SOUS-GROUPES D'INDICE FINI DANS $SL(n, Z)$

PAR H. BASS, M. LAZARD ET J-P. SERRE

Communicated by Deane Montgomery, November 18, 1963

1. **Enoncé du théorème et schéma de démonstration.** Soit n un entier $\geqq 2$, et soit $G(n)=SL(n, Z)$. Si q est un entier $\geqq 1$, nous noterons $G_q(n)$ le noyau de l'homomorphisme canonique

$$SL(n, Z) \to SL(n, Z/qZ).$$

Un sous-groupe de $G(n)$ est appelé un *sous-groupe de congruence* s'il contient l'un des $G_q(n)$. Un tel sous-groupe est évidemment d'indice fini dans $G(n)$. Réciproquement:

THÉORÈME 1. *Si $n \geqq 3$, tout sous-groupe d'indice fini de $SL(n, Z)$ est un groupe de congruence.*[1]

(Pour $n=2$, il est bien connu que l'énoncé analogue est *faux*.)

Soit $\hat{G}(n)$ (resp. $A(n)$) le complété de $G(n)$ pour la topologie des sous-groupes d'indice fini (resp. des sous-groupes de congruence). Les groupes $\hat{G}(n)$ et $A(n)$ sont des groupes *profinis*, cf. [4]. On notera que, d'après le théorème d'approximation dans le groupe SL_n, le groupe $A(n)$ s'identifie au produit des groupes $SL(n, Z_p)$, pour tous les nombres premiers p (on note Z_p l'anneau des entiers p-adiques). Il est clair que $A(n)$ s'identifie au quotient de $\hat{G}(n)$ par un sous-groupe distingué fermé $C(n)$. La suite exacte correspondante:

$$1 \to C(n) \to \hat{G}(n) \to A(n) \to 1$$

sera notée (X_n). *Le Théorème* 1 *équivaut à dire que* $C(n)=1$ *pour* $n \geqq 3$.

L'étude des groupes $C(n)$ utilise la méthode de "suspension" de [1]. De façon précise, soit S: $G(n) \to G(n+1)$ l'homomorphisme défini par la formule:

$$S(x) = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}, \qquad x \in G(n).$$

Cet homomorphisme se prolonge par continuité en un homomorphisme (encore noté S) de la suite exacte (X_n) dans la suite exacte (X_{n+1}); en particulier, S: $C(n) \to C(n+1)$ est bien défini.

[1] (Note ajoutée le 27 novembre 1963.) Nous apprenons que le théorème 1 a été également démontré par J. Mennicke; sa démonstration doit paraître dans les Ann. of Math.

Les trois propriétés suivantes seront démontrées dans les n^{os} 2 et 3:

(1) *Pour* $n \geqq 3$, *l'homomorphisme* S: $C(n-1) \to C(n)$ *est surjectif.*

(2) *Pour* $n \geqq 3$, $C(n)$ *est contenu dans le centre de* $\hat{G}(n)$.

(3) *On a* $H^1(A(2), \boldsymbol{Q}/\boldsymbol{Z}) = \boldsymbol{Z}/12\boldsymbol{Z}$ *et* $H^2(A(2), \boldsymbol{Q}/\boldsymbol{Z}) = 0$. (Il s'agit ici de cohomologie des groupes profinis, cf. [4, Chap. I]; de plus, le groupe $A(2)$ opère trivialement sur le groupe de coefficients $\boldsymbol{Q}/\boldsymbol{Z}$.)

