C. R. Acad. Sci. Paris, t. 328, Série I, p. 1123-1128, 1999
Théorie des groupes/*Group Theory*

Éléments unipotents des groupes algébriques semi-simples simplement connexes en caractéristique $p > 0$

Philippe GILLE

Département de mathématiques, CNRS, bâtiment 425, Université de Paris-Sud, 91405 Orsay cedex, France
Courriel : gille@math.u-psud.fr

(Reçu et accepté le 14 avril 1999)

Résumé. Soient k un corps de caractéristique $p > 0$ et G/k un groupe semi-simple simplement connexe. Nous démontrons le fait suivant conjecturé par Tits. Si $[k : k^p] \leq p$, alors tout sous-groupe de $G(k)$ constitué d'éléments unipotents est contenu dans le radical unipotent d'un k-sous-groupe parabolique de G. © Académie des Sciences/Elsevier, Paris

Unipotent elements of semisimple simply connected algebraic groups in characteristic $p > 0$

Abstract. *Let k be a field with positive characteristic $p > 0$ and let G/k be a simply connected semisimple group. We prove the following conjecture of Tits. If $[k : k^p] \leq p$, then any subgroup U of $G(k)$ consisting of unipotent elements is contained in the unipotent radical of a k-parabolic subgroup of G.* © Académie des Sciences/Elsevier, Paris

Abridged English Version

Let k be a field with positive characteristic $p > 0$ and k_s a separable closure of k. Let G/k be a semisimple simply connected algebraic group. A subgroup U of $G(k)$ is called unipotent if every element of U is unipotent. We prove the following result, conjectured by J. Tits:

THEOREM 1. – *Assume $[k : k^p] \leq p$. Then every unipotent subgroup U of $G(k)$ is contained in the unipotent radical of a k-parabolic subgroup of G.*

The case $p = 2$ is due to Tits [13], § 4.5, and the theorem was also known if p is not a torsion prime of G and if G has type A_n or C_n (loc. cit., § 3.5 and 4.4). One says that a k-closed unipotent U subgroup of G/k is k-embeddable in a Borel subgroup if there exists a k-Borel subgroup of G/k, which contains U. According to Proposition 3.6 of [1], an unipotent subgroup U of $G(k)$ is contained

Note présentée par Jean-Pierre SERRE.

in the unipotent radical of a k-parabolic subgroup of G if and only if each element is k_s-embeddable in a Borel subgroup. Using moreover Corollary 3.3 of [13], we are reduced to the following case: $k = k_s$, U is generated by an element u of order p, G/k is split and almost simple, G has not type C_n. Let us set $K = k((t))$ and denote by K_{mod} a maximal tamely ramified closure of K. The key point is to associate to u a cohomology class $\gamma_\chi(u) \in \mathrm{H}^1(K, G)$ in the following way: let $\chi \in \mathrm{H}^1(K, \mathbb{Z}/p\mathbb{Z})$ be a character such that the corresponding extension L/K is totally ramified (e.g. the Artin–Schreier extension $X^p - X = \frac{1}{t}$). Viewing u as a morphism $u : \mathbb{Z}/p\mathbb{Z} \to G$, one defines $\gamma_\chi(u) = u_*(\chi) \in \mathrm{H}^1(L/K, G) \subset \mathrm{H}^1(K, G)$. Using the Bruhat–Tits building of G on a suitable extension of L, we prove that the class $\gamma_\chi(u)_{K_{\text{mod}}} \in \mathrm{H}^1(K_{\text{mod}}, G)$ detects if u lies in a Borel subgroup. Kato's p-cohomological dimensions of k and K (*see* below) satisfy $\dim_p(k) \leq 1$ and $\dim_p(K) \leq 2$. The absolute Galois group $\mathrm{Gal}(K_{\text{mod}})$ is a p-group, hence $\mathrm{H}^1(K_{\text{mod}}, G) = 1$ by [7], and the proof is finished.

