Le problème des groupes de congruence pour $\mathbf{SL}_2$

par JEAN-PIERRE SERRE

Introduction

Soit K un *corps global*, autrement dit un corps de nombres algébriques ou un corps de fonctions d'une variable sur un corps fini. Soit Σ l'ensemble des places de K, soit Σ^∞ le sous-ensemble de Σ formé des places archimédiennes, et soit S une partie finie non vide de Σ contenant Σ^∞. Soit A_S l'anneau des S-entiers de K, i.e. l'ensemble des éléments de K dont la valuation est $\geqq 0$ en toute place de $\Sigma - S$.

Le "problème des groupes de congruence pour $\mathbf{SL}_2$" consiste à déterminer si tout sous-groupe d'indice fini du groupe $\mathbf{SL}_2(A_S)$ est un groupe de S-congruence (cf. n° **1.2**) et, dans le cas contraire, à voir si le groupe $C(G)$ qui mesure la déviation entre ces deux types de sous-groupes est ou non un groupe fini[1]. Comme on le verra, il y a lieu de distinguer deux cas:

(i) Le cas où Card $(S) \geqq 2$, i.e. où le groupe A_S^* des éléments inversibles de A_S est *infini*. On peut alors montrer (c'est l'objet du § 2) que la situation est la même que pour le *cas stable* de $\mathbf{SL}_n$, $n \geqq 3$, traité dans [4]. Autrement dit, le problème des groupes de congruence admet une *réponse affirmative* si l'une au moins des places de S est archimédienne réelle, ou ultramétrique; si toutes les places de S sont archimédiennes complexes, le groupe déviation $C(G)$ est isomorphe au groupe des racines de l'unité contenues dans K, et c'est un groupe cyclique *fini* (le problème a donc une réponse *presque affirmative*).

(ii) Le cas où Card $(S) = 1$, i.e. où A_S^* est fini. Lorsque K est un corps de nombres, cela signifie que $S = \Sigma^\infty$, et que K est isomorphe à $\mathbf{Q}$ ou à un corps quadratique imaginaire. Le groupe $C(G)$ est alors infini (autrement dit le problème posé a une réponse *essentiellement négative*); c'est là un résultat bien connu lorsque $K = \mathbf{Q}$ (cf. Klein [13], § 1, p. 63) et nous le démontrerons au § 3 lorsque K est imaginaire quadratique, ou de caractéristique p.

Les démonstrations du § 2, relatives au cas Card $(S) \geqq 2$, sont purement

[1] Bien entendu, un problème analogue se pose pour tout groupe algébrique simple simplement connexe G. Vu les résultats récents de Kneser [14], on peut espérer que la réponse ne dépend que de la somme s des rangs relatifs de G aux diverses places de S. De façon plus précise, est-il vrai que $C(G)$ est fini si $s \geqq 2$, et infini si $s = 1$?

algébriques; elles combinent les idées de Mennicke (qui a traité le cas, proposé par Ihara, où $K = \mathbf{Q}$ et $S = \{p, \infty\}$) avec la théorie des *revêtements universels relatifs* de C. Moore [16]. Par contre, les démonstrations du § 3 sont de nature topologique; elles utilisent "l'espace symétrique" correspondant au groupe $\mathbf{SL}_2(\hat{K})$, où $\hat{K}$ est le complété de K pour l'unique place appartenant à S.

Des conversations avec H. Bass et A. Borel m'ont été très utiles; je les en remercie vivement.

§ 1. Préliminaires

1.1. *Notations.*

On note A_S, ou simplement A, l'ensemble des $x \in K$ tels que $v(x) \geqq 0$ pour tout $v \in \Sigma - S$. C'est un anneau de Dedekind; ses idéaux maximaux correspondent bijectivement aux éléments de $\Sigma - S$.

Le groupe A^* des éléments inversibles de A est noté U. Son sous-groupe de torsion est le groupe μ des racines de l'unité contenues dans K; il est cyclique fini. Si $s = \mathrm{Card}\,(S)$, on a $U \simeq \mu \times \mathbf{Z}^{s-1}$ ("théorème des unités"); en particulier, U est fini si et seulement si $s = 1$.

On pose $G = \mathbf{SL}_2(K)$, $\Gamma_A = \mathbf{SL}_2(A)$ et

$$E_{12}(x) = \begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} \quad \text{si } x \in K\,, \qquad h(x) = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \quad \text{si } x \in K^*\,.$$

1.2. *Sous-groupes de S-congruence et sous-groupes S-arithmétiques.*

Soit $\mathfrak{q}$ un idéal $\neq 0$ de A. Le quotient $A/\mathfrak{q}$ est fini. L'homomorphisme $\mathbf{SL}_2(A) \to \mathbf{SL}_2\,(A/\mathfrak{q})$ induit par $A \to A/\mathfrak{q}$ est *surjectif* ([2], cor. 5.2); son noyau $\Gamma_{\mathfrak{q}}$ s'appelle le *groupe de S-congruence défini par* $\mathfrak{q}$; c'est un sous-groupe d'indice fini de Γ_A.

Un sous-groupe H de G est dit *S-arithmétique* s'il est commensurable à Γ_A, i.e. si $\Gamma_A \cap H$ est d'indice fini dans Γ_A et dans H; si en outre H contient l'un des $\Gamma_{\mathfrak{q}}$ (pour un idéal $\mathfrak{q} \neq 0$ convenable), on dit que H est un *groupe de S-congruence*. Si S est réduit à Σ^∞, on dit "congruence" et "arithmétique" au lieu de "S-congruence" et "S-arithmétique".

Lorsque K est un corps de nombres, ou lorsque $\mathrm{Card}\,(S) \geqq 2$, tout sous-groupe S-arithmétique de G est *de type fini*[2]; en effet, il suffit de le vérifier pour Γ_A lui-même, ce qui a été fait par O'Meara ([17], th. 24.8). Lorsque K

[2] On peut se demander si un tel groupe est *de présentation finie*, i.e. est définissable par un nombre fini de relations. C'est vrai lorsque K est un corps de nombres, d'après Behr [5]. J'ignore ce qu'il en est lorsque K est un corps de fonctions, même pour un groupe aussi simple que $\mathbf{SL}_2(\mathbf{F}_p[T, T^{-1}])$.

est un corps de fonctions, et que Card $(S) = 1$, on peut par contre montrer (cf. n° 3.2) que les sous-groupes S-arithmétiques *ne sont pas de type fini.*

1.3. *Les groupes* $\hat{G}$, $\bar{G}$ *et* $C(G)$.

Notons $\mathcal{T}$ (resp. $\mathcal{T}_c$) l'unique topologie sur G qui soit compatible avec la structure de groupe de G et admette comme base de voisinages de 1 l'ensemble des sous-groupes S-arithmétiques (resp. de S-congruence) de G (cf. [4], [16], [20]). Le groupe Γ_A est ouvert dans G pour $\mathcal{T}$ (resp. $\mathcal{T}_c$); de plus, les structures uniformes droite et gauche définies par $\mathcal{T}$ (resp. $\mathcal{T}_c$) sur Γ_A coïncident. On en conclut aussitôt (cf. Bourbaki, *Top. Gén.*, III, § 3, n° 4, th. 1) que G admet un complété $\hat{G}$ (resp. $\bar{G}$) pour $\mathcal{T}$ (resp. $\mathcal{T}_c$). Soit π la projection canonique $\hat{G} \to \bar{G}$ et soit $C(G)$ son noyau. On a des suites exactes

$$\{1\} \to C(G) \to \hat{G} \to \bar{G} \to \{1\}$$
$$\{1\} \to C(G) \to \hat{\Gamma}_A \to \bar{\Gamma}_A \to \{1\} ,$$

où $\hat{\Gamma}_A$ (resp. $\bar{\Gamma}_A$) désigne le complété de Γ_A pour $\mathcal{T}$ (resp. $\mathcal{T}_c$). On a

$$\bar{\Gamma}_A = \varprojlim \Gamma_A/\Gamma_{\mathfrak{q}} \quad \text{et} \quad \hat{\Gamma}_A = \varprojlim \Gamma_A/N ,$$

où $\mathfrak{q}$ parcourt l'ensemble des idéaux $\neq 0$ de A et N l'ensemble des sous-groupes d'indice fini de Γ_A. En particulier, $\hat{\Gamma}_A$, $\bar{\Gamma}_A$ et $C(G)$ sont des groupes *profinis*, et l'on voit que $C(G)$ mesure la "déviation" existant entre sous-groupes S-arithmétiques et sous-groupes de S-congruence.

1.4. *Les sous-groupes* $E_{\mathfrak{q}}$.

Soit $\mathfrak{q}$ un idéal $\neq 0$ de A; on note $E_{12}(\mathfrak{q})$ le sous-groupe de Γ_A formé des $E_{12}(x)$, pour $x \in \mathfrak{q}$; on note $E_{\mathfrak{q}}$ le plus petit sous-groupe distingué de Γ_A contenant $E_{12}(\mathfrak{q})$. Il est clair que l'on a $E_{\mathfrak{q}} \subset \Gamma_{\mathfrak{q}}$; l'un des buts du § 2 est de voir dans quel cas cette inclusion est une égalité.

Proposition 1. *Supposons que* K *soit un corps de nombres, ou que* Card $(S) \geqq 2$. *Soit* N *un sous-groupe d'indice fini de* Γ_A. *Il existe alors un idéal* $\mathfrak{q} \neq 0$ *de* A *tel que* $E_{\mathfrak{q}} \subset N$.

Quitte à remplacer N par l'intersection de ses conjugués, on peut supposer que N est *distingué dans* Γ_A; il suffit alors de prouver l'existence d'un idéal $\mathfrak{q} \neq 0$ tel que $E_{12}(\mathfrak{q}) \subset N$. Distinguons deux cas:

(a) K est un corps de nombres. Si $n = (\Gamma_A : N)$, on peut prendre $\mathfrak{q} = nA$.

