GROUPES ALGÉBRIQUES ET GROUPES FORMELS

PAR

P. CARTIER (1) (2) (Strasbourg)

1. INTRODUCTION

La théorie des groupes algébriques sur un corps de caractéristique non nulle est compliquée par la présence des phénomènes d'inséparabilité. On sait qu'il existe par exemple des homomorphismes bijectifs de groupes algébriques, qui ne sont pas des isomorphismes birationnels («isogénies radicielles»); de plus, le théorème d'isomorphisme classique $H/H \cap K \simeq H.\ K/K$ (où H et K sont des sous-groupes fermés d'un même groupe algébrique, et où K est invariant) n'est valable que si H et K se coupent transversalement. Dans un travail antérieur [6], j'ai donné une théorie générale des isogénies qui complétait les résultats de I. BARSOTTI [1]; mais l'objet introduit pour servir de noyau à une isogénie n'avait plus guère de parenté avec un groupe algébrique, et la théorie obtenue n'était guère maniable.

Les progrès récents de la Géométrie Algébrique ont amplement montré que le cadre naturel est celui des Schémas de A. GROTHENDIECK [14]; dans cette théorie, il y a correspondance bijective entre les sous-schémas fermés de l'espace affine à n dimensions et les idéaux de polynômes à n variables; ceci permet d'introduire de nombreuses «variétés» distinctes ayant même ensemble de points, et du même coup, de distinguer entre les «noyaux» des diverses isogénies radicielles. Autrement dit, si l'on considère les *Schémas en groupes* sur un corps de caractéristique quelconque, les difficultés précédemment mentionnées s'évanouissent. Dans

(1) Conférence prononcée à Bruxelles le 6 juin 1962 à l'occasion du *Colloque* sur la *Théorie des Groupes Algébriques* organisée par le CBRM.

(2) Les numéros entre crochets renvoient à la Bibliographie située à la fin de cet article.

cet exposé, nous introduirons deux limitations : nous ne considérerons que des schémas *affines* sur un *corps* de base; en dehors de cette catégorie, les résultats sont encore trop fragmentaires. D'autre part, nous présenterons la théorie différemment de Grothendieck, pour pouvoir manier de véritables groupes (3).

Dans un tout autre domaine, J. DIEUDONNÉ [10] [11] nous a fourni une grande variété de phénomènes algébriques nouveaux avec sa théorie des groupes formels sur un corps de caractéristique non nulle. Cette théorie, convenablement adaptée, a servi de guide aux recherches de Barsotti et moi-même sur les variétés abéliennes; on en trouvera un exemple dans l'exposé de Barsotti à ce même Colloque. Mais jusqu'à présent, la théorie des groupes algébriques et celle des groupes formels n'avaient que des rapports superficiels. C'est le but du présent exposé d'en faire la synthèse. Pour cela, nous devrons élargir un peu la notion de groupe formel, de manière à ce que tout groupe fini puisse être considéré comme un groupe formel; ceci fait, la théorie des groupes formels est équivalente à celle des hyperalgèbres (4).

En utilisant une suggestion de Grothendieck, nous associerons à tout groupe algébrique commutatif un groupe formel qui sera son dual. Le théorème de bidualité est valable; pour les groupes algébriques «finis», on retrouve la théorie de la dualité telle qu'elle est exposée (5) par P. GABRIEL [12]. D'un point de vue heuristique, on peut utiliser le tableau suivant de correspondances avec la théorie des groupes topologiques :

Groupe algébrique de type fini	——	Groupe de Lie compact
Groupe algébrique	——	Groupe compact
Groupe formel	——	Groupe discret
Dualité	——	Dualité de Pontryagin.

(3) Approximativement, un schéma est l'ensemble des sous-variétés irréductibles d'une variété algébrique, mais non l'ensemble des ses points; un schéma en groupes n'est pas un groupe! Par ailleurs, nous avons largement utilisé le langage des foncteurs (cf. GROTHENDIECK [13]); précisons seulement qu'un foncteur $T : A \to B$ covariant (resp. contravariant) est appelé une équivalence (resp. une dualité) si tout objet de B est isomorphe à un objet de la forme T(X) pour X dans A, et si T définit une bijection de Hom (X, Y) sur Hom (T(X), T(Y)) (resp. sur Hom (T(Y), T(X))) pour tout couple d'objets X et Y de A.

(4) En topologie algébrique, on utilise sous le nom d'Algèbre de Hopf une notion très proche de celle d'hyperalgèbre.

(5) Gabriel utilise le langage des hyperalgèbres, et non celui des groupes formels, ce qui oblige à de nombreuses contorsions.

Pour l'instant, nous ne savons pas définir des objets, analogues dans la correspondance ci-dessus, aux groupes commutatifs localement compacts qui ne sont ni discrets, ni compacts. La question semble importante pour certaines applications géométriques.

Le présent article n'est qu'un résumé; il ne contient pratiquement aucune démonstration, ni les applications aux variétés abéliennes. Nous publierons par ailleurs un exposé détaillé de la théorie.

2. DÉFINITION DES GROUPES ALGÉBRIQUES

Montrons d'abord comment l'on peut généraliser la notion classique de groupe algébrique de matrices. Soit n un entier strictement positif; pour tout anneau commutatif A, on note $GL(n, A)$ l'ensemble des matrices carrées d'ordre n, à coefficients dans A, et dont le déterminant est un élément inversible de A; pour la multiplication matricielle, $GL(n, A)$ est un groupe. Pour éviter la restriction gênante sur le déterminant, on emploie l'artifice classique suivant; posons $r = n^2 + 1$; on associe à toute matrice g de $GL(n, A)$ le point de A^r ayant pour coordonnées les éléments g_{ij} de la matrice g (pour $1 \leqslant i, j \leqslant n$) et l'inverse g_0 du déterminant de g. Introduisons un système X de r indéterminées X_0 et X_{ij}, et le polynôme à coefficients entiers :

$$D(X) = 1 - X_0 \cdot \det X_{ij} \tag{1}$$

Dans ces conditions, on peut identifier l'ensemble $GL(n, A)$ avec l'ensemble des points de A^r qui annulent le polynôme D.

Considérons alors un corps k et une extension algébriquement close Ω de k; selon la définition usuelle, on dit qu'un sous-groupe G de $GL(n, \Omega)$ est algébrique s'il est l'ensemble des matrices g annulant un certain nombre de polynômes de $\Omega[X]$. On dit que G est défini sur k si l'idéal des polynômes de $\Omega[X]$ nuls sur G est engendré par des polynômes à coefficients dans k; si G est un tel groupe, on notera $I_k(G)$ l'ensemble des polynômes de $k[X]$ qui s'annulent sur G; le groupe G est alors l'ensemble des zéros de l'idéal $I_k(G)$. De plus, pour qu'un idéal I de $k[X]$ soit de la forme $I_k(G)$ pour un groupe G convenable, il faut et il suffit qu'il vérifie les conditions suivantes (6).

