EXPOSÉ XVII

GROUPES ALGÉBRIQUES UNIPOTENTS. EXTENSIONS ENTRE GROUPES UNIPOTENTS ET GROUPES DE TYPE MULTIPLICATIF

par M. RAYNAUD (*)

0. Quelques notations

531

Dans le présent chapitre, nous aurons surtout à considérer des groupes algébriques définis sur un corps k. Le nombre $p \geqslant 0$ désignera toujours la caractéristique de k, $\mathbb{F}_p$ le corps premier à p éléments si $p > 0$, $\overline{k}$ une extension algébriquement close de k, q un nombre premier *distinct* de p.

Pour tout S-préschéma, $(\mathbb{G}_a)_S$ (resp. $(\mathbb{G}_m)_S$) désigne le groupe additif (resp. le groupe multiplicatif) au-dessus de S (cf. Exp. I 4.3). Pour tout entier $n > 0$, $(\boldsymbol{\mu}_n)_S$ (resp. $(\mathbb{Z}/n\mathbb{Z})_S$) désigne le groupe des racines $n^{\text{ièmes}}$ de l'unité (Exp. I 4.4.4) (resp. le groupe constant au-dessus de S, associé au groupe abstrait $\mathbb{Z}/n\mathbb{Z}$ (Exp. I 4.1)). Le groupe $(\mathbb{Z}/n\mathbb{Z})_S$ est fini et étale sur S ; le groupe $(\boldsymbol{\mu}_n)_S$ est plat et fini sur S, et est étale sur S si et seulement si n est inversible sur S (Exp. VIII 2.1).

Si S est un préschéma de caractéristique $p > 0$, pour tout entier $n > 0$, et tout S-préschéma en groupes G, nous notons ${}_{F^n}(G)$ le sous-S-préschéma en groupes radiciel de G égal au noyau du $n^{\text{ième}}$ itéré du morphisme de Frobenius relatif à G (Exp. VII_A). En particulier, si $G = (\mathbb{G}_a)_S$ nous posons ${}_{F^n}(G) = (\boldsymbol{\alpha}_{p^n})_S$, qui est un S-groupe radiciel, plat et fini sur S, qui représente le foncteur suivant : pour tout S-préschéma S', $(\boldsymbol{\alpha}_{p^n})_S(S')$ est l'ensemble des $x' \in \Gamma(S', \mathscr{O}_{S'})$ tels que $x'^{p^n} = 0$.

Le groupe $(\boldsymbol{\mu}_{p^n})_S$, déjà défini, est canoniquement isomorphe à ${}_{F^n}(\mathbb{G}_m)_S$. **532**

Lorsqu'il n'y a pas ambiguité sur le schéma de base S, nous écrirons simplement $\mathbb{G}_a$, $\mathbb{G}_m$, $\boldsymbol{\alpha}_{p^n}$, etc. au lieu de $(\mathbb{G}_a)_S$, $(\mathbb{G}_m)_S$, $(\boldsymbol{\alpha}_{p^n})_S$, etc.

Si G est un S-préschéma en groupes commutatifs, pour tout entier $n > 0$, ${}_nG$ est le sous-préschéma en groupes de G égal au noyau de l'élévation à la puissance $n^{\text{ième}}$ dans G.

---

(0) version xy du 18/11/08

(*) cf. note à la page 1 de l'exposé XV.

Pour la commodité du lecteur, nous avons rassemblé en appendice quelques propriétés des groupes algébriques démontrées dans Exp. VI et VII, ainsi que des propriétés élémentaires de la cohomologie de Hochschild, qui nous seront utiles dans ce chapitre.

1. Définition des groupes algébriques unipotents

533

Définition 1.1. — Un groupe algébrique G défini sur un corps k algébriquement clos est dit *unipotent* si G admet une suite de composition dont les quotients successifs sont isomorphes à des sous-groupes algébriques de $(\mathbb{G}_a)_k$.

Proposition 1.2. — *Soient k un corps algébriquement clos,* K *une extension algébriquement close de k,* G *un groupe algébrique défini sur k. Alors, pour que* G *soit unipotent, il faut et il suffit que* $\mathrm{G_K}$ *soit unipotent.*

La nécessité de la condition est claire puisqu'une suite de composition donne une suite de composition par extension de la base.

La démonstration de la suffisance est standard : K est limite inductive de ses sous-k-algèbres de type fini. D'après Exp. $\mathrm{VI_B}$ § 10, on peut trouver une sous-k-algèbre de type fini A de K, une suite de composition G_i de $\mathrm{G_S}$ ($\mathrm{S} = \operatorname{Spec} \mathrm{A}$) et des immersions $u_i : \mathrm{H}_i = \mathrm{G}_i/\mathrm{G}_{i+1} \to (\mathbb{G}_a)_{\mathrm{S}}$. Pour prouver que G est unipotent, il suffit alors de faire une k-extension de la base : $\mathrm{A} \to k$, ce qui est possible, car $\mathrm{Hom}_{k\text{-alg}}(\mathrm{A}, k)$ n'est pas vide, A étant une k-algèbre, non nulle, de type fini sur k algébriquement clos.

Définition 1.3. — Soit G un groupe algébrique défini sur un corps k. Nous dirons que G est *unipotent* s'il existe une extension algébriquement close $\overline{k}$ de k, telle que $\mathrm{G}_{\overline{k}}$ soit unipotent (définition 1.1).

534 D'après 1.2, la propriété est indépendante de l'extension algébriquement close $\overline{k}$ choisie.

Définition 1.4. — Soient G un groupe algébrique défini sur un corps k et H un groupe algébrique défini sur une extension k' de k. Nous dirons que H est une *forme* de G sur k' si les groupes algébriques $\mathrm{G}_{k'}$ et $\mathrm{H}_{k'}$ deviennent isomorphes sur $\overline{k}'$ (comme plus haut on voit que la propriété ne dépend pas du choix de l'extension algébriquement close $\overline{k}'$ de k'). Nous dirons encore que H est un groupe G « tordu ».

Nous sommes alors en mesure de décrire les sous-groupes algébriques de $\mathbb{G}_a$.

Proposition 1.5. — *Soit k un corps caractéristique $p \geqslant 0$. Alors un sous-groupe algébrique* H *de $(\mathbb{G}_a)_k$ est de l'un des types suivants :*

(i) $\mathrm{H} = 0$.

(ii) $\mathrm{H} = \mathbb{G}_a$.

(iii) (*Si $p > 0$*) H *est extension d'un groupe constant tordu $(\mathbb{Z}/p\mathbb{Z})^r$ par un groupe radiciel $\boldsymbol{\alpha}_{p^n}$ (r et n entiers $\geqslant 0$, $r + n > 0$). Si de plus k est* parfait, *cette extension est nécessairement triviale.*

Démonstration. Si H est de dimension 1, il est clair que $H = \mathbb{G}_a$. Sinon H est de dimension 0 et par suite est extension [1] d'un groupe étale H'' par sa composante neutre H' qui est un groupe radiciel. Pour décrire $H''_{\overline{k}}$, il suffit de connaître le groupe 535
abstrait $H''(\overline{k})$, isomorphe à $H(\overline{k})$. Or ce dernier est un sous-groupe fini de $\mathbb{G}_a(\overline{k})$, donc est nul si $p = 0$ et est de la forme $(\mathbb{Z}/p\mathbb{Z})^r$ sinon, car annulé par p. Le groupe H' est fermé dans $\mathbb{G}_a$ et est défini par une seule équation (l'anneau $k[T]$ de $\mathbb{G}_a$ est principal), qui sur $\overline{k}$ admet 0 pour seule racine, donc cette équation est de la forme $T^n = 0$. La compatibilité avec la loi de groupe entraîne que $(T + T')^n$ appartient à l'idéal engendré par T^n et T'^n dans l'anneau $k[T, T']$ donc : si $p = 0$, on a $n = 1$ et H' le groupe unité ; si $p > 0$, on a $n = p^m$ et $H' = \boldsymbol{\alpha}_{p^m}$.

La dernière assertion de 1.5 résulte plus généralement du lemme :

Lemme 1.6. — *Si k est un corps parfait, toute extension* H *d'un groupe algébrique étale* H'' *par un groupe radiciel* H' *est triviale. De plus il existe un unique relèvement de* H'' *dans* H*, à savoir* $H_{\text{réd}}$.

En effet, k étant parfait, le k-schéma réduit $H_{\text{réd}}$ est un sous-groupe algébrique de H (Exp. VI_A 0.2) géométriquement réduit, donc lisse sur k (Exp. VI_A, 1.3.1), donc étale, H étant de dimension 0. Pour voir que la projection canonique $H_{\text{réd}} \to H''$ est un isomorphisme, il suffit de le voir après extension du corps de base $k \to \overline{k}$, auquel cas il suffit de montrer que l'on a un isomorphisme sur les points à valeurs dans $\overline{k}$, ce qui est bien clair. La dernière assertion résulte du fait que tout relèvement de H'' dans H, étant étale sur k, est réduit, donc est nécessairement contenu dans $H_{\text{réd}}$. 536

Notons que $\boldsymbol{\alpha}_{p^n}$ est extension multiple de groupes isomorphes à $\boldsymbol{\alpha}_p$. On déduit alors de 1.5 le corollaire :

Corollaire 1.7. — *Pour qu'un groupe algébrique* G *défini sur un corps k algébriquement clos soit unipotent, il faut et il suffit qu'il possède une suite de composition dont les quotients successifs sont isomorphes à $\mathbb{G}_a$ si $p = 0$, et à l'un des groupes $\mathbb{G}_a$, $\mathbb{Z}/p\mathbb{Z}$, $\boldsymbol{\alpha}_p$ si $p > 0$. (Nous appellerons ces groupes,* les groupes unipotents élémentaires*).*

2. Premières propriétés des groupes unipotents

537

Proposition 2.1. — *Un groupe algébrique unipotent défini sur un corps k est* affine *sur k.*

Par descente (fpqc) des morphismes affines, il suffit de prouver 2.1 lorsque k est algébriquement clos. Dans ce cas, G est, par définition, extension multiple de groupes algébriques affines, donc est affine, d'après Exp. VI_B 9.2 (viii) appliqué aux morphismes *affines*. [2]

Proposition 2.2. — i) *La propriété pour un groupe algébrique d'être unipotent est invariante par extension du corps de base.*

---

[1] N.D.E. : référence à VII_A ?
[2] N.D.E. : vérifier cette réf.

ii) *Tout sous-groupe algébrique d'un groupe unipotent est unipotent.*

iii) *Tout groupe algébrique quotient d'un groupe unipotent est unipotent.*

iv) *Toute extension d'un groupe algébrique unipotent par un groupe algébrique unipotent est itou.*

Démonstration. i) résulte immédiatement de 1.3 et 1.2. Pour établir les autres propriétés, nous pouvons supposer le corps k algébriquement clos. Alors iv) est évident sur la définition 1.3.

538 Soient donc G un groupe algébrique unipotent, G′ un sous-groupe algébrique de G, G″ un groupe algébrique quotient de G, G_i $(i = 1, \ldots, n)$ une suite de composition de G telle que $H_i = G_i/G_{i+1}$ soit un groupe unipotent élémentaire (1.7).

Pour prouver ii), considérons la suite de composition de G′ induite par celle de G : $G'_i = G_i \cap G'$. Le groupe G'_i/G'_{i+1} s'identifie à un sous-groupe algébrique de H_i, donc est isomorphe à un sous-groupe de $\mathbb{G}_a$ et par suite G′ est unipotent.

Pour prouver iii), considérons la suite de composition de G″ image de celle de G : G''_i = image de G_i dans G″. Le groupe G''_i/G''_{i+1} est alors un quotient de H_i et il suffit de prouver le lemme :

Lemme 2.3. — *Si* H *est groupe unipotent élémentaire* (1.7) *défini sur un corps k, tout groupe algébrique quotient* H″ *de* H *est nul ou est isomorphe à* H *sur k.*

Démonstration. Si $H = \mathbb{G}_a$ en caractéristique 0, ou si $H = \boldsymbol{\alpha}_p$ ou $\mathbb{Z}/p\mathbb{Z}$ $(p > 0)$, il suffit de noter qu'il résulte de 1.5 que H ne possède pas de sous-groupes algébriques autres que 0 et H (remarquer qu'un sous-groupe algébrique non nul de $\boldsymbol{\alpha}_p$ est défini par une k-algèbre de rang sur k au moins égal à p (1.5 iii) donc est égal à $\boldsymbol{\alpha}_p$).

Soit maintenant $H = \mathbb{G}_a$ $(p > 0)$, de sorte que l'on a une suite exacte :

$$0 \longrightarrow N \longrightarrow \mathbb{G}_a \longrightarrow H'' \longrightarrow 0.$$

Si $N = \mathbb{G}_a$, alors $H'' = 0$. Sinon, procédant par récurrence sur la longueur d'une
539 suite de composition de N, on peut supposer que $N = \boldsymbol{\alpha}_p$, ou que N est une forme de $(\mathbb{Z}/p\mathbb{Z})^r$ (1.5).

a) Si $N \simeq \boldsymbol{\alpha}_p$, la démonstration de 1.5 iii) montre que N est nécessairement le noyau du morphisme de Frobenius F dans $\mathbb{G}_a$ et on conclut à l'aide de la suite exacte :

$$0 \to \boldsymbol{\alpha}_p \to \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \to 0$$

b) Si $N \simeq \mathbb{Z}/p\mathbb{Z}$, il est immédiat qu'il existe $a \in k^*$ tel que N soit le sous-schéma fermé de $\mathbb{G}_a = \operatorname{Spec} k[X]$, défini par l'équation $X^p - aX = 0$. On conclut alors à l'aide de la suite exacte :

$$0 \to N \to \mathbb{G}_a \xrightarrow{\mathscr{P}} \mathbb{G}_a \to 0,$$

où $\mathscr{P}$ est le morphisme d'Artin-Schreier : $x \mapsto x^p - ax$.

c) Si N est une forme de $(\mathbb{Z}/p\mathbb{Z})^r$, il existe une extension finie galoisienne k' de k qui trivialise N. D'après b) et une récurrence évidente sur r, $\mathbb{G}_a/N$ est une forme de $\mathbb{G}_a$ trivialisée par k'. Il suffit alors d'appliquer le lemme suivant :

Lemme 2.3 bis. — *Soit k un corps,* G *un k-groupe algébrique qui est une forme de $\mathbb{G}_a$, trivialisée par une extension finie k',* séparable *de k. Alors* G *est isomorphe à $\mathbb{G}_a$.*

En effet, le groupe des k'-automorphismes du groupe algébrique $(\mathbb{G}_a)_{k'}$ est le groupe des homothéties non nulles $(k')^\times$ (*Bible*, Exp. 9, Lemme 1) et le groupe de cohomologie galoisienne $\mathrm{H}^1(k'/k, \mathbb{G}_m)$ est nul (on peut supposer que k' est une extension galoisienne de k), d'après le théorème 90 de Hilbert. Le lemme 2.3 bis résulte alors de la classification des k-formes d'un groupe algébrique (cf. J.-P. Serre, *Cohomologie galoisienne*, Chap. III, 1.3).

Ceci achève la démonstration de 2.2. 540

Proposition 2.4. — *Soient k un corps,* M *un k-groupe de type multiplicatif* (Exp. VIII) *et de type fini,* U *un k-groupe algébrique unipotent. Alors :*

i) $\underline{\mathrm{Hom}}_{k\text{-gr}}(\mathrm{M}, \mathrm{U}) = \underline{\mathbf{e}}$ (*a fortiori* $\mathrm{Hom}_{k\text{-gr}}(\mathrm{M}, \mathrm{U}) = e$).

ii) $\mathrm{Hom}_{k\text{-gr}}(\mathrm{U}, \mathrm{M}) = e$.

Pour démontrer i) nous devons établir que pour tout préschéma S au-dessus de k, $\mathrm{Hom}_{\mathrm{S}\text{-gr}}(\mathrm{M}_\mathrm{S}, \mathrm{U}_\mathrm{S}) = e$. Mais cela résulte du lemme suivant :

Lemme 2.5. — *Soient* S *un préschéma,* M *un* S*-groupe de type multiplicatif et de type fini sur* S*,* U *un* S*-préschéma en groupes, de présentation finie sur* S*, à fibres unipotentes, alors* $\mathrm{Hom}_{\mathrm{S}\text{-gr}}(\mathrm{M}, \mathrm{U}) = e$.

En effet, avec les hypothèses faites, pour qu'un S-morphisme de groupe $u : \mathrm{M} \to \mathrm{U}$ soit l'homomorphisme unité, il suffit que la restriction de u aux fibres de M au-dessus des points de S soit le morphisme nul (Exp. IX 5.2). Nous sommes donc ramenés au cas où S est le spectre d'un corps, que l'on peut supposer de plus algébriquement clos. Vu la définition 1.1, on peut se borner à $\mathrm{U} = \mathbb{G}_a$, auquel cas la propriété a déjà été démontrée (Exp. XII 4.4.1).

Prouvons maintenant 2.4 ii). Soit donc $u : \mathrm{U} \to \mathrm{M}$ un k-morphisme de groupes. L'image $u(\mathrm{U})$ est représentable par un sous-groupe algébrique U'' de M (Exp. VI_B 5.4). [(3)] Le groupe U'' est unipotent comme quotient d'un groupe unipotent (2.2 iii)) et est de type multiplicatif comme sous-groupe d'un groupe de type multiplicatif 541
(cf. *Bible*, Exp. 4, Th. 2 cor. 1, ou Exp. IX 6.8), donc U'' est le groupe unité d'après 2.4 i).

Remarque 2.6. — Gardant les notations de 2.4, il n'est plus vrai en général que le foncteur $\underline{\mathrm{Hom}}_{k\text{-gr}}(\mathrm{U}, \mathrm{M})$ soit égal à $\underline{\mathbf{e}}$. Ainsi, prenons un préschéma S tel que $\Gamma(\mathrm{S}, \mathscr{O}_\mathrm{S})$ contienne un élément non nul ε tel que $\varepsilon^2 = 0$ (par exemple le spectre de l'algèbre des nombres duaux d'un anneau A). Pour tout S' au-dessus de S, l'application $u \mapsto 1 + \varepsilon_{\mathrm{S}'} u$ définit un homomorphisme, fonctoriel en S', du groupe additif $\Gamma(\mathrm{S}', \mathscr{O}_{\mathrm{S}'})$ dans le groupe multiplicatif $\Gamma(\mathrm{S}', \mathscr{O}_{\mathrm{S}'}^\times)$, donc définit un S-morphisme de groupes $(\mathbb{G}_a)_\mathrm{S} \to (\mathbb{G}_m)_\mathrm{S}$, et comme $\varepsilon \neq 0$, ce morphisme n'est pas nul.

Rappelons (Exp. VII_A § 3) que lorsque G est un S-préschéma en groupes commutatif, fini et plat sur S, on dispose de la dualité de Cartier, et G est réflexif au sens de Exp. VIII § 1. Plus précisément, le foncteur $\mathrm{G} \mapsto \underline{\mathrm{Hom}}_{\mathrm{S}\text{-gr}}(\mathrm{G}, \mathbb{G}_m)$ est représentable

(3) N.D.E. : vérifier cette réf.

par un S-préschéma en groupes D(G) commutatif, fini et plat sur S, et le morphisme canonique $G \to D(D(G))$ est un isomorphisme. En particulier, on obtient :

(i) $D(\boldsymbol{\mu}_n) \simeq \mathbb{Z}/n\mathbb{Z}$ et par suite $D(\mathbb{Z}/n\mathbb{Z}) \simeq \boldsymbol{\mu}_n$.

(ii) Si S est de caractéristique $p > 0$, $D(\boldsymbol{\alpha}_p) \simeq \boldsymbol{\alpha}_p$.

3. Groupes unipotents opérant sur un espace vectoriel

542

Rappelons (Exp. I ,4.6.1) que si S est un préschéma et M un faisceau de $\mathscr{O}_S$-modules, on note $\mathbf{W}(M)$ le S-foncteur : $(\mathbf{Sch}/S)^\circ \to (\mathbf{Ens})$ défini par la condition $\mathbf{W}(M)(S') = \Gamma(S', M \otimes \mathscr{O}_{S'})$ pour tout S-préschéma S′.

Par ailleurs, rappelons que si un S-groupe opère sur un S-foncteur $\mathbf{V}$, on définit le S-foncteur $\mathbf{V}^G$ des invariants de $\mathbf{V}$ sous G, comme étant le sous-foncteur de $\mathbf{V}$ dont l'ensemble des points à valeur dans un S′ au-dessus de S est l'ensemble des $x \in \mathbf{V}(S')$ tels que $x_{S''}$ soit fixe sous $G(S'')$ pour tout S″ au-dessus de S′.

Ceci étant, on a le lemme suivant :

Lemme 3.1. — *Soient* S *un préschéma,* G *un* S*-préschéma en groupes, affine sur* S*, défini par la* $\mathscr{O}_S$*-algèbre quasi-cohérente* A*. Supposons que* G *opère sur un faisceau quasi-cohérent de* $\mathscr{O}_S$*-modules* M*, et soient* $\mu : M \to A \otimes_{\mathscr{O}_S} M$ *le comorphisme définissant l'action de* G *sur* M (Exp. I 4.7.2) *et* $\nu : M \to A \otimes_{\mathscr{O}_S} M$ *le morphisme* $x \mapsto \mu(x) - 1 \otimes x$*. Alors :*

i) $\underline{M}^G(S) = \Gamma \operatorname{Ker}(\nu)$.

ii) *Si* S *est le spectre d'un corps* k, $\underline{M}^G$ *est de la forme* $W(N)$*, où* N *est un sous-espace vectoriel de* M.

iii) *Si* S *est le spectre d'un corps* k*, tout élément* x *de* M *est contenu dans un*
543 *sous-espace vectoriel de* M*, de dimension finie sur* k*, stable sous l'action de* G.

Démonstration. iii) est mis pour mémoire et a déjà été démontré dans Exp. VI_B 11.2.

i) Il est clair que $\underline{M}^G(S)$ contient $\Gamma \operatorname{Ker}(\nu)$. Pour établir la réciproque, on peut supposer S affine d'anneau B. Soit $m \in \underline{M}^G(S)$. Alors pour toute B-algèbre B′ et tout u élément de $\operatorname{Hom}_{B\text{-alg}}(A, B')$ (u correspond à un élément de $G(\operatorname{Spec} B')$), on a :

$$(u \otimes 1_M)\nu(m) = 0 \text{ dans } B' \otimes_B M.$$

Prenons en particulier $B' = A$ et u l'identité de A, on trouve bien $\nu(m) = 0$.

ii) Soit N le noyau de ν, égal à $\underline{M}^G(k)$ d'après i). Tout k-préschéma S est plat sur k, donc on a :

$$\underline{M}^G(S) = \Gamma \operatorname{Ker}(\nu \otimes_k S) = \Gamma(N \otimes_k S).$$

Donc $\underline{M}^G$ est isomorphe au foncteur $W(N)$.

Proposition 3.2. — *Soit* G *un groupe algébrique unipotent, défini sur un corps* k*, qui opère sur un* k*-espace vectoriel* V*. Alors si* $V \neq 0$*, on a* $\mathbf{V}^G \neq 0$.

Compte tenu de 3.1 ii) et iii), on peut supposer k algébriquement clos et V de dimension finie sur k.

Soit $0 \to G' \to G \to G'' \to 0$ une suite exacte de groupes algébriques et supposons que G opère sur un faisceau $\mathbf{V}$ (pour la topologie fpqc). On a bien sûr $\mathbf{V}^G \subset \mathbf{V}^{G'}$ et le préfaisceau quotient G/G' opère de façon naturelle sur $\mathbf{V}^{G'}$. Mais $\mathbf{V}^{G'}$ est un **544** faisceau (comme noyau du couple de morphismes bien connu : $V \rightrightarrows \underline{\mathrm{Hom}}(G', V)$) ; par suite, le faisceau associé à G/G', c'est-à-dire G'', opère sur $\mathbf{V}^{G'}$, et il est immédiat de vérifier que $(\mathbf{V}^{G'})^{G''} = \mathbf{V}^G = (\mathbf{V}^{G'})^{G/G'}$.

Cette remarque permet de nous ramener, pour prouver 3.2, au cas où G est un groupe unipotent élémentaire (1.7).

a) $G = \mathbb{G}_a$, $p = 0$. Il résulte de (BIBLE 4 prop. 4) qu'un morphisme de $\mathbb{G}_a$ dans le groupe linéaire GL(V) est donné par une application exponentielle :

$$T \mapsto \sum_{q=0}^{\infty} T^q \frac{n^q}{q!}$$

où n est un endomorphisme nilpotent de V. Mais alors $V \neq 0 \Rightarrow \mathrm{Ker}\, n \neq 0$, et il est clair que tout vecteur de V annulé par n est laissé fixe par G.

