal{S}_p \rightarrow I_S^p$ le morphisme définissant l'opération de $\mathcal{S}_p$ sur I_S^p (si σ est un élément de $\mathcal{S}_p$, la restriction de k à $I_S^p \times \sigma$ a pour j -ième composante pr_{σ_j}). Ceci étant, nous disons qu'un foncteur $X : (\mathbf{Sch}/S)^\circ \rightarrow (\mathbf{Ens})$ vérifie la condition (F) si X transforme les sommes directes finies en produits directs et si, pour tout S -schéma T , la suite

$$X(T \times_S \Sigma^p I_S) \longrightarrow X(T \times_S I_S^p) \xrightleftharpoons[X(T \times_S k)]{X(T \times_S \pi)} X(T \times_S I_S^p \times \mathcal{S}_p)$$

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

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

$$\begin{array}{ccc} I_S^p & \xrightarrow{x_1 \cdots x_p} & X \\ & \searrow \text{can.} \quad \nearrow \tau & \\ & \Sigma^p I_S & \end{array}$$

et définit par composition un morphisme

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

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

L'endomorphisme $x \mapsto x^{(p)}$ de $\underline{\text{Lie}}(G/S)(S)$ 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 $\underline{\text{Lie}}(G/S)(S)$ 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 :

6.4.1. — Soient M un groupe abélien « abstrait » et $D_S(M)$ le S -groupe diagonalisable de type M (I 4.4.2). Pour tout S -schéma T , on a donc $D_S(M)(T) = \text{Hom}_{(\text{Ab})}(M, \mathbf{O}(T)^*)$. Soit x un élément de $\underline{\text{Lie}}(D_S(M)/S)(S)$, c'est-à-dire un homomorphisme de groupes abéliens

$$M \xrightarrow{x} \Gamma(S, \mathcal{O}_S + d\mathcal{O}_S)^*$$

de la forme $m \mapsto 1 + d\xi(m)$, où $\xi \in \text{Hom}_{(\text{Ab})}(M, \mathbf{O}(S))$. Avec les notations de 6.2 et 6.3, le produit $x_1 \cdots x_p$ associé 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 $\mathbf{O}(\Sigma^p \mathbf{I}_S)$. Projetant l'Algèbre affine A de $\Sigma^p \mathbf{I}_S$ dans $\mathcal{O}_S[d]/(d^2)$ en annulant $\sigma_1, \dots, \sigma_{p-1}$ et en envoyant σ_p sur d , on voit que $x^{(p)}$ est l'homomorphisme

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

de M dans $\Gamma(S, \mathcal{O}_S + d\mathcal{O}_S)$.

En résumé, si l'on identifie $\underline{\text{Lie}}(\mathbf{D}_S(M)/S)(S)$ à $\text{Hom}_{(\text{Ab})}(M, \mathbf{O}(S)^*)$ comme en 5.1, la puissance p -ième symbolique associée à ξ l'homomorphisme $\xi^{(p)} : m \mapsto \xi(m)^p$.

6.4.2. — Soient $\mathcal{F}$ un $\mathcal{O}_S$ -Module et G le S -foncteur en groupes abéliens $\mathbf{W}(\mathcal{F})$ (cf. I 458 4.6). Soient y un élément de $\mathbf{W}(\mathcal{F})(S) = \Gamma(S, \mathcal{F})$ et y' l'image canonique de y dans $\mathbf{W}(\mathcal{F})(\mathbf{I}_S)$. On sait que l'application $y \mapsto dy'$ est une bijection de $\mathbf{W}(\mathcal{F})(S)$ sur $\underline{\text{Lie}}(\mathbf{W}(\mathcal{F})/S)(S)$. Si l'on pose $x = dy'$, la quantité x_i de 6.2 n'est autre que $d_i y''$, où y'' désigne l'image canonique de x dans $\mathbf{W}(\mathcal{F})(\mathbf{I}_S^p)$. Par conséquent le produit $x_1 \cdots x_p$ est égal à $(d_1 + \cdots + d_p)y''$ et appartient à $\mathbf{W}(\mathcal{F})(\Sigma^p \mathbf{I}_S)$. Comme l'application de $\mathbf{O}(\Sigma^p \mathbf{I}_S)$ dans $\mathbf{O}(\mathbf{I}_S)$, qui définit le morphisme i de 6.1, annule $d_1 + \cdots + d_p$, on voit que $x^{(p)}$ est nul.