(6) Soit Z l'ensemble des zéros de l'idéal I dans l'espace Ω^r; la condition a) signifie que l'on a $Z \subset GL(n, \Omega)$, la condition b) que Z est stable par

a) *L'idéal I contient* D.

b) *Soit* Y *une nouvelle série de r variables; posons* $Z_0 = X_0Y_0$ *et* $Z_{ik} = \sum_{1 \leqslant j \leqslant n} X_{ij}Y_{jk}$ *pour* $1 \leqslant i, k \leqslant n$. *Pour tout polynôme* P *de I, on a une relation de la forme :*

$$(2) \qquad P(Z) = \sum_{\alpha} L_\alpha(X) \cdot P_\alpha(Y) + \sum_{\beta} P'_\beta(X) \cdot L'_\beta(Y)$$

avec des polynômes L_α *et* L'_β *dans* $k[X]$ *et des polynômes* P_α *et* P'_β *dans I.*

c) *Soit* X'_0 *le déterminant de la matrice* (X_{kl}), *et* X'_{ij} *le produit de* X_0 *par le cofacteur de* X_{ij} *dans le déterminant* X'_0. *On a alors* $P(X') \in I$ *pour tout polynôme* P *dans I.*

d) *L'idéal de* $\Omega[X]$ *engendré par I est intersection d'idéaux premiers.*

Lorsque k est de caractéristique nulle, la condition d) est conséquence des autres conditions; cela résulte de théorèmes mentionnés plus loin (cf. n° 15). Mais si le corps k est de caractéristique $p \neq 0$, il n'en est plus de même comme le montre l'exemple de l'idéal $I = (X_{11}^p - 1, 1 - X_0X_{11})$ dans le cas $n = 1$. De nombreuses raisons poussent actuellement à considérer que la notion essentielle est non pas celle de groupe algébrique de matrices, mais celle d'idéal I satisfaisant aux hypothèses a), b) et c). Soit I un tel idéal; on peut définir l'ensemble G_Ω des matrices g de $GL(n, \Omega)$ annulant tous les polynômes de l'idéal I, et G_Ω est un sous-groupe algébrique de $GL(n, \Omega)$ défini sur la clôture parfaite de k; mais en général, l'idéal I est différent de l'idéal $I_k(G_\Omega)$ des polynômes nuls sur G_Ω, de sorte que l'idéal I n'est plus caractérisé par le groupe G_Ω; dans l'exemple précédent, le groupe G_Ω ne contient que la matrice unité! De manière heuristique, il faut considérer les points infinitésimaux du groupe à côté des points «finis». On doit à A. WEIL [19] une méthode rigoureuse pour traiter des points infinitésimaux; si l'on suit cette idée, on est conduit à introduire pour toute k-algèbre commutative A l'ensemble G_A des matrices g de $GL(n, A)$ qui annulent tous les polynômes de l'idéal I; il se trouve que G_A est un sous-groupe de $GL(n, A)$ et que I est l'ensemble des polynômes de $k[X]$ nuls sur G_A pour *toute* algèbre A. C'est donc la

multiplication, et c) qu'il est stable pour l'inversion; enfin d) exprime le théorème des zéros de Hilbert et assure que I est l'ensemble de tous les polynômes de $k[X]$ nuls sur Z.

collection de tous (7) les groupes G_A qui constitue le «groupe algébrique de matrices» associé à l'idéal I; pour des raisons techniques, il faut aussi considérer à côté des groupes G_A les homomorphismes $G(\sigma)$ ainsi définis : pour tout homomorphisme d'algèbres σ de A dans B, on définit un homomorphisme de groupes $G(\sigma)$ de G_A dans G_B en associant à la matrice $g = (g_{ij})$ la matrice : $\sigma \cdot g = (\sigma \cdot g_{ij})$.

Par ailleurs, J.-P. SERRE [17] a démontré récemment la nécessité de considérer des limites projectives de groupes algébriques, ou «groupes proalgébriques». Par exemple, le groupe des unités d'un corps complet muni d'une valuation discrète à corps des restes algébriquement clos, ou encore le groupe de Galois d'une extension algébrique infinie, ont tout intérêt à être considérés comme groupes proalgébriques. La définition à laquelle nous nous arrêterons est motivée par le désir d'englober au moins les groupes proalgébriques «affines».

Par définition, un «groupe algébrique» est constitué par la donnée pour toute algèbre commutative A d'un groupe G_A et pour tout homomorphisme d'algèbres $\sigma : A \to B$ d'un homomorphisme de groupes $G(\sigma) : G_A \to G_B$ satisfaisant aux axiomes suivants.

(G 1) *On a* $G(\tau\sigma) = G(\tau) \cdot G(\sigma)$ *lorsque les homomorphismes* σ *et* τ *sont composables; lorsque* σ *est l'application identique de* A, *alors* $G(\sigma)$ *est l'application identique de* G_A.

(G 2) *Il existe un point générique pour* G; *autrement dit, il existe une algèbre commutative* E *et un point x dans* G_E *tels que l'application* $\sigma \to G(\sigma).x$ *soit, pour toute algèbre* A, *une bijection de l'ensemble des homomorphismes de* E *dans* A *sur l'ensemble* G_A.

Dans le langage fonctoriel, un groupe algébrique est donc un foncteur représentable de la catégorie des algèbres commutatives dans la catégorie des groupes. On sait que la catégorie des schémas affines est équivalente à la catégorie duale de celle des anneaux

(7) Pour éviter des difficultés logiques bien connues, on peut utiliser l'artifice des univers. Un univers est un ensemble U assez vaste pour que l'on puisse effectuer sur les ensembles appartenant à U toutes les opérations usuelles de la Théorie des Ensembles. En ajoutant à la Théorie des Ensembles un axiome d'existence convenable, on peut faire en sorte que tout ensemble appartienne à un univers. Dans le cas du texte, on pourra se limiter aux groupes G_A pour A parcourant un univers donné auquel appartienne k.

commutatifs; il en résulte que notre théorie est équivalente à celle des schémas affines en groupes.

Exemples : 1) Soit n un entier > 0; pour toute algèbre commutative A, posons $GL(n)_A = GL(n, A)$, et pour tout homomorphisme d'algèbres σ de A dans B, définissons l'homomorphisme $GL(n)$ (σ) comme celui qui associe $\sigma \cdot g$ à g. On a défini ainsi un groupe algébrique $GL(n)$, dit *groupe linéaire à n variables.*

2) Soit G un groupe algébrique. On dit qu'un groupe algébrique G′ est un *sous-groupe* de G si G'_A est un sous-groupe de G_A pour toute algèbre commutative A et si $G'(\sigma)$ est la restriction de $G(\sigma)$ à G'_A pour tout homomorphisme $\sigma : A \to B$.

3) Les groupes construits précédemment au moyen d'un idéal I de $k[X]$ satisfaisant à a), b) et c) ne sont autre que les sous-groupes de $GL(n)$. Si l'idéal I est engendré par des polynômes P_α, on dira que le groupe associé à I est le sous-groupe de $GL(n)$ défini par les équations $P_\alpha = 0$.

4) Soit L une algèbre de rang fini sur k; notons I l'application identique de L. Pour toute algèbre commutative A, notons $S(L)_A$ le groupe additif de l'algèbre $L \otimes A$, et $P(L)_A$ le groupe multiplicatif des éléments inversibles de la même algèbre. Pour tout homomorphisme d'algèbres σ de A dans B, l'application linéaire $I \otimes \sigma$ de $L \otimes A$ dans $L \otimes B$ induit des homomorphismes $S(L)$ (σ) de $S(L)_A$ dans $S(L)_B$ et $P(L)$ (σ) de $P(L)_A$ dans $P(L)_B$. On définit ainsi deux groupes algébriques S(L) et P(L) appelé respectivement *le groupe additif* et *le groupe multiplicatif* de L. Lorsque $L = k$, on obtient les groupes notés respectivement G_a et G_m et appelés groupe additif et groupe multiplicatif à un paramètre. On a $G_m = GL(1)$.

5) On dit qu'un groupe algébrique G est de *type fini* s'il est isomorphe à un sous-groupe d'un groupe $GL(n)$. Il revient au même de supposer qu'il existe un point générique $x \in G_E$ tel que l'algèbre E ait un nombre fini de générateurs; cette condition est indépendante du point générique choisi. On dit que G est *fini* s'il existe un point générique $x \in G_E$ avec E de rang fini sur k.

3. Propriétés générales des groupes algébriques

La notion d'homomorphisme est primordiale. Soient G et H deux groupes algébriques; *un homomorphisme* u de G dans H est

la donnée pour toute algèbre commutative A d'un homomorphisme de groupes u_A de G_A dans H_A, vérifiant les relations $u_B \cdot G(\sigma) = H(\sigma) \cdot u_A$ pour tout homomorphisme d'algèbres σ de A dans B [8]. Introduisons des points génériques $x \in G_E$ et $y \in H_F$ pour G et H; il existe alors un homomorphisme σ de F dans E caractérisé par la formule : $u_E(x) = H(\sigma) \cdot y$; on dit que u est un monomorphisme si σ est surjectif et un épimorphisme si σ est injectif; naturellement, ces propriétés ne dépendent pas du choix des points génériques. On notera δ_G l'endomorphisme identique d'un groupe algébrique G.

