SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Groupes de congruence

Séminaire N. Bourbaki, 1968, exp. n° 330, p. 275-291

<http://www.numdam.org/item?id=SB_1966-1968__10__275_0>

Séminaire BOURBAKI
19e année, 1966/67, n°330 Juin 1967

GROUPES DE CONGRUENCE
(d'après H.BASS, H.MATSUMOTO, J.MENNICKE, J.MILNOR, C.MOORE)

par Jean-Pierre SERRE

§ 1. Le problème des groupes de congruence.

1.1. Groupes de congruence.

Soit k un corps de nombres algébriques, et soit O_k l'anneau des entiers de k. Soit G un groupe algébrique linéaire connexe défini sur k, et soit $\Gamma = G_{O_k}$ le groupe des points entiers de G (relativement à un plongement donné de G dans un groupe linéaire GL_n). Un sous-groupe Γ' de Γ est appelé un sous-groupe de congruence s'il existe un idéal $\mathfrak{q}$ non nul de O_k tel que Γ' contienne le sous-groupe $\Gamma_{\mathfrak{q}}$ de Γ formé des éléments g tels que $g \equiv 1 \bmod \mathfrak{q}$. Un tel sous-groupe est d'indice fini dans Γ. Le «problème des groupes de congruence» consiste à savoir si la réciproque est vraie, autrement dit si G vérifie la propriété suivante :

(C) - Tout sous-groupe d'indice fini de Γ est un groupe de congruence.

On vérifie que cette condition ne dépend pas du choix du plongement $G \to GL_n$ (bien que Γ en dépende).

Plus précisément, soit G_k le groupe des points rationnels de G (i.e. le groupe des points de G à valeurs dans k). Définissons une topologie T (resp. T_c) sur G_k en prenant comme base de voisinages de 1 les sous-groupes

d'indice fini de Γ (resp. les sous-groupes de congruence de Γ); ces topologies ne dépendent pas du choix du plongement $G \to GL_n$ [on donnera un peu plus loin une définition intrinsèque de T_c ; quant à T, on peut la caractériser en disant qu'un sous-groupe de G_k est ouvert pour T si et seulement si il contient un sous-groupe arithmétique de G_k, au sens de Borel-Harish-Chandra [4]]. Soit $\hat{G}_k$ (resp. $\bar{G}_k$) le complété de G_k pour T (resp. T_c). Comme T est plus fine que T_c, on a un homomorphisme canonique $\hat{G}_k \to \bar{G}_k$; on voit facilement que cet homomorphisme est surjectif, propre, et que son noyau $C(G)$ est un groupe profini (limite projective de groupes finis). D'où la suite exacte :

$$(1) \qquad 1 \to C(G) \to \hat{G}_k \to \bar{G}_k \to 1 .$$

Si l'on note de même $\hat{\Gamma}$ et $\bar{\Gamma}$ les complétés de Γ pour T et T_c, on a la suite exacte correspondante de groupes profinis :

$$(2) \qquad 1 \to C(G) \to \hat{\Gamma} \to \bar{\Gamma} \to 1 .$$

La condition (C) revient à dire que $T = T_c$, ou encore que $C(G)$ est réduit à $\{1\}$.

Remarque. Soit A_k l'anneau des adèles de k, et soit A_k^f sa composante finie (i.e. le produit restreint des complétés k_v de k pour les diverses classes de valeurs absolues ultramétriques de k). Le groupe $G_{A_k^f}$ des points de G à valeurs dans la k-algèbre A_k^f est muni d'une structure naturelle de groupe localement compact. La topologie que ce groupe induit sur le sous-groupe G_k est la topologie T_c. En particulier, $\bar{G}_k$ s'identifie à l'adhérence de G_k dans $G_{A_k^f}$. Lorsque G vérifie le « théorème d'approximation fort » de Kneser, on a $\bar{G}_k = G_{A_k^f}$ et $\bar{\Gamma} = \prod G_{O_v}$, où O_v désigne l'anneau des entiers de k_v.

