Invent. math. 124, 525–562 (1996)

Inventiones mathematicae

Exemples de plongements des groupes $\mathbf{PSL}_2(\mathbf{F}_p)$ dans des groupes de Lie simples

Jean-Pierre Serre

Collège de France, 3 rue d'Ulm, F-75005 Paris

Oblatum 25-V-1995

to Reinhold Remmert

Introduction

Les polyèdres réguliers de $\mathbf{R}^3$ correspondent à des sous-groupes remarquables de $\mathbf{SO}_3(\mathbf{R})$ et $\mathbf{PGL}_2(\mathbf{C})$:

les groupes alternés A_4 et A_5, et le groupe symétrique S_4.

Y a-t-il des analogues de ces sous-groupes finis pour les autres groupes de Lie simples, et en particulier pour les groupes de type exceptionnel G_2, F_4, E_6, E_7, E_8? Ce genre de question a été beaucoup étudié ces dernières années (cf. notamment [6–10], [17], [21], [22]), sans cependant que l'on parvienne à une solution complète. Je me propose de démontrer le résultat suivant, qui constitue un pas dans cette direction:

Théorème. *Soit G un groupe algébrique linéaire connexe semi-simple sur un corps algébriquement clos k. On suppose que G est simple* (donc de centre trivial); *soit h son nombre de Coxeter. Soit p un nombre premier. Alors*:

(i) *Si $p = h + 1$, le groupe $G(k)$ contient un sous-groupe isomorphe à $\mathbf{PGL}_2(\mathbf{F}_p)$, à une exception près*: *celle où* $\mathrm{caract}(k) = 2$ *et où* $G \simeq \mathbf{PGL}_2$.

(ii) *Si $p = 2h + 1$, $G(k)$ contient un sous-groupe isomorphe à $\mathbf{PSL}_2(\mathbf{F}_p)$.*

(Noter que, lorsque $G = \mathbf{PGL}_2$, on a $h = 2$, d'où $p = 3$ dans le cas (i) et $p = 5$ dans le cas (ii). On retrouve ainsi le fait que $\mathbf{PGL}_2(\mathbf{C})$ contient $A_4 = \mathbf{PSL}_2(\mathbf{F}_3)$, $S_4 = \mathbf{PGL}_2(\mathbf{F}_3)$ et $A_5 = \mathbf{PSL}_2(\mathbf{F}_5)$.)

En fait, la partie (ii) du théorème était déjà connue lorsque k est de caractéristique 0; elle avait été conjecturée par Kostant en 1983 (cf. Cohen–Wales [10]) et vérifiée ensuite cas par cas, parfois avec l'aide d'ordinateurs, cf. [7], [17]. Seule la partie (i) est (peut-être) nouvelle, au moins pour les types E_7 et E_8, où elle donne:

Corollaire. *Le groupe* $\mathbf{PGL}_2(\mathbf{F}_{19})$ *est plongeable dans le groupe adjoint* $E_7(\mathbf{C})$, *et* $\mathbf{PGL}_2(\mathbf{F}_{31})$ *est plongeable dans* $E_8(\mathbf{C})$.

Cela résulte de ce que $h = 18$ si G est de type E_7, et $h = 30$ si G est de type E_8.

Les §§2 à 5 contiennent la démonstration du théorème ci-dessus (sous une forme quelque peu renforcée, cf. n° 1.3). On part du cas où la caractéristique est p (§2); si $p \geqq h$, on dispose alors du plongement "principal" de $\mathbf{PGL}_2(\mathbf{F}_p)$ dans $G(\mathbf{F}_p)$, cf. Testerman [32], [33]. Dans le cas (i), il n'y a pas d'obstruction à relever ce plongement dans $G(\mathbf{Z}_p)$, cf. §3. Le cas (ii) est plus délicat: il faut remplacer $\mathbf{Z}_p$ par $\mathbf{Z}_p[\sqrt{\pm p}]$ et se borner à relever $\mathbf{PSL}_2(\mathbf{F}_p)$, cf. §4. Ceci fait, le cas où k est de caractéristique 0 est essentiellement réglé; on passe de là à une caractéristique quelconque grâce à la théorie de Bruhat–Tits, cf. §5.

Le §6 donne quelques propriétés des sous-groupes ainsi construits: classes de conjugaison, caractère de la représentation adjointe. Les annexes (§§7, 8) contiennent des résultats connus, qu'il m'a paru utile de rappeler.

Table des matières

1. Enoncé des résultats

1.1. Notations

Soit R un système de racines irréductible réduit (Bourbaki [2], Chap. VI, §1), de rang r. On en choisit une base $\{\alpha_1, \ldots, \alpha_r\}$ et l'on note s_i la symétrie associée à la racine α_i. Le groupe engendré par les s_i est le groupe de Weyl W de R. Le produit $s_1 \cdots s_r$ est l'élément de Coxeter associé à la base choisie; son ordre h est le *nombre de Coxeter* de R. On a:

$h = r + 1$ si R est de type A_r,
$h = 2r$ si R est de type B_r ou C_r,
$h = 2r - 2$ si R est de type D_r,
$h = 6, 12, 12, 18, 30$ si R est de type G_2, F_4, E_6, E_7, E_8.

On note G un schéma en groupes linéaire semi-simple déployé sur $\mathbf{Z}$, de système de racines R, et de centre trivial (type "adjoint"). Un tel schéma en

groupes existe (cf. Chevalley [5], Kostant [19] et Bruhat–Tits [3], Chap. II, n° 3.2.13), et est unique à isomorphisme près (Demazure [12], p. 305, th. 4.1). Si N est la dimension de G, on a

$$N = r + \mathrm{Card}(R) = r(h+1)\,.$$

Pour tout anneau commutatif k, on note $G(k)$ le groupe des k-points du schéma G. Lorsque k est un corps algébriquement clos, $G(k)$ est un groupe simple.

Le revêtement universel de G sera noté $\tilde{G}$. Le centre Z de $\tilde{G}$ est un schéma en groupes fini et plat, de type multiplicatif. On a $G = \tilde{G}/Z$.

Exemple. Soit n un entier $\geqq 2$, et prenons R de type A_{n-1}. On a alors $r = n-1$, $h = n$, $G = \mathbf{PGL}_n$, $\tilde{G} = \mathbf{SL}_n$, $Z = \mu_n$ (racines n-ièmes de l'unité). L'image de $\tilde{G}(k)$ dans $G(k)$ est notée $\mathbf{PSL}_n(k)$.

Lorsque $n = 2$, et que k est un corps fini $\mathbf{F}_q$ de caractéristique $\neq 2$, le groupe $\mathbf{PSL}_2(\mathbf{F}_q)$ est d'indice 2 dans $\mathbf{PGL}_2(\mathbf{F}_q)$; c'est un groupe simple si $q > 3$. Pour $q = 3, 5, 9$, on a des isomorphismes:

$$\mathbf{PSL}_2(\mathbf{F}_3) = A_4\,, \qquad \mathbf{PGL}_2(\mathbf{F}_3) = S_4\,,$$
$$\mathbf{PSL}_2(\mathbf{F}_5) = A_5\,, \qquad \mathbf{PGL}_2(\mathbf{F}_5) = S_5\,,$$
$$\mathbf{PSL}_2(\mathbf{F}_9) = A_6\,.$$

1.2. Enoncé du théorème 1

C'est celui qui a été mentionné dans l'introduction:

Théorème 1. *Soient G et h comme ci-dessus. Soit k un corps algébriquement clos et soit p un nombre premier.*

(i) *Si $p = h+1$, le groupe $G(k)$ contient un sous-groupe isomorphe à $\mathbf{PGL}_2(\mathbf{F}_p)$, sauf dans le cas $h = 2$ et* $\mathrm{caract}(k) = 2$.

(ii) *Si $p = 2h+1$, $G(k)$ contient un sous-groupe isomorphe à $\mathbf{PSL}_2(\mathbf{F}_p)$.*

L'exception de (i) est celle où G est isomorphe à $\mathbf{PGL}_2$, auquel cas on a $r = 1$, $h = 2$, $p = 3$ et $\mathbf{PGL}_2(\mathbf{F}_3) = S_4$; si $\mathrm{caract}(k) = 2$, on montre facilement que S_4 ne peut pas être plongé dans $\mathbf{PGL}_2(k) = G(k)$.

Corollaire 1. *Si $p = h+1$ ou $2h+1$, $\mathbf{PSL}_2(\mathbf{F}_p)$ est plongeable dans $G(k)$.*

Lorsque $r > 1$, ou lorsque $r = 1$ et $\mathrm{caract}(k) \neq 2$, cela résulte du th. 1 puisque $\mathbf{PSL}_2(\mathbf{F}_p)$ est un sous-groupe de $\mathbf{PGL}_2(\mathbf{F}_p)$. Lorsque $r = 1$ et $\mathrm{caract}(k) = 2$, il faut vérifier que $\mathbf{PSL}_2(\mathbf{F}_3) = A_4$ se plonge dans $G(k)$; c'est clair, car A_4 est un sous-groupe de $A_5 = \mathbf{PSL}_2(\mathbf{F}_4)$, qui est lui-même un sous-groupe de $\mathbf{PGL}_2(k) = G(k)$.

Lorsque R est de type E_7, on a $h = 18$. D'où:

Corollaire 2. *Si G est de type E_7 adjoint, $G(k)$ contient des sous-groupes isomorphes à $\mathbf{PGL}_2(\mathbf{F}_{19})$ et $\mathbf{PSL}_2(\mathbf{F}_{37})$.*

Le cas de $\mathbf{PSL}_2(\mathbf{F}_{37})$ était connu, au moins lorsque caract$(k) = 0$, cf. Kleidman–Ryba [17].

De même, pour E_8, on a $h = 30$, d'où:

Corollaire 3. *Si G est de type E_8, $G(k)$ contient des sous-groupes isomorphes à $\mathbf{PGL}_2(\mathbf{F}_{31})$ et à $\mathbf{PSL}_2(\mathbf{F}_{61})$.*

Ici encore, le cas de $\mathbf{PSL}_2(\mathbf{F}_{61})$ était connu, cf. Cohen–Griess–Lisser [7].

Remarques. 1) Le th. 1, tout comme le th. 1′ du n° 1.3, se vérifie facilement lorsque G est un groupe classique, grâce à la théorie des représentations linéaires, orthogonales, ou symplectiques, des groupes $\mathbf{PSL}_2(\mathbf{F}_p)$ et $\mathbf{PGL}_2(\mathbf{F}_p)$.

2) Les valeurs $h+1$ et $2h+1$ de p figurant dans le th. 1 sont *maximales* au sens suivant:

(i) Si $G(\mathbf{C})$ contient un sous-groupe isomorphe à $\mathbf{PGL}_2(\mathbf{F}_p)$, on peut montrer que $p-1$ divise l'un des m_i+1, où les m_i sont les exposants du système de racines R. Comme $\sup(m_i) = h-1$, cela entraîne $p \leqq h+1$.

(ii) De même, si $G(\mathbf{C})$ contient $\mathbf{PSL}_2(\mathbf{F}_p)$, on peut montrer que $p-1$ divise l'un des entiers $2(m_i+1)$, d'où $p \leqq 2h+1$.

3) Comme on l'a signalé dans l'introduction, le cas (ii) du th. 1, pour $k = \mathbf{C}$, est une conjecture de Kostant, qui a déjà été vérifiée cas par cas (cf. Cohen–Wales [10]). En fait, la conjecture de Kostant est un peu plus générale: elle s'applique à $\mathbf{PSL}_2(\mathbf{F}_q)$, où $q = 2h+1$ est une puissance d'un nombre premier (et pas seulement, comme ici, un nombre premier). Lorsque G est de type exceptionnel, cela se produit pour F_4 et E_6, avec $q = 25$; la conjecture prédit alors que $\mathbf{PSL}_2(\mathbf{F}_{25})$ est plongeable dans $F_4(\mathbf{C})$ et $E_6(\mathbf{C})$, ce qui est bien exact (Cohen–Wales [9], n° 6.6). La méthode suivie ici ne semble pas s'appliquer à cette généralisation.

4) Le th. 1 est aussi valable pour les *groupes de Lie simples compacts*. En effet, si K est un tel groupe, son complexifié est du type $G(\mathbf{C})$ considéré ci-dessus, et l'on sait que tout sous-groupe fini de $G(\mathbf{C})$ est conjugué d'un sous-groupe de K.

1.3. Un renforcement du théorème 1

Introduisons d'abord une définition.

La notion d'élément "de type principal"

Soit T le tore maximal de G associé au déploiement donné. Comme G est de type adjoint, les α_i définissent un isomorphisme

$$T \xrightarrow{\sim} \mathbf{G}_m \times \cdots \times \mathbf{G}_m \quad (r \text{ facteurs}) .$$

Si k est un corps, de clôture algébrique $\bar{k}$, nous dirons qu'un élément de $G(k)$ est *de type principal* s'il est conjugué dans $G(\bar{k})$ à un élément t de $T(\bar{k})$ qui est "diagonal", i.e. tel que $\alpha_1(t) = \cdots = \alpha_r(t)$ dans $\bar{k}^*$. Un tel élément est semi-simple.

Exemple. Si $G = \mathbf{PGL}_n$, un élément de $G(k)$ est de type principal si et seulement si on peut le représenter dans $\mathbf{GL}_n(\bar{k})$ par une matrice semi-simple dont les valeurs propres $(\lambda_1, \ldots, \lambda_n)$ sont telles que

$$\lambda_1/\lambda_2 = \lambda_2/\lambda_3 = \cdots = \lambda_{n-1}/\lambda_n \,.$$

Enoncé du théorème 1′

Théorème 1′. *Les plongements du théorème* 1 :
(i) $\mathbf{PGL}_2(\mathbf{F}_p) \to G(k)$, $p = h + 1$,
(ii) $\mathbf{PSL}_2(\mathbf{F}_p) \to G(k)$, $p = 2h + 1$,
peuvent être choisis de façon à avoir les propriétés suivantes:
(i′) *Dans le cas* (i), *tout élément de* $\mathbf{PGL}_2(\mathbf{F}_p)$ *d'ordre premier à* caract(k) *est de type principal dans* $G(k)$.
(ii′) *Dans le cas* (ii), *tout élément de* $\mathbf{PSL}_2(\mathbf{F}_p)$, *d'ordre premier à* p *et à* caract(k), *est de type principal dans* $G(k)$.
(Lorsque caract$(k) = 0$, la condition "ordre premier à caract(k)" est supprimée. Dans ce cas, (i′) signifie simplement que *tout élément de* $\mathbf{PGL}_2(\mathbf{F}_p)$ *est de type principal dans* $G(k)$.)

Remarques. 1) Dans le cas (i), il peut exister des plongements

$$\mathbf{PGL}_2(\mathbf{F}_p) \to G(\mathbf{C})$$

qui ne satisfont pas à (i'). Par exemple, si $G = \mathbf{PGL}_6$, on a $h = 6$, $p = 7$; en utilisant une représentation orthogonale irréductible de $\mathbf{PGL}_2(\mathbf{F}_7)$, on obtient un plongement

$$\mathbf{PGL}_2(\mathbf{F}_7) \to \mathbf{O}_6(\mathbf{C}) \to \mathbf{GL}_6(\mathbf{C}) \to \mathbf{PGL}_6(\mathbf{C}) \,,$$

dans lequel les éléments d'ordre 4 et 8 de $\mathbf{PGL}_2(\mathbf{F}_7)$ ne sont pas de type principal.

Un autre exemple du même genre vient d'être obtenu tout récemment par Griess et Ryba: à l'aide de calculs sur ordinateur, ils ont construit un plongement de $\mathbf{PGL}_2(\mathbf{F}_{31})$ dans $E_8(\mathbf{C})$ dans lequel les éléments d'ordre 16 et 32 ne sont pas de type principal.