Soit G′ un sous-groupe de G; l'injection de G′ dans G est alors un monomorphisme. On dit que G′ est invariant si G'_A est un sous-groupe invariant de G_A pour toute algèbre A; on peut alors construire un groupe quotient G/G′ et un épimorphisme canonique π de G sur G/G′ tel que le noyau de π_A soit égal à G'_A pour toute algèbre A; on peut donc identifier G_A/G'_A à un sous-groupe de $(G/G')_A$, mais en général, ces deux groupes seront distincts. La construction de G/G′ est assez délicate; elle peut se faire en adaptant un argument par lequel C. Chevalley [9] montre l'existence d'un homomorphisme rationnel ayant un noyau donné. En tout cas, les propriétés de G/G′ énoncées plus haut suffisent à le caractériser à un isomorphisme unique près.

Si u est un homomorphisme de G dans H, la collection N des noyaux N_A des homomorphismes u_A est un sous-groupe de G, que l'on appelle *le noyau* de u. Parmi les sous-groupes H′ de H tels que $H'_A \supset u_A(G_A)$ pour tout A, il en existe un plus petit, que l'on appelle *l'image de u*, et que l'on note $u(G)$; en général, on a $u(G)_A \neq u_A(G_A)$. Avec ces définitions, on a le *théorème de factorisation canonique* : N est un sous-groupe invariant de G, et il existe un isomorphisme u de G/N sur $u(G)$ tel que $u = \iota \cdot u \cdot \pi$ où ι est l'injection de $u(G)$ dans H et π l'homomorphisme canonique de G sur G/N. On en déduit les deux théorèmes d'isomorphisme classiques $G/G' \simeq (G/G'')/(G'/G'')$ et $G'/G' \cap L \simeq G' \cdot L/L$; on en déduit aussi que u est un monomorphisme (resp. un épimorphisme) si et seulement si l'on a $N = (e)$ (resp. $u(G) = H$), et que u est un isomorphisme si et seulement si l'on a à la fois $N = (e)$ et $u(G) = H$. Il n'y a donc plus à distinguer entre homomorphis-

[8] Un homomorphisme de groupes algébriques est donc par définition un homomorphisme de foncteurs.

mes bijectifs et isomorphismes; quant aux isogénies, on les définira comme les homomorphismes à noyau fini.

La notion de produit d'une famille, finie ou infinie, de groupes algébriques est claire; le produit est défini sans restriction. On a alors l'analogue du théorème de Peter-Weyl : tout groupe algébrique est isomorphe à un sous-groupe d'un produit $\prod_\iota \mathrm{GL}(n_\iota)$ de groupes linéaires; on en déduit que tout groupe algébrique est limite projective d'une famille filtrante de sous-groupes de groupes linéaires $\mathrm{GL}(n)$ convenables; à l'inséparabilité près, nos groupes algébriques sont donc les groupes proalgébriques *affines* de Serre. De ce qui précède, on déduit sans peine un théorème analogue au théorème de dualité de Tannaka pour les groupes compacts(cf [5] et [8]); il faut seulement noter que les représentations linéaires (9) d'un groupe algébrique ne sont pas en général complètement réductibles.

Il est nécessaire pour la suite de définir l'*extension des scalaires*. Soient G un groupe algébrique (sur le corps k) et soit λ un homomorphisme de k dans un corps k'. Pour toute algèbre A' sur k', on définit l'algèbre A_λ sur k en conservant les éléments, l'addition et la multiplication de A', mais en considérant la loi externe $(u, a') \to \lambda(u).\ a'$ (pour u dans k et a' dans A'); si σ est un k'-homomorphisme d'algèbres de A' dans B', c'est encore un k-homomorphisme de A_λ dans B_λ que l'on notera σ_λ pour éviter des confusions. Soit maintenant A une algèbre sur k; l'algèbre A^λ sur k' déduite par extension des scalaires est le produit tensoriel $k'_\lambda \otimes_k A$ muni d'une loi externe convenable; on a les règles de calcul :

$$(3) \qquad u' \otimes va = u'\lambda(v) \otimes a \qquad u' \cdot (u'' \otimes a) = u'u'' \otimes a$$

pour u', u'' dans k', v dans k et a dans A.

Le groupe algébrique G^λ sur le corps k' est alors défini par les formules :

$$(4) \qquad G^\lambda_{A'} = G_{A'_\lambda} \quad G^\lambda(\sigma) = G(\sigma_\lambda).$$

(9) Soit V un espace vectoriel de dimension finie n sur le corps k. Si L(V) est l'algèbre des endomorphismes de V, le groupe algébrique P(L(V)) se note GL(V); le choix d'une base de V définit un isomorphisme de GL(V) avec $\mathrm{GL}(n)$. Ceci étant, une représentation linéaire d'un groupe algébrique G dans l'espace vectoriel V est, par définition, un homomorphisme de G dans GL(V). On peut calquer la théorie usuelle des représentations linéaires de

Soit x dans G_E un point générique de G; soit π l'homomorphisme de E dans $F = (E^\lambda)_\lambda$ défini par $\pi(a) = 1 \otimes a$; alors le point $x' = G(\pi) \cdot x$ de $G_F = G^\lambda_{E^\lambda}$ est générique. On a $\mathrm{GL}(n)^\lambda = \mathrm{GL}(n)$, et si le sous-groupe algébrique G de $\mathrm{GL}(n)$ est défini par des équations $P_\alpha = 0$ à coefficients dans k, le sous-groupe algébrique G^λ de $\mathrm{GL}(n)$ est défini par les équations $P^\lambda_\alpha = 0$ obtenues en appliquant λ à chaque coefficient de chaque polynôme P_α.

4. Groupes algébriques commutatifs sur un corps parfait

On dit qu'un groupe algébrique G est *commutatif* si les groupes G_A sont tous commutatifs; si G et H sont deux groupes algébriques commutatifs, on peut définir une addition sur l'ensemble Hom (G, H) des homomorphismes de G dans H. Le théorème de factorisation canonique montre alors que la catégorie C des groupes algébriques commutatifs est une catégorie abélienne au sens de A. Grothendieck [13]; de plus, par des raisonnements voisins de ceux de J.-P. Serre [17], on prouve que pour tout groupe algébrique commutatif G, il existe un groupe algébrique commutatif *projectif* P et un épimorphisme de P dans G; ceci permet d'appliquer à la catégorie C les méthodes de l'Algèbre Homologique.

5. Soit G un groupe algébrique commutatif; on dit que G est *réductif* si toute représentation linéaire de G est complètement réductible. Supposons k *parfait* pour ce n° et le suivant; on notera $\bar{k}$ une clôture algébrique de k, et $\mathfrak{G}$ le groupe de Galois topologique de $\bar{k}$ sur k. Pour que G soit réductif, il faut et suffit que le groupe algébrique $\bar{G}$ sur le corps $\bar{k}$, déduit de G par extension des scalaires, soit isomorphe à un sous-groupe d'un produit de groupes tous égaux à G_m.

On notera C^r la catégorie des groupes algébriques réductifs. Pour tout groupe algébrique commutatif G, on note X(G) l'ensemble des homomorphismes de $\bar{G}$ dans G_m (sur le corps $\bar{k}$); c'est un groupe commutatif sur lequel le groupe de Galois $\mathfrak{G}$ opère de manière naturelle; de plus, pour tout χ dans X(G), l'ensemble des s dans $\mathfrak{G}$ tels que $s \cdot \chi = \chi$ est un sous-groupe ouvert

groupes, et définir les représentations irréductibles, complètement réductibles, etc.

dans $\mathfrak{G}$; dans la terminologie de J. Tate, X(G) est donc un module de Galois pour $\mathfrak{G}$. On a donc défini un foncteur contravariant X de la catégorie C^r dans la catégorie M des modules de Galois pour $\mathfrak{G}$; ce foncteur est une dualité.