1.2. Premiers résultats.

a) La condition (C) est vérifiée lorsque G est un groupe unipotent (facile) ou lorsque G est un tore (Chevalley [5]).

b) Lorsque $G = SL_2$ et $k = \mathbb{Q}$, la condition (C) n'est pas vérifiée (comme le savait déjà Klein) ; le groupe $C(G)$ est infini. Le groupe $SL_2(\mathbb{Z})$ a donc «beaucoup» de sous-groupes d'indice fini qui ne sont pas des groupes de congruence. J'ignore ce qui se passe lorsqu'on remplace $\mathbb{Q}$ par un corps de nombres quelconque.

c) Prenons pour G un groupe semi-simple non simplement connexe. Soit S son revêtement universel, de sorte que $G = S/M$ où M est un groupe algébrique de dimension zéro, non réduit à $\{1\}$. Supposons (ce qui est souvent le cas) que S vérifie le théorème d'approximation fort de Kneser, de sorte que $\bar{S}_k$ s'identifie à $S_{A_k^f}$. Considérons le diagramme commutatif :

$$\begin{array}{ccccccccc} 1 & \to & C(S) & \to & \hat{S}_k & \to & \bar{S}_k & \to & 1 \\ & & \downarrow & & \hat{\pi} \downarrow & & \bar{\pi} \downarrow & & \\ 1 & \to & C(G) & \to & \hat{G}_k & \to & \bar{G}_k & \to & 1 \ . \end{array}$$

Le noyau de $\bar{\pi}$ est $M_{A_k^f}$; c'est un groupe infini. D'autre part, en utilisant le cor.6.11 de Borel-HarishChandra [4], on montre que le noyau de $\hat{\pi}$ est M_k, qui est fini. Si E désigne l'image réciproque du sous-groupe $M_{A_k^f}$ de $\bar{S}_k$ dans $\hat{S}_k$, on en conclut que $C(G)$ contient un sous-groupe isomorphe à E/M_k ; en particulier, $C(G)$ est infini, et G ne vérifie pas (C).

d) A titre de curiosité, mentionnons que le problème des groupes de congruence garde un sens pour les variétés abéliennes. Il n'est résolu (positivement) qu'en dimension 1 (cf. [11]).

1.3. Le cas des groupes SL_n et Sp_{2n}.

Soit μ_k le groupe des racines de l'unité contenues dans k. C'est un groupe cyclique fini d'ordre pair.

THÉORÈME 1.- Soit G l'un des groupes SL_n $(n \geq 3)$ ou Sp_{2n} $(n \geq 2)$.

(i) Si k a au moins un conjugué réel, on a $C(G) = 1$, autrement dit G vérifie (C).

(ii) Si k est totalement imaginaire, $C(G)$ est canoniquement isomorphe à μ_k ; il est contenu dans le centre de $\hat{G}_k$. En particulier, G ne vérifie pas (C).

Pour SL_n, c'est une conséquence d'un théorème plus précis (cf. n° 3.1, th. 6) démontré dans [3]. Le cas de Sp_{2n} est analogue.

Remarque. Le cas particulier $k = \mathbb{Q}$ avait été résolu en 1964 par Mennicke [9] et Bass-Lazard-Serre [2]. Mennicke-Newman (non publié) ont ensuite traité le cas (i), du moins pour le groupe SL_n.

1.4. Le cas des groupes semi-simples déployés.

THÉORÈME 2.- Faisons sur G l'hypothèse suivante :

(H) G est simple, simplement connexe, déployé, de rang ≥ 2. Alors :

(i) Si k a au moins un conjugué réel, on a $C(G) = \{1\}$, autrement dit G vérifie (C).

(ii) Si k est totalement imaginaire, $C(G)$ est isomorphe à un quotient de μ_k ; il est contenu dans le centre de G_k.

Ce résultat est dû à Matsumoto ([7], [8]) ; sa méthode consiste à montrer que $C(G)$ est «plus petit» que le groupe correspondant pour SL_3 et Sp_4 (lequel est donné par le théorème 1). Il faut signaler que Mennicke a annoncé un résultat analogue. D'autre part, si l'on suppose connu que $C(G)$ est contenu dans le centre de G_k, le théorème est une simple conséquence des résultats de C. Moore [10] résumés au § 2.

Remarques.

1) Dans le cas (ii), il conviendrait de déterminer le quotient de μ_k auquel $C(G)$ est isomorphe. Peut-être est-ce toujours μ_k lui-même ?

2) On aimerait pouvoir remplacer l'hypothèse «déployé de rang ≥ 2» par «de rang relatif ≥ 2, au sens de Borel-Tits».

§ 2. Revêtements universels (C. Moore [10]).

