Théorèmes de finitude en cohomologie galoisienne

par A. Borel et J.-P. Serre

A Georges de Rham, à l'occasion de son soixantième anniversaire

Introduction

Les propriétés de finitude que nous avons en vue concernent un groupe algébrique G défini sur un corps parfait k. Il s'agit essentiellement de prouver:

(A) la finitude du nombre de classes d'espaces homogènes principaux sur k de G (resp. du nombre de k-formes de G) lorsque k est un corps p-adique et G est linéaire (resp. G est soit linéaire, soit une variété abélienne);

(B) la finitude du nombre de classes d'espaces homogènes principaux sur k de G (resp. du nombre de k-formes de G) qui sont isomorphes à un espace homogène principal donné (resp. isomorphes à G) sur toute complétion k_v de k, lorsque k est un corps de nombres algébriques, et G est linéaire (resp. G est soit linéaire, soit une variété abélienne).

On sait que les classes d'espaces homogènes principaux sur k de G correspondent aux éléments du premier ensemble de cohomologie $H^1(k, G)$. De même, les classes de k-formes de G correspondent aux éléments de $H^1(k, \mathrm{Aut}\, G)$, où $\mathrm{Aut}\, G$ désigne le foncteur des automorphismes de G. Les énoncés (A) et (B) sont donc équivalents à des propriétés de finitude de $H^1(k, G)$ (resp. de $H^1(k, \mathrm{Aut}\, G)$), et c'est sous cette forme qu'ils seront établis (cf. §§ 6, 7).

L'assertion (B) est un cas particulier de (A) lorsque $\mathrm{Aut}\, G$ est lui-même un groupe algébrique linéaire; mais ce n'est pas toujours le cas, comme le montre déjà l'exemple d'un tore G de dimension n, pour lequel $\mathrm{Aut}\, G$ peut être identifié au groupe discret $\mathbf{GL}(n, \mathbf{Z})$. Cela nous a amené à étudier la structure de $\mathrm{Aut}\, G$, lorsque G est linéaire, et à démontrer les propriétés de finitude de H^1 qui nous intéressent directement pour une classe de groupes, que nous appelons de type (ALA), classe qui comprend les groupes algébriques linéaires, leurs groupes d'automorphismes (du moins en caractéristique zéro), et les groupes d'automorphismes des variétés abéliennes. Le résultat en est un article dont la plus grande partie (§§ 1 à 5) est, à notre grand regret, consacrée à des préliminaires variés. Toutefois le lecteur qui ne s'intéresse qu'à la cohomologie des groupes linéaires peut omettre la lecture des §§ 3 à 5; de même, les §§ 4 et 5 sont inutiles pour la discussion des formes de variétés abéliennes.

Le contenu des différents paragraphes est le suivant:

Le § 1 donne les définitions et les principales propriétés des ensembles de cohomologie en dimension 0,1 d'un groupe topologique $\mathbf{g}$, à valeurs dans un groupe discret A sur lequel $\mathbf{g}$ opère continûment. Il s'agit surtout d'établir l'existence de suites exactes, et d'analyser les fibres de certaines applications figurant dans ces suites exactes. Les résultats ne sont guère qu'une transcription de faits connus dans le cas topologique (voir en particulier [8] dont nous nous sommes largement inspirés). Dans la suite, on ne s'intéressera qu'au cas où $\mathbf{g}$ est un groupe de GALOIS; ce cas est discuté dans le § 2, qui contient en outre divers résultats techniques utilisés plus loin.

Les §§ 3 et 4 introduisent trois classes de groupes: les $\mathbf{g}$-*groupes de type arithmétique*, groupes isomorphes à un sous-groupe d'indice fini du groupe d'unités $G_{\mathbf{Z}}$ d'un groupe algébrique linéaire G défini sur $\mathbf{Q}$, sur lequel le groupe profini $\mathbf{g}$ opère au moyen d'automorphismes; les *groupes localement algébriques sur* k, extensions de groupes discrets par des groupes algébriques; enfin, les *groupes de type* (ALA), extensions de $\mathbf{g}$-groupes de type arithmétique par des groupes linéaires algébriques.

Le § 4 donne en outre un critère pour que le foncteur d'automorphismes d'une variété algébrique (ou d'un groupe algébrique) soit localement algébrique. Ce critère est utilisé au § 5 pour montrer que, si G est un groupe algébrique linéaire défini sur un corps de caractéristique zéro, Aut G est un groupe de type (ALA). *Grosso modo*, on peut dire que la partie algébrique de Aut G est formée des automorphismes qui agissent trivialement sur le plus grand tore central S de la composante neutre de G, et que le quotient de type arithmétique correspond à l'image de Aut G dans Aut S.

Le § 6 prouve la finitude de $H^1(k, A)$ lorsque A est de type (ALA) et que k est p-adique, ou plus généralement, k est un corps parfait n'ayant qu'un nombre fini d'extensions de degré donné. Parmi les applications signalons, outre (A), la finitude du nombre de classes de conjugaison de sous-groupes de CARTAN définis sur k dans un groupe linéaire G, ainsi que la finitude du nombre des orbites de $G(k)$ opérant dans l'ensemble des points à valeurs dans k d'un espace homogène de G. Enfin, le § 7 traite le cas global. Dans les deux cas, on procède par «dévissage». Les démonstrations utilisent notamment deux résultats, qui sont conséquences de l'existence de domaines fondamentaux convenables pour les groupes d'unités: la finitude du nombre de classes de conjugaison de sous-groupes finis d'un groupe de type arithmétique, et le cas particulier de (B) où G est réductif connexe, et où les espaces homogènes principaux considérés ont des points à valeurs dans toutes les complétions de k.

Notations

Si k est un corps, on note $\bar{k}$ (resp. k_s) une clôture algébrique (resp. une clôture séparable) de k.

Si k' est une extension galoisienne d'un corps k, on note $\mathbf{g}(k'/k)$ le groupe de GALOIS de cette extension; c'est un groupe profini (i. e. compact totalement discontinu).

§ 1. Cohomologie non commutative

Dans tout ce paragraphe, la lettre $\mathbf{g}$ désigne un *groupe topologique*. Le lecteur qui ne s'intéresse qu'aux applications à la cohomologie galoisienne pourra supposer que $\mathbf{g}$ est *profini*.

1.1. g-ensembles. Un $\mathbf{g}$-ensemble est un espace topologique *discret* E sur lequel $\mathbf{g}$ opère à gauche de façon continue (i. e. de telle sorte que le groupe de stabilité de tout point de E soit ouvert dans $\mathbf{g}$). Le transformé de $x \in E$ par $s \in \mathbf{g}$ sera noté $s(x)$, $s \cdot x$ ou encore ${}^s x$ (mais jamais x^s pour éviter l'horrible formule $x^{(st)} = (x^t)^s$). Si E et E' sont deux $\mathbf{g}$-ensembles, un *morphisme* de E dans E' est une application $f : E \to E'$ qui commute aux opérations de $\mathbf{g}$. Les $\mathbf{g}$-ensembles forment une catégorie.

Si E est un $\mathbf{g}$-ensemble, on note $H^0(\mathbf{g}, E)$, ou $E^{\mathbf{g}}$, l'ensemble des $x \in E$ tels que ${}^s x = x$ pour tout $s \in \mathbf{g}$. On dit que c'est le *0-ième ensemble de cohomologie de* $\mathbf{g}$ *à valeurs dans* E.

1.2. g-groupes. Un $\mathbf{g}$-groupe A est un groupe dans la catégorie des $\mathbf{g}$-ensembles. En d'autres termes, c'est un $\mathbf{g}$-ensemble qui est muni d'une structure de groupe invariante par $\mathbf{g}$; on a donc ${}^s(xy) = {}^s x \, {}^s y$ pour $x, y \in A$ et $s \in \mathbf{g}$. Un $\mathbf{g}$-groupe commutatif est parfois appelé un $\mathbf{g}$-*module*.

Soit A un $\mathbf{g}$-groupe. On appelle *cochaîne de* $\mathbf{g}$ *à valeurs dans* A toute application continue $s \mapsto a_s$ de $\mathbf{g}$ dans A. On appelle *cocycle de* $\mathbf{g}$ *à valeurs dans* A toute cochaîne $a = (a_s)$ qui vérifie l'identité:

$$a_{st} = a_s \cdot {}^s a_t \quad (s, t \in \mathbf{g}) . \tag{1}$$

Si une application $a : s \mapsto a_s$ vérifie (1), on a:

$$a_1 = 1 , \; a_s \cdot {}^s a_{s^{-1}} = 1 \quad (s \in \mathbf{g}) . \tag{2}$$

L'ensemble $\mathbf{h}$ des éléments $s \in \mathbf{g}$ tels que $a_s = 1$ est donc un sous-groupe, et l'on a $a_{sh} = a_s$ pour $s \in \mathbf{g}$, $h \in \mathbf{h}$. Il s'ensuit que a est continue si et seulement si $\mathbf{h}$ est ouvert.

L'ensemble des cocycles de $\mathfrak{g}$ à valeurs dans A est noté $Z^1(\mathfrak{g}, A)$. Deux cocycles x, $y \in Z^1(\mathfrak{g}, A)$ sont dits *cohomologues* s'il existe $a \in A$ tel que $x_s = a^{-1} y_s {}^s a$ pour tout $s \in \mathfrak{g}$. C'est là une relation d'équivalence dans $Z^1(\mathfrak{g}, A)$; l'ensemble quotient est noté $H^1(\mathfrak{g}, A)$; on l'appelle le *premier ensemble de cohomologie de* $\mathfrak{g}$ *à valeurs dans* A. Si A est commutatif, $H^1(\mathfrak{g}, A)$ est un groupe commutatif, le produit étant défini à partir du produit des valeurs de cocycles représentatifs. Dans le cas général, $H^1(\mathfrak{g}, A)$ est seulement un *ensemble pointé*: il contient un élément distingué, la classe du cocycle unité; les cocycles appartenant à cette classe sont appelés *cobords*; ils sont de la forme $s \mapsto c^{-1} \cdot {}^s c$, avec $c \in A$. L'élément distingué de $H^1(\mathfrak{g}, A)$ sera noté indifféremment 0 ou 1.

Lorsque $\mathfrak{g}$ est profini, $H^1(\mathfrak{g}, A)$ s'identifie canoniquement à la limite inductive des $H^1(\mathfrak{g}/\mathfrak{h}, A^{\mathfrak{h}})$, pour $\mathfrak{h}$ parcourant l'ensemble des sous-groupes ouverts distingués de $\mathfrak{g}$.

1.3. Fonctorialités. Soient $\mathfrak{g}$ et $\mathfrak{g}'$ deux groupes topologiques, E un $\mathfrak{g}$-ensemble et E' un $\mathfrak{g}'$-ensemble. Un homomorphisme continu $\lambda : \mathfrak{g} \to \mathfrak{g}'$ et une application $\mu : E' \to E$ seront dits *compatibles* si l'on a

$$\mu(\lambda(s) \cdot x') = s \cdot \mu(x') \quad \text{pour} \quad s \in \mathfrak{g},\ x' \in E'.$$

Il est clair que μ applique alors $E'^{\mathfrak{g}'}$ dans $E^{\mathfrak{g}}$, ce qui définit une application

$$(\lambda, \mu)_*^0 : H^0(\mathfrak{g}', E') \to H^0(\mathfrak{g}, E).$$

Supposons de plus que E (resp. E') soit un $\mathfrak{g}$-groupe (resp. un $\mathfrak{g}'$-groupe) et que μ soit un homomorphisme. Soit $a' = (a'_{s'}) \in Z^1(\mathfrak{g}', E')$, et soit $a_s = \mu(a'_{\lambda(s)})$. On vérifie tout de suite que $a = (a_s)$ est un élément de $Z^1(\mathfrak{g}, E)$. De plus, l'application $(\lambda, \mu)_*^1 : Z^1(\mathfrak{g}', E') \to Z^1(\mathfrak{g}, E)$ ainsi définie est compatible avec les relations d'équivalence de ces deux ensembles, d'où, par passage aux quotients, une application de $H^1(\mathfrak{g}', E')$ dans $H^1(\mathfrak{g}, E)$ qui sera encore notée $(\lambda, \mu)_*^1$.

Lorsque $\mathfrak{g} = \mathfrak{g}'$ et que λ est l'identité, on écrit μ_*^i pour $(\lambda, \mu)_*^i$, $i = 0, 1$.

Autre cas particulier: E a même ensemble sous-jacent que E', et $\mathfrak{g}$ opère sur E par la formule $s(x) = \lambda(s) \cdot x$; on écrit alors $E = \lambda^* E'$, et l'on peut prendre pour μ l'application identique. Si en outre λ est l'inclusion d'un sous-groupe (resp. la projection de $\mathfrak{g}$ sur un groupe quotient), $(\lambda, \mu)_*^1$ est appelée l'application de *restriction* (resp. d'*inflation*), et on la note Res (resp. Inf).

1.4. Torsion. Soient A un $\mathfrak{g}$-groupe et E un $\mathfrak{g}$-ensemble. On dit que A opère sur E à gauche, de facon compatible avec $\mathfrak{g}$, si l'on s'est donné une application $(a, x) \mapsto a \cdot x$ de $A \times E$ dans E vérifiant les conditions suivantes:

$$^s(a \cdot x) = {}^s a \cdot {}^s x \quad (a \in A,\ s \in \mathbf{g},\ x \in E) \tag{3}$$

$$a \cdot (b \cdot x) = (a \cdot b) \cdot x\,, \quad 1 \cdot x = x \quad (a, b \in A,\ x \in E)\,. \tag{4}$$

Soit alors $a = (a_s) \in Z^1(\mathbf{g}, A)$. Pour tout $s \in \mathbf{g}$ et tout $x \in E$, posons:

$$^{s'}x = a_s \cdot {}^s x\,.$$

On vérifie immédiatement que cette formule définit une nouvelle opération de $\mathbf{g}$ sur E, et que cette opération est continue. Le $\mathbf{g}$-ensemble ainsi obtenu est noté E_a. On dit que E_a *s'obtient en tordant* E *au moyen du cocycle* a. Il a même ensemble sous-jacent que E.

Si $b = (b_s) \in Z^1(\mathbf{g}, A)$ est cohomologue à a, le $\mathbf{g}$-ensemble E_b est isomorphe à E_a. En effet, soit $c \in A$ tel que $b_s = c^{-1} a_s {}^s c$. On a alors

$$c \cdot (b_s {}^s x) = a_s \cdot {}^s (c \cdot x) \qquad (s \in \mathbf{g},\ x \in E)\,,$$

ce qui montre que l'application $x \mapsto c \cdot x$ est un $\mathbf{g}$-isomorphisme de E_b sur E_a. [On notera cependant qu'il n'y a pas en général d'isomorphisme *canonique* entre E_a et E_b, et par suite il n'est pas possible *d'identifier* ces deux ensembles, ni de définir un «E_α» pour $\alpha \in H^1(\mathbf{g}, A)$.]

L'opération de torsion jouit d'un certain nombre de propriétés élémentaires:

(a) E_a est fonctoriel en E (pour des A-morphismes $E \to E'$).

(b) On a $(E \times E')_a = E_a \times E'_a$.

(c) Si un $\mathbf{g}$-groupe B opère à droite sur E (de façon à commuter à l'action de A), B opère aussi sur E_a.

(d) Si E est muni d'une structure de $\mathbf{g}$-groupe, et si les éléments de A définissent des automorphismes de E, E_x est un $\mathbf{g}$-groupe. Ceci s'applique notamment au cas $E = A$, le groupe A opérant sur lui-même par *automorphismes intérieurs*. On a alors:

$$^{s'}x = a_s {}^s x a_s^{-1} \quad (s \in \mathbf{g},\ x \in A)$$

et $(A_a)^{\mathbf{g}}$ est l'ensemble des $x \in A$ tels que $a_s {}^s x = x a_s$. La cohomologie du groupe tordu A_a est isomorphe à celle de A. Plus précisément:

1.5. Proposition. *Soit* $a = (a_s) \in Z^1(\mathbf{g}, A)$ *et soit* A_a *le* $\mathbf{g}$*-groupe obtenu en tordant* A *au moyen de* a (le groupe A opérant sur lui-même par automorphismes intérieurs). *Si* $b = (b_s) \in Z^1(\mathbf{g}, A_a)$, *on a* $(b_s a_s) \in Z^1(\mathbf{g}, A)$, *et l'on obtient ainsi une bijection*

$$t_a : Z^1(\mathbf{g}, A_a) \to Z^1(\mathbf{g}, A)\,.$$

Par passage au quotient, t_a *définit une bijection*

$$\tau_a : H^1(\mathbf{g}, A_a) \to H^1(\mathbf{g}, A)\,,$$

qui transforme l'élément neutre de $H^1(\mathbf{g}, A_a)$ *en la classe* α *de* a.

Puisque $(b_s) \in Z^1(\mathbf{g}, A_a)$, on a $b_{st} = b_s{}^{s'}b_t = b_s a_s{}^s b_t a_s^{-1}$, d'où

$$b_{st}a_{st} = b_s a_s{}^s b_t a_s^{-1} \cdot a_s{}^s a_t = b_s a_s{}^{\cdot s}(b_t a_t),$$

ce qui montre bien que $(b_s a_s)$ appartient à $Z^1(\mathbf{g}, A)$. Il est alors immédiat que t_a est une bijection. Le fait que t_a, ainsi que son inverse, soit compatible avec la relation «être cohomologues» se vérifie par un calcul analogue.

Exemple: $a^{-1} = (a_s^{-1})$ appartient à $Z^1(\mathbf{g}, A_a)$, et l'on a $t_a(a^{-1}) = 1$.

Remarque. Lorsque A est *abélien*, on a $A_a = A$, et τ_a est la *translation* par la classe α de a.

1.6. Transitivité de l'opération de torsion. Soient A un g-groupe et E un g-ensemble. Supposons que A opère à gauche sur E, de façon compatible avec $\mathbf{g}$ (cf. n° 1.4). Soit $a \in Z^1(\mathbf{g}, A)$. On peut tordre à la fois A (comme au n° précédent) et E au moyen du cocycle a. Le g-groupe A_a *opère sur* E_a de façon compatible avec $\mathbf{g}$:

$$^{s'}(a \cdot x) = a_s{}^s(a \cdot x) = a_s{}^s a^s x = a_s{}^s a a_s^{-1} a_s x = {}^{s'}a \cdot {}^{s'}x\ .$$

Si $b \in Z^1(\mathbf{g}, A_a)$, on peut donc *tordre* E_a *au moyen de* b ; il est immédiat que le résultat $(E_a)_b$ est simplement $E_{t_a(b)}$ (les notations étant celles de la prop. 1.5). En particulier $(E_a)_{a^{-1}} = E$.

1.7. Espaces homogènes principaux. Soit A un g-groupe. Un espace homogène principal (à droite) sur A est un g-ensemble non vide P, sur lequel A opère à droite (de façon compatible avec $\mathbf{g}$), et qui vérifie la condition suivante:

Pour tout couple $(x, y) \in P \times P$, il existe un élément $a \in A$ et un seul tel que $x = y \cdot a$. (On dit encore que A opère de façon *simplement transitive* sur P.)

La notion *d'isomorphisme* de deux espaces homogènes principaux se définit de manière évidente. Un espace homogène principal P est dit *trivial* s'il est isomorphe à A (opérant sur lui-même par translations à droite); il revient au même de dire que $P^{\mathbf{g}}$ est non vide.

Soit P un espace homogène principal, et soit $x \in X$. Pour tout $s \in \mathbf{g}$, il existe un élément unique $a_s \in A$ tel que ${}^s x = x \cdot a_s$. On a:

$$^{st}x = {}^s(x \cdot a_t) = {}^s x \cdot a_s{}^s a_t\ ,$$

d'où $a_{st} = a_s{}^s a_t$; de plus, (a_s) ne dépend que de la classe à gauche de s modulo le groupe de stabilité de x. Il s'ensuit que $a = (a_s)$ appartient à $Z^1(\mathbf{g}, A)$. Si x est remplacé par $x \cdot c$, avec $c \in A$, le cocycle a_s est remplacé par le

cocycle cohomologue $c^{-1}a_s{}^s c$. On a donc associé à P un élément bien déterminé $\varepsilon(P)$ de $H^1(\mathfrak{g}, A)$.

1.8. Proposition. *Soit $P(A)$ l'ensemble des classes d'isomorphisme d'espaces homogènes principaux sur A. L'application*

$$\varepsilon : P(A) \to H^1(\mathfrak{g}, A)$$

définie ci-dessus est une bijection.

Montrons que ε est *injective*: soient $P, Q \in P(A)$ tels que $\varepsilon(P) = \varepsilon(Q)$. D'après ce qui précède, on peut choisir des points $x \in P$, $y \in Q$ correspondant au même cocycle (a_s). On vérifie alors immédiatement que l'application $x \cdot a \mapsto y \cdot a$ est un isomorphisme de P sur Q.

Montrons que ε est *surjective*. Soit $a \in Z^1(\mathfrak{g}, A)$, et soit X l'espace homogène principal trivial A. Le groupe A opère par translations *à gauche* sur X. Soit X_a l'espace obtenu en tordant X au moyen de a. On a ${}^{s'}x = a_s{}^s x$ pour tout $x \in X_a$. Si l'on fait opérer A sur X_a au moyen des translations *à droite*, il est immédiat que l'on obtient un espace homogène principal. De plus, le cocycle associé à l'élément unité $1 \in X_a$ n'est autre que a. Cela montre bien que ε est surjective.

Remarque. En fait, la démonstration précédente prouve que les éléments de $Z^1(\mathfrak{g}, A)$ correspondent bijectivement aux *classes de couples* (P, x) où P est un espace homogène principal sur A, et x un point de P.

1.9. Relations entre torsion et espaces homogènes principaux.

Soit A un $\mathfrak{g}$-groupe, soit P un espace homogène principal sur A, et soit E un $\mathfrak{g}$-ensemble sur lequel A opère à gauche (de façon compatible avec $\mathfrak{g}$). Sur $P \times E$, considérons la relation d'équivalence qui identifie un couple (p, x) aux couples $(p \cdot a, a^{-1} \cdot x)$, $a \in A$. Cette relation est compatible avec l'action de $\mathfrak{g}$, et le quotient est un $\mathfrak{g}$-ensemble, que nous noterons $P \times^A E$, ou encore E_P. Un élément de $P \times^A E$ s'écrit sous la forme $p \cdot x$, $p \in P$, $x \in E$ et l'on a $(pa) \cdot x = p(ax)$ pour tout $a \in A$, ce qui justifie la notation. Pour tout $p \in P$ l'application $x \mapsto p \cdot x$ est une bijection de E sur E_P; on dit que E_P est obtenu *en tordant E au moyen de P*.

La liaison avec le point de vue du n° 1.4 est facile à faire: si $p \in P$, on a vu au n° 1.7 que p définit un cocycle (a_s) tel que ${}^s p = p a_s$. La bijection $x \mapsto p \cdot x$ introduite ci-dessus est alors un *isomorphisme du $\mathfrak{g}$-ensemble E_a sur le $\mathfrak{g}$-ensemble E_P*. On a en effet:

$$p \cdot {}^{s'}x = p \cdot a_s{}^s x = {}^s p \cdot {}^s x = {}^s(p \cdot x) .$$

1.10. Utilisation de la torsion. Soient A et B deux g-groupes, et soit $u : A \to B$ un g-homomorphisme (i. e. un homomorphisme compatible avec l'action de g sur A et B). On a vu au n° 1.3 que u définit une application d'ensembles pointés

$$v = u^1_* : H^1(\mathfrak{g}, A) \to H^1(\mathfrak{g}, B) .$$

Soit $\alpha \in H^1(\mathfrak{g}, A)$, et proposons-nous de décrire la *fibre* de v passant par α, i. e. l'ensemble $v^{-1}(v(\alpha))$. Soit $a \in Z^1(\mathfrak{g}, A)$ un représentant de α, et soit b son image dans B. L'homomorphisme u définit un g-homomorphisme

$$u_a : A_a \to B_b ,$$

d'où une application $v_a = u^1_{a*} : H^1(\mathfrak{g}, A_a) \to H^1(\mathfrak{g}, B_b)$.