2) Le cas (ii) a l'air différent. Il paraît probable que (ii) $\Rightarrow$ (ii′). Peut-être même est-il vrai que les sous-groupes de $G(\mathbf{C})$ isomorphes à $\mathbf{PSL}_2(\mathbf{F}_p)$ forment *une seule classe de conjugaison*? Cela a été vérifié dans divers cas particuliers, notamment celui de E_8, cf. [7].

2. L'homomorphisme principal

Sur un corps de caractéristique 0, par exemple $\mathbf{Q}$, on dispose d'un homomorphisme "principal" $\mathbf{SL}_2 \to G$, défini par de Siebenthal [27] et Dynkin [13], et étudié en détail par Kostant [18]. Nous aurons besoin d'une version de cet homomorphisme où l'on précise les dénominateurs (cf. Testerman [32], [33]); cela nous permettra de définir un plongement de $\mathbf{PGL}_2(\mathbf{F}_p)$ dans $G(\mathbf{F}_p)$ pour tout $p \geqq h$; la question du *relèvement p-adique* de ce plongement (pour $p = h+1$ ou $p = 2h+1$) fera l'objet des §§3 et 4.

2.1. Notations

On conserve celles du §1: G est un schéma en groupes semi-simple déployé sur $\mathbf{Z}$, de type adjoint. On note R son système de racines, et $(\alpha_1, \ldots, \alpha_r)$ une base de R. On suppose R irréductible. On note R_+ l'ensemble des racines > 0 (par rapport à la base choisie). Si $\alpha = \sum n_i \alpha_i$ est un élément de R, on pose $ht(\alpha) = \sum n_i$; c'est la *hauteur* de α. Si $\alpha > 0$, on a $1 \leqq ht(\alpha) \leqq h-1$, où h est le nombre de Coxeter de G. Il sera commode de mettre sur R_+ une relation d'ordre total telle que $ht(\alpha) > ht(\beta) \Rightarrow \alpha > \beta$.

On note T et U_α ($\alpha \in R$) le tore et les sous-groupes radiciels définis par le déploiement choisi de G. Comme on l'a vu, les α_i ($1 \leqq i \leqq r$) définissent un isomorphisme de T sur $(\mathbf{G}_m)^r$. Soit $\mathrm{Lie}(T)$ l'algèbre de Lie de T (sur $\mathbf{Z}$); elle s'identifie au groupe $Q(R^\vee)$ des poids du système de racines dual $R^\vee$. En particulier, toute coracine $\alpha^\vee$ définit un élément de $\mathrm{Lie}(T)$, que nous noterons H_α (ou simplement H_i si α est l'une des racines simples α_i).

Les groupes U_α sont isomorphes au groupe additif $\mathbf{G}_a$. On choisira un isomorphisme $x_\alpha : \mathbf{G}_a \to U_\alpha$, et l'on notera X_α l'image dans $\mathrm{Lie}(\mathrm{U}_\alpha)$ de la base canonique de $\mathrm{Lie}(\mathbf{G}_a)$. Quitte à changer le signe de certains des x_α, on peut supposer que $[X_\alpha, X_{-\alpha}] = -H_\alpha$ pour tout $\alpha \in R$ (cf. e.g. [2], Chap. VIII, §2, n° 4). Lorsque $\alpha = \alpha_i$, on écrit X_i et Y_i à la place de X_{α_i} et de $X_{-\alpha_i}$.

On a $\mathrm{Lie}(G) = \mathrm{Lie}(T) \oplus \bigoplus_{\alpha \in R} \mathrm{Lie}(U_\alpha)$ et $\mathrm{Lie}(U_\alpha) = \mathbf{Z} \cdot X_\alpha$.

2.2. Systèmes de coordonnées sur le groupe unipotent U

Soit U le sous-groupe de G engendré par les $U_\alpha, \alpha > 0$. On sait (cf. [12], exposé XXII, n° 5.5) que l'application produit (relative à l'ordre choisi sur R_+) définit un *isomorphisme de schémas*

$$\prod_{\alpha > 0} U_\alpha \xrightarrow{\sim} U \ .$$

En d'autres termes, tout point u de U, à valeurs dans un anneau commutatif A, s'écrit de façon unique sous la forme

$$u = \prod_{\alpha>0} x_\alpha(t_\alpha), \quad \text{avec } t_\alpha \in A\ .$$

Les t_α forment donc un *système de coordonnées* sur U, valable sur $\mathbf{Z}$.

Mais, si l'on se place sur $\mathbf{Q}$, il y a un autre système de coordonnées qui est tout aussi naturel. En effet, si l'on désigne par $U_{/\mathbf{Q}}$ le groupe algébrique sur $\mathbf{Q}$ déduit de U par changement de base, on dispose de *l'application exponentielle*

$$\exp : \mathrm{Lie}(U)_{/\mathbf{Q}} \to U_{/\mathbf{Q}}\ ,$$

qui est un isomorphisme de groupes algébriques (lorsqu'on munit l'algèbre de Lie nilpotente $\mathrm{Lie}(U)_{/\mathbf{Q}}$ de la structure de groupe donnée par la loi de Hausdorff, cf. [2], Chap. II, §6). Or $\mathrm{Lie}(U)$ est somme directe des $\mathrm{Lie}(U_\alpha)$, $\alpha > 0$, donc a pour base les X_α. On voit donc que tout point u de U, à valeurs dans une $\mathbf{Q}$-algèbre A, s'écrit de façon unique:

$$u = \exp\left(\sum_{\alpha>0} u_\alpha X_\alpha\right), \quad \text{avec } u_\alpha \in A\ .$$

Il s'impose de comparer les deux systèmes de coordonnées (t_α) et (u_α):

Proposition 1. *Avec les notations ci-dessus, on a*

$$u_\alpha = t_\alpha + P_\alpha((t_\beta)_{\beta<\alpha})\ ,$$

où P_α est un polynôme à coefficients dans $\mathbf{Q}$ en les t_β pour $\beta < \alpha$ (et même pour $ht(\beta) < ht(\alpha)$). *De plus, les coefficients des P_α sont p-entiers pour tout nombre premier $p \geqq h$.*

(En d'autres termes, les coefficients des P_α appartiennent à $\mathbf{Z}[1/(h-1)!]$.)

Tout revient à écrire $\prod x_\alpha(t_\alpha)$ comme une exponentielle. Or on a $x_\alpha(t_\alpha) = \exp(t_\alpha X_\alpha)$, par définition des X_α. On peut alors utiliser la *formule de Hausdorff itérée* ([2], *loc.cit.*). Cette formule montre que $\prod \exp(t_\alpha X_\alpha)$ peut s'écrire sous la forme $\exp(v)$, avec

$$\begin{aligned} v &= \sum_\alpha t_\alpha X_\alpha + \frac{1}{2}\sum_{\alpha<\beta} t_\alpha t_\beta\,[X_\alpha, X_\beta] + \cdots \\ &= \sum_\alpha t_\alpha X_\alpha + \sum_\lambda c_\lambda t^\lambda Z_\lambda\ , \end{aligned}$$

où:

- λ est un multi-indice (λ_α) dont le poids total $\sum \lambda_\alpha$ est > 1;
- t^λ est le produit des $t_\alpha^{\lambda_\alpha}$;
- c_λ est un nombre rationnel, qui est p-entier si $p > \sum \lambda_\alpha$;
- Z_λ est une combinaison $\mathbf{Z}$-linéaire de crochets itérés des X_α, de multi-degré λ.

Que v soit de la forme voulue résulte alors des deux faits suivants:

(a) Les Z_λ sont des combinaisons $\mathbf{Z}$-linéaires des X_γ tels que

$$ht(\gamma) = \sum \lambda_\alpha \, ht(X_\alpha) \, .$$

En particulier, leurs X_α-composantes ne font intervenir que des X_β avec $ht(\beta) < ht(\alpha)$, donc $\beta < \alpha$.

(b) Les crochets itérés de poids total $\geqq h$ sont nuls. On peut donc borner la sommation aux λ tels que $\sum \lambda_\alpha < h$, et les coefficients c_λ correspondants sont p-entiers pour tout $p \geqq h$.

Remarques. 1) Il y a un résultat analogue pour le groupe U^- engendré par les U_α avec $\alpha < 0$. Cela se démontre de la même manière (ou cela se déduit du cas déjà traité en changeant R_+ en $-R_+$).

2) Dans la terminologie du n° 2.4 ci-après, la prop. 1 montre que l'isomorphisme

$$\exp : \mathrm{Lie}(U)_{/\mathbf{Q}} \xrightarrow{\sim} U_{/\mathbf{Q}}$$

est "défini sur l'anneau local $\mathbf{Z}_{(p)}$" pour tout $p \geqq h$. Il en est de même de l'isomorphisme réciproque

$$\log : U_{/\mathbf{Q}} \xrightarrow{\sim} \mathrm{Lie}(U)_{/\mathbf{Q}} \, .$$

2.3. *L'homomorphisme principal* (*sur le corps* $\mathbf{Q}$)

Les entiers c_i. Les $\alpha_i^\vee$ forment une base du système de racines dual $R^\vee$. On peut donc définir des entiers $c_1, \ldots, c_r$ par la formule suivante:

$$\sum_{\alpha > 0} \alpha^\vee = \sum c_i \alpha_i^\vee \, .$$

Les c_i sont des entiers $\geqq 1$, dont on trouvera les valeurs dans les Tables de Bourbaki [2], Chap. VI. Par exemple, si R est de type F_4, les c_i sont égaux à $16, 30, 42$ et 22.

Ces entiers jouissent des propriétés suivantes (que nous n'aurons pas à utiliser):

(i) le produit des c_i est égal à $(1/f) \prod m_i(m_i+1)$, où les m_i sont les exposants de R, et f son indice de connexion ([2], *loc.cit.*, p. 230, exerc. 6);

(ii) un nombre premier p divise l'un des c_i si et seulement si l'on a $p < h$.

Le triplet (X, H, Y). On a défini au n° 2.1 des éléments X_i, Y_i, H_i de $\mathrm{Lie}(G)$. En utilisant les c_i ci-dessus, on obtient des éléments

$$H = \sum c_i H_i, \qquad X = \sum X_i, \qquad Y = \sum c_i Y_i \, .$$

Ces éléments satisfont aux relations

$$[H,X] = 2X, \quad [X,Y] = -H, \quad [H,Y] = -2Y \, ,$$

cf. [2], Chap. VIII, §7, n° 5, Lemme 2. Le triplet (X, H, Y) est un $\mathfrak{sl}_2$-*triplet principal* au sens de Bourbaki, [2], Chap. VIII, §11, n° 4. On déduit de là un homomorphisme d'algèbres de Lie: $\mathrm{Lie}(\mathbf{SL}_2) \to \mathrm{Lie}(G)$, lequel donne un homomorphisme de $\mathbf{Q}$-groupes algébriques

$$\varphi : \mathbf{SL}_{2/\mathbf{Q}} \to G_{/\mathbf{Q}} .$$

Noter que l'élément H de $\mathrm{Lie}(T)$ est tel que $\alpha_i(H) = 2$ pour tout i. Il en résulte que, si l'on restreint φ au tore standard $\mathbf{G}_m$ de $\mathbf{SL}_2$, on obtient un homomorphisme $\mathbf{G}_m \to T = (\mathbf{G}_m)^r$ dont toutes les composantes dans $\mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m) = \mathbf{Z}$ sont égales à 2. Cela entraîne que φ est trivial sur le centre μ_2 de $\mathbf{SL}_2$, donc définit un homomorphisme (encore noté φ) de $\mathbf{PGL}_{2/\mathbf{Q}}$ dans $G_{/\mathbf{Q}}$. C'est cet homomorphisme que nous appellerons "homomorphisme principal".

Remarque. Si k est une extension de $\mathbf{Q}$, et si g est un élément semi-simple de $\mathbf{PGL}_2(k)$, l'élément $\varphi(g)$ de $G(k)$ est de type principal au sens du n° 1.3. En effet, quitte à conjuguer g (sur une extension convenable de k), on peut supposer que g appartient au tore standard de $\mathbf{PGL}_2$, tore dont l'image dans G est le tore *diagonal* de T. Le même argument montre que, inversement, tout élément de $G(k)$ de type principal est conjugué d'un tel $\varphi(g)$, après une extension convenable de k. Cela explique la terminologie adoptée au n° 1.3.

2.4. *L'homomorphisme principal* (*sur l'anneau local* $\mathbf{Z}_{(p)}$)

Si p est un nombre premier, on note $\mathbf{Z}_{(p)}$ l'anneau local de $\mathbf{Z}$ en l'idéal premier $p\mathbf{Z}$; c'est le sous-anneau de $\mathbf{Q}$ formé des fractions a/b avec $a, b \in \mathbf{Z}$ et $b \notin p\mathbf{Z}$.

On se propose de passer de $\mathbf{Q}$ à $\mathbf{Z}_{(p)}$. Pour le faire commodément, un peu de terminologie est nécessaire:

Terminologie. Soit A un anneau de valuation discrète de corps des fractions K, et soit S et S' des A-schémas plats. Soient $S_{/K}$ et $S'_{/K}$ les K-schémas qu'on en déduit par le changement de base $A \to K$ ("fibres génériques"). Soit F un K-morphisme de $S_{/K}$ dans $S'_{/K}$. Nous dirons que F est *défini sur* A s'il existe un A-morphisme $f : S \to S'$ qui donne F par changement de base. Un tel f est unique, et nous nous permettrons de le noter encore F.

Dans les cas que nous aurons à considérer, S et S' sont des schémas affines. Leurs algèbres affines Λ et Λ' sont des A-modules plats, c'est-à-dire sans torsion. La donnée de F équivaut à celle d'un K-homomorphisme

$$F^* : K \otimes \Lambda' \to K \otimes \Lambda .$$

Dire que F est *défini sur* A équivaut à dire que F^* *applique* Λ' *dans* Λ, autrement dit que F^* "ne fait pas intervenir de dénominateurs".

L'homomorphisme principal sur $\mathbf{Z}_{(p)}$. Nous allons appliquer ce qui précède au cas où $A = \mathbf{Z}_{(p)}$, $K = \mathbf{Q}$, $S = \mathbf{SL}_{2/A}$, $S' = G_{/A}$ et F est l'homomorphisme

principal

$$\varphi : \mathbf{SL}_{2/\mathbf{Q}} \to G_{/\mathbf{Q}}$$

défini au n° 2.3.

Proposition 2. *Si $p \geqq h$, l'homomorphisme φ est défini sur $\mathbf{Z}_{(p)}$.*

Au langage près, ce résultat est dû à D. Testerman; cf. [32], [33] qui donnent même un énoncé plus général, applicable à des homomorphismes "sous-principaux".

Démonstration de la prop. 2. Notons T_1, U_1 et U_1^- le tore maximal et les sous-groupes radiciels standard de $\mathbf{SL}_2$:

$$T_1 = \mathbf{G}_m, \qquad U_1 = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \qquad U_1^- = \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}.$$

L'application produit $U_1^- \times T_1 \times U_1 \to \mathbf{SL}_2$ définit un *isomorphisme* de $U_1^- \times T_1 \times U_1$ sur un ouvert Ω de $\mathbf{SL}_2$ (grosse cellule). Un point $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathbf{SL}_2$ appartient à Ω si et seulement si a est inversible.

La restriction φ_Ω de φ à $\Omega_{/\mathbf{Q}}$ est un morphisme de $\Omega_{/\mathbf{Q}}$ dans $G_{/\mathbf{Q}}$.

Lemme 1. *Le morphisme φ_Ω est défini sur $\mathbf{Z}_{(p)}$.*

Il suffit de voir que les restrictions de φ à $T_{1/\mathbf{Q}}$, $U_{1/\mathbf{Q}}$ et $U^-_{1/\mathbf{Q}}$ sont définies sur $\mathbf{Z}_{(p)}$. Pour $T_1 = \mathbf{G}_m$ c'est évident. Pour U_1, le morphisme φ est donné par $t \mapsto \exp(\sum tX_i)$, et il est défini sur $\mathbf{Z}_{(p)}$ grâce à l'hypothèse $p \geqq h$, cf. n° 2.2, Remarque 2. Le même argument s'applique à U_1^-.