2.1. Le cas local.

Soit k_v un corps localement compact, et soit G un groupe algébrique simple, simplement connexe, et déployé sur k_v. Le groupe G_v des points de G rationnels sur k_v est muni d'une structure naturelle de groupe localement compact. On s'intéresse aux extensions centrales de ce groupe, i.e. aux suites exactes

$$(3) \qquad 1 \to M \to E \to G_v \to 1 ,$$

où E et M sont des groupes localement compacts, avec $E/M = G$ (comme groupes topologiques), M étant contenu dans le centre de E.

Exemples.

a) Si $k_v = \mathbf{C}$, le groupe G_v est simplement connexe (au sens topologique), et une telle extension est triviale : E est canoniquement isomorphe à $G_v \times M$.

b) Si $k_v = \mathbb{R}$, le groupe G_v n'est pas simplement connexe ; son groupe fondamental $\pi_1(G_v)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (sauf si G est de type C_n, $n \geq 1$, auquel cas $\pi_1(G_v) = \mathbb{Z}$). Une extension du type (3) est alors déterminée par un élément de $\mathrm{Hom}(\pi_1(G_v), M)$.

c) Prenons pour G le groupe Sp_{2n}, $n \geq 1$. Weil [13] a construit une extension centrale de G_v, avec $M = \{\pm 1\}$, qui est non triviale pourvu que $k_v \neq \mathbb{C}$; c'est le groupe «métaplectique» relativement au corps k_v.

On peut se demander s'il existe une extension centrale

$$(4) \qquad 1 \to \pi_1(G_v) \to \tilde{G}_v \to G_v \to 1$$

telle que toute autre extension (3) s'en déduise par un unique homomorphisme $f_E : \pi_1(G_v) \to M$. L'extension en question s'appelle alors le <u>revêtement universel</u> de G_v, et son noyau $\pi_1(G_v)$ est le <u>groupe fondamental</u> de G_v.

C. Moore ([10], chap. III) a montré <u>l'existence</u> d'un tel revêtement universel et en a déterminé presque complètement la structure. De façon plus précise, bornons-nous au cas où k_v est ultramétrique, et notons μ_v le groupe des racines de l'unité contenues dans k_v. On a :

THÉORÈME 3.- a) <u>Le groupe</u> $\pi_1(G_v)$ <u>est isomorphe à un quotient de</u> μ_v.

b) <u>Lorsque</u> $G = SL_2$, <u>on a</u> $\pi_1(G_v) = \mu_v$.

c) <u>Lorsque</u> k_v <u>est de caractéristique zéro, et que</u> G <u>est isomorphe à</u> SL_n $(n \geq 2)$ <u>ou</u> Sp_{2n} $(n \geq 1)$, <u>on a</u> $\pi_1(G_v) = \mu_v$.

La méthode suivie par C. Moore est analogue à celle de Steinberg [12] dans le cas discret ; la décomposition de Bruhat de G_v y joue un rôle essentiel. On prouve

que toute extension centrale de G_v provient d'un «cocycle de Steinberg». Dans le cas de SL_2, Moore détermine tous ces cocycles ; ils proviennent essentiellement du symbole de restes normiques de Hilbert. D'où b). Lorsque G est de rang ≥ 2, on choisit une racine longue de G ; si H est le sous-groupe de rang 1 attaché à cette racine, Moore montre que $\pi_1(H_v) \to \pi_1(G_v)$ est surjectif. D'où a). Enfin c) se déduit de a) combiné avec le théorème 1.

Remarques.

1) Certains de ces résultats ont été obtenus indépendamment par T. Kubota.

2) C. Moore conjecture que $\pi_1(G_v)$ est toujours égal à μ_v.

2.2. Le cas adélique.

Soit de nouveau k un corps de nombres (Moore traite également le cas d'un corps de fonctions d'une variable sur un corps fini). Soit S un ensemble de places de k, et soit A_k^S le produit restreint des corps locaux k_v, $v \notin S$. Lorsque $S = \emptyset$ (resp. lorsque S est l'ensemble des places archimédiennes de k), on retrouve l'anneau A_k des adèles (resp. sa composante finie A_k^f).