Supposons maintenant $p > 0$.

b) $G = \boldsymbol{\alpha}_p$. Le groupe $\boldsymbol{\alpha}_p$ étant un groupe radiciel de hauteur 1 (Exp. VII$_A$ § 7), se donner une représentation de $\boldsymbol{\alpha}_p$ dans V revient à se donner une représentation de la p-algèbre de Lie $\boldsymbol{\alpha}_p$ dans $\mathfrak{gl}(V)$ (App. II 2.2), c'est-à-dire ici, à se donner un élément X de End(V) tel que $X^p = 0$ (App. II 2.1). Mais alors $V \neq 0 \Rightarrow W = \mathrm{Ker}(X) \neq 0$, et toujours d'après (App. II 2.2), on a $W = V^{\boldsymbol{\alpha}_p}$.

c) $G = \mathbb{Z}/p\mathbb{Z}$. Une représentation de G dans V équivaut à la donnée d'un élément x de Aut(V) tel que $x^p = 1$, i.e. $(1 - x)^p = 0$, donc x est de la forme $1 + n$, avec n nilpotent et $W = \mathrm{Ker}\, n$ est laissé fixe par x. **545**

d) $G = \mathbb{G}_a$. Soit G_i, $i \in I$, la famille filtrante croissante des sous-groupes algébriques étales de $\mathbb{G}_a$, donc isomorphes à $(\mathbb{Z}/p\mathbb{Z})^{r_i}$ (prop. 1.5) et soit $V_i = V^{G_i}$. Comme V est de dimension finie non nulle, et que V_i est non nul d'après c), la famille filtrante décroissante des V_i est stationnaire, et $W = \bigcap_{i \in I} V_i \neq 0$. Or on a le lemme :

Lemme 3.3. — *La famille des sous-groupes étales de* $(\mathbb{G}_a)_S$ (S-*préschéma de caractéristique* $p > 0$) *est schématiquement dense dans* G (Exp. IX 4.1).

D'après Exp. IX 4.4, il suffit de prouver le lemme lorsque S est le spectre du corps premier $\mathbb{F}_p$. Dans ce cas, il suffit de considérer la famille de sous-groupes étales G_n ($n \geqslant 1$) d'équation $X^{p^n} - X = 0$, qui est schématiquement dense dans $(\mathbb{G}_a)_{\mathbb{F}_p}$ puisqu'elle contient tout point fermé.

Ceci étant, revenons à la démonstration de 3.2 d). Si $w \in W$, son stabilisateur dans G est un sous-groupe algébrique de $\mathbb{G}_a$ qui majore G_i pour tout $i \in I$, donc est égal à $\mathbb{G}_a$ (3.3) et par suite $W = V^G$.

On déduit immédiatement de 3.2 le

Corollaire 3.4. — *Soient k un corps,* G *un k-groupe algébrique unipotent qui opère sur un k-espace vectoriel* V *de dimension finie. Alors* V *possède une suite de sous-espaces*
546 *vectoriels* V_i*, définis sur k, stables par* G*,*

$$0 = \mathrm{V}_0 \subset \mathrm{V}_1 \subset \ldots \subset \mathrm{V}_n = \mathrm{V},$$

tels que G *opère trivialement sur* $\mathrm{V}_{i+1}/\mathrm{V}_i$*. On peut de plus supposer* $\mathrm{V}_{i+1}/\mathrm{V}_i$ *de dimension* 1*.*

Nous allons maintenant résumer et compléter les propriétés déjà démontrées des groupes unipotents dans le théorème suivant :

Théorème 3.5. — *Soit* G *un groupe algébrique défini sur un corps k. Il y a équivalence entre les propriétés suivantes :*

i) G *est unipotent.*

ii) G *possède une suite de composition, définie sur k, dont les quotients successifs sont isomorphes à $\mathbb{G}_a$ si $p = 0$ (resp. à $\boldsymbol{\alpha}_p$, $\mathbb{G}_a$, ou $(\mathbb{Z}/p\mathbb{Z})^r$ tordu* (1.4) *si $p > 0$).*

iii) *Comme dans* ii)*, mais on suppose de plus la suite de composition centrale.*

iv) G *possède une suite de composition* caractéristique (Exp. $\mathrm{VI_B}$) *définie sur k, dont les quotients successifs sont isomorphes à $(\mathbb{G}_a)^r$ si $p = 0$ (resp. à $(\boldsymbol{\alpha}_p)^r$, $(\mathbb{G}_a)^s$ tordu ou $(\mathbb{Z}/p\mathbb{Z})^t$ tordu, pris dans cet ordre, si $p > 0$).*

v) G *est isomorphe à un sous-groupe algébrique du groupe* $\mathrm{Trigstr}(n)_k$ *des matrices triangulaires supérieures strictes du groupe linéaire* $\mathrm{GL}(n)_k$*, pour un entier $n \geqslant 0$ convenable.*

vi) G *est affine et pour toute représentation linéaire de* G *dans un k espace vectoriel* V*, de dimension finie, non nul, on a* $\mathrm{V}^{\mathrm{G}} \neq 0$*.*

547 *Démonstration.*

i) ⇒ vi) d'après 2.1 et 3.2.

vi) ⇒ v). Le groupe algébrique G étant affine, G est un sous-groupe algébrique d'un groupe linéaire convenable GL(V) (Exp. $\mathrm{VI_B}$ 11.3). Appliquons 3.4 à la représentation de G dans V définie par ce plongement, on trouve v).

v) ⇒ iii). On sait que le groupe algébrique $\mathrm{Trigstr}(n)$ possède une suite de composition centrale, à quotients successifs isomorphes à $\mathbb{G}_a$. La suite de composition induite sur G donne la propriété iii), compte tenu de 1.5.

iii) ⇒ ii) ⇒ i) et iv) ⇒ i) est clair.

Nous démontrerons i) ⇒ iv) dans un instant, mais notons déjà quelques conséquences de ce qui a été démontré.

Définition 3.6. — Nous dirons qu'une p-algèbre de Lie $\mathfrak{g}$ ($p > 0$) (cf. Exp. $\mathrm{VII_A}$ § 5) est *unipotente* si l'application $x \mapsto x^{(p)}$ est nilpotente, c.-à-d. si pour tout $x \in \mathfrak{g}$, il existe un entier $n > 0$, tel que $x^{(p^n)} = 0$.

Corollaire 3.7. — *Un groupe algébrique* G *unipotent est nilpotent* (Exp. $\mathrm{VI_B}$ § 8)*; son algèbre de Lie* $\mathfrak{g}$ *est nilpotente* (Bourbaki, Groupes et algèbres de Lie, Chap. 1 § 4) *et est isomorphe à une algèbre de Lie d'endomorphismes nilpotents d'un espace vectoriel*

de dimension finie. En caractéristique $p > 0$, $\mathfrak{g}$ est une p-algèbre de Lie unipotente (3.6).

Comme i) ⇒ v), il suffit de prouver 3.7 lorsque $G = \mathrm{Trigstr}(n)$. Nous avons déjà utilisé le fait que $\mathrm{Trigstr}(n)$ est un groupe algébrique nilpotent. Par ailleurs l'algèbre de Lie $\mathfrak{h}$ de $\mathrm{Trigstr}(n)$ est formée des endomorphismes de V triangulaires supérieurs **548** qui ont des zéros sur la diagonale principale. Ils sont donc nilpotents et par suite $\mathfrak{h}$ est nilpotente (Bourbaki, *loc. cit.* Chap. 1 § 4. cor. 3). Si $p > 0$, comme la puissance $p^{\text{ième}}$ dans la p-algèbre de Lie $\mathfrak{gl}(V) = \mathrm{End}(V)$ coïncide avec la puissance $p^{\text{ième}}$ des endomorphismes de V (Exp. $\mathrm{VII_A}$ 6.4.4), on voit que $\mathfrak{h}$ est unipotente.

Corollaire 3.8. — *Soit k un corps algébriquement clos et soit* G *un groupe algébrique* lisse *et affine sur k. Alors les propriétés suivantes sont équivalentes :*

i) G *est unipotent.*

ii) $G(k)$ *est formé d'éléments unipotents* (BIBLE 4 prop. 4 cor. 1)*, c'est-à-dire* G *est unipotent au sens de* BIBLE.

i) ⇒ ii) car G est isomorphe à un sous-groupe algébrique d'un groupe $\mathrm{Trigstr}(n)$ d'après 3.2 i) ⇒ v).

ii) ⇒ i). Soit donc G un groupe algébrique unipotent au sens de BIBLE et notons G^0 sa composante neutre. Les tores maximaux de G^0 étant formés d'éléments unipotents sont triviaux, donc G^0 est égal à ses sous-groupes de Cartan. Par suite, G^0 est résoluble (BIBLE 6 Th. 6), donc est triangularisable (BIBLE 6. Th. 1). Bref, G^0 est un sous-groupe algébrique d'un groupe $\mathrm{Trigstr}(n)$, il est donc unipotent au sens de cet exposé.

Le groupe $(G/G^0)(k)$ est un groupe fini formé d'éléments unipotents ; il est donc nul si $p = 0$ et égal à un p-groupe fini si $p > 0$ (BIBLE 4 prop. 4). Mais alors G/G^0 est unipotent au sens de cet exposé comme extension multiple de groupes isomorphes à $\mathbb{Z}/p\mathbb{Z}$. Ceci prouve que G est unipotent.

Fin de la démonstration de 3.5. Prouvons que i) ⇒ iv). **549**

a) $p > 0$. Considérons la suite croissante de sous-groupes algébriques de G :

$$\{e\} \subset {}_{\mathrm{F}}(G) \subset {}_{\mathrm{F}^2}(G) \subset \cdots \subset {}_{\mathrm{F}^n}(G) \subset G^0 \subset G.$$

On obtient ainsi une suite de composition caractéristique de G (App. II 1) et pour n assez grand, $G/{}_{\mathrm{F}^n}(G)$ est lisse (App. II 3.1) de sorte que les quotients successifs sont, dans l'ordre :

(1) des groupes radiciels de hauteur 1,
(2) un groupe lisse et connexe,
(3) un groupe étale.

Pour prouver i) ⇒ iv) il nous suffit donc de prouver le :

Lemme 3.9. — *Soit* G *un groupe algébrique unipotent défini sur un corps k de caractéristique $p > 0$. Alors* G *possède une suite de composition caractéristique, définie sur k, dont les quotients successifs sont isomorphes à :*

i) $(\boldsymbol{\alpha}_p)^r$ *si* G *est radiciel.*
ii) $(\mathbb{G}_a)^r$ *tordu si* G *est lisse et connexe.*

iii) $(\mathbb{Z}/p\mathbb{Z})^r$ *tordu si* G *est étale.*

Démonstration. i) Le groupe G est radiciel. Filtrant G par les $\mathrm{F}^n(\mathrm{G})$, on se ramène au cas où G est radiciel de hauteur 1. Comme G est nilpotent (3.5 i) ⇒ iii)) et que le centre d'un groupe algébrique est représentable (Exp. VIII 6.5 e)), on peut considérer
550 la suite centrale ascendante de G, évidemment caractéristique dans G, ce qui nous ramène au cas où G est de plus commutatif.

Soit $\mathfrak{g} = \mathrm{Lie}(\mathrm{G})$. Le morphisme π de puissance $p^{\text{ième}}$ est donc additif dans $\mathfrak{g}$ (Exp. $\mathrm{VII_A}$) ; nous allons nous ramener au cas où elle est nulle. Pour tout préschéma S au-dessus de k, posons $\mathfrak{g}_\mathrm{S} = \mathfrak{g} \otimes_k \mathscr{O}_\mathrm{S}$ et soit $\mathfrak{h}_\mathrm{S}$ le sous-faisceau de groupes abéliens de $\mathfrak{g}_\mathrm{S}$, image de $\mathfrak{g}_\mathrm{S}$ par π_S. Enfin soit $\overline{\mathfrak{h}}_\mathrm{S}$ le sous-faisceau de $\mathscr{O}_\mathrm{S}$-modules de $\mathfrak{g}_\mathrm{S}$ engendré par $\mathfrak{h}_\mathrm{S}$. Il est clair que $\overline{\mathfrak{h}}_\mathrm{S} = \mathfrak{h}_k \otimes_k \mathscr{O}_\mathrm{S}$ et que $\overline{\mathfrak{h}}_\mathrm{S}$ [(4)] est une sous-p-algèbre de Lie caractéristique de $\mathfrak{g}_\mathrm{S}$ (c'est-à-dire est stable par le S-foncteur $\underline{\mathrm{Aut}}_{p\text{-Lie}}(\mathfrak{g})$). Il résulte alors de App. II 2.2 que $\overline{\mathfrak{h}}_k$ est l'algèbre de Lie d'un sous-groupe algébrique H de G caractéristique dans G.

De plus, compte tenu de 3.7 et du lemme 3.9 bis ci-après, si $\mathrm{G} \neq \{e\}$, H est distinct de G, car $\overline{\mathfrak{h}}_k$ est distinct de $\mathfrak{g}$. Par ailleurs, si $\mathrm{G}/\mathrm{H} = \mathrm{G}''$, on a $\mathrm{Lie}\,\mathrm{G}'' = \mathfrak{g}/\overline{\mathfrak{h}}_k$ (App. II 2.2), et par suite, la puissance $p^{\text{ième}}$ est nulle dans $\mathrm{Lie}\,\mathrm{G}''$. Procédant par récurrence sur $\dim \mathrm{Lie}\,\mathrm{G}$, on est donc ramené au cas où $\mathrm{Lie}\,\mathrm{G}$ est une p-algèbre de Lie dans laquelle la puissance $p^{\text{ième}}$ est nulle. Mais alors $\mathrm{Lie}\,\mathrm{G}''$ est isomorphe à $\mathrm{Lie}(\boldsymbol{\alpha}_p)^r$ pour un entier $r \geqslant 0$ convenable (App. II 2.1) et par suite (App. II 2.2), G″ est isomorphe à $(\boldsymbol{\alpha}_p)^r$. Il reste à prouver le

Lemme 3.9 bis. — *Soient k un corps de caractéristique $p > 0$, $\mathfrak{g}$ une p-algèbre de Lie, commutative, unipotente* (3.6)*, de dimension finie sur k, et $\mathfrak{h}$ la sous-p-algèbre de Lie de $\mathfrak{g}$ engendrée par l'image de la puissance $p^{ième}$ dans $\mathfrak{g}$. Alors si $\mathfrak{g} \neq 0$, on a $\mathfrak{h} \neq \mathfrak{g}$.*

En effet, comme $\mathfrak{g}$ est commutative, $\mathfrak{h}$ est simplement le sous-k-espace vectoriel
551 de $\mathfrak{g}$ engendré par les $\mathrm{X}^{(p)}$ ($\mathrm{X} \in \mathfrak{g}$). Si $\mathfrak{g}$ est $\neq 0$ et est unipotente, il existe $\mathrm{X} \in \mathfrak{g}$, $\mathrm{X} \neq 0$, tel que $\mathrm{X}^{(p)} = 0$. Soit $\mathrm{X}_1, \ldots, \mathrm{X}_n$ une base d'un supplémentaire dans $\mathfrak{g}$ de la droite $k\mathrm{X}$. L'algèbre de Lie $\mathfrak{h}$ est alors le sous-k-espace vectoriel de $\mathfrak{g}$ engendré par $\mathrm{X}_1^{(p)}, \ldots, \mathrm{X}_n^{(p)}$, donc est de dimension au plus $n = \dim \mathfrak{g} - 1$.

Démonstration de 3.9 ii) G est lisse et connexe. Dans ce cas, la suite centrale descendante de G est représentable par des sous-groupes algébriques G_i lisses et connexes caractéristiques (Exp. $\mathrm{VI_B}$ 8.3 et 7.4) et $\mathrm{G}_i = 0$ pour i assez grand, puisque G est nilpotent (3.5 i) ⇒ iii)). Il suffit de prouver 3.9 pour les groupes $\mathrm{G}_i/\mathrm{G}_{i+1}$, ce qui nous ramène au cas où de plus G est commutatif. Pour tout entier $n > 0$, soit G_n le sous-groupe algébrique de G image de G par le morphisme d'élévation à la puissance p^n-ième. Le groupe G_n est donc lisse, connexe et caractéristique, et il résulte de la définition 1.1 des groupes unipotents que $\mathrm{G}_n = 0$ pour n assez grand. Remplaçant G par $\mathrm{G}_n/\mathrm{G}_{n+1}$, on peut supposer de plus que G est annulé par l'élévation à la puissance p. Mais alors, d'après (J.-P. Serre, *Groupes algébriques et corps de classe*q, chap. VII, prop. 11) G est une forme de $(\mathbb{G}_a)^r$, pour un entier r convenable.

(4) N.D.E. : on a changé $\mathfrak{h}$ en $\overline{\mathfrak{h}}$.

Démonstration de 3.9 iii) G est étale. Procédant comme dans ii), on se ramène au cas où G est commutatif, puis au cas où G est annulé par p, mais alors $G_{\overline{k}}$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$.

Démonstration de 3.5 i) $\Rightarrow$ iv) dans le cas b) $p = 0$. Le groupe G est alors lisse et connexe, et procédant comme dans 3.9 ii), on se ramène au cas où G est de plus commutatif. On a alors le résultat plus précis suivant :

Lemme 3.9 ter. — *Soient k un corps de caractéristique* 0, G *un-k-groupe algébrique unipotent, commutatif,* $\mathfrak{g} = \operatorname{Lie} G$. *Alors il existe un isomorphisme canonique :* 552

$$\exp : W(\mathfrak{g}) \xrightarrow{\sim} G$$

Le morphisme exp *est l'unique homomorphisme* $W(\mathfrak{g}) \to G$ *qui induit l'identité sur les algèbres de Lie.*

Comme G est unipotent, G se réalise comme sous-groupe algébrique de $\mathrm{Trigstr}(n)$ pour un entier n convenable (3.5 i) $\Rightarrow$ v)). Le choix d'un tel plongement permet d'identifier $\mathfrak{g}$ à une sous-algèbre de Lie de $\mathfrak{gl}(n)$ formée d'endomorphismes nilpotents. D'où un k-morphisme :

$$\exp : W(\mathfrak{g}) \longrightarrow \mathrm{GL}(n), \qquad T \mapsto \sum_{i \geqslant 0} \frac{T^i}{i!}.$$

Comme G est commutatif, le morphisme exp est un homomorphisme. Soit G' le groupe algébrique image de $W(\mathfrak{g})$ par le morphisme exp. Si l'on identifie canoniquement $\operatorname{Lie} W(\mathfrak{g})$ à $\mathfrak{g}$, l'application linéaire tangente à exp est simplement l'injection $\mathfrak{g} \to \mathfrak{gl}(n)$. Par suite $\operatorname{Lie}(G \cap G') = \mathfrak{g} \cap \mathfrak{g} = \mathfrak{g}$. Comme $G \cap G'$ est lisse (Exp. $\mathrm{VI_B}$ 1.6.1) et G connexe (car extension multiple de groupes $\mathbb{G}_a$ (3.5 i) $\Rightarrow$ ii)), on a nécessairement $G = G'$. Le noyau $\operatorname{Ker}(\exp)$ est un groupe unipotent étale, donc est le groupe unité et par suite exp est un isomorphisme de $W(\mathfrak{g})$ sur G.

Si $h : W(\mathfrak{g}) \to G$ est un autre homomorphisme tel que $\operatorname{Lie}(h)$ soit l'application identique de $\mathfrak{g}$, le morphisme $h - \exp$ est un homomorphisme (G est commutatif) donc l'application linéaire tangente est nulle. Comme k est de caractéristique 0 et 553
$W(\mathfrak{g})$ connexe, il résulte encore du théorème de Cartier que l'on a nécessairement $h = \exp$.

Proposition 3.10. — *Soit* G *un groupe algébrique défini sur un corps k algébriquement clos. Alors les propriétés suivantes sont équivalentes :*

i) *Tout morphisme d'un groupe de type multiplicatif* M *dans* G *est le morphisme nul.*

i bis) G *ne possède pas de sous-groupes de type multiplicatif non nuls.*

ii) a) *si $p = 0$:* $G(k)$ *ne contient pas de points d'ordre fini autres que e ;*

b) *si $p \neq 0$: pour tout nombre premier $q \neq p$, $x \in G(k)$ et $x^q = e$ implique $x = e$,*

pour tout $X \in \mathfrak{g} = \operatorname{Lie} G$ tel que $X^{(p)} = X$, on a $X = 0$.

ii bis) a) *si* $p = 0$ *:* *comme* ii) a) *;*

b) *si* $p \neq 0$ *:* *tout sous-groupe fini de* $\mathrm{G}(k)$ *est un* p*-groupe, pour tout* $\mathrm{X} \in \mathfrak{g} = \mathrm{Lie}\,\mathrm{G}$ *tel que* $\mathrm{X}^{(p)} = \mathrm{X}$*, on a* $\mathrm{X} = 0$.

Démonstration.

i) $\Leftrightarrow$ i bis), puisque l'image d'un groupe de type multiplicatif est de type multiplicatif (Exp. IX 2.7).

554 ii) $\Leftrightarrow$ ii bis). Car si un groupe fini ordinaire H a un ordre qui n'est pas une puissance de p, il existe un nombre premier $q \neq p$, et un élément x de H distinct de e, tel que $x^q = e$ (théorème de Sylow, cf. J.-P. Serre, *Corps locaux*, chap. IX § 2).

i) $\Rightarrow$ ii) résulte du lemme suivant :

Lemme 3.11. — *Soit* G *un groupe algébrique défini sur un corps* k.

a) *Si* k *contient les racines* $n^{\text{ièmes}}$ *de l'unité,* n *entier premier à* p*, on a :*

$$\mathrm{Hom}_{k\text{-gr}}(\boldsymbol{\mu}_n, \mathrm{G}) \simeq \mathrm{Hom}_{k\text{-gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \simeq {}_n\mathrm{G}(k)$$

(*points d'ordre* n *de* $\mathrm{G}(k)$).

b) *Si* $p > 0$, $\mathrm{Hom}_{k\text{-gr}}(\boldsymbol{\mu}_p, \mathrm{G}) \simeq \{\mathrm{X} \in \mathfrak{g} = \mathrm{Lie}\,\mathrm{G},$ *tels que* $\mathrm{X}^{(p)} = \mathrm{X}\}$.

En effet, pour démontrer a) on note que $\boldsymbol{\mu}_n$ est alors isomorphe sur k à $(\mathbb{Z}/n\mathbb{Z})$, et b) est conséquence de App. II 2.1.

ii) $\Rightarrow$ i bis). D'après le lemme 3.11, ii) équivaut au fait que quelque soit le nombre premier r, G ne contient pas de sous-groupes $\boldsymbol{\mu}_r$, ce qui entraîne i bis) en raison du :

Lemme 3.12. — *Soit* G *un* S*-groupe diagonalisable, de type fini sur* S *et distinct du groupe unité. Alors il existe un nombre premier* r *et un sous-groupe de* G *isomorphe à* $(\boldsymbol{\mu}_r)_{\mathrm{S}}$.

Soit $\mathrm{G} = \mathrm{D}_{\mathrm{S}}(\mathrm{M})$, où M est un groupe abélien de type fini, donc extension d'un groupe libre M'' par un groupe fini M'. Si $\mathrm{M}'' \neq 0$, il est clair que M admet des quotients isomorphes à $\mathbb{Z}/r\mathbb{Z}$ pour tout entier r. Si $\mathrm{M}'' = 0$, M' admet un quotient
555 isomorphe à $\mathbb{Z}/r\mathbb{Z}$ pour tout nombre premier r divisant l'ordre de M. On en déduit le lemme par dualité.

Nous avons vu (prop. 2.4) qu'un groupe unipotent satisfait aux conditions équivalentes de 3.10. Le but du paragraphe suivant est de démontrer la réciproque.

4. Une caractérisation des groupes unipotents

556

Comme annoncé, nous allons montrer qu'un groupe algébrique G défini sur un corps k algébriquement clos, qui ne contient pas de sous-groupe de type multiplicatif non nul, est unipotent. En fait, il suffit qu'il ne contienne pas de sous-groupes de type multiplicatif « élémentaires » bien particuliers, qui dépendent des hypothèses faites sur G. Avant d'énoncer le théorème général, étudions en détail quelques cas particuliers.