(b) K est un corps de fonctions sur un corps fini de caractéristique p et Card $(S) \geqq 2$. L'ensemble U' des $u \in U$ tels que $h(u) \in N$ est un sous-groupe d'indice fini de U. L'hypothèse faite sur Card (S) entraîne que U' contient un élément u *d'ordre infini*. D'autre part, soit $\mathfrak{n}$ l'ensemble des $x \in A$ tels que $E_{12}(x) \in N$. Le quotient $A/\mathfrak{n}$ est fini. De plus, $\mathfrak{n}$ est *stable* par $x \mapsto u^2x$:

cela résulte de la formule

$$h(u)E_{12}(x)h(u)^{-1} = E_{12}(u^2x) \,.$$

Si $B = \mathbf{F}_p[u^2]$ est le sous-anneau de A engendré par u^2, il s'ensuit que $\mathfrak{n}$ est un sous-B-module de A, et $A/\mathfrak{n}$ est un B-module. Mais $A/\mathfrak{n}$ est fini et B est infini (sinon l'ordre de u serait fini); il existe donc un élément $t \neq 0$ de B tel que $t.(A/\mathfrak{n}) = 0$, i.e. tel que $tA \subset \mathfrak{n}$. L'idéal $\mathfrak{q} = tA$ répond alors à la question.

COROLLAIRE. *Tout sous-groupe S-arithmétique de G contient l'un des* $E_{\mathfrak{q}}$.

C'est clair.

Remarque. Dans le cas "exceptionnel" où K est un corps de fonctions et Card $(S) = 1$, on peut montrer (en utilisant les résultats du n° 3.2) qu'il existe des sous-groupes d'indice fini de Γ_A qui ne contiennent aucun $E_{\mathfrak{q}}$.

§ 2. Le cas Card $(S) \geqq 2$

Dans ce paragraphe, on suppose que S *a au moins deux éléments*, autrement dit que U est *infini*.

2.1. *Sous-groupes à normalisateur arithmétique.*

PROPOSITION 2. *Soit X un sous-groupe de G, non contenu dans $\{\pm 1\}$, et normalisé par un sous-groupe S-arithmétique N de G. Alors X contient un groupe $E_{\mathfrak{q}}$.*

D'après le cor. à la prop. 1, il existe un idéal $\mathfrak{q}' \neq 0$ de A tel que $E_{\mathfrak{q}'} \subset N$; de plus, l'ensemble U' des éléments $u \in U$ tels que $h(u) \in N$ est un sous-groupe d'indice fini de U.

D'autre part, X contient un élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tel que $ac \neq 0$. En effet, sinon, l'adhérence de X pour la topologie de Zariski serait un sous-groupe algébrique H de $\mathbf{SL}_2$ distinct de $\mathbf{SL}_2$. Le groupe H serait normalisé par N, donc aussi par l'adhérence de N pour la topologie de Zariski, adhérence qui est égale à $\mathbf{SL}_2$ comme on le voit aussitôt (elle contient les deux sous-groupes unipotents $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ qui engendrent $\mathbf{SL}_2$); le groupe H serait donc distingué dans $\mathbf{SL}_2$, donc contenu dans $\{\pm 1\}$, ce qui est absurde.

Choisissons alors un élément $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de X, avec $ac \neq 0$. Quitte à remplacer l'idéal $\mathfrak{q}'$ par un idéal plus petit, on peut supposer que $a^{-1}c\mathfrak{q}'$ est contenu dans A. Soit u un élément de U' d'ordre infini. Puisque $A/a^{-1}c\mathfrak{q}'$ est fini, il existe un entier $n \geqq 1$ tel que $u^{2n} \equiv 1 \pmod{a^{-1}c\mathfrak{q}'}$. Ecrivons $a(u^{2n}-1)$ sous la forme ct, avec $t \in \mathfrak{q}'$, et posons

$$x' = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} x \begin{pmatrix} 1 & -t \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} .$$

On a

$$x' \in X \quad \text{et} \quad c' = c\ , \quad a' = a + ct = u^{2n}a\ .$$

Comme $h(u^n) \in N$, on a $x'' \in X$ si l'on pose:

$$x'' = h(u^n)xh(u^{-n}) = \begin{pmatrix} a & u^{2n}b \\ u^{-2n}c & d \end{pmatrix}$$

Soit $y = x'^{-1}x''$. On a $y \in X$, et

$$y = \begin{pmatrix} u^{-2n} & e \\ 0 & u^{2n} \end{pmatrix}, \qquad \text{avec } e \in K\ .$$

Si $z \in \mathfrak{q}'$, on a $y^{-1}E_{12}(z)yE_{12}(-z) \in X$. Or un tel élément s'écrit $E_{12}(r)$, avec $r = (u^{4n} - 1)z$. Il s'ensuit que X contient le sous-groupe $E_{12}(\mathfrak{q})$, avec $\mathfrak{q} = (u^{4n} - 1)\mathfrak{q}'$.

Ce qui précède s'applique aussi aux *conjugués* $\gamma X \gamma^{-1}$ de X par les éléments de Γ_A, conjugués qui sont en nombre fini puisque $(\Gamma_A \colon N \cap \Gamma_A)$ est fini. On peut donc choisir l'idéal $\mathfrak{q}$ de telle sorte que l'on ait

$$E_{12}(\mathfrak{q}) \subset \gamma X \gamma^{-1} \qquad \text{pour tout } \gamma \in \Gamma_A\ .$$

Le groupe X contient alors tous les $\gamma^{-1}E_{12}(\mathfrak{q})\gamma$, donc il contient $E_{\mathfrak{q}}$, cqfd.

2.2. *Une propriété de commutation.*

Posons $m = \text{Card}\,(\mu)$; c'est le nombre des racines de l'unité contenues dans K.

Soit $\mathfrak{q}$ un idéal $\neq 0$ de A. On pose $C_{\mathfrak{q}} = \Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$; le groupe $C_{\mathfrak{q}}$ s'identifie à un sous-groupe de $\Gamma_A/E_{\mathfrak{q}}$.

PROPOSITION 3. *Soit u un élément de U. L'image de $h(u)^m$ dans $\Gamma/E_{\mathfrak{q}}$ commute aux éléments de $C_{\mathfrak{q}}$.*

La démonstration suit de près celle donnée par Mennicke [15] pour $K = \mathbf{Q}$ et $S = \{\infty, p\}$. Elle utilise les trois lemmes suivants:

LEMME 1. *Soient $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $x' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ deux éléments de $\Gamma_{\mathfrak{q}}$.*
(i) *Si $a = a'$ et $b \equiv b'$ (mod $a\mathfrak{q}$), on a $x \equiv x'$ mod. $E_{\mathfrak{q}}$.*
(ii) *Si $b = b'$ et $a \equiv a'$ (mod $b\mathfrak{q}$), on a $x \equiv x'$ mod. $E_{\mathfrak{q}}$.*

Dans le cas (i), il existe $t \in \mathfrak{q}$ tel que $b = b' + ta$. En multipliant x' à droite par $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ on obtient $x'' = \begin{pmatrix} a & b \\ c'' & d'' \end{pmatrix}$, et $x'' \equiv x'$ mod. $E_{\mathfrak{q}}$. Le produit $x''x^{-1}$ est de la forme $\begin{pmatrix} 1 & 0 \\ e & f \end{pmatrix}$, et, comme il appartient à $\Gamma_{\mathfrak{q}}$, on a $f = 1$, $e \in \mathfrak{q}$. Si $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, on a $w\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}w^{-1} = \begin{pmatrix} 1 & -e \\ 0 & 1 \end{pmatrix}$, d'où $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix} \in E_{\mathfrak{q}}$ et $x'' \equiv x$ mod. $E_{\mathfrak{q}}$, ce qui démontre notre assertion dans le cas (i).

Dans le cas (ii), on a $a = a' + tb$, avec $t \in \mathfrak{q}$. En multipliant x' à droite par $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$, on est ramené au cas $a' = a$, $b' = b$, traité dans (i).

LEMME 2. *Soient* $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *un élément de* $\Gamma_{\mathfrak{q}}$, *et* n *un entier tels que* $u^{2n} \equiv 1 \pmod{aA}$. *Les éléments* $h(u)^n$ *et* x *commutent modulo* $E_{\mathfrak{q}}$.

On a en effet

$$h(u)^n x h(u)^{-n} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

avec $a' = a$, $b' = u^{2n}b$, et le lemme 1, (i), montre que cette matrice est congrue à x mod. $E_{\mathfrak{q}}$.

Pour tout élément non nul a de A, notons $U(a)$ le groupe multiplicatif des éléments inversibles de l'anneau A/aA; c'est un groupe fini.

LEMME 3. *Soit* l *un nombre premier, et soit* l^e *la plus grande puissance de* l *divisant* $m = \mathrm{Card}(\mu)$. *Soit* $a_0 \in A$ *et soit* $\mathfrak{r}$ *un idéal non nul de* A *tel que* a_0 *soit inversible modulo* $\mathfrak{r}$. *Il existe alors* $a \in A$, *avec* $a \equiv a_0 \pmod{\mathfrak{r}}$, *tel que* $U(a)$ *ne contienne pas d'élément d'ordre multiple de* l^{e+1}.

Pour la démonstration, voir n° 2.3 ci-après.