Soit d'autre part G un groupe algébrique simple, simplement connexe et déployé sur k. Le groupe G_k s'identifie à un sous-groupe du groupe localement compact $G_{A_k^S}$. On s'intéresse aux extensions centrales localement compactes :

$$1 \to M \to E \to G_{A_k^S} \to 1 \tag{5}$$

qui sont triviales au-dessus de G_k (autrement dit telles que E contienne un sous-groupe s'appliquant isomorphiquement sur G_k - ce sous-groupe est d'ailleurs unique puisque G_k coïncide avec son groupe des commutateurs). D'où une notion

de revêtement universel relatif de $G_{A_k^S}$ mod. G_k, ainsi qu'un groupe fondamental relatif ; nous noterons ce dernier $\pi_1^S(G,k)$. C. Moore en démontre l'existence ([10], chap.III) ; de plus :

THÉORÈME 4.- a) Si l'une des places $v \in S$ n'est pas complexe, on a $\pi_1^S(G,k) = \{1\}$.

b) Si toutes les places $v \in S$ sont complexes, $\pi_1^S(G,k)$ est isomorphe à un quotient de μ_k. Si de plus G est isomorphe à SL_n, $n \geq 2$, ou à Sp_{2n}, $n \geq 1$, le groupe $\pi_1^S(G,k)$ est isomorphe à μ_k.

(Rappelons que μ_k désigne le groupe des racines de l'unité contenues dans k.)

Pour la démonstration, voir [10], chap. III.

Remarque. Il est probable que, dans le cas b), le groupe $\pi_1^S(G,k)$ est toujours isomorphe à μ_k. Cette conjecture globale est d'ailleurs une conséquence de la conjecture locale analogue (cf. n° 2.1).

2.3. Relations entre les points de vue « groupes de congruence » et « revêtements universels » (cf. [10], chap. IV, ainsi que [3], § 15).

Conservons les notations du n° précédent, et prenons pour S l'ensemble des places archimédiennes de k, de sorte que $A_k^S = A_k^f$. Comme G est déployé, le groupe $G_{A_k^f}$ est égal à l'adhérence $\bar{G}_k$ du groupe G_k, cf. n°1.

Soit

$$(6) \qquad 1 \to \pi_1 \to E \to \bar{G}_k \to 1$$

le revêtement universel correspondant. Comparons-le à celui défini au n°1.1 :

$$(1) \qquad 1 \to C(G) \to \hat{G}_k \to \bar{G}_k \to 1 .$$

Supposons, pour simplifier, que le rang de G soit ≥ 2. D'après Matsumoto [8], cela entraîne que $C(G)$ est contenu dans le centre de $\hat{G}_k$. Comme en outre $\hat{G}_k$ contient G_k, le caractère universel de E permet de définir un homomorphisme $f : E \to \hat{G}_k$. D'autre part, l'injection $G_k \to E$ est continue pour la topologie T du n° 1.1 (cela provient de ce que E est une extension finie de $\bar{G}_k$) ; elle se prolonge donc en un homomorphisme $g : \hat{G}_k \to E$, et l'on vérifie tout de suite que $f \circ g = 1$ et $g \circ f = 1$. D'où :

THÉORÈME 5.- *Lorsque le rang de G est ≥ 2, les extensions E et $\hat{G}_k$ de $\bar{G}_k$ sont canoniquement isomorphes ; en particulier, $C(G)$ et π_1 sont isomorphes.*

(Lorsque G est de rang 1, on peut simplement affirmer que E est la plus grande extension centrale de $\bar{G}_k$ qui soit quotient de $\hat{G}_k$. Si l'on note $(\hat{G}_k, C(G))$ l'adhérence du sous-groupe de $C(G)$ engendré par les commutateurs $s^{-1}t^{-1}st$, avec $s \in \hat{G}_k$, $t \in C(G)$, cela entraîne que $C(G)/(\hat{G}_k, C(G)) \simeq \pi_1$.)

Ainsi, les points de vue « groupes de congruence » et « revêtements universels » sont équivalents dans le cas considéré ici ; d'où l'analogie entre les théorèmes 2 et 4.

§ 3. La méthode de Mennicke et Bass-Milnor pour SL_n.

3.1. Matrices élémentaires et sous-groupes associés.

Soit A un anneau de Dedekind et soit n un entier ≥ 3. Nous noterons $\Gamma(n)$ (ou simplement Γ) le groupe $SL_n(A)$. Un élément $g \in \Gamma(n)$ est appelé une matrice *élémentaire* si g est de la forme $1 + aE_{ij}$, avec $a \in A$, $1 \leq i,j \leq n$, $i \neq j$. Ces matrices engendrent un sous-groupe $E(n)$ de $\Gamma(n)$.