4.1. Groupes algébriques lisses, connexes et affines. —

Proposition 4.1.1. — *Soient k un corps, G un k-groupe algébrique, lisse, connexe et affine, $\mathfrak{g} = \mathrm{Lie}\,\mathrm{G}$. Alors les propriétés suivantes sont équivalentes :*

i) G *est unipotent.*

ii) G *possède une suite de composition centrale, dont les quotients successifs sont des formes de $\mathbb{G}_a$.*

iii) G *possède une suite de composition centrale, caractéristique, dont les quotients successifs sont des formes de $(\mathbb{G}_a)^r$.*

iv) *Il existe un entier $n > 1$, tel que $\mathrm{G}_{\overline{k}}$ ne contienne pas de sous-groupe isomorphe à $\boldsymbol{\mu}_n$.*

v) *Tout tore maximal de G est le groupe unité.*

Supposons de plus que G soit un sous-groupe algébrique d'un groupe linéaire $\mathrm{GL}(n)$. Alors les conditions précédentes sont encore équivalentes à :

vi) $\mathfrak{g} \subset \mathfrak{gl}(n)$ *est formée d'endomorphismes nilpotents.* **557**

vii) $\mathfrak{g}$ *est nilpotente et son centre ne contient pas d'endomorphisme semi-simple non nul.*

Démonstration. ii) $\Rightarrow$ i) est clair et i) $\Rightarrow$ iii) a été vu dans 3.9. L'implication iii) $\Rightarrow$ ii) va résulter du lemme suivant :

Lemme 4.1.2. — *Soient k un corps, G un k-groupe algébrique qui est une forme de $(\mathbb{G}_a)^r$. Alors :*

a) G *se réalise comme sous-groupe algébrique du groupe $(\mathbb{G}_a)^n$ pour un entier n convenable.*

b) G *possède une suite de composition dont les quotients successifs sont des formes de $\mathbb{G}_a$.*

En effet, par hypothèse, il existe une extension k' de k telle que $\mathrm{G}_{k'}$ soit isomorphe à $(\mathbb{G}_{a,\,k'})^r$. D'après le principe de l'extension finie (EGA IV 9.1.1), on peut supposer que k' est une extension finie de k. Mais alors, pour a), il suffit de considérer l'immersion fermée canonique (EGA V [(5)]) :

$$\mathrm{G} \longrightarrow \prod_{k'/k} (\mathrm{G}_{k'})/k' \xrightarrow{\sim} (\mathbb{G}_{a,\,k})^n \quad (\text{avec } n = r\deg(k'/k)).$$

Pour prouver b), compte tenu de a), on peut supposer que G est un sous-groupe fermé de $\mathrm{G}' = (\mathbb{G}_a)^n$. Si $\mathrm{G} \neq 0$, il existe un hyperplan $\mathfrak{h}$ de $\mathfrak{g}' = \mathrm{Lie}\,\mathrm{G}'$ qui ne contient pas $\mathfrak{g}$. Soit H le sous-groupe vectoriel $\mathrm{W}(\mathfrak{h})$ de $\mathrm{W}(\mathfrak{g}') = \mathrm{G}'$. Comme H est défini par une équation dans G', $\mathrm{H} \cap \mathrm{G}$ est défini par une équation dans G et on a les inégalités :

$$\begin{aligned}\dim \mathrm{G} - 1 &\leqslant \dim(\mathrm{G} \cap \mathrm{H}) \\ &\leqslant \dim \mathrm{Lie}(\mathrm{G} \cap \mathrm{H}) = \dim_k(\mathfrak{g} \cap \mathfrak{h}) = \dim_k(\mathfrak{g}) - 1 = \dim \mathrm{G} - 1\end{aligned}$$

D'où $\dim(\mathrm{G}\cap\mathrm{H}) = \dim \mathrm{Lie}(\mathrm{G}\cap\mathrm{H})$ et par suite $\mathrm{G}\cap\mathrm{H}$ est lisse. Le groupe $\mathrm{G}_1 = (\mathrm{G}\cap\mathrm{H})^0$ **558**

[(5)] N.D.E. : donner ici une autre référence...

est un sous-groupe algébrique de G, lisse et connexe, tel que G/G_1 soit lisse, connexe, de dimension 1, donc est une forme de $\mathbb{G}_a$ (4.1 i) ⇒ iii)). On termine par récurrence sur la dimension de G.

Avant de poursuivre la démonstration de 4.1, notons que l'équivalence i) ⇔ ii) et 2.3 bis entraîne le corollaire suivant :

Corollaire 4.1.3. — *Si k est un corps* parfait*, un k-groupe algébrique lisse et connexe est unipotent si et seulement si il possède une suite de composition à quotients successifs isomorphes à* $\mathbb{G}_a$.

Suite de la démonstration de 4.1.

i) ⇒ iv) d'après 2.4 i).

iv) ⇒ v). D'après Exp. XIV 4.1, G possède un tore maximal T défini sur k. Or si $r = \dim T$, $({}_nT)_{\overline{k}}$ est isomorphe à $(\boldsymbol{\mu}_n)^r$. Donc $r = 0$.

v) ⇒ i) comme on l'a remarqué dans la démonstration de 3.8.

i) ⇒ vi). D'après 3.4, G est en fait contenu dans un sous-groupe algébrique de $GL(n)$ isomorphe à $\mathrm{Trigstr}(n)$, donc $\mathfrak{g}$ est formé d'endomorphismes nilpotents.

vi) ⇒ vii). En effet, $\mathfrak{g}$ est nilpotente d'après le théorème d'Engel (Bourbaki, *Groupes et algèbres de Lie*, chap. I § 4 cor. 3).

vii) ⇒ v). Soit T un sous-tore maximal de G (Exp. XIV 1.1), $\mathfrak{t}$ son algèbre de Lie. Le plongement de G dans $GL(n)$ définit une représentation de T qui est nécessairement
559 semi-simple (cela se voit sur une clôture algébrique $\overline{k}$ de k et on applique Exp. I 4.7.3). Donc si $X \in \mathfrak{t}$, X est un endomorphisme semi-simple dans $\mathfrak{gl}(n)$. On voit immédiatement que cela entraîne que l'application :

$$\mathrm{ad}\, X : Y \longmapsto [X, Y]$$

est un endomorphisme semi-simple de $\mathfrak{gl}(n)$ donc de $\mathfrak{g}$. Comme par ailleurs cet endomorphisme est nilpotent, $\mathfrak{g}$ étant nilpotente, ad X est nul, donc X est central. Mais alors $\mathfrak{t}$ est centrale et formée d'endomorphismes semi-simples, donc est nulle par hypothèse ; a fortiori, T est le groupe unité.

Remarque 4.1.4. — a) Nous donnerons plus loin (4.3.1) une caractérisation infinitésimale des groupes unipotents en caractéristique $p > 0$, qui est indépendante d'un plongement dans $GL(n)$.

b) Lorsque k est *parfait* les conditions ii) et iii) de 4.1.1 se simplifient en raison du lemme suivant :

Lemme 4.1.5. — *Si k est un corps parfait, tout k-groupe algébrique* G *qui est une forme de* $(\mathbb{G}_a)^r$ *est isomorphe à* $(\mathbb{G}_a)^r$.

Le lemme résulte de 3.9 ter si la caractéristique p de k est nulle, et de 2.3 bis si $r = 1$. Dans le cas général ($p > 0$), réalisons G comme sous-groupe algébrique de $(\mathbb{G}_a)^n$ pour un entier n convenable (4.1.2) et raisonnons par récurrence sur l'entier $n - r$. Si $r = n$ on a bien $G = (\mathbb{G}_a)^r$. Sinon le groupe quotient $\mathbb{G}_a^n/G$ est un groupe unipotent lisse connexe, non nul, qui, compte tenu de 4.1.1 i) ⇒ ii) et de 2.3 bis,
560 possède une suite de composition à quotients isomorphes à $\mathbb{G}_a$. On en déduit qu'il existe un sous-groupe algébrique G_1 de $(\mathbb{G}_a)^n$, lisse et connexe, contenant G, tel que

$\mathbb{G}_a^n/\mathrm{G}_1 = \mathbb{G}_a$. Par récurrence il suffit de montrer que G_1 est isomorphe à $(\mathbb{G}_a)^{n-1}$. Or il est immédiat de vérifier qu'un homomorphisme de $\operatorname{Spec} k[\mathrm{X}_1, \ldots, \mathrm{X}_n] = \mathbb{G}_a^n$ dans $\mathbb{G}_a = \operatorname{Spec} k[\mathrm{T}]$ est défini par un polynôme additif de la forme :

$$\sum_{i,j} a_{i,j} \mathrm{X}_i^{p^j}.$$

Comme G_1 est lisse, la partie linéaire de ce polynôme n'est pas nulle. Quitte à faire un changement linéaire sur les coordonnées X_i, nous pouvons supposer que G_1 est un sous-groupe algébrique de $(\mathbb{G}_a)^n$ défini par l'équation :

$$(*) \quad \mathrm{P}(\mathrm{X}) = -\mathrm{X}_1 + \sum_{j=1}^{q} a_j \mathrm{X}_1^{p^j} + \mathrm{Q}(\mathrm{X}_2, \ldots, \mathrm{X}_n) = 0,$$

$$\text{avec} \quad \mathrm{Q}(\mathrm{X}_2, \ldots, \mathrm{X}_n) = \sum_{\substack{i>1 \\ j>0}} b_{i,j} \mathrm{X}_i^{p^j}.$$

Procédons alors par récurrence sur le degré de P. Si $\deg \mathrm{P} = 1$, il est clair que $\mathrm{G}_1 \xrightarrow{\sim} \mathbb{G}_a^{n-1}$. Sinon, comme k est parfait, on a $\mathrm{Q}(\mathrm{X}) = \mathrm{Q}_1(\mathrm{X})^p$ et nous pouvons définir un endomorphisme v de $\mathbb{G}_a^n$ par les formules :

$$\mathrm{X}_i \mapsto \mathrm{X}_i \quad \text{pour } i > 1, \qquad \mathrm{X}_1 \mapsto \sum_{j=1}^{q} a_j^{1/p} \mathrm{X}_1^{p^{j-1}} + \mathrm{Q}_1(\mathrm{X}).$$

Il est clair que v induit un isomorphisme sur G_1 et que $v(\mathrm{G}_1)$ a pour équation dans $\mathbb{G}_a^n$:

$$(*)_1 \qquad \mathrm{P}_1(\mathrm{X}) = -\mathrm{X}_1 + \sum_{j=1}^{q} a_j^{1/p} \mathrm{X}_1^{p^j} + \mathrm{Q}_1(\mathrm{X}_2, \ldots, \mathrm{X}_n) = 0.$$

Distinguons alors deux cas :

1^{er} *cas.* $\deg(\mathrm{Q}) = \deg \mathrm{P} > p^q$. Alors on a $\deg \mathrm{P}_1 < \deg \mathrm{P}$ et on gagne par hypothèse **561**
de récurrence.

$2^{ème}$ *cas.* $\deg \mathrm{P} = p^q$ ($a_q \neq 0$). On a alors $\deg \mathrm{P}_1 = \deg \mathrm{P} = p^q$ et $\deg \mathrm{Q}_1 < p^q$. (On ne peut pas avoir $\mathrm{Q} = 0$, sinon G_1 ne serait pas connexe). Si le polynôme Q_1 ne possède pas de partie linéaire, on peut réitérer la transformation précédente. Continuant le processus, on obtient finalement une équation de la forme :

$$(*)_s \qquad \mathrm{P}_s(\mathrm{X}) = -\mathrm{X}_1 + \sum_{j=1}^{q} a_j^{1/p^s} \mathrm{X}_1^{p^j} + \mathrm{Q}_s(\mathrm{X}),$$

où $\mathrm{Q}_s(\mathrm{X}) = \mathrm{Q}(\mathrm{X}_2, \ldots, \mathrm{X}_n)^{1/p^s}$ est un polynôme additif ayant une partie linéaire non nulle, et de plus $\deg \mathrm{Q}_s < p^q$. Supposons par exemple que le coefficient de X_2 dans Q_s ne soit pas nul, et soit $-\mathrm{L}$ la partie linéaire de $\mathrm{P}_s(\mathrm{X})$. Quitte à faire un changement linéaire de coordonnées, l'équation de G_1 devient :

$$\mathrm{P}'(\mathrm{X}) = -\mathrm{L} + \sum_{j=1}^{q} a_j^{1/p^s} \mathrm{X}_1^{p^j} + \mathrm{Q}'(\mathrm{L}, \mathrm{X}_3, \ldots, \mathrm{X}_n),$$

où Q′ est un polynôme additif, sans partie linéaire, et $\deg(Q') < p^q$. Mais alors nous sommes ramenés au premier cas [6].

4.2. Groupes radiciels. —

Proposition 4.2.1. — *Soit* G *un groupe algébrique radiciel défini sur un corps* k *de caractéristique* $p > 0$. *Alors les conditions suivantes sont équivalentes :*

i) G *est unipotent.*

ii) G *possède une suite de composition centrale, à quotients successifs isomorphes à* $\boldsymbol{\alpha}_p$.

562 iii) G *possède une suite de composition centrale et caractéristique à quotients successifs isomorphes à* $(\boldsymbol{\alpha}_p)^r$.

iv) $G_{\overline{k}}$ *ne contient pas de sous-groupe isomorphe à* $\boldsymbol{\mu}_p$.

v) $\mathfrak{g} = \mathrm{Lie}\, G$ *est une* p*-algèbre de Lie unipotente* (3.6).

Démonstration. iii) ⇒ ii) ⇒ i) est clair, i) ⇒ iii) est 3.9 i), et i) ⇒ iv) d'après 2.4 i).

Nous aurons besoin du lemme suivant sur les p-algèbres de Lie abéliennes :

Lemme 4.2.2. — *Soit* $\mathfrak{g}$ *une* p*-algèbre de Lie, abélienne, de dimension finie sur un corps* k *parfait. Alors* $\mathfrak{g}$ *s'écrit de manière unique comme somme directe d'une sous-*p*-algèbre de Lie* $\mathfrak{r}$ *sur laquelle la puissance* $p^{ième}$ *est bijective et d'une sous-*p*-algèbre de Lie* $\mathfrak{u}$, *unipotente* (3.6). (*L'algèbre* $\mathfrak{r}$ *sera appelée la* partie réductive *de* $\mathfrak{g}$ *et* $\mathfrak{u}$ *la* partie unipotente.) *La formation de* $\mathfrak{r}$ *et* $\mathfrak{u}$ *est compatible avec l'extension du corps* k. *Si de plus* k *est algébriquement clos,* $\mathfrak{r}$ *admet une base* e_i *telle que* $e_i^{(p)} = e_i$.

La démonstration de ce lemme est facile et laissée au soin du lecteur (cf. Bourbaki, *Groupes et algèbres de Lie*, chap. I § 1 exercice 23). Disons simplement que $\mathfrak{u}$ est le noyau d'un itéré convenable de l'application $X \mapsto X^{(p)}$ et que $\mathfrak{r}$ est l'image du même itéré.

563 Ceci étant, prouvons iv) ⇒ v). Quitte à faire une extension du corps de base, on peut supposer k algébriquement clos.

Soit alors X un élément de $\mathfrak{g}$ et $\mathfrak{h}$ la sous-p-algèbre de Lie engendrée par X dans $\mathfrak{g}$. L'algèbre $\mathfrak{h}$ est évidemment commutative et sa partie réductive (4.2.2) est nulle, sinon d'après *loc. cit.*, $\mathfrak{h}$ contiendrait un élément $Y \neq 0$, tel que $Y^{(p)} = Y$ et par suite (App. II 2.1 et 2.2) G contiendrait un sous-groupe isomorphe à $\boldsymbol{\mu}_p$ contrairement à l'hypothèse. Donc $\mathfrak{h}$, et par suite $\mathfrak{g}$, est une p-algèbre de Lie unipotente.

v) ⇒ i). C'est l'implication la moins triviale de 4.2.1.

a) Cas où G est de hauteur 1 (Exp. VII_A 4.1.3). Comme G est radiciel, il est affine, donc isomorphe à un sous-groupe algébrique d'un groupe linéaire GL(V) (Exp. VI_B § 11). Ce plongement identifie $\mathfrak{g}$ à une sous-p-algèbre de Lie de End(V), la puissance $p^{\text{ième}}$ de X dans $\mathfrak{g}$ coïncidant avec la puissance $p^{\text{ième}}$ de l'endomorphisme X (Exp. VII_A 6.4.4). Comme $\mathfrak{g}$ est unipotente par hypothèse, $\mathfrak{g}$ est donc une algèbre d'endomorphismes nilpotents de V et d'après le *théorème d'Engel* (Bourbaki, Groupes et

[6] N.D.E. : en remplaçant X_1 par L.

algèbres de Lie, chap. I § 4 th. 1) est une sous-algèbre de Lie de l'algèbre de Lie $\mathfrak{h}$ du groupe des matrices triangulaires supérieures strictes Trigstr(n) par rapport à une base convenable de V. Comme G est de hauteur 1, on déduit alors de App. II 2.2 que G lui-même est un sous-groupe algébrique de Trigstr(n), donc est unipotent (3.5 v) ⇒ i)).

b) Cas général. Procédons par récurrence sur la hauteur h de G (*). Le cas $h = 1$ vient d'être traité. Supposons $h > 1$, posons $G' = {}_F G$ et $G'' = G/G'$. Le groupe G' est de hauteur 1 et $\mathrm{Lie}\, G' = \mathrm{Lie}\, G$ est unipotente, donc G' est unipotent d'après a). Pour **564**
montrer que G est unipotent, il suffit donc de prouver que G'' est unipotent (2.2). Mais G'' est de hauteur $h-1$, donc, par hypothèse de récurrence, il suffit de montrer que $\mathrm{Lie}\, G''$ est unipotente. Comme iv) ⇒ v), il suffit de montrer que $G''_{\overline{k}}$ ne contient pas de groupes isomorphes à $\boldsymbol{\mu}_p$. Soit donc un sous-groupe de $G''_{\overline{k}}$ isomorphe à $\boldsymbol{\mu}_p$, H son image réciproque dans $G_{\overline{k}}$. Le groupe G' étant unipotent, nous prouverons au § 5 que l'extension :

$$e \longrightarrow G'_{\overline{k}} \longrightarrow H \longrightarrow \boldsymbol{\mu}_p \longrightarrow e$$

est nécessairement triviale (la démonstration donnée de ce fait est indépendante des résultats du présent paragraphe). Bref le groupe $\boldsymbol{\mu}_p$ se relève dans H, mais étant de hauteur 1 il est nécessairement contenu dans $G'_{\overline{k}} = {}_F G_{\overline{k}}$, d'où une contradiction, G' étant unipotent.

4.3. Groupes affines connexes en caractéristique $p > 0$. —

Proposition 4.3.1. — *Soit* G *un groupe algébrique affine connexe sur un corps k de caractéristique $p > 0$. Alors les conditions suivantes sont équivalentes :*

i) G *est unipotent.*

ii) G *possède une suite de composition à quotients successifs isomorphes à* $\boldsymbol{\alpha}_p$ *et* $\mathbb{G}_a$ (*pris dans cet ordre*).

iii) G *admet une suite de composition, caractéristique, à quotients successifs isomorphes à* $(\boldsymbol{\alpha}_p)^r$ *et* $(\mathbb{G}_a)^s$ (*pris dans cet ordre*).

iv) $G_{\overline{k}}$ *ne contient pas de sous-groupe isomorphe à* $\boldsymbol{\mu}_p$.

v) $\mathfrak{g} = \mathrm{Lie}\, G$ *est unipotente* (3.6).

vi) $\mathfrak{g}$ *est nilpotente, et la partie réductive du centre de* $\mathfrak{g}$ (4.2.2) *est triviale.* **565**

vi bis) $\mathfrak{g}$ *est nilpotente, et tout sous-groupe de type multiplicatif de la composante neutre du centre de* G *est nul.*

vi ter) G *est nilpotent, et tout sous-groupe de type multiplicatif de la composante neutre du centre de* G *est nul.*

Démonstration. Il est clair que iii) ⇒ ii) ⇒ i). Pour établir i) ⇒ iii), nous aurons besoin du lemme suivant :

(*) i.e. le plus entier tel que $F^h = \mathrm{id}_G$, cf. App. II 1.

Lemme 4.3.2. — *Soient k un corps de caractéristique $p > 0$, $n \in \mathbb{N}$, k' une extension radicielle de k telle que $(k')^{p^n}$ soit contenu dans k ; pour tout k-préschéma* X (*resp. tout k'-préschéma* X′) *notons* $\mathrm{X}^{(p^n)}$ (*resp.* X'_{φ}) *le k-préschéma déduit de* X (*resp.* X′) *par le changement de base :*

$$\mathrm{F}^n : k \longrightarrow k, \quad x \mapsto x^{p^n}, \qquad (\textit{resp.} \quad \varphi : k' \longrightarrow k, \quad x' \mapsto x'^{p^n}).$$

Alors, pour tout k-préschéma X*, il existe un isomorphisme fonctoriel :*

$$(\mathrm{X}_{k'})_{\varphi} \xrightarrow{\sim} \mathrm{X}^{(p^n)}.$$

Par suite, si X *et* Y *sont deux k-préschémas tels qu'il existe un k'-isomorphisme $u' : \mathrm{X}_{k'} \xrightarrow{\sim} \mathrm{Y}_{k'}$, alors il existe un k-isomorphisme $v : \mathrm{X}^{(p^n)} \xrightarrow{\sim} \mathrm{Y}^{(p^n)}$. Si de plus* X *et* Y *sont munis de structures de k-préschémas en groupes et si u' est un k'-homomorphisme, alors v est un k-homomorphisme.*

566 Le lemme résulte simplement de la transitivité des changements de base et du fait que le morphisme composé : $k \to k' \xrightarrow{\varphi} k$ est égal à F^n.

Suite de la démonstration de 4.3.1.

i) ⇒ iii). Procédons par récurrence sur dim G. Si dim G = 0, comme G est connexe, il est radiciel et on applique 3.9 i). Si $\dim \mathrm{G} > 0$, il existe un entier $m \geqslant 0$ tel que le quotient $\mathrm{G}/_{\mathrm{F}^m}\mathrm{G}$ soit un groupe lisse (App. II 3.1), évidemment connexe et non nul. Appliquant 4.1.1 i) ⇒ iii) à ce dernier, on voit qu'il existe un sous-groupe algébrique G′ de G qui est caractéristique et connexe et tel que le quotient $\mathrm{G}'' = \mathrm{G}/\mathrm{G}'$ soit une forme de $\mathbb{G}_a^r$ ($r > 0$). D'après 4.1.5, si K est une clôture parfaite de k, on a $\mathrm{G}''_{\mathrm{K}} \xrightarrow{\sim} (\mathbb{G}_{a,\,\mathrm{K}})^r$. Comme G″ est de type fini sur k, il existe une extension radicielle finie k' de k telle que $\mathrm{G}''_{k'} \xrightarrow{\sim} (\mathbb{G}_{a,\,k'})^r$ (Exp. VI_{B} § 10). Soit $n > 0$ tel que $(k')^{p^n} \subset k$. Gardant les notations de 4.3.2, on en déduit qu'il existe un k-isomorphisme de groupes algébriques :

$$(\mathbb{G}_{a,\,k})^r = (\mathbb{G}_{a,\,k'})^r_{\varphi} \xrightarrow{\sim} (\mathbb{G}'')^{(p^n)}.$$

Considérons alors l'homomorphisme de Frobenius relatif à G″ (Exp. $\mathrm{VII}_{\mathrm{A}}$ § 4)

$$\mathrm{F}^n : \mathrm{G}'' \longrightarrow (\mathrm{G}'')^{(p^n)}.$$

Comme G″ (donc aussi $(\mathrm{G}'')^{(p^n)}$) est lisse sur k, et que F^n est radiciel, F^n est un épimorphisme pour la topologie fpqc, de sorte que $(\mathrm{G}'')^{(p^n)}$ s'identifie à $\mathrm{G}''/_{\mathrm{F}^n}(\mathrm{G}'')$. Finalement nous avons montré que $\mathrm{G}''/_{\mathrm{F}^n}(\mathrm{G}'')$ était isomorphe, comme groupe al-
567 gébrique, à $(\mathbb{G}_a)^r$. L'image réciproque G'_n de $_{\mathrm{F}^n}(\mathrm{G}'')$ dans G est un sous-groupe de G, connexe, caractéristique, de dimension strictement inférieure à celle de G, auquel nous pouvons appliquer l'hypothèse de récurrence.

i) ⇒ iv) d'après 2.4 i).

iv) ⇒ i). Considérons G comme extension d'un groupe lisse et connexe G″ par un groupe radiciel G′ (App. II 3.1). Le groupe G′ est unipotent (4.2.1 iv) ⇔ i)). Il suffit de voir que G″ est unipotent et pour cela il suffit de montrer que $\mathrm{G}''_{\overline{k}}$ ne contient pas de sous-groupe isomorphe à $\boldsymbol{\mu}_p$ (4.1.1 i) ⇔ iv)). Or si $\mathrm{G}''_{\overline{k}}$ contenait un sous-groupe $\boldsymbol{\mu}_p$, celui-ci se relèverait dans $\mathrm{G}_{\overline{k}}$, d'après le résultat (5.1) déjà utilisé démontré dans § 5, d'où une contradiction avec iv).

i) ⇒ v) d'après 3.7.

v) ⇒ vi). En effet comme $(\operatorname{ad} X)^{p^r} = \operatorname{ad}\left(X^{(p^r)}\right)$ (VII_A 5.2), $\operatorname{ad} X$ est nilpotent si $\mathfrak{g}$ est unipotente, donc $\mathfrak{g}$ est nilpotente d'après le *théorème d'Engel* (Bourbaki, Groupes et algèbres de Lie chap. I § 4). D'autre part, si $\mathfrak{g}$ est unipotente, il en est évidemment de même de son centre, dont la partie réductive est alors triviale (4.2.2).

vi) ⇒ iv). En effet, si $G_{\overline{k}}$ contient un sous-groupe isomorphe à $\boldsymbol{\mu}_p$, il existe un élément $X \neq 0$ de son algèbre de Lie tel que $X^{(p)} = X$ (App. II 2.1), donc $X^{(p^r)} = X$ pour tout $r > 0$. Comme $\operatorname{ad} X$ est nilpotent puisque $\mathfrak{g}$ est nilpotente et que $(\operatorname{ad} X)^{p^r} = \operatorname{ad} X^{(p^r)}$, nécessairement $\operatorname{ad} X = 0$, donc X appartient à la partie réductive du centre $\mathfrak{g}_{\overline{k}}$, d'où une contradiction avec vi).

i) ⇒ vi ter) résulte de 2.4 i) et de 3.5 i) ⇒ iii).

vi ter) ⇒ vi bis). En effet, si G est nilpotent, il en est de même de son sous-groupe **568**
${}_{\mathrm{F}}G$. Il résulte d'autre part de App. II 2.2 que ${}_{\mathrm{F}}G$ est nilpotent si et seulement si $\operatorname{Lie}{}_{\mathrm{F}}G = \operatorname{Lie} G$ (Exp. VII_A) est nilpotente.

vi bis) ⇒ vi). Soit Z la composante neutre du centre de G et soit $\mathfrak{r}$ la composante réductive du centre de $\mathfrak{g}$. Nous devons montrer que $\mathfrak{r} = 0$. Or il est immédiat que $\mathfrak{r}$ est une sous-p-algèbre de Lie caractéristique de $\mathfrak{g} = \operatorname{Lie}{}_{\mathrm{F}}G$ (c.-à-d. stable par le foncteur $\underline{\mathrm{Aut}}_{p\text{-Lie}}(\mathfrak{g})$) ; donc $\mathfrak{r}$ est l'algèbre de Lie d'un sous-groupe radiciel caractéristique R de ${}_{\mathrm{F}}G$ (App. II 2.2). D'autre part, il résulte de la dernière assertion contenue dans 4.2.2 et de App. II 2.1, que R est une forme de $(\boldsymbol{\mu}_p)^r$. Le groupe R étant caractéristique dans ${}_{\mathrm{F}}G$ qui est lui-même un sous-groupe caractéristique de G (App. II 1), R est a fortiori invariant dans G, donc est central, G étant connexe (Exp. IX 5.5). Donc par l'hypothèse vi bis) R est nul, et il en est donc de même de $\mathfrak{r}$.