Introduction

Soient k un corps de caractéristique $p > 0$, k_s une clôture séparable de k et $\mathcal{G} = \mathrm{Gal}(k_s/k)$ le groupe de Galois absolu de k. Soit G/k un groupe semi-simple simplement connexe. Nous démontrons que si $[k : k^p] \leq p$, tout sous-groupe unipotent de $G(k)$ est contenu dans le radical unipotent d'un k-sous-groupe parabolique de G. Le cas $p = 2$ avait été démontré par Tits [13], § 4.5. Le théorème est également connu lorsque p n'est pas un entier de *torsion* de G et lorsque G est de type A_n ou C_n (loc. cit., § 3.5 et 4.4).

On dit qu'un sous-groupe unipotent k-fermé U de G est k-plongeable dans un sous-groupe de Borel s'il existe un k-sous-groupe de Borel B de G qui contient U. D'après la proposition 3.6 de [1], un sous-groupe unipotent de $G(k)$ est contenu dans le radical unipotent d'un k-sous-groupe parabolique de G si et seulement si tous ses éléments sont k_s-plongeables dans un sous-groupe de Borel. Cette propriété nous permet de travailler avec un seul élément unipotent u (que l'on peut supposer d'ordre p d'après le corollaire 3.3 de [13]) et de supposer G déployé et presque simple. Nous associons à un tel u deux invariants, un premier invariant $M_G(u)$ dans $K_2(k)/pK_2(k)$ et un second invariant de nature cohomologique $\gamma_\chi(u)$ dans $\mathrm{H}^1(k((t)), G)$. L'existence de tels invariants avait été pressentie par Serre ; les immeubles de Bruhat–Tits permettent de relier ces deux invariants et dans certains cas (*cf.* corollaire 2), l'invariant $M_G(u)$ détecte si u est k-plongeable dans un sous-groupe de Borel.

Notations

- $\mathrm{H}^i_{p^n}(k)$ $(n \geq 1)$ et $\mathrm{H}^i(k)\{p\} = \varinjlim_n \mathrm{H}^i_{p^n}(k)$: groupes de cohomologie de Kato [9], introduction ;
- $\dim_p(k)$ est la p-dimension cohomologique de Kato définie de la façon suivante : si $[k : k^p] = \infty$, on pose $\dim_p(k) = \infty$. Si $[k : k^p] = p^r$, on pose :
  - $\dim_p(k) = r$ si $\mathrm{H}^{r+1}_p(k') = 0$ pour toute extension finie k'/k,
  - $\dim_p(k) = r + 1$ sinon ;
- $K_2(k)$ est le second groupe de k-théorie de Milnor, i.e. le quotient du groupe abélien $k^\times \otimes_{\mathbb{Z}} k^\times$ par les relations $x \otimes (1 - x) = 0$ pour tout $x \in k^\times \setminus \{1\}$;
- pour tout caractère $\chi \in \mathrm{H}^1(k, \mathbb{Z}/p\mathbb{Z})$, on dispose du cup-produit $K_2(k) \xrightarrow{\chi \cup ?} \mathrm{H}^3_p(k)$ (ibid, § 2).

1. Invariants d'un élément unipotent d'ordre p

Dans les § 1 et § 2, on suppose G/k déployé, presque simple, de type distinct de C_n et k infini. Soient B/k un k-sous-groupe de Borel déployé de G/k et R_uB/k son radical unipotent.

1.1. L'obstruction $M_G(u)$

Le groupe $G(k)$ est presque simple et a fortiori parfait [4]. Matsumoto a démontré que

$$\mathrm{H}_2(G(k),\mathbb{Z}) = K_2(k)$$

et ainsi, on dispose de l'extension de Steinberg–Matsumoto [10], th. 5.10 :

$$(\mathcal{E}) \qquad 0 \longrightarrow K_2(k) \longrightarrow \mathrm{St}(G,k) \longrightarrow G(k) \longrightarrow 1,$$

où $\mathrm{St}(G,k)$ désigne le groupe de Steinberg de G et de k. On note $[\mathcal{E}] \in \mathrm{H}^2(G(k), K_2(k))$ la classe de cette extension universelle. Soit $u \in G(k)$ un élément unipotent d'ordre p, que l'on voit comme un morphisme $u : \mathbb{Z}/p\mathbb{Z} \to G(k)$. On définit l'obstruction $M_G(u) \in K_2(k)/pK_2(k)$ par :

$$M_G(u) := u^*\big([\mathcal{E}]\big) \in \mathrm{H}^2(\mathbb{Z}/p\mathbb{Z}, K_2(k)) = K_2(k)/pK_2(k).$$