Revenons maintenant à la démonstration de la prop. 2. Soit $w = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, et soit $\Omega' = w \cdot \Omega$ le translaté de Ω par w. Un point $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathbf{SL}_2$ appartient à Ω' si et seulement si c est inversible. Il en résulte que $\mathbf{SL}_2$ *est réunion des deux ouverts Ω et Ω'*. De plus, on peut écrire w comme produit de deux éléments x, y de $\Omega(\mathbf{Z})$, par exemple $x = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $y = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$. D'après ce qu'on vient de voir, $\varphi(x)$ et $\varphi(y)$ sont des $\mathbf{Z}_{(p)}$-points de G. On déduit de là que la restriction de φ à $\Omega'_{/\mathbf{Q}}$ est définie sur $\mathbf{Z}_{(p)}$. D'où la prop. 2, puisque $\mathbf{SL}_2$ est réunion des ouverts Ω et Ω'.

2.5. *Le sous-groupe $\mathbf{PGL}_2(\mathbf{F}_p)$ de $G(\mathbf{F}_p)$*

A partir de maintenant, on suppose $p \geqq h$ (en fait, on ne s'intéressera par la suite qu'au cas où $p = mh + 1$, avec $m \geqq 1$).

D'après la prop.2, l'homomorphisme principal φ est défini sur $\mathbf{Z}_{(p)}$. Comme $\mathbf{F}_p$ est le corps résiduel de $\mathbf{Z}_{(p)}$, on obtient ainsi, par réduction (mod p), un homomorphisme de $\mathbf{F}_p$-groupes algébriques

$$\tilde{\varphi} : \mathbf{SL}_{2/\mathbf{F}_p} \to G_{/\mathbf{F}_p}.$$

Cet homomorphisme est trivial sur le centre μ_2 de $\mathbf{SL}_{2/\mathbf{F}_p}$. Il définit donc, par passage au quotient, un homomorphisme

$$\mathbf{PGL}_{2/\mathbf{F}_p} \to G_{/\mathbf{F}_p}$$

que nous noterons encore $\tilde{\varphi}$, et que nous appellerons *l'homomorphisme principal* (mod p). Pour tout corps k de caractéristique p, on obtient ainsi un homomorphisme de $\mathbf{PGL}_2(k)$ dans $G(k)$, qui est un *plongement* (car $\tilde{\varphi}$ est visiblement non trivial, donc injectif). Ce plongement a les propriétés suivantes, qui joueront un rôle essentiel dans la suite:

a) *Un élément d'ordre p de $\mathbf{PGL}_2(k)$ est un unipotent régulier de $G(k)$.*

Il suffit de le voir pour l'élément $g = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Or, par construction, $\tilde{\varphi}(g)$ est la réduction (mod p) de $\exp(\sum X_i)$, qui peut lui-même s'écrire (grâce à la prop. 1) sous la forme $\prod_{\alpha>0} x_\alpha(t_\alpha)$, avec $t_\alpha \in \mathbf{Z}_{(p)}$ et $t_\alpha = 1$ si α est l'une des racines simples $\alpha_1, \ldots, \alpha_r$. On a donc $\tilde{\varphi}(g) = \prod x_\alpha(\tilde{t}_\alpha)$, avec $\tilde{t}_\alpha \in \mathbf{F}_p$ et $\tilde{t}_\alpha = 1$ si $\alpha \in \{\alpha_1, \ldots, \alpha_r\}$. Le fait que $\tilde{t}_\alpha \neq 0$ pour $\alpha \in \{\alpha_1, \ldots, \alpha_r\}$ entraîne que $\tilde{\varphi}(g)$ est un unipotent régulier, d'après [31], lemme 3.2.

b) *Tout élément de $\mathbf{PGL}_2(k)$ d'ordre $\neq p$ est de type principal dans $G(k)$, au sens du* n° 1.3.

On peut supposer k algébriquement clos. L'élément considéré est alors conjugué d'un élément de $T_1(k)$, où $T_1 = \mathbf{G}_m$ est le tore maximal standard de $\mathbf{PGL}_2$. Or, par construction de $\tilde{\varphi}$, l'image de ce tore dans le tore maximal $T_{/\mathbf{F}_p}$ est le tore *diagonal*, au sens du n° 1.3. D'où b).

Dans la suite, on appliquera ce qui précède avec $k = \mathbf{F}_p$; cela donne un plongement de $\mathbf{PGL}_2(\mathbf{F}_p)$ dans $G(\mathbf{F}_p)$ ayant les propriétés a) et b) ci-dessus.

2.6. Enoncés des théorèmes de relèvement p-adiques

Distinguons deux cas, suivant que p est égal à $h+1$ ou à $2h+1$:

(i) *Le cas $p = h+1$*

Soit $\mathbf{Z}_p$ l'anneau des entiers p-adiques; c'est le complété de l'anneau local $\mathbf{Z}_{(p)}$ utilisé aux n^{os} 2.4 et 2.5. Son corps résiduel est $\mathbf{F}_p$. La réduction mod p : $\mathbf{Z}_p \to \mathbf{F}_p$ donne un homomorphisme

$$G(\mathbf{Z}_p) \to G(\mathbf{F}_p),$$

qui est surjectif du fait que G est lisse.

Théorème 2. *Si $p = h+1$, le sous-groupe $\mathbf{PGL}_2(\mathbf{F}_p)$ de $G(\mathbf{F}_p)$ défini au* n° 2.5 *se relève dans $G(\mathbf{Z}_p)$.*

(Autrement dit, il existe un sous-groupe fini de $G(\mathbf{Z}_p)$ qui s'applique isomorphiquement sur $\mathbf{PGL}_2(\mathbf{F}_p)$ par réduction mod p.)

Nous donnerons deux démonstrations de ce résultat, l'une au n° 3.3, l'autre au n° 4.4.

(ii) *Le cas* $p = 2h + 1$

Dans ce cas, le th. 2 reste vrai, à condition d'y faire les deux modifications suivantes:

a) L'anneau $\mathbf{Z}_p$ est remplacé par son extension quadratique $\mathbf{Z}_p[\sqrt{p^*}]$, où $p^* = p$ si $p \equiv 1 \pmod 4$ et $p^* = -p$ si $p \equiv 3 \pmod 4$. On notera que cet anneau est encore un anneau de valuation discrète complet, de corps résiduel $\mathbf{F}_p$.

b) On ne peut relever que le sous-groupe $\mathbf{PSL}_2(\mathbf{F}_p)$ de $\mathbf{PGL}_2(\mathbf{F}_p)$.

Autrement dit:

Théorème 3. *Si* $p = 2h + 1$, *le sous-groupe* $\mathbf{PSL}_2(\mathbf{F}_p)$ *de* $G(\mathbf{F}_p)$ *défini au* n° 2.5 *se relève dans* $G(\mathbf{Z}_p[\sqrt{p^*}])$.

La démonstration sera donnée au n° 4.4.

3. Le cas $p = h + 1$

Le but de ce § est de démontrer le th. 2 du n° 2.6: si $p = h + 1$, le sous-groupe $\mathbf{PGL}_2(\mathbf{F}_p)$ de $G(\mathbf{F}_p)$ construit au n° 2.5 peut être relevé en un sous-groupe de $G(\mathbf{Z}_p)$.

3.1. La filtration de $G(\mathbf{Z}_p)$

Soit $E = G(\mathbf{Z}_p)$ le groupe des $\mathbf{Z}_p$-points de G. Si n est un entier $\geqq 0$, l'homomorphisme de réduction (mod p^n)

$$E = G(\mathbf{Z}_p) \to G(\mathbf{Z}/p^n\mathbf{Z})$$

est surjectif puisque G est lisse. Soit E_n son noyau. Les E_n forment une filtration de E:

$$E = E_0 \supset E_1 \supset E_2 \cdots ,$$

et E s'identifie à la limite projective des E/E_n. On a $E/E_1 = G(\mathbf{F}_p)$. Si $n > 0$, le quotient E_n/E_{n+1} est canoniquement isomorphe *à l'algèbre de Lie* $L = \mathrm{Lie}(G_{/\mathbf{F}_p})$ du groupe $G_{/\mathbf{F}_p}$ (cf. par exemple Demazure–Gabriel [11], Chap. II, §4, n° 3).

En particulier, les E_n/E_{n+1} sont des p-groupes élémentaires de rang $N = \dim(G)$, et E_1 est un pro-p-groupe.

3.2. Nullité de la cohomologie de l'algèbre de Lie L

Supposons $p \geqq h$, et soit A le groupe $\mathbf{PGL}_2(\mathbf{F}_p)$, plongé dans $G(\mathbf{F}_p)$ comme on l'a expliqué au n° 2.5. Via la représentation adjointe, A opère sur l'algèbre de Lie L de $G_{/\mathbf{F}_p}$.

Proposition 3. *Supposons que* $p = h + 1$. *Alors le* A*-module* L *est cohomologiquement trivial* (au sens de [24], Chap. IX).

Soit U le sous-groupe d'ordre p de A formé des images des matrices de la forme $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. C'est un p-sous-groupe de Sylow de A. D'après des résultats connus ([24], *loc.cit.*) il suffit de montrer que L est cohomologiquement trivial *comme* U*-module*, ou encore que c'est un module libre sur l'algèbre $\mathbf{F}_p[U]$. Or on a le résultat élémentaire suivant:

Lemme 2. *Soit* C *un groupe cyclique d'ordre premier* p, *et soit* V *un* $k[C]$*-module de dimension finie, où* k *est un corps de caractéristique* p. *Soit* $V^C = H^0(C, V)$ *le sous-espace de* V *fixé par* C. *On a alors*

$$(*) \qquad \dim(V) \leqq p \cdot \dim(V^C),$$

et il y a égalité si et seulement si V *est un* $k[C]$*-module libre.*

On peut supposer que V est indécomposable, auquel cas l'action d'un générateur de C est donnée par une matrice de Jordan d'un certain rang $i \leqq p$. Si $i < p$, on a $\dim(V) = i$, $\dim(V^C) = 1$, et V n'est pas cohomologiquement trivial (on a $\dim H^1(C, V) = 1$). Si $i = p$, on a $\dim(V) = p$, $\dim(V^C) = 1$, et V est $k[C]$-libre de rang 1. D'où le lemme.

(Il y a un résultat analogue lorsqu'on suppose seulement que C est un p-groupe fini, à condition d'écrire l'inégalité $(*)$ sous la forme:

$$\dim(V) \leqq |C| \cdot \dim(V^C),$$

où $|C|$ est l'ordre de C.)

On va appliquer ce lemme à l'action de U sur l'algèbre de Lie L. La dimension de L^U est donnée par le résultat suivant, valable dès que $p > h$:

Lemme 3. *La dimension de* L^U *est égale au rang* r *du groupe* G.

Soit u un générateur de U, et soit $Z_G(u)$ son centralisateur dans le groupe $G_{/\mathbf{F}_p}$. L'hypothèse $p > h$ entraîne que p est "très bon" pour G au sens de Slodowy [28]. Cela permet d'appliquer un théorème de Richardson ([28], p. 38 – voir aussi [30], I.5.1 à I.5.3) qui dit que l'algèbre de Lie de $Z_G(u)$ est égale à L^U (autrement dit, le centralisateur de u au sens schématique est lisse). On a donc $\dim(L^U) = \dim(Z_G(u))$. Mais on a vu au n° 2.5 que u est un élément unipotent *régulier*. Son centralisateur est donc de dimension r (cf. [30], [31]); d'où le lemme. (R. Steinberg m'a fait observer que ce lemme peut se déduire directement du §4 de [31]; il n'est pas nécessaire de renvoyer à [28], ni à [30].)

Revenons maintenant au cas $p = h + 1$. On a alors

$\dim(L) = N = r(h + 1) = rp = p \cdot \dim(L^U)$ d'après le lemme 3.

Vu le lemme 2, cela entraîne que L est $\mathbf{F}_p[U]$-libre; d'où la proposition.

3.3. Démonstration du théorème 2

Si $p = h+1$, il s'agit de prouver que le groupe $A = \mathbf{PGL}_2(\mathbf{F}_p)$ se relève dans le groupe $G(\mathbf{Z}_p) = E = \varprojlim(E/E_n)$, cf. n° 3.1. On raisonne par récurrence sur n, et l'on suppose que A est relevé dans $E/E_n = G(\mathbf{Z}/p^n\mathbf{Z})$. Vu la suite exacte

$$1 \to E_n/E_{n+1} \to E/E_{n+1} \to E/E_n \to 1\,,$$

l'obstruction à relever A dans E/E_{n+1} est un élément du groupe de cohomologie $H^2(A, E_n/E_{n+1}) = H^2(A, L)$. Comme on a $H^2(A, L) = 0$ d'après la prop. 3, l'obstruction en question est nulle. D'où le résultat cherché.

Remarque. La méthode suivie ici ne s'applique pas sans changement au cas $p = 2h + 1$. En fait, on peut montrer que $\dim H^2(A, L) = 1$ si $p \geqq 2h$.

4. Le cas $p = mh + 1$, $m \geqq 1$

Le but de ce § est de donner une démonstration des théorèmes de relèvement du n° 2.6 qui soit valable aussi bien pour $p = h+1$ (cas déjà traité au §3) que pour $p = 2h + 1$.

Nous supposerons donc que $p = mh + 1$, où m est un entier $\geqq 1$. L'hypothèse "$m = 1$ ou 2" n'interviendra qu'à 1a fin (n° 4.4).

4.1. Le groupe B_m et son relèvement

Définition du groupe B_m. Soit B le sous-groupe de Borel standard du groupe $\mathbf{PGL}_2(\mathbf{F}_p)$, image du groupe triangulaire $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. C'est un groupe d'ordre $p^2 - p$, produit semi-direct de $\mathbf{F}_p^*$ par $\mathbf{F}_p$. Comme $p - 1 = mh$, il existe un unique sous-groupe B_m de B d'indice m dans B. Ce groupe est produit semi-direct d'un groupe cyclique $C_h = \langle\gamma\rangle$ d'ordre h, par un sous-groupe cyclique $C_p = \langle u\rangle$ d'ordre p. On a

$$\gamma\, u\, \gamma^{-1} = u^i\,,$$

où i est un élément de $\mathbf{F}_p^*$ d'ordre h. On peut choisir pour γ et u les éléments de $\mathbf{PGL}_2(\mathbf{F}_p)$ représentés par $\left(\begin{smallmatrix} i & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Définition de l'anneau R_m. Soit z_p une racine primitive p-ième de l'unité (dans une clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$). Comme m divise $p-1$, le corps cyclotomique $\mathbf{Q}(z_p)$ contient un unique sous-corps K_m qui est de degré m sur $\mathbf{Q}$; à isomorphisme près, K_m est l'unique extension cyclique de $\mathbf{Q}$, de degré m, qui soit non ramifiée en dehors de p. Pour $m = 1$, on a $K_m = \mathbf{Q}$; pour $m = 2$, on a $K_m = \mathbf{Q}(\sqrt{p^*})$, avec $p^* = \pm p$, le signe étant choisi de telle sorte que $p^* \equiv 1 \pmod 4$, cf. n° 2.6.

Soit R_m l'anneau des entiers de K_m. Comme p est totalement ramifié dans K_m, l'anneau R_m possède un unique idéal premier $\mathfrak{p}_m$ divisant p. Le complété de R_m en $\mathfrak{p}_m$ sera noté $\hat{R}_m$; son corps résiduel est $\mathbf{F}_p$. Pour $m = 1$, on a $\hat{R}_m = \mathbf{Z}_p$; pour $m = 2$, on a $\hat{R}_m = \mathbf{Z}_p[\sqrt{p^*}]$.

Un théorème de relèvement. Identifions $\mathbf{PGL}_2(\mathbf{F}_p)$ à un sous-groupe de $G(\mathbf{F}_p)$ comme au n° 2.5. Les groupes B et B_m deviennent ainsi des sous-groupes de $G(\mathbf{F}_p)$. Comme $\mathbf{F}_p$ est quotient de $\hat{R}_m$, on a un homomorphisme

$$G(\hat{R}_m) \to G(\mathbf{F}_p)\,,$$

qui est surjectif puisque G est lisse.