Soit $\mathfrak{q}$ un idéal non nul de A. Le noyau de $SL_n(A) \to SL_n(A/\mathfrak{q})$ est le groupe de congruence $\Gamma_{\mathfrak{q}}(n)$ défini par $\mathfrak{q}$. On note $E_{\mathfrak{q}}(n)$ le sous-groupe distingué de $E(n)$ engendré par les matrices élémentaires de la forme $1 + aE_{ij}$, avec $a \in \mathfrak{q}$ (ce sont celles qui appartiennent à $\Gamma_{\mathfrak{q}}(n)$). On montre, au moyen d'un théorème de stabilité de Bass [1], que $E_{\mathfrak{q}}(n)$ est distingué dans $\Gamma(n)$, et que

$$E_{\mathfrak{q}}(n) = (E(n), E_{\mathfrak{q}}(n)).$$

On pose $C_{\mathfrak{q}}(n) = \Gamma_{\mathfrak{q}}(n)/E_{\mathfrak{q}}(n)$. On a la suite exacte :

$$(7) \qquad 1 \to C_{\mathfrak{q}}(n) \to \Gamma(n)/E_{\mathfrak{q}}(n) \to \Gamma(n)/\Gamma_{\mathfrak{q}}(n) \to 1 .$$

Lorsque $\mathfrak{q}$ varie, les suites exactes (7) forment un système projectif, à flèches surjectives.

Revenons maintenant au cas du § 1, autrement dit supposons que A soit l'anneau O_k des entiers d'un corps de nombres algébriques k. On a alors :

THEOREME 6.- a) *Le groupe $C_{\mathfrak{q}}(n)$ est isomorphe à un sous-groupe de μ_k.*

b) *Si k a un conjugué réel, ou si $\mathfrak{q} = A$, on a $C_{\mathfrak{q}}(n) = 1$.*

c) *Soit m l'ordre du groupe cyclique μ_k. Si k est totalement imaginaire et si $\mathfrak{q}$ est divisible par m^2, on a $C_{\mathfrak{q}} \simeq \mu_k$.*

COROLLAIRE.- *Le groupe $SL_n(A)$ est engendré par des matrices élémentaires.*

C'est là le principal résultat de [3]. Nous donnerons quelques indications sur sa démonstration dans les numéros suivants.

Indiquons tout de suite comment le théorème 1, pour le groupe SL_n, se déduit du théorème 6 :

On remarque d'abord que, si Γ' est un sous-groupe distingué de $\Gamma(n)$ d'indice fini d, on a $E_q(n) \subset \Gamma'$ si $d|q$. On en conclut que les sous-groupes $E_q(n)$ sont cofinaux parmi les sous-groupes d'indice fini de $\Gamma(n)$. Avec les notations du n° 1.1, on a donc $\hat{\Gamma} = \varprojlim \Gamma(n)/E_q(n)$ et évidemment $\bar{\Gamma} = \varprojlim \Gamma(n)/\Gamma_q(n)$. La limite projective des suites exactes (7) donne donc :

$$(8) \qquad 1 \to \varprojlim C_q(n) \to \hat{\Gamma} \to \bar{\Gamma} \to 1 .$$

En comparant à la suite exacte (2) du n° 1.1, on voit que $\varprojlim C_q(n)$ s'identifie au groupe que l'on avait noté $C(G)$. D'autre part, d'après le théorème 6, on a $\varprojlim C_q(n) = \{1\}$ si k a un conjugué réel, et $\varprojlim C_q(n) \simeq \mu_k$ si k est totalement imaginaire ; c'est bien ce qu'affirmait le théorème 1.

Remarque. Supposons k totalement imaginaire, et soit q un idéal non nul de O_k. On trouvera dans [3], cor.4.3, la détermination explicite du sous-groupe de μ_k auquel $C_q(n)$ est isomorphe ; ce sous-groupe ne dépend pas de n (pourvu, bien sûr, que $n \geq 3$). En particulier, on a $C_q(n) = \mu_k$ si et seulement si q est divisible par $m \prod_{p|m} p^{1/(p-1)}$.