Considérons le diagramme suivant (où les lettres τ_a et τ_b désignent les bijections définies dans la prop. 1.5):

$$\begin{array}{ccc} H^1(\mathfrak{g}, A_a) & \xrightarrow{v_a} & H^1(\mathfrak{g}, B_b) \\ \tau_a \downarrow & & \tau_b \downarrow \\ H^1(\mathfrak{g}, A) & \xrightarrow{v} & H^1(\mathfrak{g}, B) . \end{array}$$

On vérifie immédiatement que ce diagramme est *commutatif*. Comme τ_b transforme l'élément neutre de $H^1(\mathfrak{g}, B_b)$ en $v(\alpha)$, on en déduit que τ_a *induit une bijection du noyau de* v_a *sur la fibre* $v^{-1}(v(\alpha))$. En d'autres termes, la torsion permet de transformer toute fibre de v en un *noyau*; ce procédé de réduction sera utilisé plusieurs fois dans la suite.

1.11. Suite exacte associée à un sous-groupe. Soit B un g-groupe, et soit A un sous-g-groupe de B. Soit B/A l'espace homogène des classes à gauche de B suivant A ; c'est un g-ensemble, et $H^0(\mathfrak{g}, B/A)$ est défini. On notera $i : A \to B$ et $p : B \to B/A$ les applications canoniques évidentes. De plus, si $x \in H^0(\mathfrak{g}, B/A)$, l'image réciproque X de x dans B est un espace homogène principal sur A ; sa classe dans $H^1(\mathfrak{g}, A)$ sera noté $\delta(x)$. Si $b \in B$ est tel que $p(b) = x$, on a $b^{-1} \cdot {}^s b = a_s \in A$ pour tout $s \in \mathfrak{g}$, et il est clair que $a = (a_s)$ est un cocycle appartenant à la classe de $\delta(x)$. Avec ces notations, on a:

1.12. Proposition. *Soit A un sous-g-groupe de B. La suite d'applications d'ensembles pointés:*

$$0 \to H^0(\mathfrak{g}, A) \xrightarrow{i^0_*} H^0(\mathfrak{g}, B) \xrightarrow{p^0_*} H^0(\mathfrak{g}, B/A) \xrightarrow{\delta} H^1(\mathfrak{g}, A) \xrightarrow{i^1_*} H^1(\mathfrak{g}, B)$$

est exacte. De plus, δ induit une bijection de l'ensemble des orbites de $B^{\mathfrak{g}}$ dans $(B/A)^{\mathfrak{g}}$ sur le noyau de i^1_*.

(On rappelle qu'une suite d'applications d'ensembles pointés:

$$\ldots \to X_{n-1} \to X_n \to X_{n+1} \to \ldots$$

est dite *exacte* si l'image réciproque de l'élément neutre de X_{n+1} est égale à l'image de X_{n-1} dans X_n.)

Il est clair que i_*^0 est injectif, et que le noyau de p_*^0 est égal à l'image de i_*^0. Par définition, le noyau de δ est formé des éléments $x \in (B/A)^{\mathfrak{g}}$ dont l'image réciproque X dans B contient un point invariant par $\mathfrak{g}$; on a donc bien $\mathrm{Ker}(\delta) = \mathrm{Im}(p_*^0)$. L'inclusion $\mathrm{Im}(\delta) \subset \mathrm{Ker}(i_*^1)$ résulte de la définition de δ au moyen de cocycles; pour prouver l'inclusion réciproque, soit $\alpha \in \mathrm{Ker}(i_*^1)$, et soit $a \in Z^1(\mathfrak{g}, A)$ un représentant de α. Puisque $\alpha \in \mathrm{Ker}(i_*^1)$, il existe $b \in B$ tel que $a_s = b^{-1} \cdot {}^s b$ pour tout $s \in \mathfrak{g}$; si $x = p(b) \in B/A$, il est clair que x est invariant par $\mathfrak{g}$, et que $\delta(x) = \alpha$. Cela achève de prouver l'exactitude de la suite considérée.

Soient maintenant $x, y \in (B/A)^{\mathfrak{g}}$; il nous faut prouver que $\delta(x) = \delta(y)$ si et seulement si x et y sont dans la même orbite de $B^{\mathfrak{g}}$. Supposons d'abord que $\delta(x) = \delta(y)$. On peut alors trouver des représentants b, c de x, y dans B tels que:

$$b^{-1} \cdot {}^s b = a_s = c^{-1} \cdot {}^s c \quad (s \in \mathfrak{g},\ a_s \in A)\,.$$

On en déduit $bc^{-1} = {}^s(bc^{-1})$, d'où $bc^{-1} \in B^{\mathfrak{g}}$; comme l'élément bc^{-1} transforme y en x, on voit bien que x et y appartiennent à la même orbite. La réciproque se démontre par un calcul analogue.

1.13. Corollaire. *Soit $a \in Z^1(\mathfrak{g}, A)$, et soit α la classe de a dans $H^1(\mathfrak{g}, A)$. Les éléments de $H^1(\mathfrak{g}, A)$ qui ont même image que α dans $H^1(\mathfrak{g}, B)$ correspondent bijectivement aux orbites du groupe $(B_a)^{\mathfrak{g}}$ opérant dans $(B_a/A_a)^{\mathfrak{g}}$.*

Cela résulte par *torsion* de la proposition précédente (cf. n° 1.10).

Remarque. On vérifie immédiatement que l'espace homogène B_a/A_a peut être identifié au g-ensemble $(B/A)_a$ obtenu en tordant l'espace homogène B/A grâce au cocycle a (le groupe A opérant sur B/A par translations à gauche).

1.14. Si $f: X \to Y$ est une application, nous dirons que f est *propre* si l'image réciproque de tout point de Y par f est finie. (Cela revient à dire que f est une application propre au sens topologique lorsqu'on munit X et Y de la topologie discrète.)

Corollaire. *Pour que $i_*^1 : H^1(\mathfrak{g}, A) \to H^1(\mathfrak{g}, B)$ soit propre* (resp. injective), *il faut et il suffit que, pour tout $a \in Z^1(\mathfrak{g}, A)$, les orbites de $(B_a)^{\mathfrak{g}}$ dans $(B_a/A_a)^{\mathfrak{g}}$ soient en nombre fini* (resp. que $(B_a)^{\mathfrak{g}}$ opère transitivement sur $(B_a/A_a)^{\mathfrak{g}}$).

Cela résulte immédiatement du corollaire 1.13.

L'image de i_*^1 est donnée par le résultat suivant:

1.15. Proposition. *Soit $b = (b_s) \in Z^1(\mathfrak{g}, B)$ et soit β la classe de b dans $H^1(\mathfrak{g}, B)$. Pour que β appartienne à l'image de*

$$i_*^1 : H^1(\mathfrak{g}, A) \to H^1(\mathfrak{g}, B),$$

il faut et il suffit que le $\mathfrak{g}$*-ensemble* $(B/A)_b$ *obtenu en tordant* B/A *au moyen de* b *ait un point invariant par* $\mathfrak{g}$.

(Bien entendu, on fait opérer B *à gauche* sur B/A ; c'est ce qui permet de définir $(B/A)_b$.)

Pour que $\beta \in \mathrm{Im}\,(i_*^1)$, il faut et il suffit qu'il existe $b \in B$ tel que $b^{-1} b_s {}^s b$ appartienne à A pour tout $s \in \mathfrak{g}$. Si l'on pose $p(b) = c$, cela revient à dire que $c = b_s {}^s c$ dans B/A, ou encore que $c \in H^0(\mathfrak{g}, (B/A)_b)$, d'où la proposition.

Remarque. D'après le n° 1.6, le groupe tordu B_b opère à gauche sur $(B/A)_b$, et il est clair qu'il opère transitivement.

1.16. Suite exacte associée à une extension de $\mathfrak{g}$-groupes.

Soit B un $\mathfrak{g}$-groupe, soit A un sous-$\mathfrak{g}$-groupe distingué de B, et soit C le $\mathfrak{g}$-groupe quotient. Comme au n° 1.11, nous noterons i l'injection canonique de A dans B, et p la projection $B \to C$. On a donc une *suite exacte de* $\mathfrak{g}$*-groupes*

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0 .$$

Nous allons voir que le groupe $C^{\mathfrak{g}}$ *opère canoniquement à droite sur* $H^1(\mathfrak{g}, A)$. Soit donc $c \in C^{\mathfrak{g}}$, et soit $b \in B$ tel que $p(b) = c$. On a vu au n° 1.11 qu'il existe un cocycle $a = (a_s)$ de A tel que ${}^s b = b \cdot a_s$ pour tout $s \in \mathfrak{g}$. L'application $x \mapsto b^{-1} x b$ est un isomorphisme de A sur le groupe tordu A_a ; cela résulte de la formule :

$$b^{-1} \cdot {}^s x \cdot b = a_s {}^s (b^{-1} x b) \cdot a_s^{-1} .$$

Par passage à la cohomologie, on obtient ainsi une bijection

$$H^1(\mathfrak{g}, A) \to H^1(\mathfrak{g}, A_a).$$

En la composant avec la bijection canonique $\tau_a : H^1(\mathfrak{g}, A_a) \to H^1(\mathfrak{g}, A)$, on obtient une bijection

$$\varrho_b : H^1(\mathfrak{g}, A) \to H^1(\mathfrak{g}, A) .$$

Si ξ est la classe d'un cocycle $x = (x_s)$, $\varrho_b(\xi)$ est la classe du cocycle

$$(b^{-1} x_s b a_s) = (b^{-1} x_s {}^s b).$$

Il est clair que, si $b, b' \in p^{-1}(C^{\mathfrak{g}})$, on a $\varrho_{b'b} = \varrho_b \cdot \varrho_{b'}$; d'autre part, si $b \in A$, ϱ_b est l'identité. Il en résulte que ϱ_b ne dépend que de $p(b) = c$, et on peut le noter ϱ_c ; on a $\varrho_{c'c} = \varrho_c \cdot \varrho_{c'}$, ce qui signifie bien que $C^{\mathfrak{g}}$ opère *à droite* sur $H^1(\mathfrak{g}, A)$.

1.17. Proposition. *Soit* $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ *une suite exacte de* $\mathfrak{g}$*-homomorphismes de* $\mathfrak{g}$*-groupes. Alors* :

(i) *La suite* :

$0 \to H^0(\mathfrak{g}, A) \xrightarrow{i^0_*} H^0(\mathfrak{g}, B) \xrightarrow{p^0_*} H^0(\mathfrak{g}, C) \xrightarrow{\delta} H^1(\mathfrak{g}, A) \xrightarrow{i^1_*} H^1(\mathfrak{g}, B) \xrightarrow{p^1_*} H^1(\mathfrak{g}, C)$ *est exacte.*

(ii) *Si* $c \in C^{\mathfrak{g}}$, *on a* $\delta(c) = \varrho_c(1)$, *en notant* 1 *l'élément neutre de* $H^1(\mathfrak{g}, A)$.

(iii) *L'application* i^1_* *induit une bijection de l'ensemble des orbites de* $C^{\mathfrak{g}}$ *dans* $H^1(\mathfrak{g}, A)$ *sur le noyau de* p^1_*.

(iv) *Soit* $x = (x_s) \in Z^1(\mathfrak{g}, A)$, *et soit* ξ *sa classe dans* $H^1(\mathfrak{g}, A)$. *Soit* $c \in C^{\mathfrak{g}}$. *Pour que* $\varrho_c(\xi) = \xi$, *il faut et il suffit que* c *appartienne à l'image de l'homomorphisme* $(p_x)^0_* : (B_x)^{\mathfrak{g}} \to C^{\mathfrak{g}}$.

(On note B_x le groupe obtenu en tordant B au moyen du cocycle x, étant entendu que A opère sur B par automorphismes intérieurs.) Pour prouver (i), il suffit (vu la prop. 1.12) de montrer que Ker (p^1_*) est égal à Im (i^1_*). L'inclusion Im $(i^1_*) \subset$ Ker (p^1_*) résulte de ce que le composé $p \circ i$ est trivial. Inversement, soit $b = (b_s)$ un cocycle dont la classe β appartient à Ker (p^1_*). Il existe alors $u \in B$ tel que $b_s \equiv u.{}^s u^{-1} \bmod \cdot A$, d'où $u^{-1} b_s {}^s u = a_s \in A$; le cocycle (a_s) a pour classe un élément $\alpha \in H^1(\mathfrak{g}, A)$, et il est clair que $i^1_*(\alpha) = \beta$, ce qui démontre (i). L'assertion (ii) est immédiate sur la définition de ϱ_c. D'autre part, soient $x = (x_s)$ et $x' = (x'_s)$ deux éléments de $Z^1(\mathfrak{g}, A)$ qui sont cohomologues dans B; il existe $b \in B$ tel que $x'_s = b^{-1} x_s {}^s b$ pour tout $s \in \mathfrak{g}$; si $c = p(b)$, on a ${}^s c = c$, d'où $c \in C^{\mathfrak{g}}$. Il est clair que ϱ_c transforme la classe de x en celle de x'; la réciproque se démontre de même, ce qui établit (iii). Enfin, les notations étant celles de (iv), choisissons $b \in p^{-1}(c)$. L'équation $\varrho_c(\xi) = \xi$ équivaut alors à l'existence de $a \in A$ tel que $x_s = a^{-1} b^{-1} x_s {}^s b {}^s a$, ce qui s'écrit encore $ba = x_s {}^s(ba) x_s^{-1}$, ou encore $ba \in (B_x)^{\mathfrak{g}}$; d'où (iv).

1.18. Corollaire. *Soit* $b \in Z^1(\mathfrak{g}, B)$ *et soit* β *la classe de* b *dans* $H^1(\mathfrak{g}, B)$. *Les éléments de* $H^1(\mathfrak{g}, B)$ *qui ont même image que* β *dans* $H^1(\mathfrak{g}, C)$ *correspondent bijectivement aux orbites du groupe* $(C_b)^{\mathfrak{g}}$ *opérant dans* $H^1(\mathfrak{g}, A_b)$.

(Le groupe A_b (resp. C_b) est défini par torsion au moyen de b, le groupe B opérant sur A (resp. C) par restriction (resp. passage au quotient) des automorphismes intérieurs.)

Cela résulte par torsion de la partie (iii) de la proposition précédente.

1.19. Corollaire. *Si* $C^{\mathfrak{g}}$ *et* $H^1(\mathfrak{g}, B)$ *sont finis* (resp. triviaux), *il en est de même de* $H^1(\mathfrak{g}, A)$.

Cela résulte de la partie (iii) de la proposition précédente.

1.20. Corollaire. *Pour que* $p^1_* : H^1(\mathfrak{g}, B) \to H^1(\mathfrak{g}, C)$ *soit propre* (resp. injective), *il faut et il suffit que, pour tout* $b \in Z^1(\mathfrak{g}, B)$, *les orbites de* $(C_b)^{\mathfrak{g}}$ *dans* $H^1(\mathfrak{g}, A_b)$ *soient en nombre fini* (resp. que $(C_b)^{\mathfrak{g}}$ opère transitivement sur $H^1(\mathfrak{g}, A_b)$).

Cela résulte du corollaire 1.18.

Remarque. La condition du corollaire 1.20 est notamment vérifiée lorsque tous les $H^1(\mathfrak{g}, A_b)$ sont finis (resp. nuls).

1.21. Cas d'un sous-groupe abélien distingué.
On garde les notations et hypothèses des n^{os} 1.16 à 1.20, et on suppose en outre que A est *abélien*. On note additivement le groupe $H^1(\mathfrak{g}, A)$. D'autre part, l'homomorphisme $C^{\mathfrak{g}} \to \mathrm{Aut}(A)$ permet de faire opérer $C^{\mathfrak{g}}$ à gauche sur $H^1(\mathfrak{g}, A)$. Nous noterons $c \cdot \alpha$ cette opération $(c \in C^{\mathfrak{g}}, \alpha \in H^1(\mathfrak{g}, A))$.

1.22. Proposition. *Soit B un $\mathfrak{g}$-groupe, soit A un sous-$\mathfrak{g}$-groupe abélien distingué de B, et soit $C = B/A$. On a:*

$$\varrho_c(\alpha) = c^{-1} \cdot \alpha + \delta(c) \quad \textit{pour tout} \quad \alpha \in H^1(\mathfrak{g}, A) \quad \textit{et tout} \quad c \in C^{\mathfrak{g}}.$$

Soit b un élément de B relevant c. On a ${}^s b = b \cdot x_s$, et $x = (x_s)$ est un cocycle de classe $\delta(c)$. D'autre part, si $a = (a_s)$ est un cocycle de classe α, on peut prendre pour représentant de $\varrho_c(\alpha)$ le cocycle $b^{-1} a_s {}^s b$, et pour représentant de $c^{-1} \cdot \alpha$ le cocycle $b^{-1} a_s b$. La proposition résulte alors de la formule:

$$b^{-1} a_s {}^s b = b^{-1} a_s b \cdot x_s .$$

1.23. Corollaire. (a) *On a $\delta(c'c) = \delta(c) + c^{-1} \cdot \delta(c')$ pour $c, c' \in C^{\mathfrak{g}}$.*

(b) *Si A est contenu dans le centre de B, l'application $\delta : C^{\mathfrak{g}} \to H^1(\mathfrak{g}, A)$ est un homomorphisme, et l'on a $\varrho_c(\alpha) = \alpha + \delta(c)$ pour $c \in C^{\mathfrak{g}}$, $\alpha \in H^1(\mathfrak{g}, A)$.*

Soit $\alpha \in H^1(\mathfrak{g}, A)$. On sait que $\varrho_{c'c}(\alpha) = \varrho_c(\varrho_{c'}(\alpha))$. La proposition 1.22 permet de calculer les deux membres de cette formule. Pour le premier, on trouve $c^{-1} c'^{-1} \alpha + \delta(c'c)$, et pour le second:

$$c^{-1} c'^{-1} \alpha + c^{-1} \delta(c') + \delta(c) .$$

En comparant, on obtient (a). L'assertion (b) résulte immédiatement de 1.22 et de (a).

Remarque. Lorsque $\mathfrak{g}$ est un groupe profini (ou un groupe discret), on peut aller plus loin: on définit pour tout $c \in Z^1(\mathfrak{g}, C)$ un élément $\Delta(c) \in H^2(\mathfrak{g}, A_c)$, et l'on montre que $\Delta(c) = 0$ si et seulement si la classe de c appartient à $\mathrm{Im}\,(p_*^1)$. Comme nous n'aurons pas besoin de ce résultat dans la suite, nous nous bornerons à renvoyer le lecteur à GROTHENDIECK [8], ou à [19], Chap. I, n^{os} 5.6 et 5.7.

1.24. Action des automorphismes intérieurs. Soit A un $\mathfrak{g}$-groupe, et soit $t \in \mathfrak{g}$. Définissons des applications

$$\lambda_t : \mathfrak{g} \to \mathfrak{g} \quad \text{et} \quad \mu_t : A \to A$$

par les formules:

$$\lambda_t(s) = t^{-1} s t , \quad \mu_t(x) = {}^t x .$$

Ces applications sont *compatibles* entre elles, au sens du n° 1.3. Elles définissent donc des applications

$$(\lambda_t, \mu_t)^i_* : H^i(\mathbf{g}, A) \to H^i(\mathbf{g}, A), \quad i = 0,1.$$

1.25. Proposition. *Pour tout* $t \in \mathbf{g}$, $(\lambda_t, \mu_t)^i_*$ *est l'application identique de* $H^i(\mathbf{g}, A)$ *sur lui-même.*

Pour $i = 0$, on a $H^0(\mathbf{g}, A) = A^{\mathbf{g}}$, et si $x \in A^{\mathbf{g}}$, on a $\mu_t(x) = x$. D'où le fait que $(\lambda_t, \mu_t)^0_*$ est l'identité.

Soit maintenant $\alpha \in H^1(\mathbf{g}, A)$, et soit $a = (a_s)$ un cocycle représentant α. La classe de cohomologie $(\lambda_t, \mu_t)^1_*(\alpha)$ est celle du cocycle $b = (b_s)$ défini par la formule:

$$b_s = {}^t(a_{t^{-1}st}).$$

Utilisant le fait que a est un cocycle, on obtient:

$$b_s = {}^t(a_{t^{-1}} \cdot {}^{t^{-1}}a_{st}) = {}^t a_{t^{-1}} \cdot a_{st} = a_t^{-1} \cdot a_{st} = a_t^{-1} \cdot a_s \cdot {}^s a_t,$$

ce qui montre que b_s est cohomologue à a_s, d'où la proposition.

1.26. Conservons les notations des deux n^{os} ci-dessus, et soit $\mathbf{h}$ un *sous-groupe distingué* de $\mathbf{g}$. Si $t \in \mathbf{g}$, l'homomorphisme λ_t applique $\mathbf{h}$ dans lui-même. Les applications

$$\lambda_t : \mathbf{h} \to \mathbf{h}, \quad \mu_t : A \to A$$

sont encore compatibles. On en déduit comme ci-dessus des applications

$$(\lambda_t, \mu_t)^i_* : H^i(\mathbf{h}, A) \to H^i(\mathbf{h}, A)$$

que nous noterons σ_t pour abréger. Il est clair que $\sigma_{tt'} = \sigma_t \circ \sigma_{t'}$. D'autre part, la proposition 1.25, appliquée au groupe $\mathbf{h}$, montre que $\sigma_t = 1$ si $t \in \mathbf{h}$. On peut donc définir σ_t pour $t \in \mathbf{g}/\mathbf{h}$, et l'on voit que $\mathbf{g}/\mathbf{h}$ *opère à gauche sur* $H^i(\mathbf{h}, A)$. Pour $i = 0$, on retrouve les opérations évidentes de $\mathbf{g}/\mathbf{h}$ sur $A^{\mathbf{h}}$.

Remarque. Supposons que tout sous-groupe ouvert de $\mathbf{g}$ contienne un sous-groupe ouvert distingué (ce qui est notamment le cas lorsque $\mathbf{g}$ est *profini*). Alors $\mathbf{g}/\mathbf{h}$ opère *continûment* sur $H^1(\mathbf{h}, A)$. (Bien entendu, $\mathbf{g}/\mathbf{h}$ opère toujours continûment sur $H^0(\mathbf{h}, A)$.)

1.27. Proposition. *Soit* $\mathbf{h}$ *un sous-groupe distingué de* $\mathbf{g}$, *et soit* A *un* $\mathbf{g}$*-groupe. On a alors une suite exacte:*

$$0 \to H^1(\mathbf{g}/\mathbf{h}, A^{\mathbf{h}}) \xrightarrow{\alpha} H^1(\mathbf{g}, A) \xrightarrow{\beta} H^1(\mathbf{h}, A),$$

où α *est l'application associée à la projection* $\mathbf{g} \to \mathbf{g}/\mathbf{h}$ *et à l'inclusion* $A^{\mathbf{h}} \to A$, *et où* β *est la restriction. De plus* α *est injectif et l'image de* β *est contenue dans l'ensemble des éléments de* $H^1(\mathbf{h}, A)$ *invariants par* $\mathbf{g}/\mathbf{h}$ (pour les opérations σ_t définies ci-dessus).