Théorème 4. *Le sous-groupe B_m de $G(\mathbf{F}_p)$ est relevable dans $G(\hat{R}_m)$.*

La démonstration de ce théorème fait l'objet des n°s 4.2 et 4.3 ci-dessous. On verra au n° 4.4 comment on en déduit les théorèmes 2 et 3 du n° 2.5, lorsque $m = 1, 2$.

4.2. Certains éléments d'ordre p de G

Dans ce n°, k est un corps algébriquement clos de caractéristique 0.

Proposition 4. *Il existe un couple d'éléments (c,x) de $G(k)$ ayant les propriétés suivantes*:

(1) *c est un élément régulier d'ordre h de type principal* (au sens du n° 1.3, et aussi au sens de Kostant [18]);

(2) *x est un élément régulier d'ordre p*;

(3) *On a $cxc^{-1} = x^i$, où i est un élément donné de $\mathbf{F}_p^*$ d'ordre h.*

(Ces propriétés entraînent que le groupe $\langle c,x\rangle$ engendré par c et x est isomorphe au groupe B_m du n° 4.1.)

Démonstration. Soit N le normalisateur du tore maximal T. Le quotient $W = N/T$ est le groupe de Weyl du système de racines R. Soit w un élément de Coxeter de W ([2], Chap. V, §6), et soit c un représentant de w dans $N(k)$. D'après Kostant [18], l'élément c satisfait à (1) : c'est un élément régulier, d'ordre h, et de type principal (de plus, tout élément régulier d'ordre h de $G(k)$ est conjugué de c).

Soit $T[p]$ le groupe des points de division par p dans le tore $T(k)$. L'élément c agit par conjugaison sur $T[p]$, via l'élément de Coxeter w. Comme l'ordre h de c est premier à p, cette action est semi-simple; les valeurs propres de c sont les réductions en caractéristique p des valeurs propres de w dans sa représentation naturelle de rang r. Or on sait ([2], *loc.cit.*) que ces dernières contiennent, avec multiplicité 1, toutes les racines primitives h-ièmes de l'unité. Le même résultat est donc vrai en caractéristique p. On en déduit qu'il existe $x \in T[p]$, $x \neq 1$, tel que $cxc^{-1} = x^i$.

Il reste à montrer que x est régulier, i.e. que l'on a $\alpha(x) \neq 1$ pour toute racine α. Soit $R(x)$ le sous-ensemble de R formé des α tels que $\alpha(x) = 1$, et soit $W(x)$ le sous-groupe de W engendré par les symétries s_α avec $\alpha \in R(x)$. Il est clair que x est fixé par $W(x)$. De plus, $W(x)$ est normalisé par le sous-groupe $\langle w \rangle$ de W engendré par l'élément de Coxeter w, et l'on a $\langle w \rangle \cap W(x) = 1$. Soit $W'(x)$ le produit semi-direct $\langle w \rangle \cdot W(x)$. Notons $D(x)$ le sous-groupe de $T[p]$ engendré par x. Puisque la valeur propre i de w sur $T[p]$ est de multiplicité 1, $D(x)$ est égal à l'ensemble des $y \in T[p]$ tels que $w(y) = y^i$ et il en résulte que $D(x)$ est *stable* par $W'(x)$. Si l'on emploie une notation additive dans $T[p]$, cela entraîne que $D(x)$ est une *droite* du $\mathbf{F}_p$-espace vectoriel $T[p]$, qui est stable par $W'(x)$; de plus l'action de $W(x)$ sur $D(x)$ est triviale, et l'action de w se fait par une racine primitive h-ième de l'unité. Or p est premier à l'ordre de W (car $p > h$) donc *a fortiori* à l'ordre de $W'(x)$. On déduit de là, et d'une forme élémentaire de la théorie de Brauer, que la représentation géométrique de $W'(x)$, en caractéristique 0, contient une représentation de dimension 1 du même type que $D(x)$. En d'autres termes, si l'on note $V_{\mathbf{C}}$ le complexifié de la représentation géométrique de W, il existe $x_0 \neq 0$ dans $V_{\mathbf{C}}$ ayant les deux propriétés suivantes:

a) x_0 est fixé par $W(x)$;

b) $w(x_0) = \lambda x_0$, où λ est une racine primitive h-ième de l'unité.

Mais on sait ([2], Chap. V, p. 121, Remarque) qu'un tel x_0 n'appartient à aucun hyperplan radiciel (i.e. w est un élément *régulier* de W, au sens de Springer [29]). On a donc $s_\alpha(x_0) \neq x_0$ pour tout $\alpha \in R$. Vu a), cela entraîne qu'aucune symétrie s_α n'appartient à $W(x)$, autrement dit que l'ensemble noté plus haut $R(x)$ est vide; d'où le fait que x est régulier.

Remarques. 1) Le fait que x soit régulier peut aussi se déduire du th. 1 de Pianzola [23].

2) Si c et x sont comme ci-dessus, il est bien connu que la classe de c est **Q**-*rationnelle* au sens du n° 8.1, autrement dit que c est conjugué de c^j pour tout j premier à h (c'est en effet la seule classe de conjugaison formée d'éléments réguliers d'ordre h). Quant à la classe de x, la propriété (3) de la prop. 4 montre qu'elle est rationnelle sur le corps K_m du n° 4.1; il n'est d'ailleurs pas difficile de démontrer que son corps de rationalité est *égal* à K_m.

3) Soit $\tilde{G}$ le revêtement universel de G. Le noyau de $\tilde{G} \to G$ est d'ordre $\leqq h$, donc premier à p. Il en résulte que x se relève *de façon unique* en un élément $\tilde{x}$ d'ordre p de $\tilde{G}(k)$; la classe de $\tilde{x}$ est rationnelle sur K_m.

Valeurs des caractères de $\tilde{G}$ sur $\tilde{x}$. On va s'intéresser aux valeurs que prennent sur $\tilde{x}$ les caractères des représentations linéaires de $\tilde{G}$.

Notons $R(\tilde{G})$ le *groupe de Grothendieck* de la catégorie des représentations linéaires de $\tilde{G}$ (sur **Z**, ou sur un corps: c'est la même chose d'après [26], th. 4 et th. 5). Si P désigne le *groupe des poids* du système de racines R, on sait (*loc.cit.*) que l'on a un isomorphisme naturel

$$R(\tilde{G}) = \mathbf{Z}[P]^W ,$$

où $\mathbf{Z}[P]^W$ est *l'anneau des invariants exponentiels* de R ([2], Chap. VI, §3), i.e. la sous-algèbre de $\mathbf{Z}[P]$ formée des éléments invariants par W. Si $f \in R(\tilde{G})$, et si z est un point de $\tilde{G}$, on notera $f(z)$ la *trace* de z dans la représentation (virtuelle) de $\tilde{G}$ associée à f. Cela permet d'interpréter les éléments de $R(\tilde{G})$ comme des morphismes de $\tilde{G}$ dans la droite affine **Aff**, invariants par conjugaison ("fonctions centrales sur $\mathbf{Z}$").

Notons $\deg : R(\tilde{G}) \to \mathbf{Z}$ l'homomorphisme "degré"; avec les notations ci-dessus, on a $\deg(f) = f(1)$.

Proposition 5. *Soit $\tilde{x}$ un élément d'ordre p de $\tilde{G}(k)$ du type ci-dessus, et soit $f \in R(\tilde{G})$. Alors*:

(a) *$f(\tilde{x})$ appartient à l'anneau R_m du* n° 4.1.

(b) *On a $f(\tilde{x}) \equiv \deg(f) \pmod{\mathfrak{p}_m}$, où $\mathfrak{p}_m$ désigne l'idéal premier de R_m divisant p*, cf. n° 4.1.

(Lorsque $m = 1$, (a) signifie que $f(\tilde{x})$ appartient à $\mathbf{Z}$.)

Il suffit de prouver (a) et (b) lorsque f correspond à une représentation linéaire de $\tilde{G}$ (et pas seulement à une représentation virtuelle): le cas général en résulte par linéarité. Or, dans ce cas, le fait que la classe de $\tilde{x}$ soit K_m-rationnelle entraîne $f(\tilde{x}) \in K_m$, cf. n° 8.2. De plus, si $d = \deg(f)$, il est clair que $f(\tilde{x})$ est somme de d racines p-ièmes de l'unité, donc est un entier algébrique. D'où $f(\tilde{x}) \in R_m$. Enfin, la réduction en caractéristique p d'une racine p-ième de l'unité est égale à 1. On en conclut que l'image de $f(\tilde{x})$ dans $\mathbf{F}_p$ est égale à $d \pmod{p}$, d'où (b).

4.3. Relèvement de B_m

Dans ce n°, tous les schémas considérés sont *sur l'anneau $\hat{R}_m$*. Pour alléger les notations, on se permet de noter G le schéma en groupes sur $\hat{R}_m$ déduit du $\mathbf{Z}$-schéma G par le changement de base $\mathbf{Z} \to \hat{R}_m$; même convention pour $\tilde{G}$, ainsi que pour la droite affine **Aff**.

Le morphisme **f**. On sait ([2], Chap. VI, §3) que l'algèbre $R(\tilde{G}) = \mathbf{Z}[P]^W$ est isomorphe à une algèbre de polynômes en r générateurs. On peut donc choisir des éléments $f_1, \ldots, f_r$ de $R(\tilde{G})$, algébriquement indépendants, qui engendrent $R(\tilde{G})$; un choix possible consiste à prendre des f_i correspondant aux r représentations fondamentales de $\tilde{G}$, cf. [2], Chap. VIII, §7, th. 2.

Soit $(f_1, \ldots, f_r)$ une telle famille de générateurs. Les f_i définissent un morphisme

$$\mathbf{f} : \tilde{G} \to \mathbf{Aff}^{\mathrm{r}},$$

où $\mathbf{Aff}^{\mathrm{r}}$ est le produit de r copies de la droite affine **Aff**.

L'ouvert $\tilde{G}^{\mathrm{reg}}$. Nous noterons $\tilde{G}^{\mathrm{reg}}$ l'ouvert de $\tilde{G}$ formé des points en lesquels le morphisme **f** ci-dessus est *lisse*. Il est clair que cette définition ne dépend pas du choix du système générateur $(f_1, \ldots, f_r)$. D'après un théorème de Steinberg

([31], th. 8.1) un point de $\tilde{G}$ à valeurs dans un corps K appartient à G^{reg} si et seulement si il est *régulier*.

(Noter que tout ceci pourrait se faire sur un anneau quelconque.)

Considérons maintenant le point $\tilde{x}$ de $\tilde{G}$ défini au n° précédent. D'après la prop. 5, les scalaires $a_i = f_i(\tilde{x})$ appartiennent à l'anneau $\hat{R}_m$. Ils définissent donc un point $\mathbf{a} = (a_1, \ldots, a_r)$ de $\mathbf{Aff}^{\mathrm{r}}(\hat{R}_m)$.

Soit $Y = \mathbf{f}^{-1}(\mathbf{a})$ le sous-schéma de $\tilde{G}^{\mathrm{reg}}$ défini par l'équation $\mathbf{f}(g) = \mathbf{a}$. C'est un $\hat{R}_m$-schéma lisse. On peut l'interpréter comme la "classe de conjugaison schématique" de $\tilde{x}$. On a en effet:

Proposition 6. (a) *Soit k un corps algébriquement clos contenant $\hat{R}_m$. Pour qu'un élément de $\tilde{G}(k)$ appartienne à $Y(k)$, il faut et il suffit qu'il soit conjugué de $\tilde{x}$.*

(b) *Soit k un corps de caractéristique p. Pour qu'un élément de $\tilde{G}(k)$ appartienne à $Y(k)$, il faut et il suffit qu'il soit unipotent régulier.*

Dans le cas (a), il est clair que tout conjugué de $\tilde{x}$ est dans $\tilde{G}^{\mathrm{reg}}$ (en effet $\tilde{x}$ est régulier, puisque x l'est), et a même image par $\mathbf{f}$ que $\tilde{x}$; un tel conjugué appartient donc à $Y(k)$. Inversement, si $g \in Y(k)$, le fait que g et $\tilde{x}$ soient tous deux réguliers et aient même image par $\mathbf{f}$ entraîne que g et $\tilde{x}$ sont conjugués ([31], cor. 6.6).

Dans le cas (b), on remarque que, d'après la prop. 5 (b), les a_i ont même image que $f_i(1)$ dans $\mathbf{F}_p$. Les points de $Y(k)$ sont donc les éléments réguliers g de $\tilde{G}(k)$ tels que $\mathbf{f}(g) = \mathbf{f}(1)$. D'après [31], cor. 6.7, ce sont les éléments unipotents réguliers de $\tilde{G}(k)$.

Corollaire. *Si g est un point de Y* (à valeurs dans un anneau quelconque) *on a $g^p = 1$.*

En effet, comme Y est lisse, il suffit de le vérifier pour les points à valeurs dans des corps de caractéristique 0, et cela résulte alors de (a).

Revenons maintenant à la démonstration du th. 4, i.e. au relèvement du sous-groupe B_m de $G(\mathbf{F}_p)$ engendré par γ et u. Rappelons les propriétés de ces éléments:

γ est d'ordre h;
u est un élément unipotent régulier d'ordre p;
on a $\gamma u \gamma^{-1} = u^i$, avec $i \in \mathbf{F}_p^*$ d'ordre h.

Comme u est unipotent, il est l'image d'un unique unipotent $\tilde{u}$ de $\tilde{G}(\mathbf{F}_p)$, qui est régulier puisque u l'est. D'après la prop. 6(b), $\tilde{u}$ appartient à $Y(\mathbf{F}_p)$. Vu la lissité de Y, cela montre déjà que $\tilde{u}$ se relève en un point de $Y(\hat{R}_m)$, lequel est d'ordre p d'après le cor. à la prop. 6. Toutefois, ce résultat ne suffit pas: il faut relever $\tilde{u}$ de façon "équivariante" vis-à-vis de γ. Cela conduit à introduire un certain automorphisme de Y:

L'automorphisme τ. L'ordre h de γ est premier à p; cela entraîne que γ se relève en un élément d'ordre h de $G(\hat{R}_m)$, élément que nous noterons encore γ.

Comme G s'identifie à un sous-groupe de Aut $\tilde{G}$, γ définit un automorphisme Int_γ de $\tilde{G}$, d'ordre h. Cet automorphisme laisse évidemment stables les schémas $\tilde{G}^{\mathrm{reg}}$ et Y.

D'autre part, tout point g de Y est tel que $g^p = 1$ d'après le corollaire à la prop. 6. De plus, g^i est un point de Y; en effet, il suffit de le prouver pour les points à valeurs dans un corps de caractéristique 0, et cela résulte alors de la prop. 6, et de la propriété analogue pour $\tilde{x}$. L'application $g \mapsto g^i$ définit donc un endomorphisme σ_i de Y. Si $j \in \mathbf{F}_p^*$ est tel que $ij = 1$, on a $\sigma_i \circ \sigma_j = \mathrm{Id}$, ce qui montre que σ_i est un automorphisme de Y. On a $(\sigma_i)^h = \mathrm{Id}$ puisque $i^h = 1$.

On définit un automorphisme τ de Y par $\tau = \sigma_i^{-1} \circ \mathrm{Int}_\gamma$. Comme σ_i et Int_γ commutent, on a $\tau^h = \mathrm{Id}$.

Si l'on applique σ_i et Int_γ à l'élément $\tilde{u}$ de $Y(\mathbf{F}_p)$, on trouve $\sigma_i(\tilde{u}) = \tilde{u}^i$ et $\mathrm{Int}_\gamma(\tilde{u}) = \tilde{u}^i$). Il en résulte que *$\tilde{u}$ est fixé par τ*.