Pour tout $\mathcal{O}_S$ -Module $\mathcal{F}$, l'opération puissance p -ième symbolique dans l'algèbre de Lie de $\mathbf{W}(\mathcal{F})$ est donc nulle.

6.4.3. — Soient X un S -schéma, G le S -foncteur en groupes $\underline{\text{Aut}}_S X$ et D une S -dérivation du faisceau structural $\mathcal{O}_X$. D'après 6.1, D peut être identifié à un $\mathbf{I}_S$ -automorphisme x de $X_{\mathbf{I}_S}$ qu'on peut décrire comme suit : si s est une section de $\mathcal{O}_S[d]/(d^2)$ de la forme $a + db$, posons $\mathbf{D}_{\mathbf{I}_S} s = Da + d(Db)$; autrement dit, $\mathbf{D}_{\mathbf{I}_S}$ est déduit de D par le changement de base $\mathbf{I}_S \rightarrow S$; l'automorphisme en question de $X_{\mathbf{I}_S}$ est alors associé à l'endomorphisme $s \mapsto s + d(\mathbf{D}_{\mathbf{I}_S} s)$ de $\mathcal{O}_S[d]/(d^2)$.

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

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

c'est-à-dire à $1 + \sigma_1 \mathbf{D}_{\mathbf{I}_S^p} + \sigma_2 (\mathbf{D}_{\mathbf{I}_S^p})^2 + \cdots + \sigma_p (\mathbf{D}_{\mathbf{I}_S^p})^p$.

459

Le coefficient de σ_p est $(\mathbf{D}_{\mathbf{I}_S^p})^p$, ce qui signifie que la bijection $D \mapsto x$ de l'algèbre de Lie des S -dérivations de $\mathcal{O}_X$ sur l'algèbre de Lie de $\underline{\text{Aut}}_S X$ est un isomorphisme de p -algèbres de Lie.

6.4.4. — En utilisant la même méthode, on voit que, pour tout $\mathcal{O}_S$ -Module $\mathcal{F}$, la bijection décrite en II 4.5 est un isomorphisme de p -algèbres de Lie de $\text{End}_{\mathbf{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})$ sur $\underline{\text{Lie}}(\underline{\text{Aut}}_{\mathbf{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})/S)(S)$.

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

460

7. Groupes radiciels de hauteur 1

Soit S un schéma de caractéristique $p > 0$. Nous dirons qu'une $\mathcal{O}_S$ -Algèbre $\mathcal{A}$ (resp. une $\mathcal{O}_S$ - p -algèbre de Lie $\mathcal{L}$) est *finie localement libre* si le $\mathcal{O}_S$ -Module sous-jacent à $\mathcal{A}$ (resp. $\mathcal{L}$) est localement libre et de type fini. Si $\mathcal{L}$ est une $\mathcal{O}_S$ - p -algèbre de Lie finie localement libre, nous savons que le S -foncteur en groupes

$$G_p(\mathcal{L}) = \text{Spec}^* \mathcal{U}_p(\mathcal{L})$$

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

7.1. — Considérons d'abord une $\mathcal{O}_S$ - p -Algèbre de Lie quasi-cohérente $\mathcal{L}$. Lorsque V parcourt les ouverts de S , les applications $j : \Gamma(V, \mathcal{L}) \rightarrow U_p(\Gamma(V, \mathcal{L}))$ de 5.3 définissent un morphisme $\underline{j} : \mathcal{L} \rightarrow \mathcal{U}_p(\mathcal{L})$. D'autre part, d'après 3.2.3, la $\mathcal{O}_S$ -Algèbre de Lie du S -foncteur en groupes $G_p(\mathcal{L})$ est le noyau du morphisme

$$\Delta - \text{in}_1 - \text{in}_2 : \mathcal{U}_p(\mathcal{L}) \longrightarrow \mathcal{U}_p(\mathcal{L}) \otimes_{\mathcal{O}_S} \mathcal{U}_p(\mathcal{L}),$$

où Δ désigne le morphisme diagonal et où in_1, in_2 sont les injections $x \mapsto x \otimes 1$ et $x \mapsto 1 \otimes x$. Il est clair que l'image de $\underline{j}$ est contenue dans le noyau $\text{Lie } G_p(\mathcal{L})$ de $\Delta - \text{in}_1 - \text{in}_2$; c'est pourquoi nous noterons $\underline{j}_{\mathcal{L}} : \mathcal{L} \rightarrow \underline{\text{Lie}} G_p(\mathcal{L})$ le morphisme de $\mathcal{O}_S$ - p -Algèbres de Lie qui est induit par $\underline{j}$ (6.4.4).