Soient $a = (a_s)$ et $b = (b_s)$ deux cocycles de $\mathbf{g}/\mathbf{h}$ dans $A^{\mathbf{h}}$ qui sont cohomologues dans $Z^1(\mathbf{g}, A)$. Il existe donc $c \in A$ tel que

$$b_s = c^{-1} a_s {}^s c .$$

Si l'on prend s dans $\mathbf{h}$, on a $a_s = b_s = 1$, d'où ${}^s c = c$, ce qui montre que c appartient à $A^{\mathbf{h}}$; les cocycles a et b sont donc cohomologues dans $Z^1(\mathbf{g}/\mathbf{h}, A^{\mathbf{h}})$, ce qui prouve que α est injectif.

L'inclusion $\mathrm{Im}\,(\alpha) \subset \mathrm{Ker}\,(\beta)$ est évidente. Pour prouver l'inclusion opposée, soit $a = (a_s)$ un cocycle de $\mathbf{g}$ dont la restriction à $\mathbf{h}$ est un cobord. Il existe $c \in A$ tel que $a_s = c^{-1} \cdot {}^s c$ si $s \in \mathbf{h}$; quitte à remplacer (a_s) par le cocycle cohomologue $(c^{-1} a_s {}^s c)$, on peut donc supposer que $a_s = 1$ pour $s \in \mathbf{h}$. L'identité $a_{st} = a_s {}^s a_t$ montre alors que a_s ne dépend que de la classe de $s \bmod \cdot \mathbf{h}$, et appartient à $A^{\mathbf{h}}$. Le cocycle a provient donc d'un cocycle de $\mathbf{g}/\mathbf{h}$ à valeurs dans $A^{\mathbf{h}}$, ce qui achève de prouver que $\mathrm{Im}\,(\alpha) = \mathrm{Ker}\,(\beta)$.

Enfin, il est clair que $\beta : H^1(\mathbf{g}, A) \to H^1(\mathbf{h}, A)$ est compatible avec l'action de $\mathbf{g}$ sur ces deux ensembles. D'après la proposition 1.25, $\mathbf{g}$ opère trivialement sur $H^1(\mathbf{g}, A)$. Il opère donc aussi trivialement sur $\mathrm{Im}\,(\beta)$, d'où la proposition.

1.28. Induction. Soit $\mathbf{h}$ un sous-groupe de $\mathbf{g}$, et soit E un $\mathbf{h}$-ensemble. Soit E^* l'ensemble des applications $f : \mathbf{g} \to E$ qui vérifient les deux conditions suivantes:

(a) f est constante sur les classes à gauche modulo un sous-groupe ouvert de $\mathbf{g}$,

(b) $f(h \cdot x) = {}^h(f(x))$ pour $x \in \mathbf{g}$, $h \in \mathbf{h}$.

(Lorsque $\mathbf{g}$ est *profini*, ou *discret*, la condition (a) signifie simplement que f est continue.)

Si $f \in E^*$ et $g \in \mathbf{g}$, soit ${}^g f : \mathbf{g} \to E$ l'application définie par la formule:

$$({}^g f)(x) = f(xg) .$$

On constate sans difficultés que ${}^g f$ vérifie les conditions (a) et (b) et que ${}^g({}^{g'} f) = {}^{(gg')} f$. Le groupe $\mathbf{g}$ opère donc à gauche sur E^*, et la propriété (a) assure que cette opération est continue. Ainsi, E^* est muni d'une structure de $\mathbf{g}$-ensemble; on dit que c'est le $\mathbf{g}$-ensemble *induit* du $\mathbf{h}$-ensemble E. Lorsque E est un $\mathbf{h}$-groupe, E^* est un $\mathbf{g}$-groupe.

D'après (b), l'application $\mu : E^* \to E$ qui associe à tout $f \in E^*$ sa valeur à l'élément neutre est compatible (au sens du n° 1.3) avec l'homomorphisme d'inclusion $\lambda : \mathbf{h} \to \mathbf{g}$.

1.29. Proposition. *Soit $\mathbf{h}$ un sous-groupe de $\mathbf{g}$, soit A un $\mathbf{h}$-groupe, et soit A^* le $\mathbf{g}$-groupe induit correspondant. Supposons que les sous-groupes ouverts distin-*

gués de $\mathbf{g}$ *forment un système fondamental de voisinages de l'élément neutre. Alors les applications*

$$(\lambda, \mu)^i_* : H^i(\mathbf{g}, A^*) \to H^i(\mathbf{h}, A) \quad (i = 0,1)$$

sont bijectives.

Le cas $i = 0$ est trivial (et ne nécessite d'ailleurs aucune hypothèse sur $\mathbf{g}$). Nous supposerons donc que $i = 1$; nous noterons φ l'application de $Z^1(\mathbf{g}, A^*)$ dans $Z^1(\mathbf{h}, A)$ définie par (λ, μ), et Φ l'application correspondante de $H^1(\mathbf{g}, A^*)$ dans $H^1(\mathbf{h}, A)$.

Soit $F = (F_s) \in Z^1(\mathbf{g}, A^*)$. On a:

$$F_s(h \cdot x) = {}^h(F_s(x)) \quad (h \in \mathbf{h},\ x,\ s \in \mathbf{g}), \tag{1}$$

$$F_{st}(x) = F_s(x) \cdot F_t(xs) \quad (s,\ t,\ x \in \mathbf{g}). \tag{2}$$

(3) Il existe un sous-groupe ouvert distingué $\mathbf{n}$ de $\mathbf{g}$ tel que $F_s(x) = 1$ si $s \in \mathbf{n}$. Vu (2), cela équivaut à dire que $F_s(x)$ *ne dépend que des classes de* s *et de* x *modulo* $\mathbf{n}$.

Ces trois propriétés *caractérisent* les éléments de $Z^1(\mathbf{g}, A^*)$.

Si $F \in Z^1(\mathbf{g}, A^*)$ on notera F' l'application de $\mathbf{g}$ dans A définie par la formule:

$$F'(s) = F_s(1).$$

Il résulte de (2) que l'on a:

$$F_s(x) = F'(x)^{-1} F'(xs) \quad (x,\ s \in \mathbf{g}), \tag{4}$$

ce qui montre que F' détermine F. De plus (1) et (2) impliquent:

$$F'(h \cdot x) = F'(h)\ {}^h(F'(x)) \quad (h \in \mathbf{h},\ x \in \mathbf{g}), \tag{5}$$

et (3) implique:

(6) Il existe un sous-groupe ouvert distingué $\mathbf{n}$ de $\mathbf{g}$ tel que $F'(x)$ ne dépende que de la classe de x modulo $\mathbf{n}$.

Inversement, si $F' : \mathbf{g} \to A$ vérifie (5) et (6), l'application F définie par la formule (4) vérifie les conditions (1), (2), (3): la vérification est immédiate. De plus $\varphi(F)$ est la restriction de F' à $\mathbf{h}$.

Si $F, G \in Z^1(\mathbf{g}, A^*)$ sont cohomologues, il existe $c \in A^*$ tel que:

$$G'(s) = c(1)^{-1} F'(s) c(s) \quad (s \in \mathbf{g}), \tag{7}$$

et réciproquement, s'il existe $c \in A^*$ vérifiant (7), la formule (4) montre que F et G sont cohomologues.

Montrons maintenant que Φ est *surjective*. Soit $z \in Z^1(\mathbf{h}, A)$, et soit $\mathbf{n}$ un sous-groupe ouvert distingué de $\mathbf{g}$ tel que z soit constant sur les classes de $\mathbf{h}$ modulo $\mathbf{h} \cap \mathbf{n}$. Soit $(s_i)_{i \in I}$ un système de représentants des classes à droite de $\mathbf{g}$ modulo $\mathbf{h} \cdot \mathbf{n}$; nous supposerons que ce système contient l'élément 1.

Si l'on a

$$h \cdot n \cdot s_i = h' \cdot n' \cdot s_j \quad (h,\ h' \in \mathbf{h},\ n,\ n' \in \mathbf{n},\ i,\ j \in I),$$

on a évidemment $i = j$ et $h \equiv h' \bmod \mathbf{h} \cap \mathbf{n}$, d'où $z_h = z_{h'}$. Il existe donc une application $F' : \mathbf{g} \to A$ telle que:

$$F'(h \cdot n \cdot s_i) = z_h \quad \text{si} \quad h \in \mathbf{h},\ n \in \mathbf{n},\ i \in I\ . \tag{8}$$

Il est clair que F' vérifie (5) et (6). De plus, la restriction de F' à $\mathbf{h}$ est égale à z. Compte tenu de ce qui a été dit plus haut, cela prouve que φ est surjective, donc aussi Φ.

Il reste à prouver que Φ est *injective*. Soient $F, G \in Z^1(\mathbf{g}, A^*)$ tels que $\varphi(F)$ et $\varphi(G)$ soient cohomologues. Il existe alors $a \in A$ tel que l'on ait:

$$G'(h) = a^{-1} F'(h)^h a \quad (h \in \mathbf{h})\ . \tag{9}$$

Soit $\mathbf{n}$ un sous-groupe ouvert distingué de $\mathbf{g}$ tel que a soit invariant par $\mathbf{n}$, et que F' et G' soient constantes sur les classes de $\mathbf{g}$ modulo $\mathbf{n}$. Soit de nouveau $(s_i)_{i \in I}$ un système de représentants des classes à droite de $\mathbf{g}$ modulo $\mathbf{h} \cdot \mathbf{n}$; on suppose encore que ce système contient l'élément 1. Si $i \in I$, soit a_i l'élément de A défini par la formule:

$$G'(s_i) = a^{-1} F'(s_i) a_i\ . \tag{10}$$

Si $t \in \mathbf{h} \cap \mathbf{n}$, on a ${}^t(G'(x)) = G'(x)$ pour tout $x \in \mathbf{g}$, et de même pour F'. En appliquant ceci à $x = s_i$, on voit que ${}^t a_i = a_i$; les a_i sont donc *invariants par* $\mathbf{h} \cap \mathbf{n}$. On en déduit comme ci-dessus l'existence d'une application $c : \mathbf{g} \to A$ telle que:

$$c(h \cdot n \cdot s_i) = {}^h a_i \quad \text{si} \quad h \in \mathbf{h},\ n \in \mathbf{n},\ i \in I\ . \tag{11}$$

Il est clair que c est constante sur les classes modulo $\mathbf{n}$, et vérifie l'identité $c(h \cdot x) = {}^h(c(x))$ pour $h \in \mathbf{h}$, $x \in \mathbf{g}$; on a donc $c \in A^*$. Comme $F'(1) = G'(1) = 1$, on a en outre $c(1) = a$.

Soit maintenant $x = h \cdot n \cdot s_i$ $(h \in \mathbf{h},\ n \in \mathbf{n},\ i \in I)$ un élément de $\mathbf{g}$. On a:

$$\begin{aligned} G'(x) &= G'(h) \cdot {}^h(G'(n \cdot s_i)) = G'(h) \cdot {}^h(G'(s_i)) \\ &= a^{-1} F'(h)^h a^h (G'(s_i)) \\ &= a^{-1} F(h)^h (F'(s_i) a_i) = a^{-1} F'(h \cdot s_i)^h a_i \\ &= c(1)^{-1} F'(x) c(x)\ . \end{aligned}$$

D'après (7), cela signifie que F et G sont cohomologues, ce qui achève la démonstration.

§ 2. Cohomologie galoisienne

2.1. Cohomologie d'un foncteur.

Soit k un corps et soit S la catégorie des extensions algébriques séparables de k (ou bien la catégorie de toutes les extensions de k). Soit A un foncteur de S

dans la catégorie *Ens* des ensembles (resp. dans la catégorie *Gr* des groupes). Nous supposerons que A vérifie les trois conditions suivantes:

(1) Si $K \to K'$ est un morphisme ($K, K' \in S$), le morphisme correspondant $A(K) \to A(K')$ est injectif.

(2) Si K' est une extension galoisienne de K ($K, K' \in S$), $A(K)$ s'identifie au sous-ensemble de $A(K')$ formé des éléments invariants par les opérations du groupe de GALOIS $\mathfrak{g}(K'/K)$.

(3) Pour tout $K \in S$, on a $A(K) = \varinjlim \cdot A(K_\alpha)$, pour K_α parcourant l'ensemble des sous-extensions de K qui sont de type fini sur k.

Soit K'/K une extension galoisienne (avec $K, K' \in S$). La condition (3) montre que $\mathfrak{g}(K'/K)$ opère continûment sur $A(K')$; ainsi $A(K')$ est muni d'une structure de $\mathfrak{g}(K'/K)$-*ensemble* (resp. de $\mathfrak{g}(K'/K)$-*groupe*, lorsque le foncteur A est à valeurs dans *Gr*). Le i-ième ensemble de cohomologie $H^i(\mathfrak{g}(K'/K), A(K'))$ est donc défini pour $i = 0$ (resp. pour $i = 0,1$), cf. § 1; on le notera $H^i(K'/K, A)$ et l'on écrira de même $Z^1(K'/K, A)$ à la place de $Z^1(\mathfrak{g}(K'/K), A(K'))$. D'après (2), on a:

$$H^0(K'/K, A) = A(K).$$

Remarque. Lorsque A prend ses valeurs dans la catégorie des groupes *commutatifs*, on peut définir pour tout $i \geqslant 0$ des groupes de cohomologie $H^i(K'/K, A)$, cf. [13] ainsi que [19], Chap. II.

2.2. Propriétés fonctorielles. Il est clair que les $H^i(K'/K, A)$ sont fonctoriels par rapport à A.

D'autre part, pour A fixé, considérons deux extensions galoisiennes K_1'/K_1 et K_2'/K_2, de groupes de GALOIS $\mathfrak{g}_1$ et $\mathfrak{g}_2$. Soit $f: K_1 \to K_2$ un morphisme dans la catégorie S. Supposons qu'il *existe* un morphisme $F: K_1' \to K_2'$ prolongeant f. D'après la théorie de GALOIS, le corps $F(K_1')$ ne dépend pas du chois de F, et l'extension $F(K_1') \cdot K_2/K_2$ est galoisienne. Pour tout $s \in \mathfrak{g}_2$, il existe un unique élément $\lambda_F(s) \in \mathfrak{g}_1$ tel que $s \circ F = F \circ \lambda_F(s)$. L'application $\lambda_F: \mathfrak{g}_2 \to \mathfrak{g}_1$ ainsi définie est un homomorphisme, qui est compatible avec l'application

$$\mu_F: A(K_1') \to A(K_2')$$

définie par F. On en déduit (cf. n° 1.3) des applications

$$(\lambda_F, \mu_F)^i_*: H^i(K_1'/K_1, A) \to H^i(K_2'/K_2, A).$$

Lemme. *Les applications définies ci-dessus ne dépendent pas du choix de F.*

Soit F' un morphisme de K_1' dans K_2' prolongeant f. D'après la théorie de GALOIS, il existe $t \in \mathfrak{g}_1$ tel que $F' = F \circ t$. On a $\lambda_{F'} = \lambda_t \circ \lambda_F$, où λ_t désigne

l'automorphisme intérieur de $\mathfrak{g}_1$ défini par t^{-1}, et $\mu_{F'} = \mu_F \circ \mu_t$. Le lemme résulte alors du fait que $(\lambda_t, \mu_t)^i_*$ est l'identité (cf. n° 1.25).

Ainsi, les applications $H^i(K_1'/K_1, A) \to H^i(K_2'/K_2, A)$ ne dépendent que de f; pour $i = 0$, on obtient évidemment l'application de $A(K_1)$ dans $A(K_2)$ définie par f.

Prenons en particulier $K_1 = K_2 = k$ (f étant l'application identique) et pour K_1' et K_2' deux clôtures séparables de k. Le lemme ci-dessus donne une bijection *canonique* de $H^i(K_1'/k, A)$ sur $H^i(K_2'/k, A)$. On identifiera entre eux ces ensembles, et on les notera $H^i(k_s/k, A)$, ou simplement $H^i(k, A)$. Ce sont des foncteurs par rapport à k.

2.3. Exemples. (a) Soit X un *schéma* sur k. Pour toute extension K/k, nous noterons X_K, ou $X(K)$, l'ensemble des points de X à valeurs dans K (rappelons que c'est l'ensemble des k-morphismes de Spec (K) dans X). On définit ainsi un foncteur sur S à valeurs dans Ens, que l'on note encore X. Ce foncteur vérifie les conditions (1) et (2) du n° 2.1; il vérifie la condition (3) pourvu que l'on suppose que X est localement de type fini sur k (cf. [9], Chap. IV). Lorsque X est un *schéma en groupes* sur k, le foncteur correspondant prend ses valeurs dans la catégorie des groupes, et $H^i(K'/K, X)$ est défini pour $i = 0,1$.

(b) Soit X un schéma de type fini sur k. Pour toute extension K/k, soit $\mathrm{Aut}\, X(K)$ le groupe des K-automorphismes du schéma étendu $X \otimes_k K$. On obtient ici encore un foncteur $\mathrm{Aut}\, X : S \to Gr$, vérifiant les conditions (1), (2), (3) du n° 2.1. Il en est de même lorsque X est un schéma en groupes de type fini sur k, et que l'on se borne aux automorphismes respectant cette structure de groupe.

Nous verrons dans les §§ 4 et 5 que, dans certains cas, le foncteur $\mathrm{Aut}\, X$ provient d'un schéma en groupes sur k.

2.4. Conjugaison. Soit k'/k une extension galoisienne, de groupe de GALOIS $\mathfrak{g}$, et soit X' un k'-schéma. Si $s \in \mathfrak{g}$, on note ${}^sX'$ le schéma obtenu à partir de X' par le changement de base $s : k' \to k'$; si $x \in X'(k')$, on note ${}^sx$ le point correspondant de $({}^sX)(k')$; si $f' : X' \to Y'$ est un morphisme de k'-schémas, on note ${}^sf'$ le morphisme de ${}^sX'$ dans ${}^sY'$ déduit de f' par changement de base. On a la formule:

$$({}^sf')({}^sx) = {}^s(f'(x)) \text{ , pour } s \in \mathfrak{g} \text{ , } x \in X(k') \text{ .}$$

Si $X' = X \otimes_k k'$ et $Y' = Y \otimes_k k'$, on peut identifier ${}^sX'$ à X' et ${}^sY'$ à Y'; on a alors ${}^sf' = f'$ pour tout $s \in \mathfrak{g}$ si et seulement si f' est «défini sur k», i. e. s'il existe un morphisme $f : X \to Y$ tel que $f' = f \otimes 1$; le morphisme f est alors unique.

2.5. Torsion. Soit k'/k une extension galoisienne, de groupe de GALOIS $\mathbf{g}$, et soit X un schéma de type fini sur k (resp. un schéma en groupes de type fini sur k). Nous supposerons que X est *quasi-projectif*. Soit Aut X le foncteur d'automorphismes de X (cf. n° 2.3).

2.6. Proposition. *Soit* $a = (a_s) \in Z^1(k'/k, \mathrm{Aut}\, X)$. *Il existe un* k*-schéma de type fini (resp. un* k*-schéma en groupes de type fini)* Y *et un* k'*-isomorphisme* $f' : X \otimes_k k' \to Y \otimes_k k'$ *tels que l'on ait*:

$$^s f' = f' \circ a_s \quad \textit{pour tout} \quad s \in \mathbf{g}\,.$$

Le couple (Y, f') *est unique, à isomorphisme unique près.*

La continuité du cocycle a permet de se ramener au cas où l'extension k'/k est *finie*. On applique alors à (a_s) le théorème de «descente du corps de base» de WEIL (cf. par exemple [17], Chap. V., § 4, n° 20). Cela revient simplement à ceci:

Si l'on pose $b_s = a_s \circ (1 \otimes s)$, on a $b_{st} = b_s \circ b_t$, et l'on peut faire opérer $\mathbf{g}$ sur $X \otimes_k k'$ au moyen des b_s; ces opérations sont compatibles avec celles de $\mathbf{g}$ sur k'. Il en résulte que $\mathbf{g}$ opère librement, et l'on prend pour Y le schéma quotient $(X \otimes_k k')/\mathbf{g}$ (ce quotient existe grâce au fait que X est supposée quasi-projective). On vérifie immédiatement que Y a les propriétés voulues.

Le schéma Y ainsi obtenu sera noté X_a; on dit qu'il s'obtient *en tordant* X *au moyen de* a. L'ensemble des isomorphismes de $X \otimes_k k'$ sur $Y \otimes_k k'$ est un *espace homogène principal* de Aut $X(k')$, et la classe de cohomologie correspondante est celle de a. On en déduit que X_a est isomorphe à X_b si et seulement si a et b sont cohomologues. *Les éléments de* $H^1(k'/k, \mathrm{Aut}\, X)$ *correspondent donc bijectivement aux classes d'isomorphisme de* k*-schémas* (resp. de k-schémas en groupes) Y *tels que* $Y \otimes_k k'$ *soit isomorphe à* $X \otimes_k k'$. (Un tel k-schéma Y est appelé une k'/k*-forme* de X – lorsque $k' = k_s$, on dit simplement une k*-forme*.)

Exemple. Soit A un schéma en groupes de type fini sur k, et soit $a = (a_s) \in Z^1(k'/k, A)$. Si l'on fait opérer A à gauche sur lui-même (par translations), on peut tordre A au moyen de a. Le schéma P_a ainsi obtenu est un *espace homogène principal* sur A (cf. par exemple [17], Chap. V, n° 21 ou [13]) tel que $P_a(k') \neq \varnothing$. On retrouve ainsi la correspondance bien connue entre les *classes* de tels espaces et les *éléments* de $H^1(k'/k, A)$.

La notion de «torsion» définie plus haut est compatible avec celle du § 1. De façon précise:

2.7. Proposition. *Soient* X, Y, a, f' *vérifiant les hypothèses de* 2.6. *L'application* $f' : X(k') \to Y(k')$ *est un isomorphisme du* g*-ensemble tordu* $X(k')_a$ *sur le* g*-ensemble* $Y(k')$.

Cela résulte de la formule:

$$f'(a_s({}^s x)) = (f' \circ a_s)({}^s x) = ({}^s f')({}^s x) = {}^s(f'(x)) \quad (x \in X(k'),\ s \in \mathbf{g}) .$$

2.8. Restriction des scalaires. Soient k_1 une extension finie séparable de k, et k' une extension galoisienne de k contenant k_1; notons $\mathbf{g}$ (resp. $\mathbf{h}$) le groupe de GALOIS de k'/k (resp. de k'/k_1); l'ensemble des k-morphismes de k_1 dans k' s'identifie canoniquement à l'espace homogène $\mathbf{g}/\mathbf{h}$. Soit X un schéma sur k_1; si $s \in \mathbf{g}$, le conjugué ${}^s X$ de X ne dépend que de la classe de s modulo $\mathbf{h}$. Soit d'autre part Y un schéma sur k, et soit $p : Y \otimes_k k_1 \to X$ un k_1-morphisme. La collection des conjugués $({}^s p)_{s \in \mathbf{g}/\mathbf{h}}$ définit un morphisme

$$({}^s p) : Y \otimes_k k' \to \coprod_{s \in \mathbf{g}/\mathbf{h}} {}^s X \otimes k' .$$

Lorsque $({}^s p)$ est un isomorphisme, on dit (cf. WEIL [21], n° 1.3) que Y s'obtient à partir de X *par restriction des scalaires de* k_1 *à* k; le couple (Y, p) est alors unique, à un isomorphisme unique près. On écrit $Y = R_{k_1/k}(X)$ ou encore $Y = \coprod_{k_1/k}(X)$, cette dernière notation étant celle de GROTHENDIECK. *L'existence* de $R_{k_1/k}(X)$ peut se démontrer, par exemple, lorsque X est quasi-projectif sur k.

Supposons que $Y = R_{k_1/k}(X)$ existe; soit E le $\mathbf{h}$-ensemble $X(k')$, et soit E^* le $\mathbf{g}$-ensemble induit (cf. n° 1.28). Nous allons voir que E^* *peut être identifié à* $Y(k')$. De façon plus précise, soit $y \in Y(k')$, et soit $\vartheta(y)$ l'application de $\mathbf{g}$ dans E définie par la formule:

$$\vartheta(y)(s) = {}^s(({}^{s^{-1}} p)(y)) ,$$

formule qui a un sens, puisque $({}^{s^{-1}} p)(y)$ appartient à ${}^{s^{-1}} X(k')$.