Pour qu'un groupe réductif G soit de type fini, il faut et suffit que X(G) soit un groupe abélien de type fini. Pour que G soit «connexe», il faut et suffit que X(G) soit sans torsion; enfin pour que G soit «simplement connexe» au sens de SERRE [17], il faut et suffit que le groupe X(G) soit divisible. Appelons tore algébrique tout groupe réductif connexe de type fini; ce qui précède montre que les tores algébriques correspondent par X aux modules de Galois pour $\mathfrak{G}$ qui sont des groupes abéliens libres de type fini (théorème de Tate).

6. On dit que le groupe algébrique commutatif G est *unipotent* si toute représentation linéaire irréductible de G est triviale (cette définition a un sens si k n'est pas parfait). Il revient au même de supposer que tout homomorphisme de $\bar{G}$ dans G_m (sur le corps $\bar{k}$) est nul.

Supposons k de caractéristique *nulle*. Pour qu'un groupe algébrique commutatif G soit unipotent, il faut et suffit qu'il soit isomorphe au produit d'une famille, finie ou infinie, de groupes égaux à G_a. De manière plus intrinsèque, posons $V(G) = \mathrm{Hom}(G, G_a)$; c'est un espace vectoriel sur le corps k; de plus, le foncteur V est une dualité de la catégorie des groupes unipotents avec la catégorie des espaces vectoriels sur k. Pour que G soit de type fini, il faut et suffit que l'espace vectoriel $V(G)$ soit de dimension finie.

Revenons au cas d'un corps k de caractéristique quelconque. Pour qu'un groupe algébrique commutatif soit réductif (resp. unipotent), il faut et suffit qu'il soit limite projective de groupes algébriques commutatifs de type fini qui soient réductifs (resp. unipotents). Pour les groupes de type fini, la terminologie : réductif — unipotent est en accord avec les conventions usuelles. Enfin, tout groupe algébrique commutatif G se décompose de manière unique comme produit $G^r \times G^u$ d'un groupe réductif G^r et d'un groupe unipotent G^u.

7. GROUPES ALGÉBRIQUES SUR UN CORPS DE CARACTÉRISTIQUE NON NULLE

Supposons k de caractéristique $p \neq 0$; nous allons rencontrer ici les phénomènes algébriques les plus intéressants. Donnons d'abord quelques exemples importants.

Soit n un entier > 0; pour tout anneau commutatif A de caractéristique p, on sait définir l'anneau $W_n(A)$ des vecteurs de Witt de longueur n sur A; de plus, pour tout homomorphisme σ de A dans un anneau B de caractéristique p, on définit un homomorphisme d'anneau de $W_n(A)$ dans $W_n(B)$ en posant :

$$W_n(\sigma)(x_0, \ldots, x_{n-1}) = (\sigma \cdot x_0, \ldots, \sigma \cdot x_{n-1}). \tag{5}$$

La collection des groupes additifs $W_n(A)$ pour les k-algèbres commutatives A, et des homomorphismes $W_n(\sigma)$ est un groupe algébrique commutatif, que l'on notera W_n.

On notera par ailleurs E_n l'anneau des endomorphismes du groupe algébrique commutatif W_n. On définit d'abord deux éléments V et F de E_n par les formules de Witt :

$$F_A(x_0, \ldots, x_{n-1}) = (x_0^p, \ldots, x_{n-1}^p) \tag{6}$$

$$V_A(x_0, \ldots, x_{n-1}) = (0, x_0, \ldots, x_{n-2}). \tag{7}$$

De plus, en utilisant la structure d'anneau de $W_n(A)$, on définit pour tout vecteur de Witt w dans $W_n(k) = \Lambda_n$ un opérateur de multiplication par w qui est un endomorphisme $R(w)$ de W_n. Enfin, on posera :

$$F_k(w) = w^\pi \qquad V_k(w) = w^\delta \qquad (w \in \Lambda_n).$$

On a alors le système de relations :

$$\begin{cases} VF = FV = p \cdot \delta_{W_n} & V^n = 0 \\ F \cdot R(w) \, R(w^\pi) \cdot F & V \cdot R(w^\pi) = R(w) \cdot V \end{cases} \tag{8}$$

$$V \cdot R(w) \cdot F = R(w^\delta) \tag{9}$$

et tout élément de E_n s'écrit de manière unique sous la forme :

$$\sum_{i>0} R(w_i) \cdot F^i + \sum_{0 \leqslant j < n} V^j \cdot R(w'_j) \tag{10}$$

avec des vecteurs de Witt w_i et w'_j dans Λ_n, nuls sauf un nombre

fini d'entre eux ([10]). Enfin, l'application $w \to R(w)$ est un isomorphisme de Λ_n sur un sous-anneau de E_n.

On a $W_1 = G_a$; l'endomorphisme V de G_a est nul, et l'on a $F_A(x) = x^p$ pour x dans une algèbre commutative A. Dans la théorie des groupes algébriques finis, le noyau $W_{n,r}$ de l'endomorphisme F^r de W_n joue un rôle important.

8. On note φ l'endomorphisme du corps k défini par $\varphi(x)=x^p$. De plus, pour toute algèbre commutative A sur k, on note φ_A l'homomorphisme de A dans A_φ défini par $\varphi_A(a) = a^p$. Soit alors G un groupe algébrique; pour toute algèbre commutative A, l'homomorphisme $F_A = G(\varphi_A)$ de G_A dans $G_{A_\varphi} = G_A^\varphi$ est défini; la collection des F_A est un homomorphisme de G dans G^φ, appelé *homomorphisme de Frobenius*. Si G est l'un des groupes $GL(n)$, G_a, G_m, W_n, on a $G^\varphi = G$, et l'homomorphisme de Frobenius consiste à élever chaque coordonnée à la puissance p-ième; la notation F est donc cohérente avec celle introduite pour W_n.

Supposons maintenant G commutatif; on peut définir comme suit un homomorphisme V de G^φ dans G. Soient L et A deux algèbres commutatives; dans le produit tensoriel $L \otimes A_\varphi$ on a la relation :

$$(\lambda x) \otimes a = x \otimes (\lambda^p a) = \lambda(x \otimes a) \tag{11}$$

pour λ dans k, x dans L et a dans A; il en résulte qu'il existe un homomorphisme d'algèbres $\tau_{L,A}$ de $L \otimes A_\varphi$ dans $(L \otimes A)_\varphi$ défini par:

$$\tau_{L,A}(x \otimes a) = x^p \otimes a. \tag{12}$$

L'homomorphisme V est alors *caractérisé* par la relation :

$$\tau_{L,A_\varphi} \cdot u_A = u_A \cdot V_A \tag{13}$$

pour tout homomorphisme u de G dans le groupe multiplicatif P(L) d'une algèbre commutative L. On a :

$$V \cdot F = p \cdot \delta_G. \tag{14}$$

([10]) Cf. J. DIEUDONNÉ [10], démonstration du théorème 1. L'hypothèse que K est parfait est inutile, en vertu de la relation (9) qui permet de simplifier les produits $V^i R(w) F^j$. On remarquera que Dieudonné note respectivement p et t ce que nous notons F et V.

Lorsque $G = W_n$, l'homomorphisme V de $W_n^\varphi = W_n$ dans W_n est identique à celui qu'on a défini plus haut. La *construction* directe de V est assez compliquée et utilise un lemme curieux d'algèbre linéaire qui se formule ainsi ([11]) :

Soit E *une algèbre sur le corps* k *de caractéristique* $p \neq 0$. *Dans l'algèbre produit tensoriel de p algèbres égales à* E, *soit* S_p *la sous-algèbre formée des tenseurs symétriques; l'ensemble des tenseurs symétrisés est un idéal* I *de* S_p; *de plus, il existe un homomorphisme u de* S_p *sur* E^φ *de noyau* I, *caractérisé par* $u(x \otimes \ldots \otimes x) = 1 \otimes x$ *pour* x *dans* E.