Considérons maintenant un très bon S -foncteur en groupes G vérifiant la condition (F) de 6.3 et soit $h : G_p(\mathcal{L}) \rightarrow G$ un homomorphisme de S -foncteurs en groupes. D'après 6.3, le morphisme $\text{Lie } h : \text{Lie } G_p(\mathcal{L}) \rightarrow \text{Lie } G$ est un homomorphisme de $\mathcal{O}_S$ -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 $(\text{Lie } h) \circ \underline{j}_{\mathcal{L}}$. Si nous notons $\text{Hom}_p(\mathcal{L}, \text{Lie } G)$ l'ensemble des homomorphismes de $\mathcal{O}_S$ -Algèbres de Lie, qui sont compatibles avec l'élévation à la puissance p -ième symbolique, on a donc une application $J(\mathcal{L}, G) : h \mapsto (\text{Lie } h) \circ \underline{j}_{\mathcal{L}}$ de $\text{Hom}_{S\text{-gr.}}(G_p(\mathcal{L}), G)$ dans $\text{Hom}_p(\mathcal{L}, \underline{\text{Lie}} G)$.

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

$$J(\mathcal{L}, G) : \text{Hom}_{S\text{-gr.}}(G_p(\mathcal{L}), G) \longrightarrow \text{Hom}_p(\mathcal{L}, \text{Lie } G)$$

est bijective dans chacun des cas suivants :

- (i) G est un S -schéma en groupes ;
- (ii) G est de la forme $\underline{\text{Aut}}_S X$, où X est un S -schéma ;
- (iii) G est de l'une des formes $\mathbf{W}(\mathcal{F})$ ou $\underline{\text{Aut}}_{\mathcal{O}_S\text{-mod}} \mathbf{W}(\mathcal{F})$, où $\mathcal{F}$ désigne un $\mathcal{O}_S$ -Module quasi-cohérent.

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

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

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

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

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

où $b(\mathcal{A})$ et $j(\mathcal{A})$ sont définis comme en 4.3.3. Comme le $\mathcal{O}_S$ -Module dual de $\mathcal{S}^p \mathcal{A}$ n'est autre que le sous-Module $\Sigma^p \mathcal{U}$ de $\bigotimes^p \mathcal{U}$ 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 :

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

où $a(\mathcal{U})$ est induit par le morphisme $(\Delta \otimes \mathcal{U} \otimes \cdots \otimes \mathcal{U}) \cdots (\Delta \otimes \mathcal{U}) \Delta$ de $\mathcal{U}$ dans $\bigotimes^p \mathcal{U}$ (Δ est le morphisme diagonal de $\mathcal{U}$); de même, $r(\mathcal{U})$ 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 $\mathcal{I}$. Comme Φ^* est un homomorphisme d'Algèbres, il suffit de voir que Φ^* s'annule sur $\text{Im } \underline{j}_{\mathcal{L}}$. Ceci résulte de la formule $\Delta s = s \otimes 1 + 1 \otimes s$, lorsque $s \in \text{Im } \underline{j}_{\mathcal{L}}$.