2.9. Proposition. *Pour tout* $y \in Y(k')$, *on a* $\vartheta(y) \in E^*$. *L'application* $\vartheta : Y(k') \to E^*$ *ainsi définie est un isomorphisme de* g*-ensembles.*

Il faut d'abord prouver que $\vartheta(y)$ vérifie les conditions (a) et (b) du n° 1.28. La condition (a) (continuité) est immédiate. La condition (b) s'écrit:

$$\vartheta(y)(h \cdot s) = {}^h(\vartheta(y)(s)) , \quad h \in \mathbf{h} , s \in \mathbf{g} .$$

Elle résulte du fait que ${}^h p = p$. L'application ϑ est donc bien définie. On vérifie sans difficultés que c'est une bijection. Le fait que ϑ soit un morphisme de $\mathbf{g}$-ensembles résulte du calcul suivant:

$$\begin{aligned}\vartheta(y)(s\cdot g) &= {}^{sg}(({}^{g^{-1}s^{-1}}p)(y))\\ &= {}^{sg}({}^{g^{-1}}(({}^{s^{-1}}p)({}^{g}y))) = {}^{s}(({}^{s^{-1}}p)({}^{g}y))\\ &= \vartheta({}^{g}y)(s)\,.\end{aligned}$$

Lorsque X est un *schéma en groupes*, il en est de même de Y, et l'application ϑ est compatible avec les structures de groupes de $Y(k')$ et de E^*. Compte tenu de la prop. 1.29, cela donne:

2.10. Corollaire. *Si* $Y = R_{k_1/k}(X)$, *il existe une bijection canonique de* $H^i(k'/k, Y)$ *sur* $H^i(k'/k_1, X)$, $i = 0,1$.

En particulier, prenant $k' = k_s$, on voit qu'on peut *identifier* $H^i(k, Y)$ et $H^i(k_1, X)$.

Remarque. Pour $i = 0$, on retrouve la bijection canonique de $Y(k)$ sur $X(k_1)$, cf. WEIL, *loc. cit.* Pour $i = 1$, on peut interpréter la bijection $H^1(k'/k_1, X) \to H^1(k'/k, Y)$ de la manière suivante: à tout espace homogène principal P sur X, ayant un point dans k', on associe l'espace homogène principal $R_{k_1/k}(P)$ sur Y.

2.11. Variétés algébriques et groupes algébriques. Soit k un corps. Nous appellerons *variété algébrique définie sur* k (ou simplement *k-variété*) tout schéma X de type fini sur k qui est *absolument réduit*. Rappelons que cette dernière condition signifie que, pour toute extension k'/k, le schéma étendu $X \otimes_k k'$ est réduit (son faisceau structural n'a pas d'éléments nilpotents); en particulier X est réduit; la réciproque est vraie lorsque k est *parfait*, ce qui sera toujours le cas à partir du § 4. Lorsque k est *algébriquement clos*, la notion de «variété algébrique» définie ici est équivalente à celle de FAC.

De même, nous appellerons *groupe algébrique* défini sur k tout schéma en groupes G sur k qui est une variété algébrique (pour la structure de schéma sous-jacente). Il revient au même de dire que G est de type fini sur k, et *simple* sur k (au sens de GROTHENDIECK [10] – autrement dit «lisse» au sens de GROTHENDIECK [9], Chap. IV).

Lemme. (i) *Si* V *est une variété algébrique définie sur* k, $V(k_s)$ *est dense dans* V.

(ii) *Soient* V *et* W *deux k-variétés, et soient* f *et* f' *deux morphismes de* V *dans* W. *Si* f *et* f' *définissent la même application de* $V(k_s)$ *dans* $W(k_s)$, *on a* $f = f'$.

L'assertion (i) est bien connue, cf. par exemple [17], Chap. V, n° 23. L'assertion (ii) résulte de (i) et du fait que V est un schéma réduit.

Application. Soit P un espace homogène principal sur un groupe algébrique A ; il existe une extension k' de k telle que $P \otimes_k k'$ soit isomorphe à $A \otimes_k k'$ (par exemple $k' = \bar{k}$). Comme A est une variété algébrique, il en est de même de P, et le lemme ci-dessus montre que $P(k_s) \neq \varnothing$. On en conclut que P *est défini par un élément de* $H^1(k, A)$, cf. n° 2.6.

2.12. Un lemme de descente du corps de base. Soient k un corps, k_1 une extension finie de k contenue dans k_s, et $\mathbf{g}$ le groupe de GALOIS de k_s/k. Soit V une k_1-variété algébrique. On suppose $V(k_s)$ muni d'une structure de $\mathbf{g}$-ensemble, et l'on note $s(x)$ le transformé de $x \in V(k_s)$ par $s \in \mathbf{g}$. On se propose de donner des conditions pour qu'il existe une variété algébrique W définie sur k et un isomorphisme $\vartheta : V \otimes_{k_1} k_s \to W \otimes_k k_s$ tels que l'application correspondante $\vartheta : V(k_s) \to W(k_s)$ soit un isomorphisme de $\mathbf{g}$-ensembles.

Soit $s \in \mathbf{g}$. Soit ${}^sV$ le schéma sur ${}^sk_1$ obtenu à partir de V par le changement de base $s : k_1 \to {}^sk_1$. On a une bijection canonique $x \mapsto {}^sx$ de $V(k_s)$ sur $({}^sV)(k_s)$, d'où une application bien définie $f_s : ({}^sV)(k_s) \to V(k_s)$ vérifiant la formule :

$$f_s({}^sx) = s(x) .$$

Lemme. *Supposons vérifiées les trois conditions suivantes :*

(a) *Pour tout* $s \in \mathbf{g}$, *il existe un morphisme* $F_s : {}^sV \otimes k_s \to V \otimes k_s$ *dont l'action sur les points à valeurs dans* k_s *coïncide avec* f_s.

(b) *Il existe une extension finie séparable* k_2/k_1 *telle que* $f_s = 1$ *si* $s \in \mathbf{g}(k_s/k_2)$.

(c) *Il existe un recouvrement de* $V \otimes k_s$ *par des ouverts affines* U_α *tels que* $U_\alpha(k_s)$ *soit stable par* $\mathbf{g}$ *pour tout* α.

Il existe alors une k*-variété* W *et un isomorphisme* $\vartheta : V \otimes_{k_1} k_s \to W \otimes_k k_s$ *tels que* $\vartheta : V(k_s) \to W(k_s)$ *soit un isomorphisme de* $\mathbf{g}$*-ensembles. Le couple* (W, ϑ) *est unique, à un isomorphisme unique près.*

Il est clair que l'on peut supposer que $k_1 = k_2$, et que ce corps est une extension galoisienne de k. Le groupe $\mathbf{h} = \mathbf{g}(k_s/k_2)$ est alors un sous-groupe ouvert distingué de $\mathbf{g}$. Soient $s, t \in \mathbf{g}$ et soit $x \in V(k_s)$. On a :

$$F_{st}({}^{st}x) = st(x) = s(F_t({}^tx)) = F_s({}^s(F_t({}^tx))) = (F_s \circ {}^sF_t)({}^{st}x) .$$

On en conclut (cf. n° 2.11) que $F_{st} = F_s \circ {}^sF_t$. La condition (b) montre d'autre part que $F_s = 1$ si $s \in \mathbf{h}$. Ainsi F_s ne dépend que de la classe de s modulo $\mathbf{h}$, et est défini sur k_1. On peut alors appliquer le critère de descente du corps de base aux F_s (cf. par exemple [17], Chap. V, § 4, n° 20). On en déduit l'existence d'une k-variété algébrique W et d'un isomorphisme $\vartheta : V \otimes k_s \to W \otimes k_s$ tel que $F_s = \vartheta^{-1} \circ {}^s\vartheta$ $(s \in \mathbf{g})$. Si $x \in V(k_s)$, on a $F_s({}^sx) = s(x)$, d'où :

$$({}^s\vartheta)({}^sx) = \vartheta(s(x)), \text{ i. e. } {}^s(\vartheta(x)) = \vartheta(s(x)) ,$$

ce qui montre que le couple (W, ϑ) répond à la question posée. L'unicité est immédiate.

Remarque. Il est facile de vérifier que les conditions (a), (b), (c) du lemme sont non seulement suffisantes, mais aussi *nécessaires.*

Donnons pour terminer un résultat inédit de SPRINGER dont nous aurons besoin au § 6:

2.13. Proposition. *Soient k un corps parfait, A un k-groupe algébrique H un sous-groupe algébrique de A, et N le normalisateur de H dans A. Soit $a = (a_s) \in Z_1(\bar{k}/k, A)$, et soit $\alpha \in H^1(k, A)$ la classe de cohomologie correspondante. Soit A_a le groupe algébrique obtenu en tordant A au moyen de a* (le groupe A opérant sur lui-même par automorphismes intérieurs). *Les deux conditions suivantes sont équivalentes*:

(i) *α appartient à l'image de $H^1(k, N) \to H^1(k, A)$.*

(ii) *Il existe un sous-groupe algébrique H' de A_a tel que $H' \otimes \bar{k}$ et $H \otimes \bar{k}$ soit conjugués par un automorphisme intérieur défini par un élément de $A(\bar{k})$.*

(La condition (ii) a un sens, grâce au fait que $A_a \otimes \bar{k}$ peut être canoniquement identifié à $A \otimes \bar{k}$.)

Posons $\mathfrak{g} = \mathfrak{g}(\bar{k}/k)$, soit $X = A(\bar{k})/N(\bar{k})$, et soit X_a le $\mathfrak{g}$-ensemble obtenu en tordant X au moyen de a (le groupe $A(\bar{k})$ opérant *à gauche* sur X). A tout $x \in X_a$, associons le sous-groupe $H_x = \mathrm{Int}(x)(H \otimes \bar{k})$ de $A_a \otimes \bar{k}$. On vérifie sans difficultés que l'on obtient ainsi un isomorphisme de X_a sur le $\mathfrak{g}$-ensemble des sous-groupes algébriques H_1' de $A_a \otimes \bar{k}$ qui sont conjugués de $H \otimes \bar{k}$ par un automorphisme intérieur de $A(\bar{k})$. La condition (ii) équivaut donc à dire que $H^0(\mathfrak{g}, X_a)$ est *non vide*, et son équivalence avec la condition (i) résulte de la proposition 1.15.

2.14. Corollaire. *Supposons que A soit linéaire, et que H soit un sous-groupe de* CARTAN *de A. L'application canonique*:

$$H^1(k, N) \to H^1(k, A)$$

est alors surjective.

Soit $a \in Z^1(\bar{k}/k, A)$. On sait (cf. [16]) que A_a possède un sous-groupe de CARTAN H' (défini sur k, bien entendu); de plus la conjugaison des sous-groupes de CARTAN (cf. par exemple [6], 7.01) montre que $H \otimes \bar{k}$ et $H' \otimes \bar{k}$ sont conjugués par un élément de $A(\bar{k})$. La proposition précédente s'applique, et l'on en déduit que la classe de cohomologie de a appartient à l'image de $H^1(k, N) \to H^1(k, A)$, d'où le corollaire.

§ 3. Groupes de type arithmétique

3.1. Groupes de type arithmétique. Soit G un groupe algébrique linéaire défini sur $\mathbf{Q}$, et soit $G_{\mathbf{Q}}$ le groupe de ses points rationnels. Si r est un plongement de G dans un groupe $\mathbf{GL}_n$, nous noterons $G_{\mathbf{Z}}(r)$ le sous-groupe de $G_{\mathbf{Q}}$ formé des éléments g tels que $r(g) \in \mathbf{GL}_n(\mathbf{Z})$. Un sous-groupe Γ de $G_{\mathbf{Q}}$ est dit *de type arithmétique dans* $G_{\mathbf{Q}}$ s'il existe un plongement r tel que $G_{\mathbf{Z}}(r)$ soit *commensurable* à Γ; rappelons que cela signifie que $\Gamma \cap G_{\mathbf{Z}}(r)$ est d'indice fini à la fois dans Γ et dans $G_{\mathbf{Z}}(r)$. On sait que, si cette condition est vérifiée pour un plongement r, elle l'est pour tout plongement. De plus, si Γ est de type arithmétique dans G, on peut choisir r de telle sorte que Γ soit *contenu dans* $G_{\mathbf{Z}}(r)$; en effet, les transformés par les éléments $\gamma \in \Gamma$ du réseau $\mathbf{Z}^n$ sont en nombre fini, et engendrent un réseau X stable par Γ; si $u \in \mathbf{GL}_n(\mathbf{Q})$ transforme $\mathbf{Z}^n$ en X, le plongement r' défini par $r'(g) = u^{-1} r(g) u$ est tel que $\Gamma \subset G_{\mathbf{Z}}(r')$.

Un groupe Γ sera dit *de type arithmétique* s'il est possible de le plonger comme sous-groupe de type arithmétique dans un groupe algébrique linéaire défini sur $\mathbf{Q}$.

3.2. Exemples. Le groupe $\mathbf{Z}$, le groupe $\mathbf{GL}_n(\mathbf{Z})$, un groupe fini, sont des groupes de type arithmétique.

Le produit d'un nombre fini de groupes de type arithmétique est de type arithmétique.

Soit R un anneau qui soit un $\mathbf{Z}$-module libre de type fini, et soit R^* le groupe des éléments inversibles de R. Le groupe R^* est *de type arithmétique*. En effet, si l'on identifie R à $\mathbf{Z}^n$, on voit facilement qu'il existe un sous-groupe algébrique G de $\mathbf{GL}_n$ dont les points rationnels correspondent bijectivement aux éléments inversibles de l'algèbre $R \otimes \mathbf{Q}$. Comme $R^* = G_{\mathbf{Z}}$, cela montre bien que R est de type arithmétique. [En fait, G peut même être défini comme *schéma en groupes sur* $\mathbf{Z}$ grâce au foncteur correspondant $G(A) = (R \otimes A)^*$, A parcourant la catégorie des anneaux commutatifs.]

3.3. Proposition. *Soit Γ un groupe de type arithmétique.*

(i) *Γ est de présentation finie* (autrement dit, Γ peut être défini par un nombre fini de générateurs et de relations).

(ii) *Les sous-groupes finis de Γ forment un nombre fini de classes modulo conjugaison.*

Pour la démonstration, voir [2] et [4].

Remarque. On peut se demander si la propriété (ii) est simplement une conséquence de la propriété (i). LAZARD nous a fait observer qu'il n'en est rien: il existe en effet un groupe de présentation finie qui contient des sous-groupes finis de tout ordre (cf. HIGMAN, Proc. Royal Soc. London, *262*, 1961).

3.4. g-groupes de type arithmétique. Soit $\mathbf{g}$ un groupe profini et soit Γ un $\mathbf{g}$-groupe (cf. n° 1.2). Nous dirons que Γ est *de type arithmétique* si l'on peut trouver:

(a) un groupe algébrique linéaire G défini sur $\mathbf{Q}$,

(b) un plongement $f: \Gamma \to G_{\mathbf{Q}}$,

(c) un homomorphisme continu de $\mathbf{g}$ dans le groupe $\mathrm{Aut}\, G(\mathbf{Q})$ des automorphismes de G, le groupe $\mathrm{Aut}\, G(\mathbf{Q})$ étant muni de la topologie discrète (l'image de $\mathbf{g}$ dans ce groupe est donc finie, ce qui permet de considérer $G_{\mathbf{Q}}$ comme un $\mathbf{g}$-groupe),

ces données étant assujetties aux deux conditions suivantes:

(i) $f(\Gamma)$ est un sous-groupe de type arithmétique de $G_{\mathbf{Q}}$ (cf. n° 3.1),

(ii) le plongement $f: \Gamma \to G_{\mathbf{Q}}$ est compatible avec les structures de $\mathbf{g}$-groupes de Γ et de $G_{\mathbf{Q}}$.

Puisque l'homomorphisme $\mathbf{g} \to \mathrm{Aut}\, G(\mathbf{Q})$ est continu, son noyau $\mathbf{h}$ est un sous-groupe ouvert distingué de $\mathbf{g}$, et il est clair que le $\mathbf{g}/\mathbf{h}$-groupe Γ est de type arithmétique.

On notera également que, lorsque $\mathbf{g}$ est réduit à l'identité, on retrouve la notion définie au n° 3.1.

3.5. Exemples. Tout $\mathbf{g}$-groupe fini, tout produit fini de $\mathbf{g}$-groupes de type arithmétique est de type arithmétique.

Soit R un anneau qui soit un $\mathbf{Z}$-module libre de type fini, et supposons que le groupe profini $\mathbf{g}$ opère continûment sur R. Le groupe R^* est alors un *$\mathbf{g}$-groupe de type arithmétique*. Cela se voit en reprenant la construction du n° 3.2, et en remarquant que $\mathbf{g}$ opère sur le groupe algébrique G construit à cet endroit.

Soit C une variété abélienne définie sur un corps k, et soit $\mathbf{g}$ le groupe de Galois de k_s/k. Le groupe $\mathrm{Aut}\, C(k_s)$ des automorphismes de $C \otimes_k k_s$ est un *$\mathbf{g}$-groupe de type arithmétique*. En effet, soit R l'anneau des endomorphismes de $C \otimes_k k_s$; on sait que R est un $\mathbf{Z}$-module libre de type fini, et l'on a $R^* = \mathrm{Aut}\, C(k_s)$; on est alors ramené à l'exemple précédent. (Le même argument s'applique, plus généralement, à tout groupe algébrique commutatif qui est extension d'une variété abélienne par un tore.)

3.6. Proposition. *Soit Γ un $\mathbf{g}$-groupe de type arithmétique, et soit $\mathbf{h}$ un sous-groupe de $\mathbf{g}$. Le groupe $\Gamma^{\mathbf{h}}$ des éléments de Γ invariants par $\mathbf{h}$ est un groupe de type arithmétique. Si de plus $\mathbf{h}$ est un sous-groupe distingué fermé de $\mathbf{g}$, le $\mathbf{g}/\mathbf{h}$-groupe $\Gamma^{\mathbf{h}}$ est de type arithmétique.*

Soit $f: \Gamma \to G_{\mathbf{Q}}$ un plongement vérifiant les conditions du n° 3.4. Soit H le sous-groupe de G formé des éléments invariants par $\mathbf{h}$. C'est un groupe algébrique défini sur $\mathbf{Q}$, et l'on a $f(\Gamma^{\mathbf{h}}) = f(\Gamma) \cap H_{\mathbf{Q}}$, ce qui montre que $\Gamma^{\mathbf{h}}$

est un sous-groupe de type arithmétique de $H_{\mathbf{Q}}$. Si de plus $\mathbf{h}$ est un sous-groupe distingué fermé de $\mathbf{g}$, le groupe $\mathbf{g}/\mathbf{h}$ opère sur H, et la restriction de f à $\Gamma^{\mathbf{h}}$ est compatible avec les structures de $\mathbf{g}/\mathbf{h}$-groupes de $\Gamma^{\mathbf{h}}$ et de $H_{\mathbf{Q}}$, ce qui achève de démontrer la proposition.

3.7. Proposition. *Soit Γ un $\mathbf{g}$-groupe de type arithmétique, et soit $a = (a_s)$ un élément de $Z^1(\mathbf{g}, \Gamma)$. Le $\mathbf{g}$-groupe Γ_a obtenu en tordant Γ au moyen de a* (cf. n° 1.4) *est de type arithmétique.*

Soit $f : \Gamma \to G_{\mathbf{Q}}$ un plongement vérifiant les conditions du n° 3.4.

Pour tout $s \in \mathbf{g}$, soit r_s l'automorphisme intérieur de G défini par $f(a_s)$. Faisons opérer $\mathbf{g}$ sur G au moyen des $r_s \circ s$; le sous-groupe $f(\Gamma)$ de $G_{\mathbf{Q}}$ est stable par ces opérations, et l'action de $\mathbf{g}$ sur Γ ainsi définie est celle du groupe tordu Γ_a. D'où la proposition.

3.8. Proposition. *Soit $\mathbf{g}$ un groupe fini, et soit Γ un $\mathbf{g}$-groupe de type arithmétique. Alors:*

(i) *Le produit semi-direct Γ' de Γ par $\mathbf{g}$ est un groupe de type arithmétique.*

(ii) *$H^1(\mathbf{g}, \Gamma)$ est fini.*

Soit $f : \Gamma \to G_{\mathbf{Q}}$ un plongement vérifiant les conditions du n° 3.4. Convenons de noter $\mathbf{g}$ le groupe algébrique de dimension zéro défini canoniquement par $\mathbf{g}$ (en tant que schéma, c'est simplement $\mathbf{g}$ muni du faisceau d'anneaux constant $\mathbf{Q}$). Comme $\mathbf{g}$ opère sur G, on peut former le produit semi-direct G' de G par $\mathbf{g}$; c'est un groupe algébrique linéaire défini sur $\mathbf{Q}$. Le groupe $G'_{\mathbf{Q}}$ est produit semi-direct de $G_{\mathbf{Q}}$ par $\mathbf{g}$; le groupe Γ' se plonge donc de façon naturelle dans $G'_{\mathbf{Q}}$. Comme de plus Γ est d'indice fini dans Γ', on voit que Γ' est un sous-groupe de type arithmétique de $G'_{\mathbf{Q}}$, d'où (i).

Soit maintenant $a = (a_s)$ un élément de $Z^1(\mathbf{g}, \Gamma)$. Si nous convenons d'écrire les éléments du produit semi-direct Γ' sous la forme $\gamma \cdot s$, avec $\gamma \in \Gamma$ et $s \in \mathbf{g}$, le cocycle a définit un *homomorphisme* $\vartheta_a : \mathbf{g} \to \Gamma'$ par la formule $\vartheta_a(s) = a_s s$. L'image C_a de $\mathbf{g}$ par ϑ_a est un sous-groupe fini de Γ', dont la connaissance équivaut à celle de a. Comme Γ' est de type arithmétique, la proposition 3.3 montre que les sous-groupes C_a se déduisent d'un nombre fini d'entre eux par conjugaison par les éléments de Γ', donc aussi par ceux de Γ, puisque Γ'/Γ est fini. Ainsi, il existe $a_1, \ldots, a_n \in Z^1(\mathbf{g}, \Gamma)$ tels que, pour tout $a \in Z^1(\mathbf{g}, \Gamma)$, il existe un indice i et un élément $\gamma \in \Gamma$ tels que $C_{a_i} = \gamma C_a \gamma^{-1}$; on tire de là:

$$\vartheta_{a_i}(s) = \gamma \vartheta_a(s) \gamma^{-1}, \quad \text{d'où} \quad a_s = \gamma^{-1}(a_i)_s{}^s\gamma ,$$

ce qui montre que a et a_i sont cohomologues. D'où la finitude de $H^1(\mathbf{g}, \Gamma)$.

§ 4. Groupes localement algébriques et groupes d'automorphismes

Dans tout ce paragraphe, la lettre k désigne un corps *parfait*. On note $\mathbf{g}$ le groupe de GALOIS $\mathbf{g}(\bar{k}/k)$.

4.1. Schémas localement algébriques. Soit X un schéma sur k. Nous dirons que X est *localement algébrique* s'il est réunion de sous-schémas ouverts et fermés qui sont des variétés algébriques au sens du n° 2.11. Un tel schéma est absolument réduit, et localement de type fini sur k; il résulte de 2.11 que $X(\bar{k})$ est dense dans X.

Dans ce qui suit, nous noterons C_k la catégorie des schémas localement algébriques sur k. Si k' est une extension de k, le foncteur $X \to X \otimes k'$ définit une équivalence de C_k sur une sous-catégorie de $C_{k'}$.