Démontrons maintenant la proposition 3. Soit $\xi \in C_{\mathfrak{q}}$. Utilisant le lemme 1, on peut choisir un représentant $x_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$ de ξ tel que $a_0 \neq 0$, $b_0 \neq 0$. Comme A/a_0A est fini, le lemme 2 montre qu'il existe un entier $n \geqq 1$ tel que $h(u)^n$ commute à x_0 mod. $E_{\mathfrak{q}}$. Soit N le plus petit entier $\geqq 1$ jouissant de cette propriété. Il nous faut voir que N divise m. Supposons que ce ne soit pas le cas. Il existerait alors un nombre premier l tel que l^{e+1} divise N, les notations étant celles du lemme 3. Ce dernier lemme, appliqué à $\mathfrak{r} = b_0\mathfrak{q}$, montre qu'il existe $a \equiv a_0 \pmod{b_0\mathfrak{q}}$ tel que $U(a)$ ne contienne aucun élément d'ordre divisible par l^{e+1}. Mais on vérifie immédiatement (cf. [4], lemme 5.3) qu'il existe $c, d \in A$ tels que la matrice $x = \begin{pmatrix} a & b_0 \\ c & d \end{pmatrix}$ appartienne à $\Gamma_{\mathfrak{q}}$. D'après le lemme 1, (ii), x est un représentant de ξ mod. $E_{\mathfrak{q}}$. Soit m_1 l'ordre de l'image de u^2 dans $U(a)$. D'après le lemme 2, $h(u)^{m_1}$ commute à x mod. $E_{\mathfrak{q}}$; donc N divise m_1, et *a fortiori* l^{e+1} divise m_1. Ceci contredit l'hypothèse faite sur $U(a)$, d'où la proposition.

2.3. *Démonstration du lemme* 3.

Nous le déduirons du suivant:

LEMME 4. *Soit* $a_0 \in A$ *et soit* $\mathfrak{r}$ *un idéal non nul de* A *tel que* a_0 *soit inversible* $\pmod{\mathfrak{r}}$. *Soit* L/K *une extension abélienne finie de* K, *distincte de* K, *et soit* P *l'ensemble des places* $v \in \Sigma - S$ *qui sont non ramifiées dans* L *et ne se décomposent pas complètement dans* L. *Soit* P' *une partie finie de* P.

Il existe alors $a \in A$ vérifiant les conditions suivantes:

(1) $a \equiv a_0 \pmod{\mathfrak{r}}$.

(2) *L'idéal aA est produit d'idéaux premiers distincts, appartenant tous à $P - P'$.*

(Ici, et dans toute la suite, on identifie une place $v \in \Sigma - S$ à l'idéal premier correspondant de A.)

Soit $H_\mathfrak{r}$ le groupe des classes d'idéaux mod $\mathfrak{r}$ (rappelons que deux idéaux fractionnaires de K relativement à A, premiers à $\mathfrak{r}$, sont dits équivalents mod $\mathfrak{r}$ si leur quotient est de la forme λA, avec λ congru multiplicativement à 1 mod $\mathfrak{r}$). D'après le théorème d'existence de la théorie du corps de classes, il existe une extension abélienne finie $K_\mathfrak{r}$ de K telle que l'application de réciprocité d'Artin donne un isomorphisme de $H_\mathfrak{r}$ sur le groupe de Galois $\mathrm{Gal}(K_\mathfrak{r}/K)$. [Pour tout ce qui concerne la théorie du corps de classes, voir [1], [8] ou [25].] Soit $L_\mathfrak{r}$ l'extension composée $L \cdot K_\mathfrak{r}$. Choisissons dans $\mathrm{Gal}(L_\mathfrak{r}/K)$ un élément α_0 dont l'image dans $H_\mathfrak{r} = \mathrm{Gal}(K_\mathfrak{r}/K)$ soit la classe de a_0. On peut trouver des éléments $\alpha_i \in \mathrm{Gal}(L_\mathfrak{r}/K)$, $i = 1$ ou $i = 1, 2$, ayant les deux propriétés suivantes:

(1′) $\prod \alpha_i = \alpha_0$.

(2′) Pour tout i, l'image de α_i dans $\mathrm{Gal}(L/K)$ est $\neq 1$.

En effet, si l'image de α_0 dans $\mathrm{Gal}(L/K)$ est $\neq 1$, on prend un seul α_i, à savoir α_0 luimême. Si l'image de α_0 est 1, on prend pour α_1 n'importe quel élément de $\mathrm{Gal}(L_\mathfrak{r}/K)$ dont l'image dans $\mathrm{Gal}(L/K)$ est $\neq 1$ (un tel élément existe puisque L est distinct de K), et on prend pour α_2 l'élément $\alpha_0\alpha_1^{-1}$.

Appliquons maintenant le théorème de densité de Čebotarev (cf. [25], p. 289) à l'extension $L_\mathfrak{r}/K$. On en déduit que, pour chaque i, il existe une infinité de places v_i dont l'élément de Frobenius est α_i; on peut donc choisir les v_i de telle sorte qu'elles soient distinctes, et n'appartiennent pas à $S \cup P'$. De plus, comme l'élément de Frobenius de v_i dans $\mathrm{Gal}(L/K)$ est $\neq 1$, on a $v_i \in P$ pour tout i. Enfin, la propriété (1′) entraîne que l'idéal $\prod v_i$ est équivalent (mod $\mathfrak{r}$) à l'idéal principal a_0A; il existe donc $\lambda \equiv 1 \pmod{\mathfrak{r}}$ tel que

$$a_0A = \lambda \prod v_i \, .$$

L'élément $a = \lambda^{-1}a_0$ répond alors à la question.

Fin de la démonstration du lemme 3.

Le cas où l est égal à la caractéristique de K est trivial. Ce cas écarté, soit z une racine primitive l^{e+1}-ème de l'unité (dans une clôture séparable de K), et soit $L = K(z)$. L'extension L/K est abélienne, finie, et non triviale (sinon, on aurait $z \in K$, contrairement à la définition de e). Soit $v \in \Sigma - S$; si la caractéristique résiduelle p_v de v est $\neq l$, on sait que v se décompose complètement dans L si et seulement si le corps résiduel A/v de v contient une racine primitive l^{e+1}-ème de l'unité; si l'on pose $Nv = \mathrm{Card}\,(A/v)$, cela signifie que $Nv \equiv 1 \pmod{l^{e+1}}$. En appliquant le lemme 4, on voit donc qu'il existe $a \in A$ vérifiant $a \equiv a_0 \pmod{\mathfrak{r}}$ tel que l'idéal aA soit un produit de v_i distincts, avec $Nv_i \not\equiv 1 \pmod{l^{e+1}}$. Mais l'anneau A/aA est isomorphe au produit des corps A/v_i; son groupe multiplicatif ne contient donc pas d'élément d'ordre multiple de l^{e+1}, cqfd.

2.4. *Le groupe* C.

Si $\mathfrak{q}$ et $\mathfrak{q}'$ sont deux idéaux $\neq 0$ de A, avec $\mathfrak{q}' \subset \mathfrak{q}$, les inclusions $\Gamma_{\mathfrak{q}'} \to \Gamma_{\mathfrak{q}}$ et $E_{\mathfrak{q}'} \to E_{\mathfrak{q}}$ définissent un homomorphisme de $C_{\mathfrak{q}'} = \Gamma_{\mathfrak{q}'}/E_{\mathfrak{q}'}$ dans $C_{\mathfrak{q}} = \Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$; cet homomorphisme est *surjectif* (cf. [4], lemme 2.3).

Lorsque $\mathfrak{q}$ varie, les $C_{\mathfrak{q}}$ forment un *système projectif*. On pose:

$$C = \varprojlim C_{\mathfrak{q}} .$$

Les homomorphismes $C \to C_{\mathfrak{q}}$ sont *surjectifs*; cela résulte de la surjectivité des homomorphismes de transition $C_{\mathfrak{q}'} \to C_{\mathfrak{q}}$ et du fait que l'ensemble des idéaux de A est dénombrable.

Le groupe Γ_A opère par automorphismes intérieurs sur les $C_{\mathfrak{q}}$; il opère donc aussi sur C. En fait, cette action *se prolonge en une action de* G *tout entier*. Cela va résulter du lemme suivant:

LEMME 5. *Soient* $\mathfrak{q}$ *un idéal non nul de* A, *et* g *un élément de* G. *Il existe un idéal non nul* $\mathfrak{q}'$ *de* A *tel que* $g\Gamma_{\mathfrak{q}}g^{-1}$ *contienne* $\Gamma_{\mathfrak{q}'}$ *et que* $gE_{\mathfrak{q}}g^{-1}$ *contienne* $E_{\mathfrak{q}'}$.

L'existence d'un idéal non nul $\mathfrak{q}_1'$ tel que $g\Gamma_{\mathfrak{q}}g^{-1} \supset \Gamma_{\mathfrak{q}_1'}$ est triviale; si les coefficients de g appartiennent à $x^{-1}A$, où x est un élément non nul de A, on peut prendre $\mathfrak{q}_1' = x^2\mathfrak{q}$, comme on le voit aussitôt. D'autre part, $gE_{\mathfrak{q}}g^{-1}$ est normalisé par $g\Gamma_{\mathfrak{q}}g^{-1}$, donc aussi par $\Gamma_{\mathfrak{q}_1'}$; d'après la prop. 2, cela entraîne l'existence d'un idéal non nul $\mathfrak{q}_2'$ tel que $gE_{\mathfrak{q}}g^{-1} \supset E_{\mathfrak{q}_2'}$. L'idéal $\mathfrak{q}' = \mathfrak{q}_1' \cap \mathfrak{q}_2'$ répond alors à la question.