4.4. Groupes étales. — La proposition suivante est une conséquence facile des théorèmes de Sylow et de la structure des q-groupes finis (cf. J.-P. Serre, *Corps locaux*, chap. IX § 1).

Proposition 4.4.1. — *Soient* G *un groupe algébrique fini étale défini sur un corps k algébriquement clos. Alors pour que* G *soit unipotent, il faut et il suffit que pour tout nombre premier q distinct de la caractéristique p de k,* G *ne contienne pas de sous-groupe isomorphe à $\boldsymbol{\mu}_q$.*

4.5. Variétés abéliennes. — Soit G une variété abélienne définie sur un corps k **569**
algébriquement clos. Alors les conditions suivantes sont équivalentes :

i) G est unipotent.
ii) $G = 0$.
iii) Il existe un entier n, premier à la caractéristique p de k, tel que G ne contienne pas de sous-groupe isomorphe à $\boldsymbol{\mu}_n$.

En effet, si G est une variété abélienne de dimension d, on sait (cf. S. Lang, *Abelian varieties*, chap. IV § 3. th. 6.) que le groupe ${}_nG(k)$ (n entier premier à p) est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^{2d}$, donc est isomorphe à $(\boldsymbol{\mu}_n)^{2d}$. D'où iii) ⇒ ii), et ii) ⇒ i) ⇒ iii) sont évidents.

4.6. Cas général. — Si G et H sont deux groupes algébriques définis sur un corps k algébriquement clos, nous noterons $\mathrm{P}(\mathrm{G},\mathrm{H})$ la propriété : « il n'existe pas de sous-groupe algébrique de G isomorphe à H ». On obtient alors les caractérisations suivantes des groupes unipotents :

Théorème 4.6.1. — *Soit* G *un groupe algébrique défini sur un corps k algébriquement clos de caractéristique p. Alors :*

i) *Si* G *est lisse, affine et connexe :*

G *est unipotent* $\iff \exists\, n>1$ *tel que* $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ *soit vraie* $\iff \mathrm{P}(\mathrm{G},\mathbb{G}_m)$*est vraie.*

ii) *Si* G *est lisse et connexe :*

G *est unipotent* $\iff \exists\, n$ *premier à p tel que* $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ *soit vraie.*

570 iii) *Si* G *est lisse :*

G *est unipotent* $\iff$ *pour tout nombre premier $n\neq p$,* $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$*est vraie.*

iv) G *est affine connexe et $p>0$:* G *unipotent* $\iff \mathrm{P}(\mathrm{G},\boldsymbol{\mu}_p)$ *est vraie.*

v) G *est connexe et $p>0$:*

G *unipotent* $\iff \exists\, n$ *premier à p tel que* $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ *soit vraie et* $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_p)$ *est vraie.*

vi) G *groupe algébrique quelconque :*

G *est unipotent* $\iff$ *pour tout nombre premier n,* $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ *est vraie.*

Démonstration. i) résulte de 4.1.1, et iv) de 4.3.1. Nous allons prouver vi) ; ii), iii), v) se démontrent de façon analogue et sont laissées au soin du lecteur.

Soit donc G un groupe algébrique. Si G est unipotent, $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ est vraie pour tout $n>1$ (2.4 i)). Réciproquement, supposons $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ vraie pour tout nombre premier n et montrons que G est unipotent. Soit G^0 la composante neutre de G. Si G^0 est lisse, il résulte d'un théorème classique de Chevalley (*) que G^0 est extension d'une variété abélienne A par un groupe affine, connexe, lisse, L. Si G n'est pas lisse, ce qui suppose $p>0$ (Exp. $\mathrm{VI_B}$ 1.6.1), il existe un entier $n>0$ tel que $\mathrm{G}''=\mathrm{G}^0/_{\mathrm{F}^n}(\mathrm{G})$ soit lisse (App. II 3.1). Donc G'' est extension d'une variété abélienne A par un groupe linéaire lisse et connexe L''. Notons L l'image réciproque de L'' dans G^0, qui est encore
571 affine et connexe, puisque ${}_{\mathrm{F}^n}(\mathrm{G})$ est radiciel. Dans tous les cas, G possède donc une suite de composition :

$$0\subset \mathrm{L}\subset \mathrm{G}^0\subset \mathrm{G}$$

telle que L soit affine et connexe, $\mathrm{G}^0/\mathrm{L}=\mathrm{A}$ soit une variété abélienne, et G/G^0 un groupe étale.

Si $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$ est vraie, a fortiori $\mathrm{P}(\mathrm{L},\boldsymbol{\mu}_n)$ est vraie, donc L est unipotent (4.1.1 et 4.3.1). Si A n'est pas nul, il existe un nombre premier n, et un sous-groupe de A isomorphe à $\boldsymbol{\mu}_n$ (4.5) ; d'après 5.1 ci-après, ce sous-groupe se relève dans G, ce qui contredit l'hypothèse $\mathrm{P}(\mathrm{G},\boldsymbol{\mu}_n)$; donc $\mathrm{A}=0$. Enfin si G/G^0 n'est pas unipotent, il existe un entier q et un sous-groupe de G/G^0 isomorphe à $\boldsymbol{\mu}_q$ (4.4.1). On en déduit

(*) Sém. Bourbaki n°145, 1956/57.

comme ci-dessus que $P(G, \boldsymbol{\mu}_q)$ n'est pas vraie ; donc G/G^0 est unipotent, et par suite il en est de même de G.

5. Extension d'un groupe de type multiplicatif par un groupe unipotent

572

5.1. Énoncé du théorème. —

Définition 5.1.0. — Soient k un corps, G un k-groupe algébrique. Suivant la terminologie introduite par Rosenlicht (*Questions of rationality for solvable algebraic groups over non perfect fields*, Annali di Math. 61 (1963)), nous dirons que G est « k-résoluble » s'il satisfait aux conditions équivalentes suivantes :

i) G possède une suite de composition à quotients successifs isomorphes à $\mathbb{G}_a$.

ii) G possède une suite de composition caractéristique (G_i), telle que les quotients successifs G_i/G_{i+1} soient commutatifs et possèdent une suite de composition à quotients successifs isomorphes à $\mathbb{G}_a$.

Le fait que i) $\Rightarrow$ ii) est prouvé dans *loc. cit.*. En fait, on peut prendre pour suite de composition (G_i), la suite de composition introduite dans la démonstration de 3.9 ii).

Théorème 5.1.1. — *Soient k un corps,* U *un k-groupe algébrique unipotent,* H *un k-groupe de type multiplicatif,* E *un k-groupe algébrique extension de* H *par* U*, de sorte que l'on a la suite exacte :*

$$1 \longrightarrow U \longrightarrow E \longrightarrow H \longrightarrow 1.$$

Alors : 573

i) *L'extension* E *est triviale dans chacun des cas suivants :* 574

a) *k est algébriquement clos.*

b) *k est parfait et l'un des groupes* U *ou* H *est connexe.*

c) U *est k-résoluble.*

d) U *est lisse et* H *est connexe.*

ii) *Si* H' *et* H'' *sont deux relèvements de* H *dans* E*, alors* H' *et* H'' *sont conjugués par un élément de* $U(k)$ *dans chacun des cas suivants :*

a) *k est algébriquement clos et* H *est lisse.*

b) *k est algébriquement clos et* U *est lisse.*

(Nous signalons en cours de démonstration, d'autres cas où la conclusion de ii) est vraie sans supposer k algébriquement clos).

Si U est un groupe algébrique (resp. un groupe algébrique commutatif) défini sur un corps k, nous notons $H^1(k, U)$ (resp. $H^i(k, U)$, $i \geqslant 0$) l'ensemble pointé (resp. le $i^{\text{ième}}$ groupe) de cohomologie galoisienne de k à valeurs dans U (cf. J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes Maths. n°5, Springer).

Si S est un préschéma, H un S-préschéma en groupes commutatifs, G un S-préschéma en groupes qui opère sur H, nous notons $H^i(G, H)$ [7] le $i^{\text{ième}}$ groupe de cohomologie de Hochschild de G à valeurs dans H (App. I 1).

Pour prouver 5.1.1, nous procèderons en plusieurs étapes.

575

5.2. Démonstration de 5.1.1 i) et ii) dans le cas U lisse et H étale. —

Lemme 5.2.1. — *Avec les notations de* 5.1.1*, si* H *est étale, le morphisme canonique* $E \to H$ *possède une section* $s : H \to E$*, définie sur* k*, dans les cas suivants :*

a) k *est algébriquement clos.*
b) k *est parfait et* U *est lisse et connexe.*
c) U *est « k-résoluble ».*

a) résulte simplement du fait que $E(k) \to H(k)$ est surjectif. On a b) $\Rightarrow$ c) d'après 4.1.2. b) et 2.3 (bis). Il suffit donc de traiter le cas c). Or soit x un point de H, x est donc une partie à la fois ouverte et fermée de H, et le sous-schéma induit est isomorphe à $\operatorname{Spec} K$, où K est une extension finie séparable de k. Soit X l'image réciproque dans E du schéma x. Le K-schéma X est un K-espace principal homogène sous le groupe U_K. Mais U_K possède une suite de composition à quotients successifs isomorphes à $(\mathbb{G}_a)_K$, donc $H^1(K, U_K) = 0$ (J.-P. Serre, *Cohomologie Galoisienne*, chap. III, prop. 6) et par suite X est trivial, donc possède un point rationnel sur K. On obtient ainsi une k-section de $E \to H$ au-dessus de x, pour tout point x de H, d'où l'existence d'une section $H \to E$.

Lemme 5.2.3. — [8] *Avec les notations de* 5.1.1*, supposons* H *étale. Alors :*

i) *L'extension* E *est triviale dans chacun des cas suivants :*
   a) U *est commutatif et* $E \to H$ *possède une section.*
576 b) k *est algébriquement clos.*
   c) k *est parfait et* U *est connexe.*
   d) U *est « k-résoluble ».*

De plus, dans chacun des cas ci-dessus, deux relèvements H' *et* H'' *de* H *dans* E *sont conjugués par un élément de* $U(k)$.

ii) *Soit* R *le k-foncteur :* $(\mathbf{Sch}/k)^\circ \to \mathbf{Ens}$ *tel que, pour tout k-préschéma* S, R(S) *soit l'ensemble des relèvements de* H_S *dans* E_S*. Alors si* U *est commutatif,* R *est représentable par un k-schéma affine, non vide. Le groupe* U *opère par automorphismes intérieurs sur* R*, et cette opération fait de* R *un espace homogène sous* U (*pour la topologie* fpqc (cf. Exp. IV)).

Démonstration de i). Nous allons ramener les cas b), c) et d) au cas a).

Cas b) Comme U possède une suite de composition caractéristique, à quotients successifs commutatifs (3.5 i) $\Leftrightarrow$ iv)), on se ramène immédiatement au cas où U est

[7] N.D.E. : on a remplacé H_0^i par H^i, pour se mettre en accord avec les notations de App. I et de Exp. I.
[8] N.D.E. : il n'y a pas de numéro 5.2.2.

commutatif. De plus $E \to H$ possède une section d'après 5.2.1 a) et nous sommes ramenés au cas a).

Cas d) On procède de même en utilisant 5.1.0 ii) et 5.2.1 c).

Cas c) Soit $E_{réd}$ le sous-groupe réduit associé à E. Comme H est lisse, $E_{réd}$ est extension de H par $U' = U \cap E_{réd}$, et on peut remplacer E par $E_{réd}$. Mais U, donc aussi U′, est connexe, et il est clair que U′ est la composante neutre de $E_{réd}$, donc est lisse. Mais alors U′ est lisse et connexe, k est parfait, donc U′ est k-résoluble (4.1.4 b)) et nous sommes ramenés au cas d).

Les réductions précédentes montrent que dans les cas b), c) et d) on peut supposer **577** que U possède une suite de composition (U_i), caractéristique, telle que U_i/U_{i+1} soit commutatif et telle que les applications $U_i(k) \to (U_i/U_{i+1})(k)$ soient surjectives (dans les cas c) et d), ce dernier point provient de $H^1(k, \mathbb{G}_a) = 0$). Un dévissage immédiat montre alors qu'il suffit de prouver la conjugaison de deux relèvements H′ et H″ dans E lorsque U est commutatif. Bref, il suffit de prouver i) a). Dans ce cas, la trivialité de l'extension E est assurée si $H^2(H, U) = 0$ (App. I 3.1) et la conjugaison de H′ et H″ l'est si $H^1(H, U) = 0$. Or nous avons le lemme suivant :

Lemme 5.2.4. — *Soient* S *un préschéma,* U *un* S*-préschéma en groupes commutatif,* H *un* S*-préschéma en groupes, étale, fini, de rang* n*, qui opère sur* U*. Alors les groupes* $H^i(H, U)$ $(i > 0)$ *sont annulés par* n *dans les deux cas suivants :*

a) H *est un* S*-groupe constant* (Exp. I 4.1).

b) S *est le spectre d'un corps.*

Démonstration de a). Le groupe H est par hypothèse le groupe constant associé à un groupe ordinaire {H} d'ordre n. Il est clair[(9)] alors que $H^i(H, U)$ est isomorphe au $i^{\text{ème}}$ groupe de cohomologie $H^i(\{H\}, U(S))$ du groupe {H}, à valeurs dans le groupe ordinaire U(S), et il est classique que ces groupes sont annulés par n (J.-P. Serre, *Corps locaux*, Chap. VIII, prop. 4 cor. 1).

Démonstration de b). Soit $x \in H^i(H, U)$ $(i > 0)$ que l'on représente par un i-cocycle **578** $f : H^{(i)} \to U$ (où $H^{(i)}$ désigne le produit, sur k, de i copies de H). Si K est une extension finie galoisienne de k qui décompose H, il résulte de a) que nf_K est un cobord. Plus précisément, un calcul facile montre que si on définit le K-morphisme $F_K : H_K^{(i-1)} \to U_K$ par la formule :

$$F_K(h_1, \ldots, h_{i-1}) = \sum_{h \in H(K)} f_K(h_1, \ldots, h_{i-1}, h),$$

on a au signe près :

$$d(F_K) = nf_K \qquad (d \text{ opérateur cobord}).$$

Or un argument galoisien immédiat, montre que F_K provient d'un k-morphisme $F : H^{(i-1)} \to U$, et par suite, on a $d(F) = nf$.

(9) N.D.E. : Il s'agit de la proposition III.6.4.2 du livre de M. Demazure et P. Gabriel, *Groupes algébriques* I, Masson & North-Holland (1970).

Corollaire 5.2.4 bis. — *Avec les notations de* 5.2.4*, supposons de plus que* U *est plat et de présentation finie sur* S*, à fibres unipotentes, et que* n *est premier aux caractéristiques résiduelles de* S*. Alors, dans les cas* a) *et* b) *ci-dessus, on a* $\mathrm{H}^i(\mathrm{H}, \mathrm{U}) = 0$ *pour* $i > 0$.

Il suffit de montrer que l'élévation à la puissance n dans U est un isomorphisme, car cela entraînera que la multiplication par n dans $\mathrm{H}^i(\mathrm{H}, \mathrm{U})$ sera à la fois un isomorphisme et le morphisme nul, donc $\mathrm{H}^i(\mathrm{H}, \mathrm{U}) = 0$. Or, avec les hypothèses faites sur U, il suffit de vérifier que l'élévation à la puissance $n^{\text{ième}}$ est un isomorphisme sur les fibres de U (EGA IV 17.9.5) ce qui nous ramène au cas où S est le spectre d'un corps k de caractéristique p. Comme $(n, p) = 1$, l'élévation à la puissance $n^{\text{ième}}$ dans U est un morphisme étale (Exp. VII), et c'est un monomorphisme (2.4 i)), donc une immersion
579 ouverte (EGA IV 17.9.1). Cela prouve déjà que la restriction à la composante neutre U^0 est un isomorphisme ; comme U/U^0 est un p-groupe fini, on a terminé.

Ceci achève de prouver 5.2.3 i) a), puisque H, étant un groupe de type multiplicatif étale, est d'ordre premier à p.

Démonstration de 5.2.3 ii). Il est clair que R est un faisceau pour la topologie fpqc. Par ailleurs, compte tenu de la descente des schémas affines, les assertions de 5.2.3 ii) sont locales pour la topologie fpqc. Nous pouvons donc supposer k algébriquement clos. Le groupe H est alors décomposé et l'extension E est triviale (i b)) ; soit H' un relèvement de H dans E. Pour tout k-préschéma S, et tout relèvement H'' de H_S dans E_S, H'_S et H'' sont conjugués par un élément de U(S) puisque $\mathrm{H}^1(\mathrm{H}_\mathrm{S}, \mathrm{U}_\mathrm{S}) = 0$ (5.2.4 bis). Soit alors $\mathrm{U}^{\mathrm{H}'}$ le faisceau des invariants de U sous H', qui est représentable par un sous-groupe algébrique de U (Exp. VIII 6.5 d)). Il résulte des remarques précédentes que le k-morphisme :

$$\mathrm{U} \longrightarrow \mathrm{R}, \qquad u \mapsto \mathrm{int}(u)\mathrm{H}' \quad (u \in \mathrm{U}(\mathrm{S}))$$

définit un k-isomorphisme $\mathrm{U}/\mathrm{U}^{\mathrm{H}'} \xrightarrow{\sim} \mathrm{R}$. Ceci prouve la représentabilité de R et le fait que R est affine (2.1).

Remarque 5.2.5. — On peut montrer que les assertions de 5.2.3 ii) sont encore vraies lorsque U n'est pas commutatif, mais nous n'en aurons pas besoin pour prouver 5.1.1.

580

5.3. Étude du cas H lisse. —

Proposition 5.3.1. — *Les assertions contenues dans* 5.2.3 i) *restent vraies lorsque l'on remplace l'hypothèse «* H *étale » par «* H *lisse ».*

Procédant comme dans la démonstration de 5.2.3 i), on se ramène au cas où de plus U est commutatif.

Soit $\mathbb{N}'$ l'ensemble des entiers > 0, premiers à p, ordonné par la relation de divisibilité. Pour tout $n \in \mathbb{N}'$, ${}_n\mathrm{H}'$ est un groupe étale et la famille des ${}_n\mathrm{H}'$ ($n \in \mathbb{N}'$) est schématiquement dense dans H, puisque H est lisse (Exp. IX 4.10). Notons E_n l'image réciproque de ${}_n\mathrm{H}$ dans E, de sorte que E_n est une extension de ${}_n\mathrm{H}$ par U, enfin soit R_n le k-foncteur des relèvements de ${}_n\mathrm{H}$ dans E_n (cf. 5.2.3 ii)). Si n divise m, il est clair que l'on a un k-morphisme naturel $\mathrm{R}_m \to \mathrm{R}_n$, de sorte que les R_n forment un système projectif de k-foncteurs. Comme R_n est représentable par un k-schéma affine non

vide (5.2.3 ii)), et qu'une limite inductive filtrante d'anneaux non nuls est non nulle, le foncteur $R = \varprojlim R_n$ est représentable par un k-schéma affine non vide (EGA IV 8 et 1.9.1). Il existe donc une extension K de k et un point $u \in R(K)$. L'image u_n de u dans $R_n(K)$ correspond à un relèvement H'_n de $({}_nH)_K$ dans $(E_n)_K$. Par construction, $H'_n = {}_n(H'_m)$ si n divise m. Posons $U_n = (U_K)^{H'_n}$. Le choix de H'_n permet d'identifier $(R_n)_K$ à U_K/U_n. Mais la famille des H'_n est filtrante croissante, donc la famille des U_n est filtrante décroissante et par suite est stationnaire pour n assez grand (U_K est noethérien). Il en résulte que la famille des $(R_n)_K$ est stationnaire, et par suite il en **581**
est de même de la famille des R_n. Bref, on a $R_n = R$ pour n assez grand.

Avec les hypothèses faites, il résulte de 5.2.3 i) que $R_n(k)$ n'est pas vide. On peut donc trouver un système cohérent de relèvements H'_n de ${}_nH$ pour $n \in \mathbb{N}'$. Notons H' le plus petit sous-schéma fermé de E qui majore H'_n pour tout n (Exp. VI_B § 7). Le raisonnement fait dans Exp. XV 4.6 montre que H' est un groupe algébrique lisse, commutatif, dont la formation commute à l'extension du corps de base. Pour montrer que H' est un relèvement de H dans E, nous pouvons donc supposer k algébriquement clos. D'après BIBLE 4 th. 4, H' est alors le produit direct d'un groupe de type multiplicatif M (lisse) par un groupe unipotent V. Les groupes H'_n sont alors nécessairement contenus dans M (2.4) et vu la définition de H' cela entraîne $H' = M$. Donc H' est de type multiplicatif et par suite $H' \cap U = 0$. Le morphisme $H' \to H$ est donc un monomorphisme, par ailleurs il résulte du théorème de densité (Exp. IX 4.10) que c'est un épimorphisme, c'est donc bien un isomorphisme.

Soient maintenant H' et H'' deux relèvements de H dans E. Pour tout $n \in \mathbb{N}'$, notons $T_n = \underline{\mathrm{Transp}}({}_nH', {}_nH'')$ le transporteur de ${}_nH'$ dans ${}_nH''$, qui est représentable par un sous-schéma fermé de U (Exp. VIII 6.5 e)). Les T_n forment une famille filtrante décroissante de sous-schémas fermés de U, non vides d'après 5.2.3 i a). Soit T la valeur stationnaire. Sous les hypothèses de 5.2.3 i), $T_n(k)$ n'est pas vide. Il existe donc un élément u de $U(k)$ tel que ${}_nH'' = \mathrm{int}(u)({}_nH')$ pour tout $n \in N'$. Mais alors $H'' = \mathrm{int}(u)H'$ (Exp. IX 4.8 b). **582**

5.4. Étude du cas U radiciel. —

Proposition 5.4.1. — *Si k est un corps parfait de caractéristique $p > 0$, et si* U *est radiciel, l'extension* E *de* 5.1.1 *est triviale.*

Utilisant une suite de composition caractéristique de U, nous pouvons nous limiter au cas où U est égal à $(\boldsymbol{\alpha}_p)^r$ (3.9).

