Astérisque

JEAN-PIERRE SERRE

Sous-groupes finis des groupes de Lie

Astérisque, tome 266 (2000), Séminaire Bourbaki,
exp. n° 864, p. 415-430

<http://www.numdam.org/item?id=SB_1998-1999__41__415_0>

Séminaire BOURBAKI
51ème année, 1998-99, n° 864

Juin 1999

SOUS-GROUPES FINIS DES GROUPES DE LIE

par **Jean–Pierre SERRE**

INTRODUCTION

Les sous-groupes finis du groupe des rotations $\mathrm{SO}_3(\mathbf{R})$ sont bien connus. Ce sont :

les groupes cycliques C_n d'ordre $n = 1, 2, \ldots$;

les groupes diédraux D_n d'ordre $2n$, $n = 2, 3, \ldots$;

le groupe alterné Alt_4 d'ordre 12 ;

le groupe symétrique Sym_4 d'ordre 24 ;

le groupe alterné Alt_5 d'ordre 60.

On aimerait avoir une liste analogue pour d'autres groupes de Lie compacts, ou d'autres groupes algébriques (en caractéristique zéro, et même en caractéristique > 0). Ce serait utile pour beaucoup de questions (représentations ℓ-adiques, par exemple). Bien sûr, c'est trop demander, vu que tout groupe fini se plonge dans un groupe unitaire convenable ! On va voir que l'on peut tout de même dire pas mal de choses si l'on se borne à des groupes finis qui sont, soit abéliens, soit simples.

HYPOTHÈSES ET NOTATIONS

Plutôt que de travailler dans la catégorie des groupes de Lie compacts, on préfère se placer dans celle des groupes réductifs complexes. Cela ne change rien : on sait que, si K est un groupe de Lie compact, il possède un complexifié G qui est un groupe réductif sur $\mathbf{C}$; le groupe K est un sous-groupe compact maximal de $G(\mathbf{C})$. Tout sous-groupe fini de $G(\mathbf{C})$ est conjugué à un sous-groupe de K ; de plus, K "contrôle la fusion de K dans $G(\mathbf{C})$" au sens suivant : si A, B sont deux sous-groupes de K, et si $g \in G(\mathbf{C})$ est tel que $gAg^{-1} = B$, il existe un élément g_0 de K tel que $g_0 a g_0^{-1} = gag^{-1}$ pour tout $a \in A$ (cela se déduit de la décomposition de Cartan de $G(\mathbf{C})$).

(Dans le cas particulier $K = \mathrm{SO}_3(\mathbf{R})$, on a $G = \mathrm{PGL}_2$, de sorte que les groupes $C_n, D_n, \ldots, \mathrm{Alt}_5$ s'interprètent comme des sous-groupes finis de $\mathrm{PGL}_2(\mathbf{C})$, c'est-à-dire

comme des groupes finis d'automorphismes de la droite projective.)

Dans ce qui suit, on adoptera le point de vue des groupes algébriques (qui a, entre autres avantages, celui de permettre des réductions modulo p). On fixe un corps k algébriquement clos de caractéristique zéro, ainsi qu'un groupe réductif connexe G défini sur k ; on se permet d'identifier G à $G(k)$. Le cas le plus intéressant est celui où G est "presque simple", i.e. semi-simple à système de racines irréductible ; le groupe adjoint G^{ad} est alors un groupe simple, au sens usuel du terme.

1. LE CAS (PRESQUE) ABÉLIEN

Lorsque $G = \mathrm{PGL}_2$ les sous-groupes abéliens finis de G sont les groupes cycliques C_n et le groupe diédral D_2 qui est abélien élémentaire de type $(2,2)$. Les C_n sont contenus dans un tore maximal, alors que D_2 ne l'est pas ; le nombre premier $p = 2$ joue donc un rôle particulier pour PGL_2. Nous allons trouver une situation analogue dans le cas général.

1.1. Sous-groupes toraux

Un sous-groupe fini A de G est dit *toral* s'il est contenu dans un tore maximal T de G. La structure d'un tel sous-groupe est évidente : si $r = \dim T$ est le rang de G, A peut être engendré par r éléments ; inversement, tout groupe abélien ayant cette propriété est isomorphe à un sous-groupe toral de G.

Soit $N = N_G(T)$ le normalisateur de T dans G. Le quotient $W = N/T$ est le *groupe de Weyl* de G (plus correctement : du couple (G,T)). Ce groupe opère sur T par conjugaison, et il contrôle la fusion de T dans G :

1.1.1. *Si A et B sont des sous-groupes de T, et si $g \in G$ est tel que $gAg^{-1} = B$, il existe $w \in W$ tel que $w(a) = gag^{-1}$ pour tout $a \in A$.*

Cet énoncé est l'exact analogue d'un théorème de Burnside sur les sous-groupes du centre d'un p-groupe de Sylow. Il se démontre de la même manière : on remarque que T et $g^{-1}Tg$ sont des tores maximaux du centralisateur $Z_G(A)$ de A, donc sont conjugués par $Z_G(A)$. Cela permet de remplacer g par un élément de N ; d'où le résultat cherché.

Les groupes abéliens ayant très peu de générateurs sont toraux :

1.1.2. *Soit A un sous-groupe abélien fini de G. Alors A est toral dans chacun des deux cas suivants :*

a) *A est cyclique ;*

b) *G est simplement connexe, et A est engendré par deux éléments.*

Le cas a) est immédiat : tout élément d'ordre fini est semi-simple, donc contenu dans un tore maximal. Dans le cas b), supposons A engendré par x, y. Du fait que G est simplement connexe, le centralisateur $Z_G(x)$ est connexe. Le même argument que dans a) montre qu'il existe un tore maximal T de $Z_G(x)$ qui contient y. Ce tore est un tore maximal de G et il contient x, donc A.