Proposition 7. *Il existe un relèvement $\tilde{z}$ de $\tilde{u}$ dans $Y(\hat{R}_m)$ qui est fixé par τ.*

Si n est un entier > 0, soit A_n le quotient de R_m par la n-ième puissance de l'idéal $\mathfrak{p}_m$. On construit par récurrence sur n un relèvement z_n de u dans $Y(A_n)$ qui soit fixé par τ. Pour $n = 1$, on prend $z_1 = \tilde{u}$. Pour passer de n à $n+1$, on remarque que, comme Y est lisse, les relèvements de z_n dans $Y(A_{n+1})$ forment de façon naturelle un espace homogène principal sous l'espace tangent à la variété $Y_{/\mathbf{F}_p}$ en $\tilde{u}$. Le groupe $\langle\tau\rangle$ opère de façon affine sur cet espace homogène. Comme il est d'ordre premier à p, cette action a un point fixe (prendre le barycentre d'une orbite); on choisit pour z_{n+1} un tel point fixe. Ceci fait, la suite des z_n définit un point $\tilde{z}$ de $Y(\hat{R}_m)$ qui répond à la question.

(On pourrait aussi invoquer le résultat général suivant: si $X \to S$ est un morphisme lisse, et si Γ est un groupe fini de S-automorphismes de X, d'ordre premier aux caractéristiques résiduelles, le sous-schéma X^Γ de X fixé par Γ est lisse sur S. Lorsque S est le spectre d'un corps, cela se trouve démontré dans Iversen [15], prop. 1.3.)

Exemple. Indiquons ce que donnent les constructions ci-dessus dans le cas le plus simple, celui du rang 1. On a alors $G = \mathbf{PGL}_2$, $\tilde{G} = \mathbf{SL}_2$, $h = 2$, $i = -1$, $m = (p-1)/2$, et K_m est le sous-corps réel maximal du corps cyclotomique $\mathbf{Q}(z_p)$. Le morphisme $\mathbf{f} : \mathbf{SL}_2 \to \mathbf{Aff}$ peut être choisi égal à la *trace*. On a $\mathbf{SL}_2^{\mathrm{reg}} = \mathbf{SL}_2 - \mu_2$, où μ_2 est identifié au centre de $\mathbf{SL}_2$. Si l'on écrit les points de $\mathbf{SL}_2$ comme des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ avec $ad - bc = 1$, $\mathbf{SL}_2^{\mathrm{reg}}$ est la réunion des trois ouverts affines suivants: b inversible, c inversible, $a - d$ inversible.

On peut prendre pour $\tilde{x}$ une matrice de valeurs propres z_p et z_p^{-1}. Sa trace est $z_p + z_p^{-1}$. On en déduit que le schéma Y est formé des $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathbf{SL}_2^{\mathrm{reg}}$ tels que $a + d = z_p + z_p^{-1}$. On a $\tilde{u} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et l'on peut prendre pour γ l'image de $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ dans $\mathbf{PGL}_2$. Les automorphismes $\mathrm{Int}_\gamma, \sigma_i$ et τ de Y sont donnés respectivement par:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}, \quad \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \text{ et } \begin{pmatrix} d & b \\ c & a \end{pmatrix}.$$

Le sous-schéma de Y fixé par τ est formé des points $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de Y tels que $a = d$. La prop. 7 dit que l'on peut choisir un tel point, à coordonnées dans $\hat{R}_m$, tel que $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \pmod{\mathfrak{p}_m}$; or c'est immédiat: on prend par exemple $a = (z_p + z_p^{-1})/2,\ b = 1,\ c = a^2 - 1,\ d = a$.

Fin de la démonstration du th. 4. On choisit $\gamma \in G(\hat{R}_m)$ et $\tilde{z} \in \tilde{G}(\hat{R}_m)$ comme ci-dessus. Le fait que $\tilde{z}$ soit un point de Y entraîne que $\tilde{z}^p = 1$; comme de plus $\tilde{z}$ est fixé par τ on a $\mathrm{Int}_\gamma(\tilde{z}) = \tilde{z}^i$. Si z désigne l'image de $\tilde{z}$ dans $G(\hat{R}_m)$, on a donc $z^p = 1$ et $\gamma z \gamma^{-1} = z^i$. Il est alors clair que le groupe engendré par γ et z est un relèvement de B_m dans $G(\hat{R}_m)$.

Remarque. On peut espérer qu'il existe une démonstration plus directe du th. 4, basée sur une construction *explicite* d'un relèvement de B_m et utilisant les représentants canoniques des classes de conjugaison donnés par Steinberg [31], th. 7.9.

4.4. *Application*: *démonstration du* th. 2 *et du* th. 3

On revient maintenant au cas où $m \leqq 2$. Posons:

$$A = \begin{cases} \mathbf{PGL}_2(\mathbf{F}_p) & \text{si } m = 1 \text{ (i.e. } p = h + 1) \\ \mathbf{PSL}_2(\mathbf{F}_p) & \text{si } m = 2 \text{ (i.e. } p = 2h + 1)\,. \end{cases}$$

Dans les deux cas, B_m est un sous-groupe de A : c'est le normalisateur du p-Sylow $C_p = \langle u \rangle$ de A. Soit P le noyau de la projection

$$G(\hat{R}_m) \to G(\mathbf{F}_p)\,.$$

On voit comme au n° 3.1 que P est un pro-p-groupe. Soit E l'image réciproque de A dans $G(\hat{R}_m)$. On a une suite exacte

$$1 \to P \to E \to A \to 1\,.$$

Vu le th. 4, le sous-groupe B_m de A est relevable dans E. En appliquant le th. 5 du n° 7.3, on en déduit que A est relevable. Cela démontre le th. 2 (si $m = 1$) et le th. 3 (si $m = 2$).

Remarque. Il y a en fait *un et un seul* relèvement de A qui prolonge un relèvement donné de B_m. Pour le voir, on applique la prop. 14 du n° 7.3, et l'on est ramené à prouver que *l'action de B_m sur l'algèbre de Lie $L = \mathrm{Lie}(G_{/\mathbf{F}_p})$ n'a pas de point fixe $\neq 0$*. (En effet, un tel point fixe appartient à la fois à l'algèbre de Lie du centralisateur de γ, qui est un tore, et à l'algèbre de Lie du centralisateur de u, qui est un groupe unipotent. Or les algèbres de Lie d'un tore et d'un groupe unipotent ont une intersection triviale.)

5. Changement de corps

Pour compléter les démonstrations des théorèmes 1 et 1′ du §1, il nous reste essentiellement à passer de la caractéristique 0 à une caractéristique quelconque. Comme on va le voir, cela se fait sans difficulté, grâce à la théorie de Bruhat–Tits.

5.1. Bonne réduction

Soit K un corps muni d'une valuation discrète v, de corps résiduel k et d'anneau de valuation O_K.

Soit A un sous-groupe fini de $G(K)$. Supposons que A ait *bonne réduction*, i.e. soit contenu dans $G(O_K)$. L'homomorphisme $G(O_K) \to G(k)$ donne par restriction à A un homomorphisme $A \to G(k)$.

Lemme 4. *Le noyau de $A \to G(k)$ est trivial si k est de caractéristique 0. C'est un ℓ-groupe si k est de caractéristique $\ell > 0$.*

C'est là un résultat standard, que l'on peut démontrer en utilisant une filtration de $G(O_K)$ analogue à celle du n° 3.1.

Lemme 5. *Soit $a \in A$ d'ordre premier à la caractéristique de k, et soit a_0 son image dans $G(k)$. Les deux conditions suivantes sont équivalentes*:

(1) *a est de type principal dans $G(K)$*

(2) *a_0 est de type principal dans $G(k)$.*

(Pour la définition du "type principal", voir n° 1.3.)

Quitte à agrandir K, on peut supposer que K est complet, et aussi que a_0 est conjugué dans $G(k)$ d'un élément du tore maximal T: on a

$$a_0 = g_0 t_0 g_0^{-1}, \text{ avec } g_0 \in G(k) \text{ et } t_0 \in T(k)\,.$$

On peut relever g_0 en un élément g de $G(O_K)$ et conjuguer a par g. On est ainsi ramené au cas où a_0 appartient à $T(k_0)$. Le fait que l'ordre de a soit premier à caract(k) entraîne alors que a_0 possède un relèvement a_1 dans $T(O_K)$, et un seul, qui a même ordre que a_0 et a. Les éléments a et a_1 de $G(O_K)$, étant des relèvements de même ordre de a_0, sont conjugués dans $G(O_K)$; ici encore, cela se voit en utilisant le fait que leurs ordres sont premiers à caract(k). On peut donc remplacer a par a_1, i.e. supposer $a \in T(O_K)$.

Supposons que a soit de type principal. Cela signifie qu'il existe une base B du système de racines R telle que les $\alpha(a), \alpha \in B$, soient égaux entre eux. Il en est alors de même des $\alpha(a_0), \alpha \in B$, qui sont les images des $\alpha(a)$ dans k^*. D'où (1) $\Rightarrow$ (2).

L'implication (2) $\Rightarrow$ (1) se démontre de façon analogue; si la base B est choisie de telle sorte que les $\alpha(a_0), \alpha \in B$, soient égaux entre eux, il en est de même des $\alpha(a)$: en effet, l'application $O_K^* \to k^*$ est injective sur les éléments d'ordre fini premier à caract(k).

5.2. Bonne réduction à conjugaison près

Conservons les notations ci-dessus. Soit K' une extension finie de K, de degré d. Nous dirons que K'/K est *totalement ramifiée* si la valuation v de K se prolonge en une valuation v' de K' dont l'indice de ramification $e(v'/v)$ est égal à d; s'il en est ainsi, v' est unique, et le corps résiduel de K' est égal à k, cf. e.g. [24], Chap. I. On note $O_{K'}$ l'anneau de la valuation v'.

Par exemple, si π est une uniformisante de K, on peut prendre pour K' l'extension $K(\pi^{1/d})$.

Proposition 8. *Il existe une extension finie totalement ramifiée K'/K ayant la propriété suivante*:

$(*)$ *Pour tout sous-groupe fini A de $G(K)$, il existe $g \in G(K')$ tel que gAg^{-1} ait bonne réduction dans $G(K')$* (i.e. $gAg^{-1} \subset G(O_{K'})$).

(Cet énoncé vaut, plus généralement, pour les sous-groupes *bornés* de $G(K)$, au sens de [3].)

Soit X l'immeuble de Bruhat–Tits associé à G et à K, cf. [3], et soit P_0 le sommet de X correspondant au sous-groupe borné $G(O_K)$; soit App l'appartement de X associé au tore T. Notons X', P_0', App$'$ l'immeuble, le sommet, et l'appartement relatifs à une extension totalement ramifiée K' de K. L'immeuble X se plonge de façon naturelle dans l'immeuble X', et ce plongement applique P_0 sur P_0' et App sur App$'$. De plus, si l'on identifie App et App$'$ à $Q \otimes \mathbf{R}$, où Q est le groupe des poids radiciels du systéme dual (Bourbaki [2], Chap. VI, §2), l'isomorphisme App $\to$ App$'$ est donné par $x \mapsto d \cdot x$, où $d = [K' : K]$. Il résulte de ceci que, si d est divisible par un nombre δ convenable (ne dépendant que du système de racines R), *tout sommet*, *et tout barycentre de face*, *de l'appartement* App *devient dans* App$'$ *un translaté de* P_0 *par* Q, donc un conjugué de $P_0 = P_0'$ par un élément de $T(K')$ (ce genre d'argument est bien connu, cf. Gille [14], I.1.3 ainsi que Larsen [20], lemme 2.4). Si d est choisi de cette façon, la propriété $(*)$ est satisfaite. En effet, soit A un sous-groupe fini de $G(K)$. D'après le théorème de point fixe de Bruhat–Tits ([3], Chap. I, §3), A fixe un point de l'immeuble X, que l'on peut supposer être le barycentre d'une face; quitte à conjuguer A par un élément de $G(K)$, on peut aussi supposer que ce point fixe appartient à App, et d'après ce qui précède on peut l'écrire sous la forme $g^{-1}P_0$, avec $g \in G(K')$. Le groupe gAg^{-1} fixe P_0; c'est donc un sous-groupe de $G(O_{K'})$.

Remarque. Le même énoncé est valable sans supposer G adjoint. Le cas simplement connexe est même plus simple, car alors tout sous-groupe borné fixe un sommet de X, et il n'est plus nécessaire de faire intervenir les barycentres des faces. Ainsi, pour le type E_8, il suffit que le degré de K'/K soit divisible par 60.

Corollaire. *Soit A un sous-groupe fini de $G(K)$. Supposons que k soit de caractéristique* 0, *ou que k soit de caractéristique $\ell > 0$ et que A ne possède*

pas de ℓ-sous-groupe normal $\neq 1$. Il existe alors un plongement de A dans $G(k)$ ayant la propriété suivante:

(P) – *Tout élément de A de type principal dans $G(K)$, et d'ordre premier à la caractéristique de k, est de type principal dans $G(k)$.*

Quitte à remplacer K par une extension totalement ramifiée (ce qui ne change pas le corps résiduel k), on peut supposer que A est contenu dans $G(O_K)$. L'homomorphisme $A \to G(O_K) \to G(k)$ est injectif d'après le lemme 4 du n° 5.1. On obtient ainsi un plongement de A dans $G(k)$, qui jouit de la propriété (P) d'après le lemme 5 du n° 5.1.

5.3. Fin de la démonstration des théorèmes 1 *et* 1′

Il suffit de démontrer le th. 1′, qui est plus précis. Cela va se faire en plusieurs étapes.

Posons $A = \mathbf{PGL}_2(\mathbf{F}_p)$ dans le cas (i), et $A = \mathbf{PSL}_2(\mathbf{F}_p)$ dans le cas (ii). Disons qu'un corps K *convient* s'il existe un plongement de A dans $G(K)$ ayant les propriétés du th. 1′:

dans le cas (i), tout élément de A d'ordre premier à caract(K) est de type principal dans $G(K)$;

dans le cas (ii), tout élément de A d'ordre premier à p et à caract(K) est de type principal dans $G(K)$.

(1) *Il existe un corps K de caractéristique* 0 *qui convient*

On prend $K = \mathbf{Q}_p$ dans le cas (i) et $K = \mathbf{Q}_p(\sqrt{p^*})$ dans le cas (ii). Il faut voir que les plongements de A dans $G(K)$ définis aux §§3,4 satisfont aux conditions ci-dessus. Or, si $a \in A$ est d'ordre $\neq p$, c'est un élément de type principal de $G(\mathbf{F}_p)$, par construction; vu le lemme 5, a est de type principal dans $G(K)$. Il reste à voir, dans le cas (i), qu'un élément a de A d'ordre p est de type principal dans $G(K)$. Or, on a $p = h+1$, et l'on a vu que a est *régulier* dans G; ces propriétés entraînent (cf. [16]) que les "coordonnées de Kac" de a sont égales à (2;1,1,...,1), ce qui montre bien que a est de type principal (autre méthode : utiliser le fait que a est conjugué des a^i pour i premier à p, donc que la classe de a est $\mathbf{Q}$-rationnelle, au sens du n° 8.1).

(2) *Il existe un corps de nombres K qui convient*

Tout d'abord, il existe un corps K de type fini sur $\mathbf{Q}$ qui convient: cela résulte de (1), en remarquant que les coordonnées des points de A ne font intervenir qu'un nombre fini d'éléments de K. Soit n le degré de transcendance de K sur $\mathbf{Q}$. Si $n = 0$, K est un corps on nombres et (2) est vrai. Si $n > 0$, on démontre facilement qu'il existe une valuation discrète v de K dont le corps résiduel k est une extension de $\mathbf{Q}$ de degré de transcendance $n-1$. D'après le cor. à la prop. 8, le corps k convient. D'où le résultat cherché, en raisonnant par récurrence sur n.