Les propriétés de la conjugaison données dans 2.4 s'étendent immédiatement aux schémas localement algébriques. En particulier, si X, $Y \in C_k$, et si $f \in \mathrm{Hom}(X \otimes \bar{k}, Y \otimes \bar{k})$, le morphisme f est «défini sur k» si et seulement si ${}^s f = f$ pour tout $s \in \mathbf{g}$. D'après le lemme 2.11, il faut et il suffit pour cela que l'on ait:

$$f({}^s x) = {}^s(f(x)) \quad \text{pour} \quad s \in \mathbf{g},\ x \in X(\bar{k}) .$$

4.2. Groupes localement algébriques. Soit G un schéma en groupes sur k. Nous dirons que G est un *groupe localement algébrique* si sa structure de schéma sous-jacente est localement algébrique (autrement dit si c'est un groupe dans la catégorie C_k). Un tel groupe est *simple* sur k (cf. [10]); sa composante neutre G^0 est un groupe *algébrique* connexe, qui est ouvert et fermé dans G.

Un groupe localement algébrique G tel que $G^0 = 1$ sera dit *discret*, ou *de dimension zéro*. Un tel groupe est déterminé à isomorphisme près par le $\mathbf{g}$-groupe $G(\bar{k})$, et nous nous permettrons parfois l'abus de langage consistant à identifier G à $G(\bar{k})$.

Si G est un groupe localement algébrique quelconque, le quotient G/G^0 est défini: c'est le groupe de dimension zéro qui correspond à $G(\bar{k})/G^0(\bar{k})$. On a ainsi une suite exacte:

$$0 \to G^0 \to G \to G/G^0 \to 0 ,$$

avec G^0 algébrique connexe et G/G^0 discret. Il est clair que tout k-sous-groupe de G/G^0 définit un sous-groupe ouvert de G; en particulier, les k-sous-groupes *finis* de G/G^0 correspondent aux sous-groupes *algébriques* ouverts de G.

4.3. Groupes de type (ALA). Un groupe localement algébrique A sur k sera dit *de type* (ALA) si sa composante neutre A^0 est un groupe algébrique *linéaire*, et si le $\mathbf{g}$-groupe $A(\bar{k})/A^0(\bar{k})$ est extension d'un $\mathbf{g}$-*groupe de type*

arithmétique Γ (cf. n° 3.4) par un g-*groupe fini* N. L'image réciproque A_1 de N dans A est un sous-groupe algébrique linéaire de A, qui est distingué dans A, et $A(\bar{k})/A_1(\bar{k}) = \Gamma$. On obtient ainsi une suite exacte

$$0 \to A_1 \to A \to \Gamma \to 0\,,$$

où A_1 est algébrique linéaire, et où Γ est un g-groupe de type arithmétique. Réciproquement, il est clair que tout groupe localement algébrique A qui est extension d'un g-groupe de type arithmétique par un groupe algébrique linéaire, est de type (ALA); le sigle choisi rappelle ce fait (Algébrique Linéaire — Arithmétique).

4.4. Le foncteur Aut X. Soit X une k-variété algébrique (resp. un k-groupe algébrique), et soit $Y \in \mathcal{C}_k$. On dit que Y *agit sur* X si l'on s'est donné un morphisme $f: Y \times X \to X$ tel que $(pr_1, f): Y \times X \to Y \times X$ soit un isomorphisme (resp. un isomorphisme respectant la structure de groupe des fibres de pr_1). L'ensemble des actions de Y sur X sera noté Aut $X(Y)$; c'est également l'ensemble des automorphismes de $X \times Y$, considéré comme Y-schéma (resp. comme Y-schéma en groupes); en particulier, Aut $X(Y)$ a une structure naturelle de *groupe*. Si $Y, Y' \in \mathcal{C}_k$, et si $q \in \mathrm{Hom}(Y, Y')$, on définit de façon évidente Aut $X(q)$: Aut $X(Y') \to$ Aut $X(Y)$. Ainsi Aut X est un *foncteur contravariant* de $\mathcal{C}_k$ dans la catégorie $\mathcal{G}r$ des groupes.

Soit Y un groupe localement algébrique sur k. On dit que Y *opère sur* X s'il agit sur X et si cette action $f: Y \times X \to X$ est telle que le diagramme

$$\begin{array}{ccc} Y \times Y \times X & \xrightarrow{id \times f} & Y \times X \\ {\scriptstyle q \times id}\downarrow & & \downarrow{\scriptstyle f} \\ Y \times X & \xrightarrow{f} & X\,, \end{array}$$

où q désigne la loi de composition de Y, est commutatif. Cela entraîne que l'élément neutre de Y agit trivialement sur X.

Nous dirons que *le foncteur* Aut X *est localement algébrique* (ou encore que Aut X *est un groupe localement algébrique*) si ce foncteur est *représentable* dans $\mathcal{C}_k$. Cela signifie qu'il existe $A \in \mathcal{C}_k$ et une action α de A sur X telle que, pour tout $Y \in \mathcal{C}_k$, l'application de Hom (Y, A) dans Aut $X(Y)$ définie par α soit une bijection. On sait que le couple (A, α) est alors unique (à isomorphisme unique près), et que A est un groupe localement algébrique opérant sur X au moyen de α. On identifiera le plus souvent Aut X à A.

Soit $\mathcal{R}ed_k$ la catégorie des k-schémas *réduits* (non nécessairement localement algébriques). On a:

4.5. Proposition. *Soit X une variété algébrique (resp. un groupe algébrique) sur k, et supposons que* Aut X *soit représentable dans C_k par un groupe localement algébrique A. Alors A représente également le foncteur* Aut X *dans la catégorie Red_k.*

Il faut montrer que, pour tout $S \in Red_k$, l'homomorphisme canonique

$$\alpha_S : \mathrm{Hom}\,(S, A) \to \mathrm{Aut}\,X(S)$$

est un isomorphisme. En localisant, on se ramène au cas où S est *affine*; soit A la k-algèbre correspondante. Soit (A_i) la famille des sous-algèbres de A qui sont de type fini sur k, et posons $S_i = \mathrm{Spec}(A_i)$. D'après GROTHENDIECK (cf. [9], Chap. IV, § 8), on a:

$$\mathrm{Hom}\,(S, A) = \varinjlim \mathrm{Hom}\,(S_i, A) \text{ et } \mathrm{Aut}\,X(S) = \varinjlim \mathrm{Aut}\,X(S_i)\,.$$

Comme les S_i appartiennent à C_k, les homomorphismes

$$\alpha_{S_i} : \mathrm{Hom}\,(S_i, A) \to \mathrm{Aut}\,X(S_i)$$

sont des isomorphismes. Il en est donc de même de α_S.

4.6. Corollaire. *Soit K une extension de k. Alors:*

(a) *Le foncteur* Aut $(X \otimes K)$ *est représentable par $A \otimes K$. En particulier le groupe* Aut $X(K)$ *s'identifie à $A(K)$.*

(b) *Si X est quasi-projective, les K-formes de $X \otimes K$ correspondent bijectivement aux éléments de $H^1(K, A)$.*

L'assertion (a) est une conséquence immédiate de la proposition précédente (en considérant C_K comme sous-catégorie de Red_k). L'assertion (b) résulte de (a) et de 2.6.

4.7. Opérations effectives. Soit X une variété algébrique (resp. un groupe algébrique) sur k, soit A un groupe algébrique sur k, et supposons que A opère sur X. On dit que A opère *effectivement* s'il existe une famille finie $(x_i)_{i \in I}$ de points de $X(\bar{k})$ telle que les relations $a \cdot x_i = a' \cdot x_i$ pour tout $i \in I$, avec $a, a' \in A(k)$, entraînent $a = a'$. Si $Y \in C_k$, l'application canonique de Hom (Y, A) dans Aut $X(Y)$ est alors *injective.*

Lemme. *Supposons k de caractéristique zéro. Soient X une variété algébrique (resp. un groupe algébrique) sur k, A un groupe algébrique opérant effectivement sur X, et Y un élément de C_k agissant sur X. On suppose que, pour tout $y \in Y(\bar{k})$, l'automorphisme correspondant de $X \otimes \bar{k}$ peut être défini par un élément*

de $A(\bar{k})$. L'action de Y sur X provient alors d'un morphisme de Y dans A, et ce morphisme est unique.

Soit $(x_i)_{i\in I}$ une famille finie de points de $X(\bar{k})$ telle que les relations $a\cdot x_i = a'\cdot x_i$ pour tout $i\in I$ entraînent $a = a'$. Considérons l'application $m: A(\bar{k}) \to X(\bar{k})^I$ définie par la formule

$$m(a) = (a\cdot x_i)_{i\in I}\ .$$

Par hypothèse cette application est injective. Son image est l'orbite d'un groupe algébrique d'automorphismes de $X(\bar{k})^I$, donc est simple (nous commettons ici l'abus de langage consistant à identifier le schéma $X\otimes\bar{k}$ avec l'ensemble de ses points à valeurs dans $\bar{k}$, et de même pour A). Comme la caractéristique de k est nulle, on obtient ainsi un *isomorphisme* de $A\otimes\bar{k}$ sur une sous-variété algébrique de $(X\otimes\bar{k})^I$. Soit alors q l'application de $Y(\bar{k})$ dans $X(\bar{k})^I$ définie par la formule

$$q(y) = (y\cdot x_i)_{i\in I}\ .$$

Par hypothèse, l'image de q est contenue dans celle de m. On en déduit l'existence d'un morphisme $f: Y\otimes\bar{k}\to A\otimes\bar{k}$ tel que

$$f(y)\cdot x_i = y\cdot x_i \text{ pour tout } i\in I \quad (y\in Y(\bar{k}))\ .$$

Si $y\in Y(\bar{k})$, il existe par hypothèse un élément $F(y)\in A(k)$ tel que $y\cdot x = F(y)\cdot x$ pour tout $x\in X(\bar{k})$. En appliquant ceci à $x = x_i$ $(i\in I)$, on voit que $F(y) = f(y)$. On a donc:

$$f(y)\cdot x = y\cdot x \text{ pour tout } y\in Y(\bar{k}) \text{ et tout } x\in X(\bar{k})\ .$$

Il reste à voir que f est défini sur k, autrement dit (cf. n° 4.1) que $f({}^s y) = {}^s(f(y))$ pour tout $s\in\mathbf{g}$ et tout $y\in Y(\bar{k})$. Or, si $x\in X(\bar{k})$, on a:

$$f({}^s y)\cdot {}^s x = {}^s y\cdot {}^s x = {}^s(y\cdot x) = {}^s(f(y)\cdot x) = {}^s(f(y))\cdot {}^s x\ ,$$

ce qui montre que $f({}^s y)$ et ${}^s(f(y))$ opèrent de la même manière sur $X(\bar{k})$. Ils sont donc égaux.

4.8. Proposition. *Supposons k de caractéristique zéro. Soient X une variété algébrique (resp. un groupe algébrique) sur k, et A_0 un groupe algébrique connexe sur k opérant effectivement sur X, de manière à vérifier la propriété universelle suivante:*

(*) *Si V est une variété algébrique connexe sur $\bar{k}$ agissant sur $X\otimes\bar{k}$, et si, pour un $v\in V(\bar{k})$, l'automorphisme correspondant de $X\otimes\bar{k}$ peut être défini par un élément de $A_0(\bar{k})$, il en est de même pour tous les éléments de $V(\bar{k})$.*

Alors Aut X *est un groupe localement algébrique sur* k, *dont* A_0 *est la composante neutre.*

(De façon plus précise, le foncteur Aut X est représentable par un groupe localement algébrique A dont la composante neutre s'identifie canoniquement à A_0, en tant que groupe opérant sur X.)

Supposons tout d'abord k algébriquement clos. Le groupe $A_0(k)$ s'identifie à un sous-groupe de Aut $X(k)$. Soit $b \in \mathrm{Aut}\, X(k)$. On peut faire opérer A_0 sur X en faisant correspondre à tout $a \in A_0(k)$ l'automorphisme bab^{-1} de X; lorsque $a = 1$, on a $bab^{-1} = 1$. L'hypothèse (*) et le lemme 4.7 montrent alors qu'il existe un unique automorphisme $\sigma_b : A_0 \to A_0$ tel que $\sigma_b(a) = bab^{-1}$ pour tout $a \in A_0(k)$; en particulier, $A_0(k)$ est un sous-groupe *distingué* de Aut $X(k)$ et les automorphismes de A_0 induits par les automorphismes intérieurs de Aut $X(k)$ respectent la structure algébrique de $A_0(k)$. Chaque classe à gauche de Aut $X(k)$ modulo $A_0(k)$ possède donc une unique structure de k-variété telle que la translation $a \mapsto b \cdot a$ $(a \in A_0(k),\ b \in \mathrm{Aut}\, X(k))$ soit un isomorphisme de la variété $A_0(k)$ sur $b \cdot A_0(k)$; en faisant la somme disjointe de ces variétés, on obtient un groupe localement algébrique A, opérant sur X, de composante neutre A_0, et tel que $A(k) = \mathrm{Aut}\, X(k)$. Il reste à voir que A représente le foncteur Aut X. Pour cela, considérons d'abord une variété connexe V agissant sur X. Si $v \in V(k)$, notons v' l'élément de $A(k)$ défini par v. Soient u et v_0 deux éléments de $V(k)$. L'hypothèse (*) entraîne que $(v_0^{-1}u)' \in A_0(k)$; d'après 4.7 il existe donc un unique morphisme $f : V \to A_0$ tel que $(v_0^{-1}u)' = (v_0^{-1})' f(u)$ pour tout $u \in V(k)$, d'où un morphisme $g : V \to A$ tel que $u' = g(u)$ pour tout $u \in V(k)$. Soit Y un élément quelconque de C_k agissant sur X. Comme Y est réunion disjointe de sous-variétés ouvertes du type ci-dessus, ce qui précède montre qu'il existe un unique morphisme $g : Y \to A$ tel que Y agisse sur X par l'intermédiaire de g. On a donc bien démontré que A représente Aut X.

Revenons maintenant au cas général, où k n'est pas nécessairement algébriquement clos. On vient de prouver l'existence d'un groupe localement algébrique $\bar{A}$ sur $\bar{k}$, de composante neutre $A_0 \otimes \bar{k}$, qui représente Aut $(X \otimes \bar{k})$. Admettons pour l'instant que $\bar{A}$ peut s'écrire sous la forme $\bar{A} = A \otimes \bar{k}$, où A est un groupe localement algébrique sur k, l'identification $A(\bar{k}) = \mathrm{Aut}\, X(\bar{k})$ étant un isomorphisme de g-groupes. Vu 4.1, cette dernière condition implique que l'opération de $\bar{A}$ sur $X \otimes \bar{k}$ provient, par extension des scalaires, d'une opération de A sur k. Montrons que A représente Aut X. Soit $Y \in C_k$ agissant sur X. Il existe alors un unique morphisme $\bar{g} : Y \otimes \bar{k} \to \bar{A}$ tel que $Y \otimes \bar{k}$ agisse sur $X \otimes \bar{k}$ à travers $\bar{g}$. On voit alors exactement comme au n° 4.7 que ${}^s\bar{g} = \bar{g}$ pour tout $s \in \mathbf{g}$; donc $\bar{g}$ provient d'un morphisme $g : Y \to A$, ce qui montre bien que

A représente Aut X. De plus, il est clair que la composante neutre de A s'identifie à A_0. La proposition sera donc démontrée si nous prouvons l'existence de A.

Le groupe $A_0(\bar{k})$ opère par translations à gauche sur $\bar{A}(\bar{k})$; ses orbites sont des ensembles ouverts et fermés disjoints, et pour tout $b \in \bar{A}(\bar{k})$, le groupe de stabilité de b est réduit à l'élément neutre. Il est clair que la structure algébrique de $\bar{A}$ est complètement déterminée par celle de A_0 et par les conditions précédentes. L'existence de A résulte alors de la proposition suivante:

4.9. Proposition. *Soit B un k-groupe algébrique, et soit M un ensemble sur lequel $B(\bar{k})$ et $\mathbf{g}$ opèrent. Supposons vérifiées les deux conditions suivantes:*

(i) *Pour tout $m \in M$, le groupe de stabilité de m dans $B(\bar{k})$ est le groupe des $\bar{k}$-points d'un sous-groupe algébrique H_m de $B \otimes \bar{k}$.*

(ii) *$\mathbf{g}$ opère continûment sur M, et l'on a ${}^s(b \cdot m) = {}^s b \cdot {}^s m$ pour $s \in \mathbf{g}$, $b \in B(\bar{k})$, et $m \in M$.*

Il existe alors $Y \in C_k$ ayant les propriétés suivantes: B opère sur Y; l'ensemble $Y(\bar{k})$ s'identifie à M de façon compatible avec les opérations de $B(\bar{k})$ et de $\mathbf{g}$; pour tout $y \in Y(\bar{k})$, correspondant à $m \in M$, l'orbite $B(\bar{k}) \cdot y$ de y est ouverte et fermée dans $Y(\bar{k})$, et isomorphe à $(B/H_m)(\bar{k})$.

(On applique cette proposition en prenant $B = A_0$, $M = \bar{A}(\bar{k}) = \mathrm{Aut}\, X(\bar{k})$.)

L'ensemble M est réunion disjointe d'ensembles de la forme $B(\bar{k}) \cdot \mathbf{g}(m)$, $m \in M$, où $\mathbf{g}(m)$ désigne l'orbite de m par $\mathbf{g}$. Vu (ii), $\mathbf{g}(m)$ est fini. Il suffit donc de considérer le cas où le quotient X de M par $B(\bar{k})$ est *fini*. L'ensemble X est muni d'une structure de $\mathbf{g}$-ensemble, quotient de celle de M; si $x \in X$, on notera ${}^s x$ son transformé par $s \in \mathbf{g}$. Pour tout $x \in X$, choisissons un représentant $\alpha(x)$ de x dans M; il existe une extension galoisienne finie k_1/k telle que ${}^s\alpha(x) = \alpha(x)$ pour tout $s \in \mathbf{h}$, où $\mathbf{h} = \mathbf{g}(\bar{k}/k_1)$; le groupe $\mathbf{h}$ opère alors trivialement sur X. Il résulte des hypothèses (i) et (ii) que, si $x \in X$ et $s \in \mathbf{g}$, on a ${}^s(H_{\alpha(x)}) = H_{s_{\alpha(x)}}$; en particulier (prenant $s \in \mathbf{h}$) on voit que les $H_{\alpha(x)}$ sont définis sur k_1. De plus, ${}^s\alpha(x)$ et $\alpha({}^s x)$ font partie de la même orbite de $B(\bar{k})$; il existe donc $u_{s,x} \in B(\bar{k})$ tel que ${}^s\alpha(x) = u_{s,x}\alpha({}^s x)$.

Soit maintenant V la k_1-variété somme des espaces homogènes $(B \otimes k_1)/H_{\alpha(x)}$, $x \in X$. On identifie $V(\bar{k})$ à M en faisant correspondre à $b' \in B(\bar{k})/H_{\alpha(x)}(\bar{k})$ le transformé $b \cdot \alpha(x)$ de $\alpha(x)$ par un représentant b de b'. Cette identification permet de transporter à $V(\bar{k})$ la structure de $\mathbf{g}$-ensemble de M; nous noterons $s(v)$ le transformé, pour cette structure, de l'élément $v \in V(\bar{k})$ par l'élément

$s \in \mathbf{g}$. Si $v \in B(\bar{k})/H_{\alpha(x)}(\bar{k})$, et si b est un représentant de v, on vérifie immédiatement la formule:

$$s(v) = {}^s b \cdot u_{s,x} \cdot \alpha({}^s x) . \tag{1}$$

Nous allons voir que les conditions (a), (b), (c) du lemme 2.12 sont vérifiées par la variété V et par la structure de $\mathbf{g}$-ensemble de $V(\bar{k})$. La variété ${}^s V (s \in \mathbf{g})$ est somme disjointe des espaces homogènes $(B \otimes k_1)/{}^s H_{\alpha(x)} = (B \otimes k_1)/H_{s_{\alpha(x)}}$, et, si v, b sont comme ci-dessus, ${}^s v$ est l'image de ${}^s b$ par la projection naturelle de $B(\bar{k})$ sur $B(\bar{k})/{}^s H_{\alpha(x)}$. Soit $f_s : ({}^s V)(\bar{k}) \to V(\bar{k})$ l'application définie dans 2.12. Il résulte de (1) que la restriction de f_s à $B(\bar{k})/{}^s H_{\alpha(x)}(\bar{k})$ est l'application de cet espace sur $B(\bar{k})/H_{\alpha({}^s x)}(\bar{k})$ induite par la translation $b \mapsto b \cdot u_{s,x}$. Elle est donc bien définie à partir d'un morphisme $F_s : {}^s V \otimes \bar{k} \to V \otimes \bar{k}$, ce qui montre que (a) est vérifiée. Si $s \in \mathbf{h}$, on a ${}^s x = x$, d'où $u_{s,x} \in H_{\alpha({}^s x)}(\bar{k})$, et $F_s = 1$, ce qui établit (b). Enfin, la condition (c) provient de ce que tout sous-ensemble fini d'un espace homogène est contenu dans un ouvert affine (cf. [17], p. 111). On peut donc descendre le corps de base de V de k_1 à k, et la variété Y ainsi obtenue vérifie les conditions voulues.

Indiquons une application de la proposition 4.9:

4.10. Construction de variétés de sous-groupes. Soit B un k-groupe algébrique et soit M un ensemble non vide de sous-groupes algébriques de $B \otimes \bar{k}$. Faisons les deux hypothèses suivantes:

(a) Si $C \in M$, on a ${}^s C \in M$ pour tout $s \in \mathbf{g}$.

(b) Le groupe $B(\bar{k})$ opère transitivement (par conjugaison) sur M. (En d'autres termes, si $C_0 \in M$, les éléments de M sont les sous-groupes de la forme $\mathrm{Int}\, x\,(C_0)$, avec $x \in B(\bar{k})$.)

Les groupes $\mathbf{g}$ et $B(\bar{k})$ opèrent sur M. De plus, le groupe d'isotropie d'un élément $C \in M$ est le groupe $N(\bar{k})$ des $\bar{k}$-points du *normalisateur* de C dans $B \otimes \bar{k}$. Toutes les hypothèses de 4.9 sont donc vérifiées. On en conclut qu'il existe un espace homogène V de B et une bijection $V(\bar{k}) \to M$ compatible avec les opérations de $\mathbf{g}$ et de $B(\bar{k})$. En particulier, les éléments de $V(k)$ correspondent aux sous-groupes $C \in M$ qui sont définis sur k. On dit que V est la *variété des sous-groupes appartenant à* M. Si $C \in M$, et si N est le normalisateur de C, il est clair que $V \otimes \bar{k}$ est isomorphe à $(B \otimes \bar{k})/N$.

Lorsque k est un corps *fini*, et B *connexe*, alors, d'après un théorème de Lang [12], V possède un point à valeurs dans k, et il existe $C \in M$ défini sur k. Si de plus le normalisateur N de C est *connexe*, et $C' \in M$ est défini sur k,

il existe $b \in B(k)$ tel que Int $(C) = C'$; en effet, le sous-schéma de B formé des éléments transformant C dans C' est un espace homogène de N, et possède donc un point à valeurs dans k, d'après le théorème de LANG cité ci-dessus.

Comme exemple d'ensemble M, on peut prendre, lorsque B est linéaire, l'ensemble des tores maximaux (resp. des sous-groupes de CARTAN, resp. des sous-groupes résolubles connexes maximaux) de $B \otimes \bar{k}$. D'après ce qui précède, si B est linéaire connexe, et si k est fini, B possède un tore maximal (resp. un sous-groupe de CARTAN, resp. un sous-groupe résoluble connexe maximal) défini sur k.