Il résulte de App. II 2.2 et 2.1 que l'on a des isomorphismes de k-foncteurs :

$$\underline{\mathrm{Aut}}_{k\text{-gr}}(\boldsymbol{\alpha}_p)^r \xrightarrow{\sim} \underline{\mathrm{Aut}}_{p\text{-Lie}}(\mathrm{Lie}(\boldsymbol{\alpha}_p)^r) \xrightarrow{\sim} \mathrm{GL}(\mathrm{Lie}(\boldsymbol{\alpha}_p)^r).$$

Considérons alors un k-espace vectoriel V de rang r, le k-schéma en groupes vectoriel W(V) (Exp. I 4.6), et identifions $(\boldsymbol{\alpha}_p)^r$ à ${}_FV$. Les remarques qui précèdent montrent alors que l'action de H sur ${}_FV$, définie par l'extension E, provient d'une représentation linéaire v de H dans V. Considérons alors la suite exacte :

$$(*) \qquad 0 \to {}_FV \to V \xrightarrow{F} V^{(p)} \to 0,$$

où F est le morphisme de Frobenius. Alors $(*)$ est une suite exacte de H-groupes, à condition de faire opérer H sur le facteur $V^{(p)}$ grâce à la représentation linéaire $H \xrightarrow{v} GL(V) \xrightarrow{F} GL(V^{(p)})$.

Comme le corps k est parfait, le morphisme $F : V \to V^{(p)}$ induit une application surjective $V(k) \to V^{(p)}(k)$. Il résulte alors de App. I 2.1 que la suite exacte $(*)$ définit
583 une suite exacte :

$$(**) \qquad H^1(H, V^{(p)}) \longrightarrow \mathrm{Ext}_{\mathrm{alg}}(H, {}_F V) \longrightarrow \mathrm{Ext}_{\mathrm{alg}}(H, V).$$

Montrons que $\mathrm{Ext}_{\mathrm{alg}}(H, V) = 0$. Soit donc E' un groupe algébrique extension de H par V :

$$1 \to V \to E' \xrightarrow{h} H \to 1.$$

Le schéma E' est un torseur de base H est de groupe $\mathbb{G}_a^r$, donc définit un élément de $H^1(H, \mathscr{O}_H^r)$ (au sens de la cohomologie des faisceaux cohérents). Comme H est affine, on a $H^1(H, \mathscr{O}_H^r) = 0$ (EGA III § 1). C'est dire que $E' \to H$ possède une section. Par suite, le groupe $\mathrm{Ext}_{\mathrm{alg}}(H, V)$ est isomorphe à $H^2(H, V)$ (App. I 3.1). Or $H^i(H, V) = H^i(H, W(V)) = 0$ pour $i > 0$ (Exp. IX 3.1). On conclut alors, par la suite exacte $(**)$, que $\mathrm{Ext}_{\mathrm{alg}}(H, {}_F V) = 0$, donc que E est une extension triviale.

5.5. Démonstration de 5.1.1 i). — Si k est de caractéristique 0, U est k-résoluble (4.1.3) et H est lisse ; le fait que E soit une extension triviale résulte donc de 5.3.1 et de 5.2.3 d). On prouve de même que deux relèvements de H, dans E, sont conjugués par un élément de $U(k)$.

Désormais, nous supposons donc que k est un corps de caractéristique $p > 0$.

Démonstration de i) b) : *Cas k parfait,* U *connexe.*

Nous allons nous ramener au cas où U est radiciel. Pour cela notons que k étant parfait, $H_{\text{réd}}$ est lisse ; soit E' son image réciproque dans E. Il résulte alors de 5.3.1 et
584 de 5.2.3 i) c) que l'extension :

$$1 \longrightarrow U \longrightarrow E' \longrightarrow H_{\text{réd}} \longrightarrow 1$$

est triviale. Soit H_1 un relèvement de $H_{\text{réd}}$ dans E. D'après App. II 3.1, il existe un entier $n > 0$ tel que $E^{(n)} = E/{}_{F^n}(E)$ soit lisse ; soit E'' le sous-groupe algébrique de E engendré par H_1 et ${}_{F^n}(E)$ (c.-à-d. l'image réciproque dans E de l'image de H_1 dans $E^{(n)}$). Notons H'' l'image de E'' dans H. Alors je dis que $H'' = H$. En effet, notons R l'image de ${}_{F^n}(E)$ dans H, de sorte que H'' est engendré par R et $H_{\text{réd}}$. Le groupe H/R est un quotient de $E^{(n)}$ donc est lisse ; par suite le morphisme canonique

$$H_{\text{réd}} \longrightarrow H/R$$

est un épimorphisme, donc H est engendré par R et $H_{\text{réd}}$, donc est égal à H''. On obtient ainsi une suite exacte :

$$(\dagger) \qquad 1 \longrightarrow U'' = U \cap E'' \longrightarrow E'' \longrightarrow H \longrightarrow 1.$$

Mais E'' a même espace sous-jacent que H_1 donc U'' est radiciel. Par ailleurs, il est clair qu'il suffit de prouver que l'extension $(\dagger)$ est triviale, ce qui résulte de 5.4.1.

Démonstration de i) b) : *Cas k parfait,* H *connexe.*

Le groupe U est extension d'un groupe étale par sa composante neutre U^0. Le cas U connexe venant d'être traité, il suffit d'examiner le cas U étale. On a alors le lemme plus précis :

Lemme 5.5.1. — *Avec les notations de* 5.1.1*, supposons de plus* U *étale. Alors :*

i) *Si* H *est connexe, il existe un unique relèvement de* H *dans* E*, à savoir la composante neutre* E^0 *de* E. **585**

ii) *Si* k *est algébriquement clos,* E *est triviale, et deux relèvements de* H *dans* E *sont conjugués par un élément de* $U(k)$.

i) La formation de la composante neutre commutant à l'extension du corps de base, nous pouvons nous limiter au cas k algébriquement clos. Si H est un tore, E est triviale (5.3.1 et 5.2.3 i b)), et il est clair que E^0 est l'unique relèvement de H. Ceci prouve déjà que dans le cas général, $E^0 \cap U$ est radiciel ; comme par ailleurs il est étale (U étant étale), il est nul. Le morphisme $E^0 \to H$ est donc un monomorphisme, plat (car E^0 est ouvert dans E) et surjectif (H est connexe), donc est un isomorphisme. Si maintenant H' est un autre relèvement de H, H' est connexe, donc contenu dans E^0 et par suite est égal à E^0.

ii) Soit H^0 la composante neutre de H. D'après i), E^0 est l'unique relèvement de H^0 dans E. Posons $E' = E/E^0$, $H' = H/H^0$, de sorte que l'on a l'extension :

$$1 \longrightarrow U \longrightarrow E' \longrightarrow H' \longrightarrow 1.$$

H' étant étale, cette extension est triviale (5.2.3 i b)). Si H'_1 est un relèvement de H' dans E', H_1 son image réciproque dans E, il est clair que H_1 relève H dans E. Si H_2 est un deuxième relèvement de H dans E, il contient E^0 ; d'après 5.2.3 i b), l'image de H_2 dans E' est conjuguée de H'_1 par un élément u de $U(k)$, d'où immédiatement $H_2 = \mathrm{int}(u)H_1$.

Remarque 5.5.2. — Sous les hypothèses de 5.5.1 i), il est facile de voir que E^0 centralise U. **586**

Démonstration de 5.1.1 i) a). Utilisant la suite de composition

$$1 \longrightarrow U^0 \longrightarrow U \longrightarrow U/U^0 \longrightarrow 1,$$

i) a) résulte de la conjonction de i) b) et de 5.5.1 ii).

Avant de prouver 5.1.1 c) et d), nous allons d'abord établir 5.1.1 ii).

Démonstration de 5.5.1 ii) a). Faute de disposer d'un énoncé général satisfaisant, nous allons décrire un certain nombre de cas où, lorsque H est lisse, deux relèvements de H dans E sont conjugués :

Proposition 5.6.1. — *Avec les notations de* 5.1.1*, supposons de plus* H lisse*, et soient* H' *et* H'' *deux relèvements de* H *dans* E. *Alors* H' *et* H'' *sont conjugués par un élément de* $U(k)$ *dans chacun des cas suivants :*

a) k *est algébriquement clos.*

b) U *est commutatif.*

c) k *est parfait et* U *est connexe.*

d) U *est k-résoluble.*

e) *Le centralisateur de* H′ *dans* U *est k-résoluble.*

f) *Le groupe de type multiplicatif* H *est trivialisé par une extension finie galoisienne* K *de k de degré premier à p.*

587 *Démonstration.* a), b), c), d) résultent de 5.3.1.

e) Soient Z le centralisateur de H′ dans U, T le transporteur de H′ dans H″. D'après a), T n'est pas vide, donc T est un espace principal homogène sous Z, et l'hypothèse faite sur Z entraîne qu'il est trivial.

f) Procédant comme dans 5.3.1, on voit qu'il suffit de considérer le cas H étale. Supposons d'abord H diagonalisable, défini par le groupe ordinaire M, d'ordre m premier à p. La donnée des deux relèvements H′ et H″ définit un 1-cocycle de M à valeurs dans $\mathrm{U}(k)$, c'est-à-dire une application h de M dans $\mathrm{U}(k)$ telle que $h(mn) = h(m)\,{}^m h(n)$ pour tout couple m, n d'éléments de M. Les groupes H′ et H″ sont conjugués par un élément de $\mathrm{U}(k)$ si et seulement si il existe $a \in \mathrm{U}(k)$ tel que

$$h(m) = a^{-1}\,({}^m a).$$

Or le groupe abstrait $\mathrm{U}(k)$ possède une suite de composition à quotients successifs commutatifs et annulés par une puissance de p (il est loisible de supposer $p > 0$ compte tenu de 5.6.1 c)). On en déduit immédiatement dans ce cas que h est un cobord.

Examinons maintenant le cas général. Notons encore Z le centralisateur de H′ dans U et T le transporteur de H′ dans H″ qui est un torseur sous Z. Par hypothèse, il existe une extension galoisienne finie K de k, de groupe de Galois G, d'ordre premier à p, qui trivialise H. D'après l'étude faite plus haut, H'_{K} et $\mathrm{H}''_{\mathrm{K}}$ sont conjugués par
588 un élément de U(K), donc T_{K} est trivial. Par suite T est défini par un élément de $\mathrm{H}^1(\mathrm{G}, \mathrm{Z})$. Pour les mêmes raisons que plus haut, l'hypothèse faite sur G entraîne que $\mathrm{H}^1(\mathrm{G}, \mathrm{Z}) = e$, donc T est trivial.

5.7. Démonstration de 5.1.1 ii) b). —

Lemme 5.7.1. — *Soient* S *un préschéma,* G *un* S*-préschéma en groupes, séparé et* lisse *sur* S*,* H *un* S*-groupe de type multiplicatif qui opère sur* G*. Alors le* S*-foncteur* $\mathrm{Z} = \mathrm{G}^{\mathrm{H}}$ *des invariants de* G *sous* H *est représentable par un sous-*S*-préschéma en groupes de* G*, fermé et* lisse *sur* S*.*

Le fait que G^{H} soit représentable par un sous-préschéma en groupes fermé de G résulte de Exp. VIII 6.5 d). Considérons alors le produit semi-direct $\mathrm{K} = \mathrm{G} \times_{\mathrm{S}} \mathrm{H}$. Le centralisateur de H dans K est alors égal à $\mathrm{Z} \times_{\mathrm{S}} \mathrm{H}$. Pour prouver que Z est lisse, nous devons vérifier que si S est affine, si S_0 est un sous-schéma fermé de S défini par un idéal de carré nul, et si u_0 est un élément de $\mathrm{Z}(\mathrm{S}_0)$, alors il existe un élément u de Z(S) qui relève u_0. Or comme G est lisse sur S, il existe un élément u de G(S) qui relève u_0. Soit i l'immersion canonique de H dans K et considérons les deux S-morphismes de groupes

$$\mathrm{H} \rightrightarrows \mathrm{K}, \qquad i \quad \text{et} \quad \mathrm{int}(u)i = j.$$

Comme u_0 appartient à $\mathrm{Z}(\mathrm{S}_0)$, on a $i_{\mathrm{S}_0} = j_{\mathrm{S}_0}$. D'après Exp. IX 3.2, il existe $v \in \mathrm{K}(\mathrm{S})$
589 qui relève la section unité de $\mathrm{K}(\mathrm{S}_0)$, et qui est tel que

$$i = \mathrm{int}(v)j = \mathrm{int}(vu)i.$$

Donc $vu = (u', v')$ appartient à $(\mathrm{Z} \times_{\mathrm{S}} \mathrm{H})(\mathrm{S})$. Donc u' appartient à $\mathrm{Z}(\mathrm{S})$ et relève u_0.

Lemme 5.7.2. — *Soient k un corps,* H *un k-groupe algébrique et soit* P(H) *la propriété suivante :*

> *« pour tout k-groupe lisse et unipotent* U*, et pour toute extension* E *de* H *par* U*, deux relèvements de* H *dans* E *sont conjugués par un élément de* $\mathrm{U}(k)$ *».*

Alors si H *est un groupe algébrique extension d'un groupe de type multiplicatif* H′′ *par un groupe de type multiplicatif* H′ *et si* P(H′) *et* P(H′′) *sont vraies,* P(H) *est vraie.*

En effet, soit U un k-groupe unipotent lisse, E une extension de H par U, H_1 et H_2 deux relèvements de H dans E, H'_1 et H'_2 les relèvements correspondants de H′. Comme P(H′) est vraie, il existe $u \in \mathrm{U}(k)$ tel que $\mathrm{H}'_2 = \mathrm{int}(u)\mathrm{H}'_1$. Quitte à remplacer H_1 par $\mathrm{int}(u)\mathrm{H}_1$, nous pouvons supposer $\mathrm{H}'_1 = \mathrm{H}'_2$, que nous nous permettons de noter simplement H′. Soit $\mathrm{E}' = \underline{\mathrm{Centr}}_{\mathrm{E}}\,\mathrm{H}'$, qui est égal à

$$\mathrm{U}^{\mathrm{H}'} \cdot \mathrm{H}_1 = \mathrm{U}^{\mathrm{H}'} \cdot \mathrm{H}_2\ .$$

D'après 5.6.1, $\mathrm{U}^{\mathrm{H}'} = \mathrm{U}'$ est lisse. Considérons alors l'extension

$$1 \longrightarrow \mathrm{U}' \longrightarrow \mathrm{E}' \longrightarrow \mathrm{H} \longrightarrow 1.$$

Par construction H′ est central dans E′, donc invariant. Par passage au quotient, on obtient la suite exacte :

$$1 \longrightarrow \mathrm{U}' \longrightarrow \mathrm{E}'' \longrightarrow \mathrm{H}'' \longrightarrow 1.$$

Comme U′ est lisse, et comme P(H′′) est vraie, les deux images de H_1 et de H_2 dans E′′ sont conjuguées par un élément u de $\mathrm{U}'(k)$, mais alors $\mathrm{H}_1 = \mathrm{int}(u)\mathrm{H}_2$. **590**

Pour démontrer 5.1.1 ii) b) notons alors que, k étant algébriquement clos, H possède une suite de composition dont les quotients successifs sont lisses ou isomorphes à $\boldsymbol{\mu}_p$ lorsque $p > 0$. Par utilisation répétée de 5.7.2, nous sommes ramenés au cas où H est lisse ou égal à $\boldsymbol{\mu}_p$. Dans le premier cas, il suffit d'appliquer 5.1.1 ii) a). Reste le cas $\mathrm{H} = \boldsymbol{\mu}_p$. Comme U est lisse, U possède une suite de composition caractéristique à quotients successifs étales ou isomorphes à $(\mathbb{G}_a)^r$ (3.9). Si U est étale, on applique 5.5.1. Il reste finalement le cas $\mathrm{H} = \boldsymbol{\mu}_p$, $\mathrm{U} = \mathbb{G}_a^r$.

Nous devons montrer que $\mathrm{H}^1(\boldsymbol{\mu}_p, \mathrm{U}) = 0$. La méthode utilisée dans 5.4.1 ne s'applique plus ici, car $\boldsymbol{\mu}_p$ n'opère pas en général linéairement sur $(\mathbb{G}_a)^r$. Fixons les notations : H′ désigne un relèvement de H dans E, $\mathfrak{e} = \mathrm{Lie}\,\mathrm{E}$, $\mathfrak{u} = \mathrm{Lie}\,\mathrm{U}$, $\mathfrak{h} = \mathrm{Lie}\,\mathrm{H}$, $\mathfrak{h}' = \mathrm{Lie}\,\mathrm{H}'$. Soit X un élément non nul de $\mathfrak{h}$ tel que $\mathrm{X}^{(p)} = \mathrm{X}$ (App. II 3.1) et soit X′ son relèvement dans $\mathfrak{h}'$.

Comme $\boldsymbol{\mu}_p$ est un groupe radiciel de hauteur 1, il y a correspondance biunivoque entre l'ensemble des relèvements de H dans E, et l'ensemble A des $\mathrm{Y} \in \mathfrak{e}$, tels que $\mathrm{Y}^{(p)} = \mathrm{Y}$, qui se projettent sur X (App. II 2.2). De même si $\mathrm{Y} \in \mathrm{A}$ correspond au relèvement H′′ de H dans E, et si $u \in \mathrm{U}(k)$, alors $\mathrm{int}(u)\mathrm{H}' = \mathrm{H}''$ si et seulement si $\mathrm{Ad}(u)\mathrm{X} = \mathrm{Y}$. Soit donc B le sous-ensemble des $\mathrm{Y} \in \mathfrak{e}$, de la forme $\mathrm{Ad}(u)\mathrm{X}$, où $u \in \mathrm{U}(k)$. On a évidemment $\mathrm{B} \subset \mathrm{A}$, et tout revient à montrer que $\mathrm{A} = \mathrm{B}$ si k est **591**

algébriquement clos.

a) Étude de A. Comme $\mathfrak{u}$ est commutative et normalisée par $\mathfrak{h}$, la formule de Jacobson (Exp. VII$_A$ 5.2) donne simplement ici, pour $u \in \mathfrak{u}$:

$$(X' + u)^{(p)} = X'^{(p)} + u^{(p)} + (\operatorname{ad} X')^{p-1}(u) = X' + (\operatorname{ad} X')^{p-1}(u),$$

de sorte que $X' + u \in A \Leftrightarrow u = (\operatorname{ad} X')^{p-1}(u)$.

Or soit $\mathfrak{u} = \coprod_{n \in \mathbb{Z}/p\mathbb{Z}} \mathfrak{u}_n$ la décomposition canonique de $\mathfrak{u}$ sous l'action de H', que l'on peut encore écrire :

$$\mathfrak{u} = \mathfrak{u}_0 \oplus \coprod_{n \in (\mathbb{Z}/p\mathbb{Z})^\times} \mathfrak{u}_n.$$

Si $u \in \mathfrak{u}_0$, on a $\operatorname{ad} X'(u) = 0$. Si $u \in \mathfrak{u}_n$ ($n \in (\mathbb{Z}/p\mathbb{Z})^\times$), on a $(\operatorname{ad} X')^{p-1}(u) = u$. Finalement, $Y = X' + u$ est un élément de A si et seulement si $u \in \coprod_{n \in (\mathbb{Z}/p\mathbb{Z})^\times} \mathfrak{u}_n$. Retenons que A est l'ensemble des points rationnels sur k d'un sous-schéma irréductible de $W(\mathfrak{e})$, de dimension égale à $\operatorname{rg} \mathfrak{u} - \operatorname{rg} \mathfrak{u}_0 = \operatorname{rg} \mathfrak{u} - \operatorname{rg} \operatorname{Centr}_{\mathfrak{u}}(X')$.

b) Étude de B. Nous aurons besoin du lemme suivant :

Lemme 5.7.3. — (Rosenlicht). *Soit* U *un groupe algébrique unipotent sur un corps k qui opère sur un k-schéma quasi-affine* X. *Alors l'orbite de tout point $x \in X(k)$ est fermée dans* X (*par orbite de x nous entendons le sous-ensemble de* ens(X) *image de* G *par le morphisme $g \mapsto g \cdot x$*).

592 Par fonctorialité, G opère sur l'enveloppe affine de X (c'est-à-dire $\operatorname{Spec} \Gamma(X, \mathscr{O}_X)$), ce qui nous permet de supposer X affine. On peut ensuite supposer k algébriquement clos, X réduit et U lisse (noter que $U_{\text{réd}}$ opère sur $X_{\text{réd}}$ si k est parfait). Soit Y l'image schématique de G (EGA I 9.5.1) par le morphisme $g \mapsto g \cdot x$, qui est un sous-schéma fermé et réduit de X sur lequel G opère. Il résulte facilement de EGA IV 1.8.6 que l'orbite de x est une partie ouverte Z de Y, dense dans Y. Nous devons montrer que $Z = \text{ens}(Y)$. Soit F le sous-schéma fermé réduit de Y ayant $Y \setminus Z$ pour espace sous-jacent. On a donc $F = V(J)$, où J est un idéal non nul de $\Gamma(Y, \mathscr{O}_Y)$. Comme G est lisse, G opère sur F, donc sur J et par suite (3.2) $J^G \neq 0$. Si a est un élément non nul de J^G, a est nécessairement constante sur l'orbite Z, donc est constante sur Y, Z étant dense dans Y. Mais alors l'idéal J contient k et $F = \varnothing$.

Ceci étant, appliquons le lemme précédent au groupe U opérant sur l'espace affine $W(\mathfrak{e})$ par l'intermédiaire de la représentation adjointe. On obtient que l'orbite de X' est l'ensemble sous-jacent à un sous-préschéma fermé de $W(\mathfrak{e})$. Par ailleurs, le stabilisateur Z de X' est le centralisateur de X' dans U, et l'on a une immersion fermée :

$$U/Z \longrightarrow W(\mathfrak{e}).$$

Retenons que l'orbite de X' est l'espace sous-jacent à un sous-schéma fermé de $W(\mathfrak{e})$ de dimension égale à $\dim U - \dim Z$.

c) fin de la démonstration de 5.1.1 ii) b). Lorsque k est algébriquement clos, l'ap-
593 plication canonique $U(k) \to (U/Z)(k)$ est surjective, de sorte que d'après le point b) précédent, B est l'ensemble des points rationnels d'un sous-schéma fermé de $W(\mathfrak{e})$ de

dimension $\dim \mathrm{U} - \dim \mathrm{Z}$. Compte tenu du point a), pour prouver que $\mathrm{A} = \mathrm{B}$, il suffit alors de montrer que l'on a :

$$\operatorname{rg} \mathfrak{u} - \operatorname{rg} \mathrm{Centr}_{\mathfrak{u}}(\mathrm{X}') \leqslant \dim \mathrm{U} - \dim \underline{\mathrm{Centr}}_{\mathrm{U}}(\mathrm{X}').$$

Or U étant lisse, on a $\dim \mathrm{U} = \operatorname{rg} \mathfrak{u}$. D'autre part, on a (Exp. II 5.3.3) :

$$\dim \underline{\mathrm{Centr}}_{\mathrm{U}}(\mathrm{X}') \leqslant \operatorname{rg} \mathrm{Centr}_{\mathfrak{u}}(\mathrm{X}'),$$

d'où le résultat (notons que l'on a en fait $\dim \underline{\mathrm{Centr}}_{\mathrm{U}}(\mathrm{X}') = \operatorname{rg} \mathrm{Centr}_{\mathfrak{u}}(\mathrm{X}')$, ce qui redémontre que Z est lisse (5.7.1).