Nous pouvons maintenant définir *l'action de* G *sur* C. Soit $g \in G$ et soit $\mathfrak{q}$ un idéal non nul. D'après le lemme ci-dessus, appliqué à g^{-1}, il existe un idéal non nul $\mathfrak{q}'$ tel que l'on ait

$$gE_{\mathfrak{q}'}g^{-1} \subset E_{\mathfrak{q}} \quad \text{et} \quad g\Gamma_{\mathfrak{q}'}g^{-1} \subset \Gamma_{\mathfrak{q}} .$$

L'application $x \mapsto gxg^{-1}$ définit donc, par passage au quotient, un homomorphisme $C_{\mathfrak{q}'} \to C_{\mathfrak{q}}$. Par composition avec la projection canonique $C \to C_{\mathfrak{q}'}$, on en déduit un homomorphisme $i_{g,\mathfrak{q}}$ de C dans $C_{\mathfrak{q}}$ qui ne dépend pas du choix de $\mathfrak{q}'$. Si $\mathfrak{q}_1 \subset \mathfrak{q}_2$, le composé de $i_{g,\mathfrak{q}_1}$ avec la projection $C_{\mathfrak{q}_1} \to C_{\mathfrak{q}_2}$ est $i_{g,\mathfrak{q}_2}$; les $i_{g,\mathfrak{q}}$ définissent donc un homomorphisme de C dans $\varprojlim C_{\mathfrak{q}}$, i.e. un endomorphisme i_g de C. On vérifie sans difficulté que i_1 est l'identité et que

$i_{g_1g_2} = i_{g_1} \circ i_{g_2}$. Les i_g définissent donc bien une *loi d'opération du groupe* G *sur le groupe* C, et il est clair que cette loi prolonge celle de Γ_A sur C.

[*Variante*. Le lemme 5 montre qu'il existe sur G une topologie compatible avec la structure de groupe de G et admettant comme base de voisinages de 1 la famille des $E_\mathfrak{q}$. Si $\hat{G}_E$ est le complété de G pour cette topologie, le noyau de $\hat{G}_E \rightarrow \bar{G}$ s'identifie à $C = \varprojlim C_\mathfrak{q}$ et l'action de G sur C décrite ci-dessus n'est autre que l'action naturelle du sous-groupe G de $\hat{G}_E$ sur C, par automorphismes intérieurs.]

PROPOSITION 4. *L'action de* G *sur* C *est triviale.*

Soit H le sous-groupe distingué de G formé des éléments qui agissent trivialement sur C. D'après la prop. 2, H contient les éléments de la forme $h(u)^m$, avec $u \in U$ et $m = \text{Card}(\mu)$. Comme $\text{Card}(S) \geqq 2$, cela montre que H est infini. Mais les seuls sous-groupes distingués de $G = \mathbf{SL}_2(K)$ sont $\{1\}$, $\{\pm 1\}$ et G. On a donc $H = G$, ce qui démontre la proposition.

COROLLAIRE 1. *Si* $\mathfrak{q}$ *est un idéal* $\neq 0$ *de* A, *le groupe* $C_\mathfrak{q}$ *est contenu dans le centre de* $\Gamma_A/E_\mathfrak{q}$.

(En d'autres termes, on a la formule $(\Gamma_A, \Gamma_\mathfrak{q}) \subset E_\mathfrak{q}$.) En effet, la proposition montre que Γ_A opère trivialement sur C, donc aussi sur $C_\mathfrak{q}$ qui en est un quotient.

COROLLAIRE 2. *Les groupes* $C_\mathfrak{q}$ *sont des groupes abéliens de type fini.*

Le fait que les $C_\mathfrak{q}$ soient abéliens résulte du cor. 1; qu'ils soient de type fini résulte de ce que $\Gamma_\mathfrak{q}$ est de type fini, cf. n° 1.2.

2.5. *Expression de* $C(G)$ *en termes des* $C_\mathfrak{q}$.

Revenons aux complétés $\hat{G}$, $\bar{G}$, $\hat{\Gamma}_A$, $\bar{\Gamma}_A$ définis au n° 1.3. On a

$$\hat{\Gamma}_A = \varprojlim \Gamma_A/N ,$$

où N parcourt l'ensemble $\mathcal{F}$ des sous-groupes d'indice fini de Γ_A. Si $N \in \mathcal{F}$, la prop. 1 montre qu'il existe un idéal $\mathfrak{q} \neq 0$ tel que $E_\mathfrak{q} \subset N$. On en conclut que

$$\hat{\Gamma}_A = \varprojlim (\Gamma_A/E_\mathfrak{q})^\wedge,$$

où $(\Gamma_A/E_\mathfrak{q})^\wedge$ désigne le complété de $\Gamma_A/E_\mathfrak{q}$ pour la topologie des sous-groupes d'indice fini. Comme $C_\mathfrak{q} = \Gamma_\mathfrak{q}/E_\mathfrak{q}$ est un sous-groupe d'indice fini de $\Gamma_A/E_\mathfrak{q}$, son complété $\hat{C}_\mathfrak{q}$ pour la topologie des sous-groupes d'indice fini s'identifie à l'adhérence de $C_\mathfrak{q}$ dans $(\Gamma_A/E_\mathfrak{q})^\wedge$ et l'on a la suite exacte

$$\{1\} \longrightarrow \hat{C}_\mathfrak{q} \longrightarrow (\Gamma_A/E_\mathfrak{q})^\wedge \longrightarrow \Gamma_A/\Gamma_\mathfrak{q} \longrightarrow \{1\} .$$

En passant à la limite projective (ce qui est loisible, puisque les groupes en question sont *compacts*), on obtient la suite exacte

$$\{1\} \to \varprojlim \hat{C}_{\mathfrak{q}} \to \varprojlim (\Gamma_A/E_{\mathfrak{q}})^{\wedge} \to \varprojlim (\Gamma_A/\Gamma_{\mathfrak{q}}) \to \{1\} ,$$

ou encore:

$$\{1\} \to \varprojlim \hat{C}_{\mathfrak{q}} \to \hat{\Gamma}_A \to \bar{\Gamma}_A \to \{1\} .$$

En comparant à la suite exacte

$$\{1\} \to C(G) \to \hat{\Gamma}_A \to \bar{\Gamma}_A \to \{1\} ,$$

on voit que l'on a démontré:

PROPOSITION 5. *Le groupe* $C(G)$ *peut être identifié à la limite projective* $\varprojlim \hat{C}_{\mathfrak{q}}$ *des complétés des groupes* $C_{\mathfrak{q}}$.

On va en déduire:

COROLLAIRE. *Le groupe* $C(G)$ *est contenu dans le centre du groupe* G.

Il faut prouver que les éléments de $\hat{G}$ et de $\varprojlim \hat{C}_{\mathfrak{q}}$ commutent. Comme G est dense dans $\hat{G}$ et $\varprojlim C_{\mathfrak{q}}$ dense dans $\varprojlim \hat{C}_{\mathfrak{q}}$, il suffit de prouver que, si $g \in G$ et $x \in \varprojlim C_{\mathfrak{q}}$, on a $gxg^{-1} = x$. Or, on vérifie aussitôt que $gxg^{-1} = i_g(x)$, les notations étant celles du n° 2.4. La formule $gxg^{-1} = x$ résulte alors de la prop. 4.

Remarque. Au lieu d'utiliser la prop. 4, on peut se contenter d'utiliser la prop. 3; celle-ci montre en effet que les éléments de Γ_A de la forme $h(u)^m$, avec $u \in U$ et $m = \mathrm{Card}\,(\mu)$, centralisent $C(G) = \varprojlim \hat{C}_{\mathfrak{q}}$; comme le seul sous-groupe distingué de G contenant ces éléments est G lui-même, on en déduit que $C(G)$ est centralisé par G, donc aussi par $\hat{G}$.

2.6. *Utilisation de la théorie de C. Moore.*

Puisque $C(G)$ est contenu dans le centre de $\hat{G}$, on peut appliquer le th. 13.1 de [16] (voir aussi [4], chap. IV, § 15), et l'on obtient:

THÉORÈME 1. *Le groupe* $\hat{G}$ *est le revêtement universel de* $\bar{G}$ *relativement à* G (au sens de C. Moore [16]); *le groupe* $C(G)$ *est isomorphe au groupe fondamental relatif* $\pi_1(\bar{G}, G)$.

Nous dirons que S est *totalement imaginaire* si toutes les places $v \in S$ sont archimédiennes complexes. Cela équivaut à dire que K est un corps de nombres totalement imaginaire et que S est égal à l'ensemble Σ^∞ de ses places archimédiennes (noter que le degré de ce corps est $\geqq 4$, puisqu'on a $\mathrm{Card}\,(S) \geqq 2$).

THÉORÈME 2. (a) *Le groupe* $C(G)$ *est un groupe cyclique fini, isomorphe à* μ *si* S *est totalement imaginaire, et réduit à l'élément neutre sinon.*

(b) *Les groupes* $C_{\mathfrak{q}}$ *sont cycliques finis d'ordre divisant* $m = \mathrm{Card}\,(\mu)$; *ils sont réduits à* $\{1\}$ *si* S *n'est pas totalement imaginaire.*

(c) *Le groupe C est isomorphe à $C(G)$.*

L'assertion (a) résulte de la détermination du groupe fondamental relatif $\pi_1(\bar{G}, G)$ faite par C. Moore ([16], th. 12.3). D'autre part, puisque $\hat{C}_{\mathfrak{q}}$ est isomorphe à un quotient de $C(G)$, c'est aussi un groupe cyclique fini. Mais $C_{\mathfrak{q}}$ est un groupe abélien de type fini (cor. 2 à la prop. 4); si son complété est un groupe fini, c'est qu'il est lui-même un groupe fini, et l'on a $C_{\mathfrak{q}} = \hat{C}_{\mathfrak{q}}$, d'où (b) et (c).

COROLLAIRE 1. *Pour qu'un sous-groupe de Γ_A soit d'indice fini, il faut et il suffit qu'il contienne un $E_{\mathfrak{q}}$.*

La nécessité résulte de la prop. 1; la suffisance résulte de ce que $E_{\mathfrak{q}}$ est d'indice fini dans Γ_A, puisque $C_{\mathfrak{q}} = \Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ est fini.