1.2. Plongements dans N

À défaut de pouvoir plonger un groupe abélien fini dans un tore maximal, on peut essayer de le plonger dans le normalisateur d'un tel tore. C'est toujours possible. Plus généralement (cf. Borel-Serre [6], Borel-Mostow [5] et Springer-Steinberg [33], II.5.6) :

1.2.1. *Soit A un sous-groupe fini hyper-résoluble de G. Il existe un tore maximal T de G dont le normalisateur N contient A.*

Rappelons qu'un groupe A est dit hyper-résoluble ("supersolvable") s'il admet une suite de composition :

$$1 = A_0 \subset A_1 \subset \ldots \subset A_n = A,$$

où les A_i sont normaux dans A, et A_i/A_{i-1} est cyclique pour tout $i \geq 1$. On a les implications :

$$\text{abélien} \Longrightarrow \text{nilpotent} \Longrightarrow \text{hyper-résoluble} \Longrightarrow \text{résoluble}.$$

Voici une application simple de 1.2.1 :

1.2.2. *Soit p un nombre premier ne divisant pas l'ordre du groupe de Weyl W. Si A est un p-groupe contenu dans G, A est abélien et toral.*

En effet, on peut supposer, d'après 1.2.1, que A est contenu dans N. Vu l'hypothèse faite sur p, son image dans $W = N/T$ est triviale. Il est donc contenu dans T.

Remarque : Le groupe N est une extension, en général non triviale, de W par T. On trouvera dans Tits ([35],[36]) une description de cette extension, en termes d'un certain groupe fini $N_{\mathbf{Z}}$ défini explicitement par générateurs et relations ; voir aussi Bourbaki, LIE IX, p. 115, exerc. 12.

1.3. Nombres premiers de torsion

(Références : Borel [4], Steinberg [34] et Bourbaki, LIE IX, p. 120-121, exerc. 7 à 12.)

Un nombre premier p est dit *de torsion* (pour G) s'il vérifie les conditions équivalentes suivantes :

a) *Il existe un p-sous-groupe abélien de G qui n'est pas toral.*

a') *Il existe un p-sous-groupe abélien élémentaire de G, de rang ≤ 3, qui n'est pas toral.*

On note $\mathrm{Tors}(G)$ l'ensemble de ces nombres premiers ; d'après 1.2.2, c'est un sous-ensemble de l'ensemble des diviseurs premiers de l'ordre de W. Dans le cas particulier où $G = \mathrm{PGL}_2$, on a $\mathrm{Tors}(G) = \{2\}$.

Le terme de "torsion" provient du résultat suivant, dans lequel je suppose que $k = \mathbf{C}$ (sinon il faut faire intervenir la cohomologie étale) :

1.3.1. (cf. [4],[34]) *Pour que p appartienne à $\mathrm{Tors}(G)$, il faut et il suffit que l'un des groupes d'homologie $H_i(G, \mathbf{Z})$ contienne un élément d'ordre p.*

(Noter qu'il revient au même de considérer l'homologie de $G = G(\mathbf{C})$ ou celle d'un compact maximal K, car $G(\mathbf{C})$ et K ont même type d'homotopie.)

On trouvera dans [4] et [34] une longue liste de propriétés caractérisant les éléments de $\mathrm{Tors}(G)$. En voici quelques-unes :

1.3.2. *On a $\mathrm{Tors}(G) = \mathrm{Tors}(G')$, où G' est le groupe dérivé de G.*

Comme G' est semi-simple, cela ramène l'étude de $\mathrm{Tors}(G)$ au cas où G est semi-simple. Dans ce cas, notons $\overline{G}$ le revêtement universel de G, notons $\pi_1(G)$ le noyau de $\overline{G} \to G$ et soit $\mathrm{Tors}(\pi_1(G))$ l'ensemble des nombres premiers qui divisent l'ordre du groupe fini $\pi_1(G)$. Alors :

1.3.3. *On a $\mathrm{Tors}(G) = \cup_H \mathrm{Tors}(\pi_1(H'))$, où H parcourt les sous-groupes réductifs connexes de G ayant même rang que G.*

1.3.4. *On a $\mathrm{Tors}(G) = \mathrm{Tors}(\overline{G}) \cup \mathrm{Tors}(\pi_1(G))$.*

Cet énoncé ramène la détermination de $\mathrm{Tors}(G)$ au cas où G est simplement connexe. En utilisant 1.3.3, on en déduit (cf. [4],[34]) :

1.3.5. *Supposons G simplement connexe et presque simple. Soit (α_i) une base de son système de racines, soit β la plus grande racine, et écrivons la racine duale $\beta^\vee$ de β sous la forme :*

$$\beta^\vee = \sum n_i \alpha_i^\vee,$$

où les n_i sont des entiers > 0. Alors, pour que p soit de torsion pour G, il faut et il suffit qu'on ait $p \leq \sup(n_i)$.

D'où :

1.3.6. *Supposons G simplement connexe et presque simple. Alors :*

$\mathrm{Tors}(G) = \emptyset$ *si G est de type A_n ou C_n ;*

$\mathrm{Tors}(G) = \{2\}$ *si G est de type B_n $(n \geq 3)$, D_n $(n \geq 4)$ ou G_2 ;*

$\mathrm{Tors}(G) = \{2, 3\}$ *si G est de type F_4, E_6 ou E_7 ;*

$\mathrm{Tors}(G) = \{2, 3, 5\}$ *si G est de type E_8.*

1.4. Exemples de groupes abéliens élémentaires non toraux

(Références : Adams [1], Borel [4], Borel–Serre [6], Cohen-Seitz [10], Steinberg [34] et (surtout) Griess [17].)

Je me borne à deux exemples, l'un relatif à $p = 2$ et l'autre à $p = 5$.

1.4.1. Supposons que -1 appartienne au groupe de Weyl W ; c'est le cas pour les groupes de type A_1, B_n, C_n, D_n (n pair), G_2, F_4, E_7, E_8. Soit $g \in N$ un représentant de l'élément -1 de W. On peut montrer que g^2 est d'ordre 1 ou 2, et appartient au centre de G. Supposons que $g^2 = 1$ (c'est le cas si G est de type adjoint). Soit A le groupe engendré par g et par les éléments d'ordre 2 de T ; c'est un groupe abélien élémentaire d'ordre 2^{n+1}, où n est le rang de G, i.e. la dimension de T. *Ce groupe n'est pas toral* ; on peut même montrer que son centralisateur $Z_G(A)$ est fini.