3.2. Symboles de Mennicke.

Conservons les notations du n° précédent ; soit q un idéal non nul de l'anneau de Dedekind A. Soit W_q l'ensemble des couples (a,b), $a,b \in A$, avec $a \equiv 1 \bmod. q$, $b \equiv 0 \bmod. q$, et $aA + bA = A$. Si $(a,b) \in W_q$, on voit facilement qu'il existe un élément $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(A)$, dont la première ligne est (a,b), et qui vérifie $\alpha \equiv 1 \bmod. q$. Soit $\alpha' = \begin{pmatrix} \alpha & 0 \\ 0 & 1_{n-2} \end{pmatrix}$, et soit $\begin{bmatrix} b \\ a \end{bmatrix}$ l'image de α' dans $C_q(n)$.

On voit facilement que $\left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ ne dépend pas du choix de (c,d). On a donc défini une application $W_q \to C_q(n)$; elle jouit des propriétés suivantes :

THÉORÈME 7.- i) $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = 1$; $\left[\begin{smallmatrix} b+ta \\ a \end{smallmatrix}\right] = \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ pour tout $t \in q$; $\left[\begin{smallmatrix} b \\ a+tb \end{smallmatrix}\right] = \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ pour tout $t \in A$.

ii) Si $(a,b_1) \in W_q$ et $(a,b_2) \in W_q$, on a $\left[\begin{smallmatrix} b_1 b_2 \\ a \end{smallmatrix}\right] = \left[\begin{smallmatrix} b_1 \\ a \end{smallmatrix}\right]\left[\begin{smallmatrix} b_2 \\ a \end{smallmatrix}\right]$.

iii) Tout élément de $C_q(n)$ est de la forme $\left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$.

L'assertion i) est triviale. L'assertion ii), due à Mennicke, se démontre par un calcul de matrices dans $SL_3(A)$; il faut vérifier que les matrices

$$\begin{pmatrix} a & b_1 & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a & b_2 & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} a & b_1 b_2 & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

sont congrues mod. $E_q(3)$, ce qui se fait par un calcul explicite ([3], lemme 5.5). Enfin, iii) résulte d'un théorème de stabilité de Bass [1].

DÉFINITION.- Soient q un idéal non nul de A et C un groupe. On appelle symbole de Mennicke relativement à q et C toute application $(a,b) \longmapsto \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ de W_q dans C qui vérifie les propriétés i) et ii) du théorème 7.

On montre (cf. [3], § 2) qu'un symbole de Mennicke vérifie les propriétés suivantes :

iv) Si $(a_1,b) \in W_q$ et $(a_2,b) \in W_q$, on a $\left[\begin{smallmatrix} b \\ a_1 a_2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} b \\ a_1 \end{smallmatrix}\right]\left[\begin{smallmatrix} b \\ a_2 \end{smallmatrix}\right]$.

v) Soient $a,d \in A$, $t \in q$, avec $aA + dA = A$ et $a \equiv d \equiv 1$ mod. t. Alors $\left[\begin{smallmatrix} at \\ d \end{smallmatrix}\right] = \left[\begin{smallmatrix} dt \\ a \end{smallmatrix}\right]$.

Pour tout idéal $q \neq 0$, il existe un symbole de Mennicke universel $W_q \to C_q$, défini à isomorphisme unique près ; il suffit de prendre pour C_q le quotient du

groupe libre engendré par W_q par les relations fournies par i) et ii). En fait, il est inutile d'aller chercher si loin :

THÉORÈME 8.- Pour tout $n \geq 3$, le symbole de Mennicke $W_q \to C_q(n)$ construit plus haut est universel.

COROLLAIRE.- L'application $C_q(n) \to C_q(n+1)$ définie par la suspension $\alpha \longmapsto \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ est un isomorphisme.

C'est le théorème 4.1 de [3] ; sa démonstration occupe une bonne vingtaine de pages. Il s'agit de prouver que tout symbole de Mennicke $W_q \to C$ se factorise en $W_q \to C_q(n) \to C$, autrement dit définit un homomorphisme de $\Gamma_q(n)$ dans C qui est trivial sur $E_q(n)$. Cela se fait en plusieurs étapes :

1) Soit $\Gamma_q(2)$ le sous-groupe de congruence de $SL_2(A)$ correspondant à q. Le symbole de Mennicke $\left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ donné définit une application $\varphi_2 : \Gamma_q(2) \to C$ par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$. Le premier point consiste à vérifier que φ_2 est un homomorphisme, et que $\varphi_2(sts^{-1}) = \varphi_2(t)$ si $t \in \Gamma_q(2)$ et si s est une matrice élémentaire de $SL_2(A)$. Voir pour cela Kubota [6] ainsi que [3], th. 6.1.