COROLLAIRE 2. *Soit N un sous-groupe d'indice fini de Γ_A, et soit N_1 le plus petit sous-groupe de S-congruence contenant N. Alors N est distingué dans N_1 et le quotient N_1/N est cyclique d'ordre un diviseur de m.*

On peut choisir un idéal $\mathfrak{q}$ non nul tel que $E_{\mathfrak{q}} \subset N$ et $\Gamma_{\mathfrak{q}} \subset N_1$. Si $x \in N$, $y \in \Gamma_{\mathfrak{q}}$, on a $yxy^{-1}x^{-1} \in E_{\mathfrak{q}}$ (cf. cor. 1 à la prop. 4), donc yxy^{-1} appartient à N. Ainsi, N est normalisé par $\Gamma_{\mathfrak{q}}$. Le groupe $N.\Gamma_{\mathfrak{q}}$ est un groupe de congruence contenant N et contenu dans N_1; il est donc égal à N_1. Cela montre que N est distingué dans N_1 et que N_1/N est isomorphe à un quotient de $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$, donc est cyclique d'ordre un diviseur de m.

COROLLAIRE 3. *Si S n'est pas totalement imaginaire, on a $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}$ pour tout $\mathfrak{q}$; tout sous-groupe S-arithmétique de G est un groupe de S-congruence.*

La première assertion traduit le fait que $C_{\mathfrak{q}} = \{1\}$; la seconde résulte de la première.

Exemple. Le cor. 3 s'applique notamment lorsque K est un *corps de fonctions*, ou lorsque S contient une *place non-archimédienne* (par exemple, lorsque $K = \mathbf{Q}$ et $S = \{\infty, p_1, \cdots, p_k\}$, $k \geqq 1$, les p_i étant des nombres premiers). *Remarque.* Le cas où $K = \mathbf{Q}$ peut aussi se traiter sans utiliser la théorie de Moore, comme dans [3]: l'extension centrale (**) donne la suite exacte de cohomologie suivante (il s'agit de cohomologie de *groupes profinis*, à coefficients dans le groupe discret $\mathbf{Q}/\mathbf{Z}$):

$$0 \rightarrow H^1(\bar{\Gamma}_A) \rightarrow H^1(\hat{\Gamma}_A) \rightarrow H^1(C(G)) \rightarrow H^2(\bar{\Gamma}_A) .$$

Or le groupe $\bar{\Gamma}_A$ est isomorphe à $\prod_{p \notin S} \mathbf{SL}_2(\mathbf{Z}_p)$. Comme la cohomologie de $\mathbf{SL}_2(\mathbf{Z}_p)$ est connue (cf. [3], n° 3), on en déduit que $H^2(\bar{\Gamma}_A) = 0$ et que $H^1(\bar{\Gamma}_A)$ est cyclique d'ordre 12, 4, 3, ou 1 suivant que l'on a $2, 3 \notin S$, ou $3 \in S$, $2 \notin S$, ou $2 \in S$, $3 \notin S$ ou $2, 3 \in S$. D'autre part, le groupe $H^1(\hat{\Gamma}_A)$ est isomorphe à

Hom $(\Gamma_A, \mathbf{Q}/\mathbf{Z})$ et ce dernier groupe n'est pas difficile à déterminer (on peut, par exemple, procéder par récurrence sur k, en utilisant la structure de Γ_A comme somme amalgamée, cf. Ihara [12] ou [22], chap. II, n° 1.4). On trouve ainsi que $H^1(\hat{\Gamma}_A)$ a même ordre que $H^1(\bar{\Gamma}_A)$; d'où $H^1(C(G)) = 0$ et $C(G) = \{1\}$; la trivialité des $C_\mathfrak{q}$ en résulte, comme on l'a vu ci-dessus.

Lorsque $k = 1$, cette méthode est essentiellement équivalente à celle utilisée par Mennicke [15].

COROLLAIRE 4. *Supposons S totalement imaginaire, et $\mathfrak{q}$ divisible par $m' = m\prod_{p|m} p^{1/(p-1)}$. Alors $(\Gamma_\mathfrak{q}: E_\mathfrak{q}) = m$; l'homomorphisme de Kubota* (cf. [4], § 6) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (b/a)_m$ *définit par passage au quotient un isomorphisme de $\Gamma_\mathfrak{q}/E_\mathfrak{q}$ sur μ.* (On note $(b/a)_m$ le symbole de reste de m-ième puissance.)

On sait en effet (cf. [4], th. 6.1) que l'homomorphisme de Kubota

$$\Gamma_\mathfrak{q}/E_\mathfrak{q} \to \mu$$

est surjectif. Comme $\Gamma_\mathfrak{q}/E_\mathfrak{q}$ est d'ordre un diviseur de m, c'est donc un isomorphisme.

Remarques (sur le cas totalement imaginaire).

(1) Si $\mathfrak{q}$ est divisible par m', le cor. 4 montre que $E_\mathfrak{q}$ est égal à l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\Gamma_\mathfrak{q}$ telles que $(b/a)_m = 1$.

(2) Pour tout idéal non nul $\mathfrak{q}$ de A, on a défini dans [4], th. 3.6, un certain diviseur $r(\mathfrak{q})$ de m, et montré que le groupe "stable" $C_\mathfrak{q}(n)$, relatif à $\mathbf{SL}_n$, $n \geqq 3$, est cyclique d'ordre $r(\mathfrak{q})$. Comme $C_\mathfrak{q} \to C_\mathfrak{q}(n)$ est surjectif, il s'ensuit que l'ordre de $C_\mathfrak{q}$ est multiple de $r(\mathfrak{q})$. En fait, H. Bass m'a communiqué une démonstration du fait que l'ordre de $C_\mathfrak{q}$ est *égal* à $r(\mathfrak{q})$, autrement dit que $C_\mathfrak{q} \to C_\mathfrak{q}(n)$ est toujours un *isomorphisme*. En particulier, $C_\mathfrak{q}$ est réduit à $\{1\}$ pour $\mathfrak{q} = A$: le groupe Γ_A est engendré par les conjugués des $E_{12}(x)$, $x \in A$.

Il serait intéressant d'étendre ce résultat de Bass (resp. les résultats de [4]) au cas d'un groupe $\mathbf{SL}(\Lambda)$, où Λ est un A-module projectif de rang 2 (resp. de rang $n \geqq 3$), cf. O'Meara [17]; on définit alors les $E_\mathfrak{q}$ au moyen d'une décomposition de Λ en somme directe de modules de rang 1, ou, ce qui revient au même, au moyen du choix d'un sous-groupe radiciel de $\mathbf{SL}_2$ (resp. de $\mathbf{SL}_n$); il est d'ailleurs probable que $E_\mathfrak{q}$ ne dépend pas d'un tel choix.

THÉORÈME 3. *Soit N un sous-groupe S-arithmétique de G. Tout sous-groupe distingué de N est contenu dans $\{\pm 1\}$ ou est d'indice fini dans N.*

Soit X un sous-groupe distingué de N non contenu dans $\{\pm 1\}$. D'après la prop. 2, X contient un $E_\mathfrak{q}$ et d'après le cor. 1 au th. 2 $E_\mathfrak{q}$ est d'indice fini dans Γ_A; comme $(N: \Gamma_A \cap N)$ est fini, on en déduit bien que X est d'indice fini dans N.

COROLLAIRE. *Le quotient N^{ab} de N par son groupe dérivé (N, N) est fini.*

En effet, il est clair que (N, N) n'est pas contenu dans $\{\pm 1\}$.

2.7. *Application: représentations linéaires des groupes S-arithmétiques.*

Soit N un sous-groupe S-arithmétique de G, soit k un corps commutatif, et soit $\rho\colon N \to \mathbf{GL}_n(k)$ une représentation linéaire de N sur k.

THÉORÈME 4. *Si les caractéristiques de k et K sont différentes, l'image de N par ρ est finie.*

Quitte à agrandir k, on peut le supposer algébriquement clos. D'après la prop. 1, il existe un idéal $\mathfrak{q} \neq 0$ de A tel que $E_{\mathfrak{q}}$ soit contenu dans N; d'autre part, l'ensemble U' des $u \in U$ tels que $h(u) \in N$ est un sous-groupe d'indice fini de U. Soit B le sous-groupe de N engendré par $E_{12}(\mathfrak{q})$ et $h(U')$; c'est un groupe résoluble. Le groupe $\rho(B)$ est un sous-groupe résoluble de $\mathbf{GL}_n(k)$; soit H son adhérence pour la topologie de Zariski, et soit H^0 la composante neutre de H. Quitte à remplacer ρ par une représentation équivalente, on peut supposer que les éléments de H^0 sont *triangulaires* (cela résulte du théorème de Lie-Kolchin, puisque H^0 est résoluble et connexe). Soit X l'ensemble des $x \in \mathfrak{q}$ tels que $\rho(E_{12}(x)) \in H^0$ et soit U_1 l'ensemble des $u \in U$ tels que $\rho(h(u)) \in H^0$; le groupe X (resp. U_1) est d'indice fini dans A (resp. dans U). Soit $u \in U_1$ tel que $u^2 \neq 1$ (on peut, par exemble, prendre u d'ordre infini). Les éléments $\rho(E_{12}(y))$, avec $y \in (u^2 - 1)X$, appartiennent au *groupe dérivé* de H^0, et sont donc des matrices triangulaires *unipotentes* (leurs coefficients diagonaux sont égaux à 1). Distinguons alors deux cas:

(a) K est de caractéristique p, et k de caractéristique $\neq p$. Les éléments $E_{12}(y)$ sont alors d'ordre p si $y \neq 0$, et d'autre part aucune matrice unipotente de $\mathbf{GL}_n(k)$ n'est d'ordre p. On en conclut que les $E_{12}(y)$, avec $y \in (u^2 - 1)X$, appartiennent au noyau Z de ρ. Le groupe Z n'est donc pas contenu dans $\{\pm 1\}$, et le théorème 3 montre que $(N: Z)$ est fini.