Montrons comment ces propriétés entraînent le Théorème 1:

La suite spectrale des extensions de groupes, appliquée à (X_2) et au groupe de coefficients $I = \boldsymbol{Q}/\boldsymbol{Z}$, donne la suite exacte:

$$0 \to H^1(A(2), I) \to H^1(\hat{G}(2), I) \to H^1(C(2), I)^{A(2)} \to H^2(A(2), I).$$

D'après (3), on a $H^1(A(2), I) = \boldsymbol{Z}/12\boldsymbol{Z}$. D'autre part, le groupe $H^1(\hat{G}(2), I)$ s'identifie à $\mathrm{Hom}(G(2), I)$, qui est aussi cyclique d'ordre 12 (cela se voit, par exemple, sur la présentation standard de $G(2)$ au moyen de deux générateurs x, y liés par les relations $x^4 = 1$, $x^2 = y^3$). Il suit de là que $H^1(A(2), I) \to H^1(\hat{G}(2), I)$ est bijectif. La suite exacte écrite plus haut, jointe à la propriété (3), montre alors que $H^1(C(2), I)^{A(2)} = 0$. Mais ce groupe est dual du quotient $C(2)/D(2)$, où $D(2)$ désigne l'adhérence du groupe de commutateurs $(\hat{G}(2), C(2))$. Ainsi, $(\hat{G}(2), C(2))$ est dense dans $C(2)$. La propriété (1), appliquée au cas $n = 3$, montre alors que $(S(\hat{G}(2)), C(3))$ est dense dans $C(3)$; d'après la propriété (2), on a donc $C(3) = 1$, d'où $C(n) = 1$ pour tout $n \geqq 3$ d'après la propriété (1).

2. **Démonstration des propriétés (1) et (2).** Soit R un anneau commutatif, et soit M un R-module. Un élément $x \in M$ est dit *unimodulaire* s'il existe une forme linéaire f sur M telle que $f(x) = 1$.

LEMME 1. *Soit* $x = (x_1, \cdots, x_m)$ *un élément unimodulaire de* R^m. *Si l'anneau* R *est semi-local, il existe une famille* $(y_2, \cdots, y_m)$ *d'éléments de* R *telle que* $x_1 + y_2x_2 + \cdots + y_mx_m$ *soit inversible dans* R.

Quitte à diviser par le radical de R, on peut supposer que R est semi-simple; dans ce cas, c'est un composé direct de corps commutatifs, et le lemme est immédiat.

Rappelons d'autre part qu'une matrice carrée $s \in \boldsymbol{M}_n(\boldsymbol{Z})$ est dite *élémentaire* si elle est de la forme $s = 1 + aE_{ij}$, avec $i \neq j$, $a \in \boldsymbol{Z}$. Du fait que $\boldsymbol{Z}$ est un anneau *euclidien*, le groupe engendré par les matrices élémentaires est égal à $\boldsymbol{SL}(n, \boldsymbol{Z}) = G(n)$. Pour tout entier $q \geqq 1$, nous noterons $E_q(n)$ le *sous-groupe distingué* de $G(n)$ engendré par les matrices élémentaires appartenant à $G_q(n)$, autrement dit de la forme $1 + aE_{ij}$, avec $i \neq j$, $a \in q\boldsymbol{Z}$.

LEMME 2. *Soient* $x = (x_1, \cdots, x_n)$ *et* $x' = (x_1', \cdots, x_n')$ *deux élé-*

ments de $\mathbf{Z}^n$. Soit I une partie de $[1, n]$ telle que $x_i = x_i'$ pour $i \in I$, et soit $\mathfrak{a}$ l'idéal de $\mathbf{Z}$ engendré par les x_i, $i \in I$. Supposons que l'on ait

$$x_j' \equiv x_j \text{ mod. } q\mathfrak{a} \qquad \textit{pour tout } j \notin I.$$

Il existe alors $s \in E_q(n)$ qui transforme x en x'.

Par hypothèse, on a $x_j' = x_j + \sum_{i \in I} qt_{ij}x_i$, avec $t_{ij} \in \mathbf{Z}$. On prend alors pour s le produit des matrices $1 + qt_{ij}E_{ji}$, pour tous les couples (i, j) tels que $i \in I$, $j \notin I$.