5.8. Fin de la démonstration de 5.1.1 i). — Il nous reste à prouver i) c) et i) d).

Démonstration de 5.1.1 i) d) (U lisse, H connexe). Nous aurons besoin du lemme suivant :

Lemme 5.8.1. — *Avec les notations de* 5.1.1*, supposons* U *lisse et* H *radiciel, et soit* H_1 *un sous-groupe algébrique de* H *qui possède un relèvement* H'_1 *dans* E*. Alors* H *possède un relèvement* H' *dans* E *qui majore* H'_1*.*

Par récurrence sur la hauteur de H/H_1, on peut supposer H/H_1 de hauteur 1. Soit $\mathrm{C}' = \underline{\mathrm{Centr}}_{\mathrm{E}}(\mathrm{H}'_1)$. Je dis que le morphisme canonique $\mathrm{C}' \to \mathrm{H}$ est un épimorphisme. Pour établir ce point, nous pouvons supposer k algébriquement clos ; mais alors, l'extension E est triviale (5.1.1 i a)) ; soient H'' un relèvement de H dans E, H''_1 l'image réciproque de H_1 dans H''. Les groupes H'_1 et H''_1 sont deux relèvements de H_1 dans E, donc sont conjugués par un élément de $\mathrm{U}(k)$, puisque k est algébriquement clos et U lisse (5.1.1 ii b)). Il est clair alors que pour prouver l'assertion sur C', il suffit de la prouver pour $\mathrm{C}'' = \underline{\mathrm{Centr}}_{\mathrm{E}}(\mathrm{H}''_1)$. Mais dans ce cas, C'' majore H'', et la propriété est claire. Par ailleurs il résulte de 5.7.1 que $\mathrm{C} \cap \mathrm{U}$ est lisse. Il est clair alors que nous pouvons remplacer E par C, donc supposer H'_1 central. Mais alors, quitte à passer au quotient par H'_1, nous pouvons supposer $\mathrm{H}_1 = 0$ et H de hauteur 1. 594

Comme U est lisse, on a la suite exacte de p-algèbres de Lie : (App. II 3.2) :

$$(*) \qquad 0 \longrightarrow \operatorname{Lie} \mathrm{U} \longrightarrow \operatorname{Lie} \mathrm{E} \longrightarrow \operatorname{Lie} \mathrm{H} \longrightarrow 0.$$

Compte tenu de App. II 2.2, dire que E est triviale équivaut à dire que $(*)$ est une extension triviale de p-algèbres de Lie. Supposons $\mathrm{H} \neq 0$ (donc $\operatorname{Lie} \mathrm{H} \neq 0$) et supposons avoir trouvé une sous-p-algèbre de Lie $\mathfrak{h}_1$ de $\mathfrak{h} = \operatorname{Lie} \mathrm{H}$ qui soit non nulle et qui se relève en une sous-p-algèbre de Lie $\mathfrak{h}'_1$ de Lie E. D'après *loc. cit.*, il existe un sous-groupe H_1 de H, tel que $\operatorname{Lie} \mathrm{H}_1 = \mathfrak{h}_1$, et un relèvement H'_1 de H_1 dans E tel que $\operatorname{Lie} \mathrm{H}'_1 = \mathfrak{h}'_1$. Appliquant à nouveau la réduction décrite plus haut, on se ramène au même problème, où l'on a remplacé H par H/H_1. Comme H est de hauteur 1, $\operatorname{Lie}(\mathrm{H}/\mathrm{H}_1) = \operatorname{Lie} \mathrm{H}/\operatorname{Lie} \mathrm{H}_1$ (*loc. cit.*), donc $\operatorname{rg} \operatorname{Lie}(\mathrm{H}/\mathrm{H}_1) \leqslant \operatorname{rg} \operatorname{Lie}(\mathrm{H}) - 1$. Bref, procédant par récurrence sur le rang de $\operatorname{Lie} \mathrm{H}$, on voit qu'il suffit, lorsque $\mathfrak{h} \neq 0$, de trouver une sous-algèbre de Lie non nulle de $\operatorname{Lie} \mathrm{H}$ qui se relève dans $\operatorname{Lie} \mathrm{E}$. Or on a le lemme suivant : 595

Lemme 5.8.2. — *Soient k un corps de caractéristique $p > 0$, et φ un morphisme surjectif de p-k-algèbres de Lie de rang fini $\mathfrak{g} \to \mathfrak{h}$. Alors :*

i) *Si* $\mathfrak{h}_{\overline{k}}$ *est réductive* (4.2.2) *et* $\neq 0$*, il existe une sous-algèbre de* Lie *réductive* $\mathfrak{h}_1$ *de* $\mathfrak{g}$*, dont l'image dans* $\mathfrak{h}$ *est non nulle.*

ii) *Si* k *est parfait et si* u *est un élément unipotent de* $\mathfrak{h}$ (*i.e. il existe* n *tel que* $u^{(p^n)} = 0$)*, alors* u *se relève en un élément unipotent de* $\mathfrak{g}$.

Prenons pour X un élément $\neq 0$ de $\mathfrak{h}$ dans le cas i) et u dans le cas ii), et soit X' un relèvement de X dans $\mathfrak{g}$. La sous-p-algèbre de Lie de $\mathfrak{g}$ engendrée par X' est une p-algèbre de Lie abélienne (Exp.VII) $\mathfrak{h}'$.

Cas i). Il est clair sur la description donnée dans 4.2.2 que la partie réductive (*loc. cit.*) de $\mathfrak{h}'_k$ est déjà définie sur k, notons-la $\mathfrak{r}'$. Je dis que l'image de $\mathfrak{r}'$ dans $\mathfrak{h}$ est non nulle. Pour établir ce point nous pouvons supposer k algébriquement clos, de sorte que $\mathfrak{h}' = \mathfrak{r}' \oplus \mathfrak{u}'$ ($\mathfrak{u}'$ partie unipotente de $\mathfrak{h}'$). Si l'image de $\mathfrak{r}'$ dans $\mathfrak{h}$ était nulle, l'image de $\mathfrak{h}'$ dans $\mathfrak{h}$ serait unipotente, donc serait nulle puisque $\mathfrak{h}$ est réductive (cf. 2.4 ii)), or par construction elle contient X.

Cas ii). On procède de même, en échangeant les rôles de $\mathfrak{r}'$ et de $\mathfrak{u}'$.

596 *Fin de la démonstration de* 5.8.1. Supposant $H \neq 0$, il existe d'après 5.8.2 une sous-algèbre de Lie réductive non nulle $\mathfrak{h}'_1$ de Lie E. Comme Lie U est unipotente (4.3 i)), on a nécessairement $(\mathrm{Lie}\,U) \cap \mathfrak{h}'_1 = 0$, de sorte que $\mathfrak{h}'_1$ est un relèvement d'une sous-p-algèbre de Lie de Lie H.

Fin de la démonstration de 5.1.1 i d). D'après 5.8.1, il existe une famille de sous-groupes algébriques H'_n ($n \in \mathbb{N}$) de E, telle que H'_{n+1} majore H'_n et telle que H'_n relève ${}_{F^n}H$. La suite décroissante de sous-groupes $\underline{\mathrm{Centr}}_E(H'_n)$ est stationnaire, soit C la valeur stationnaire. Le centre Z de C majore H'_n pour tout n, donc l'image de Z dans H majore ${}_{F^n}(H)$ pour tout n, et par suite, est un sous-groupe ouvert de H (Exp. VII_A § 4), donc est égale à H puisque H est connexe. Pour prouver que E est triviale, on peut donc remplacer E par Z, donc supposer E commutatif. Nous verrons alors dans 7.2.1 que E contient un sous-groupe de type multiplicatif maximal M, dont la formation commute à l'extension du corps de base. Comme $E_{\overline{k}}$ est une extension triviale (5.1.1 i) a)) et que U est unipotent, il est clair que M est l'unique relèvement de H dans E.

Démonstration de 5.1.1 i) c) (U k-résoluble). Comme $(H/H)^0(k)$ est d'ordre premier à p, il est immédiat par dualité qu'il existe un entier n tel que ${}_nH$ soit un sous-groupe étale et tel que le morphisme canonique ${}_nH \to H/H^0$ soit un épimorphisme, de sorte que $H/{}_nH$ est connexe. D'après 5.2.3 d), il existe un relèvement H' de ${}_nH$ dans E. On
597 montre, comme dans le début de la démonstration de 5.8.1, que $C = \underline{\mathrm{Centr}}_E(H')$ est un sous-groupe de E tel que $C \to H$ soit un épimorphisme et tel que $C \cap U$ soit lisse. Remplaçant E par C et passant au quotient par H', on est ramené au cas où U est lisse et H connexe, c'est-à-dire au cas i) d).

Ceci achève la démonstration de 5.1.1.

5.9. Contre-exemples. — Indiquons d'abord un procédé pour obtenir des extensions non triviales d'un k-groupe de type multiplicatif H par un k-groupe unipotent U. Supposons donnée une action de H sur U, et soit E le produit semi-direct $E = U \cdot H$. Soit d'autre part un élément de $H^1(k, U)$ représenté par un 1-cocycle a. Le groupe U

opère par automorphismes intérieurs sur E. La donnée de a définit donc une k-forme de E notée E_a. Supposons de plus que U soit commutatif, alors U opère trivialement sur U et sur le quotient $\mathrm{E}/\mathrm{U} = \mathrm{H}$, de sorte que E_a est encore une extension de H par U. Supposons, pour simplifier, que H soit un groupe étale diagonalisable, de sorte que le groupe de Galois $\mathscr{G}$ de $\overline{k}/k$ opère trivialement sur $\mathrm{H}(k)$; l'action de $\mathscr{G}$ sur les points de $\mathrm{E}_a(\overline{k})$ est alors donnée par la formule :

$$^g(u,h) = (^g u + a(g) - {}^h a(g), h) \qquad (g \in \mathscr{G},\ u \in \mathrm{U}(\overline{k}),\ h \in \mathrm{H}(\overline{k})).$$

Si h est un point de $\mathrm{H}(k)$, X son image réciproque dans E_a, X est donc un torseur sous U défini par la classe du 1-cocycle de $\mathscr{G}$ à valeur dans U, $g \mapsto a(g) - {}^h a(g)$. Il en résulte que s'il existe un point h de $\mathrm{H}(k)$ tel que le 1-cocycle précédent ne soit pas **598**
trivial, l'extension E_a n'est pas triviale. Nous allons appliquer cette construction dans deux cas particuliers :

a) *Extension non triviale d'un groupe étale diagonalisable* H *par* $\mathbb{Z}/p\mathbb{Z}$.

Prenons pour H le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ que l'on fait opérer par multiplication sur $\mathrm{U} = \mathbb{Z}/p\mathbb{Z}$. Soient d'autre part k un corps de caractéristique p, K une extension de k de groupe de Galois $\mathscr{G}$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$, a un élément non nul de $\mathrm{H}^1(\mathscr{G}, \mathrm{U}) = \mathrm{Hom}(\mathscr{G}, \mathrm{U})$. Le groupe E_a répond alors à la question.

b) *Exemple d'une extension non triviale d'un groupe étale diagonalisable* H*, par un groupe unipotent lisse et connexe* U.

Prenons pour corps k un corps non parfait tel qu'il existe une k-forme U de $\mathbb{G}_a$, telle que $\mathrm{H}^1(k, \mathrm{U}) \neq 0$. Par exemple (cf. J.-P. Serre, *Cohomologie Galoisienne*), on peut prendre pour k le corps des fractions d'un anneau de valuation discrète d'égale caractéristique $p > 0$, et pour U le sous-groupe algébrique de $\mathbb{G}_a \times_k \mathbb{G}_a$, d'équation $\mathrm{X}^p + \mathrm{X} + t\mathrm{Y}^p = 0$, où t désigne une uniformisante de k. En effet, supposant pour simplifier que k contient les racines $(p-1)^{\text{ièmes}}$ de l'unité, on a une suite exacte de groupes algébriques :

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{U} & \longrightarrow \mathbb{G}_a & \longrightarrow 0 \\ & & & & (x,y) & \longmapsto\ y & \end{array},$$

donc une suite exacte de cohomologie : **599**

$$\mathbb{G}_a(k) \xrightarrow{d} \mathrm{H}^1(k, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(k, \mathrm{U}) \to 0,$$

où d fait correspondre à x l'espace homogène sous $\mathbb{Z}/p\mathbb{Z}$ d'équation

$$\mathrm{X}^p + \mathrm{X} + tx^p = 0.$$

Par ailleurs, on sait que $\mathrm{H}^1(k, \mathbb{Z}/p\mathbb{Z})$ est isomorphe à $k/\mathfrak{P}(k)$ (où $\mathfrak{P}(x) = x^p + x$), donc $\mathrm{H}^1(k, \mathrm{U})$ est isomorphe à $k/(\mathfrak{P}(k) + tk^p)$. Supposons de plus $p \neq 2$, il est alors clair que t^2 est un élément de k qui n'appartient pas à $\mathfrak{P}(k) + tk^p$, donc $\mathrm{H}^1(k, \mathrm{U}) \neq 0$.

D'autre part $\boldsymbol{\mu}_{p-1}$ opère sur U par la formule :

$$(h, x, y) \longmapsto (hx, hy).$$

Notons $\mathscr{G}$ le groupe de Galois de l'extension K définie par l'équation

$$\mathrm{X}^p + \mathrm{X} + t^2 = 0,$$

et soit $a \in \mathrm{H}^1(\mathscr{G}, \mathrm{U})$ l'élément non nul décrit plus haut. On vérifie immédiatement que E_a est alors une extension non triviale de $\boldsymbol{\mu}_{p-1}$ par U.

c) *Extension non triviale de* $\mathbb{G}_m$ *par* $\boldsymbol{\alpha}_p$.

D'après 5.1.1 i) b), une telle extension ne peut exister que sur un corps k non parfait. Soit donc k un corps non parfait, G le produit semi-direct de $\mathrm{U} = \mathbb{G}_a$ par $\mathrm{H} = \mathbb{G}_m$, $\mathbb{G}_m$ opérant sur $\mathbb{G}_a$ par homothéties. Comme U est invariant dans G, alors ${}_{\mathrm{F}}\mathrm{U}$ l'est aussi. Soit $\mathrm{G}' = \mathrm{G}/{}_{\mathrm{F}}\mathrm{U}$. Le groupe G' est isomorphe à $\mathbb{G}_a \cdot \mathbb{G}_m$, où $\mathbb{G}_m$ opère sur $\mathbb{G}_a$ par la formule :

$$(h, u) \longmapsto h^p\, u.$$

600 Le foncteur $\mathscr{T}_{\mathrm{G}}$ (resp. $\mathscr{T}_{\mathrm{G}''}$) des sous-tores de G (resp. G'') (cf. Exp. XV) est isomorphe à $\mathbb{G}_a$, et le morphisme $\mathscr{T}_{\mathrm{G}} \to \mathscr{T}_{\mathrm{G}''}$ déduit du morphisme $\mathrm{G} \to \mathrm{G}''$ s'identifie au morphisme $u \mapsto u^p$. Il en résulte que si T'' est un sous-tore de G'' qui correspond à un point x de $k \simeq \mathbb{G}_a(k)$ tel que $x^{1/p}$ ne soit pas dans k, l'image réciproque E de T'' dans G sera extension d'un tore T'' par ${}_{\mathrm{F}}\mathrm{U} = \boldsymbol{\alpha}_p$, ne possèdera pas de tores maximaux définis sur k, donc ne sera pas triviale. On trouve pour E le sous-groupe de $\mathrm{G} = \mathrm{Spec}[\mathrm{U}, \mathrm{T}, \mathrm{T}^{-1}]$ d'équation $\mathrm{U}^p = x - x\mathrm{T}^p$.

Remarque 5.9.1. — Ce dernier exemple montre qu'un groupe algébrique non lisse, défini sur un corps non parfait, ne possède pas nécessairement de tores maximaux et répond ainsi à la question posée dans Exp. XIV 1.5 b).

d) Donnons maintenant un *exemple d'extension triviale* E *d'un groupe de type multiplicatif* H *par un groupe unipotent* U*, et de deux relèvements* H' *et* H'' *de* H *qui ne soient pas conjugués par un élément de* $\mathrm{U}(k)$.

Prenons pour E le produit semi-direct de $\mathrm{U} = \mathbb{G}_a$ par $\boldsymbol{\mu}_p = \mathrm{Spec}\, k[\mathrm{T}]/(\mathrm{T}^p - 1)$, l'action de $\boldsymbol{\mu}_p$ sur $\mathbb{G}_a = \mathrm{Spec}\, k[\mathrm{U}]$, étant définie par le comorphisme :

$$\mathrm{U} \mapsto (\mathrm{U} + \mathrm{U}^p)\mathrm{T} - \mathrm{U}^p.$$

Le centralisateur de $\boldsymbol{\mu}_p$ dans U est alors le groupe étale Z d'équation $\mathrm{U} + \mathrm{U}^p = 0$. Il en résulte que si k n'est pas algébriquement clos, l'application canonique $\mathrm{U}(k) \to$
601 $(\mathrm{U}/\mathrm{Z})(k)$ n'est pas en général surjective, donc, compte tenu de 5.1.1 ii) b), deux relèvements de $\boldsymbol{\mu}_p$ dans E ne sont pas nécessairement conjugués par un élément de $\mathrm{U}(k)$.

Voici un autre exemple, avec k *algébriquement clos* de caractéristique $p > 0$. Soit G le groupe radiciel produit semi-direct de $\boldsymbol{\mu}_p$ par $\boldsymbol{\alpha}_p$, où $\boldsymbol{\mu}_p$ opère sur $\boldsymbol{\alpha}_p$ par « homothéties ». On a alors une suite exacte de groupes algébriques, à groupes d'opérateurs $\boldsymbol{\mu}_p$:

$$\begin{array}{ccccccc} 0 & \to & \boldsymbol{\alpha}_p & \to & \mathbb{G}_a & \to & \mathbb{G}_a \to 0 \\ & & & & x & \mapsto & x^p \qquad , \end{array}$$

où $\boldsymbol{\mu}_p$ opère par homothéties sur le premier terme $\mathbb{G}_a$, et trivialement sur le second. La suite exacte de cohomologie (App. I, prop. 11) fournit ici la suite exacte :

$$0 \longrightarrow \mathbb{G}_a(k) \longrightarrow \mathrm{H}^1(\boldsymbol{\mu}_p, \boldsymbol{\alpha}_p) \longrightarrow \mathrm{H}^1(\boldsymbol{\mu}_p, \mathbb{G}_a).$$

Comme le dernier terme est nul (I 5.3.3), on voit que $\mathrm{H}^1(\boldsymbol{\mu}_p, \boldsymbol{\alpha}_p)$ est non nul, donc deux relèvements de $\boldsymbol{\mu}_p$ dans G ne sont pas nécessairement conjugués.

6. Extension d'un groupe unipotent par un groupe de type multiplicatif

602

6.1. Énoncé du théorème. —

Théorème 6.1.1. — *Soient k un corps,* U *un k-groupe algébrique unipotent,* H *un k-groupe de type multiplicatif,* E *un k-groupe algébrique extension de* U *par* H*, de sorte que l'on a la suite exacte*

$$1 \longrightarrow \mathrm{H} \longrightarrow \mathrm{E} \longrightarrow \mathrm{U} \longrightarrow 1.$$

Alors l'extension E *est* triviale *et il existe un unique relèvement de* U *dans* E *dans chacun des cas suivants :*

A) *Le groupe* U *est lisse et l'une des conditions suivantes est réalisée :*
   i) U *est connexe et le morphisme canonique* $\mathrm{E} \to \mathrm{U}$ *possède une section.*
   ii) U *possède une suite de composition à quotients successifs isomorphes à* $\mathbb{G}_a$.
   iii) H *est étale.*
   iv) k *est parfait.*

B) $\mathrm{U} = \boldsymbol{\alpha}_p$ *et k est parfait.*

C) E *est commutatif et k est parfait.*

6.2. Démonstration de 6.1.1 A). — Établissons d'abord trois lemmes.

Lemme 6.2.1. — *Soient* S *un préschéma,* E *un* S*-préschéma en groupes, extension d'un* S*-préschéma en groupes* U*, à* fibres connexes*, par un* S*-groupe de type multiplicatif et de type fini* H (c.-à-d. U *est le quotient de* E *par* H *pour la topologie* fpqc)*. Alors* E *est une* extension centrale*.* 603

En effet, comme H est commutatif, le groupe U opère par automorphismes intérieurs sur H, par l'intermédiaire d'un S-morphisme de groupes

$$u : \mathrm{U} \longrightarrow \underline{\mathrm{Aut}}_{\mathrm{S\text{-}gr}}(\mathrm{H}).$$

Le foncteur $\underline{\mathrm{Aut}}_{\mathrm{S\text{-}gr}}(\mathrm{H})$ est représentable par un S-schéma étale (Exp. X 5.10) et par suite la section unité est une immersion à la fois ouverte et fermée. Comme U est à fibres connexes, on en déduit que u est le morphisme unité.

Lemme 6.2.2. — *Avec les notations de* 6.1.1*, si* E *est triviale, il existe un unique relèvement de* U *dans* E*.*

Soient donc U' et U'' deux relèvements de U dans E. Pour montrer que $\mathrm{U}' = \mathrm{U}''$, nous pouvons supposer k algébriquement clos et il suffit de montrer que $\mathrm{H}^1(\mathrm{U}, \mathrm{H}) = 0$. Si U est connexe, U centralise H (6.2.1), donc

$$\mathrm{H}^1(\mathrm{U}, \mathrm{H}) = \mathrm{Hom}_{k\text{-gr}}(\mathrm{U}, \mathrm{H}) = 0$$

d'après 2.4 ii). Dans le cas général, notons U^0_1 l'unique relèvement dans E de la composante connexe U^0 de U, et soit $\mathrm{N} = \underline{\mathrm{Norm}}_{\mathrm{E}}(\mathrm{U}^0_1)$. Si $g \in \mathrm{E}(k)$, $\mathrm{int}(g)\mathrm{U}^0_1$ est un relèvement de U^0 donc est égal à U^0_1 et par suite $\mathrm{N}(k) \supset \mathrm{E}(k)$. Par ailleurs, N majore H (6.2.1) et U^0_1, d'où immédiatement le fait que $\mathrm{N} = \mathrm{E}$. Passant au quotient par U^0_1 on est ramené au cas où U est étale. Dans ce cas, k étant algébriquement clos, $\mathrm{H}^1(\mathrm{U}, \mathrm{H})$ 604

s'identifie au groupe de cohomologie ordinaire $\mathrm{H}^1(\mathrm{U}(k), \mathrm{H}(k))$ [(10)] et par suite est nul, puisque $\mathrm{U}(k)$ est un p-groupe fini et que $\mathrm{H}(k)$ est uniquement p-divisible.

Corollaire 6.2.3. — *Pour prouver que* E *est triviale, il suffit de montrer que* E *devient triviale après extension finie* séparable *du corps de base, en particulier, on peut supposer* H *diagonalisable.*

Lemme 6.2.4. — *Pour que toute* extension centrale E *de* U *par un k-groupe diagonalisable* H *soit triviale, il suffit que toute extension centrale de* U *par $\mathbb{G}_m$ soit triviale.*

En effet, par récurrence sur r, on note d'abord que l'hypothèse faite entraîne que E est triviale si $\mathrm{H} = \mathbb{G}_m^r$. Dans le cas général, H se plonge dans $\mathbb{G}_m^r$ pour un entier r convenable (c'est immédiat par dualité) ; soit $\mathrm{H}'' = \mathbb{G}_m^r/\mathrm{H}$. On obtient la suite exacte (App. I 2.1) :

$$\mathrm{Z}^1(\mathrm{U}, \mathrm{H}'') \longrightarrow \mathrm{Ext}_{\mathrm{alg}}(\mathrm{U}, \mathrm{H}) \longrightarrow \mathrm{Ext}_{\mathrm{alg}}(\mathrm{U}, \mathbb{G}_m^r) = 0$$

(où U opère trivialement sur H, H'', $\mathbb{G}_m^r$). Mais $\mathrm{Z}^1(\mathrm{U}, \mathrm{H}'') = \mathrm{Hom}_{k\text{-gr}}(\mathrm{U}, \mathrm{H}'') = 0$ (2.4 ii)), donc $\mathrm{Ext}_{\mathrm{alg}}(\mathrm{U}, \mathrm{H}) = 0$.

Démonstration de 6.1.1 A) i). Comme $\mathrm{E} \to \mathrm{U}$ possède une section, E définit un élément $\overline{f}$ de $\mathrm{H}^2(\mathrm{U}, \mathrm{H})$ (App. I 3.1). Nous devons montrer que $\overline{f}$ est nulle, et pour cela, il suffit de montrer qu'un 2-cocycle $f : \mathrm{U} \times_k \mathrm{U} \to \mathrm{H}$ est un morphisme constant, ce qui va résulter du lemme suivant :

605 ***Lemme 6.2.5***. — *Soient* U *un k-groupe algébrique unipotent lisse et connexe,* H *un k-groupe de type multiplicatif ; alors tout k-morphisme* (*de préschémas*) *:*

$$f : \mathrm{U} \longrightarrow \mathrm{H}$$

est constant.

Pour démontrer ce lemme, nous pouvons supposer k algébriquement clos. Nous procédons par récurrence croissante sur $\dim \mathrm{U}$. Si $\dim \mathrm{U} > 0$, U possède une suite de composition (cf. 3.9) :

$$1 \to \mathrm{U}' \to \mathrm{U} \xrightarrow{\pi} \mathrm{U}'' \to 1$$

avec $\mathrm{U}' \simeq \mathbb{G}_a$ et $\dim \mathrm{U}'' < \dim \mathrm{U}$. Il suffit de montrer que f se factorise à travers U''. Comme le graphe de la relation d'équivalence définie par π est lisse sur k, donc réduit, il suffit de montrer que si $x, y \in \mathrm{U}(k)$ ont même image z dans $\mathrm{U}''(k)$, alors $f(x) = f(y)$. Or $\pi^{-1}(z)$ est isomorphe à $\mathbb{G}_a$, donc la restriction de f à $\pi^{-1}(z)$ se factorise à travers une composante irréductible réduite de H, donc à travers un k-schéma isomorphe à $(\mathbb{G}_m)^r$. Il suffit alors de noter que tout morphisme de $\mathbb{G}_a$ dans $(\mathbb{G}_m)^r$ est constant, puisque toute fonction régulière inversible sur $\mathbb{G}_a$ est constante.