Lorsque G est PGL_2, le groupe A est le groupe diédral D_2. Lorsque G est de type G_2, F_4 ou E_8, A est d'ordre 2^3, 2^5, 2^9 ; de tels sous-groupes jouent un grand rôle dans la cohomologie (usuelle – ou galoisienne) du groupe G. Noter que, dans ces trois cas, A est un sous-groupe élémentaire *maximal* de G : de façon générale, si G est simplement connexe, les p-sous-groupes abéliens de G sont de rang $\leq n+1$ si $p = 2$, et de rang $\leq n$ si $p > 2$, cf. Borel [4] et Cohen-Seitz [10].

1.4.2. Le groupe $G = E_8$ contient un élément z d'ordre 5 dont le centralisateur $Z_G(z)$ est de la forme $G_1 \cdot G_2$, où G_1 et G_2 sont isomorphes à SL_5, commutent, et ont pour intersection $\langle z \rangle$ (cela se déduit du diagramme de Dynkin complété de E_8 en remarquant que, si l'on en retranche la racine simple qui a le coefficient 5 dans la plus grande racine, on trouve deux diagrammes de type A_4). Dans $G_1 = \mathrm{SL}_5$, il est facile de trouver des éléments x_1 , y_1 d'ordre 5 tels que $x_1 y_1 x_1^{-1} y_1^{-1} = z$; de même, il existe dans G_2 des éléments x_2 , y_2 d'ordre 5 tels que $x_2 y_2 x_2^{-1} y_2^{-1} = z^{-1}$. Si l'on pose $x = x_1 x_2$ et $y = y_1 y_2$, on constate que le groupe $A = \langle x, y, z \rangle$ est abélien élémentaire d'ordre 5^3. *Ce groupe n'est pas toral* ; on peut même montrer que $Z_G(A)$ est égal à A.

1.5. Relations entre cohomologie galoisienne et sous-groupes non toraux

Qu'il existe de telles relations est connu depuis longtemps. Voici deux exemples :

1.5.1 (Grothendieck [23]). *Les deux propriétés suivantes sont équivalentes* :

a) $\mathrm{Tors}(G) = \emptyset$ (cela équivaut à dire que tout sous-groupe abélien de G est toral).

b) $H^1(K, G) = 0$ *pour toute extension* K *de* k.

(Pour la définition de $H^1(K, G)$, voir par exemple [30].)

Lorsque G est semi-simple, ces propriétés sont satisfaites si et seulement si G est un produit de groupes simplement connexes de type A ou C, cf. § 1.3. Un tel groupe

est parfois dit "spécial".

1.5.2. *Supposons que G soit égal à PGL_2, ou soit de type G_2. Soit A le 2-sous-groupe élémentaire non toral de G défini dans* 1.4.1. *Alors, pour toute extension K de k, l'application $H^1(K,A) \to H^1(K,G)$ est surjective.*

Noter que $H^1(K,A)$ n'est autre que $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), A)$. Dans le cas de PGL_2, les éléments de $H^1(K,A)$ peuvent donc s'interpréter comme des couples (λ,μ) d'éléments de K^*/K^{*2} et l'élément correspondant de $H^1(K,\mathrm{PGL}_2)$ est l'algèbre de quaternions définie par deux générateurs i et j soumis aux relations

$$i^2 = \lambda\ , \quad j^2 = \mu\ , \quad ij = -ji.$$

Même chose pour G_2, les quaternions étant remplacés par les octonions.

L'énoncé 1.5.2, pour agréable qu'il soit, ne donne pas de moyen de prouver la non trivialité des éléments de $H^1(K,G)$ ainsi obtenus ; il faut le compléter par la construction d'*invariants cohomologiques*, cf. [30], §§ 6,7 et n et Youssin [29] ont obtenu un résultat bien plus satisfaisant. Pour le formuler, il faut d'abord définir la *dimension essentielle* $\mathrm{ed}(x)$ d'un élément x de $H^1(K,G)$: c'est la borne inférieure des degrés de transcendance sur k des sous-extensions K' de K telles que x appartienne à l'image de $H^1(K',G) \to H^1(K,G)$. (En termes plus géométriques – et plus vagues – c'est le nombre minimum de paramètres dont on a besoin pour écrire le G-torseur x.) La borne supérieure des $\mathrm{ed}(x)$, quand K et x varient, est la *dimension essentielle* de G ; elle est notée $\mathrm{ed}(G)$. Nous pouvons maintenant énoncer le théorème principal de [29] :

1.5.3. *Si G contient un p-sous-groupe abélien élémentaire A dont le centralisateur est fini, on a* $\mathrm{ed}(G) \geq \mathrm{rang}(A)$.

En combinant cet énoncé avec 1.4.1, on obtient :

1.5.4. *On a* $\mathrm{ed}(E_7^{\mathrm{ad}}) \geq 8$ et $\mathrm{ed}(E_8) \geq 9$.

Ainsi, il existe des E_8-torseurs dont la construction exige au moins 9 paramètres !

Remarques

1) L'hypothèse faite sur A dans 1.5.3 est équivalente à dire que A n'appartient à aucun sous-groupe parabolique propre de G. Elle entraîne que A n'est pas toral.

2) L'énoncé démontré dans [29] est plus précis que 1.5.3 ; c'est :

$$\mathrm{ed}(G;p) \geq \mathrm{rang}(A),$$

où $\mathrm{ed}(G;p)$ est la dimension essentielle de G "en p" (i.e. en considérant comme négligeables les extensions de corps de degré premier à p).

3) Les démonstrations de [29] utilisent la *résolution des singularités* (sous forme équivariante). Elles ne s'étendent pas, pour l'instant, aux corps de caractéristique $\neq 0$.

2. LE CAS (PRESQUE) SIMPLE

On va maintenant s'intéresser aux plongements d'un groupe simple (fini, non abélien) dans G.

Il est commode de considérer, plus généralement, les plongements des groupes $\overline{S}$ qui sont des extensions centrales de S (on peut imposer à $\overline{S}$ d'être égal à son groupe dérivé, cela ne change rien). Exemple typique :

$$S = L_2(q) = \mathrm{PSL}_2(\mathbf{F}_q) \quad \text{et} \quad \overline{S} = 2 \cdot L_2(q) = \mathrm{SL}_2(\mathbf{F}_q)\ , \qquad q \text{ impair.}$$

(Les notations $L_2(q)$ et $2 \cdot L_2(q)$ sont celles de l'ATLAS [15].)