PROPOSITION 1. *Supposons $n \geqq 3$, et $q \geqq 1$. Soient $a = (a_1, \cdots, a_n)$ et $a' = (a_1', \cdots, a_n')$ deux éléments unimodulaires de $\mathbf{Z}^n$ tels que $a \equiv a'$ mod. q. Il existe alors $s \in E_q(n)$ qui transforme a en a'.*

Il est clair que le groupe $E_1(n) = G(n)$ opère transitivement sur l'ensemble des éléments unimodulaires de $\mathbf{Z}^n$. On peut donc supposer que a' est égal au vecteur coordonnée $e_1 = (1, 0, \cdots, 0)$ et que $q > 1$. Posons $a_1 = 1 - r$, avec $r \in q\mathbf{Z}$. L'image de $(a_2, ra_3, \cdots, ra_n)$ dans le $(\mathbf{Z}/a_1\mathbf{Z})$-module $(\mathbf{Z}/a_1\mathbf{Z})^{n-1}$ est unimodulaire. Comme $\mathbf{Z}/a_1\mathbf{Z}$ est semi-local, le Lemme 1 montre qu'il existe des entiers $t_3, \cdots, t_n$ tels que l'élément $b = a_2 + \sum_{i \geqq 3} t_i r a_i$ soit inversible mod. a_1. En appliquant le Lemme 2 avec $I = [3, n]$, on voit qu'il existe $s_1 \in E_q(n)$ tel que $s_1(a)$ soit égal à l'élément $c' = (a_1, b, a_3, \cdots, a_n)$. Comme a_1 et b sont premiers entre eux, le Lemme 2 (appliqué avec $I = [1, 2]$ cette fois) montre qu'il existe $s_2 \in E_q(n)$ transformant c' en $a'' = (a_1, b, r, 0, \cdots, 0)$. Soit maintenant θ l'élément de $SL(n, \mathbf{Z})$ qui laisse fixes les vecteurs coordonnées e_i $(i \neq 3)$ et transforme e_3 en $e_3 + e_1$. On a $\theta e_1 = e_1$, et $\theta a'' = (1, b, r, 0, \cdots, 0)$. Le Lemme 2, appliqué avec $I = \{1\}$, montre qu'il existe $s_3 \in E_q(n)$ transformant $\theta a''$ en e_1. L'élément $\theta^{-1}s_3\theta \cdot s_2 s_1$ transforme alors a en e_1, ce qui achève de démontrer la proposition.

COROLLAIRE 1. *Pour $n \geqq 3$, $G_q(n) = E_q(n) \cdot G_q(n-1)$.*

(On convient d'identifier $G(n-1)$ à un sous-groupe de $G(n)$ au moyen de l'homomorphisme de suspension S.)

Soit $t \in G_q(n)$. On peut appliquer la Proposition 1 aux éléments $e_n = (0, \cdots, 0, 1)$ et $t(e_n)$ de $\mathbf{Z}^n$; il existe donc $s \in E_q(n)$ tel que $st(e_n) = e_n$. La matrice de st est de la forme

$$\begin{pmatrix} A & 0 \\ x & 1 \end{pmatrix},$$

avec $A \in G_q(n-1)$ et $x \in q\mathbf{Z}^{n-1}$. Soit $y = -xA^{-1}$; en multipliant à gauche

$$\begin{pmatrix} A & 0 \\ x & 1 \end{pmatrix} \text{ par } \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix},$$

on obtient

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

qui appartient à $G_q(n-1)$. Comme on a évidemment

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \in E_q(n),$$

cela montre bien que t appartient à $E_q(n) \cdot G_q(n-1)$.

COROLLAIRE 2. *Pour $n \geqq 3$, on a $(G(n), G_q(n)) \subset E_q(n)$.*

Il suffit de prouver que, si $s \in G_q(n)$, et si t est élémentaire, le commutateur $(s, t) = s^{-1}t^{-1}st$ appartient à $E_q(n)$. Après conjugaison, on peut supposer t de la forme

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

avec $x \in \boldsymbol{Z}^{n-1}$; le Corollaire 1 montre qu'on peut d'autre part supposer s de la forme

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

avec $A \in G_q(n-1)$. On a alors:

$$(s, t) = \begin{pmatrix} 1 & 0 \\ x(1 - A) & 1 \end{pmatrix},$$

et il est immédiat que cet élément appartient à $E_q(n)$.