(b) K est de caractéristique 0 et k de caractéristique p. Toute matrice unipotente z de $\mathbf{GL}_n(k)$ vérifie alors la relation $z^{p^{n-1}} = 1$. On en conclut que le noyau de ρ contient les éléments de la forme $E_{12}(y)$, avec $y \in p^{n-1}(u^2 - 1)X$, et on conclut comme précédemment.

Supposons maintenant que les corps K et k soient *tous deux de caractéristique zéro* (j'ignore ce qui se passe quand tous deux sont de caractéristique p). Soit $H = R_{K/\mathbf{Q}}(\mathbf{SL}_{2/K})$ le groupe algébrique sur $\mathbf{Q}$ déduit de $\mathbf{SL}_{2/K}$ par l'opération $R_{K/\mathbf{Q}}$ de restriction des scalaires de K à $\mathbf{Q}$ (au sens de Weil [24], § 1.3); le groupe $H(\mathbf{Q})$ des points rationnels de H s'identifie à $G = \mathbf{SL}_2(K)$. Si $f\colon H_{n/k} \to \mathbf{GL}_{n/k}$ est un homomorphisme de k-groupes algébriques, la restriction de f à N est une représentation linéaire de N; une telle représentation sera dite *algébrique*.

THÉORÈME 5. *Si K et k sont de caractéristique zéro, il existe un sous-groupe N_1 de N, d'indice fini, tel que la restriction de ρ à N_1 soit algébrique.*

On en déduit, comme dans [4], § 16:

COROLLAIRE 1. *La représentation ρ est semi-simple.*

COROLLAIRE 2. *Si V est un $k[N]$-module de rang fini sur k, le groupe de cohomologie $H^1(N, V)$ est réduit à* 0.

(Lorsque l'action de N sur V est triviale, la nullité de $H^1(N, V)$ équivaut à la finitude de $N/(N, N)$, qui a déjà été démontrée; lorsqu'on prend pour V la représentation adjointe de N, la nullité de $H^1(N, V)$ entraîne que N est *rigide*.)

Remarque. Quitte à remplacer N_1 par l'intersection de ses conjugués, on peut supposer qu'il est *distingué* dans N. Supposons que ce soit le cas, et écrivons les $\rho(n)$, $n \in N$, sous la forme $u(n)f(n)$, où f est algébrique et coïncide avec ρ sur N_1. Si $n \in N$ et $n_1 \in N_1$, on a:

$$\begin{aligned} u(n)f(n_1) &= \rho(n)f(n)^{-1}f(n_1) = \rho(n)f(n^{-1}n_1n)f(n)^{-1} \\ &= \rho(n)\rho(n^{-1}n_1n)f(n)^{-1} = \rho(n_1)\rho(n)f(n)^{-1} \\ &= f(n_1)u(n) \ , \end{aligned}$$

ce qui montre que $u(n)$ commute aux éléments de $f(N_1)$. Mais N_1 est dense dans H pour la topologie de Zariski. Il s'ensuit que les $u(n)$ commutent à $f(H)$, et que u est un homomorphisme. Le couple (u, f) est donc une représentation du groupe $N/N_1 \times H_{/k}$. On en tire en particulier:

COROLLAIRE 3. *Supposons k algébriquement clos, et soient $\sigma_1, \cdots, \sigma_r$ les différents plongements de K dans k, avec $r = [K: \mathbf{Q}]$. Si $1 \leqq i \leqq r$, soit V_i la représentation de degré 2 de $\mathbf{SL}_2(K)$ donnée par σ_i. Toute représentation simple de N est isomorphe à une représentation de la forme*

$$W \otimes \mathrm{Sym}^{m_1}(V_1) \otimes \cdots \otimes \mathrm{Sym}^{m_r}(V_r)$$

où W est une représentation simple de N à noyau d'indice fini, et où les m_i sont des entiers $\geqq 0$.

(Cela résulte de ce qui précède, combiné avec le fait que toute représentation simple de $\mathbf{SL}_2$ est une puissance symétrique de la représentation fondamentale.)

Le corollaire précédent entraîne:

COROLLAIRE 4. *Soit $x \in N$. Les valeurs propres de $\rho(x)$ sont produits de racines de l'unité et de conjuguées des valeurs propres de x.*

Démonstration du théorème 5.

Elle comporte plusieurs étapes.

(i) *Le cas* $k = \mathbf{Q}$.

La démonstration donnée dans [4], § 16 pour les groupes arithmétiques s'applique presque sans changement à N; il est inutile de la reproduire. (Le point essentiel était la finitude de $C(G)$, et celle-ci a été démontrée plus haut.) Il y a toutefois une précaution à prendre: le nombre premier p utilisé dans la démonstration doit être distinct des caractéristiques résiduelles de S.

(ii) *Le cas où* k *est algébrique sur* $\mathbf{Q}$.

Comme N est de type fini, les coefficients des $\rho(x)$, $x \in N$, appartiennent à un sous-corps de k de degré fini sur $\mathbf{Q}$. On peut donc supposer que $[k: \mathbf{Q}]$ est fini. Soit $d = [k: \mathbf{Q}]$. Le choix d'une base de k permet d'identifier le groupe $R_{k/\mathbf{Q}}(\mathbf{GL}_{n/k})$ au commutant dans $\mathbf{GL}_{nd}$ du tore $T = R_{k/\mathbf{Q}}(\mathbf{G}_{m/k})$ défini par k. D'après (i), appliqué à nd, il existe un sous-groupe N_1 d'indice fini de N tel que la restriction de ρ à N_1 se prolonge en un homomorphisme de $\mathbf{Q}$-groupes algébriques

$$f_1: H \longrightarrow \mathbf{GL}_{nd} .$$

Comme N_1 est dense dans H pour la topologie de Zariski, l'image de f_1 commute à T. On peut donc interpréter f_1 comme un homomorphisme de H dans le groupe $R_{k/\mathbf{Q}}(\mathbf{GL}_{n/k})$, ou, ce qui revient au même, comme un k-homomorphisme de $H_{/k}$ dans $\mathbf{GL}_{n/k}$; d'où le théorème dans ce cas.

(iii) *Algébricité des traces.*

Soit $\bar{k}$ une clôture algébrique de k, soit $\overline{\mathbf{Q}}$ la fermeture algébrique de $\mathbf{Q}$ dans $\bar{k}$, et soit $k_0 = k \cap \overline{\mathbf{Q}}$. Nous allons montrer que *les éléments* $\operatorname{Tr}\big(\rho(x)\big)$, *avec* $x \in N$, *appartiennent à* k_0.

Tout d'abord, puisque N est de type fini, il existe un sous-anneau Λ de k, de type fini sur $\mathbf{Z}$ (comme algèbre), tel que ρ soit à valeurs dans $\mathbf{GL}_n(\Lambda)$. Soit $x \in N$ tel que $t = \operatorname{Tr}\big(\rho(x)\big)$ ne soit pas dans k_0. Le sous-anneau $\mathbf{Z}[t]$ de Λ est isomorphe à l'algèbre des polynômes $\mathbf{Z}[T]$. D'après un résultat connu (cf. Bourbaki, *Alg. Comm.*, chap. V, § 3, cor. 3 au th. 1), il existe un polynôme $P \neq 0$ de $\mathbf{Z}[T]$ jouissant de la propriété suivante: tout homomorphisme $\varphi: \mathbf{Z}[t] \longrightarrow \overline{\mathbf{Q}}$ tel que $\varphi\big(P(t)\big) \neq 0$ est prolongeable en un homomorphisme de Λ dans $\overline{\mathbf{Q}}$. En d'autres termes, il existe un sous-ensemble fini I de $\overline{\mathbf{Q}}$ tel que, pour tout $\alpha \notin I$, il existe un homomorphisme $\varphi_\alpha: \Lambda \longrightarrow \overline{\mathbf{Q}}$ tel que $\varphi_\alpha(t) = \alpha$. En composant ρ avec l'homomorphisme de $\mathbf{GL}_n(\Lambda)$ dans $\mathbf{GL}_n(\overline{\mathbf{Q}})$ donné par φ_α, on obtient alors une représentation $\rho_\alpha: N \longrightarrow \mathbf{GL}_n(\overline{\mathbf{Q}})$ telle que $\operatorname{Tr}\big(\rho_\alpha(x)\big) = \alpha$. Soit d'autre part P_S l'ensemble des caractéristiques résiduelles des places ultramétriques appartenant à S, et soit w une place ultramétrique de $\overline{\mathbf{Q}}$ dont la caractéristique résiduelle n'appartient pas à P_S. D'après le cor. 4, appliqué à ρ_α (ce qui est loisible, puisque le th. 5 est démontré pour $\overline{\mathbf{Q}}$), les valeurs propres de $\rho_\alpha(x)$ appartiennent à l'anneau local de w, i.e. sont *w-entières*. Il en est donc de même de $\alpha = \mathrm{Tr}\,(\rho_\alpha(x))$. Mais c'est absurde, puisque α peut être choisi arbitrairement en dehors de l'ensemble fini I. Ainsi, $\mathrm{Tr}\,(\rho(x))$ appartient bien à k_0 pour tout $x \in N$.

(iv) *Le cas où ρ est semi-simple et k algébriquement clos.*

Avec les notations ci-dessus, on a $k_0 = \overline{\mathbf{Q}}$. Soit $\overline{\mathbf{Q}}\Lambda$ la sous-$\overline{\mathbf{Q}}$-algèbre de k engendrée par Λ. D'après Bourbaki, *loc. cit.*, il existe un homomorphisme $\theta\colon \overline{\mathbf{Q}}\Lambda \to \overline{\mathbf{Q}}$ dont la restriction à $\overline{\mathbf{Q}}$ est l'identité. En transformant ρ par θ, on obtient une représentation $\rho'\colon N \to \mathbf{GL}_n(\overline{\mathbf{Q}})$ et, d'après (iii), les représentations ρ et ρ' ont *même trace*. La représentation ρ' est semi-simple, d'après (ii); si l'on suppose qu'il en est de même de ρ, on voit que ρ et ρ' sont *équivalentes*. Comme le th. 5 s'applique à ρ', il s'applique aussi à ρ.