Un plongement d'un tel groupe $\overline{S}$ dans G est appelé un *plongement projectif* de S. Le principal avantage de cette notion est la propriété d'invariance suivante : si $G' \to G$ est une isogénie, S a un plongement projectif dans G si et seulement si il a un plongement projectif dans G'.

Lorsque S et G sont donnés, et que G est un groupe classique, l'examen de la table des caractères de S (et de ses extensions centrales) permet de décider si S a un plongement (ou un plongement projectif) dans G ; c'est clair lorsque G est de type A_n, et c'est facile pour les types B_n, C_n, D_n. Une méthode analogue s'applique à G_2 (en utilisant sa représentation irréductible de degré 7 et la forme trilinéaire alternée correspondante), cf. Aschbacher [2] et Cohen–Wales [11]. Les types F_4, E_6, E_7, E_8 sont plus difficiles ; ce n'est que récemment (Griess–Ryba [22]) que la liste des S possibles a été complétée. Avant de donner cette liste (que l'on trouvera au § 2.4), je vais parler du cas $S = L_2(q)$, qui est le seul où l'on ait des énoncés généraux, i.e. valables aussi bien pour les groupes classiques que pour les groupes exceptionnels.

2.1. Plongements projectifs de $L_2(q)$ dans G ; énoncé du résultat

On suppose $q > 2$. Le groupe $S = L_2(q) = \mathrm{PSL}_2(\mathbf{F}_q)$ est alors un groupe simple (sauf si $q = 3$, où c'est le groupe Alt_4), et toute extension centrale $\overline{S}$ de S, égale à son groupe dérivé, est isomorphe, soit à $2 \cdot S = \mathrm{SL}_2(\mathbf{F}_q)$, soit à S (sauf si $q = 4$ ou 9). On va donc s'intéresser aux homomorphismes

$$f : \mathrm{SL}_2(\mathbf{F}_q) \longrightarrow G$$

de noyau égal à 1 ou à (± 1). Un tel homomorphisme sera dit *non dégénéré*.

Écrivons q sous la forme p^e, avec p premier, $e \geq 1$. Le p-groupe de Sylow $U = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ de $\mathrm{SL}_2(\mathbf{F}_q)$ est isomorphe à $\mathbf{F}_q$. Le groupe $A = f(U)$ est un p-groupe abélien élémentaire de G de rang e. Nous dirons que f est *de type toral* si A est toral au sens du § 1.1. C'est le cas si $e = 1$, ou si $e = 2$ et G est simplement connexe (1.1.2), ou si p n'est pas un nombre premier de torsion pour G.

Nous allons donner un *critère pour l'existence d'un f non dégénéré de type toral.* Supposons G presque simple, de rang r ; soient k_i $(i = 1, \ldots, r)$ les exposants de son groupe de Weyl et soient $d_i = k_i + 1$ les degrés correspondants (Bourbaki, LIE V, § 6, prop. 3). L'énoncé suivant résume une série de résultats dus à divers auteurs ([2], [8], [9], [11], [12], [14], [19], [20], [24], [28], [31]) :

2.1.1. *Pour qu'il existe un homomorphisme non dégénéré de type toral de* $\mathrm{SL}_2(\mathbf{F}_q)$ *dans G, il faut et il suffit que $q - 1$ divise l'un des entiers $2d_1, \ldots, 2d_r$.*

Remarque.— Lorsque $p = 2$ ou 3, il existe quelques plongements de $L_2(p^e)$ qui ne sont pas de type toral, par exemple :

$$L_2(4) \longrightarrow \mathrm{PGL}_2\ ,\ L_2(8) \longrightarrow G_2\ ,\ L_2(16) \longrightarrow D_8\ , L_2(32) \longrightarrow E_8\ ;$$
$$L_2(9) \longrightarrow \mathrm{PGL}_3\ ,\ L_2(27) \longrightarrow F_4.$$

Je ne sais pas en donner de description systématique.

Exemples

1) Si $G = \mathrm{SL}_2$, on a $r = 1$ et $d_1 = 2$; la condition dit alors que $q - 1$ divise 4, d'où $q = 3$ et $q = 5$, ce qui donne des plongements de $\mathrm{SL}_2(\mathbf{F}_3)$ et $\mathrm{SL}_2(\mathbf{F}_5)$ dans SL_2 ; d'où des plongements de $\mathrm{PSL}_2(\mathbf{F}_3) = \mathrm{Alt}_4$ et de $\mathrm{PSL}_2(\mathbf{F}_5) = \mathrm{Alt}_5$ dans PGL_2. On retrouve ainsi les groupes du tétraèdre et de l'icosaèdre (quant au groupe du cube, Sym_4, il s'interprète aussi comme $\mathrm{PGL}_2(\mathbf{F}_3)$, et c'est le normalisateur du groupe Alt_4).

2) Si $G = G_2$, on a $r = 2$, $d_1 = 2$, $d_2 = 6$; la condition dit que $q - 1$ divise 12, ce qui donne des plongements projectifs pour $q = 3, 5, 7, 13$. En fait, si $q = 7$ ou 13, ces plongements projectifs sont de vrais plongements de $L_2(q)$, car sinon leurs images seraient contenues dans le centralisateur d'un élément d'ordre 2, qui est de type $A_1 \cdot A_1$, et cela contredirait l'exemple 1. (Ce genre d'argument s'applique à beaucoup d'autres cas : les plongements projectifs intéressants sont de vrais plongements.)

3) Si $G = E_8$, on a $(d_1, \ldots, d_8) = (2, 8, 12, 14, 18, 20, 24, 30)$ et l'on en déduit notamment des plongements de $L_2(q)$ pour $q = 16, 31, 41, 49, 61$.

4) Le plus grand des entiers d_i est le *nombre de Coxeter* h, égal à $(\dim G)/r - 1$. L'énoncé 2.1.1 contient donc comme cas particulier la *conjecture de Kostant* : *si* $q = 2h + 1$ *est une puissance d'un nombre premier, le groupe* G^{ad} *contient un sous-groupe isomorphe à* $L_2(q)$.