Par construction, la restriction de l'extension $\mathcal{E}$ à $R_uB(k)$ est triviale ; si l'élément u est k-plongeable dans un sous-groupe de Borel, c'est-à-dire inclus dans un conjugué de $R_uB(k)$, on a $M_G(u) = 0$. L'élément $M_G(u)$ est donc une obstruction pour le plongement de u dans le radical unipotent d'un sous-groupe de Borel de G.

1.2. Lien avec la cohomologie galoisienne

Soit $K = K((t))$, soient K_s une clôture séparable et $K_{\mathrm{mod}} \subset K_s$ l'extension modérément ramifiée maximale de k. Soit L/K une extension cyclique d'ordre p totalement ramifiée, d'anneau de valuation O_L (par exemple donnée par l'équation d'Artin-Schreier $X^p - X = \frac{1}{t}$). Soit σ un générateur de $\Gamma = \mathrm{Gal}(L/K)$ et soit $\chi \in \mathrm{Hom}_c(\mathrm{Gal}(K_s/K), \mathbb{Z}/p\mathbb{Z}) = \mathrm{H}^1(K, \mathbb{Z}/p\mathbb{Z})$ le caractère correspondant à L/K. On définit le 1-cocycle f_u à valeurs dans $G(k)$ par $f_u(\sigma^i) = u^i$ pour tout $i \in \mathbb{Z}/p\mathbb{Z}$. On définit la classe de cohomologie galoisienne :

$$\gamma_\chi(u) := u_*(\chi) \in \mathrm{H}^1(\Gamma, G(L)) \subset \mathrm{H}^1(K,G),$$

qui est représentée par le cocycle f_u. On note $\mathrm{r}_K : \mathrm{H}^1(K,G) \to \mathrm{H}^3(K)\{p\}$ l'invariant de Rost p-primaire de G/K défini dans l'appendice B de [5]. Un calcul fondé sur [6] donne la formule :

$$\mathrm{r}_K\big(\gamma_\chi(u)\big) = \chi \cup M_G(u) \ \text{ dans } \ \mathrm{H}^3_p(K) \subset \mathrm{H}^3(K). \qquad (*)$$

2. Techniques immobilières

Le point-clef se trouve dans la proposition suivante où l'on montre que la classe $\gamma_\chi(u)$ détecte si u est k-plongeable dans un sous-groupe de Borel de G.

PROPOSITION 1. – *Les propriétés suivantes sont équivalentes :*
(i) *u est k-plongeable dans un sous-groupe de Borel,*
(ii) *$\gamma_\chi(u) = 1$ dans $\mathrm{H}^1(K,G)$,*
(iii) *$\gamma_\chi(u)_{K_{\mathrm{mod}}} = 1$ dans $\mathrm{H}^1(K_{\mathrm{mod}},G)$.*

Démonstration. – (i)$\Longrightarrow$(ii) : Quitte à conjuguer, on peut supposer $u \in R_uB(k) \subset R_uB(L)$. Comme R_uB est déployé, on sait que $\mathrm{H}^1(K, R_uB) = 1$, donc $\gamma_\chi(u) = 1$. L'assertion (ii)$\Longrightarrow$(iii) est évidente.