(3) *Pour tout nombre premier ℓ, il existe un corps fini K de caractéristique ℓ qui convient* (à la seule exception de $\ell = 2, h = 2$)

On choisit un corps de nombres K qui convient, ainsi qu'une valuation discrète v de K dont le corps résiduel k est de caractéristique ℓ. On applique à nouveau le corollaire à la prop. 8, et l'on obtient le plongement cherché. Le cas d'exception provient de ce que, pour $\ell = 2$ et $p = 3$, le groupe A possède un ℓ-sous-groupe normal non trivial.

Les théorèmes 1 et 1′ résultent de (2) et (3), puisque tout corps algébriquement clos contient, soit un corps de nombres, soit un corps fini.

6. Compléments

Ce § donne quelques propriétés des sous-groupes finis de $G(k)$ construits dans les §§ précédents. Pour simplifier, on suppose k algébriquement clos de caractéristique 0.

6.1. Notations

On note $m_1, m_2, \ldots, m_r$ les *exposants* de R, rangés par ordre croissant:

$$1 = m_1 \leqq m_2 \leqq \cdots \leqq m_r = h - 1 .$$

La famille des m_i est symétrique par rapport à $h/2$: on a

$$m_{r+1-i} = h - m_i \quad \text{pour } i = 1, \ldots, r . \tag{1}$$

Si $\alpha \in R$, on note $ht(\alpha)$ la *hauteur* de α, cf. n° 2.1. On définit un élément f de l'anneau $\mathbf{Z}[X, X^{-1}]$ par:

$$f(X) = r + \sum_{\alpha \in R} X^{ht(\alpha)} . \tag{2}$$

D'après Kostant [18], on a:

$$f(X) = \sum_i (X^{m_i} + X^{m_i - 1} + \cdots + X^{-m_i}) , \tag{3}$$

ou encore:

$$(X - 1) f(X) = \sum (X^{m_i + 1} - X^{-m_i}) . \tag{4}$$

Nous aurons besoin de la formule suivante:

Proposition 9. *On a*:

$$(X - 1) f(X) = (X - X^{-h}) \sum X^{m_i} . \tag{5}$$

On utilise (1) pour récrire (4) sous la forme

$$\begin{aligned} 2 \cdot (X - 1) f(X) &= \sum (X^{m_i + 1} - X^{-m_i} + X^{h + 2 - m_i} - X^{m_i - h}) \\ &= (X - X^{-h}) \sum (X^{m_i} + X^{h - m_i}) . \end{aligned}$$

D'où (5) puisque $\sum X^{m_i} = \sum X^{h - m_i}$, d'après (1).

Corollaire. *Soit x un élément inversible $\neq 1$ d'un anneau intègre.*
(a) *Si $x^h = 1$, on a $f(x) = \sum x^{m_i}$.*
(b) *Si $x^{h+1} = 1$, on a $f(x) = 0$.*
(c) *Si $x^{h+2} = 1$, on a $f(x) = -\sum x^{m_i+1}$.*

Si $x^{h+2} = 1$, on a $x^{-h} = x^2$ et la formule (5) donne

$$(x-1)f(x) = (x-x^2)\sum x^{m_i} = -(x-1)\sum x^{m_i+1} .$$

D'où (c), en divisant par $(x-1)$. Les démonstrations de (a) et (b) sont analogues.

6.2. *Le cas $p = h+1$: classes de conjugaison*

Dans ce n° et le suivant, on s'intéresse au sous-groupe $A = \mathbf{PGL}_2(\mathbf{F}_p)$ de $G(k)$ construit au §3.

Commençons par les classes de conjugaison (dans $G(k)$) des éléments de A.

Tout élément $\neq 1$ de A est contenu dans un unique sous-groupe cyclique maximal. Ce sous-groupe est de l'un des trois types suivants:

(a) *Sous-groupe de Cartan déployé*. C'est un groupe cyclique d'ordre $p-1 = h$. Un générateur de ce groupe est un élément "de type principal" de $G(k)$, au sens de Kostant (cf. [18], ainsi que le n° 4.2). Ses coordonnées de Kac (cf. [16]) sont $(1;1,\ldots,1)$; sa classe de conjugaison dans $G(k)$ est $\mathbf{Q}$-rationnelle.

(b) *Sous-groupe d'ordre $p = h+1$*. Un élément $\neq 1$ de ce groupe est du type étudié par Kac dans [16]. Ses coordonnées de Kac sont $(2;1,\ldots,1)$; sa classe de conjugaison dans $G(k)$ est $\mathbf{Q}$-rationnelle.

(c) *Sous-groupe de Cartan non déployé.* C'est un groupe cyclique d'ordre $p+1 = h+2$. Un générateur g de ce groupe est un élément régulier de G (car de type principal et d'ordre $\geqq h$). Le tableau suivant donne, pour les groupes exceptionnels, le corps de rationalité de la classe de conjugaison de g dans $G(k)$:

Type	h	p	ordre de g	corps de rationalité
G_2	6	7	8	$\mathbf{Q}$
F_4, E_6	12	13	14	corps cubique $\mathbf{Q}(z_7 + z_7^{-1})$
E_7	18	19	20	$\mathbf{Q}(\sqrt{5}) = \mathbf{Q}(z_5 + z_5^{-1})$
E_8	30	31	32	$\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(z_8 + z_8^{-1})$.

(Dans ces formules, z_n désigne une racine primitive n-ième de l'unité.)

Indiquons par exemple comment on traite le cas de E_8. Le calcul de la trace de g dans la représentation adjointe de E_8 (cf. n° 6.3) montre que le corps de rationalité de la classe de g contient le corps $\mathbf{Q}(\sqrt{2})$. S'il était distinct de

$\mathbf{Q}(\sqrt{2})$, il serait de degré $\geqq 4$, et les g^i, i impair, appartiendraient à au moins 4 classes de conjugaison différentes. Mais ces classes, comme celle de g, sont régulières. Or la liste des coordonnées de Kac d'une classe régulière d'ordre 32 est facile à faire: avec l'indexation des racines de Bourbaki, c'est:

$$(3;1,1,1,1,1,1,1,1), \quad (1;2,1,1,1,1,1,1,1) \quad \text{et} \quad (1;1,1,1,1,1,1,1,2)\,.$$

Il n'y a donc que 3 telles classes. D'où la contradiction cherchée.

Remarques. 1) Les cas de F_4 et de E_6 sont essentiellement les mêmes: le sous-groupe A de $E_6(k)$ se déduit de celui de $F_4(k)$ par l'injection naturelle de F_4 dans E_6. Même chose pour les injections $C_r \to A_{2r-1}$, $B_r \to D_{r+1}$ et $G_2 \to B_3 \to D_4$. La même remarque s'applique au cas (ii).

2) Si G est de type E_7, on peut se demander quelle est l'image réciproque $\tilde{A}$ de $A = \mathbf{PGL}_2(\mathbf{F}_{19})$ dans le revêtement universel $\tilde{G}$ de G. On trouve que c'est l'unique extension de A par $\{\pm 1\}$ dans laquelle -1 est le seul élément d'ordre 2 (autrement dit les éléments d'ordre 2 de A deviennent d'ordre 4 dans $\tilde{A}$). On peut identifier $\tilde{A}$ au sous-groupe de $\mathbf{SL}_2(\mathbf{F}_{19^2})$ formé des éléments s tels que $\bar{s} = \pm s$, où $s \mapsto \bar{s}$ désigne la conjugaison relativement à l'extension quadratique $\mathbf{F}_{19^2}/\mathbf{F}_{19}$.

6.3. *Le cas $p = h + 1$: la représentation adjointe*

On conserve les notations du n° précédent. L'action de A par conjugaison sur l'algèbre de Lie de G définit une représentation linéaire de A, de dimension N, que nous appellerons la *représentation adjointe* de A dans G. Son caractére sera noté $g \mapsto \mathrm{Tr}_{\mathrm{ad}}(g)$. Pour en donner un calcul explicite, il est commode de prendre pour corps de base le corps $\bar{\mathbf{Q}}_p$, vu que la représentation en question est définie de façon naturelle sur $\mathbf{Q}_p$, et même sur $\mathbf{Z}_p$, cf. §3.

Introduisons d'abord une notation. Si $g \in A$ est d'ordre premier à p, relevons-le en un élément $\tilde{g}$ de $\mathbf{GL}_2(\mathbf{F}_p)$; si λ et μ sont les valeurs propres de $\tilde{g}$, posons $\tilde{x} = \lambda/\mu$. Le couple $(\tilde{x}, \tilde{x}^{-1})$ est bien défini par g. On a $\tilde{x} \in \mathbf{F}_{p^2}^*$; c'est un élément d'ordre égal à celui de g. Le *représentant multiplicatif* de $\tilde{x}$ dans $\bar{\mathbf{Q}}_p$ sera noté x. C'est une racine de l'unité d'ordre égal à l'ordre de g.

Proposition 10. (1) *Si $g \in A$ est d'ordre premier à p, et si x est la racine de l'unité associée à g comme ci-dessus, on a*

$$\mathrm{Tr}_{\mathrm{ad}}(g) = f(x)\,, \tag{6}$$

où f est le polynôme de Laurent défini au n° 6.1.

(2) *Si $g \in A$ est d'ordre p, on a* $\mathrm{Tr}_{\mathrm{ad}}(g) = 0$.

(Noter, dans le cas (1), que $f(x) = f(x^{-1})$, de sorte que l'ambïguité de la définition de x n'a pas d'importance.)

Pour (1), on remarque que les valeurs propres de g opérant sur l'algèbre de Lie de G en caractéristique p sont les $\tilde{x}^{ht(\alpha)}$, ainsi que 1, répété r fois: cela résulte de la définition de l'homomorphisme principal, cf. §2. Les valeurs

propres de g opérant sur l'algèbre de Lie de G en caractéristique 0 sont les représentants multiplicatifs des précédentes. Leur somme est donc égale à $f(x)$, d'après la formule (2).

Lorsque g est d'ordre p, on a vu que c'est un élément du type de Kac, et la trace d'un tel élément dans la représentation adjointe est connue pour être 0. (Cela peut aussi se déduire du fait que la représentation adjointe est définie sur $\mathbf{Z}_p$ par un module projectif.) D'où (2).

Corollaire 1. *Si $g \neq 1$ appartient à un sous-groupe de Cartan déployé, on a*:

$$\mathrm{Tr}_{\mathrm{ad}}(g) = \sum x^{m_i} . \tag{7}$$

Cela résulte de (6), et de la partie (a) du corollaire à la prop. 9, vu que l'on a alors $x^h = 1$ et $x \neq 1$.

Corollaire 2. *Si $g \neq 1$ appartient à un sous-groupe de Cartan non déployé, on a*:

$$\mathrm{Tr}_{\mathrm{ad}}(g) = -\sum x^{m_i+1} . \tag{8}$$

Cela se démontre de manière analogue, en utilisant la partie (c) du corollaire à la prop. 9.

Exemples. (a) Prenons g d'ordre 2 (de type déployé, ou non déployé, peu importe). On a $x = -1$, et les formules (7) et (8) donnent

$$\mathrm{Tr}_{\mathrm{ad}}(g) = r' - r'' ,$$

où r' (resp. r'') est le nombre des i tels que m_i soit pair (resp. impair). Si -1 appartient au groupe de Weyl, on a $r' = 0$, $r'' = r$, d'où

$$\mathrm{Tr}_{\mathrm{ad}}(g) = -r .$$

C'est ce qui se produit pour les types G_2, F_4, E_7, E_8.

(b) Prenons G de type G_2, et g d'ordre 8. Comme $m_1 = 1$, $m_2 = 5$, la formule (8) donne $\mathrm{Tr}_{\mathrm{ad}}(g) = -x^2 - x^6 = 0$ (car $x^4 = -1$ puisque x est d'ordre 8).

(c) Prenons G de type E_8, et g d'ordre 16 dans $\mathbf{PSL}_2(\mathbf{F}_{31})$. La formule (8) donne

$$\mathrm{Tr}_{\mathrm{ad}}(g) = -(x^2 + x^8 + x^{12} + x^{14} + x^{18} + x^{20} + x^{24} + x^{30}) .$$

Comme x est d'ordre 16, on a $x^8 = -1$, d'où:

$$\begin{aligned} \mathrm{Tr}_{\mathrm{ad}}(g) &= -(x^2 - 1 - x^4 - x^{-2} + x^2 + x^4 - 1 + x^{-2}) \\ &= 2 - 2(x^2 + x^{-2}) = 2 \pm 2\sqrt{2} . \end{aligned}$$

On obtient ainsi une valeur de la trace qui avait été déclarée (à tort) impossible dans [6], p. 392–394.

Remarque. Les valeurs de $\mathrm{Tr}_{\mathrm{ad}}(g)$ données dans la prop. 10 et ses corollaires déterminent sans ambiguïté la représentation adjointe de A dans G. Je me borne à énoncer le résultat, sans entrer dans les détails:

Soit s le nombre des i tels que $m_i = h/2$, et soit $t = (r-s)/2$. (On a $s = 1$ si r est impair, et $s = 0$ ou 2 si r est pair, le cas $s = 2$ n'intervenant que pour le type D_r.) On trouve que la représentation en question est somme directe de:

t représentations irréductibles de degré $p+1$, induites à partir des caractères d'exposants m_i, $1 \leqq i \leqq t$ (le caractère "d'exposant m" étant celui qui transforme un élément de $\mathbf{F}_p^*$ en la m-ième puissance de son représentant multiplicatif);

t représentations irréductibles de degré $p-1$, induites (à la Deligne–Lusztig) à partir des caractères d'un sous-groupe de Cartan non déployé d'exposants $m_i + 1, 1 \leqq i \leqq t$ (en un sens analogue au précédent);

s représentations irréductibles de degré p, prolongeant la représentation de Steinberg de $\mathbf{PSL}_2(\mathbf{F}_p)$.

6.4. *Le cas $p = 2h+1$: classes de conjugaison*

Dans ce n° et le suivant, on s'intéresse au cas (ii), où $p = 2h+1$ et $A = \mathbf{PSL}_2(\mathbf{F}_p)$.

Ici encore, il y a trois types de sous-groupes cycliques maximaux:

(a) *Sous-groupe de Cartan déployé*. C'est un groupe cyclique d'ordre $(p-1)/2 = h$. Un générateur de ce groupe est un élément de type principal, au sens de Kostant [18]; sa classe de conjugaison est $\mathbf{Q}$-rationnelle.

(b) *Sous-groupe d'ordre $p = 2h+1$*. Un élément $\neq 1$ de ce groupe est régulier; le corps de rationalité de sa classe de conjugaison est $\mathbf{Q}(\sqrt{p^*})$. Un tel élément n'est pas de type principal, sauf bien sûr si $G = \mathbf{PGL}_2$.

(c) *Sous-groupe de Cartan non déployé, d'ordre $(p+1)/2 = h+1$*. Un générateur de ce groupe est du type de Kac [16]. Sa classe de conjugaison est $\mathbf{Q}$-rationnelle.

Noter que toutes les classes de conjugaison des éléments de A sont rationnelles sur le corps $K = \mathbf{Q}(\sqrt{p^*})$. On peut se poser à ce sujet la question suivante (liée à celle de la Remarque 2) du n° 1.3):

existe-t-il une K-forme G' de G telle que $G'(K)$ contienne A?

6.5. *Le cas $p = 2h+1$: la représentation adjointe*

La représentation adjointe de A dans G se définit comme au n° 6.3, dont on adopte les notations: $\mathrm{Tr}_{\mathrm{ad}}(g)$, x, etc.

L'analogue de la première partie de la prop. 10 est vrai:

Proposition 11. *Si $g \in A$ est d'ordre premier à p, on a $\mathrm{Tr}_{\mathrm{ad}}(g) = f(x)$.*

La démonstration est la même.

On en déduit, grâce au corollaire à la prop. 9:

Corollaire 1. *Si $g \neq 1$ appartient à un sous-groupe de Cartan déployé, on a*

$$\mathrm{Tr}_{\mathrm{ad}}(g) = \sum x^{m_i} . \tag{9}$$

Corollaire 2. *Si $g \neq 1$ appartient à un sous-groupe de Cartan non déployé, on a*

$$\mathrm{Tr}_{\mathrm{ad}}(g) = 0 . \tag{10}$$

Le calcul de la trace d'un élément d'ordre p est moins évident. Comme au n° 6.3, notons s le nombre des i tels que $m_i = h/2$, et posons $t = (r-s)/2$.