COROLLAIRE 3. *Pour $n \geqq 3$, les sous-groupes $E_q(n)$ sont d'indice fini dans $G(n)$.*

On utilise le lemme suivant, qui est bien connu:

LEMME 3. *Soit $1 \to H \to G \to \pi \to 1$ une suite exacte de groupes. Si π et $G/(G, G)$ sont finis, $G/(G, H)$ l'est aussi.*

(Rappelons la démonstration: il suffit de prouver que $H/(G, H)$ est fini; cela résulte de la suite exacte:

$$H_2(\pi, \boldsymbol{Z}) \to H/(G, H) \to G/(G, G),$$

et du fait que $H_2(\pi, \boldsymbol{Z})$ est fini.)

En appliquant ce lemme au groupe $G=G(n)$, et au sous-groupe distingué $H=G_q(n)$, on voit que $(G(n), G_q(n))$ est d'indice fini dans $G(n)$, et il en est donc de même de $E_q(n)$, d'après le Corollaire 2.

Démonstration des propriétés (1) *et* (2) *du* n°1. Soit $n \geqq 3$. Soit H un sous-groupe d'indice fini de $G(n)$; il existe un sous-groupe distingué H' d'indice fini dans $G(n)$ qui est contenu dans H (par exemple l'intersection des conjugués de H). Si $q=(G: H')$, on a $E_q(n) \subset H'$, puisque $E_q(n)$ est engendré par des puissances q ièmes. Ce résultat, joint au Corollaire 3 ci-dessus, montre que les $E_q(n)$ sont *cofinaux* parmi les sous-groupes d'indice fini de $G(n)$. Cela nous permet d'écrire:

$$\hat{G}(n) = \text{lim. proj. } G(n)/E_q(n), \qquad A(n) = \text{lim. proj. } G(n)/G_q(n),$$

d'où:

$$C(n) = \text{lim. proj. } G_q(n)/E_q(n).$$

Les propriétés (1) et (2) sont alors conséquences immédiates des Corollaires 1 et 2, respectivement.

3. **Cohomologie des groupes $SL(2, Z_p)$.** Posons, pour simplifier les notations:

$$G_p = SL(2, Z_p), \qquad I = Q/Z, \qquad I_p = Q_p/Z_p.$$

Le groupe $A(2)$ est produit des groupes G_p. On en conclut facilement que la propriété (3) du n°1 est conséquence de la proposition plus précise suivante:

PROPOSITION 2. (a) *On a* $H^1(G_2, I)=Z/4Z$, $H^1(G_3, I)=Z/3Z$ *et* $H^1(G_p, I)=0$ *pour* $p \geqq 5$.

(b) *On a* $H^2(G_p, I)=0$ *pour tout* p.

Soit V le groupe des commutateurs de G_p. C'est un sous-groupe ouvert de G_p. L'assertion (a) équivaut à dire que G_p/V est isomorphe à $Z/4Z$ pour $p=2$, $Z/3Z$ pour $p=3$, et est trivial pour $p \geqq 5$, ce qui se vérifie sans difficultés.

Pour prouver (b), il suffit de voir que $H^2(G_p, I_l)=0$ pour tout nombre premier l. Or, si $l \neq p$, les l-groupes de Sylow de G_p sont isomorphes à ceux de $SL(2, F_p)$, et sont cycliques finis (ou quaternioniens si $l=2$); leur deuxième groupe de cohomologie à valeurs dans I_l est donc nul, et l'on a *a fortiori* $H^2(G_p, I_l)=0$. *Reste donc à prouver que* $H^2(G_p, I_p)=0$.