2) La partie la plus délicate de la démonstration (due à Bass) consiste à prolonger φ_2 en un homomorphisme $\varphi_3 : \Gamma_q(3) \to C$. Pour cela, on écrit tout élément $\sigma \in \Gamma_q(3)$ sous la forme

$$\sigma = \begin{pmatrix} & & * \\ & (\alpha) & * \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ t & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & * & * \\ 0 & & \\ 0 & & (\beta) \end{pmatrix} \quad \text{avec } t \in q,\ \alpha,\ \beta \in \Gamma_q(2).$$

On pose $\varphi_3(\sigma) = \varphi_2(\alpha)\varphi_2(\beta)$, le membre de droite étant indépendant de la décomposition de σ choisie ([3], lemme 8.11). Il reste alors à montrer que φ_3 est un homomorphisme, et que φ_3 est trivial sur $E_q(3)$; ce n'est pas facile ([3], §§ 9, 10).

3) Le passage de φ_3 à $\varphi_4, \ldots, \varphi_n$ se fait comme celui de φ_2 à φ_3, la seule difficulté supplémentaire étant une difficulté d'écriture.

Remarque. La méthode décrite ci-dessus fournit en même temps une démonstration d'un « théorème de stabilité » pour $K^1(A)$, A étant un anneau commutatif quelconque ; cf. [3], th. 11.2 et cor. 11.3.

3.3. Détermination des symboles de Mennicke dans le cas arithmétique.

Revenons maintenant au cas où $A = O_k$, et soit m l'ordre de μ_k. Soit $\mathfrak{p}$ un idéal premier de O_k, premier à m, et soit x un élément de k qui est une unité en $\mathfrak{p}$; on sait qu'il existe alors un unique élément $\varepsilon \in \mu_k$, noté $(\frac{x}{\mathfrak{p}})$, tel que

$$x^{(N\mathfrak{p}-1)/m} \equiv \varepsilon \mod \mathfrak{p}, \quad N\mathfrak{p} \text{ étant la norme de } \mathfrak{p}.$$

Le caractère $x \longmapsto (\frac{x}{\mathfrak{p}})$ est la généralisation naturelle du symbole de Legendre.

Soient maintenant a et b deux éléments de A; supposons a étranger à la fois à b et à m. On pose :

$$(\frac{b}{a}) = \prod_{\mathfrak{p}|a} (\frac{b}{\mathfrak{p}})^{v_{\mathfrak{p}}(a)},$$

où $v_{\mathfrak{p}}$ désigne la valuation discrète associée à $\mathfrak{p}$.

THÉORÈME 9.- Supposons que k soit totalement imaginaire, et que q soit divisible par

$$m \prod_{\mathfrak{p}|m} p^{1/(p-1)}.$$

L'application $W_q \to \mu_k$ définie par $(a,b) \longmapsto (\frac{b}{a})$ est alors un symbole de Mennicke. (Lorsque $b = 0$, on convient que $(\frac{b}{a}) = 1$.)

On utilise la décomposition de $(\frac{b}{a})$ en produit de symboles de Hilbert :

$$(\frac{b}{a}) = \overline{\prod_{p \nmid a} (\frac{a,b}{p})} \ .$$

La démonstration n'est pas difficile (cf. [3], prop. 3.1).

THÉORÈME 10.- a) Si k a un conjugué réel, ou si $q = A$, tout symbole de Mennicke relativement à q est trivial.

b) Si k est totalement imaginaire, et si q est divisible par $m \prod_{p|m} p^{1/(p-1)}$, le symbole de Mennicke $(a,b) \longmapsto (\frac{b}{a})$ est universel.

(Il est clair que ce théorème, combiné avec le théorème 8, entraîne les parties b) et c) du théorème 6, et en particulier résout le problème des groupes de congruence pour SL_n. La partie a) du théorème 6 se démontre de manière analogue.)

Indiquons, à titre d'exemple, la démonstration de b). Soit $(a,b) \longmapsto \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ le symbole de Mennicke universel $W_q \to C_q$. Vu le théorème 9, on a un homomorphisme surjectif $C_q \to \mu_k$, et il suffit de prouver que Card $(C_q) \leqq m$.