7.2.1. — Posons $G_p = G_p(\mathcal{L})$. Nous allons d'abord prouver l'assertion (ii) du théorème 7.2 en conservant les notations ci-dessus. Comme tout élément de $\mathcal{I}$ a une puissance p -ième nulle et que $\mathcal{I}$ est un $\mathcal{O}_S$ -Module de type fini, $\mathcal{I}$ est localement nilpotent. On a donc $(G_p)_{\text{réd}} = S_{\text{réd}}$. Or les homomorphismes h de G_p dans $\underline{\text{Aut}} X$ correspondent biunivoquement aux opérations à gauche $h' : G_p \times X \rightarrow X$ 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 schémas 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 :

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

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

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

Dans ces formules, u désigne une section quelconque de $\mathcal{U}$ sur un ouvert affine V , x et y des sections de $\mathcal{C}$ sur V ; on désigne par $1_{\mathcal{C}}$ la section unité de $\mathcal{C}$, par ε et Δ l'augmentation et le morphisme diagonal de $\mathcal{U}$. Une opération h' de G à gauche sur X est définie par un homomorphisme d'Algèbres $\lambda : \mathcal{C} \rightarrow \mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{C}$. Nous noterons μ le morphisme composé

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

où γ est la « contraction » de $\mathcal{A}^* \otimes_{\mathcal{O}_S} \mathcal{A}$ dans $\mathcal{O}_S$. On sait que l'application $\lambda \mapsto (\gamma \otimes \mathcal{C})(\mathcal{U} \otimes \lambda)$ est une bijection de $\text{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{A} \otimes \mathcal{C})$ sur $\text{Hom}_{\mathcal{O}_S}(\mathcal{U} \otimes \mathcal{C}, \mathcal{C})$. 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 $\mathcal{U}$ dans le $\mathcal{O}_S$ -Module $\mathcal{C}$, les sections u de $\mathcal{U}$ qui vérifient les conditions du lemme précédent forment une sous-Algèbre de $\mathcal{U}$. 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 $\text{Im } j_{\mathcal{L}}$. Si u est une section de $\text{Im } j_{\mathcal{L}}$, ces conditions signifient que $u(1_{\mathcal{C}}) = 0$ et que $u(xy) = u(x)y + xu(y)$. Tout homomorphisme h de $G_p = G_p(\mathcal{L})$ dans $\underline{\text{Aut}} X$ définit donc un homomorphisme H de $\mathcal{U}$ dans $\text{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{C})$ qui envoie $\text{Im } j_{\mathcal{L}}$ dans l'ensemble des $\mathcal{O}_S$ -dérivations de $\mathcal{C}$. L'application $H \circ j_{\mathcal{L}}$ est un homomorphisme de p -Algèbres de Lie de $\mathcal{L}$ dans le faisceau $\text{Dér}_{X/S}$ des $\mathcal{O}_S$ -dérivations de $\mathcal{C}$. De plus, l'application $h \mapsto H \circ j_{\mathcal{L}}$ est évidemment bijective; il resterait à vérifier qu'en identifiant $\text{Dér}_{X/S}$ à $\underline{\text{Lie}}(\underline{\text{Aut}} X/S)$ comme en 2.5, on identifie l'application $h \mapsto H \circ j_{\mathcal{L}}$ 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 -schéma et x un élément de $G(T)$, nous notons ℓ_x^T (resp. r_x^T) la translation à gauche (resp. à droite) de G_T qui est définie par x . Les applications $\ell_x^T : x \mapsto \ell_x^T$ déterminent donc un homomorphisme ℓ de G dans $\underline{\text{Aut}} G$. 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 $\underline{\text{Aut}} G$, donc aussi sur les foncteurs $T \mapsto \text{Hom}_{T\text{-Gr.}}(G_p(\mathcal{L}_T), \underline{\text{Aut}} G_T)$ et $T \mapsto \text{Hom}_p(\mathcal{L}_T, \underline{\text{Lie}}(\underline{\text{Aut}} G_T/T))$. D'autre part, l'homomorphisme ℓ induit des carrés commutatifs

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

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 $\underline{\text{Aut}}_{\mathcal{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})$ (le cas de $\mathbf{W}(\mathcal{F})$ est analogue). Posons $G_p = G_p(\mathcal{L})$. Un homomorphisme de G_p dans $\underline{\text{Aut}}_{\mathcal{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})$