Proposition 12. *Si $u \in A$ est d'ordre p, on a*

$$\mathrm{Tr}_{\mathrm{ad}}(u) = (r \pm s\sqrt{p^*})/2 . \tag{11}$$

Soit ρ la représentation adjointe de A dans G. Si l'on décompose ρ en somme de représentations irréductibles, la représentation unité n'intervient pas (car B_2 ne fixe aucun élément $\neq 0$ de l'algèbre de Lie, cf. n° 4.4). Or les autres représentations irréductibles de A sont de degrés $p, (p+1)/2, p+1, (p-1)/2$ et $p-1$. Le degré N de ρ se décompose donc sous la forme

$$N = a(p+1)/2 + b(p-1)/2 + cp, \quad \text{avec } a,b,c \text{ entiers} \geqq 0 .$$

Comme $N = r(h+1) = r(p+1)/2$, on voit que $a \leqq r$ et $r - a + b \equiv 0 \pmod{p}$. Mais on a $r < h$ (cela se vérifie cas par cas), d'où ici $r < (p-1)/2$. On a d'autre part $b(p-1)/2 \leqq N = r(p+1)/2 < (p-1)(p+1)/4$ d'où $b < (p+1)/2$ et finalement $r - a + b < (p-1)/2 + (p+1)/2 = p$. Comme $r - a + b$ est divisible par p, cela entraîne $r = a$, $b = 0$ d'où $c = 0$. Ainsi, la représentation ρ *ne fait intervenir que des représentations irréductibles de degré* $p+1$ *ou* $(p+1)/2$. Comme on connaît son caractère sur le sous-groupe de Cartan déployé, cf. (9), on en déduit que ρ se décompose en somme de:

t représentations irréductibles de degré $p+1$, induites à partir des caractères d'exposants m_i, $1 \leqq i \leqq t$;

s représentations irréductibles de degré $(p+1)/2$.

Or la trace de u dans une représentation irréductible de degré $(p+1)/2$ (resp. $p+1$) est $(1 \pm \sqrt{p^*})/2$ (resp. 1). Cela donne la formule (11) si $s = 0$ ou 1. Dans le cas $s = 2$, il reste à voir que les 2 représentations irréductibles de degré $(p+1)/2$ qui interviennent sont isomorphes. Comme le groupe G est alors de type D_r, un calcul explicite est possible; il donne le résultat voulu. (Inutile de dire que l'on aimerait une démonstration plus directe …)

Corollaire. *Si aucun des m_i n'est égal à $h/2$* (ce qui est le cas pour les types G_2, F_4, E_6 et E_8), *on a* $\mathrm{Tr}_{\mathrm{ad}}(u) = r$.

Annexes

7. Un théorème de relèvement

7.1. Notations

Dans ce section, on note A un groupe fini, B un sous-groupe de A, et p un nombre premier. On s'intéresse au cas où B est "strongly p-embedded" dans A; cela signifie que les deux propriétés suivantes sont satisfaites:

(α) *B contient un p-sous-groupe de Sylow de A*, autrement dit $(A : B)$ est premier à p;

(β) *Pour tout $x \in A-B$, le groupe $B \cap xBx^{-1}$ est d'ordre premier à p.*

On peut reformuler ceci en termes de l'action de A sur l'espace homogène A/B:

(γ) *Si S est un p-sous-groupe de Sylow de A, il existe un point P de A/B qui est fixé par S, et S opère librement sur le complémentaire de P.*

Noter une conséquence de (γ): si p^a est l'ordre de S, on a

$$(A : B) \equiv 1 \pmod{p^a}.$$

Exemples. Soit S un p-sous-groupe de Sylow d'un groupe fini A et choisissons pour B le normalisateur $N_A(S)$ de S dans A. La condition (α) est satisfaite. En ce qui concerne (β), notons que S est l'unique p-Sylow de B, donc que $S \cap xSx^{-1}$ est l'unique p-Sylow de $B \cap xBx^{-1}$. La condition (β) est donc équivalente à:

(β') $S \cap xSx^{-1} = 1$ *pour tout* $x \in A-B$.

Comme $B = N_A(S)$, l'hypothèse $x \in A-B$ équivaut à $xSx^{-1} \neq S$, et l'on voit que (β') peut se récrire:

(β'') *Si S' est un p-Sylow de A distinct de S, on a $S \cap S' = 1$.*

Autrement dit, les p-Sylow de A ont la "propriété d'intersection triviale".

Ceci s'applique notamment lorsque A est l'un des groupes $\mathbf{GL}_2(\mathbf{F}_q)$, $\mathbf{SL}_2(\mathbf{F}_q)$, $\mathbf{PGL}_2(\mathbf{F}_q)$, $\mathbf{PSL}_2(\mathbf{F}_q)$, avec q une puissance de p, et B est un sous-groupe de Borel de A (groupe triangulaire); c'est le cas utilisé au n° 4.4. Autres choix possibles: les groupes de rang relatif 1 sur $\mathbf{F}_q$, par exemple $\mathbf{SU}_3(\mathbf{F}_{q^2})$, ou les groupes de Suzuki et de Ree en caractéristique 2 et 3.

7.2. Comparaison des groupes de cohomologie de A et de B

Soit M un A-module. Pour tout $q > 0$, le groupe de cohomologie $H^q(A, M)$ est un groupe de torsion; notons $H^q(A, M)_{(p)}$ sa composante p-primaire, et définissons de même $H^q(B, M)_{(p)}$.

Soient

$$\mathrm{Res} : H^q(A, M) \to H^q(B, M) \quad \text{et} \quad \mathrm{Cor} : H^q(B, M) \to H^q(A, M)$$

les homomorphismes de *restriction* et de *corestriction* associés au couple (A,B).

Proposition 13. *Si les propriétés* (α) *et* (β) *du* n° 7.1 *sont satisfaites, les homomorphismes*

$$\mathrm{Res} : H^q(A,M)_{(p)} \to H^q(B,M)_{(p)} \quad et \quad \mathrm{Cor} : H^q(B,M)_{(p)} \to H^q(A,M)_{(p)}$$

sont des isomorphismes réciproques l'un de l'autre (quels que soient le A-module M et l'entier $q > 0$).

En d'autres termes, on peut identifier $H^q(A,M)_{(p)}$ à $H^q(B,M)_{(p)}$.

Corollaire. *Si M est un groupe de torsion p-primaire, les homomorphismes*

$$\mathrm{Res} : H^q(A,M) \to H^q(B,M) \quad et \quad \mathrm{Cor} : H^q(B,M) \to H^q(A,M)$$

sont des isomorphismes réciproques l'un de l'autre.

En effet, les groupes $H^q(A,M)$ et $H^q(B,M)$ sont des groupes de torsion p-primaires.

Remarques. 1) La prop. 13 s'étend aux valeurs négatives de q à condition de remplacer les H^q par les groupes de cohomologie $\hat{H}^q$ modifiés à la Tate (cf. e.g. [4], Chap. XII).

2) La prop. 13 admet une réciproque: si un couple (A,B) jouit de la propriété cohomologique énoncée, on peut montrer que (α) et (β) sont satisfaites.

3) Dans le cas de l'*exemple* du n° 7.1, où $B = N_A(S)$, le groupe $H^q(B,M)_{(p)}$ s'identifie au sous-groupe de $H^q(S,M)$ fixé par l'action de B/S ([4], Chap. XII, th. 10.1). On obtient ainsi une description de $H^q(A,M)_{(p)}$ à partir de $H^q(S,M)$ et de l'action de B/S sur ce groupe. C'est le cas traité dans Benson [1], cor. 3.6.19.

Démonstration de la prop. 13. Soit p^a l'ordre d'un p-Sylow S de A, et soit $N = (A : B)$. On a vu au n° 7.1 que $N \equiv 1 \pmod{p^a}$. Or le composé $\mathrm{Cor} \circ \mathrm{Res}$ est égal à la multiplication par N, et l'on a $p^a x = 0$ pour tout $x \in H^q(A,M)_{(p)}$. On en tire: $\mathrm{Cor}(\mathrm{Res}(x)) = Nx = x$, ce qui montre que le composé $\mathrm{Cor} \circ \mathrm{Res}$ est l'identité sur $H^q(A,M)_{(p)}$.

Reste à voir que l'on a $\mathrm{Res} \circ \mathrm{Cor} = 1$ sur $H^q(B,M)_{(p)}$. Décomposons A en:

$$A = \bigcup Ba_jB$$

où les a_j sont des représentants des doubles classes de A mod B, choisis de telle sorte que $a_1 = 1$. Posons $B_j = B \cap a_j B a_j^{-1}$; si $j = 1$, on a $B_j = B$; si $j \neq 1$, on a $a_j \in A - B$, et B_j est d'ordre premier à p vu l'hypothèse (β). D'après une formule connue ([4], Chap. XII, prop. 9.1), le composé $\mathrm{Res} \circ \mathrm{Cor}$ peut s'écrire comme une somme

$$\mathrm{Res} \circ \mathrm{Cor} = \sum f_j ,$$

où $f_j : H^q(B,M) \to H^q(B,M)$ est le composé des trois homomorphismes suivants:

$$\text{restriction} : H^q(B,M) \to H^q(B_j,M)\,,$$

$$\text{conjugaison par } a_j : H^q(B_j,M) \to H^q(a_j^{-1}B_j a_j,M)\,,$$

$$\text{corestriction} : H^q(a_j^{-1}B_j a_j,M) \to H^q(B,M)\,.$$

(Noter que $a_j^{-1}B_j a_j$ est contenu dans B.)

Lorsque $j = 1$, les trois homomorphismes ci-dessus sont l'identité, et l'on a donc $f_j = 1$. Lorsque $j \neq 1$, l'ordre de B_j est premier à p, et la composante p-primaire de $H^q(B_j,M)$ est 0; on a donc $f_j = 0$ sur $H^q(B,M)_{(p)}$. Puisque $\mathrm{Res} \circ \mathrm{Cor}$ est la somme des f_j, on obtient bien la formule voulue, à savoir

$$\mathrm{Res}(\mathrm{Cor}(x)) = x \quad \text{pour tout } x \in H^q(B,M)_{(p)}\,.$$

Variante. On peut aussi démontrer la prop. 13 en introduisant le *module de permutation* $\mathbf{Z}[X]$, où $X = A/B$. Ce module contient le module trivial $\mathbf{Z}$. Soit $I = \mathbf{Z}[X]/\mathbf{Z}$ le module quotient. D'après (γ), le S-module I est isomorphe à un multiple de la représentation régulière de S. On en déduit que $\mathbf{Z}_p \otimes I$ est *cohomologiquement trivial* comme S-module, donc aussi comme A-module (cf. [24], Chap. IX). Cela entraîne (*loc.cit.*) que l'homomorphisme

$$H^q(A, \mathbf{Z}_p \otimes M) \to H^q(A, \mathbf{Z}_p[X] \otimes M)$$

est un isomorphisme. Or le premier de ces deux groupes s'identifie à $H^q(A,M)_{(p)}$ et le second à $H^q(B,M)_{(p)}$ d'après le "lemme de Shapiro". On obtient donc bien un isomorphisme des groupes en question, et il n'est pas difficile de voir que c'est Res et que son inverse est Cor.

7.3. Relèvements

On conserve les notations ci-dessus, et l'on s'intéresse maintenant à une suite exacte

$$1 \to P \to E \to A \to 1\,,$$

où E est un groupe *profini*, et P un sous-groupe ouvert normal de E. On suppose que *P est un pro-p-groupe*.

Théorème 5. *Soit B un sous-groupe de A satisfaisant aux propriétés* (α) *et* (β) *du* n° 7.1. *Soit $\varphi : B \to E$ un relèvement de B dans E. Il existe alors un relèvement $\psi : A \to E$ qui prolonge φ.*

(Par un "relèvement" de B, on entend un homomorphisme $B \to E$ dont le composé avec $E \to A$ soit égal à l'injection $B \to A$.)

Corollaire. *Si l'extension E est scindée au-dessus de B, elle est scindée au-dessus de A.*

Démonstration du th. 5. On procède en trois étapes:

(1) *Le cas où P est abélien fini.* Le groupe P est alors muni d'une structure naturelle de A-module, et l'extension E définit un élément (E) de $H^2(A,P)$. Puisque E est scindée au-dessus de B, la restriction de (E) à B est 0; vu la prop. 13 (appliquée pour $q=2$), on a $(E)=0$, i.e. E est scindée. Choisissons un relèvement $\psi_1 : A \to E$, et soit φ_1 sa restriction à B. On peut écrire φ_1 sous la forme

$$b \mapsto \lambda(b)\,\varphi(b)\,,$$

où $\lambda : B \to P$ est un 1-cocycle. Soit $(\lambda) \in H^1(B,P)$ la classe de ce cocycle. D'après la prop. 13 (appliquée pour $q=1$), il existe un 1-cocycle $\mu : A \to P$ dont la restriction à B est cohomologue à λ. Si l'on note P additivement, cela signifie qu'il existe $z \in P$ tel que

$$\mu(b) = \lambda(b) + b \cdot z - z \quad \text{pour tout } b \in B\,.$$

Quitte à modiifier μ par le cobord $a \mapsto a \cdot z - z$, on peut donc supposer que μ prolonge λ. Revenons alors en notation multiplicative, et posons

$$\psi(a) = \mu(a)^{-1}\psi_1(a) \quad \text{pour tout } a \in A\,.$$

On obtient ainsi un relèvement $\psi : A \to E$, et il est clair que l'on a

$$\psi(b) = \varphi(b) \quad \text{pour tout } b \in B\,.$$

(2) *Le cas où P est fini.* On procède par récurrence sur l'ordre de P. Le cas où P est abélien vient d'être traité. Si P n'est pas abélien, soit $Z(P)$ son centre. On applique l'hypothèse de récurrence à l'extension

$$1 \to P/Z(P) \to E/Z(P) \to A \to 1\,.$$

On en déduit un relèvement $A \to E/Z(P)$ prolongeant le relèvement donné de B. D'où un plongement de A dans $E/Z(P)$; soit E' l'image réciproque de ce sous-groupe dans E. On a une suite exacte

$$1 \to Z(P) \to E' \to A \to 1\,.$$

Par construction, le relèvement donné $B \to E$ est à valeurs dans E'. On peut donc appliquer l'hypothèse de récurrence à l'extension E', et l'on obtient le relèvement cherché.

(3) *Le cas général.* On peut écrire le pro-p-groupe P comme limite projective

$$P = \varprojlim P/P_i\,,$$

où les P_i sont des sous-groupes ouverts de P qui sont normaux dans E (cf. e.g. [25], Chap. I, §1). Pour chaque i on a une extension

$$1 \to P/P_i \to E/P_i \to A \to 1\,,$$

qui est munie d'un relèvement φ_i de B (déduit du relèvement donné φ). Soit X_i l'ensemble des relèvements ψ_i de A dans E/P_i qui prolongent φ_i. Les X_i

forment de façon naturelle un système projectif. Comme ils sont finis et non vides (d'après (2)), leur limite projective est non vide (*loc.cit.* lemme 3). Un élément $\psi = (\psi_i)$ de cette limite projective donne le relèvement cherché.

Unicité du relèvement. Je me borne à un cas simple, qui est celui qui intervient au n° 4.4: on suppose que $P = \varprojlim P/P_n$ $(n = 0, 1, \ldots)$, où les P_n forment une suite décroissante de sous-groupes ouverts de P, normaux dans E, avec $P = P_0$ et P_n/P_{n+1} commutatif pour tout n. On fait en outre l'hypothèse suivante:

(δ) *Pour tout* $n \geqq 0$, *le* B*-module* P_n/P_{n+1} *ne contient aucun élément invariant* $\neq 0$.