Démonstration de 6.1.1 A) ii). Grâce à 6.2.1, 6.2.3 et 6.2.4, nous pouvons supposer que $\mathrm{H} = \mathbb{G}_m$. Par hypothèse, U possède une suite de composition $\mathrm{U} \supset \mathrm{U}_1 \supset \cdots$, telle que $\mathrm{U}_i/\mathrm{U}_{i+1}$ soit isomorphe à $\mathbb{G}_a$. Soit E_1 l'image réciproque de U_1 dans E. Par récurrence sur $\dim \mathrm{U}$, on peut supposer que l'extension E_1 est triviale ; soit U_1' l'unique

[(10)] N.D.E. : voir, par exemple, la proposition III.6.4.2 du livre de M. Demazure et P. Gabriel, *Groupes algébriques* I, Masson & North-Holland (1970.

relèvement de U_1. Procédant comme dans la démonstration de 6.2.4, on montre que **606**
U'_1 est invariant dans E. Après passage au quotient par U'_1, on est ramené au cas où $U = \mathbb{G}_a$. Le S-schéma E (où $S = U$) est alors un torseur sous le S-groupe $\mathbb{G}_m \times_k S$, donc possède une section, puisque $\mathrm{Pic}(S) = 0$ (Exp. VIII 4.3). L'extension E est alors triviale d'après A) i).

Démonstration de 6.1.1 A) iii) (U *lisse,* H *étale*). Supposons d'abord U connexe. Le groupe $U_{\overline{k}}$ possède alors une suite de composition à quotients successifs isomorphes à $\mathbb{G}_a$, donc $E_{\overline{k}}$ est triviale d'après A) ii). Comme H est étale, il est clair que l'unique relèvement de $U_{\overline{k}}$ dans $E_{\overline{k}}$ est la composante connexe de $E_{\overline{k}}$, donc ce relèvement est déjà défini sur k. Dans le cas général, quitte à passer au quotient par la composante connexe de E, on est ramené au cas où E est étale, puis au cas où E est complètement décomposé (6.2.3). Comme $U(k)$ est un p-groupe et que $H(k)$ est d'ordre premier à p, on peut prendre pour relèvement de $U(k)$ le p-groupe de Sylow de $E(k)$.

Démonstration de 6.1.1 A) iv) (U *lisse, k parfait*). Si U est connexe, U possède une suite de composition à quotients successifs isomorphes à $\mathbb{G}_a$ (4.1.2 b)) et on applique A) ii). Dans le cas général, ce qui précède permet de nous ramener au cas où U est étale, puis au cas où U est complètement décomposé et H diagonalisable (6.2.3). Utilisant maintenant une suite de composition caractéristique de H ($H \supset H^0 \supset {}_{F^n}(H) \supset 0$), on se ramène au cas où H est de l'un des trois types suivants :

a) H est étale. **607**
b) $H = \mathbb{G}_m^r$.
c) H est radiciel.

Dans le cas a), on applique A) iii) ; dans le cas c), on applique 1.6. Enfin dans le cas b), on remarque qu'en vertu du théorème 90 de Hilbert, $E \to U$ possède une section, de sorte qu'il suffit de montrer que $H^2(U, \mathbb{G}_m^r) = H^2(U(k), \mathbb{G}_m^r(k)) = 0$. Or $U(k)$ est un p-groupe fini, tandis que $\mathbb{G}_m^r(k)$ est uniquement p-divisible (car k est parfait).

6.3. Démonstration de 6.1.1 B) et C). — Grâce à 6.2.1, 6.2.3, 6.2.4, on voit qu'il suffit de démontrer B) lorsque $H = \mathbb{G}_m$. On a donc une suite exacte :

$$1 \longrightarrow \mathbb{G}_m \longrightarrow E \longrightarrow \boldsymbol{\alpha}_p \longrightarrow 1.$$

Comme $\mathbb{G}_m$ est lisse, on en déduit une suite exacte de p-algèbres de Lie (App. II 3.2) :

$$(*) \qquad 0 \longrightarrow \mathrm{Lie}\,\mathbb{G}_m \longrightarrow \mathrm{Lie}\,E \longrightarrow \mathrm{Lie}\,\boldsymbol{\alpha}_p \longrightarrow 0.$$

Le groupe $\boldsymbol{\alpha}_p$ étant de hauteur 1, l'extension E est triviale si et seulement si (App. II 2.2) la suite exacte $(*)$ de p-algèbres de Lie est scindée. On sait que $\mathrm{Lie}\,\boldsymbol{\alpha}_p$ est engendrée par un élément $X \neq 0$ tel que $X^{(p)} = 0$ (App. II 2.1) ; il suffit donc de montrer que X se relève en un élément Z de $\mathrm{Lie}\,E$, tel que $Z^{(p)} = 0$. Or d'après 5.8.2 ii), il existe un élément unipotent Z de $\mathrm{Lie}\,E$ qui relève X. Comme la partie unipotente de $\mathrm{Lie}\,E$ est clairement au plus de dimension 1, on a nécessairement $Z^{(p)} = 0$.

Démonstration de 6.1.1 C). Si U'_1 est un relèvement dans E d'un sous-groupe algé- **608**
brique U_1 de U, U'_1 est invariant dans E, puisque E est supposé commutatif, et nous pouvons passer au quotient par U'_1. Utilisant une suite de composition de U (3.5 ii)),

la remarque précédente permet de nous ramener au cas où U est lisse ou égal à $\boldsymbol{\alpha}_p$. Mais alors E est triviale d'après A) iv) et B).

6.4. Exemples d'extensions d'un groupe unipotent U **par un groupe de type multiplicatif** H **qui ne sont pas triviales.** —

Vu 6.1.1 A) iv), le problème ne se pose qu'en caractéristique $p > 0$.

a) $\mathrm{H} = \mathbb{G}_m$, U est une forme non triviale de $\mathbb{G}_a$ (cf. App. III, § 5).

Soit k un corps non parfait de caractéristique 2, u un élément de k tel que $u^{1/2}$ n'appartienne pas à k. Considérons le groupe affine E, d'anneau $k[\mathrm{X}, \mathrm{Y}, (\mathrm{X}^2+u\mathrm{Y}^2)^{-1}]$, où la multiplication est donnée par le comorphisme :

$$(\mathrm{X}, \mathrm{Y}) \longmapsto (\mathrm{XX}' + u\mathrm{YY}', \mathrm{XY}' + \mathrm{YX}').$$

Le groupe E est lisse, connexe, commutatif, de dimension 2 ; le sous-schéma $\mathrm{Y} = 0$ définit un sous-groupe $\mathrm{H} \simeq \mathbb{G}_m$. Le noyau K de l'élévation à la puissance $2^{\text{ième}}$ dans E a pour équation :

$$\mathrm{X}^2 + u\mathrm{Y}^2 = 1,$$

donc est de dimension 1. Le groupe K contient le radical unipotent de E (défini sur $\overline{k}$) mais aussi la contribution de H qui est isomorphe à $\boldsymbol{\mu}_2$. Comme K est réduit sur
609 k, le radical unipotent de E n'est pas défini sur k et $\mathrm{U} = \mathrm{E}/\mathrm{H}$ ne se relève pas dans E. (On vérifie immédiatement que U est la forme de $\mathbb{G}_a$ ayant pour anneau $k[\mathrm{V}, \mathrm{W}]/(\mathrm{V} + u\mathrm{V}^2 + \mathrm{W}^2)$, le morphisme $\mathrm{E} \to \mathrm{U}$ correspondant au comorphisme : $\mathrm{V} \mapsto \mathrm{Y}^2/(\mathrm{X}^2 + \mathrm{Y}^2 u)$, $\mathrm{W} \mapsto \mathrm{XY}/(\mathrm{X}^2 + \mathrm{Y}^2 u)$).

b) $\mathrm{H} = \mathbb{G}_m$, $\mathrm{U} = \mathbb{Z}/2\mathbb{Z}$, k non parfait de caractéristique 2.

Choisissant k et u comme dans a), considérons le sous-groupe E de GL_2 engendré par l'élément X tel que :

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ u & 0 \end{pmatrix} = \begin{pmatrix} u^{1/2} & 0 \\ 0 & u^{1/2} \end{pmatrix} \begin{pmatrix} 0 & u^{-1/2} \\ u^{1/2} & 0 \end{pmatrix}.$$

Le groupe E est extension de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{G}_m$, mais cette extension n'est pas triviale car la partie unipotente de X n'est pas définie sur k.

c) $\mathrm{H} = \boldsymbol{\mu}_p$, $\mathrm{U} = \boldsymbol{\alpha}_p$, k non parfait.

Soit $\mathfrak{e}$ la p-algèbre de Lie commutative engendrée par deux éléments X et Y tels que $\mathrm{X}^{(p)} = \mathrm{X}$ et $\mathrm{Y}^{(p)} = a\mathrm{X}$. D'après App. II 2.2, $\mathfrak{e}$ est la p-algèbre de Lie d'un groupe algébrique E extension de $\boldsymbol{\alpha}_p$ par $\boldsymbol{\mu}_p$, mais cette extension est triviale si et seulement si, il existe $b \in k$ tel que $b^p = a$ (car on a alors $(b\mathrm{X} + \mathrm{Y})^{(p)} = 0$).

d) $\mathrm{H} = \boldsymbol{\mu}_2$, $\mathrm{U} = \boldsymbol{\alpha}_2 \times \boldsymbol{\alpha}_2$, E non commutative, k corps de caractéristique 2.

Considérons le groupe spécial linéaire $\mathrm{SL}_{2,k}$ et soit $\mathrm{E} = {}_{\mathrm{F}}(\mathrm{SL}_{2,k})$. Le groupe E est
610 un groupe radiciel de hauteur 1, dont l'algèbre de Lie est engendrée par trois éléments X, Y, Z vérifiant les relations suivantes :

$$[\mathrm{X}, \mathrm{Y}] = \mathrm{Z}, \qquad [\mathrm{X}, \mathrm{Z}] = [\mathrm{Y}, \mathrm{Z}] = 0$$
$$\mathrm{X}^{(p)} = \mathrm{Y}^{(p)} = 0, \qquad \mathrm{Z}^{(p)} = \mathrm{Z}.$$

Par suite, E est extension centrale de $U \simeq \boldsymbol{\alpha}_2 \times \boldsymbol{\alpha}_2$ par $\boldsymbol{\mu}_2$. Chaque facteur $\boldsymbol{\alpha}_2$ de U se relève de manière unique dans E, mais U lui-même ne se relève pas dans E, car $[X, Y] \neq 0$.

7. Groupes algébriques affines nilpotents

611

7.1. Extensions de groupes de type multiplicatif. —

Proposition 7.1.1. — *Soient* S *un préschéma,* H *et* K *deux* S*-préschémas en groupes de type multiplicatif et de type fini,* E *un préschéma en groupes extension de* K *par* H (c.-à-d. K *est le quotient de* E *par* H *pour la topologie* fpqc). *Alors* E *est de type multiplicatif dans les deux cas suivants :*

a) E *est commutatif.*

b) *Les fibres de* K *sont connexes.*

Démonstration. i) *Cas où* S *est le spectre d'un corps* k.

L'assertion à démontrer est locale pour la topologie fpqc, ce qui nous permet de supposer k algébriquement clos, donc H et K diagonalisables. Notons que K opère trivialement sur H par automorphismes intérieurs : c'est clair dans le cas a) et cela résulte de 6.2.1 dans le cas b). Par récurrence sur la longueur d'une suite de composition convenable de K, on est ramené au cas où K est de l'un des trois types suivants : a) $K = \mathbb{G}_m$, b) $K = \boldsymbol{\mu}_p$, c) $K = \boldsymbol{\mu}_q$ avec $(q, p) = 1$ et, dans ce cas, E est commutatif. Utilisant maintenant un plongement de H dans $\mathbb{G}_m^r$, on en déduit que E se plonge dans une extension de K par $\mathbb{G}_m^r$. On peut donc supposer que $H = \mathbb{G}_m^r$.

a) Si $K = \mathbb{G}_m$, E est un groupe algébrique lisse, connexe, affine (Exp. VI_B 9.2) de rang unipotent nul, c'est donc un tore.

b) $K = \boldsymbol{\mu}_p$. Dans ce cas E est une extension triviale. En effet, comme H est lisse, le 612
morphisme canonique $\mathrm{Lie}\, E \to \mathrm{Lie}\, \boldsymbol{\mu}_p$ est surjectif (App. II 3.2) et il suffit d'appliquer 5.8.2 i), compte tenu de App. II 2.2.

c) $K = \boldsymbol{\mu}_q$, avec $(q, p) = 1$ et E commutative. Là encore l'extension E est triviale. En effet, soit $x \in E(k)$ un relèvement d'un générateur $\overline{x}$ de $\boldsymbol{\mu}_q(k)$. L'élément x^q est un élément de $H(k)$ donc est de la forme y^q, $y \in H(k)$ (noter que $\mathbb{G}_m^r(k)$ est q-divisible). Comme E est commutatif, $y^{-1}x$ est un relèvement de x qui est d'ordre q.

ii) *Cas général.* Les groupes H et K sont plats, affines et de présentation finie sur S (Exp. IX 2.1) et par suite il en est de même de E (Exp. VI_B 9.2). Utilisant alors la technique générale de VI_B § 10, nous nous ramenons au cas où S est noethérien. Pour montrer que E est de type multiplicatif, il suffit alors de prouver que E est commutatif et que ${}_nE$ est fini sur S pour tout n (Exp. X 4.8 b).

a) E est commutatif. On doit vérifier que le morphisme :

$$E \times_S E \longrightarrow E, \qquad (x, y) \mapsto [x, y] = xyx^{-1}y^{-1}$$

se factorise à travers la section unité de E, et il suffit de le vérifier lorsque S est le spectre d'un anneau local artinien. Mais alors E est de type multiplicatif d'après i) et Exp. X 2.3.

b) ${}_nE$ est fini sur S. En effet, on a la suite exacte :

$$0 \to {}_nH \to {}_nE \to {}_nK \xrightarrow{u} H_n$$

613 (où H_n est le conoyau de l'élévation à la puissance n dans H). On sait que H_n est de type multiplicatif (Exp. IX 2.7) donc séparé, et que ${}_nH$ et ${}_nK$ sont finis sur S ; Ker u est un sous-groupe fermé de ${}_nK$, donc est fini sur S, et ${}_nE$ est fini sur S, comme extension d'un groupe fini par un groupe fini (Exp. VI_B 9.2).

7.2. Structure des groupes algébriques affines commutatifs. —

Théorème 7.2.1. — *Soient k un corps,* G *un k-groupe algébrique affine commutatif. Alors :*

a) G *contient un plus grand sous-groupe de type multiplicatif* M. *Le groupe* M *est caractéristique dans* G *et* G/M *est unipotent, et sa formation commute à l'extension du corps k.*

b) *Si k est parfait,* G *est le produit direct de* M *et d'un sous-groupe algébrique unipotent* U*, et ceci de manière unique.*

Démonstration. i) k algébriquement clos.

Lorsque G est lisse, 7.2.1 b) est bien connu (BIBLE § 4 Th. 4). Si G est radiciel de hauteur 1, à la décomposition de Lie G décrite dans 4.2.2 correspond, compte tenu de 4.3.1 v) et de App. II 2.2, une décomposition de G du type 7.2.1 b). Dans le cas général, G admet une suite de composition dont les quotients successifs sont lisses ou radiciels de hauteur 1 (App. II 3.1). Pour prouver 7.2.1 b), il suffit alors de noter que si l'on a une suite exacte de groupes algébriques commutatifs :

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0,$$

614 où G' (resp. G'') est produit d'un groupe de type multiplicatif par un groupe unipotent $G' = M' \cdot U'$ (resp. $G'' = M'' \cdot U''$), alors il en est de même de G. En effet, considérons la suite exacte :

$$0 \longrightarrow G'/U' \longrightarrow G/U' \longrightarrow G'' \longrightarrow 0.$$

D'après 7.1.1 a), l'image réciproque dans G/U' de M'' est un sous-groupe de type multiplicatif M_1. Le groupe M_1 se relève en un sous-groupe M de G (5.1.1 i) a)). De même, utilisant cette fois 6.1.1 C), on prouve qu'il existe un sous-groupe unipotent U de G extension de U'' par U'. Il est clair que $G = M \cdot U$.

ii) k quelconque. D'après i), $G_{\overline{k}}$ est produit direct d'un groupe de type multiplicatif $M_{\overline{k}}$ par un groupe unipotent $U_{\overline{k}}$. Posons $S = \overline{k} \times_k \overline{k}$ et soient M_1 et M_2 les deux images inverses de $M_{\overline{k}}$ par les deux projections $S \rightrightarrows \overline{k}$. Le groupe $G_S/M_2 = (G/M_{\overline{k}})_S$ a ses fibres unipotentes, donc l'image de M_1 dans G_S/M_2 est nulle (2.4 i)) et M_2 majore M_1. De même M_1 majore M_2, et finalement $M_1 = M_2$. Par descente fpqc, il en résulte que $M_{\overline{k}}$ provient d'un sous-groupe algébrique M de G. Il est clair que M est de type multiplicatif, que G/M est unipotent et que la formation de M est compatible avec toute extension du corps k. Pour tout k-préschéma S, tout sous-groupe de type multiplicatif H de G_S est contenu dans M_S. En effet, d'après 2.5, son image dans le groupe à fibres unipotentes $(G/M)_S = G_S/M_S$ est nulle. Prenant en particulier

pour H le transformé de M_S par un automorphisme de G_S, on en déduit que M est caractéristique dans G.

Enfin si k est parfait, G/M se relève dans G en un groupe unipotent, et ce de manière unique d'après 6.1.1 C).

615

Remarque 7.2.2. — i) Si k n'est pas parfait, la composante unipotente de $G_{\overline{k}}$ n'est pas nécessairement définie sur k, comme le montre l'exemple 6.4 a).

ii) Contrairement à ce qui se passe pour la composante de type multiplicatif M, la composante unipotente U n'est pas en général caractéristique dans G (et ceci quelle que soit la caractéristique de k). Bien sûr, l'unicité de la décomposition 7.2.1 b) entraîne que U est invariant par tout k-automorphisme de G. Mais si U et M sont tels qu'il existe un k-préschéma S et un S-homomorphisme non nul $h : U_S \to M_S$ (cf. 2.6), on en déduit un S-automorphisme de G_S, $(u, m) \mapsto (u, h(u) + m)$, qui ne laisse pas U_S invariant.

iii) Si G est fini sur k, G/M correspond par la dualité de Cartier (2.6) à la composante connexe du dual D(G) de G.

7.3. Structure des groupes algébriques affines nilpotents. —

Théorème 7.3.1. — *Soient k un corps,* G *un k-groupe algébrique nilpotent* (Exp. VI_B § 8)*, affine, connexe. Alors* G *possède un plus grand sous-groupe de type multiplicatif* M*. Le groupe* M *est central et caractéristique, et* G/M *est un groupe algébrique unipotent.*

Soit Z le centre de G, M le plus grand sous-groupe de type multiplicatif de Z (7.2.1). Comme Z est caractéristique dans G et M caractéristique dans Z, M est caractéristique dans G. Il suffit de montrer que G/M est unipotent. Par récurrence sur la longueur de la suite centrale ascendante de G, ceci va résulter plus généralement du lemme 616
suivant :

Lemme 7.3.2. — (Rosenlicht). *Soit* G *un k-groupe algébrique connexe,* Z *son centre. Alors le centre* Z′ *de* $G' = G/Z$ *est unipotent.*

Démonstration. Nous pouvons supposer k algébriquement clos. Il suffit alors de montrer que Z′ ne contient pas de sous-groupe isomorphe à $\boldsymbol{\mu}_\ell$ pour tout nombre premier ℓ (4.6.1 vi)). Soit donc $\boldsymbol{\mu}_\ell$ un sous-groupe de Z′, N son image réciproque dans G. Comme $\boldsymbol{\mu}_\ell$ est central dans G′, N est invariant dans G.

i) Cas où $(\ell, p) = 1$. On peut trouver un élément x de $N(k)$ et un entier n possédant les propriétés suivantes :

a) x relève un générateur $\overline{x}$ de $\boldsymbol{\mu}_\ell$.

b) $x^{\ell^n} \in Z^0(k)$;

(il suffit de choisir un relèvement de $\overline{x}$ dont l'image dans $N/Z^0(k)$ appartienne au ℓ-sous-groupe de Sylow).

L'élévation à la puissance $\ell^{\text{ième}}$ dans le groupe commutatif Z^0 est un morphisme étale, donc $Z^0(k)$ est ℓ-divisible. Par suite, quitte à multiplier x par un élément de $Z^0(k)$, on peut supposer que $x^{\ell^n} = 0$. Le groupe N est alors engendré par deux groupes

commutatifs qui commutent (Z et le groupe engendré par x), donc est commutatif. Le groupe ${}_{\ell^n}\mathrm{N}$ est un groupe de type multiplicatif, caractéristique dans N, donc invariant dans G, et par suite central, G étant connexe (Exp. IX 5.5). Donc ${}_{\ell^n}\mathrm{N}$ est contenu dans Z, ce qui contredit le fait que son image dans G′ contient $\boldsymbol{\mu}_\ell$.

617 ii) $\ell = p$. Il existe alors un entier n, tel que l'image de ${}_{\mathrm{F}^n}\mathrm{N}$ dans G′ contienne $\boldsymbol{\mu}_p$, de sorte que l'on a la suite exacte :

$$(*) \qquad 1 \longrightarrow \mathrm{K} \longrightarrow {}_{\mathrm{F}^n}\mathrm{N} \longrightarrow \boldsymbol{\mu}_p \longrightarrow 1.$$

Le groupe K est contenu dans Z, donc est commutatif ; il résulte alors de 7.2.1 et de 7.1.1 b) et 5.5.1 qu'il existe un sous-groupe de type multiplicatif contenu dans ${}_{\mathrm{F}^n}\mathrm{N}$ dont l'image dans le quotient par K est $\boldsymbol{\mu}_p$. On en déduit comme dans i) que ${}_{\mathrm{F}^n}\mathrm{N}$ est commutatif. La composante de type multiplicatif de ${}_{\mathrm{F}^n}\mathrm{N}$ (7.2.1) est caractéristique dans ${}_{\mathrm{F}^n}\mathrm{N}$, donc invariante dans G, donc centrale (Exp. IX 5.5) ; comme son image dans G′ contient $\boldsymbol{\mu}_p$ on obtient une contradiction.

A. Appendice I. Cohomologie de Hochschild et extensions de groupes algébriques

618

A.1. Définition des groupes de cohomologie. — Soient k un corps, G un k-groupe algébrique, $(\mathbf{Ab})_\mathrm{G}$ la catégorie abélienne des k-groupes algébriques commutatifs sur lesquels G opère. Si $\mathrm{A} \in \mathrm{Ob}(\mathbf{Ab})_\mathrm{G}$, le foncteur $h_\mathrm{A} : (\mathbf{Sch}/k)^\circ \to (\mathbf{Ens})$ canoniquement défini par A, est un G-$\mathbb{Z}$-module au sens de I 3.2. Nous pouvons donc considérer le complexe standard $\mathrm{C}^\bullet(\mathrm{G}, \mathrm{A})$ des *cochaines algébriques* de G à valeur dans A (Exp. I 5.1), ainsi que le groupe des i-cocycles $\mathrm{Z}^i(\mathrm{G}, \mathrm{A})$, des i-cobords $\mathrm{B}^i(\mathrm{G}, \mathrm{A})$ et le $i^{\text{ème}}$ groupe de cohomologie $\mathrm{H}^i(\mathrm{G}, \mathrm{A})$. Comme d'habitude, $\mathrm{H}^0(\mathrm{G}, \mathrm{A})$ s'identifie au groupe $\mathrm{A}^\mathrm{G}(k)$, où A^G est le k-foncteur des invariants de A sous G. Le groupe $\mathrm{H}^1(\mathrm{G}, \mathrm{A})$ classifie les espaces principaux homogènes sous A, triviaux, sur lesquels G opère.

Le foncteur $\mathrm{A} \mapsto \mathrm{H}^\bullet(\mathrm{G}, \mathrm{A})$ n'est pas en général un foncteur cohomologique de la catégorie $(\mathbf{Ab})_\mathrm{G}$ à valeur dans $\mathbf{Ab}$; toutefois, on a la proposition suivante :

Proposition A.1.1. — *Soit* $0 \to \mathrm{A}' \xrightarrow{u} \mathrm{A} \xrightarrow{v} \mathrm{A}'' \to 0$ *une suite exacte dans* $(\mathbf{Ab})_\mathrm{G}$. *Alors :*

a) *Si v possède une section (c'est-à-dire s'il existe un k-morphisme de préschémas* $s : \mathrm{A}'' \to \mathrm{A}$ *tel que* $vs = 1_{\mathrm{A}''}$*), on a la suite exacte de cohomologie habituelle :*

$$\cdots \to \mathrm{H}^i(\mathrm{G}, \mathrm{A}) \to \mathrm{H}^i(\mathrm{G}, \mathrm{A}'') \xrightarrow{d} \mathrm{H}^{i+1}(\mathrm{G}, \mathrm{A}') \to \cdots$$

619 b) *Si* $\mathrm{A}(k) \to \mathrm{A}''(k)$ *est surjectif, on a la suite exacte :*

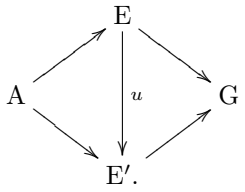
$$(1) \qquad 0 \to \mathrm{A}'^\mathrm{G}(k) \to \mathrm{A}^\mathrm{G}(k) \to \mathrm{A}''^\mathrm{G}(k) \xrightarrow{d} \mathrm{H}^1(\mathrm{G}, \mathrm{A}') \to \mathrm{H}^1(\mathrm{G}, \mathrm{A}) \to \mathrm{H}^1(\mathrm{G}, \mathrm{A}'').$$

Démonstration. a) On note que l'existence d'une section entraîne l'exactitude de la suite de complexes :

$$0 \longrightarrow \mathrm{C}^\bullet(\mathrm{G}, \mathrm{A}') \longrightarrow \mathrm{C}^\bullet(\mathrm{G}, \mathrm{A}) \longrightarrow \mathrm{C}^\bullet(\mathrm{G}, \mathrm{A}'') \longrightarrow 0.$$

b) Si $x'' \in A''^{G}(k)$, son image réciproque dans A est un espace principal homogène sous A′, trivial (car $A(k) \to A''(k)$ est supposé surjectif), sur lequel G opère, donc définit un élément $d(x'') \in H^1(G, A')$. L'exactitude de la suite (1) est alors immédiate.