(iii) $\Longrightarrow$ (i) : Par hypothèse, il existe une extension modérément ramifiée K'/K d'anneau de valuation O'/O et d'extension résiduelle séparable k'/k telle que $\gamma_\chi(u)_{K'} = 1$ dans $\mathrm{H}^1(K', G)$. On note $L' = L \cdot K'/K'$ qui est galoisienne de groupe $\Gamma = \mathrm{Gal}(L'/K') = \langle \sigma \rangle$ et d'anneau de valuation $O_{L'}$. On considère l'immeuble de Bruhat–Tits $\mathcal{I}$ du groupe $G_{L'}$ [2], § I.7.4. Cet immeuble est muni d'une action du groupe $G(L')$ et d'une action du groupe Γ; on note $x \mapsto {}^\sigma x$ l'action du générateur σ. On désigne par c le centre de l'immeuble, i.e. le point de $\mathcal{I}$ dont le fixateur dans $G(L')$ est $G(O_{L'})$. On note F_0 la chambre standard de $\mathcal{I}$, i.e. la chambre dont le fixateur est $\mathfrak{B}(O_{L'})$, où $\mathfrak{B}_{/\mathrm{Spec}(O_{L'})}$ désigne le sous-groupe d'Iwahori standard ; le groupe $\mathfrak{B}(O_{L'}) \subset G(L')$ est l'image inverse de $B(k')$ par l'homomorphisme $G(O_{L'}) \to G(k')$. Le centre c et la chambre F_0 sont fixés par σ. Soit $[f_u]$ la classe du cocycle f_u dans $\mathrm{H}^1(\Gamma, G(O_{L'}))$.

Lemme 3

$$[f_u] \in \mathrm{Im}\Big(\mathrm{H}^1(\Gamma, \mathfrak{B}(O_{L'})) \to \mathrm{H}^1(\Gamma, G(O_{L'}))\Big).$$

Montrons tout d'abord que ce lemme entraîne l'assertion (i). En effet, il existe alors $h \in G(O_{L'})$ tel que $hu({}^\sigma \mathrm{H}^{-1}) \in \mathfrak{B}(O_{L'})$. Soit $\overline{h}$ l'image de h dans $G(k')$. Alors $\overline{h}\, u(\overline{h})^{-1} \in B(k')$ (on a utilisé ici que L'/K' est totalement ramifiée puisque L/K l'est). L'extension k'/k est séparable, l'élément u est donc contenu dans le radical unipotent d'un k-sous-groupe parabolique propre de G d'après la proposition 3.1 de [1], et puisque G est déployé, est donc k-plongeable dans un sous-groupe de Borel de G.

Montrons le lemme. On définit une action tordue de Γ sur $\mathcal{I}$ par

$$\sigma \cdot x = u \cdot {}^\sigma x.$$

Par hypothèse, il existe $g \in G(L)$ satisfaisant

$$u = g^{-1\sigma} g.$$

Soit F la chambre $g^{-1}F_0$. Elle est fixée points par points pour cette action tordue de Γ. En effet, pour tout $x = g^{-1}x_0 \in F$, comme ${}^\sigma x_0 = x_0$, on a

$$\sigma \cdot x = u\big({}^\sigma(g^{-1} \cdot x_0)\big) = u({}^\sigma g)^{-1} \cdot x_0 = x.$$

On remarque que u appartient à $G(k)$, le point c est donc fixé par σ pour l'action tordue. L'ensemble de points fixes $\mathcal{I}^\sigma$ est un sous-complexe fermé convexe et contient à la fois c et F. Un sous-complexe convexe et fermé contenant une chambre est réunion d'adhérences de chambres ; on en déduit qu'il existe une chambre F' de $\mathcal{I}$ fixée par σ pour l'action tordue dont l'adhérence contient le point c. On considère maintenant l'*étoile* $\mathrm{Star}(c)$ de c dans $\mathcal{I}$, qui s'identifie à l'immeuble sphérique de G/k' [2], § II.4.6.33. Le groupe $G(k')$ agit transitivement sur l'ensemble des chambres de $\mathrm{Star}(c)$, c'est-à-dire sur l'ensemble des chambres de $\mathcal{I}$ contenant c. D'après le lemme de Hensel, l'homomorphisme $G(O_{L'}) \to G(k')$ est surjectif, donc le groupe $G(O_{L'})$ agit transitivement sur les chambres de $\mathrm{Star}(c)$. Il existe donc un élément $h \in G(O_{L'})$ tel que $F' = h \cdot F_0$. Soit $x = h \cdot x_0 \in F'$; on a :

$$\mathrm{h}^{-1}u({}^\sigma h) \cdot x_0 = h^{-1} \cdot \big(\sigma \cdot (h \cdot x_0)\big) = h^{-1} \cdot (h \cdot x_0) = x_0.$$