9. Nous allons maintenant énoncer le théorème de structure des groupes algébriques commutatifs unipotents. Tout d'abord, pour tout entier $n > 0$, on définit des homomorphismes :

$$G \xrightarrow{F^n} G^{\varphi^n} \xrightarrow{V^n} G$$

On peut, soit itérer F et V convenablement, soit recommencer les constructions du n° 8, en remplaçant p par p^n. On notera U_n la catégorie des groupes algébriques commutatifs G pour lesquels l'homomorphisme V^n de G^{φ^n} dans G est nul. Par ailleurs, pour tout groupe algébrique commutatif G, on pose $V_n(G) = \mathrm{Hom}(G, W_n)$; on définit sur $V_n(G)$ une structure naturelle de module à gauche sur l'anneau $E_n = \mathrm{Hom}(W_n, W_n)$; alors V_n est un foncteur contravariant de la catégorie C des groupes algébriques commutatifs dans la catégorie des modules à gauche sur l'anneau E_n. On a $V_n(G) = 0$ si G est réductif.

THÉORÈME 1. *Soit* G *un groupe algébrique commutatif sur un corps* k *de caractéristique* $p \neq 0$.

a) *Supposons* G *de type fini. Pour qu'il soit unipotent, il faut et suffit qu'il existe un entier* $n > 0$ *tel que l'homomorphisme* V^n *de* G^{φ^n} *dans* G *soit nul.*

b) *Soit* n *un entier* > 0. *Pour que* V^n *soit nul, il faut et suffit que* G *soit isomorphe à un sous-groupe algébrique du produit d'une famille, finie ou infinie, de groupes* W_n.

c) *Le foncteur* V_n *est une dualité de la catégorie* U_n *avec celle des modules à gauche sur l'anneau* E_n.

([11]) Géométriquement, on peut dire que si V est une variété algébrique, et Σ le produit symétrique d'ordre p de V, l'image dans Σ de la diagonale du produit $V \times V \times \ldots \times V$ est une variété isomorphe à V^φ.

La démonstration de a) repose sur des raisonnements souvent utilisés dans la théorie des groupes algébriques linéaires; essentiellement, on utilise la caractérisation des matrices unipotentes par la relation : $X^{p^n} = 1$ pour n assez grand, et la formule $V^n F^n = p^n \delta_G$ qui montre que $V^n = 0$ entraîne $p^n \cdot \delta_G = 0$. La démonstration de b) est nettement plus délicate, et utilise la structure des extensions d'un groupe de Witt par un autre (cf. SERRE [18]); enfin, c) résulte facilement de b) et du fait que W_n est un objet injectif de la catégorie abélienne U_n.

La structure des modules sur un anneau du type E_n est assez bien connue, tout au moins à condition de «négliger» les modules de longueur finie; on pourra consulter J. DIEUDONNÉ [11], O. ORE [16] et P. GABRIEL [12]. Par ce genre de raisonnement, on peut obtenir assez facilement le résultat suivant de C. CHEVALLEY [18].

COROLLAIRE. *Soit k un corps algébriquement clos de caractéristique $p \neq 0$. Tout groupe algébrique commutatif unipotent de type fini est isogène à un produit de groupes de Witt.*

Lorsque $n = 1$, les résultats du théorème 1 se simplifient. En particulier, l'homomorphisme V de G^{φ} dans G est nul si et seulement si G est isomorphe à un sous-groupe algébrique d'un produit de groupes G_a; les modules à gauche sur l'anneau E_1 sont les espaces vectoriels V sur le corps k, munis d'un opérateur additif F vérifiant $F(\lambda \cdot v) = \lambda^p \cdot F(v)$ pour λ dans k et v dans V. Ceci permet d'aborder l'étude des «formes» du groupe G_a sur un corps non parfait, c'est-à-dire les groupes algébriques G qui deviennent isomorphes à G_a après extension des scalaires de k à sa clôture algébrique; ceci est lié à la cohomologie des extensions algébriques, séparables ou non, problème que nous aborderons ultérieurement.

10. GROUPES FORMELS

Nous présenterons les groupes formels de la même manière que les groupes algébriques. Un groupe formel G sera donc défini comme un foncteur de la catégorie des algèbres commutatives dans la catégorie des groupes; au lieu d'imposer l'existence d'un point générique, nous supposerons vérifié l'axiome suivant.

(G 3) *Il existe une famille d'algèbres commutatives E_a de rang fini sur k, et de points $x_a \in G_{E_a}$ ayant les propriétés suivantes :*

a) *Si σ et τ sont deux homomorphismes distincts de E_a dans une algèbre A, on a $\sigma \cdot x_a \neq \tau \cdot x_a$.*

b) *Etant données des algèbres $A_1, \ldots, A_n$ et des points $g_i \in G_{A_i}$ pour $1 \leqslant i \leqslant n$, il existe un indice a et des homomorphismes $\sigma_i : E_a \to A_i$ tel que $\sigma_i \cdot x_a = g_i$.*

On peut répéter pour les groupes formels une bonne partie du n° 3; on définira homomorphismes, monomorphismes, épimorphismes, sous-groupes et groupes quotients, de même que l'extension des scalaires. Le lemme de factorisation canonique est encore valable, mais sa démonstration est assez différente; il en résulte que les groupes formels commutatifs forment une catégorie abélienne. Enfin, si k est de caractéristique $p \neq 0$, on peut définir des homomorphismes :

$$G \xrightarrow{F^n} G^{\varphi^n} \xrightarrow{V^n} G$$

et l'on a $V^n \cdot F^n = p^n \cdot \delta_G$. La seule différence importante est qu'en général, le produit d'une famille *infinie* de groupes formels n'existe pas.

Soit G un groupe formel; on appelle *fonction f* sur G une famille d'applications $f_A : G_A \to A$ (pour toute algèbre commutative A) vérifiant les relations

$$\sigma \cdot f_A = f_B \cdot G(\sigma) \tag{15}$$

pour tout homomorphisme d'algèbres σ de A dans B. L'ensemble des fonctions sur G sera noté $O(G)$; c'est de manière naturelle une algèbre; pour toute algèbre commutative A et tout x dans G_A, on définit un homomorphisme d'algèbres χ_x de $O(G)$ dans A par $\chi_x(f) = f_A(x)$. Les algèbres A étant considérées comme discrètes, on munit $O(G)$ de la topologie la moins fine pour laquelle tous les homomorphismes χ_x sont continus; alors, $O(G)$ est un anneau topologique commutatif séparé et complet; tout voisinage de 0 contient un idéal ouvert, et tout idéal ouvert est de codimension finie. Enfin, pour toute algèbre A, l'application $x \to \chi_x$ est une bijection de G_A sur l'ensemble des homomorphismes d'algèbres de $O(G)$ dans A dont le noyau est un idéal ouvert.

On appelle *distribution* sur le groupe G toute forme linéaire T sur $O(G)$ dont le noyau est ouvert; l'espace vectoriel des distributions se note U(G); on note $U^+(G)$ l'ensemble des distribu-

tions T telles que $< T, 1 > = 0$. Par analogie avec la théorie des distributions sur un groupe de Lie, on peut définir un produit de convolution sur U(G), pour lequel U(G) devient une algèbre associative; cette algèbre est commutative si et seulement si le groupe formel G est commutatif. «En transposant la multiplication» dans l'anneau $O(G)$, on peut définir un homomorphisme P de U(G) dans $U(G) \otimes U(G)$, appelé coproduit. La liste des propriétés de P est trop longue pour être répétée ici; on pourra se reporter à [7], exposé n° 2, où l'on omettra ce qui concerne les filtrations. En bref, nous dirons que U(G) est une *hyperalgèbre*.

Soit A une algèbre; on peut identifier $U(G) \otimes A$ à un ensemble d'applications linéaires de $O(G)$ dans A, puisque U(G) est un sous-espace du dual de l'espace vectoriel $O(G)$. On définit trois homomorphismes d'algèbres de $U(G) \otimes A$ dans $U(G) \otimes U(G) \otimes A$ par les formules :

$$(16) \qquad P'(T \otimes a) = P(T) \otimes a, \quad \varepsilon(T \otimes a) = T \otimes 1 \otimes a, \quad \varepsilon'(T \otimes a) = 1 \otimes T \otimes a$$

Alors, on a $\chi_x \cdot \chi_y = \chi_{xy}$ pour x, y dans G_A, et l'application $x \to \chi_x$ est une bijection de G_A sur l'ensemble des éléments Z de $U(G) \otimes A$ congrus à $1 \otimes 1$ modulo $U^+(G) \otimes A$ et tels que $P'(z) = \varepsilon(z) \cdot \varepsilon'(z)$. Il n'existe d'ailleurs qu'un seul produit et qu'un seul coproduit sur U(G) pour lesquels ces propriétés soient valables pour toute algèbre commutative A.