5) On a un énoncé analogue à celui de Kostant lorsque $h + 1$ est une puissance d'un nombre premier, d'où par exemple $L_2(19) \to E_7^{\mathrm{ad}}$ et $L_2(31) \to E_8$. Lorsque $h+1$ est égal à un nombre premier p, on a un résultat plus précis (cf. [31]) : le groupe $\mathrm{PGL}_2(\mathbf{F}_p)$ (qui est "deux fois plus grand" que $\mathrm{PSL}_2(\mathbf{F}_p)$) est, lui aussi, plongeable dans G^{ad}. Lorsque $G = \mathrm{PGL}_2$, on retrouve le groupe du cube $\mathrm{PGL}_2(\mathbf{F}_3)$, cf. exemple 1. De ce point de vue, on peut dire que "les analogues" pour E_8 des groupes Alt_4, Sym_4, et Alt_5 du début de l'exposé sont respectivement $\mathrm{PSL}_2(\mathbf{F}_{31})$, $\mathrm{PGL}_2(\mathbf{F}_{31})$ et $\mathrm{PSL}_2(\mathbf{F}_{61})$.

2.2. Le critère 2.1.1 : démonstration de la nécessité

Il s'agit de prouver que, si $f : \mathrm{SL}_2(\mathbf{F}_q) \to G$ est un homomorphisme non dégénéré de type toral, alors $q - 1$ divise l'un des entiers $2d_i$.

On utilise :

2.2.1. *Soit* A *un* p*-sous-groupe élémentaire toral de* G*, et soit* $g \in N_G(A)$. *Soit* $I_g \in \mathrm{GL}(A)$ *l'automorphisme de* A (vu comme espace vectoriel sur $\mathbf{F}_p$) *défini par la conjugaison par* g. *Soit* λ *une valeur propre de* I_g *dans* $\overline{\mathbf{F}}_p$ *et soit* m *l'ordre de* λ (*dans* $\overline{\mathbf{F}}_p^*$). *Alors* m *divise l'un des* d_i.

(On peut supposer que A est contenu dans T ; d'après 1.1.1, il existe $w \in W$ qui induit I_g sur A. L'une des valeurs propres de w en caractéristique 0 a pour réduction λ en caractéristique p. Son ordre est donc de la forme mp^a, avec $a \geq 0$. D'après un théorème de Springer ([32], th. 3.4 (i)), mp^a divise l'un des d_i. Il en est donc de même de m.)

Revenons à f, et au p-Sylow $U = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Soit $A = f(U)$, et soit $g = f(h)$, où $h = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$ est un générateur du sous-groupe diagonal de $\mathrm{SL}_2(\mathbf{F}_q)$. Si l'on identifie U à $\mathbf{F}_q$, l'action de h sur ce groupe est l'homothétie de rapport c^2 ; ses valeurs propres (dans $\overline{\mathbf{F}}_p$) sont les conjugués de c^2, qui sont d'ordre $m = (q-1)/2$ si $p > 2$ et $m = q - 1$ si $p = 2$. En appliquant 2.2.1 à A et g, on voit que m divise l'un des entiers d_i ; donc $q - 1$ divise l'un des entiers $2d_i$.

Remarque.— Le même argument montre que, si f est un homomorphisme de $\mathrm{GL}_2(\mathbf{F}_q)$

dans G, qui est non dégénéré et de type toral (en un sens évident), alors $q-1$ divise l'un des d_i.

2.3. Le critère 2.1.1 : vérification de la suffisance

On doit montrer que, si $q-1$ divise l'un des entiers $2d_i$, il existe $f : \mathrm{SL}_2(\mathbf{F}_q) \to G$ qui est non dégénéré de type toral.

On ne connaît pas de démonstration générale de cet énoncé. On procède cas par cas :

1) Le cas où G est de type classique se traite facilement, grâce à la connaissance de la table des caractères de $\mathrm{SL}_2(\mathbf{F}_q)$; les caractères irréductibles de degré $(q \pm 1)/2$ sont particulièrement utiles. La condition de toralité est trivialement satisfaite si $p \neq 2$; dans le cas où $p = 2$, et où G est un groupe orthogonal, il faut faire un peu attention. La même méthode s'applique à G_2 (voir aussi [2], [11], [28]).

2) Pour les groupes exceptionnels, les inclusions des groupes classiques dans ceux-ci, et les plongements

$$G_2 \longrightarrow F_4 \longrightarrow E_6 \longrightarrow E_7 \longrightarrow E_8,$$

montrent qu'il suffit de traiter les cas suivants :

$$F_4\ (q = 25) \quad ; \quad E_6\ (q = 19) \quad ; \quad E_7\ (q = 29, 37) \quad ; \quad E_8\ (q = 16, 31, 41, 49, 61).$$

Le cas $(E_8\,;\,16)$ se traite en remarquant que $L_2(16)$ se plonge dans un groupe de type D_8, donc dans un groupe de type E_8 ; ce plongement n'est pas de type toral dans D_8, mais il le devient dans E_8 comme on le voit en appliquant [8], prop. 3.8.

Le cas $(F_4\,;\,25)$ se déduit de ce que $L_2(25)$ se plonge dans le groupe de Tits ${}^2F_4(2)'$, qui lui-même se plonge dans E_6, cf. 2.4.2, b) ci-après. On vérifie par un calcul de caractères que le sous-groupe de E_6 ainsi obtenu est contenu dans un conjugué de F_4, cf. Cohen–Wales [14].

Les cas $(E_6\,;\,19)$, $(E_7\,;\,37)$, $(E_8\,;\,31)$, $(E_8\,;\,41)$, $(E_8\,;\,49)$, $(E_8\,;\,61)$ ont été vérifiés par des calculs sur ordinateur, cf. Cohen–Wales [14], Kleidman–Ryba [24], Griess–Ryba [19] et [20], Cohen–Griess–Lisser [9].

Les cas $(E_7\,;\,37)$, $(E_8\,;\,31)$ et $(E_8\,;\,61)$ sont traités dans [31] par une méthode p-adique qui consiste à relever un plongement (bien choisi) de la caractéristique p à la caractéristique 0. Une variante non encore publiée de cette méthode permet de traiter aussi $(E_6\,;\,19)$, $(E_7\,;\,29)$ et $(E_8\,;\,41)$. Ainsi, *tous les cas où q est premier peuvent être obtenus sans ordinateur.*

Remarque.— Les calculs sur ordinateur ont un inconvénient évident : ils ne sont pas vérifiables pas à pas, comme une démonstration doit l'être. Ils ont toutefois un avantage : dans certains cas, ils montrent *l'unicité* du plongement considéré (à conjugaison près), cf. [19], [20]. C'est là un résultat que la méthode p-adique ne donne pas, au moins pour le moment.