est un homomorphisme multiplicatif de G_p dans $\underline{\text{End}}_{\mathcal{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})$ qui est compatible avec les sections unités de G_p et de $\underline{\text{End}}_{\mathcal{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})$. Or un morphisme de S -foncteurs $h : G_p \rightarrow \underline{\text{End}}_{\mathcal{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F})$ est par définition un endomorphisme de $\mathbf{W}(\mathcal{O}_{G_p} \otimes_{\mathcal{O}_S} \mathcal{F})$; d'après I 4.6.2 (ii), un tel endomorphisme est induit par un endomorphisme de $\mathcal{O}_{G_p} \otimes_{\mathcal{O}_S} \mathcal{F}$, c'est-à-dire par un endomorphisme $\mathcal{A}$ -linéaire du faisceau $\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{F}$, où $\mathcal{A}$ est la $\mathcal{O}_S$ -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 $\mathcal{O}_S$ -Modules de $\mathcal{F}$ dans $\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{F}$. Si l'on pose $\mu = (\gamma \otimes \mathcal{F})(\mathcal{U} \otimes \lambda)$ comme en 7.2.1, h est finalement déterminé par $\mu : \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{F} \rightarrow \mathcal{F}$. Les hypothèses faites sur h se traduisent en disant que μ définit une structure de $\mathcal{U}$ -Module sur $\mathcal{F}$. Une telle structure de Module est définie par un homomorphisme de p -Algèbres de Lie de $\mathcal{L}$ dans $\text{End}_{\mathcal{O}_S}(\mathcal{F})$, qui égale $\text{Lie}(\underline{\text{Aut}}_{\mathcal{O}_S\text{-mod.}} \mathbf{W}(\mathcal{F}))$.

7.3. Lemme. — *Si $\mathcal{L}$ est une $\mathcal{O}_S$ - p -algèbre de Lie finie localement libre, le morphisme $j_{\mathcal{L}} : \mathcal{L} \rightarrow \text{Lie } G_p(\mathcal{L})$ 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 $\mathcal{L}$ est le faisceau associé à une R - p -algèbre de Lie de base $x_1, \dots, x_r$. Nous pouvons alors utiliser les notations de 5.3.3 et poser $z^n = \prod_i z^{n_i}$ pour tout r -uplet $(n_1, \dots, n_r)$ formés d'entiers naturels tels que $0 \leq n_i < p$. Posant en outre $n! = \prod_i (n_i)!$ et munissant le monoïde $\mathbb{N}^r$ de l'ordre produit, on voit facilement qu'on a

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

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

7.4. — Pour terminer l'exposé, nous allons donner une caractérisation des S -schémas en groupes de la forme $G_p(\mathcal{L})$, où $\mathcal{L}$ est une $\mathcal{O}_S$ - p -Algèbre de Lie finie localement libre.

Soient G un S -schéma en groupes, ε_G la section unité et $\mathcal{I}$ le noyau du morphisme de $\varepsilon_G^{-1}(\mathcal{O}_G)$ dans $\mathcal{O}_S$ qui définit ε_G . L'image canonique de $\underline{\text{Lie}}(G/S)(S)$ dans $U(G)$ (2.5) s'identifie d'après 1.3 aux morphismes de $\mathcal{O}_S$ -Modules de $\varepsilon_G^{-1}(\mathcal{O}_G)$ dans $\mathcal{O}_S$ qui s'annulent sur la section unité de $\varepsilon_G^{-1}(\mathcal{O}_G)$ et sur $\mathcal{I}^2$. On retrouve ainsi l'isomorphisme canonique de $\underline{\text{Lie}}(G/S)(S)$ sur $\text{Hom}_{\mathcal{O}_S}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_S)$ de l'exposé II. Nous poserons d'ailleurs $\omega_{G/S} = \mathcal{I}/\mathcal{I}^2$ comme dans l'exposé II, de sorte que le faisceau $\text{Lie}(G/S)$ s'identifie à $\text{Hom}_{\mathcal{O}_S}(\omega_{G/S}, \mathcal{O}_S)$.