A.2. Le groupe $\mathrm{Ext}_{\mathrm{alg}}(G, A)$**.** — Soient A et G deux k-groupes algébriques, E et E′ deux k-groupes algébriques extension de G par A. Ces deux extensions sont dites *isomorphes* s'il existe un k-morphisme de groupes $u : E \to E'$ qui rende commutatif le diagramme :



Le groupe E opère sur A par automorphismes intérieurs et si A est commutatif, cette action se factorise à travers G, donc G opère sur A. Réciproquement, si $A \in \mathrm{Ob}(\mathbf{Ab})_G$, nous notons $\mathrm{Ext}_{\mathrm{alg}}(G, A)$ l'ensemble des classes d'extensions algébriques E de G par A pour lesquelles l'action de G sur A définie par E, et celle provenant de la structure **620**
d'objet de $(\mathbf{Ab})_G$, coïncident.

$\mathrm{Ext}_{\mathrm{alg}}(G, A)$ est de façon naturelle un bifoncteur covariant en A et contravariant en G. Plus précisément :

a) si $f : A \to B$ est un morphisme dans $(\mathbf{Ab})_G$, et si E représente un élément de $\mathrm{Ext}_{\mathrm{alg}}(G, A)$, on définit $f_*(E) \in \mathrm{Ext}_{\mathrm{alg}}(G, B)$ comme étant la classe de l'extension de G par B égale au quotient du produit semi-direct $B \cdot E$ (E opérant sur B à travers G) par le sous-groupe algébrique image de A par le morphisme (f, i) (ce quotient est représentable d'après Exp. VI_A § 5), de sorte que l'on a un diagramme commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & B & \longrightarrow & f_*(E) & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

b) Si $g : H \to G$ est un k-morphisme de k-groupes algébriques, et si E est une extension de G par A, le produit fibré $E \times_G H$ est de façon naturelle une extension de H par A, notée $g^*(E)$. On a donc un diagramme commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & g^*(E) & \longrightarrow & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_A} & & \downarrow & & \downarrow{\scriptstyle g} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

En adaptant les démonstrations données dans J.-P. Serre, *Groupes algébriques et corps de classe,* chap. VII, on munit $\mathrm{Ext}_{\mathrm{alg}}(G, A)$ d'une structure naturelle de *groupe abélien,* fonctorielle en A et G.

621 ***Proposition A.2.1***. — *Soit :* $0 \to A' \to A \to A'' \to 0$ *une suite exacte dans* $(\mathbf{Ab})_G$, *alors :*

a) *On a une suite exacte canonique de groupes abéliens :*

$$Z^1(G, A) \to Z^1(G, A'') \xrightarrow{d} \mathrm{Ext}_{\mathrm{alg}}(G, A') \to \mathrm{Ext}_{\mathrm{alg}}(G, A) \to \mathrm{Ext}_{\mathrm{alg}}(G, A'').$$

b) *Si* $A(k) \to A''(k)$ *est surjective, on déduit de* a) *la suite exacte :*

(2) $$H^1(G, A) \to H^1(G, A'') \xrightarrow{d} \mathrm{Ext}_{\mathrm{alg}}(G, A') \to \mathrm{Ext}_{\mathrm{alg}}(G, A) \to \mathrm{Ext}_{alg}(G, A'').$$

La suite exacte de a) généralise la suite exacte habituelle des $\mathrm{Hom}(\cdot, \cdot)$ valable dans le cadre des extensions commutatives (*loc. cit.*) et se démontre de la même façon. Rappelons simplement la définition du cobord $d : Z^1(G, A'') \to \mathrm{Ext}_{\mathrm{alg}}(G, A')$. Pour cela, considérons l'extension

$$1 \longrightarrow A' \longrightarrow A \cdot G \longrightarrow A'' \cdot G \longrightarrow 1,$$

déduite de façon évidente de la suite exacte $0 \to A' \to A \to A'' \to 0$. Si $u \in Z^1(G, A'')$, u définit de la façon habituelle un homomorphisme section $u : G \to A'' \cdot G$. On a alors $d(u) = u^*(A \cdot G)$.

A.3. Comparaison de $H^2(G, A)$ et de $\mathrm{Ext}_{\mathrm{alg}}(G, A)$. — Il est bien connu, dans le cas des groupes abstraits, qu'il existe un isomorphisme fonctoriel entre les groupes abéliens $H^2(G, A)$ et $\mathrm{Ext}(G, A)$. De même dans le cas présent, si A est un élément de $(\mathbf{Ab})_G$, à tout 2-cocycle $u \in Z^2(G, A)$ on peut faire correspondre une structure de groupe algébrique sur le préschéma $A \times_k G$ qui en fait un élément de $\mathrm{Ext}_{\mathrm{alg}}(G, A)$. De plus cette extension est triviale si et seulement si $u \in B^2(G, A)$ (cf. Exp. III 1.2.2). Rappelons que la loi de composition sur $A \times G$ est définie par la formule :

$$(a, g)(a', g') = a + {}^g a' + u(g, g').$$

622 Il est clair que les extensions de G par A ainsi obtenues ne sont pas quelconques, puisqu'elles possèdent une section. Mais réciproquement, si $E \in \mathrm{Ext}_{\mathrm{alg}}(G, A)$ possède une section s, E est isomorphe à l'extension de G par A associée au 2-cocycle u tel que :

$$u(g, g') = s(g)s(g')s(gg')^{-1}.$$

On obtient finalement la proposition suivante :

Proposition A.3.1. — *Il existe un isomorphisme fonctoriel entre les bifoncteurs à valeur dans les groupes abéliens :*

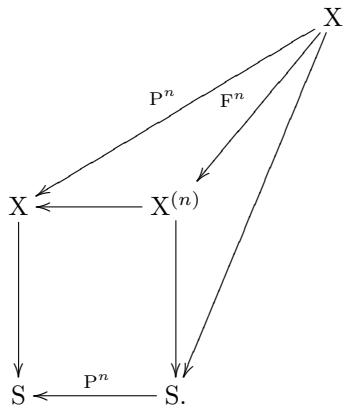
$$(G, A) \mapsto H^2(G, A) \qquad et \qquad (G, A) \mapsto \mathrm{Ext}_s(G, A),$$

où $\mathrm{Ext}_s(G, A)$ *désigne le sous-groupe de* $\mathrm{Ext}_{\mathrm{alg}}(G, A)$ *formé des classes d'extension de* G *par* A *qui possèdent une section.*

B. Appendice II. Rappels et compléments sur les groupes radiciels

623 Soit p un nombre premier > 1 et soit S un $\mathbb{F}_p$-préschéma.

B.1. Le morphisme de Frobenius. — Pour tout S-préschéma X et tout entier $n > 0$, notons $\mathrm{P}^n : \mathrm{X} \to \mathrm{X}$ le $\mathbb{F}_p$-endomorphisme qui correspond à l'élévation à la puissance p^n-ième dans $\mathscr{O}_\mathrm{X}$ et notons $\mathrm{X}^{(n)}$ le S-préschéma image inverse de X par le morphisme $\mathrm{P}^n : \mathrm{S} \to \mathrm{S}$. Il existe alors un unique S-morphisme $\mathrm{F}^n : \mathrm{X} \to \mathrm{X}^{(n)}$ qui rend commutatif le diagramme :



Il est clair que F^n s'identifie au « $n^{\text{ième}}$ itéré » de $\mathrm{F}^1 = \mathrm{F}$, appelé *morphisme de Frobenius de* X/S.

Si G est un S-préschéma en groupes, $\mathrm{G}^{(n)}$ est un S-préschéma en groupes et $\mathrm{F}^n : \mathrm{G} \to \mathrm{G}^{(n)}$ est un S-morphisme de groupes. Son noyau ${}_{\mathrm{F}^n}(\mathrm{G})$ est un sous-préschéma en groupes caractéristique de G (c.-à-d. stable par le foncteur $\underline{\mathrm{Aut}}_{\text{S-gr}}(\mathrm{G})$), et radiciel sur S. Si G est un S-préschéma en groupes radiciel, on dit que G est de *hauteur* $\leqslant h$, si ${}_{\mathrm{F}^h}(\mathrm{G}) = \mathrm{G}$.

624

B.2. Groupes et p-algèbres de Lie. — Si G est un S-préschéma en groupes, Lie(G) (Exp. II) est de façon naturelle une p-Algèbre de Lie restreinte (Exp. VII_A §§ 5 et 6). En particulier on a le résultat suivant (cf. Exp. VII_A) :

Proposition B.2.1. — i) $\mathrm{Lie}(\boldsymbol{\alpha}_p)_\mathrm{S} = \mathrm{Lie}(\mathbb{G}_a)_\mathrm{S}$ [(11)] *est un faisceau de* $\mathscr{O}_\mathrm{S}$*-modules, libre sur* $\mathscr{O}_\mathrm{S}$ *de rang* 1 *engendré par un élément* X *tel que* $\mathrm{X}^{(p)} = 0$.

ii) $\mathrm{Lie}(\boldsymbol{\mu}_p)_\mathrm{S} = \mathrm{Lie}(\mathbb{G}_m)_\mathrm{S}$ *est un faisceau de* $\mathscr{O}_\mathrm{S}$*-modules, libre sur* $\mathscr{O}_\mathrm{S}$ *de rang* 1*, possédant une base canonique* X *telle que* $\mathrm{X}^{(p)} = \mathrm{X}$.

Rappelons maintenant le résultat fondamental prouvé dans Exp. VII_A § 7 :

Théorème B.2.2. — *Supposons* S *affine d'anneau* A*. Alors le foncteur :*

$$\mathrm{G} \longmapsto \mathrm{Lie}\,\mathrm{G}$$

établit une équivalence de catégories entre, d'une part, la catégorie des S*-préschémas en groupes* G *de présentation finie et plats sur* S*, de hauteur* 1*, dont l'algèbre de*

(11) N.D.E. : on a supprimé ici la définition de $\boldsymbol{\alpha}_p$, déjà donnée au début de cet Exposé.

Lie est localement libre sur $\mathscr{O}_S$ et, d'autre part, la catégorie des p-A-algèbres de Lie restreintes localement libres de rang fini.

De plus, si G *est comme ci-dessus et si* H *est un* S*-préschéma en groupes de présentation finie, le morphisme canonique :*

$$\mathrm{Hom}_{S\text{-gr}}(G, H) \longrightarrow \mathrm{Hom}_{p\text{-A-Lie}}(\mathrm{Lie}\, G(S), \mathrm{Lie}\, H(S))$$

est un isomorphisme.

625

B.3. Groupes radiciels et groupes lisses. — Nous supposons maintenant que S est le spectre d'un corps k de caractéristique p.

Rappelons que dans Exp. $\mathrm{VI_A}$ § 5, on a montré que si G est un k-groupe algébrique, H un sous-groupe algébrique de G, alors le faisceau G/H (faisceau pour la topologie fpqc) est représentable. Rappelons alors ($\mathrm{VII_A}$ 8.3) :

Proposition B.3.1. — *Soit* G *un k-groupe algébrique. Alors il existe un entier m, tel que pour tout $n \geqslant m$, le groupe algébrique* $G/F^n(G)$ *soit lisse sur k.*

Proposition B.3.2. — *Considérons une suite exacte de k-groupes algébriques :*

$$1 \to G' \to G \xrightarrow{u} G'' \to 1$$

et les assertions suivantes :

i) *Le morphisme u est lisse.*

ii) G' *est lisse sur k.*

iii) *Pour tout entier $n > 0$, on a la suite exacte :*

$$1 \longrightarrow {}_{F^n}(G') \longrightarrow {}_{F^n}(G) \longrightarrow {}_{F^n}(G'') \longrightarrow 1.$$

iv) *Le morphisme* ${}_F G \to {}_F G''$ *est un épimorphisme.*

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

Alors, on a les implications suivantes :

$$\text{i)} \iff \text{ii)} \implies \text{iii)} \implies \text{iv)} \iff \text{(v)}.$$

De plus, si G *est lisse, les cinq assertions sont équivalentes.*

626 i) $\Leftrightarrow$ ii) d'après Exp. $\mathrm{VI_B}$ 9.2 vii).

ii) $\Rightarrow$ iii). Si G' est lisse, $F^n : G' \to G'^{(n)}$ est un épimorphisme et iii) résulte du diagramme du « serpent ».

iii) $\Rightarrow$ iv) est clair.

iv) $\Leftrightarrow$ v) d'après le théorème B.2.2.

v) $\Rightarrow$ ii) lorsque G est lisse. En effet G'' est alors lisse, et v) entraîne que l'on a $\dim G' = \dim_k(\mathrm{Lie}\, G')(k)$, donc G' est lisse.

C. Appendice III. Remarques et compléments concernant les exposés XV, XVI, XVII

627

C.1. Il se peut que les propositions 1.2 et 1.2 bis de XV restent vraies si on supprime l'hypothèse que H_0 est lisse sur S_0. C'est en particulier le cas si G est fini, plat et commutatif.

C.2. Complément à XV 4.8. — La proposition suivante ainsi que les théorèmes C.3.1 et C.4.1 ci-après figureront dans un article en préparation de M. Raynaud sur les schémas en groupes sur un anneau de valuation discrète. (12)

Proposition C.2.1. — *Soient* S *le spectre d'un anneau de valuation discrète, t son point générique,* G *un* S*-préschéma en groupes de type fini et plat,* $\widetilde{\mathrm{G}} = \mathrm{Spec}\,\Gamma(\mathrm{G}, \mathscr{O}_{\mathrm{G}})$, $u : \mathrm{G} \to \widetilde{\mathrm{G}}$ *le morphisme canonique. Alors :*

(1) $\widetilde{\mathrm{G}}$ *est de façon naturelle un* S*-schéma en groupes et u est un homomorphisme.*

(2) $\mathrm{Ker}(u)$ *est plat sur* S *et* $(\widetilde{\mathrm{G}}, u)$ *est un quotient* fpqc *de* G *par* $\mathrm{Ker}(u)$*, de sorte que* $\widetilde{\mathrm{G}}$ *est le plus grand quotient affine de* G*.*

(3) *Si* G_t *est affine,* $\mathrm{Ker}(u)$ *est un groupe étale sur* S*, égal au groupe unité si et seulement si* G *est séparé sur* S*. En particulier, un* S*-schéma en groupes* G*, plat, de type fini, séparé, à fibre générique affine est affine.*

C.3. Dans l'énoncé de XV 6.6, l'hypothèse que H soit égal à son normalisateur connexe est inutile pour que l'ensemble des points s de S tels que H_s soit un sous-groupe parabolique de G_s soit un ensemble ouvert. En effet, reprenons la démonstration donnée dans le paragraphe c) précédant le lemme 6.9, et notons $\overline{\mathrm{N}}$ l'adhérence schématique de N_t dans G. Donc $\overline{\mathrm{N}}$ est un sous-schéma en groupes fermé de G, plat sur S, qui majore H et qui est contenu dans N. Il résulte alors du théorème ci-après **628**
que $\mathrm{G}/\overline{\mathrm{N}}$ est représentable. Comme $\mathrm{G}_s/\overline{\mathrm{N}}_s$ est propre et connexe, on termine comme dans *loc. cit.*

Théorème C.3.1. — (13) *Soient* S *le spectre d'un anneau de valuation discrète hensélien,* G *un* S*-préschéma en groupes localement de type fini,* H *un sous-préschéma en groupes fermé de* G*, plat sur* S*, alors* G/H *est représentable.*

C.4. Complément à (XVI 1.1). — Le théorème suivant précise (VIII 7.9).

Théorème C.4.1. — *Soit* S *le spectre d'un anneau de valuation discrète de caractéristique résiduelle* $p > 0$ *et soit* G *un* S*-schéma en groupes, commutatif, lisse, de type fini et séparé sur* S*. Alors les conditions suivantes sont équivalentes :*

(i) ${}_p\mathrm{G}$ *est fini sur* S*.*

(ii) *Pour tout* S*-préschéma* S′ *et pour tout* S′*-préschéma en groupes* H′*, de présentation finie sur* S′*, séparé sur* S′*, tout* S′*-monomorphisme* $u : \mathrm{G}_{\mathrm{S}'} \to \mathrm{H}'$ *est une immersion.*

(12) N.D.E. : commentaires à ajouter ici, dont renvois à $\mathrm{VI}_{\mathrm{B}}\ldots$

(13) N.D.E. : Voir le théorème 4C dans : S. Anantharaman, *Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension* 1, Bull. Soc. Math. France, Mém. **33** (1976), 5-79.

C.5. L'exemple (XVII 6.4 a)) fournit un exemple de groupe lisse sur un corps k, dont le radical unipotent n'est pas défini sur k. La proposition suivante donne une méthode générale pour obtenir de tels groupes :

Proposition C.5.1. — *Soient k un corps, K une extension finie de k, radicielle, de degré > 1, H un K-groupe algébrique connexe, lisse, de dimension r, $\mathrm{G} = \prod_{\mathrm{K}/k} \mathrm{H}/\mathrm{K}$, qui est un k-groupe algébrique, lisse, connexe, de dimension $r[\mathrm{K} : k]$. Soient $u : \mathrm{G}_{\mathrm{K}} \to \mathrm{H}$ l'homomorphisme canonique, et $\mathrm{R} = \mathrm{Ker}(u)$. Alors :*

629 i) *Le morphisme u est un épimorphisme et R est un groupe algébrique, lisse, unipotent, connexe.*

ii) *Si U est un sous-groupe algébrique lisse de G, tel que U_{K} majore R, alors $\mathrm{U} = \mathrm{G}$.*

Corollaire. — *Gardons les notations de la proposition précédente.*

a) *Si H n'est pas unipotent, le radical unipotent de $\mathrm{G}_{\overline{k}}$ n'est pas défini sur k.*

b) *Si H est une variété abélienne, non nulle, G n'est pas extension d'une variété abélienne par un groupe linéaire lisse.*

c) *Si H n'est pas résoluble, le radical résoluble de $\mathrm{G}_{\overline{k}}$ n'est pas défini sur k, et G ne possède pas de sous-groupe de Borel défini sur k.*

Montrons d'abord comment le corollaire résulte de la proposition.

a) Soit U un radical unipotent de G. Alors U_{K} est le radical unipotent de G_{K}, donc majore R, puisque R est lisse unipotent connexe d'après i), donc $\mathrm{U} = \mathrm{G}$ d'après ii). Or G_{K} admet H comme quotient, et H n'est pas unipotent par hypothèse, donc G n'est pas unipotent, d'où une contradiction.

b) Si G est extension d'une variété abélienne par un groupe linéaire L, lisse sur k, nécessairement L_{K} majore R, donc $\mathrm{L} = \mathrm{G}$. Or G ne peut être un groupe linéaire puisque G_{K} possède un quotient qui est une variété abélienne non nulle.

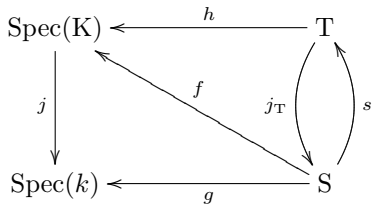
c) Soit S (resp. B) un radical résoluble de G (resp. un sous-groupe de Borel de G), alors S_{K} (resp. B_{K}) majore R, donc $\mathrm{S} = \mathrm{G}$ (resp. $\mathrm{B} = \mathrm{G}$). Mais alors G est résoluble, ce qui contredit le fait que G_{K} possède un quotient qui n'est pas résoluble.

Démonstration de la proposition 5.1 :

i) Commençons par décrire le morphisme u. La donnée d'un K-schéma

$$f : \mathrm{S} \longrightarrow \mathrm{Spec}(\mathrm{K})$$

630 permet de construire le diagramme :



où $g = j \circ f$, $\mathrm{T} = \mathrm{Spec}(\mathrm{K}) \times_{\mathrm{Spec}(k)} \mathrm{S}$, h et j_{T} sont les deux projections et s est la section de T au-dessus de S telle que $h \circ s = f$. L'application

$$u(\mathrm{S}) : \mathrm{G_K}(\mathrm{S}) \longrightarrow \mathrm{H}(\mathrm{S})$$

est simplement l'application composée :

$$\mathrm{G_K}(\mathrm{S}) \xrightarrow{\sim} \mathrm{H}(\mathrm{T}) \to \mathrm{H}(\mathrm{S}),$$

où la dernière flèche est définie par la section s.

Prenons en particulier pour S le spectre d'une clôture algébrique $\overline{k}$ de k et pour f l'unique k-morphisme $\mathrm{K} \to \overline{k}$, de sorte que T est un schéma local artinien. Pour prouver i) il suffit de le faire après extension $\mathrm{K} \to \overline{k}$ du corps de base. Or il est clair que $\mathrm{G_S} = \prod_{\mathrm{T/S}} \mathrm{H_T/T}$ représente le foncteur de Greenberg de $\mathrm{H_T}$ relativement à S (M. J. Greenberg, *Schemata over local rings*, Ann. of Maths. 73, 1961, p. 624-648). La description faite plus haut montre alors que, moyennant cette dernière identification, u_{S} est le morphisme de transition canonique :

$$\mathrm{Green}(\mathrm{H_T}) \longrightarrow \mathrm{H_S} = \mathrm{H_T} \times_{\mathrm{T}} \mathrm{S}.$$

L'assertion i) résulte alors du fait que H est lisse sur K et de (M. J. Greenberg, *Schemata over local rings* II, Ann. of Maths. 78, 1963, p. 256-266).

ii) Pour établir ii) nous pouvons supposer k séparablement clos. Soit donc U un sous-groupe algébrique lisse de G tel que $\mathrm{U_K} \supset \mathrm{R}$ et montrons que $\mathrm{U} = \mathrm{G}$. Comme **631**
G est connexe, on peut supposer U connexe. Soient V le sous-groupe algébrique lisse et connexe $u(\mathrm{U_K})$ de H et $\mathrm{V}' = \prod_{\mathrm{K}/k} \mathrm{V/K}$, qui est un sous-groupe algébrique lisse et connexe de G. Le groupe $\mathrm{V'_K}$ est un sous-groupe algébrique de $\mathrm{G_K}$ et le morphisme canonique $\mathrm{V'_K} \to \mathrm{V}$ est simplement la restriction de u à $\mathrm{V'_K}$. Par hypothèse, $\mathrm{U_K}$ majore R, a fortiori, $\mathrm{U_K}$ majore $\mathrm{Ker}(\mathrm{V'_K} \to \mathrm{V})$; d'autre part, par construction, l'image de $\mathrm{U_K}$ dans H est égale à V. On en déduit que $\mathrm{U_K}$ majore $\mathrm{V'_K}$, donc que U majore V'. D'autre part, l'isomorphisme canonique :

$$\mathrm{G}(k) \hookrightarrow \mathrm{G}(\mathrm{K}) \xrightarrow{u(\mathrm{K})} \mathrm{H}(\mathrm{K})$$

envoie évidemment $\mathrm{U}(k)$ dans $\mathrm{V}(\mathrm{K}) = \mathrm{V}'(k)$; c'est dire que $\mathrm{U}(k)$ est contenu dans $\mathrm{V}'(k)$. Comme U est lisse et k séparablement clos, cela entraîne $\mathrm{U} \subset \mathrm{V}'$, d'où $\mathrm{U} = \mathrm{V}'$. On a alors les égalités :

$$([\mathrm{K} : k] - 1) \dim \mathrm{V} = \dim \mathrm{Ker}(\mathrm{V'_K} \to \mathrm{V}) = \dim \mathrm{R} = ([\mathrm{K} : k] - 1) \dim \mathrm{H}.$$

Comme $\mathrm{K} \neq k$, on conclut que $\dim \mathrm{V} = \dim \mathrm{H}$, d'où $\mathrm{V} = \mathrm{H}$ et finalement $\mathrm{U} = \mathrm{V}' = \mathrm{G}$.