Ceci montre que l'élément $h^{-1}u({}^\sigma h)$ fixe points par points la chambre F_0, donc $h^{-1}u({}^\sigma h)$ appartient à $\mathfrak{B}(O_{L'})$. On en conclut que $[f_u]$ provient de $\mathrm{H}^1(\Gamma, \mathfrak{B}(O_{L'}))$. □

Le groupe d'inertie sauvage $\mathrm{Gal}(K_s/K)$ est un pro-p-groupe. Si p n'est pas un entier de torsion de G, on sait que $\mathrm{H}^1(K_{\mathrm{mod}}, G) = 1$ [12], th. 4", et ainsi la proposition permet de retrouver le résultat de Tits. Le corollaire suivant résulte immédiatement de la proposition et de la formule (*) du § 1.2.

COROLLAIRE 1. – *On suppose que l'invariant de Rost (p-primaire)*

$$\mathrm{r}_{K_{\mathrm{mod}}} : \mathrm{H}^1(K_{\mathrm{mod}}, G) \longrightarrow \mathrm{H}^3(K_{\mathrm{mod}})\{p\}$$

a un noyau trivial. Alors pour tout élément unipotent u de $G(k)$, les conditions suivantes sont équivalentes :

(i) $M_G(u) = 0$ *dans* $K_2(k)/pK_2(k)$,

(ii) u *est k-plongeable dans un sous-groupe de Borel.*

La condition sur l'invariant de Rost est vérifiée dans les cas suivants D_4, G_2, F_4 si $p = 2$, F_4 si $p = 3$ et E_8 si $p = 5$ (*voir* [6], [12]). Notons que le cas E_8, $p = 5$ est la version en caractéristique 5 d'un théorème de Chernousov [3].

COROLLAIRE 2. – *Notons X le type de G. On suppose que $X = D_4$, F_4, ou G_2 si $p = 2$, $X = F_4$ si $p = 3$ et $X = E_8$ si $p = 5$. Alors pour tout élément unipotent u de $G(k)$ d'ordre p, les conditions suivantes sont équivalentes :*

(i) $M_G(u) = 0$ *dans* $K_2(k)/pK_2(k)$,

(ii) u *est k-plongeable dans un sous-groupe de Borel.*

Cela résulte du corollaire 1.

3. Preuve de la conjecture de Tits

On ne suppose plus ici que G/k est déployé ; il est loisible de supposer G/k absolument presque k-simple. Dans son exposé [12], Serre suggère la version suivante en caractéristique p positive de la conjecture II [11], § III.3.

CONJECTURE II. – *On note $S(G)$ l'ensemble des premiers de torsion de G* [12]. *Pour tout premier $\ell \in S(G)$, on fait l'hypothèse suivante :*

a) *si ℓ est inversible dans k, $cd_\ell(k) \leq 2$,*

b) *si $\ell = p$, pour toute extension* séparable *k'/k, le groupe de cohomologie $\mathrm{H}^3_p(k')$ de Kato est nul.*

Alors $\mathrm{H}^1(k, G) = 1$.