4.11. Remarque. Dans tout ce qui précède, nous nous sommes placés dans le cadre de la catégorie $\mathcal{C}_k$; on pourrait également considérer la catégorie plus vaste $\mathcal{C}_k^*$ formée des sommes disjointes de schémas algébriques non nécessairement réduits (ou même la catégorie de tous les schémas). Si X est une k-variété, le foncteur Aut $X : \mathcal{C}_k \to \mathcal{G}r$ se prolonge en un foncteur Aut* $X : \mathcal{C}_k^* \to \mathcal{G}r$. *Il se peut que* Aut X *soit représentable sans que* Aut*X *le soit,* et cela même si la caractéristique de k est zéro, et même si X est un groupe linéaire. Un exemple simple est fourni par $X = \mathbf{G}_a \times \mathbf{G}_m$. Dans ce cas, Aut X est représentable par le groupe $A = \mathbf{G}_m \times \mathbf{Z}/2\mathbf{Z}$ opérant de manière évidente; si Aut*X était représentable, il le serait par le même groupe A (cela résulte du fait que, en caractéristique zéro, tout schéma en groupes localement de type fini est automatiquement réduit). Or, il est facile de voir que, si l'on prend $V = \mathrm{Spec}\, k[T]/(T^2)$, le groupe Aut*$X(V)$ est strictement plus grand que le groupe $A(V)$ [le groupe $\mathbf{G}_a \times \mathbf{G}_m$ a des automorphismes «infinitésimaux» qui ne proviennent pas de l'action d'un groupe algébrique]. Le foncteur Aut*X n'est donc pas représentable.

§ 5. Groupe d'automorphismes d'un groupe algébrique linéaire

Dans ce paragraphe, k désigne un corps *de caractéristique zéro,* et $\mathbf{g}$ le groupe de GALOIS de $\bar{k}$ sur k. Nous nous proposons de démontrer que le foncteur d'automorphismes d'un k-groupe algébrique linéaire est un groupe localement algébrique de type (ALA) (cf. n° 4.3). Pour passer des groupes réductifs ou unipotents au cas général, nous utiliserons la proposition suivante, qui précise un résultat de MOSTOW [14]:

5.1. Proposition. *Soit G un k-groupe algébrique linéaire, et soit U son radical unipotent. Il existe alors un sous-groupe algébrique H de G (défini sur k) tel que G soit produit semi-direct de H et de U. Deux tels sous-groupes sont*

conjugués par un élément de $U(k)$. *Tout k-sous-groupe réductif* L *de* G *est conjugué à un sous-groupe de* H *par un élément de* $U(k)$.

(On rappelle que le *radical unipotent* d'un groupe algébrique linéaire G est par définition le plus grand sous-groupe algébrique distingué unipotent de G.)

Cette proposition est connue lorsque $G(k)$ est dense dans G (cf. [14], théorème 7.1), donc en particulier lorsque $k = \bar{k}$. Par conséquent, $U(\bar{k})$ opère transitivement, par automorphismes intérieurs, sur l'ensemble M des sous-groupes algébriques $\bar{H}$ de $G \otimes \bar{k}$ tels que $G \otimes \bar{k}$ soit produit semi-direct de $\bar{H}$ et de $U \otimes \bar{k}$. Les conditions de 4.10 sont vérifiées; il existe donc un espace homogène V de U tel que $M = V(\bar{k})$. Puisque U est unipotent et k parfait, un théorème de ROSENLICHT ([15], théorème 10) montre que $V(k)$ est non vide, d'où la première assertion. Si H et H' sont deux éléments de $V(k)$, soit P l'ensemble des éléments de $U(\bar{k})$ qui transforment H en H'; si U' désigne le groupe de stabilité de H dans U, il est clair que le $\mathbf{g}$-ensemble P est un espace homogène principal de $U'(\bar{k})$. Comme U' est unipotent, P possède un point invariant par $\mathbf{g}$, d'où la deuxième assertion. Enfin, soit $G' = L \cdot U$. Le groupe G' est produit semi-direct de U et de $L' = G' \cap H$; la dernière assertion résulte donc des deux premières, appliquées à G'.

Remarque. Soit H un k-sous-groupe de G. La proposition précédente montre que G est produit semi-direct de H et de U si et seulement si H est réductif maximal.

5.2. Notations. Dans toute la suite de ce paragraphe, G est un k-groupe algébrique *linéaire*, U son radical unipotent, H un sous-groupe algébrique réductif maximal de G. On note H^0 la composante neutre de H et S (resp. T) le groupe dérivé (resp. la composante neutre du centre) de H^0; le groupe S est *semi-simple*, le groupe T est un *tore*, on a $H^0 = S \cdot T$, et $S \cap T$ est fini.

Si M est un groupe algébrique quelconque, on note $Z(M)$ le *centre* de M. Si N est un sous-groupe algébrique de M, soit $N' = N \cap Z(M)$; le groupe N/N' opère effectivement sur M (par automorphismes intérieurs); on le note $\mathrm{Int}_M N$. En particulier, $\mathrm{Int}_H H^0$ s'identifie à $H^0/(H^0 \cap Z(H))$.

5.3. Cas élémentaires. Enumérons d'abord quelques cas où il est facile de vérifier que Aut G est, soit un groupe algébrique linéaire, soit un groupe discret de type arithmétique:

(a) Si G est *fini*, Aut G est fini.

(b) Si G est *unipotent*, l'exponentielle permet de transformer Aut G en le foncteur d'automorphismes de *l'algèbre de* LIE de G; cela montre que Aut G est un groupe algébrique linéaire.

(c) Si G est *semi-simple connexe*, Aut G est un groupe algébrique dont la composante neutre est le *groupe adjoint* $\mathrm{Int}_G G = G/Z(G)$ de G.

(d) Si $G = (\mathbf{G}_m)^n$, Aut G est le groupe localement algébrique de dimension zéro défini par $\mathbf{GL}_n(\mathbf{Z})$, considéré comme groupe discret sur lequel $\mathbf{g}$ opère trivialement; cela s'écrit plus simplement:

$$\mathrm{Aut}\,(\mathbf{G}_m)^n = \mathbf{GL}_n(\mathbf{Z})\,.$$

Plus généralement, si T est un *tore* quelconque, et si Y désigne le $\mathbf{g}$-module des groupes à 1 paramètre de $T \otimes \bar{k}$ (cf. [6], exposé 11), Aut T s'identifie au $\mathbf{g}$-groupe Aut Y, cf. n° 3.5.

Nous ramènerons le cas général à ces différents cas particuliers en utilisant les décompositions $G = H \cdot U$ et $H^0 = S \cdot T$ introduites ci-dessus.

5.4. Le groupe Aut H.

Proposition. (a) *Le foncteur d'automorphismes* Aut H *est un groupe localement algébrique dont la composante neutre* B^0 *est égale à* $\mathrm{Int}_H H^0$.

(b) *Le noyau* B_1 *du morphisme canonique* Aut $H \to$ Aut $T \times$ Aut (H/H^0) *est un sous-groupe ouvert de* Aut H.

Pour démontrer (a), il suffit (cf. prop. 4.8) de prouver que, si V est une $\bar{k}$-variété connexe agissant sur $H \otimes \bar{k}$ par l'intermédiaire d'un morphisme ϱ, et si $\varrho(v) \in \mathrm{Int}_H H^0(\bar{k})$ pour un $v \in V(\bar{k})$, alors $\varrho(V(\bar{k})) \subset \mathrm{Int}_H H^0(\bar{k})$. Quitte à remplacer k par $\bar{k}$, on peut supposer k algébriquement clos, ce qui nous permettra d'identifier une variété algébrique à l'ensemble de ses points.

Il est clair que V agit trivialement sur T et sur H/H^0, et que V agit sur S par automorphismes intérieurs (cf. 5.3). Commençons par traiter un cas particulier:

(i) V *agit trivialement sur* H^0. Soit F le groupe fini H/H^0; le groupe F opère par automorphismes intérieurs sur le groupe abélien $Z(H^0)$. Soit L (resp. M) le groupe des 1-cocycles (resp. 1-cobords) de F à valeurs dans $Z(H^0)$. Si $n = \mathrm{Card}\,(F)$, les groupes L et M s'identifient à des sous-groupes algébriques du produit de n copies de $Z(H^0)$. De plus M est *ouvert* dans L; en effet, $M/L = H^1(F, Z(H^0))$ est un groupe algébrique dont tout élément est d'ordre divisant n (en vertu d'une propriété bien connue des groupes de cohomologie), et, puisque k est de caractéristique zéro, c'est un groupe fini. Si $z \in L$, l'application $u_z : H \to H$ définie par la formule:

$$u_z(x) = z(\bar{x}) \cdot x \quad (x \in H,\ \bar{x} \text{ projection de } x \text{ dans } F)\,,$$

est un automorphisme de H. On vérifie immédiatement que l'on obtient ainsi une bijection σ de L sur l'ensemble des automorphismes de H qui agissent

trivialement sur H^0 et H/H^0; on a $\sigma(M) = \mathrm{Int}_H Z(H^0) = \sigma(L) \cap \mathrm{Int}_H H^0$. L'application $\sigma^{-1} \circ \varrho : V \to L$ est alors un morphisme qui applique v dans M, donc aussi V dans M puisque V est connexe et M ouvert dans L; cela démontre (a) dans le cas considéré.

(ii) *Cas général.* Soit V' la sous-variété de $V \times S$ formée des couples (x, s) tels que $\varrho(x) = \mathrm{Int}_{H^0}(s^{-1})$ sur H^0; on vérifie facilement que c'est un revêtement galoisien étale de V, de groupe de GALOIS le groupe $Z(S)$. L'image réciproque de v dans V' est formée de couples $(v, s_i)_{i \in I}$, avec $s_i \in S$; on sait (c'est une propriété générale des revêtements étales) que toute composante connexe V'_α de V' contient l'un des (v, s_i). Faisons agir V' sur H en faisant correspondre à $(x, s) \in V'$ l'automorphisme $\varrho(x) \cdot \mathrm{Int}_H(s)$. Cette action de V' sur H est triviale sur H^0 et sur H/H^0; de plus, les automorphismes correspondant aux points (v, s_i) appartiennent à $\mathrm{Int}_H H^0$ par hypothèse. En appliquant (i) aux V'_α, on en conclut que tous les $\varrho(x) \cdot \mathrm{Int}_H(s)$, avec $(x, s) \in V'$, appartiennent à $\mathrm{Int}_H H^0$; il en est alors de même des $\varrho(x)$, ce qui achève la démonstration de (a).

Passons à (b). Il est clair que B_1 contient B^0, donc est un sous-groupe localement algébrique ouvert de $B = \mathrm{Aut}\, H$. Pour prouver que c'est un groupe algébrique, il faut montrer que B_1/B^0 est fini. Ici encore on peut supposer que $k = \bar{k}$. Soit B_2 le sous-groupe de B_1 formé des éléments dont la restriction à S est un automorphisme intérieur. Comme B_1/B_2 est fini, on est ramené à prouver que B_2/B^0 est fini. Les groupes B_2 et B^0 contiennent respectivement les groupes $\sigma(L)$ et $\sigma(M)$ introduits dans (i). De plus, L/M s'applique *sur* B_2/B^0; en effet, si $u \in B_2$, il existe $s \in S$ tel que u et $\mathrm{Int}_H(s)$ coïncident sur S, donc aussi sur H^0, et l'on peut écrire u sous la forme $u = u' \cdot \mathrm{Int}_H(s)$, avec $u' \in \sigma(L)$. Comme L/M est fini (cf. (i)), notre assertion est établie.

5.5. Les groupes C_1 et C_2. La projection canonique $\pi : G \to G/U$ induit un isomorphisme de H sur G/U (cf. n° 5.1). On posera $\bar{T} = \pi(T)$. Tout automorphisme de G définit par passage au quotient un automorphisme de G/U qui laisse stable $\bar{T}$, d'où des homomorphismes

$$\mathrm{Aut}\, G \to \mathrm{Aut}\, G/U \to \mathrm{Aut}\, \bar{T}\,.$$

D'autre part, G opère par automorphismes intérieurs sur lui-même en laissant stable U, d'où un morphisme $r : G \to \mathrm{Aut}\, U$.

Soit C le sous-foncteur de $\mathrm{Aut}\, G$ formé des automorphismes qui laissent stable H et dont l'image dans $\mathrm{Aut}\, H$ appartient au groupe $B^0 = \mathrm{Int}_H H^0$ (cf. prop. 5.4). On a un morphisme injectif

$$C \to \mathrm{Aut}\, U \times B^0\,,$$

et l'on vérifie facilement que C est un sous-groupe algébrique du groupe algébrique $\mathrm{Aut}\, U \times B^0$. De façon plus précise, $C(\bar{k})$ est l'ensemble des couples (u, v) $(u \in \mathrm{Aut}\, U(\bar{k}), v \in B^0(\bar{k}))$ qui vérifient la condition

$$u \cdot r(h) = r(v(h)) \cdot u \quad \text{pour tout} \quad h \in H(\bar{k});$$

un tel couple opère sur $G \otimes \bar{k}$ par la formule:

$$(u, v)(x \cdot y) = u(x) \cdot v(y) \quad (x \in U(\bar{k}), y \in H(\bar{k})).$$

Comme $\mathrm{Aut}\, U$ et B^0 sont des k-groupes algébriques linéaires, il en est de même de C.

Le groupe C opère par restriction sur U, et l'on peut former le produit semi-direct $U \cdot C$. On vérifie aisément que $U \cdot C$ opère sur G par l'intermédiaire d'une opération qui associe au produit $u \cdot c$ $(u \in U(\bar{k}), c \in C(\bar{k}))$ l'automorphisme $\mathrm{Int}_G(u) \cdot c$ de $G \otimes \bar{k}$. Cette opération n'est pas effective en général; nous noterons C_1 le quotient de $U \cdot C$ qui opère effectivement sur G; c'est encore un groupe algébrique linéaire, et il s'identifie (en tant que foncteur) à un sous-foncteur de $\mathrm{Aut}\, G$.

Nous noterons d'autre part C_2 le noyau du morphisme canonique

$$\mathrm{Aut}\, G \to \mathrm{Aut}\, \overline{T} \times \mathrm{Aut}\, (G/G^0).$$

Il est clair que C_1 est contenu dans C_2.

5.6. Proposition. *Le foncteur d'automorphismes* $\mathrm{Aut}\, G$ *est un groupe localement algébrique, contenant* C_1 *et* C_2 *comme sous-groupes algébriques distingués ouverts. Un élément de* $\mathrm{Aut}\, G(\bar{k})$ *appartient à* $C_1(\bar{k})$ *si et seulement si son image dans* $\mathrm{Aut}\, G/U(\bar{k})$ *appartient à* $\mathrm{Int}_{G/U}(G/U)^0(\bar{k})$.

Démontrons d'abord la deuxième assertion. Il est trivial que la condition est nécessaire. Réciproquement, soit x un élément de $\mathrm{Aut}\, G(\bar{k})$ la vérifiant. Le transformé $x(\bar{H})$ de $\bar{H} = H \otimes \bar{k}$ par x est un sous-groupe réductif maximal de $G \otimes \bar{k}$; d'après 5.1, il existe donc $u \in U(\bar{k})$ tel que $x(\bar{H}) = \mathrm{Int}_G(u)(\bar{H})$. Quitte à multiplier x à droite par $\mathrm{Int}_G(u^{-1})$, on peut donc supposer que $x(\bar{H}) = \bar{H}$. L'hypothèse entraîne alors que x appartient à $C(\bar{k})$, donc aussi à $C_1(\bar{k})$, ce qui achève de prouver notre assertion. On en déduit en particulier que $C_1(\bar{k})$ est un sous-groupe *distingué* de $\mathrm{Aut}\, G(\bar{k})$; le même résultat est évident pour C_2.

D'autre part, l'homomorphisme canonique de $\mathrm{Aut}\, G$ dans $\mathrm{Aut}\, G/U \approx \mathrm{Aut}\, H$ induit une application de $C_2(\bar{k})/C_1(\bar{k})$ dans $B_1(\bar{k})/B^0(\bar{k})$ (les

notations étant celles de 5.4); d'après ce que l'on vient de voir, cette application est injective. Comme $B_1(\bar{k})/B^0(\bar{k})$ est fini (cf. 5.4), il en est de même de $C_2(\bar{k})/C_1(\bar{k})$.

Pour terminer la démonstration, il suffit donc de prouver que la composante neutre C_1^0 de C_1 vérifie la condition (*) de la prop. 4.8. Soit donc V une $\bar{k}$-variété connexe agissant sur $G \otimes \bar{k}$, et supposons que, pour un élément v de $V(\bar{k})$, l'automorphisme correspondant appartienne à $C_1^0(\bar{k})$. D'après la prop. 5.4, les automorphismes de $G/U \otimes \bar{k}$ définis par les éléments de $V(\bar{k})$ appartiennent au groupe $\mathrm{Int}_{G/U}(G/U)^0(\bar{k})$. La deuxième assertion de 5.6, démontrée ci-dessus, entraîne alors que les automorphismes de $G \otimes \bar{k}$ définis par les éléments de $V(\bar{k})$ appartiennent à $C_1(\bar{k})$. D'après le lemme 4.7, cela signifie que V agit sur $G \otimes \bar{k}$ par l'intermédiaire d'un morphisme $V \to C_1 \otimes \bar{k}$. Comme V est connexe, ce morphisme est nécessairement à valeurs dans $C_1^0 \otimes \bar{k}$, ce qui achève la démonstration.

5.7. Le plus grand tore central de G^0. Le tore T opère sur U. On sait (cf. [6], exposé 9, lemme 2) qu'il existe une suite de composition (U_i) de $U \otimes \bar{k}$ formée de sous-groupes algébriques connexes stables par T, telle que U_i/U_{i+1} soit isomorphe au groupe additif $\mathbf{G}_a$; de plus T opère sur U_i/U_{i+1} par multiplication par un caractère χ_i et U_i est engendré par U_{i+1} et par les éléments qui sont invariants par le noyau de χ_i. Si T'désigne le plus grand tore central de G^0, on voit que $T' \otimes \bar{k}$ est la composante neutre de l'intersection des noyaux des χ_i. Chaque χ_i s'identifie à un caractère de $T/T' \otimes \bar{k}$, donc aussi de $\bar{T}/\bar{T}' \otimes \bar{k}$, avec $\bar{T} = \pi(T)$, $\bar{T}' = \pi(T')$, cf. n° 5.5. L'ensemble Ψ des caractères de $\bar{T}/\bar{T}' \otimes \bar{k}$ ainsi obtenus est indépendant du choix de T (c'est-à-dire du choix de H) ainsi que du choix de la suite (U_i); cela résulte de la prop. 5.1 combinée avec les résultats de [6], *loc. cit.* Par suite, tout automorphisme $\sigma \in \mathrm{Aut}\, G(\bar{k})$ définit un automorphisme de $\bar{T}/\bar{T}' \otimes \bar{k}$ qui laisse stable Ψ. Notons $X(\bar{T}/\bar{T}')$ le groupe des caractères de $\bar{T}/\bar{T}' \otimes \bar{k}$; comme $\bar{T}' \otimes \bar{k}$ est la composante neutre de l'intersection des noyaux des χ_i, le groupe engendré par Ψ est d'indice fini dans $X(\bar{T}/\bar{T}')$, et les automorphismes de $\bar{T}/\bar{T}' \otimes \bar{k}$ qui laissent stable Ψ forment un groupe fini. Il est clair d'autre part que le groupe C_2 opère trivialement sur $\bar{T}$. On obtient donc le résultat suivant:

5.8. Lemme. *Soit Γ le groupe* $\mathrm{Aut}\, G(\bar{k})/C_2(\bar{k})$. *Les éléments de Γ opèrent sur $\bar{T} \otimes \bar{k}$ en laissant stable $\bar{T}' \otimes \bar{k}$. Leurs images dans* $\mathrm{Aut}\,(\bar{T}/\bar{T}')(\bar{k})$ *forment un groupe fini Φ.*

5.9. Le groupe Γ_+. Les automorphismes intérieurs du groupe G/U opèrent sur la composante neutre $(G/U)^0$ et en particulier sur le tore $\bar{T}$. Comme $\bar{T}$ est contenu dans le centre de $(G/U)^0$, on voit que le quotient $(G/U)/(G/U)^0 = G/G^0$ opère sur $\bar{T}$. On notera ϑ l'homomorphisme de G/G^0 dans $\mathrm{Aut}\,\bar{T}$ ainsi défini.

Posons $W = G/G^0(\bar{k})$; les groupes W et $\mathrm{Aut}\,W$ sont des g-*groupes finis.*

Lemme. *Soit Γ_+ l'ensemble des couples $(\alpha, \beta) \in \mathrm{Aut}\,\bar{T}(\bar{k}) \times \mathrm{Aut}\,W$ qui vérifient les deux conditions suivantes*:

(a) $\alpha \cdot \vartheta(w) \cdot \alpha^{-1} = \vartheta(\beta(w))$ *pour tout* $w \in W$,

(b) α *laisse stable* $\bar{T}' \otimes \bar{k}$ *et l'élément de* $\mathrm{Aut}\,(\bar{T}/\bar{T}')(\bar{k})$ *qu'il définit appartient au groupe* Φ (cf. 5.8).

Alors Γ_+ est un g-*sous-groupe de* $\mathrm{Aut}\,\bar{T}(\bar{k}) \times \mathrm{Aut}\,W$ *contenant* Γ.

La définition de Γ au moyen de C_2 (cf. 5.8) montre que Γ s'identifie de façon naturelle à un g-sous-groupe de $\mathrm{Aut}\,\bar{T}(\bar{k}) \times \mathrm{Aut}\,W$. On a déjà vu que ses éléments vérifient (b), et il est immédiat qu'ils vérifient également (a). D'autre part, chacune des conditions (a) et (b) définit un sous-groupe de $\mathrm{Aut}\,\bar{T}(\bar{k}) \times \mathrm{Aut}\,W$ stable par $\mathbf{g}$: c'est évident pour (b), et, pour (a), cela résulte du fait que $\vartheta : W \to \mathrm{Aut}\,\bar{T}(\bar{k})$ est un morphisme de g-groupes.

5.10. Lemme. *Le groupe Γ_+ est un* g-*groupe de type arithmétique* (cf. 3.4), *et Γ est d'indice fini dans Γ_+. En particulier, Γ est un* g-*groupe de type arithmétique.*

Soit Y le g-module des *groupes à* 1 *paramètre* de $\bar{T} \otimes \bar{k}$, autrement dit le dual du groupe $X(\bar{T})$ des caractères de $\bar{T} \otimes \bar{k}$, et soit Y' celui de $\bar{T}'$ (cf. [6], exposé 11). Ce sont des $\mathbf{Z}$-modules libres de type fini, et Y' est facteur direct de Y (comme groupe abélien — pas nécessairement comme g-module). Les g-groupes $\mathrm{Aut}\,\bar{T}(\bar{k})$ et $\mathrm{Aut}\,\bar{T}'(\bar{k})$ s'identifient respectivement à $\mathrm{Aut}\,Y$ et $\mathrm{Aut}\,Y'$ (cf. 5.3), et Φ s'identifie à un g-sous-groupe de $\mathrm{Aut}\,Y/Y'$. On peut donc considérer Γ_+ comme le sous-groupe de $\mathrm{Aut}\,Y \times \mathrm{Aut}\,W$ formé des couples (α, β) vérifiant des conditions (a') et (b') qui se déduisent immédiatement de (a) et de (b).