Enfin, le foncteur U qui associe à tout groupe formel G l'hyperalgèbre U(G) est une équivalence de la catégorie des groupes formels avec celle des hyperalgèbres.

11. Groupes séparables et infinitésimaux

Soit $\bar{k}$ une clôture algébrique de k; on notera $\mathfrak{G}$ le groupe des k-automorphismes de $\bar{k}$, et l'on étendra la terminologie de module de Galois au cas d'un groupe non commutatif sur lequel $\mathfrak{G}$ opère de manière que le stabilisateur de tout point soit ouvert dans $\mathfrak{G}$. Enfin, rappelons qu'une algèbre commutative E de rang fini sur k est dite séparable si elle est composée directe d'extensions algébriques séparables du corps k.

Soit G un groupe formel. On dit que G est *séparable* si, pour toute algèbre commutative A et tout g dans G_A, il existe une

algèbre E séparable de rang fini, h dans G_E et un homomorphisme σ de E dans A tels que $g = G(\sigma) \cdot h$. Supposons G séparable; le groupe $G_{\bar{k}}$ est alors un module de Galois pour $\mathfrak{G}$, et le foncteur qui associe $G_{\bar{k}}$ à G est une équivalence de la catégorie des groupes formels séparables sur la catégorie des modules de Galois pour $\mathfrak{G}$. Lorsque k est algébriquement clos, d'où $\bar{k} = k$ et $\mathfrak{G} = (1)$, on explicite comme suit les groupes G_A en fonction de $\Gamma = G_k$. Dans l'algèbre du groupe Γ à coefficients dans A, on considère les éléments de la forme $\Sigma_\gamma e_\gamma . \gamma$ où les e_γ sont des idempotents de A, deux à deux orthogonaux, nuls sauf un nombre fini, et de somme 1. Pour la multiplication de l'algèbre du groupe Γ, ces éléments forment un groupe, qui est isomorphe de manière naturelle à G_A; en particulier, si tout idempotent de A est égal à 0 ou 1, le groupe G_A est isomorphe à Γ.

On dira que le groupe formel G est *infinitésimal* si le groupe $G_{\bar{k}}$ est réduit à son élément neutre e; dans ce cas, $O(G)$ est un anneau local admettant pour idéal maximal $\mathfrak{m}$ l'ensemble des fonctions f telles que $f_{\bar{k}}(e) = 0$. On dira que G est infinitésimal de type fini si l'idéal $\mathfrak{m}$ est engendré par un nombre fini d'éléments; il revient au même de supposer que l'espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$ est de dimension finie; s'il en est ainsi, les idéaux $\mathfrak{m}^n$ forment un système fondamental de voisinages de 0 dans $O(G)$.

Théorème 2. *Soit* G *un groupe formel sur un corps parfait* k.

a) *On peut décomposer* G *de manière unique sous forme de produit semi-direct* $G^s \times G^i$ *d'un sous-groupe séparable* G^s *et d'un sous-groupe invariant infinitésimal* G^i.

b) *Supposons* G *infinitésimal de type fini et* k *de caractéristique nulle. Alors l'algèbre topologique* $O(G)$ *est isomorphe à une algèbre de séries formelles* $k[[T_1, \ldots, T_r]]$.

c) *Supposons* G *infinitésimal de type fini et* k *de caractéristique* $p \neq 0$. *L'algèbre topologique* $O(G)$ *est isomorphe à une algèbre de séries formelles tronquées* $k[[T_1, \ldots, T_{r+s}]]/(T_{r+1}^{p^{n_1}}, \ldots, T_{r+s}^{p^{n_s}})$ (avec $r \geqslant 0$, $s \geqslant 0$, $n_i \geqslant 0$).

La démonstration de a) repose sur le théorème classique qu'une algèbre de rang fini sur un corps parfait est somme directe d'une sous-algèbre séparable et d'un idéal nilpotent. L'assertion b) est une conséquence du théorème de structure de l'hyperalgèbre d'un groupe infinitésimal qui sera donné au n° suivant; quant à l'asser-

tion c), elle se démontre de manière fort laborieuse en utilisant toute la technique de Dieudonné pour les hyperalgèbres.

Les groupes formels étudiés par Dieudonné sont les groupes infinitésimaux pour lesquels l'algèbre $O(G)$ est isomorphe à une algèbre de séries formelles à un nombre fini de variables. Choisissons un isomorphisme :

$$\eta : k[[T_1; \ldots, T_r]] \to O(G)$$

et notons u_i la fonction $\eta(T_i)$ sur G. Alors, pour toute algèbre commutative A, l'application $g \to ((u_1)_A(g), \ldots, (u_r)_A(g))$ est une bijection de G_A sur l'ensemble des vecteurs de A^r à coordonnées nilpotentes.

12. Groupes formels et algèbres de Lie

Nous distinguerons deux cas très différents selon que la caractéristique de k est nulle ou non.

Supposons d'abord k de caractéristique nulle. Soit G un groupe formel; dans l'ensemble U(G) des distributions sur G, nous considérerons le sous-espace vectoriel L(G) formé des T telles que :

$$P(T) = T \otimes 1 + 1 \otimes T \tag{17}$$

(«éléments primitifs» au sens des algèbres de Hopf). Si T et T' sont dans L(G), il en est de même de $[T, T'] = TT' - T'T$; par conséquent, L(G) est une algèbre de Lie pour le crochet précédent; c'est l'*algèbre de Lie de* G. Supposons G infinitésimal. On peut définir un isomorphisme naturel d'espaces vectoriels de L(G) sur le dual de $\mathfrak{m}/\mathfrak{m}^2$ (en notant $\mathfrak{m}$ l'idéal maximal de $O(G)$); par suite, G est de type fini si et seulement si l'algèbre de Lie L(G) est de dimension finie.

Théorème 3. *Soit k un corps de caractéristique nulle.*

a) *Si* G *est un groupe infinitésimal sur k, l'algèbre associative* U(G) *est l'algèbre enveloppante universelle* [12] *de l'algèbre de Lie* L(G).

[12] Ceci signifie que toute application linéaire f de L(G) dans une algèbre associative R qui vérifie $f([x, y]) = f(x)f(y) - f(y)f(x)$ se prolonge de manière unique en un homomorphisme d'algèbres de U(G) dans R.

b) *Le foncteur L est une équivalence de la catégorie des groupes infinitésimaux avec la catégorie des algèbres de Lie.*

Le théorème 3, a) implique facilement le théorème 2, b) au moyen du théorème de Poincaré-Birkhoff-Witt (cf. N. Bourbaki [4]).

Soit $\mathfrak{g}$ une algèbre de Lie. On peut construire comme suit un groupe infinitésimal G dont l'algèbre de Lie est isomorphe à $\mathfrak{g}$. Soit A une algèbre commutative et soit $\mathfrak{n}(A)$ l'idéal des éléments nilpotents de A. Sur le produit tensoriel $\mathfrak{g} \otimes \mathfrak{n}(A)$, on définit une structure d'algèbre de Lie par la formule :

$$[x \otimes a, \quad y \otimes b] = [x, y] \otimes ab. \tag{18}$$

Puis, sur l'algèbre de Lie $\mathfrak{g} \otimes \mathfrak{n}(A)$, on définit une structure de groupe au moyen de la formule de Campbell-Hausdorff-Dynkin :

$$x \cdot y = \Sigma(\Sigma_i (p_i + q_i))^{-1} (\Pi_i (-1)^{p_i+q_i} p_i ! \, q_i !)^{-1} \tag{19}$$
$$[\underbrace{x_1, [\ldots, [x_1}_{p_1}, \underbrace{[x_2, [\ldots, [x_2}_{q_1}, [\ldots \underbrace{[x_1, \ldots, [x_1}_{p_m}, x_2] \ldots]$$

la sommation étant étendue à tous les systèmes d'entiers $p_1, \ldots p_m$, $q_1, \ldots, q_m$ avec m quelconque et, ou bien $q_m = 1$, ou bien $p_m = 1$ et $q_m = 0$. On notera G_A le groupe défini par la loi (19) sur l'ensemble $\mathfrak{g} \otimes \mathfrak{n}(A)$; si σ est un homomorphisme de A dans une algèbre B, l'application $I \otimes \sigma$ de $\mathfrak{g} \otimes A$ dans $\mathfrak{g} \otimes B$ induit par restriction un homomorphisme de groupes $G(\sigma)$ de G_A dans G_B (on a noté I l'application identique de $\mathfrak{g}$). Ceci achève la construction de G.