LEMME 4. *On a* $H^1(V, I_p)=0$.

La suite spectrale des extensions de groupes donne la suite exacte:

$$0 \to H^1(G_p/V, I_p) \to H^1(G_p, I_p) \to H^0(G_p/V, H^1(V, I_p)) \to H^2(G_p/V, I_p).$$

Par définition même de V, l'homomorphisme $H^1(G_p/V, I_p)\to H^1(G_p, I_p)$ est bijectif; d'autre part, puisque G_p/V est cyclique, $H^2(G_p/V, I_p)=0$. On en conclut que $H^0(G_p/V, H^1(V, I_p))=0$. Mais G_p/V est un p-groupe, et il en est de même de $H^1(V, I_p)$; d'après un résultat élémentaire, il en résulte bien que $H^1(V, I_p)=0$.

Il résulte de ce lemme que $H^2(G_p, I_p)$ est isomorphe à un sous-groupe de $H^2(V, I_p)$ et il suffit de prouver la nullité de ce dernier groupe, ou encore, *celle de* $H^2(U, I_p)$, *où* U *désigne un* p*-groupe de Sylow de* V. Or, on a le lemme suivant:

LEMME 5. *Soit* P *un pro-*p*-groupe. Supposons vérifiées les conditions suivantes*:

(a) P *est un groupe de Poincaré* (*cf.* [**4**, *Chap. I, n*° 4.5]) *de dimension* 3.

(b) *Le module dualisant de* P *est isomorphe à* I_p (*avec opérateurs triviaux*).

(c) *L'adhérence du groupe des commutateurs* (P, P) *est un sous-groupe ouvert de* P.

On a alors $H^2(P, I_p)=0$.

Comme $I_p=\text{lim. ind. } \mathbf{Z}/p^n\mathbf{Z}$, on a $H^2(P, I_p)=\text{lim. ind. } H^2(P, \mathbf{Z}/p^n\mathbf{Z})$. D'après les hypothèses (a) et (b), $H^2(P, \mathbf{Z}/p^n\mathbf{Z})$ est dual de $H^1(P, \mathbf{Z}/p^n\mathbf{Z})$. Le dual du groupe $H^2(P, I_p)$ est donc isomorphe à lim. proj. $\mathrm{Hom}(P, \mathbf{Z}/p^n\mathbf{Z})$, groupe des homomorphismes de P dans $\mathbf{Z}_p$. D'après (c), ce dernier groupe est réduit à 0.

Tout revient à voir que le groupe U vérifie les hypothèses du lemme précédent. Séparons les cas:

(i) $p=2$. Le groupe U est alors un sous-groupe distingué d'indice 3 dans V (donc d'indice 12 dans G_2); un élément $s\in G_2$ appartient à U si et seulement si $s=1+2t$, où $t\in \mathbf{M}_2(\mathbf{Z}_2)$ est congrue mod. 2 à l'une des quatre matrices

$$0,\quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix},\quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

D'après [**3**, Chap. IV], U est un groupe *p-valuable* (au sens de [**3**, Chap. III, n° 3.1]). Il en résulte que c'est un groupe de Poincaré (loc. cit., Chap. V) et sa dimension est évidemment égale à 3. Le fait que U opère trivialement sur son module dualisant résulte par exemple de ce que U est contenu dans le groupe des commutateurs de G_2 (ou bien, si l'on préfère, de ce que $\mathbf{SL}_2$ est "unimodulaire"). Enfin, la propriété (c) est évidente.

(ii) $p=3$. Le groupe U est alors l'ensemble des $s\in G_3$ tels que $s\equiv 1$ mod. 3. D'après [**3**, Chap. III, n° 3.2.6], c'est un groupe *p-saturable*, donc *a fortiori* p-valuable, et les mêmes arguments que ci-dessus s'appliquent.

(iii) $p \geqq 5$. On a $V = G_p$, et U est donc simplement un p-groupe de Sylow de G_p. D'après [3, Chap. III, n° 3.2.7], c'est un groupe *p-saturable*, et on conclut comme ci-dessus, cqfd.