Pour préciser ceci, choisissons une base $(e_1, \ldots, e_n)$ de Y dont les m premiers éléments forment une base de Y' ($n = \dim \cdot T$, $m = \dim \cdot T'$). Les éléments de Φ s'identifient à des éléments de $\mathbf{GL}_{n-m}(\mathbf{Z})$. De même, les automorphismes $\vartheta(w)$ et les éléments α vérifiant (b') s'identifient à des éléments de $\mathbf{GL}_n(\mathbf{Z})$ de la forme

$$\begin{pmatrix} * & * \\ 0 & \varphi \end{pmatrix}, \quad \text{avec } \varphi \in \Phi .$$

Soit $Tr_{n,m}$ le sous-groupe de $\mathbf{GL}_n$ dont les éléments sont de la forme $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ comme ci-dessus; c'est un groupe algébrique sur $\mathbf{Q}$ (provenant d'ailleurs d'un schéma en groupes sur $\mathbf{Z}$), et l'on a un homomorphisme canonique $Tr_{n,m} \to \mathbf{GL}_{n-m}$. L'image réciproque de Φ par cet homomorphisme est un $\mathbf{Q}$-groupe algébrique Σ. Dans le produit $\Sigma \times \mathrm{Aut}\, W$, les couples (α, β) vérifiant la condition (a') sont les points d'un $\mathbf{Q}$-sous-groupe algébrique Σ', dont Γ_+ est un sous-groupe de type arithmétique. De plus, les éléments de $\mathbf{g}$ définissent des automorphismes de Σ' qui laissent stable Γ_+; cela achève de prouver que Γ_+ est un $\mathbf{g}$-groupe de type arithmétique.

Il reste à montrer que Γ est d'indice fini dans Γ_+. Nous allons plus précisément construire un sous-groupe de $\mathrm{Aut}\, G(\bar{k})$ qui s'applique isomorphiquement sur un sous-groupe Γ_- d'indice fini de Γ_+.

D'après le lemme 5.11 ci-après, il existe un sous-groupe fini $\bar{W}$ de $H(\bar{k})$ qui s'applique *sur* $W = H/H^0(\bar{k})$ par la projection canonique. La décomposition $H^0(\bar{k}) = T(\bar{k}) \cdot S(\bar{k})$ permet d'écrire les éléments de $\bar{W} \cap H^0(\bar{k})$ sous la forme $t_i \cdot s_i$, avec $t_i \in T(\bar{k})$ et $s_i \in S(\bar{k})$. Soit P le sous-ensemble de $T(\bar{k})$ réunion des t_i et de $T(\bar{k}) \cap S(\bar{k})$; c'est un ensemble fini, dont tout élément est d'ordre fini dans $T(\bar{k})$. Soit $\bar{P}$ le sous-ensemble correspondant de $\bar{T}(\bar{k})$. On définit Γ_- comme le sous-groupe de Γ_+ formé des couples (α, β) tels que:

(i) $\beta = 1$ (ce qui, vu (a), entraîne que α commute à tous les $\vartheta(w)$, $w \in W$),

(ii) α laisse fixes les éléments de $\bar{P}$,

(iii) l'élément de Φ défini par α est égal à 1.

Il est clair que Γ_- est un sous-groupe d'indice fini de Γ_+. Soit d'autre part $(\alpha, 1) \in \Gamma_-$. Identifions α à un automorphisme de $T \otimes \bar{k}$, et prolongeons-le en un automorphisme de $H^0 \otimes \bar{k}$ qui soit l'identité sur $S \otimes \bar{k}$; c'est possible puisque α laisse fixes les éléments de $T(\bar{k}) \cap S(\bar{k})$, en vertu de la condition (ii). De même, (i) et (ii) permettent de prolonger α en un automorphisme de $H \otimes \bar{k}$ qui soit l'identité sur $\bar{W}$. Enfin, la décomposition $G = H \cdot U$ permet de prolonger α en un automorphisme de la variété $G \otimes k$, au moyen de la formule

$$\alpha(h \cdot u) = \alpha(h) \cdot u \quad (h \in H(\bar{k}),\ u \in U(\bar{k}))\ .$$

On obtient de cette manière un automorphisme du *groupe* algébrique $G \otimes \bar{k}$; en effet, il suffit de vérifier que l'on a l'identité

$$huh^{-1} = \alpha(h) u \alpha(h)^{-1} \quad (h \in H(\bar{k})\ ,\ u \in U(\bar{k}))\ .$$

Or, il résulte de (iii) que $\alpha(h) = t' \cdot h$ avec $t' \in T'(\bar{k})$, et l'identité ci-dessus provient du fait que T' centralise U. On a bien obtenu ainsi un relèvement du groupe Γ_- dans $\mathrm{Aut}\, G(\bar{k})$.

Il nous reste à démontrer le lemme suivant, utilisé en cours de démonstration:

5.11. Lemme. *Soit L un k-groupe algébrique linéaire. Il existe un sous-groupe fini $\bar{W}$ de $L(\bar{k})$ qui rencontre chaque composante connexe de $L(\bar{k})$.*

On peut supposer que $\bar{k} = k$, ce qui nous permettra d'identifier L et $L(\bar{k})$. Soit C un sous-groupe de CARTAN de L^0 et soit N son normalisateur dans L. Comme les sous-groupes de CARTAN de L^0 sont conjugués par automorphismes intérieurs, N rencontre chaque composante connexe de L; de plus, par définition même des sous-groupes de CARTAN, on a $N^0 = C$. On est donc ramené au cas où $L^0 = C$ est *nilpotent*, puis (en utilisant la suite centrale descendante de L^0), au cas où L^0 est *commutatif*. Soit $W = L/L^0$; l'extension L de W par L^0 est alors caractérisée par une classe de cohomologie $\gamma \in H^2(W, L^0)$. Soit n l'ordre de W. L'homomorphisme $f: L^0 \to L^0$ qui applique x sur x^n est surjectif et de noyau R fini (puisque k est de caractéristique zéro). La suite exacte de cohomologie, appliquée à la suite exacte de coefficients

$$0 \to R \to L^0 \xrightarrow{f} L^0 \to 0$$

donne alors la suite exacte

$$H^2(W, R) \to H^2(W, L^0) \xrightarrow{n} H^2(W, L^0).$$

Comme W est d'ordre n, l'homomorphisme $n: H^2(W, L^0) \to H^2(W, L^0)$ est nul. Il s'ensuit que γ est l'image d'un élément $\bar{\gamma}$ de $H^2(W, R)$. Ce dernier représente une extension $\bar{W}$ de W par R, qui s'applique dans L par un homomorphisme compatible avec la projection sur W. Le groupe $\bar{W}$ répond donc à la question.[1])

5.12. Théorème. *Le foncteur des automorphismes d'un groupe algébrique linéaire sur un corps de caractéristique zéro est un groupe localement algébrique de type* (ALA).

Cela résulte de la proposition 5.4 et du lemme 5.10.

5.13. Remarque. Si G est un groupe algébrique quelconque (non nécessairement linéaire) nous ignorons si Aut G est encore un groupe localement algébrique. En tout cas, ce n'est pas toujours un groupe de type (ALA), comme le montre l'exemple du produit semi-direct d'une variété abélienne par un groupe fini (le groupe fini opérant de façon non triviale sur la variété abélienne).

[1]) Si L est réductif, C est un tore, et la démonstration vaut sans changement sur un corps de caractéristique quelconque. En fait, le lemme 5.11 est valable pour un groupe algébrique (non nécessairement linéaire) sur un corps parfait quelconque K, et l'on peut en outre démontrer l'existence d'un sous-groupe W défini sur K.

§ 6. Théorèmes de finitude (corps locaux)

6.1. Théorème. *Si k est un corps localement compact de caractéristique zéro, et si A est un k-groupe de type* (ALA), *$H^1(k, A)$ est fini.*

(En particulier, $H^1(k, G)$ est fini quand G est un groupe algébrique linéaire défini sur k.)

On sait que tout corps commutatif localement compact de caractéristique zéro est isomorphe à $\mathbf{R}$, à $\mathbf{C}$, où à un corps p-adique (extension finie du corps $\mathbf{Q}_p$). Il est classique qu'un tel corps n'a qu'*un nombre fini d'extensions de degré donné*. Indiquons-en brièvement une démonstration: il suffit de prouver que tout corps p-adique n'a qu'un nombre fini d'extensions totalement ramifiées de degré n donné. Or une telle extension est définie par une «équation d'EISENSTEIN» de degré n; ces équations forment un espace compact (pour la topologie définie par la convergence des coefficients), et deux équations assez voisines définissent des extensions isomorphes (cf. par exemple [1], p. 41); d'où la finitude en question.

Le théorème 6.1 est donc une conséquence du suivant:

6.2. Théorème. *Soit k un corps parfait n'ayant qu'un nombre fini d'extensions de degré donné. Si A est un k-groupe de type* (ALA), *$H^1(k, A)$ est fini.*

(Outre le cas p-adique, l'hypothèse faite sur k est vérifiée par les corps finis, et par les corps de séries formelles à une variable sur un corps algébriquement clos de caractéristique zéro.)

Notons $\mathfrak{g}$ le groupe de GALOIS de $\bar{k}/k$. Nous allons procéder par étapes:

(a) *Finitude de $H^1(\mathfrak{g}, \Gamma)$ lorsque Γ est un $\mathfrak{g}$-groupe de type arithmétique.*

D'après la proposition 3.3, il existe un entier n tel que tout sous-groupe fini de Γ soit d'ordre $\leqslant n$. Soit $\mathfrak{g}_0$ un sous-groupe ouvert distingué de $\mathfrak{g}$ opérant trivialement sur Γ. Vu l'hypothèse faite sur le corps k, les sous-groupes ouverts de $\mathfrak{g}_0$ d'indice $\leqslant n$ sont en nombre fini; leur intersection $\mathfrak{g}_1$ est un sous-groupe ouvert distingué de $\mathfrak{g}$. Tout homomorphisme continu de $\mathfrak{g}_0$ dans Γ a une image finie, donc est trivial sur $\mathfrak{g}_1$. *A fortiori*, l'application composée:

$$H^1(\mathfrak{g}, \Gamma) \to H^1(\mathfrak{g}_0, \Gamma) \to H^1(\mathfrak{g}_1, \Gamma)$$

est triviale. D'après le n° 1.27, il s'ensuit que $H^1(\mathfrak{g}, \Gamma)$ s'identifie à $H^1(\mathfrak{g}/\mathfrak{g}_1, \Gamma)$; comme Γ est un $\mathfrak{g}/\mathfrak{g}_1$-groupe de type arithmétique (cf. proposition 3.6), la proposition 3.8 montre que $H^1(\mathfrak{g}/\mathfrak{g}_1, \Gamma)$ est fini, d'où la finitude de $H^1(\mathfrak{g}, \Gamma)$.

(b) *Finitude de $H^1(k, A)$ lorsque A est un groupe algébrique linéaire résoluble et connexe.*

En appliquant la prop. 1.17, on se ramène au cas où A est unipotent et au cas où A est un tore. Dans le premier cas, on a $H^1(k, A) = 0$, cf. par exemple [18], prop. 3.3.1. Supposons donc que A soit un tore. Il existe alors une extension galoisienne finie k'/k telle que $A \otimes k'$ soit isomorphe à un produit

de groupes $\mathbf{G}_m$. Comme $H^1(k', \mathbf{G}_m) = 0$, la prop. 1.27 montre que $H^1(k, A)$ s'identifie à $H^1(k'/k, A)$. En particulier, si $n = [k' : k]$, on a $nx = 0$ pour tout $x \in H^1(k, A)$. Soit A_n le noyau de l'homothétie $n : A \to A$. La suite exacte:

$$0 \to A_n \to A \xrightarrow{n} A \to 0$$

donne naissance à une suite exacte de cohomologie. Cette dernière montre que $H^1(k, A_n)$ s'applique sur le noyau de $n : H^1(k, A) \to H^1(k, A)$, c'est-à-dire sur $H^1(k, A)$ tout entier. Mais $A_n(\bar{k})$ est un g-groupe fini, donc de type arithmétique, et le cas (a) montre que $H^1(k, A_n)$ est fini; il en est donc bien de même de $H^1(k, A)$.

(c) *Finitude de $H^1(k, A)$ lorsque A est un groupe algébrique linéaire.*

D'après ROSENLICHT [16], il existe un sous-groupe de CARTAN H de A; soit N le normalisateur de H dans A. Le quotient N/H est fini; d'après (a), $H^1(k, N/H)$ est aussi fini; en appliquant (b) et le cor. 1.20, on en déduit que $H^1(k, N)$ est fini. Comme $H^1(k, N) \to H^1(k, A)$ est surjectif (cor. 2.14), il en résulte bien que $H^1(k, A)$ est fini [2]).

(d) *Cas général.*

Puisque A est de type (ALA), on peut trouver une suite exacte

$$0 \to A^1 \to A \to \Gamma \to 0\,,$$

où A^1 est algébrique linéaire, et où $\Gamma(\bar{k})$ est un g-groupe de type arithmétique (cf. n° 4.3). D'après (a), $H^1(k, \Gamma)$ est fini, D'autre part, pour tout $x \in Z^1(\mathbf{g}, A)$, le groupe tordu A^1_x est linéaire, et d'après (c), $H^1(k, A^1_x)$ est fini. La finitude de $H^1(k, A)$ résulte alors du cor. 1.20.

Dans les corollaires ci-après, k désigne un corps *vérifiant les conditions du théorème* 6.2.

6.3. Corollaire. (i) *Les k-formes d'une variété abélienne définie sur k sont en nombre fini (à isomorphisme près).*

(ii) *Il en est de même des k-formes d'une algèbre de dimension finie sur k.*

(iii) *Lorsque k est de caractéristique zéro, il en est de même des k-formes d'un groupe algébrique linéaire.*

Précisons que, dans (i), nous prenons le terme de «variété abélienne» au sens de «variété abélienne munie d'une structure de groupe algébrique». Si C est une telle variété, on sait que Aut $C(\bar{k})$ est un g-groupe de type arithmétique (cf. n° 3.5) et l'assertion (i) résulte alors de la correspondance entre «k-formes de C» et éléments de $H^1(k, \text{Aut } C)$, cf. n° 2.6. De même, l'assertion (ii) résulte de ce que le foncteur d'automorphismes d'une k-algèbre de dimen-

[2]) L'idée d'utiliser le corollaire 2.14 nous a été indiquée par T. SPRINGER. Notre démonstration initiale était plus compliquée.

sion finie est un groupe algébrique linéaire (le même argument s'applique plus généralement à la structure formée par un *espace vectoriel muni de tenseurs* de types quelconques, cf. [19], Chap. III, n° 1.1). Enfin, (iii) résulte de ce que, en caractéristique zéro, le foncteur d'automorphismes d'un groupe algébrique linéaire est de type (ALA), cf. théorème 5.12.

6.4. Corollaire. *Soit G un k-groupe algébrique, et soit V un espace homogène de G. Les orbites de $G(k)$ dans $V(k)$ sont en nombre fini.*

La variété V est réunion d'un nombre fini d'orbites de la composante neutre de G; cela permet de se ramener *au cas où G est connexe*. Si $V(k) = \varnothing$, il n'y a rien à démontrer. Sinon, soit $v \in V(k)$, et soit H le groupe de stabilité de v. L'application canonique $G/H \to V$ est radicielle. Comme k est parfait, cette application définit une bijection de $(G/H)(k)$ sur $V(k)$. Or, d'après la prop. 1.12, les orbites de $G(k)$ dans $(G/H)(k)$ correspondent bijectivement aux éléments du noyau de l'application canonique

$$\alpha : H^1(k, H) \to H^1(k, G) .$$

Il nous suffira donc de prouver que α est *propre* (cf. n° 1.14).

Soit R le plus grand sous-groupe linéaire connexe de G, soit $S = R \cap H$, et soient $C = G/R$, $B = H/S$. Le groupe C est une variété abélienne (théorème de CHEVALLEY), et B s'envoie injectivement dans C. On a un diagramme commutatif:

$$\begin{array}{ccc} H^1(k, H) & \xrightarrow{\alpha} & H^1(k, G) \\ \downarrow \gamma & & \downarrow \beta \\ H^1(k, B) & \xrightarrow{\delta} & H^1(k, C) . \end{array}$$

Pour tout $z \in Z^1(\mathfrak{g}, H)$, le groupe tordu S_z est linéaire; d'après le théorème 6.2, $H^1(k, S_z)$ est fini. Appliquant le cor. 1.20, on en déduit que γ est propre. D'autre part, en utilisant le «théorème de complète réductibilité» de WEIL (cf. [20], p. 94), on voit qu'il existe une variété abélienne B' de même dimension que B, et un homomorphisme $C \to B'$ tels que le composé $B \to C \to B'$ soit surjectif. Comme le noyau de $B \to B'$ est fini, l'argument utilisé ci-dessus pour prouver la propreté de γ montre que le composé

$$H^1(k, B) \xrightarrow{\delta} H^1(k, C) \to H^1(k, B')$$

est propre. Il s'ensuit que δ est propre, donc aussi $\delta \circ \gamma = \beta \circ \alpha$, donc aussi α, cqfd.

6.5. Corollaire. *Soit G un groupe algébrique linéaire défini sur k. Les tores maximaux (resp. les sous-groupes de CARTAN) de G définis sur k forment un nombre fini de classes pour la conjugaison par les éléments de $G(k)$.*

Cela résulte du corollaire 6.4, appliqué à la «variété des tores maximaux» (resp. à la «variété des sous-groupes de CARTAN») de G, cf. n° 4.10.

6.6. Corollaire. *Supposons k de caractéristique zéro. Soit G un groupe algébrique semi-simple défini sur k, et soit $\mathfrak{g}$ son algèbre de LIE. Les éléments unipotents de $G(k)$ (resp. les éléments nilpotents de $\mathfrak{g}(k)$) forment un nombre fini de classes pour la conjugaison par les éléments de $G(k)$.*

Soit U (resp. N) la sous-variété de G (resp. $\mathfrak{g}$) formée des éléments unipotents (resp. nilpotents). L'exponentielle définit une bijection de $N(k)$ sur $U(k)$; il suffit donc de prouver la finitude de $N(k)/G(k)$. D'après KOSTANT (cf. [11], cor. 3.7 et lemme 5.1), les orbites de $G(\bar{k})$ dans $N(\bar{k})$ sont en nombre fini (en fait, KOSTANT se borne au cas de $\mathbf{C}$, mais le cas général s'en déduit par application du «principe de LEFSCHETZ»). Il suffit donc de prouver que, si X est une telle orbite, les éléments de $X(k) = X \cap N(k)$ forment un nombre fini de classes modulo les opérations de $G(k)$. C'est clair si $X(k) = \varnothing$. Sinon soit $x \in X(k)$, et soit $H \subset G$ le stabilisateur de x. On peut identifier X (resp. $X(k)$) à l'ensemble des points de G/H à valeurs dans $\bar{k}$ (resp. dans k); notre assertion résulte alors du cor. 6.4, appliqué à l'espace homogène G/H.

6.7. Le cas réel. Les résultats des n^{os} précédents s'appliquent bien entendu au corps $\mathbf{R}$. Certains peuvent d'ailleurs s'obtenir de façon plus simple par des arguments topologiques. Ainsi par exemple le corollaire 6.4 résulte du fait (démontré par WHITNEY) que, si V est une $\mathbf{R}$-variété algébrique, l'espace topologique $V(\mathbf{R})$ n'a qu'un nombre fini de composantes connexes.

Nous allons voir que, pour certains groupes, on peut aller plus loin et déterminer explicitement H^1:

Partons d'un groupe de LIE compact K. Soit R l'algèbre des fonctions continues sur K qui sont combinaisons linéaires de coefficients de représentations matricielles (complexes) de K, et soit R_0 la sous-algèbre de R formée des fonctions à valeurs réelles. On a $R = R_0 \otimes_{\mathbf{R}} \mathbf{C}$. On définit de façon naturelle un homomorphisme $\delta : R_0 \to R_0 \otimes R_0$. Si l'on pose $G = \mathrm{Spec}(R_0)$, δ définit un morphisme de $G \times G$ dans G, et l'on obtient ainsi sur G une structure de *groupe algébrique sur* $\mathbf{R}$ (cf. CHEVALLEY [5], Chap. VI, § VIII). Le groupe $G(\mathbf{R})$ des points réels de G s'identifie à K. Le groupe $G(\mathbf{C})$ s'appelle le *complexifié* de K. Le groupe de GALOIS $\mathfrak{g} = \mathfrak{g}(\mathbf{C}/\mathbf{R})$ opère sur $G(\mathbf{C})$.

6.8. Théorème. *L'application canonique $H^1(\mathfrak{g}, K) \to H^1(\mathfrak{g}, G(\mathbf{C}))$ est bijective.*

(Comme $\mathfrak{g}$ opère trivialement sur K, $H^1(\mathfrak{g}, K)$ est l'ensemble des classes dans K, modulo conjugaison, des éléments x tels que $x^2 = 1$.)

Le groupe $\mathfrak{g}$ opère sur l'algèbre de LIE $\mathfrak{g}(\mathbf{C})$ de $G(\mathbf{C})$; les éléments invariants forment l'algèbre de LIE $\mathfrak{k}$ de K, et les éléments anti-invariants forment un supplémentaire $\mathfrak{p}$ de $\mathfrak{k}$ dans $\mathfrak{g}(\mathbf{C})$. L'exponentielle définit un isomorphisme analytique réel de $\mathfrak{p}$ sur une sous-variété fermée P de $G(\mathbf{C})$; on a $xPx^{-1} = P$ pour tout $x \in K$; de plus (CHEVALLEY, *loc. cit.*, p. 201) tout élément $z \in G(\mathbf{C})$ s'écrit de façon unique sous la forme $z = xp$, avec $x \in K$ et $p \in P$.

Ces résultats étant rappelés, montrons que $H^1(\mathfrak{g}, K) \to H^1(\mathfrak{g}, G(\mathbf{C}))$ est *surjectif*. Un élément de $Z^1(\mathfrak{g}, G(\mathbf{C}))$ s'identifie à un élément $z \in G(\mathbf{C})$ tel que $z\bar{z} = 1$. Si l'on écrit z sous la forme xp, avec $x \in K$ et $p \in P$, on a $xpxp^{-1} = 1$ (car $\bar{p} = p^{-1}$), d'où $p = x^2 \cdot x^{-1}px$. Mais $x^{-1}px$ appartient à P, et l'unicité de la décomposition $G(\mathbf{C}) = K \cdot P$ montre que $x^2 = 1$ et $x^{-1}px = p$. Si P_x est la partie de P formée des éléments commutant à x, on voit facilement que P_x est l'exponentielle d'un sous-espace vectoriel de $\mathfrak{p}$. On en conclut qu'on peut écrire p sous la forme $p = q^2$, avec $q \in P_x$. On en tire $z = qxq$, et comme $\bar{q} = q^{-1}$, on voit que le cocycle z est cohomologue au cocycle x, qui est à valeurs dans K.

Montrons maintenant que $H^1(\mathfrak{g}, K) \to H^1(\mathfrak{g}, G(\mathbf{C}))$ est *injectif*. Soient $x \in K$ et $x' \in K$ deux éléments tels que $x^2 = 1$, $x'^2 = 1$, et supposons qu'ils soient cohomologues dans $G(\mathbf{C})$, autrement dit qu'il existe $z \in G(\mathbf{C})$ tel que $x' = z^{-1}x\bar{z}$. Ecrivons z sous la forme $z = yp$, avec $y \in K$ et $p \in P$. On a:

$$x' = p^{-1}y^{-1}xyp^{-1}, \text{ d'où } x' \cdot x'^{-1}px' = y^{-1}xy \cdot p^{-1}.$$

Appliquant à nouveau l'unicité de la décomposition $G(\mathbf{C}) = K \cdot P$, on en tire $x' = y^{-1}xy$, ce qui signifie que x et x' sont conjugués dans K, et achève la démonstration.