(v) *Le cas où k est algébriquement clos.*

Vu ce qui précède, il suffit de prouver que toute représentation de N sur k est semi-simple, ou encore que toute extension de deux représentations simples V_1 et V_2 est scindée. Mais les classes d'extensions de V_1 par V_2 correspondent bijectivement aux éléments de $H^1(N, W)$, où $W = \mathrm{Hom}\,(V_1, V_2)$. D'après (iv), V_1 et V_2 proviennent par extension des scalaires de représentations V_1^0 et V_2^0 définies sur $\overline{\mathbf{Q}}$; si l'on pose $W^0 = \mathrm{Hom}\,(V_1^0, V_2^0)$, on a donc $W = k \otimes W^0$ (le produit tensoriel étant pris sur $\overline{\mathbf{Q}}$), d'où $H^1(N, W) = k \otimes H^1(N, W^0)$ puisque N est de type fini. Mais, d'après (ii), toute représentation linéaire de N sur $\overline{\mathbf{Q}}$ est semi-simple; on a donc $H^1(N, W^0) = 0$, d'où $H^1(N, W) = 0$, ce qui démontre notre assertion.

(vi) *Cas général.*

Soit $\bar{k}$ une clôture algébrique de k. En appliquant (v), on voit qu'il existe un sous-groupe N_1 de N, d'indice fini, tel que la restriction de ρ à N_1 se prolonge en un $\bar{k}$-homomorphisme $\bar{f}$ de $H_{/\bar{k}}$ dans $\mathbf{GL}_{n/\bar{k}}$. Mais N_1 est dense dans H pour la topologie de Zariski, et $\bar{f}(N_1)$ est contenu dans $\mathbf{GL}_n(k)$; on déduit de là que $\bar{f}$ est "défini sur k", i.e. provient par extension des scalaires d'un homomorphisme $f\colon H_{/k} \to \mathbf{GL}_{n/k}$, cqfd.

Remarque. Les mêmes arguments que ci-dessus permettent d'étendre le th. 16.2 de [4] au cas d'un corps de caractéristique zéro quelconque.

§ 3. Le cas Card $(S) = 1$.

Dans ce paragraphe, on suppose que *S est réduit à un seul élément.*

Lorsque K est de caractéristique $p > 0$, cela signifie que A est l'anneau de coordonnées d'une courbe affine obtenue en enlevant un point à une courbe projective lisse sur un corps fini k de caractéristique p; l'exemple le plus simple est $K = k(T)$, $A = k[T]$.

Lorsque K est un corps de nombres algébriques, cela signifie que $S = \Sigma^\infty$ et Card $(\Sigma^\infty) = 1$, autrement dit que A est l'anneau des entiers de K et que ce dernier est isomorphe, soit au corps $\mathbf{Q}$ des nombres rationnels, soit à un corps quadratique imaginaire $\mathbf{Q}(\sqrt{-d})$, avec $d \in \mathbf{Z}$, $d \geqq 1$.

Dans ce qui suit, ces cas seront appelés respectivement le cas *de caractéristique p*, le cas *rationnel*, et le cas *quadratique imaginaire*.

3.1. *Les groupes Γ^{ab} et le problème des groupes de congruence.*

Soit Γ un sous-groupe S-arithmétique de G. Nous supposerons[3] dans tout ce qui suit que Γ est *net* au sens de [7], § 17.1; cela équivaut à dire qu'aucun élément de Γ n'admet comme valeur propre (dans une clôture algébrique de K) une racine de l'unité $\neq 1$.

L'existence de tels sous-groupes est facile à prouver: pour le cas des corps de nombres, voir [7], § 17.4; dans le cas des corps de fonctions, il suffit de prendre pour Γ un groupe de S-congruence $\Gamma_{\mathfrak{q}}$, avec $\mathfrak{q} \neq A$.

THÉORÈME 6. *Dans le cas rationnel et dans le cas quadratique imaginaire, Γ^{ab} est un groupe abélien infini, de type fini.*

Dans le cas de caractéristique p, Γ^{ab} est somme directe d'un groupe de type fini et d'un $\mathbf{F}_p$-espace vectoriel de dimension $\aleph_0$.

(Pour tout groupe H, on note H^{ab} le quotient de H par son groupe dérivé (H, H).)

Le cas rationnel est bien connu. En effet, Γ est alors un sous-groupe sans torsion de $\mathbf{SL}_2(\mathbf{R})$, commensurable à $\Gamma_A = \mathbf{SL}_2(\mathbf{Z})$, et le quotient $\mathbf{SL}_2(\mathbf{R})/\Gamma$ n'est pas compact. En utilisant l'action de Γ sur le demi-plan de Poincaré $X = \mathbf{SL}_2(\mathbf{R})/\mathbf{SO}_2(\mathbf{R})$, on en déduit que Γ est un *groupe libre* non abélien, de rang fini $c \geqq 2$, et le groupe Γ^{ab} est isomorphe à $\mathbf{Z}^c$, donc infini. On peut donner la valeur de c: si $\Gamma \cap \Gamma_A$ est d'indice d dans Γ et d'indice e dans Γ_A, on a $c = 1 + e/12d$ (utiliser le fait que la caractéristique d'Euler-Poincaré de $\mathbf{SL}_2(\mathbf{Z})$ est $-1/12$).

Dans les deux autres cas, le théorème se démontre en comparant Γ^{ab} à la somme directe des différentes classes de sous-groupes unipotents de Γ, cf. n° 3.2, th. 7.

COROLLAIRE 1. *Dans le cas de caractéristique p, aucun sous-groupe S-arithmétique G n'est de type fini.*

Supposons en effet qu'un tel sous-groupe H soit de type fini. Comme

[3] Il suffirait en fait de supposer que l'image Γ' de Γ dans le groupe $G' = G/\{\pm 1\}$ est un groupe *net*. Lorsque K est de caractéristique 0 (resp. de caractéristique $p > 0$), cela signifie que Γ' est *sans torsion* (resp. *sans p'-torsion*, i.e. tout élément de Γ' est d'ordre infini ou d'ordre une puissance de p).

$H \cap \Gamma$ est d'indice fini dans H et dans Γ, le groupe Γ serait de type fini, et il en serait *a fortiori* de même de Γ^{ab}, ce qui contredirait le théorème 6.

COROLLAIRE 2. *Le noyau $C(G)$ de $\hat{G} \to \bar{G}$ est infini.*

(Autrement dit, le problème des groupes de congruence a une solution *essentiellement négative.*)

Plaçons-nous d'abord dans le cas rationnel ou imaginaire quadratique. Soit $\hat{\Gamma}$ (resp. $\bar{\Gamma}$) l'adhérence de Γ dans $\hat{G}$ (resp. dans $\bar{G}$), et soit $C_\Gamma = C(G) \cap \hat{\Gamma}$ le noyau de $\hat{\Gamma} \to \bar{\Gamma}$. Si $C(G)$ était fini, il en serait de même de C_Γ et l'on pourrait appliquer le th. 16.2 de [4]; il en résulterait que $H^1(\Gamma, \mathbf{Z})$ serait *fini*; comme $H^1(\Gamma, \mathbf{Z}) = \mathrm{Hom}\,(\Gamma^{ab}, \mathbf{Z})$, cela contredirait le théorème 6.

Dans le cas de caractéristique p, définissons $\hat{\Gamma}$ et $\bar{\Gamma}$ comme ci-dessus. Ce sont des groupes profinis. Comme la topologie des groupes de congruence admet une base dénombrable de voisinages de l'élément neutre, on voit que Card $(\bar{\Gamma})$ est égal à $\mathfrak{c} = 2^{\aleph_0}$. D'autre part, le théorème 6 montre qu'il existe un homomorphisme surjectif $\varepsilon\colon \Gamma \to V$, où V désigne un $\mathbf{F}_p$-espace vectoriel de dimension $\aleph_0$. Comme $\hat{\Gamma}$ est le complété de Γ pour la topologie des sous-groupes d'indice fini, on en déduit un homomorphisme surjectif $\hat{\varepsilon}\colon \hat{\Gamma} \to \hat{V}$. Mais on voit tout de suite que $\hat{V}$ n'est autre que le *bidual* V'' de V, muni de la topologie de la convergence simple sur le dual V'. On a

$$\mathrm{Card}\,(V') = \mathfrak{c} \ \text{ et } \ \mathrm{Card}\,(\hat{V}) = \mathrm{Card}\,(V'') = 2^{\mathfrak{c}}\ ,$$

d'où Card $(\hat{\Gamma}) \geqq 2^{\mathfrak{c}} > \mathfrak{c} =$ Card $(\bar{\Gamma})$. Il en résulte que C_Γ est infini, et même de cardinal $\geqq 2^{\mathfrak{c}}$, d'où le même résultat pour $C(G)$.

Remarque. On a en fait:

Card $\big(C(G)\big) = \mathfrak{c}$ dans le cas rationnel ou imaginaire quadratique

Card $\big(C(G)\big) = 2^{\mathfrak{c}}$ dans le cas de caractéristique p.

3.2. *Classes de sous-groupes unipotents.*

Soit V le K-espace vectoriel K^2, et soit $\mathbf{P} = \big(V - \{0\}\big)/K^*$ la droite projective correspondante. Le groupe G opère de façon naturelle sur V et $\mathbf{P}$.