Proposition 14. *Si les hypothèses ci-dessus sont satisfaites, il n'existe qu'un seul relèvement* $\psi : A \to E$ *qui prolonge un relèvement donné* $\varphi : B \to E$.

Démonstration. Soient ψ et ψ' deux tels relèvements. On va montrer par récurrence sur n que l'on a

$$\psi'(a) \equiv \psi(a) \pmod{P_n} \quad \text{pour tout } a \in A .$$

Comme P est limite projective des P/P_n, cela montrera bien que $\psi = \psi'$.

Le cas $n = 0$ est clair, puisque $P_0 = P$. Pour passer de n à $n+1$, définissons $\mu : A \to P$ par

$$\psi'(a) = \mu(a)\psi(a) \quad \text{pour tout } a \in A .$$

Vu l'hypothèse de récurrence, les valeurs de μ appartiennent à P_n. Notons

$$\bar{\mu} : A \to P_n/P_{n+1}$$

l'application déduite de μ par passage au quotient $\bmod P_{n+1}$. C'est un 1-cocycle de A à valeurs dans P_n/P_{n+1} et sa restriction à B est 0 puisque l'on a $\psi'(b) = \varphi(b) = \psi(b)$ pour tout $b \in B$. D'après la prop. 13 (appliquée pour $q = 1$), $\bar{\mu}$ est un cobord; en notation additive, cela signifie qu'il existe $z \in P_n/P_{n+1}$ tel que $\bar{\mu}(a) = a \cdot z - z$ pour tout $a \in A$. Comme la restriction de $\bar{\mu}$ à B est 0, on a $b \cdot z = z$ pour tout $b \in B$. Vu l'hypothèse (δ), cela entraîne $z = 0$, d'où $\bar{\mu} = 0$, ce qui montre que μ est à valeurs dans P_{n+1}, et achève la démonstration.

8. Corps de rationalité des classes de conjugaison d'ordre fini

8.1. La notion de corps de rationalité

Soit Γ un groupe, et soit γ un élément de Γ d'ordre fini. Choisissons un entier $n \geqq 1$ tel que $\gamma^n = 1$. Soit Σ un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$. Nous dirons que *la classe de* γ *est* Σ*-rationnelle* si γ et γ^i sont conjugués dans Γ pour tout $i \in \Sigma$.

Soit k un corps de caractéristique première à n, et soit k_n l'extension de k engendrée par les racines n-ièmes de l'unité. Le groupe $\mathrm{Gal}(k_n/k)$ s'identifie à un sous-groupe $\Sigma(k, n)$ de $(\mathbf{Z}/n\mathbf{Z})^*$. Si $i \in \Sigma(k, n)$, on note σ_i l'élément

correspondant de $\mathrm{Gal}(k_n/k)$; on a $\sigma_i(z) = z^i$ pour toute racine n-ième de l'unité z. Si γ est comme ci-dessus, on dit que *la classe de γ est k-rationnelle* si elle est $\Sigma(k,n)$-rationnelle. Cette définition ne dépend pas du choix de l'entier n, pourvu bien sûr que $\gamma^n = 1$.

Par exemple, dire que la classe de γ est $\mathbf{Q}$-*rationnelle* signifie que γ est conjugué à tous les γ^i, avec $(i,n) = 1$, ou encore que les générateurs du groupe cyclique $\langle\gamma\rangle$ sont conjugués entre eux.

Pour γ donné, il existe une plus petite extension de $\mathbf{Q}$ (dans une clôture algébrique $\overline{\mathbf{Q}}$ fixée) sur laquelle la classe de γ est rationnelle. On l'appelle le *corps de rationalité* de la classe en question. Par exemple, si γ est un élément d'ordre p de $\Gamma = \mathbf{SL}_2(\mathbf{F}_p)$, avec p premier > 2, le corps de rationalité de la classe de γ est l'extension quadratique de $\mathbf{Q}$ contenue dans le p-ième corps cyclotomique, i.e. $\mathbf{Q}(\sqrt{p^*})$.

L'énoncé suivant est bien connu:

Proposition 15. *Supposons Γ fini. Il y a équivalence entre*:
(a) *La classe de γ dans Γ est k-rationnelle.*
(b) *Pour tout caractère χ de Γ* (sur une clôture algébrique $\overline{k}$ de k) *on a* $\chi(\gamma) \in k$.

Puisque $\gamma^n = 1$, $\chi(\gamma)$ est somme de racines n-ièmes de l'unité, et appartient au corps k_n. On en déduit que

$$\sigma_i(\chi(\gamma)) = \chi(\gamma^i) \quad \text{pour tout } i \in \Sigma(k,n)\,.$$

Si (a) est vrai, γ et γ^i sont conjugués, d'où $\chi(\gamma^i) = \chi(\gamma)$, et l'on voit que $\chi(\gamma)$ est fixé par tous les σ_i, donc appartient à k, ce qui démontre (b). Inversement, si (b) est vrai, tous les caractères prennent la même valeur sur γ et sur γ^i, et l'on sait que cela entraîne que ces éléments sont conjugués (puisque leur ordre est premier à la caractéristique de k). D'où (a).

Voici un autre résultat élémentaire du même type:

Proposition 16. *Supposons que $\Gamma = \mathbf{GL}_N(K)$, où K est une extension de k, et N un entier positif. Si γ est un élément de Γ d'ordre premier à la caractéristique de k, les propriétés suivantes sont équivalentes*:
(a) *La classe de γ dans $\mathbf{GL}_N(K)$ est k-rationnelle.*
(b) *La classe de γ dans $\mathbf{GL}_N(K)$ contient un élément de $\mathbf{GL}_N(k)$.*
(c) *Les coefficients du polynôme caractéristique de γ appartiennent à k.*

L'implication (b) $\Rightarrow$ (c) est évidente. Inversement, si (c) est vraie, il existe une matrice M de $\mathbf{GL}_N(k)$ ayant même polynôme caractéristique que γ; quitte à remplacer M par sa composante semi-simple, on peut supposer que M est semi-simple (sur k); comme les valeurs propres de M sont des racines n-ièmes de l'unité, M est semi-simple sur K. Les matrices γ et M, étant semi-simples et de même polynôme caractéristique, sont conjuguées dans $\mathbf{GL}_N(K)$. D'où (b). Pour la même raison, (a) signifie que γ et γ^i ont même polynôme caractéristique, quel que soit $i \in \Sigma(k,n)$; d'où (a) $\Leftrightarrow$ (c).

8.2. Le cas des groupes semi-simples

La prop. 16 montre que, au moins pour $\mathbf{GL}_N$, la rationalité d'une classe de conjugaison n'est pas très différente de la rationalité de ses éléments, au sens usuel de ce terme en géométrie algébrique. Nous allons voir qu'il en est de même pour les groupes semi-simples déployés.

Pour simplifier les démonstrations, je supposerai que le corps de base k est *parfait*; soit $\bar{k}$ une clôture algébrique de k. Soit L un groupe semi-simple connexe sur k. On s'intéresse au groupe $\Gamma = L(\bar{k})$. On a tout d'abord:

Proposition 17. *Soit γ un élément de $L(\bar{k})$ d'ordre n premier à la caractéristique de k. Les propriétés suivantes sont équivalentes*:
(a) *La classe de γ dans $L(\bar{k})$ est k-rationnelle.*
(b) *Pour tout caractère χ de L sur $\bar{k}$, on a $\chi(\gamma) \in k$.*

(Par "caractère de L sur $\bar{k}$" on entend la trace d'une représentation linéaire de L définie sur $\bar{k}$.)

La démonstration est la même que celle de la prop. 15. Le point essentiel est que deux éléments semi-simples γ_1 et γ_2 de $L(\bar{k})$ sont conjugués si et seulement si l'on a $\chi(\gamma_1) = \chi(\gamma_2)$ pour tout χ, cf. Steinberg [31], cor. 6.6.

Corollaire. *Supposons L de type intérieur* (voir ci-après). *Les propriétés* (a) *et* (b) *sont alors équivalentes à*:
(c) *La classe de γ dans $L(\bar{k})$ est stable par* $\mathrm{Gal}(\bar{k}/k)$.

(Rappelons que L est dit "de type intérieur" si l'action de $\mathrm{Gal}(\bar{k}/k)$ sur son diagramme de Dynkin est triviale.)

Les caractères irréductibles de L sur $\bar{k}$ correspondent bijectivement aux poids dominants. L'hypothèse "de type intérieur" équivaut à dire qu'ils sont invariants par $\mathrm{Gal}(\bar{k}/k)$. Si $\sigma \in \mathrm{Gal}(\bar{k}/k)$, on a donc

$$\sigma(\chi(\gamma)) = \chi(\sigma(\gamma)) .$$

pour tout χ. La propriété (b) équivaut donc à:

$$\chi(\gamma) = \chi(\sigma(\gamma)) \quad \text{pour tout } \sigma \in \mathrm{Gal}(\bar{k}/k) \text{ et tout } \chi .$$

D'après Steinberg, *loc.cit.*, cela veut dire que γ et $\sigma(\gamma)$ sont conjugués pour tout $\sigma \in \mathrm{Gal}(\bar{k}/k)$, ce qui est (c).

Remarque. L'hypothèse faite sur L est automatiquement satisfaite lorsque le diagramme de Dynkin de L n'a pas d'automorphisme non trivial, par exemple lorsque L est de type G_2, F_4, E_7 ou E_8.

Proposition 18. *Supposons L déployé sur k. Soit f l'ordre du groupe fondamental de L* (autrement dit le degré de l'isogénie $\tilde{L} \to L$, où $\tilde{L}$ est le revêtement universel de L). *Soit $\gamma \in L(\bar{k})$ d'ordre fini n; supposons n premier à f ainsi qu'à la caractéristique de k. Les propriétés* (a), (b), (c) *ci-dessus sont alors équivalentes à*:
(d) *La classe de conjugaison de γ dans $L(\bar{k})$ rencontre $L(k)$.*

L'implication (d) $\Rightarrow$ (c) est claire. Inversement, supposons (c) vérifiée. Puisque $(n, f)=1$, il existe un unique relèvement $\tilde{\gamma}$ de γ dans $L(\bar{k})$ qui est d'ordre n. Si $\sigma \in \mathrm{Gal}(\bar{k}/k), \sigma(\gamma)$ et γ sont conjugués dans $L(k)$, et il en résulte que $\sigma(\tilde{\gamma})$ et $\tilde{\gamma}$ sont conjugués dans $\tilde{L}(k)$. Ainsi, la classe de conjugaison de $\tilde{\gamma}$ dans $L(k)$ est stable par $\mathrm{Gal}(\bar{k}/k)$. D'après un théorème de Steinberg (*loc.cit.*, th. 1.7), cela entraîne que $\tilde{\gamma}$ est conjugué d'un élément de $\tilde{L}(k)$; d'où le fait que γ est conjugué d'un élément de $L(k)$, ce qui prouve (d).

Ce travail a bénéficié d'une abondante correspondance avec A.M. Cohen, R.L. Griess et D. Testerman. Je les remercie vivement tous les trois.

Bibliographie

1. Benson, D.J.: Representations and cohomology (2 vol.). Cambridge University Press, Cambridge, 1991
2. Bourbaki, N.: Groupes et Algèbres de Lie. Chap. II–III, Paris, Masson, 1982; Chap. IV–V–VI, Paris, Masson, 1981; Chap. VII–VIII, Paris, Masson, 1990
3. Bruhat, F., Tits, J.: Groupes réductifs sur un corps local. Publ. Math. I.H.E.S. **41**, 5–252 (1972); II, *ibid.* **60**, 5–184 (1984)
4. Cartan, H., Eilenberg, S.: Homological Algebra. Princeton University Press, Princeton, 1956
5. Chevalley, C.: Certains schémas de groupes semi-simples. Sém. Bourbaki 1960/1961, exposé 219
6. Cohen, A.M., Griess, R.L.: On finite simple subgroups of the complex Lie group of type E_8. A.M.S. Proc. Symp. Pure Math. **47**, vol. II, 367–405 (1987)
7. Cohen, A.M., Griess, R.L., Lisser, B.: The group $L(2, 61)$ embeds in the Lie group of type E_8. Comm. Algebra **21**, 1889–1907 (1993)
8. Cohen, A.M., Wales, D.B.: Finite subgroups of $G_2(\mathbf{C})$. Comm. Algebra **11**, 441–459 (1983)
9. Cohen, A.M., Wales, D.B.: On finite subgroups of $E_6(\mathbf{C})$ and $F_4(\mathbf{C})$ (à paraître)
10. Cohen, A.M., Wales, D.B.: Finite simple subgroups of semisimple complex Lie groups – a survey. In: Groups of Lie type and their geometries. L.M.S. Lecture Notes **207**, 77–96 (1995)
11. Demazure, M., Gabriel, P.: Groupes Algébriques. Masson et North-Holland, Paris-Amsterdam, 1970
12. Demazure, M., Grothendieck, A.: Structure des Schémas en Groupes Réductifs (S.G.A.3, vol. III), Lect. Notes in Math. **153**, Springer-Verlag, 1970
13. Dynkin, E.B.: Sous-algèbres semi-simples des algèbres de Lie semi-simples (en russe), Mat. Sbornik **30**, 349–462; traduction anglaise: A.M.S. Transl. series 2, vol. **6**, 111–244 (1957)
14. Gille, P.: Torseurs sur la droite affine et R-équivalence. Thèse, Orsay, 1994
15. Iversen, B.: A fixed point formula for action of tori on algebraic varieties. Invent. math. **16**, 229–236 (1972)
16. Kac, V.: Simple Lie groups and the Legendre symbol. Lect. Notes in Math. **848**, 110–123 (1981)
17. Kleidman, P.D., Ryba, A.J.E.: Kostant's conjecture holds for $E_7 : L(2, 37) < E_7$ $(\mathbf{C})$. J. Algebra **161**, 316–330 (1993)
18. Kostant, B.: The principal 3-dimensional subgroup and the Betti numbers of a complex simple Lie group. Amer. J. Math. **81**, 973–1032 (1959)
19. Kostant, B.: Groups over $\mathbf{Z}$. A.M.S. Proc. Symp. Pure Math. **9**, 90–98 (1966)
20. Larsen, M.: Maximality of Galois actions for compatible systems. Duke Math. J. (à paraître)

21. Liebeck, M.W., Seitz, G.: Maximal subgroups of exceptional groups of Lie type, finite and algebraic. Geom. Dedicata **25**, 353–387 (1990)
22. Meurman, A.: An embedding of PSL$(2,13)$ in $G_2(\mathbf{C})$. Lect. Notes in Math. **933**, 157–162 (1982)
23. Pianzola, A.: On the regularity and rationality of certain elements of finite order in Lie groups. J. Crelle **377**, 40–48 (1987)
24. Serre, J-P.: Corps Locaux. Hermann, Paris, 1962
25. Serre, J-P.: Cohomologie Galoisienne. Lect. Notes in Math. **5**, Springer-Verlag, 1964; cinquième édition, révisée et complétée, 1994
26. Serre, J-P.: Groupes de Grothendieck des schémas en groupes réductifs déployés. Publ. Math. I.H.E.S. **34**, 37–52 (1968); = Oe.81
27. de Siebenthal, J.: Sur certains sous-groupes de rang un des groupes de Lie clos, C. R. Acad. Sci. Paris **230**, 910–912 (1950)
28. Slodowy, P.: Simple singularities and simple algebraic groups. Lect. Notes in Math. **815**, Springer-Verlag, 1980
29. Springer, T.A.: Regular elements of finite reflection groups. Invent. math. **25**, 159–198 (1974)
30. Springer, T.A., Steinberg, R.: Conjugacy classes. Lect. Notes in Math. **131**, 167–266 (1970)
31. Steinberg, R.: Regular elements of semisimple algebraic groups. Publ. Math. I.H.E.S. **25**, 281–312 (1965)
32. Testerman, D.: The construction of the maximal A_1's in the exceptional algebraic groups. Proc. A.M.S. **116**, 635–644 (1993)
33. Testerman, D.: A_1-type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups, J. Algebra **177**, 34–76 (1995)