13. Etudions maintenant le cas où k est de caractéristique $p \neq 0$. Soit G un groupe formel. On définit l'algèbre de Lie L(G) comme au n° 12; mais, pour T dans L(G), on a aussi $T^p \in L(G)$, de sorte que L(G) est une p-algèbre de Lie au sens de Jacobson [15]. Lorsque G est commutatif, on peut relier cette p-opération dans L(G) à l'homomorphisme V de G^{φ} dans G; en effet, on peut identifier $L(G^{\varphi})$ à l'algèbre de Lie $L(G)^{\varphi}$; et l'homomorphisme d'algèbres de Lie η de $L(G)^{\varphi}$ dans L(G) induit par V est donné par la formule :

$$\eta(x \otimes T) = x \cdot T^p \qquad (x \in k, \ T \in L(G)) \tag{20}$$

De plus, le théorème 3 a ici l'analogue suivant.

THÉORÈME 4. *Soit k un corps de caractéristique $p \neq 0$.*

a) *Soit* G *un groupe formel sur k. Pour que* G *soit infinitésimal, il faut et suffit que pour toute algèbre* A, *le groupe* G_A *soit réunion des noyaux des homomorphismes* F_A^n *de* G_A *dans* $G_A^{\varphi^n}$.

b) *Soit* G *un groupe formel tel que l'homomorphisme* F *soit trivial. Alors l'algèbre associative* U(G) *est algèbre enveloppante universelle* [13] *de la p-algèbre de Lie* L(G).

c) *Le foncteur* L *est une équivalence de la catégorie des groupes formels pour lesquels l'homomorphisme de Frobenius est trivial avec la catégorie des p-algèbres de Lie.*

Pour l'instant, on ne sait pas généraliser les assertions b) et c) précédentes pour les groupes formels dans lesquels F^n est trivial. La question est liée à une généralisation non commutative du théorème 1, comme le montre la théorie de la dualité.

14. DUALITÉ ENTRE GROUPES ALGÉBRIQUES ET GROUPES FORMELS

Nous considérerons la catégorie C des groupes algébriques commutatifs et la catégorie F des groupes formels commutatifs. Tout d'abord, étant donnés un groupe G dans C et un groupe H dans F, on appelle accouplement de G et H une famille d'applications bilinéaires :

$$u_A : G_A \times H_A \to (G_m)_A$$

(pour toute algèbre commutative A) vérifiant les relations de commutation :

$$u_B(G(\sigma) \cdot g, \quad H(\sigma) \cdot h) = \sigma \cdot u_A(g, h) \tag{21}$$

pour tout homomorphisme d'algèbres σ de A dans B, g dans G_A et h dans H_A. L'ensemble des accouplements de G et H est un groupe commutatif noté Acc (G, H); c'est un bifoncteur contravariant par rapport à G et H.

On peut alors construire deux foncteurs contravariants :

$$D : C \to F \qquad D' : F \to C$$

dont la description importe peu, mais qui sont caractérisés par l'assertion suivantes a).

[13] Cf. remarque [12], mais il faut imposer à f la relation supplémentaire $f(x^p) = f(x)^p$.

a) *Il existe des isomorphismes de* Acc(G, H) *sur* Hom(G, D'(H)) *et sur* Hom (H, D(G)), *fonctoriels par rapport à* G *et* H.

b) *Tout groupe algébrique commutatif* G *est isomorphe à* D'(D(G)) *au moyen d'un certain homomorphisme canonique; de même, tout groupe formel commutatif* H *est isomorphe à* D(D'(H)).

c) *Les foncteurs* D *et* D' *sont des dualités.*

On dit que le groupe formel D(G) est le *dual* du groupe algébrique commutatif G; on cite l'assertion b) sous le nom de théorème de bidualité. Il résulte de la construction explicite de D(G) que l'on a :

$$D(G)_k = \mathrm{Hom}\,(G, G_m). \tag{22}$$

Au moyen de la dualité, on traduit facilement les propriétés des groupes algébriques en propriétés de groupes formels. Par exemple, pour que le groupe algébrique commutatif G soit réductif (resp. unipotent), il faut et suffit que le groupe formel commutatif D(G) soit séparable (resp. infinitésimal).

Supposons k de caractéristique $p \neq 0$. Nous identifierons les groupes formels $D(G^\varphi)$ et $D(G)^\varphi$; ceci étant, la suite d'homomorphismes :

$$G \xrightarrow{F} G^\varphi \xrightarrow{V} G$$

est transformée par le foncteur contravariant D en la suite :

$$D(G) \xleftarrow{V} D(G)^\varphi \xleftarrow{F} D(G)$$

Cette propriété donne une construction plus naturelle de l'homomorphisme V de G^φ dans G au moyen de l'homomorphisme de Frobenius pour les groupes formels et de la dualité.

Si l'on tient compte des théorèmes 1 et 4, on obtient le théorème de structure pour les groupes infinitésimaux commutatifs.

THÉORÈME 5. *Pour tout groupe formel commutatif* G, *posons* :

$$V_n'(G) = \mathrm{Hom}\,(D(W_n), G)$$

Le foncteur V_n' est une équivalence de la catégorie des groupes formels commutatifs pour lesquels F^n *est nul, avec la catégorie des modules à gauche sur l'anneau E_n.*

Moyennant un passage à la limite sur n, le théorème précédent redonne facilement le théorème fondamental de DIEUDONNÉ [10] sur la structure des groupes infinitésimaux commutatifs.

Exemples : 1) Le dual de G_m est le groupe formel séparable associé au groupe des entiers sur lequel le groupe de Galois $\mathfrak{G}$ de $\bar{k}$ sur k opère trivialement.

2) Soit G un groupe algébrique commutatif réductif. Le dual D(G) est le groupe formel séparable associé au module de Galois X(G) défini au n° 5.

3) Soit r un entier $\geqslant 2$; on note μ_r le noyau de l'homomorphisme $r \cdot \delta_{G_m}$ du groupe G_m dans lui-même. C'est un groupe algébrique réductif, dont le dual est le groupe formel séparable associé au groupe additif des entiers modulo r sur lequel le groupe de Galois $\mathfrak{G}$ de $\bar{k}$ sur k opère trivialement.

4) Soit W le groupe formel dual de G_a. Pour toute algèbre commutative A, le groupe W_A est le groupe multiplicatif des polynômes P(T) à coefficients dans A qui vérifient :

$$P(T + T') = P(T) \cdot P(T') \tag{23}$$

(«polynômes multiplicatifs»). Lorsque k est de caractéristique nulle, ces polynômes sont les e^{aT} pour a nilpotent dans A; on peut donc identifier W_A au groupe additif des éléments nilpotents de A. Lorsque k est de caractéristique $p \neq 0$, la forme générale des polynômes multiplicatifs est la suivante :

$$P(T) = \prod_{i>0} \exp\, a_i T^{p^i} \tag{24}$$

avec des a_i nuls sauf un nombre fini d'entre eux, de puissance p-ième nulle, de sorte que les séries exponentielles écrites aient un sens. On peut identifier W_A au groupe additif des vecteurs de Witt $(a_0, a_1, \ldots)$ de longueur infinie dont toutes les coordonnées vérifient $a_i^p = 0$ et sont nulles sauf un nombre fini d'entre elles.

5) Au moyen de l'exponentielle de Hasse-Witt, on peut définir un accouplement de $W_{n,r}$ et $W_{r,n}$ qui définit un isomorphisme de chacun de ces groupes sur le dual de l'autre ($W_{n,r}$ est à la fois un groupe algébrique et un groupe formel).