REMARQUE. Il devrait être possible de démontrer directement la Proposition 2, à partir d'une présentation de $SL(2, Z_p)$ par générateurs et relations (dans le cas d'un corps de base, c'est la méthode de Steinberg [5]).

4. **Compléments.** En combinant le Théorème 1 avec certains résultats de [1] et [2], on obtient:

COROLLAIRE 1. *Tout sous-groupe distingué de* $SL(n, Z)$, $n \geqq 3$, *est l'image réciproque d'un sous-groupe du centre de* $SL(n, Z/qZ)$, *pour un entier* $q \geqq 0$ *convenable.*

Soit maintenant S un ensemble fini de nombres premiers, et soit Z_S l'anneau de fractions de Z relativement à la partie multiplicative engendrée par S. Si q est un entier $\geqq 1$ et premier aux éléments de S, nous noterons $SL_q(n, Z_S)$ le noyau de $SL(n, Z_S) \to SL(n, Z/qZ)$; un sous-groupe de $SL(n, Z_S)$ est appelé un sous-groupe *de S-congruence* s'il contient l'un des $SL_q(n, Z_S)$.

COROLLAIRE 2. *Si* $n \geqq 3$, *tout sous-groupe d'indice fini de* $SL(n, Z_S)$ *est un groupe de S-congruence.*

Cela se démontre sans difficultés, à partir du Théorème 1, et du théorème d'approximation dans le groupe SL_n.

Soit R un sous-anneau de l'anneau des entiers d'un corps de nombres algébriques. Si l'on pose $G_R(n) = SL(n, R)$, on définit comme au n° 1 une extension:

$$1 \to C_R(n) \to \hat{G}_R(n) \to A_R(n) \to 1.$$

On peut se demander si l'on a encore $C_R(n) = 1$ pour $n \geqq 3$. Nous ne savons démontrer que le résultat plus faible suivant:

THÉORÈME 2. *Pour n assez grand, on a*:

(i) $C_R(n)$ *est un groupe fini.*

(ii) *Les propriétés* (1) *et* (2) *du n°* 1 *sont vérifiées pour* $C_R(n)$.

(iii) *Tout sous-groupe distingué de* $G_R(n)$ *est soit fini, soit d'indice fini.*

La démonstration est analogue à celle du Théorème 1. On fait intervenir les deux faits suivants:

(a) $H^2(A_R(n), I)$ est fini (résulte de [3] et [5]).

(b) Pour n assez grand $G_R(n)/(G_R(n), G_R(n))$ est fini (cf. [**2**, n° 4]).

Signalons enfin le cas du groupe *symplectique*:

THÉORÈME 3. *Tout sous-groupe d'indice fini du groupe* $\boldsymbol{Sp}(2n, \boldsymbol{Z})$, $n \geqq 2$, *est un groupe de congruence.*

Le schéma de démonstration est le même que pour le groupe $\boldsymbol{SL}_n$. Les propriétés (1) et (2) se démontrent par des procédés analogues, mais un peu plus compliqués. La propriété (3) résulte simplement de l'égalité $\boldsymbol{Sp}_2 = \boldsymbol{SL}_2$.

BIBLIOGRAPHIE

1. H. Bass, *K-theory and stable algebra*, Inst. Hautes Études Sci. Publ. Math. (àparaître).

2. ———, *The stable structure of quite general linear groups*, Bull. Amer. Math. Soc. **70** (1964), 430–434.

3. M. Lazard, *Groupes analytiques p-adeques*, Inst. Hautes Études Sci. Publ. Math. (àparaître).

4. J.-P. Serre, *Cohomologie galoisienne*, cours au Collège de France 1963 (notes polycopiées).

5. R. Steinberg, *Générateurs, relations et revêtements de groupes algébriques*, Colloque de Bruxelles, 1962, pp. 113–127.

PARIS