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

(i) *Il existe une $\mathcal{O}_S$ - p -Algèbre de Lie finie localement libre $\mathcal{L}$ telle que G soit isomorphe à $G_p(\mathcal{L})$.*

(ii) G est affine sur S ; $\omega_{G/S}$ est un $\mathcal{O}_S$ -Module localement libre de type fini et l'Algèbre affine de G est localement isomorphe au quotient de l'Algèbre symétrique $S_{\mathcal{O}_S}(\omega_{G/S})$ 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 ≤ 1 (4.1.3) et $\omega_{G/S}$ est localement libre. ^(*)

467 **7.4.1.** — L'implication (ii) $\Rightarrow$ (iii) étant claire, montrons d'abord que (i) entraîne (ii) : nous considérons pour cela la suite exacte

$$(*) \quad 0 \longrightarrow \mathcal{L} \xrightarrow{j_{\mathcal{L}}} \mathcal{I} \xrightarrow{\delta} \mathcal{I} \otimes_{\mathcal{O}_S} \mathcal{I},$$

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

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

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

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

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

Supposons maintenant S affine. Il y a alors une section $\sigma : \omega_{G/S} \rightarrow \mathcal{I}$ de la projection canonique de $\mathcal{I}$ sur $\mathcal{I}/\mathcal{I}^2$; une telle section induit (lemme 7.2) un homomorphisme d'algèbres $h : S_{\mathcal{O}_S}[\omega_{G/S}]/(x^p)_{x \in \omega_{G/S}} \rightarrow \mathcal{A}$. Si l'on filtre $\mathcal{A}$ (resp. $S_{\mathcal{O}_S}[\omega]/(x^p)_{x \in \omega}$) par les puissances de $\mathcal{I}$ (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 $\mathcal{O}_S$ -Modules localement libres de même rang; donc h est un isomorphisme.

468 **7.4.2.** — Montrons enfin que (iii) entraîne (i) : comme le morphisme de Frobenius 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-schéma fermé de G défini par un certain Idéal $\mathcal{I}$ de $\mathcal{O}_G$. Comme G est localement de présentation finie sur S et que toute section de $\mathcal{I}$ a une puissance p -ième nulle, $\mathcal{I}$ est localement nilpotent et G est affine sur S (EGA I, 5.1.9), donc fini sur S .

^(*) 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 .

Soit donc $\mathcal{A}$ la $\mathcal{O}_S$ -Algèbre affine de G ; posons $\mathcal{L} = \text{Lie}(G/S)$, $\mathcal{A}_p = \mathcal{U}_p(\mathcal{L})^*$ et soit $G_p = G_p(\mathcal{L})$ le spectre de $\mathcal{A}_p$. D'après le théorème 7.2, l'identité de $\mathcal{L}$ est définie par un homomorphisme de groupes $h : G_p(\mathcal{L}) \rightarrow G$, donc par un homomorphisme de $\mathcal{O}_S$ -Algèbres $a : \mathcal{A} \rightarrow \mathcal{A}_p$. Il s'agit de montrer que a , 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 $\mathcal{J}$ sur $\omega_{G/S}$. Comme toute section de $\mathcal{J}$ a une puissance p -ième nulle, τ induit un homomorphisme de $\mathcal{O}_S$ -Algèbres

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

Il est clair que b est un épimorphisme de $\mathcal{O}_S$ -Modules (confer 7.4.1). D'autre part, nous avons vu en 7.4.1 que ab est un isomorphisme. Il en va donc de même pour a , cqfd

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 S -schéma en groupes est algébrique si le schéma sous-jacent est de type fini sur S : d'après le théorème 7.2 le foncteur G_p , qui associe à toute k - p -algèbre de Lie $\mathcal{L}$ de dimension finie sur k le k -groupe $G_p(\mathcal{L})$, est alors 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, le foncteur $G_p : \mathcal{L} \mapsto G_p(\mathcal{L})$ induit une équivalence de la catégorie des k - p -algèbres de Lie de dimension finie, sur celle des k -groupes algébriques de hauteur ≤ 1 . Comme G_p est un foncteur adjoint à gauche, il commute aux limites inductives ; comme l'inclusion de la catégorie des k -groupes algébriques de hauteur ≤ 1 dans celle de tous les groupes algébriques commute manifestement aux limites projectives finies, on voit finalement que G_p est un foncteur exact : par exemple, si $i : \mathcal{L}_0 \rightarrow \mathcal{L}_1$ et $q : \mathcal{L}_1 \rightarrow \mathcal{L}_2$ sont des homomorphismes de k - p -algèbres de Lie et si la suite

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

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

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

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

et les assertions suivantes :

- (i) *Le morphisme u est lisse.*
- (ii) *G' est lisse.*

(iii) Pour tout entier $n > 0$, la suite

$$1 \longrightarrow {}_{\mathrm{Fr}^n} G' \xrightarrow{{}_{\mathrm{Fr}^n} v} {}_{\mathrm{Fr}^n} G \xrightarrow{{}_{\mathrm{Fr}^n} u} {}_{\mathrm{Fr}^n} G'' \longrightarrow 1$$

470 est exacte.