15. Relations entre groupes algébriques et groupes formels

Elles sont de deux sortes. Tout d'abord, à tout groupe algébrique G, on peut associer un groupe formel $\widehat{G}$, appelé le *complété* de G; le groupe $\widehat{G}_A$ est le sous-groupe de G_A formé des g pour

lesquels il existe une algèbre commutative E de rang fini, h dans G_E et un homomorphisme α de E dans A tels que $g = G(\alpha) \cdot h$; de plus, pour tout homomorphisme d'algèbres σ de A dans B, l'homomorphisme $\widehat{G}(\sigma)$ est la restriction de $G(\sigma)$ à $\widehat{G}_A$. On peut relier cette opération de complétion à l'opération de complétion d'un anneau topologique; pour simplifier, nous supposerons G *de type fini, et k algébriquement clos*. On peut définir la notion de fonction sur un groupe algébrique comme on l'a fait pour les groupes formels; les fonctions sur G forment une algèbre $O(G)$, et pour tout point x du groupe G_k, les fonctions f sur G telles que $f_k(x) = 0$ forment un idéal maximal $\mathfrak{m}_x$ de l'algèbre $O(G)$; d'ailleurs, l'algèbre $O(G)$ a un nombre fini de générateurs, et le théorème des zéros de Hilbert montre que la correspondance $x \to \mathfrak{m}_x$ est une bijection de G_k sur l'ensemble des idéaux maximaux de $O(G)$. Ceci étant, *l'algèbre* $O(\widehat{G})$ *des fonctions sur le groupe formel* $\widehat{G}$ *est isomorphe au produit des anneaux locaux complétés de* $O(G)$ *par rapport aux idéaux premiers* $\mathfrak{m}_x$ (x *parcourant* G_k).

Supposons alors k de caractéristique nulle. En utilisant la décomposition de $\widehat{G}$ en produit semi-direct d'un groupe séparable $\widehat{G}^s$ et d'un groupe infinitésimal $\widehat{G}^i$, on voit que tous les anneaux locaux complétés précédents sont isomorphes à $O(\widehat{G}^i)$; mais, $\widehat{G}^i$ est un groupe infinitésimal de type fini, et d'après le théorème 2, b), l'anneau $O(\widehat{G}^i)$ est isomorphe à un anneau de séries formelles, donc sans élément nilpotent non nul. Comme $O(G)$ est un sous-anneau de $O(\widehat{G})$, il en résulte facilement que l'*anneau* $O(G)$ *n'a pas d'élément nilpotent non nul* (14).

16. Pour qu'un foncteur de la catégorie des algèbres dans la catégorie des groupes soit un groupe algébrique fini, il faut et suffit qu'il vérifie les axiomes (G 2) et (G 3) c'est-à-dire qu'il soit à la fois un groupe algébrique et un groupe formel.

La théorie de la dualité fournit donc une autodualité pour la catégorie des groupes algébriques finis commutatifs; dans ce cas, on a $D(G) = D'(G)$, de sorte que G est isomorphe à $D(D(G))$;

(14) Un raisonnement tout semblable prouve qu'un schéma en groupes de type fini sur un corps de caractéristique nulle est *réduit*

de plus, on peut définir un isomorphisme naturel d'algèbres de U(G) sur $O(D(G))$ et de $O(G)$ sur $U(D(G))$ [15].

Si k est de caractéristique nulle, les groupes algébriques finis sont tous séparables et correspondent aux modules de Galois finis. Si k est parfait de caractéristique $p \neq 0$, tout groupe algébrique *commutatif* fini s'écrit de manière unique sous la forme :

$$G = G^{sr} \times G^{su} \times G^{ir} \times G^{iu}$$

G^{sr} séparable et réductif
G^{su} séparable et unipotent
G^{ir} infinitésimal et réductif
G^{iu} infinitésimal et unipotent.

De plus, G^{sr} correspond à un module de Galois fini d'ordre premier à p, G^{su} à un module de Galois fini d'ordre une puissance de p, G^{ir} est le dual d'un groupe formel correspondant à un module de Galois fini d'ordre une puissance de p; enfin, G^{iu} constitue un morceau irréductible à la théorie de Galois usuelle, mais, par le théorème 5, on peut lui faire correspondre un module de longueur finie sur un anneau dérivé des E_n par passage à la limite. Nous renvoyons pour cette étude à P. GABRIEL [12].

Sans entrer dans la théorie des variétés abéliennes, mentionnons seulement que le noyau d'une isogénie $\alpha : A \to B$ de variétés abéliennes est un groupe algébrique commutatif fini N. Si ${}^t\alpha$ est l'isogénie transposée de α, allant de Pic(B) à Pic(A), on peut montrer que le noyau de ${}^t\alpha$ est isomorphe à D(N) de manière naturelle.

(15) On retrouve donc dans ce cas la définition du dual due à GABRIEL [12].

BIBLIOGRAPHIE

[1] I. BARSOTTI, Abelian Varieties over fields of positive characteristic, *Rend. del Circ. Math. Palermo*, 1956, t.V, pp. 1-25.
[2] I. BARSOTTI, Repartitions on abelian varieties. *Illinois Journ. of Maths*, 1958, t. 2, pp. 43-70.
[3] I. BARSOTTI, Analytical methods for Abelian varietes in positive characteristique, 77-85, ce même volume.
[4] N. BOURBAKI, Groupes et Algèbres de Lie, chapitre I, Actualités Scientifiques et Industrielles n° 1285, Hermann, Paris, 1960.
[5] P. CARTIER, Dualité de Tannaka des groupes et algèbres de Lie, *C.R. Acad. Sciences de Paris*, 1956, t. 242, pp. 322-325.
[6] P. CARTIER, Isogénies des variétés de groupes. *Bull. Soc. Math. de France*, 1959, t. 87, pp. 191-220.
[7] P. CARTIER, Hyperalgèbres et groupes de Lie formels, Séminaire Sophus Lie, 2e année, Secrétariat Mathématique, Paris, 1957.
[8] C. CHEVALLEY, Theory of Lie groups, *Princeton Mathematical Series* n° 8, Princeton, 1946.
[9] C. CHEVALLEY, Théorie des groupes de Lie, Tome II, Actualités Scientifiques et Industrielles, n° 1152, Hermann, Paris, 1951.
[10] J. DIEUDONNÉ, Lie groups et Lie hyperalgebras over a field of characteristic $p > 0$ (IV), *Amer. Journ. of Math.*, t. 77, 1955, pp. 429-452.
[11] J. DIEUDONNÉ, Groupes de Lie et hyperalgèbres sur un corps de caractéristique $p > 0$ (V), *Math. Annalen*, t. 134, 1957, pp. 114-133.
[12] P. GABRIEL, Sur les catégories abéliennes localement noethériennes et leurs applications aux algèbres étudiées par Dieudonné, Séminaire J.-P. SERRE, Collège de France, 1960 (multigraphié).
[13] A. GROTHENDIECK, Sur quelques points d'algèbre homologique, *Tôhoku Math. Journ.*, t. IX, 1957, pp. 119-221.
[14] A. GROTHENDIECK et J. DIEUDONNÉ, Eléments de Géométrie Algébrique, I, II, III, *Publ. Maths. I.H.E.S.*, Presses Universitaires de France, Paris, 1960 et 1961.
[15] N. JACOBSON, Abstract derivations and Lie algebras, *Trans. Amer. Math. Soc.*, t. 42, 1937, pp. 206-224.
[16] O. ORE, Theory of non-commutative polynomials, *Ann. of Maths*, t. 34, 1933, pp. 480-508.
[17] J.-P. SERRE, Groupes proalgébriques, *Publ. Maths. I.H.É.S.* n° 7, Presses Universitaires de France, Paris, 1960.
[18] J.-P. SERRE, Groupes algébriques et corps de classes, *Actualités Scientifiques et Industrielles*, n° 1264, Hermann, Paris, 1959.
[19] A. WEIL, Théorie des points proches sur les variétés différentiables, Colloque de Géométrie différentielle du C.N.R.S., Strasbourg 1953.