Pour les corps de fonctions de courbes sur les corps finis, la conjecture est vraie d'après Harder [8]. Cette conjecture est vraie pour les groupes de type ${}^1A_n$ (théorème de Merkurjev–Suslin si $(n + 1, p) = 1$ et [6] sinon), F_4 et G_2 d'après Serre (*voir* [6], [12]). Le résultat principal de [7] est le suivant :

THÉORÈME 1. – *Dans les cas suivants :*

1) *G est quasi-déployé et n'est pas de type E_8,*

2) *le groupe G est de type E_8 et $\mathrm{Gal}(k_s/k)$ est un pro-ℓ-groupe (ℓ premier),*

la conjecture II *est vraie.*

Nous allons voir que ce résultat et la proposition entraînent le :

THÉORÈME 2. – *On suppose $[k : k^p] \leq p$. Tout sous-groupe unipotent U de $G(k)$ est contenu dans le radical unipotent d'un k-sous-groupe parabolique de G.*

Démonstration. – D'après la proposition 3.1 de [1], on peut supposer $k = k_s$, et le corollaire 3.3 de [13] nous permet de supposer que U est engendré par un élément u d'ordre p. De plus, on peut supposer que k est infini et que G n'est pas de type C_n. Comme k est séparablement clos, on a ${}_p\mathrm{Br}(k') = \mathrm{H}^2_p(k') = 0$ pour toute extension finie k'/k, et donc $\dim_p(k) \leq 1$. Notant toujours $K = k((t))$, on sait que $\dim_p(K) \leq 2$ ([9], corollaire au th. 3) et par définition, on a $\mathrm{H}^3_p(K') = 0$ pour toute extension finie K'/K. Comme le groupe d'inertie sauvage $\mathrm{Gal}(K_s/K_{\mathrm{mod}})$ est un pro-p-groupe, le théorème précédent entraîne

$$\mathrm{H}^1(K_{\mathrm{mod}}, G) = 1.$$

La proposition montre alors que l'élement u est k-plongeable dans un sous-groupe de Borel. □

Remerciements. Cette Note est l'aboutissement de conversations avec Jean-Pierre Serre suite au cours de Jacques Tits sur les mauvais éléments unipotents des groupes algébriques linéaires. Je les remercie vivement tous les deux.

Références bibliographiques

[1] Borel A., Tits J., Éléments unipotents et sous-groupes paraboliques des groupes réductifs, Invent. Math. 12 (1971) 95–104.
[2] Bruhat F., Tits J., Groupes réductifs sur un corps local, I, Publ. Math. IHES 41 (1972) 5–252 ; II, Publ. Math. IHES 60 (1984).
[3] Chernousov V., Remark on the Serre mod-5 invariant for groups of type E_8, Math. Zametki 56 (1) (1994) 116–121 ; traduction anglaise : Math. Notes 56 (1) (1994) 730–733.
[4] Chevalley C., Sur certains groupes simples, Tohoku Math. J. 7 (1955) 14–66.
[5] Esnault H., Kahn B., Levine M., Viehweg E., The Arason invariant and mod 2 algebraic cycles, J. Amer. Math. Soc. 11 (1) (1998) 73–118.
[6] Gille P., Invariants cohomologiques de Rost en caractéristique positive, prépublication, 1998.
[7] Gille P., Cohomologie galoisienne des groupes quasi-déployés sur des corps de dimension cohomologique ≤ 2, prépublication, 1998.
[8] Harder G., Über die Galoiskohomologie halbeinfacher Matrizengruppen III, J. für die Reine und Angew. Math. 274/5 (1975) 125–138.
[9] Kato K., Galois cohomology of complete discrete valuation fields, Lect. Notes in Math. 967, Springer-Verlag, 1982, pp. 215–238.
[10] Matsumoto I., Sur les sous-groupes arithmétiques des groupes semi-simples déployés, Ann. Sci. Éc. Norm. Sup. 2 (1969) 1–62.
[11] Serre J.-P., Cohomologie galoisienne, Lect. Notes in Math. 5, 5ième édition, Springer-Verlag, 1994.
[12] Serre J.-P., Cohomologie galoisienne : progrès et problèmes, Séminaire Bourbaki, exposé 783 (1993-94), Astérisque 227, 1995.
[13] Tits J., Unipotent elements and parabolic subgroups of reductive groups. II, Lect. Notes in Math. 1271, Springer-Verlag, 1986, pp. 33–62.