(iv) Le morphisme ${}_{\mathrm{Fr}} u : {}_{\mathrm{Fr}} G \rightarrow {}_{\mathrm{Fr}} G''$ est un épimorphisme.

(v) Le morphisme $\mathcal{L}ie(u) : \mathcal{L}ie(G) \rightarrow \mathcal{L}ie(G'')$ 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 : rappelons en effet que (i) entraîne (ii) d'après SGA II 1.3 ; d'autre part (ii) signifie que u est lisse à l'origine (SGA 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 ≤ 1 et celle des p -algèbres de Lie de dimension finie sur k .

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

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

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

Enfin, lorsque G est lisse sur k , $\mathrm{Fr}(G/k)$ 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 $\mathrm{Fr}(G'/k)$ 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 $G/{}_{\mathrm{Fr}^n} G$ soit lisse sur k pour $n \geq n_0$.

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

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

où l'on a posé $H = G_{\mathrm{réd}} \backslash G$. Or H est le spectre d'une k -algèbre finie, locale, de corps résiduel k (VI_B). Par conséquent, il existe un entier n_0 tel que $\mathrm{Fr}^n(H/k)$ se factorise

à travers l'unique section de $\text{Spec } k$ dans $H^{(p^n)}$, lorsque $n \geq n_0$. Il s'ensuit que, pour $n \geq n_0$, $\text{Fr}^n(G/k)$ se factorise à travers $G_{\text{réd}}^{(p^n)}$; l'homomorphisme $h : G/\text{Fr}^n G \rightarrow G_{\text{réd}}^{(p^n)}$, qui est défini par cette factorisation, est un monomorphisme (VI_A 5.4) et induit un homéomorphisme des espaces topologiques sous-jacents; c'est donc un isomorphisme (VI_B, $G_{\text{réd}}^{(p^n)}$ est réduit. Comme $G_{\text{réd}}^{(p^n)}$ est lisse sur k (VI_A, 1.3.1), $G/\text{Fr}^n G$ est lisse sur k , lorsque $n \geq n_0$.

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

Si G est lisse sur k , G est réduit et $\text{Fr}^n(G/k)$ est surjectif, donc est un épimorphisme. Réciproquement, comme $\text{Fr}^n(G/k)^{(p^n)}$ coïncide avec $\text{Fr}^n(G^{(p^n)}/k)$ (confer 4.1.3), alors $\text{Fr}^{nm}(G/k)$ est un épimorphisme pour tout m si $\text{Fr}^n(G/k)$ en est un. On a alors $G/\text{Fr}^{nm} G \simeq G^{(p^{nm})}$. Comme $G/\text{Fr}^{nm} G$ est lisse sur k pour m grand, $G^{(p^{nm})}$ et G le sont également.

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 ≥ 1 (resp. un entier ≥ 1 et premier à p) : dans les deux cas, nous disons simplement que n est premier à la caractéristique de k . De plus, si G est un schéma en groupes sur k , nous notons $n_G : G \rightarrow G$ le morphisme de k -schémas qui applique un élément x de $G(T)$ sur $x^n \in G(T)$, lorsque T est un k -schéma. 472

Proposition. — *Soient G un groupe algébrique sur un corps k et n un entier premier à la caractéristique de k . Alors $n_G : G \rightarrow G$ 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 $\text{Lie } n_G : \text{Lie } G \rightarrow \text{Lie } G$, 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 (VI_B 1.6.1; voir aussi VII_B § 3); donc A est régulier et n induit un automorphisme du gradué associé à A , donc aussi un automorphisme du complété $\hat{A}$ de A .

Si la caractéristique est $p > 0$ et si G est de hauteur ≤ 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 $\leq r$ et si nous supposons notre assertion démontrée pour les groupes de hauteur $\leq r - 1$, soient B , A et C les algèbres affines de $\text{Fr} G$, G et $G_{\text{Fr}} = \text{Fr} G \backslash G$. Appelons n_B , n_A et n_C les morphismes de B , A et C qui sont induits par $n_{\text{Fr} G}$, n_G et $n_{G_{\text{Fr}}}$. 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

473 $_{F^r}G$; 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 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 $\hat{A}$.