Exemples. (a) Supposons que K soit *connexe*, et soit T l'un de ses tores maximaux. Soit T_2 l'ensemble des $t \in T$ tels que $t^2 = 1$; on sait que tout élément $x \in K$ tel que $x^2 = 1$ est conjugué d'un élément $t \in T_2$; de plus deux éléments de T_2 sont conjugués dans K si et seulement si ils sont transformés l'un en l'autre par un élément du *groupe de* WEYL W de K (par rapport à T). Il résulte donc du théorème 6.8 que $H^1(\mathbf{R}, G)$ (égal par définition à $H^1(\mathfrak{g}, G(\mathbf{C}))$) *s'identifie à l'ensemble quotient* T_2/W.

(b) Prenons pour K le *groupe des automorphismes* d'un groupe compact semi-simple connexe S. Soit A (resp. G) le groupe algébrique associé comme ci-dessus à K (resp. à S). On sait que A *est le groupe d'automorphismes* Aut G de G. Les éléments de $H^1(\mathbf{R}, A)$ correspondent donc aux *formes réelles* du groupe G, et le théorème 6.8 redonne la classification de ces formes au moyen de classes d'«involutions» de S (résultat dû à ELIE CARTAN).

§ 7. Théorèmes de finitude (corps de nombres)

Dans tout ce paragraphe, k désigne un *corps de nombres algébriques*, c'est-à-dire une extension finie du corps $\mathbf{Q}$, et $\mathbf{g}$ désigne le groupe de GALOIS $\mathbf{g}(\bar{k}/k)$. On note V l'ensemble des *places* de k; rappelons qu'une place est une classe d'équivalence de valeurs absolues non discrètes (deux valeurs absolues étant dites équivalentes si elles définissent la même topologie). Si $v \in V$, on note k_v le complété de k pour la topologie définie par v; les corps k_v sont des corps localement compacts de caractéristique zéro.

Si A est un groupe localement algébrique sur k, chacun des plongements $k \to k_v$ définit une application $\omega_v : H^1(k, A) \to H^1(k_v, A)$, cf. 2.2. Pour toute partie S de V, ces applications définissent une application canonique

$$\omega_S : H^1(k, A) \to \prod_{v \in V - S} H^1(k_v, A) .$$

7.1. Théorème. *Si S est un ensemble fini de places de k, et si A est un k-groupe de type* (ALA), *l'application*

$$\omega_S : H^1(k, A) \to \prod_{v \in V - S} H^1(k_v, A)$$

est propre (cf. n° 1.14).

En particulier, on voit que les éléments de $H^1(k, A)$ qui sont «nuls localement» (c'est-à-dire dont l'image dans chacun des $H^1(k_v, A)$ est nulle) sont en nombre fini; cela généralise un résultat de [3], résultat qui va d'ailleurs être utilisé dans la démonstration ci-dessous.

Avant de donner cette démonstration, il est bon de faire deux remarques:

(i) Si le théorème est vrai pour A et pour un certain S, il est vrai pour A et pour tout autre ensemble fini S'. Cela résulte simplement de la finitude des $H^1(k_v, A)$, démontrée au § 6. En particulier, on peut toujours se ramener au cas où $S = \varnothing$.

(ii) Pour prouver le théorème 7.1, il suffit de prouver que *le noyau de ω_S est fini* pour le groupe A considéré et pour tous les groupes tordus A_x, avec $x \in Z^1(k, A)$. Cela résulte des propriétés élémentaires de la torsion, cf. n° 1.10.

7.2. Démonstration du théorème 7.1 lorsque A est connexe. Puisque A est de type (ALA), c'est un groupe linéaire connexe. Soit U la partie unipotente du radical de A et soit $H = A/U$. Le groupe H est réductif connexe. Comme la cohomologie d'un groupe unipotent est triviale, les applications canoniques:

$$H^1(k, A) \to H^1(k, H) \quad \text{et} \quad H^1(k_v, A) \to H^1(k_v, H)$$

sont injectives (cf. n° 1.20). On est donc ramené à prouver le théorème pour le groupe H. De plus, d'après les remarques (i) et (ii) du n° 7.1, il suffit de montrer que, pour tout $x \in Z^1(k, H)$, le noyau de

$$H^1(k, H_x) \to \prod_{v \in V} H^1(k_v, H_x)$$

est fini. Or, c'est là un résultat connu ([3], th. 6.8).

7.3. Lemme. *Soit A un $\mathbf{g}$-groupe discret sur lequel $\mathbf{g}$ opère trivialement, et soit S un sous-ensemble fini de V. Le noyau de l'application*

$$\omega_S : H^1(k, A) \to \prod_{v \in V - S} H^1(k_v, A)$$

est alors réduit à 0.

Soit x un élément de ce noyau, et choisissons une extension galoisienne k'/k telle que x appartienne à $H^1(k'/k, A)$. Soit $\mathbf{g}'$ le groupe de GALOIS de k'/k; comme $\mathbf{g}'$ opère trivialement sur A, l'élément x est représenté par un cocycle ξ qui est un *homomorphisme de* $\mathbf{g}'$ dans A. Soit V' l'ensemble des places de k', et soit S' le sous-ensemble de V' formé des places qui prolongent les places de S. Soit $w \in V' - S'$, soit v la place correspondante de $V - S$, et soit $\mathbf{g}'_w$ le groupe de décomposition de w. Dire que x donne zéro dans $H^1(k_v, A)$ signifie que la restriction de ξ à $\mathbf{g}'_w$ est triviale (i. e. ξ applique $\mathbf{g}'_w$ dans l'élément neutre de A). Mais l'on sait que, lorsque w parcourt $V' - S'$, *la réunion des $\mathbf{g}'_w$ est $\mathbf{g}'$ tout entier*; de façon plus précise, tout sous-groupe cyclique de $\mathbf{g}'$ est un groupe de décomposition $\mathbf{g}'_w$ pour une infinité de w (cela résulte du théorème de densité d'ARTIN-ČEBOTAREV, ou même, plus simplement, du théorème de densité de FROBENIUS [7]). Il s'ensuit que ξ est trivial, d'où le lemme.

7.4. Démonstration du théorème 7.1 lorsque A est discret. En vertu de la remarque (ii) du n° 7.1, il suffit de prouver que *le noyau* de ω_S est fini. Nous noterons ce noyau $H^1_S(k, A)$.

Puisque A est de type (ALA), c'est une extension d'un $\mathbf{g}$-groupe Γ de type arithmétique par un $\mathbf{g}$-groupe fini C; on a $A/C = \Gamma$. Comme Γ est de type fini (cf. n° 3.3), il en est de même de A; comme $\mathbf{g}$ opère continûment, on en conclut qu'il existe un sous-groupe ouvert distingué $\mathbf{h}$ de $\mathbf{g}$ qui opère trivialement sur A. On notera k' le sous-corps de k correspondant à $\mathbf{h}$, et S' l'ensemble des places de k' prolongeant l'une des places de S. Si $x \in H^1_S(k, A)$, l'image x' de x dans $H^1(k', A)$ appartient à $H^1_{S'}(k', A)$: c'est immédiat. Mais, puisque $\mathbf{h}$ opère trivialement sur A, le lemme 7.3 (appliqué à k' et S') montre que $H^1_{S'}(k', A)$ est réduit à 0. D'après 1.27, il en résulte que x appartient à $H^1(k'/k, A) = H^1(\mathbf{g}/\mathbf{h}, A)$. Mais $\mathbf{g}/\mathbf{h}$ est fini, donc aussi $H^1(\mathbf{g}/\mathbf{h}, \Gamma)$, cf. n° 3.8; il en est de même des $H^1(\mathbf{g}/\mathbf{h}, C_x)$, où x désigne un 1-cocycle de $\mathbf{g}/\mathbf{h}$ dans A; d'après 1.20,

il s'ensuit que $H^1(\mathfrak{g}/\mathfrak{h}, A)$ est fini. Comme $H^1_S(k, A)$ est un sous-ensemble de $H^1(\mathfrak{g}/\mathfrak{h}, A)$, cela démontre bien le théorème 7.1 dans ce cas.

7.5. Pour aller plus loin, nous aurons besoin d'un résultat élémentaire sur les «réductions mod. p». Indiquons rapidement de quoi il s'agit (pour plus de détails, voir [9], Chap. IV):

Soit X un schéma de type fini sur le corps k, et soit $\mathfrak{o}_k$ l'anneau des entiers de k; le corps k est le corps des fractions de $\mathfrak{o}_k$, c'est-à-dire le corps des fonctions rationnelles de Spec $(\mathfrak{o}_k)$. Il en résulte facilement qu'on peut trouver une «forme de X sur $\mathfrak{o}_k$», c'est-à-dire un schéma X_0 de type fini sur Spec $(\mathfrak{o}_k)$ tel que $X = X_0 \otimes_{\mathfrak{o}_k} k$. Si v est un idéal maximal de $\mathfrak{o}_k$, de corps résiduel $\kappa(v)$, on peut parler du schéma $X_0 \otimes_{\mathfrak{o}_k} \kappa(v)$ obtenu à partir de X_0 par réduction en v. Ses points rationnels sur $\kappa(v)$ forment un ensemble fini $(X_0)_{\kappa(v)}$. De même, si $\mathfrak{o}_v$ désigne l'anneau des entiers du corps local k_v, X_0 définit par changement de base un schéma sur $\mathfrak{o}_v$; les points de ce schéma à valeurs dans $\mathfrak{o}_v$ seront notés $(X_0)_{\mathfrak{o}_v}$. En fait, on emploie très souvent les notations incorrectes $X_{\kappa(v)}$ et $X_{\mathfrak{o}_v}$ pour désigner $(X_0)_{\kappa(v)}$ et $(X_0)_{\mathfrak{o}_v}$. Cet abus d'écriture est sans danger si l'on ne s'intéresse qu'à des questions où n'interviennent que «presque tous les v». En effet, on démontre sans peine que, si X_0 et X_0' sont deux formes de X sur $\mathfrak{o}_k$, il existe un ouvert non vide U de Spec $(\mathfrak{o}_k)$ au-dessus duquel X_0 et X_0' sont isomorphes; si $v \in U$ on peut alors identifier $(X_0)_{\kappa(v)}$ et $(X_0')_{\kappa(v)}$ et de même pour les points à valeurs dans $\mathfrak{o}_v$. C'est cette notation que nous utiliserons dans la proposition suivante:

7.6. Proposition. *Soit G un k-groupe algébrique connexe, et soit P un espace fibré principal pour G dont la base B est une variété algébrique de dimension zéro. Il existe alors une partie finie S de V, contenant toutes les places archimédiennes, et telle que, si $v \in V - S$, on ait $B_{\mathfrak{o}_v} = B_{k_v}$ et que $P_{\mathfrak{o}_v} \to B_{\mathfrak{o}_v}$ soit surjectif.*

(L'hypothèse faite sur P équivaut à dire que $P \otimes \bar{k}$ est réunion disjointe d'espaces homogènes principaux sur $G \otimes \bar{k}$.)

On choisit comme ci-dessus des formes de G, P, B sur $\mathfrak{o}_k$; on les notera encore G, P, B (c'est l'abus d'écriture signalé plus haut). Si l'on se place sur un ouvert $U = \text{Spec}\,(\mathfrak{o}_k) - S$ assez petit de Spec $(\mathfrak{o}_k)$, ces schémas sont *simples* sur U (cf. GROTHENDIECK [10]), B est propre, G est un schéma en groupes à fibres connexes, et P est un espace fibré principal de base B et de groupe G (cela signifie ici que le morphisme évident de $P \times_U G$ dans $P \times_U P$ est un isomorphisme). Soit $v \in U$; comme B est simple et propre sur U, on a $B_{\kappa(v)} = B_{\mathfrak{o}_v} = B_{k_v}$. De même, la simplicité de P entraîne que $P_{\mathfrak{o}_v} \to P_{\kappa(v)}$ soit surjectif (pour ces propriétés de la simplicité – qui ne sont au fond qu'une forme du «lemme de HENSEL» — voir GROTHENDIECK [10]). D'autre part, si

$x \in B_{\kappa(v)}$, la fibre de x dans P est un espace homogène principal sur le groupe $G \otimes_{o_k} \kappa(v)$ déduit de G par réduction en v; comme $G \otimes_{o_k} \kappa(v)$ est connexe, cet espace a un point à valeurs dans $\kappa(v)$(cf. LANG [12]). Il s'ensuit que $P_{\kappa(v)} \to B_{\kappa(v)}$ est surjectif, d'où le résultat cherché.

7.7. Corollaire. *L'application $P_{k_v} \to B_{k_v}$ est surjective pour tout $v \in V - S$.*
C'est évident.

Remarque. Lorsque, dans la proposition 7.6, on ne suppose plus que B soit de dimension zéro, il est encore vrai que $P_{o_v} \to B_{o_v}$ est surjectif pour presque tout v.

7.8. Revenons maintenant à la démonstration du théorème 7.1. Soit G la composante neutre du groupe A, et soit $L = A/G$; nous identifierons (par abus de langage) L au g-groupe $L(\bar{k})$.

7.9. Lemme. *Il existe un sous-ensemble fini S de V tel que l'application $H^0(k_v, A) \to H^0(k_v, L)$ soit surjective pour tout $v \in V - S$.*

Comme A est de type (ALA), le groupe L est extension d'un g-groupe Γ de type arithmétique par un g-groupe fini C. Comme on l'a déjà remarqué, il existe un sous-groupe ouvert distingué $\mathbf{h}$ de $\mathbf{g}$ qui opère trivialement sur L. Posons $\mathbf{g}' = \mathbf{g}/\mathbf{h}$, et soit $\mathbf{h}'$ un sous-groupe de $\mathbf{g}'$. On a la suite exacte:

$$0 \to H^0(\mathbf{h}', C) \to H^0(\mathbf{h}', L) \to H^0(\mathbf{h}', \Gamma) \to H^1(\mathbf{h}', C),$$

où $H^0(\mathbf{h}', C)$ et $H^1(\mathbf{h}', C)$ sont finis. Comme d'autre part $H^0(\mathbf{h}', \Gamma)$ est un groupe de type fini (cf. 3.3 et 3.6) on en déduit facilement que $H^0(\mathbf{h}', L)$ est aussi de type fini. Puisque les $\mathbf{h}'$ sont en nombre fini, on en conclut qu'il existe un *sous-ensemble fini B de L tel que $B \cap H^0(\mathbf{h}', L)$ engendre $H^0(\mathbf{h}', L)$ pour tout* $\mathbf{h}'$; on peut en outre s'arranger pour que B soit stable par $\mathbf{g}$, ce qui permet de l'identifier à une k-sous-variété de dimension zéro de $L = A/G$. Soit P l'image réciproque de cette sous-variété dans A; c'est un espace fibré principal pour G de base B. Appliquant 7.7, on voit qu'il existe une partie finie S de V telle que $H^0(k_v, P) \to H^0(k_v, B)$ soit surjectif pour tout $v \in V - S$. *Cette propriété entraîne que*

$$H^0(k_v, A) \to H^0(k_v, L)$$

est surjectif pour tout $v \in V - S$. En effet, l'image I_v de cet homomorphisme contient l'image de $H^0(k_v, P)$, qui est égale à $H^0(k_v, B)$. Or, si $\mathbf{g}'_v$ désigne l'un des groupes de décomposition associés à v dans $\mathbf{g}'$, on peut identifier $H^0(k_v, L)$ à $H^0(\mathbf{g}'_v, L)$ et $H^0(k_v, B)$ à $H^0(\mathbf{g}'_v, B)$, c'est-à-dire à $B \cap H^0(\mathbf{g}'_v, L)$. Il en résulte (vu la définition de B) que $H^0(k_v, B)$ *engendre* $H^0(k_v, L)$. Comme I_v contient $H^0(k_v, B)$, on a donc bien $I_v = H^0(k_v, L)$, ce qui achève la démonstration du lemme.

7.10. Fin de la démonstration du théorème 7.1. On conserve les notations ci-dessus. On suppose en outre que $S = \varnothing$, ce qui est licite vu la remarque (i). On a un diagramme commutatif

$$\begin{array}{ccccc} H^1(k,G) & \xrightarrow{\alpha} & H^1(k,A) & \xrightarrow{\beta} & H^1(k,L) \\ \downarrow\omega' & & \downarrow\omega & & \downarrow\omega'' \\ \prod_{v\in V} H^1(k_v,G) & \xrightarrow{\varphi} & \prod_{v\in V} H^1(k_v,A) & \xrightarrow{\psi} & \prod_{v\in V} H^1(k_v,L)\,. \end{array}$$

On va d'abord prouver *que l'application*

$$(\beta,\omega): H^1(k,A) \to H^1(k,L) \times \prod_{v\in V} H^1(k_v,A)$$

est propre.

Pour cela, soit $x\in Z^1(k,A)$, soit ξ l'image de x dans $H^1(k,A)$ et soit X l'ensemble des éléments de $H^1(k,A)$ dont l'image par (β,ω) est la même que celle de ξ; on doit prouver que X est *fini*. Quitte à remplacer A par A_x, on peut supposer que $x=0$. Il en résulte que X est contenu dans l'image de $\alpha: H^1(k,G) \to H^1(k,A)$. Soit $Y = \alpha^{-1}(X)$, et soit

$$Y' = \omega'(Y) \subset \prod_{v\in V} H^1(k_v,G).$$

Comme $\omega\circ\alpha = \varphi\circ\omega'$, les éléments de Y' appartiennent au noyau de φ. Mais, d'après 7.9, il existe un sous-ensemble fini S de V tel que $H^0(k_v,A) \to H^0(k_v,L)$ soit surjectif pour $v\in V-S$; vu 1.17, ceci entraîne que le noyau de $H^1(k_v,G) \to H^1(k_v,A)$ est réduit à 0 (pour $v\in V-S$). On en conclut que l'image Y'' de Y dans $\prod_{v\in V-S} H^1(k_v,G)$ est réduite à 0, ce qui montre (cf. 7.2) que Y est fini; comme $X=\alpha(Y)$, il en est de même de X, ce qui démontre notre assertion.

Notons maintenant que, d'après 7.4, l'application ω'' est propre. Il en est donc de même de l'application $(\omega''\times 1)\circ(\beta,\omega)$ qui applique $H^1(k,A)$ dans $\prod_{v\in V} H^1(k_v,L) \times \prod_{v\in V} H^1(k_v,A)$. Comme cette application se factorise par l'application ω, on en conclut que ω est propre, cqfd.

7.11. Corollaire. *Soit G une variété abélienne (resp. un groupe algébrique linéaire, resp. une algèbre de dimension finie) sur k, et soit S un ensemble fini de places de k. Les k-formes de G qui sont k_v-isomorphes à G pour tout v non dans S sont en nombre fini (à isomorphisme près).*

Cela résulte de ce que, dans chaque cas, Aut (G) est un groupe de type (ALA).

7.12. Corollaire. *Soit G un k-groupe algébrique, soit V un espace homogène de G, soit $x\in V(k)$ et soit S un ensemble fini de places de k. Soit X la partie de*

$V(k)$ formée des éléments x' tels que pour tout $v \in V - S$, il existe $g_v \in G(k_v)$ qui transforme x en x'. Supposons enfin que le groupe de stabilité H de x soit un groupe linéaire. Les orbites de $G(k)$ dans X sont alors en nombre fini.

Soit Y le quotient de X par $G(k)$; d'après 1.12, Y s'identifie à un sous-ensemble de $H^1(k, H)$. De plus, la définition même de X montre que l'image de Y dans chacun des $H^1(k_v, H)$, $v \in V - S$, est réduite à 0. Comme H est linéaire, le théorème 7.1 s'applique, et montre que Y est fini, cqfd.

Remarques. (1) Si G est un groupe algébrique linéaire, le corollaire ci-dessus s'applique à la variété des tores maximaux (resp. des sous-groupes de CARTAN, resp. etc.) de G. Nous laissons au lecteur le soin d'expliciter le résultat obtenu.

(2) Les hypothèses et notations étant celles de 7.12, soit x' un point de X. Par hypothèse, pour tout $v \in V - S$, il existe $g_v \in G_{k_v}$ qui transforme x en x'. *On peut s'arranger pour que g_v appartienne à G_{o_v} pour presque tout v.* En effet, soit P la sous-variété algébrique de G dont les points sont les éléments g transformant x en x'; c'est un espace homogène principal sur H. Si H^0 désigne la composante neutre de H, P peut aussi être considérée comme espace principal de groupe H^0 et de base finie $B = P/H^0$. D'après 7.6, l'application $P_{o_v} \to B_{k_v}$ est surjective pour presque tout v; d'autre part, l'existence d'un $g_v \in P_{k_v}$ montre que B_{k_v} est non vide. Il s'ensuit que P_{o_v} est non vide pour presque tout v, ce qui démontre notre assertion.

Ceci permet de traduire 7.12 en termes adéliques, comme dans [3].

BIBLIOGRAPHIE

[1] E. ARTIN. *Algebraic numbers and algebraic functions.* New York Univ., 1951 (notes polycopiées).

[2] A. BOREL. *Arithmetic properties of algebraic groups.* Cong. Inter., Stockholm, 1962, p. 10–22.

[3] A. BOREL, *Some finiteness properties of adele groups over number fields.* Publ. Math. Inst. Hautes Etudes Sci., n° 16, 1963, p. 5–30.

[4] A. BOREL and HARISH-CHANDRA, *Arithmetic subgroups of algebraic groups.* Annals of Maths., *75*, 1962, p. 485–535.

[5] C. CHEVALLEY, *Theory of LIE groups.* Princeton Math. Ser., n° 8, 1946.

[6] C. CHEVALLEY. *Classification des groupes de LIE algébriques.* Séminaire Ecole Normale Sup., 1956–58.

[7] G. FROBENIUS. *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe.* Sitzber. Berlin Akad., *32*, 1896, p. 689–705.

[8] A. GROTHENDIECK, *A general theory of fibre spaces with structure sheaf.* Univ. Kansas, Report n° 4, 1955.

[9] A. GROTHENDIECK, *Eléments de géométrie algébrique* (rédigés avec la collaboration de J. DIEUDONNÉ). Inst. Hautes Etudes Sci., Publ. Math. 1960–61–62–63- . . .

[10] A. GROTHENDIECK. *Séminaire de géométrie algébrique.* Inst. Hautes Etudes Sci., 1960–61.

[11] B. KOSTANT, *The principal three-dimensional subgroup and the BETTI numbers of a complex simple LIE group.* Amer. J. of Maths., *81*, 1959, p. 973–1032.

[12] S. LANG, *Algebraic groups over finite fields*. Amer. J. of Maths., *78*, 1956, p. 555–563.
[13] S. LANG and J. TATE, *Principal homogeneous spaces over abelian varieties*. Amer. J. of Maths., *80*, 1958, p. 659–684.
[14] G. MOSTOW, *Fully reducible subgroups of algebraic groups*. Amer. J. of Maths., *78*, 1956, p. 200-221.
[15] M. ROSENLICHT, *Some basic theorems on algebraic groups*. Amer. J. of Maths., *78*, 1956, p. 401–443.
[16] M. ROSENLICHT, *Some rationality questions on algebraic groups*. Annali di Mat. Pura Appl., *43*, 1957, p. 25–50.
[17] J.-P. SERRE, *Groupes algébriques et corps de classes*. Act. Sci. Ind., n° 1264, Paris, Hermann, 1959.
[18] J.-P. SERRE, *Cohomologie galoisienne des groupes algébriques linéaires*. Colloque de Bruxelles, 1962, p. 53–67.
[19] J.-P. SERRE, *Cohomologie galoisienne*. Collège de France, 1963 (notes polycopiées).
[20] A. WEIL. *Variétés abéliennes et courbes algébriques*. Act. Sci. Ind., n° 1064, Paris, Hermann, 1948.
[21] A. WEIL, *Adeles and algebraic groups*. Inst. Adv. Study, 1961 (notes polycopiées rédigées par M. DEMAZURE et T. ONO).

(Reçu le 16 janvier 1964)