On montre tout d'abord (Mennicke-Newman, cf. [3], lemme 2.4) qu'étant donnés des éléments $(a_i,b_i) \in W_q$, en nombre fini, on peut trouver d'autres éléments $(a,c_i) \in W_q$, ayant même première coordonnée a, tels que $\left[\begin{smallmatrix} b_i \\ a_i \end{smallmatrix}\right] = \left[\begin{smallmatrix} c_i \\ a \end{smallmatrix}\right]$ pour tout i ; de plus on peut s'arranger pour que a soit premier (i.e. que l'idéal aA soit premier). Mais, d'après la propriété ii) des symboles de Mennicke, l'application $b \longmapsto \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$ définit un homomorphisme $U(A/aA) \to C$, où $U(A/aA)$ désigne le groupe des unités de l'anneau A/aA. Comme A/aA est un corps fini, on en conclut que $U(A/aA)$ est un groupe cyclique fini ; d'où : tout sous-ensemble fini de C est contenu dans un sous-groupe cyclique fini de C.

Soit maintenant p un nombre premier, et soit p^n la plus grande puissance de p divisant m. Vu ce qui précède, il suffit de prouver qu'aucun élément $\begin{bmatrix} b \\ a \end{bmatrix}$ de C n'est d'ordre p^{n+1}. Soit P l'ensemble des idéaux premiers $\mathfrak{p}$, premiers à p, tels que $N\mathfrak{p} \not\equiv 1 \bmod. p^{n+1}$. En utilisant le fait que k ne contient pas les racines p^{n+1}-èmes de l'unité, on montre que P est infini. De plus, le théorème de la progression arithmétique montre (cf. [3], th. 3.2) qu'il existe $(c,d) \in W_q$, avec $\begin{bmatrix} d \\ c \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$, et $cA = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2 \in P$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$. L'élément $\begin{bmatrix} b \\ a \end{bmatrix}$ appartient alors à l'image de $U(A/cA) = U(A/\mathfrak{p}_1) \times U(A/\mathfrak{p}_2)$ dans C. Puisque $\mathfrak{p}_1$ et $\mathfrak{p}_2$ appartiennent à P, il est donc bien impossible que $\begin{bmatrix} b \\ a \end{bmatrix}$ soit d'ordre p^{n+1}, cqfd.

BIBLIOGRAPHIE

[1] H. BASS - K-theory and stable algebra, Publ. Math. I.H.E.S., n°22 (1964), p. 5-60.

[2] H. BASS, M. LAZARD et J.-P. SERRE - Sous-groupes d'indice fini dans $SL(n,\mathbb{Z})$, Bull. Amer. Math. Soc., 70 (1964), p. 385-392.

[3] H. BASS, J. MILNOR et J.-P. SERRE - Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, Publ. Math. I.H.E.S. (à paraître prochainement).

[4] A. BOREL et HARISH-CHANDRA - Arithmetic subgroups of algebraic groups, Ann. of Maths., 75 (1962), p. 485-535.

[5] C. CHEVALLEY - Deux théorèmes d'arithmétique, J. Math. Soc. Japan, 3 (1951), p. 36-44.

[6] T. KUBOTA - Ein arithmetischer Satz über eine Matrizengruppe, J. für Math., 222 (1965), p. 55-57.

[7] H. MATSUMOTO - Subgroups of finite index in certain arithmetic groups, Proc. Symp. Pure Math., vol. 9, A.M.S. 1966, p. 99-103.

[8] H. MATSUMOTO - Sur les sous-groupes de congruence des groupes simples déployés simplement connexes (en préparation).

[9] J. MENNICKE - Finite factor groups of the unimodular group, Ann. of Maths., 81 (1965), p. 31-37.

[10] C. MOORE - Group extensions of p-adic and adelic linear groups, à paraître prochainement.

[11] J.-P. SERRE - Sur les groupes de congruence des variétés abéliennes, Izv. Akad. Nauk, 28 (1964), p. 3-20.

[12] R. STEINBERG - Générateurs, relations, et revêtements de groupes algébriques, Colloque de Bruxelles (1962), p. 113-127.

[13] A. WEIL - Sur certains groupes d'opérateurs unitaires, Acta Math., 111 (1964), p. 143-211.

ERRATUM

Page 330-06. Dans l'exemple (c), il faut supposer que la caractéristique du corps de base k_v est $\neq 2$.