8.5. Proposition. — Soit G un groupe algébrique fini, de rang n sur le corps k . Alors $n_G : G \rightarrow G$ est le morphisme nul de G (confer 8.4).

Soit F un sous-groupe distingué de G de rang m sur k . Avec les notations de VI_A, 3.2 le carré

$$\begin{array}{ccc} F \times G & \xrightarrow{\lambda} & G \\ \text{pr}_2 \downarrow & & \downarrow \text{can.} \\ G & \xrightarrow{\text{can.}} & F \backslash G \end{array}$$

est cartésien. Comme $G \rightarrow F \backslash G$ 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 $G \rightarrow F \backslash G$ est localement libre de rang m . On a donc $\text{rg}_k(F \backslash G) \times \text{rg}_k F = \text{rg}_k G$.

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

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

quel que soit le k -schéma T ; il est donc clair que n_G est nul si m_F et $(nm^{-1})_{F \backslash G}$ le sont. Si F est la composante connexe de l'origine de G , $F \backslash G$ 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.

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

Ceci nous ramène au cas où G est de hauteur ≤ 1 : soient alors A l'algèbre affine de G et L son algèbre de Lie; si $[L : k] = r$, le rang de G sur k est p^r (VII_A 5.3.3); nous allons donc étudier le morphisme $p_G : G \rightarrow G$ 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 $U = U_p(L)$ de L . L'application p_U se décompose comme suit :

$$U \xrightarrow{\Delta_U^p} \bigotimes_k^p U \xrightarrow{m_U^p} U$$

où Δ_U^p désigne l'homomorphisme d'algèbres qui applique $x \in L \subset U$ 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_U^p est l'application linéaire qui envoie $u_1 \otimes u_2 \otimes \cdots \otimes u_p$ sur le produit $u_1 u_2 \cdots u_p$. Si $x_1, x_2, \dots, x_t$ sont t éléments de $L \subset U$, on a donc

$$p_U(x_1 x_2 \cdots x_t) = m_U^p \left(\prod_{j=1}^t \sum_{i=1}^p 1 \otimes \cdots \otimes \overset{i}{\downarrow} x_j \otimes \cdots \otimes 1 \right)$$

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 $\{1, 2, \dots, t\}$ dans $\{1, 2, \dots, p\}$. Une telle application définit un préordre sur $\{1, 2, \dots, t\}$ tel qu'on ait $i \leq j$ si et seulement si $h(i) \leq h(j)$; de plus, on a $m_U^p(x_h) = m_U^p(x_\ell)$ si h et ℓ définissent le même préordre, de sorte que nous pouvons écrire $m_U^p(x_h) = x_{\mathfrak{o}}$, où $\mathfrak{o}$ est le préordre défini par h . On a par conséquent

$$p_U(x_1 x_2 \cdots x_t) = \sum_{\mathfrak{o}} \binom{p}{s(\mathfrak{o})} \cdot x_{\mathfrak{o}},$$

où $\mathfrak{o}$ parcourt les relations de préordre sur $\{1, \dots, t\}$ 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 $\mathfrak{o}$.

Lorsque $t < p$, tous les termes $\binom{p}{s(\mathfrak{o})}$, sont nuls, de sorte que $p_U(x_1 \cdots x_t) = 0$. 475

Autrement dit, p_U s'annule sur le sous-espace vectoriel U_{p-1}^+ de U , qui est engendré par les produits $x_1 \cdots x_t$, $t < p$, $x_i \in L$. 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 I_A^p (I_A = idéal d'augmentation de A ; confer aussi VII_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

$$I_A \xrightarrow{p_A} I_A \xrightarrow{\text{can.}} I_A/I_A^p$$

est nulle. Donc p_A applique I_A dans I_A^p et $(p_A)^r$ applique I_A dans I_A^{pr} . Comme $I^{r(p-1)+1}A$ est nul d'après le théorème 7.4, l'égalité $p^r > r(p-1)$ montre que p_A^r annule I_A , cqfd