2.4. Plongements projectifs des groupes finis simples dans les groupes de type exceptionnel

La table suivante est extraite de Griess-Ryba [22] (avec une petite correction relative à F_4). Elle donne la liste des groupes simples ayant un plongement projectif dans $G_2, \ldots, E_8$. Je renvoie à [22] et [27] pour divers renseignements supplémentaires sur ces plongements, ainsi que pour des références.

Table

$\mathbf{G_2}$ – Alt_n, $n = 5, 6$; $L_2(q)$, $q = 7, 8, 13$; $\mathrm{SU}_3(3) = G_2(2)'$.

$\mathbf{F_4}$ – *ceux de* G_2 *et* : Alt_n, $n = 7, 8, 9, 10$; $L_2(q)$, $q = 17, 25, 27$; $L_3(3)$; $\mathrm{SU}_4(2)$; $\mathrm{Sp}_6(2) = O_7(2)$; $O_8^+(2)$; ${}^3D_4(2)$.

$\mathbf{E_6}$ – *ceux de* F_4 *et* : Alt_{11} ; $L_2(q)$, $q = 11, 19$; $L_3(4)$; $\mathrm{PSU}_4(3)$; ${}^2F_4(2)'$; M_{11} ; $HJ = J_2$.

$\mathbf{E_7}$ – *ceux de* E_6 *et* : Alt_n, $n = 12, 13$; $L_2(q)$, $q = 29, 37$; $\mathrm{PSU}_3(8)$; M_{12}.

$\mathbf{E_8}$ – *ceux de* E_7 *et* : Alt_n, $n = 14, 15, 16, 17$; $L_2(q)$, $q = 16, 31, 32, 41, 49, 61$; $L_3(5)$; $\mathrm{PSp}_4(5)$; $G_2(3)$; ${}^2B_2(8) = Sz(8)$.

(Les notations sont celles de l'ATLAS [15]. En particulier $L_n(q)$ désigne le groupe $\mathrm{PSL}_n(\mathbf{F}_q)$. Vu que $\mathrm{Alt}_5 = L_2(4) = L_2(5)$ et $\mathrm{Alt}_6 = L_2(9)$, la liste pour G_2 pourrait aussi être écrite :

$\mathbf{G_2}$ – $L_2(q)$, $q = 4, 5, 7, 8, 9, 13$; $\mathrm{SU}_3(3) = G_2(2)'$.

De même, pour F_4, on peut remplacer Alt_8 par $L_4(2)$.)

La vérification de l'exactitude de cette table comporte deux parties. Tout d'abord :

2.4.1. *Un groupe simple qui ne figure pas dans la table n'a pas de plongement projectif dans* G.

Comme on peut s'y attendre, le point de départ est la *classification des groupes simples finis*, qui est admise (le lecteur curieux de savoir quelle partie de cette classification reste à démontrer pourra consulter Aschbacher [3]). Cela permet de passer

en revue les différents cas possibles : groupes alternés, groupes de type algébrique, groupes sporadiques. Pour éliminer un groupe S, on utilise des arguments variés, par exemple 1.2.2 ou 2.2.1 (qui suffisent si le groupe est très gros), ou (dans les cas difficiles) la table des caractères du groupe. C'est un travail délicat. La moindre erreur peut conduire à éliminer à tort le groupe en question. C'est ce qui s'était passé dans une liste précédente [8] pour les groupes $L_2(41)$, $L_2(49)$ et $Sz(8)$ qui avaient été déclarés non plongeables dans E_8.

2.4.2. *Tout groupe figurant dans la table a au moins un plongement projectif dans G.*

On utilise différentes méthodes. Par exemple :

a) Le cas le plus facile est celui où l'on connaît un sous-groupe de G dans lequel S a un plongement projectif. Ainsi, pour traiter le cas de Alt_{10} et F_4, il suffit de remarquer que Alt_{10} a une représentation orthogonale évidente de degré 9, autrement dit se plonge dans un groupe de type B_4, et l'on utilise le plongement de B_4 dans F_4.

b) Certains cas peuvent se traiter à partir de la table des caractères de S (et de ses extensions centrales). Outre $G = G_2$, déjà signalé, il faut mentionner le cas où $G = E_6$ et où S est le groupe de Tits ${}^2F_4(2)'$ (Cohen–Wales [14]). On part du fait que le groupe $S \cdot 2 = {}^2F_4(2)$ a une représentation irréductible V de dimension 78 (cf. [15], p. 75). Un calcul de caractères montre que $\wedge^2 V$ contient V ; il existe donc un homomorphisme non nul $\wedge^2 V \to V$ compatible avec l'action de $S \cdot 2$, et un autre calcul de caractères montre que l'identité de Jacobi est satisfaite. D'où une structure d'algèbre de Lie sur V. Il est clair que cette algèbre de Lie est simple ; puisqu'elle est de dimension 78, elle est de type B_6, C_6 ou E_6. On élimine les types B_6 et C_6 qui conduiraient à des représentations de $S \cdot 2$ de degré trop petit. L'algèbre de Lie V est donc de type E_6, ce qui fournit un plongement de $S \cdot 2$ dans E_6^{ad}, donc *a fortiori* un plongement de S. (On aimerait avoir davantage d'exemples de ce genre !)

c) La plupart des autres plongements ont été construits au moyen de calculs sur ordinateur. Je renvoie à [22] pour une description des méthodes employées. Je signale seulement que les calculs ne se font pas sur le corps k, mais sur un corps fini $\mathbf{F}_\ell$, où ℓ est un nombre premier ne divisant pas l'ordre de S et tel que $\mathbf{F}_\ell$ contienne les racines de l'unité intervenant dans la construction : ainsi, pour plonger $L_2(61)$ dans E_8, Cohen–Griess–Lisser [9] choisissent $\ell = 1831$. Le relèvement de $\mathbf{F}_\ell$ à $\mathbf{Z}_\ell$ (donc à la caractéristique 0) ne présente aucune difficulté vu que ℓ ne divise pas $|S|$. Il semble que, dans chaque cas, le calcul comporte suffisamment de vérifications internes pour qu'on puisse lui faire confiance.

2.5. Compléments

2.5.1. *Classification en caractéristique* > 0

L'analogue de 2.4 en caractéristique p a été fait par Liebeck–Seitz [27]. Tout groupe S intervenant en caractéristique 0 intervient aussi en caractéristique p (quel que soit p) ; c'est là une conséquence simple de la théorie de Bruhat–Tits, cf. [31], § 5. Outre ces groupes, et ceux qui sont "de caractéristique p", Liebeck–Seitz donnent la liste suivante :

$\mathbf{G_2}$ – $p = 2 : J_2$; $p = 5 : \mathrm{Alt}_7$; $p = 11 : J_1$.

$\mathbf{F_4}$ – *ceux de* G_2 *et* $p = 2 : L_4(3)$; $p = 3 : L_3(4)$; $p = 5 : Sz(8)$; $p = 11 : M_{11}$, Alt_{11}.

$\mathbf{E_6}$ – *ceux de* F_4 *et* $p = 2 : M_{12}, \mathrm{Alt}_{12}, G_2(3), O_7(3), M_{22}, J_3, Fi_{22}$; $p = 3 : M_{12}$, Alt_{12} ; $p = 5 : M_{12}$; $p = 7 : M_{22}$.

$\mathbf{E_7}$ – *ceux de* E_6 *et* $p = 5 : M_{22}, Ru, HS$; $p = 7 : \mathrm{Alt}_{14}$.

$\mathbf{E_8}$ – *ceux de* E_7 *et* $p = 2 : L_4(5)$; $p = 3 : \mathrm{Alt}_{18}, Th$; $p = 5 : Sz(32)$.

Noter en particulier le groupe de Janko J_1 dans $G_2(\mathbf{F}_{11})$ et le groupe de Thompson Th dans $E_8(\mathbf{F}_3)$.

2.5.2. *Classes de conjugaison de plongements*

On aimerait pouvoir compléter la table 2.4 en décrivant les plongements à conjugaison près. Cela a été fait dans certains cas, mais pas dans tous, cf. [22]. Le cas des plongements de Alt_5 dans E_8 est particulièrement intéressant (cf. Frey [16]) ; on peut déterminer les triplets (x, y, z) de classes de conjugaison de E_8 d'ordres $(2, 3, 5)$ qui sont représentables dans un même sous-groupe Alt_5. Pour tous ces triplets, sauf un (celui appelé "844" dans [16]), Frey détermine le nombre de classes de conjugaison correspondantes (une ou deux). Par contre, pour le cas "844" (qui est le seul où le centralisateur du sous-groupe Alt_5 soit fini), on ne sait pas combien il y a de classes de conjugaison ; on dispose de plusieurs tels sous-groupes (par exemple un sous-groupe du groupe de Borovik [7], ou un sous-groupe de $L_2(41)$, ou de $L_2(61)$,...), mais il n'est pas facile de voir s'ils sont ou non conjugués. Comme Alt_5 admet la présentation :

$$(x, y, z \mid x^2 = y^3 = z^5 = 1\ ,\ xyz = 1),$$

c'est là un problème analogue à celui de la "rigidité" intervenant pour la classification des revêtements galoisiens de la droite projective ramifiés en 3 points.

2.5.3. *Rationalité*

On sait que G provient par extension des scalaires d'un groupe *déployé* G_{dep} défini sur $\mathbf{Q}$. Si S (ou $\overline{S}$) est plongeable dans $G(k)$, on peut se demander quels sont les sous-corps k' de k tels que S soit plongeable dans $G_{\mathrm{dep}}(k')$. Cette question est étroitement liée à la précédente (celle des classes de conjugaison) : voir là-dessus [19], App. 2. Voici un exemple typique :

D'après Aschbacher [2], le groupe $S \cdot 2 = G_2(2)$ admet un plongement dans $G_2(k)$, et un seul, à conjugaison près. Or, à la fois $S \cdot 2$ et G_2 ont un centre trivial, et pas d'automorphisme externe. De plus, le centralisateur de $2 \cdot S$ est trivial. Soit P l'ensemble de ces plongements ; c'est un G_2-torseur qui est défini de façon naturelle sur $\mathbf{Q}$. Il définit donc une $\mathbf{Q}$-forme G_2^0 de G_2, et l'on peut plonger $S \cdot 2$ dans $G_2^0(\mathbf{Q})$ par définition même de G_2^0. Or, il n'y a que deux formes de G_2 sur $\mathbf{Q}$, que l'on distingue par leurs points réels ; la forme déployée ne peut pas contenir $2 \cdot S$: son compact maximal est trop petit. Ainsi, G_2^0 est la forme non déployée de G_2, celle qui correspond aux octonions usuels. On conclut de là que le plongement cherché de $S \cdot 2$ dans $G_{\mathrm{dep}}(k')$ existe si et seulement si G_{dep} et G_2^0 sont k'-isomorphes, i.e. *si et seulement si* -1 *est somme de* 4 *carrés dans* k'. Un argument analogue montre que $L_2(13)$ est plongeable dans $G_{\mathrm{dep}}(k')$ si et seulement si k' contient $\sqrt{13}$ et -1 est somme de 4 carrés dans k' ; même chose pour $L_2(8)$, avec $\sqrt{13}$ remplacé par $z_9+\overline{z}_9$, où z_9 est une racine primitive 9-ème de l'unité. (Noter l'analogie de ces énoncés avec le suivant, connu depuis longtemps : Alt_4, Sym_4 et Alt_5 sont plongeables dans $\mathrm{PGL}_2(k')$ si et seulement si -1 est somme de 2 carrés dans k' et (pour Alt_5) k' contient $\sqrt{5}$.)

BIBLIOGRAPHIE

[1] J.F. ADAMS - 2-*tori in* E_8, Math. Ann. **287** (1987), 29-39 (= *Selected Works,* vol. II, 264-274).

[2] M. ASCHBACHER - *Chevalley groups of type* G_2 *as the group of a trilinear form*, J. Alg. **109** (1987), 193-259.

[3] M. ASCHBACHER - *Quasithin groups*, in *Algebraic Groups and their Representations* (R. Carter and J. Saxl edit.), NATO AS series, vol. **517**, 321-340, Kluwer, 1998.

[4] A. BOREL - *Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tôhoku Math. J. **13** (1961), 216-240 (= *Oe.* II, n° 53 et *Commentaires*, 775-777).

[5] A. BOREL and G.D. MOSTOW - *On semi-simple automorphisms of Lie algebras*, Ann. Math. **61** (1955), 389-405 (= A. Borel, *Oe.* I, n° 36).

[6] A. BOREL et J.-P. SERRE - *Sur certains sous-groupes des groupes de Lie compacts*, Comm. Math. Helv. **27** (1953), 128-139 (= A. Borel, *Oe.* I, n° 24).

[7] A.V. BOROVIK - *A maximal subgroup in the simple finite group* $E_8(q)$, Contemp. Math. A.M.S. **131** (1992), vol. I, 67-79.

[8] A.M. COHEN and R.L. GRIESS, Jr - *On finite simple subgroups of the complex Lie groups of type* E_8, AMS Proc. Symp. Pure Math. **47** (1987), vol. II, 367-405.

[9] A.M. COHEN, R.L. GRIESS, Jr and B. LISSER - *The group* $L(2,61)$ *embeds in the Lie group of type* E_8, Comm. Alg. **21** (1993), 1889-1907.

[10] A.M. COHEN and G.M. SEITZ - *The r-rank of the groups of exceptional Lie type*, Indag. Math. **49** (1987), 251-259.

[11] A.M. COHEN and D.B. WALES - *Finite subgroups of* $G_2(\mathbf{C})$, Comm. Alg. **11** (1983), 441-459.

[12] A.M. COHEN and D.B. WALES - *Embeddings of the group* $L(2,13)$ *in groups of Lie type* E_6, Israel J. Math. **82** (1993), 45-86.

[13] A.M. COHEN and D.B. WALES - *Finite simple subgroups of semisimple complex Lie groups – a survey*, in *Groups of Lie type and their geometries*, LMS Lect. Notes **207** (1995), 77-96.

[14] A.M. COHEN and D.B. WALES - *Finite subgroups of* $F_4(\mathbf{C})$ *and* $E_6(\mathbf{C})$, Proc. London Math. Soc. **74** (1997), 105-150.

[15] J.H. CONWAY, R.T. CURTIS, S.P. NORTON, R.A. PARKER and R.A. WILSON - *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[16] D. FREY - *Conjugacy of alternating groups of degree* 5 *and* $\mathrm{SL}(2,5)$ *subgroups of the complex Lie groups of type* E_8, Memoirs AMS **634** (1998).

[17] R.L. GRIESS, Jr - *Elementary abelian subgroups of algebraic groups*, Geom. Dedicata **39** (1991), 253-305.

[18] R.L. GRIESS, Jr and A.J.E. RYBA - *Embeddings of* $U(3,8)$, $Sz(8)$ *and the Rudvalis group in algebraic groups of type* E_7, Invent. math. **116** (1994), 215-241.

[19] R.L. GRIESS, Jr and A.J.E. RYBA - *Embeddings of* $\mathrm{PGL}(2,31)$ *and* $\mathrm{SL}(2,32)$ *in* $E_8(\mathbf{C})$, Duke Math. J. **94** (1998), 181-211.

[20] R.L. GRIESS, Jr and A.J.E. RYBA - *Embeddings of* $\mathrm{PSL}(2,41)$ *and* $\mathrm{PSL}(2,49)$ *in* $E_8(\mathbf{C})$, J. Symb. Comp. **11** (1999), 1-17.

[21] R.L. GRIESS, Jr and A.J.E. RYBA - *Embeddings of* $Sz(8)$ *into exceptional Lie groups*, soumis au J. Crelle.

[22] R.L. GRIESS, Jr and A.J.E. RYBA - *Finite simple groups which projectively embed in an exceptional Lie group are classified !*, Bull. AMS **36** (1999), 75-93.

[23] A. GROTHENDIECK - *Torsion homologique et sections rationnelles*, Sém. Chevalley (1958), *Anneaux de Chow et Applications*, exposé 5.

[24] P.B. KLEIDMAN and A.J.E. RYBA - *Kostant's conjecture holds for* E_7 : $L_2(37) < E_7(\mathbf{C})$, J. Alg. **161** (1993), 535-540.

[25] M.-A. KNUS, A. MERKURJEV, M. ROST and J.-P. TIGNOL - *The Book of Involutions*, AMS Colloquium Publ. **44**, 1998.

[26] M.W. LIEBECK - *Subgroups of exceptional groups*, in *Algebraic Groups and their Representations* (R.W. Carter and J. Saxl edit.), NATO AS series, vol. **517**, 275-290, Kluwer, 1998.

[27] M.W. LIEBECK and G.M. SEITZ - *On finite subgroups of exceptional algebraic groups*, 1999, à paraître au J. Crelle.

[28] A. MEURMAN - *An embedding of* $\mathrm{PSL}(2,13)$ *in* $G_2(\mathbf{C})$, Lect. Notes in Math. **933** (1982), 157-162.

[29] Z. REICHSTEIN and B. YOUSSIN - *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, 1999, à paraître.

[30] J.-P. SERRE - *Cohomologie galoisienne : progrès et problèmes*, Sém. Bourbaki 1993-94, exposé n° 783 (SMF, Astérisque **227** (1995), 229-257).

[31] J.-P. SERRE - *Exemples de plongements des groupes* $\mathbf{PSL}_2(\mathbf{F}_p)$ *dans des groupes de Lie simples*, Invent. math. **124** (1996), 525-562.

[32] T.A. SPRINGER - *Regular elements of finite reflection groups*, Invent. math. **25** (1974), 159-198.

[33] T.A. SPRINGER and R. STEINBERG - *Conjugacy classes*, Lect. Notes in Math. **131** (1970), 281-312 (= R. Steinberg, *C.P.*, 293-323).

[34] R. STEINBERG - *Torsion in reductive groups*, Adv. in Math. **15** (1975), 63-92 (= *C.P.*, 415-444).

[35] J. TITS - *Normalisateurs de tores*, I. *Groupes de Coxeter étendus*, J. Alg. **4** (1966), 96-116.

[36] J. TITS - *Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples*, Publ. Math. IHES **31** (1966), 21-58.

Jean–Pierre SERRE

Collège de France
3, rue d'Ulm
F-75005 PARIS
E-mail : serre@dmi.ens.fr