LEMME 6. *Soit N un sous-groupe S-arithmétique de G. Le nombre h_N des orbites de N dans $\mathbf{P}$ est fini; lorsque $N = \Gamma_A$, ce nombre est égal au nombre de classes h de l'anneau de Dedekind A.*

Rappelons brièvement la démonstration de ce résultat bien connu. Comme N est commensurable à Γ_A, il suffit de prouver la dernière assertion. Soit Λ le réseau A^2 de V, et soit $D \in \mathbf{P}$; le point D détermine une droite de V, que l'on note encore D. Le A-module $D \cap \Lambda$ est projectif de rang 1; soit $c(D)$ son image dans le groupe $c(A)$ des classes d'idéaux de A. Si $\gamma \in \Gamma_A$, on a $c(\gamma D) = c(D)$; ainsi, $D \mapsto c(D)$ définit par passage au quotient une application

$c\colon \mathbf{P}/\Gamma_A \to c(A)$. En utilisant la structure des modules sur les anneaux de Dedekind (Bourbaki, *Alg. Comm.*, chap. VII, § 4, n° 10), on montre que c est une *bijection*; on a donc bien Card $(\mathbf{P}/\Gamma_A) = h$.

Si $D \in \mathbf{P}$, notons B_D (resp. U_D) le sous-groupe de Borel (resp. le sous-groupe unipotent) de G défini par D, autrement dit l'ensemble des $g \in G$ tels que $gD = D$ (resp. tels que $gx = x$ pour tout $x \in D$).

LEMME 7. *Soit $D \in \mathbf{P}$ et soit N un sous-groupe S-arithmétique de G. Le groupe $U_D \cap N$ est un sous-groupe distingué d'indice fini du groupe $B_D \cap N$; on a $U_D \cap N = B_D \cap N$ si N est net.*

Si $g \in B_D$, notons $\omega(g)$ l'élément de K^* tel que $gx = \omega(g)x$ pour tout $x \in D$; on a la suite exacte

$$\{1\} \longrightarrow U_D \longrightarrow B_D \xrightarrow{\omega} K^* \longrightarrow \{1\} .$$

D'autre part, si γ appartient à un sous-groupe S-arithmétique de G, les valeurs propres de γ sont des éléments *entiers* sur A.

En particulier, si $\gamma \in B_D \cap N$, on a $\omega(\gamma) \in A^*$, d'où une suite exacte

$$\{1\} \longrightarrow U_D \cap N \longrightarrow B_D \cap N \longrightarrow A^* .$$

Comme Card $(S) = 1$, le groupe A^* est *fini*; on voit donc bien que $U_D \cap N$ est d'indice fini dans $B_D \cap N$. Si en outre N est net, on a $\omega(\gamma) = 1$ pour tout $\gamma \in B_D \cap N$, puisque $\omega(\gamma)$ est une racine de l'unité; d'où le fait que $U_D \cap N = B_D \cap N$ dans ce cas.

Revenons maintenant aux notations et hypothèses du n° 3.1, et soit Γ un sous-groupe S-arithmétique net de G. Choisissons des représentants (D_i), $i \in \mathbf{P}/\Gamma$, des éléments de $\mathbf{P}/\Gamma$; pour tout i, posons

$$\Gamma_i = U_{D_i} \cap \Gamma = B_{D_i} \cap \Gamma ,$$

cf. lemme 7. Les Γ_i sont des groupes abéliens; notons $U(\Gamma)$ leur *somme directe* $\coprod_{i \in \mathbf{P}/\Gamma} \Gamma_i$; à isomorphisme canonique près, elle est indépendante du choix des représentants D_i. L'inclusion $\Gamma_i \to \Gamma$ définit un homomorphisme $\alpha_i\colon \Gamma_i \to \Gamma^{ab}$, d'où, par somme directe, un homomorphisme

$$\alpha\colon U(\Gamma) \to \Gamma^{ab} .$$

THÉORÈME 7. (a) *Dans le cas de caractéristique p, $U(\Gamma)$ est un $\mathbf{F}_p$-espace vectoriel de dimension $\aleph_0$, le noyau de α est fini, et son conoyau est de type fini.*

(b) *Dans le cas quadratique imaginaire, $U(\Gamma)$ est un groupe abélien libre de rang $2h_\Gamma$, et le noyau de α est de rang h_Γ.*

(Rappelons que h_Γ désigne le nombre d'éléments de $\mathbf{P}/\Gamma$, cf. lemme 6.)

Chacun des Γ_i est un sous-groupe S-arithmétique du groupe additif $\mathbf{G}_a$, donc est isomorphe à un sous-groupe d'indice fini de A. Dans le cas (a), A est un $\mathbf{F}_p$-espace vectoriel de dimension $\aleph_0$, et dans le cas (b), A est isomorphe à $\mathbf{Z}^2$. Comme le nombre de facteurs de $U(\Gamma)$ est h_Γ, on en déduit bien les assertions relatives à la structure de $U(\Gamma)$. Celles relatives à α seront démontrées aux n^os^ 3.3 et 3.4 ci-après.

Montrons que *le théorème* 7 *entraîne le théorème* 6. C'est clair dans le cas quadratique imaginaire, puisque l'image de α est un sous-groupe de Γ^{ab} de rang $2h_\Gamma - h_\Gamma = h_\Gamma \geqq 1$, donc a une infinité d'éléments. Dans le cas de caractéristique p, le th. 7 montre que l'on a une suite exacte

$$0 \longrightarrow W \longrightarrow \Gamma^{ab} \longrightarrow E \longrightarrow 0 \; ,$$

où W est un $\mathbf{F}_p$-espace vectoriel de dimension $\aleph_0$ et E un groupe abélien de type fini. Soit $e \in \mathrm{Ext}\,(E, W)$ la classe de cette extension. Comme E est de type fini, on peut décomposer W en $W_1 \times W_2$, avec W_2 de dimension finie, de telle sorte que e appartienne à la composante $\mathrm{Ext}\,(E, W_2)$ de $\mathrm{Ext}\,(E, W)$. Le groupe Γ^{ab} est donc isomorphe au produit direct de W_1 par un groupe E_2 extension de E par W_2; comme E_2 est de type fini, cela démontre bien le th. 6 dans le cas considéré.

Remarque. Bien que ce soit inutile pour notre objet, signalons que, *dans le cas rationnel*, le groupe $U(\Gamma)$ est libre de rang h_Γ et l'on a une suite exacte

$$0 \longrightarrow \mathbf{Z} \longrightarrow U(\Gamma) \xrightarrow{\alpha} \Gamma^{ab} \longrightarrow \mathbf{Z}^{2g_\Gamma} \longrightarrow 0 \; ,$$

où g_Γ désigne le *genre* de la surface de Riemann compactifiée de X/Γ (cf. démonstration du théorème 6). Cela résulte de la structure bien connue du premier groupe d'homologie d'une surface compacte dont on a retiré un nombre fini de points.

3.3. *Propriétés de* α: $U(\Gamma) \to \Gamma^{ab}$ (*cas de caractéristique* p).

Il s'agit de prouver que le noyau et le conoyau de α sont de type fini. Nous nous bornerons à indiquer les grandes lignes de la démonstration, renvoyant pour plus de détails à [22], chap. II, § 2.

(a) *L'arbre* X.

Soient v l'unique élément de S, O_v l'anneau de valuation correspondant et π une uniformisante de O_v. Un sous-O_v-module L de $V = K^2$ est appelé un *réseau* s'il est libre de rang 2, auquel cas il engendre le K-espace vectoriel V. Deux réseaux L et L' sont dits *équivalents* s'il existe $\lambda \in K^*$ tel que $\lambda L = L'$. Soit X l'ensemble des classes d'équivalence de réseaux de V. Deux éléments x, x' de X sont dits *voisins* si l'on peut les représenter par des réseaux L et L' tels que $L \supset L'$ et que L/L' soit un O_v-module de longueur 1. La relation de voisinage munit X d'une structure de *graphe combinatoire*; on vérifie facilement que ce graphe est connexe, non vide, et ne contient pas de circuit, autrement dit que c'est un *arbre* (cf. [22], chap. II, n° 1.1). Si $\hat{K}_v$ désigne le complété de K pour v, le groupe $\mathbf{PGL}_2(\hat{K}_v)$ opère de façon naturelle sur X; les stabilisateurs des sommets de X sont les sous-groupes compacts maximaux de $\mathbf{PGL}_2(\hat{K}_v)$. *L'arbre X joue pour $\mathbf{PGL}_2(\hat{K}_v)$ le rôle que joue le demi-plan de Poincaré pour $\mathbf{PGL}_2(\mathbf{R})$*[4].

(b) *Pointes.*

Soit d'abord $L_0 = (O_v)^2$ le réseau standard de $V = K^2$, et soit x_0 le point correspondant de X.

Soit $D \in \mathbf{P}$; comme au n° 3.2, nous identifions D à une droite de V. Si m est un entier $\geqq 0$, nous noterons $L(m, D)$ le sous-réseau de L_0 engendré par $\pi^m L_0$ et $L_0 \cap D$; soit $x(m, D)$ son image dans X. On a $x(0, D) = x_0$. Pour D fixé, les $x(m, D)$, $m = 0, 1, \cdots$, sont les sommets d'un "droit chemin" de X d'origine x_0, i.e. forment un sous-graphe de la forme

$$x_0 \circ\!\!-\!\!\!-\!\!\!-\!\!\circ\!\!-\!\!\!-\!\!\!-\!\!\circ\!\!-\!\!\!-\!\!\!-\!\!\circ\!\!-\!\!-\cdots .$$

Ce droit chemin p_D est la *pointe* définie par D; à un nombre fini de sommets près, elle ne dépend pas du choix de l'origine x_0. Si N est un entier $\geqq 0$, nous noterons $p_D(N)$ le sous-graphe de p_D formé des $x(m, D)$ tels que $m \geqq N$.

(c) *Action de Γ sur X.*

Soient Γ et $D_i (i \in \mathbf{P}/\Gamma)$ comme au n° 3.2. Le groupe Γ opère sur X.

LEMME 8. *Il existe une partie finie F de X et un entier $N \geqq 0$ tels que:*

(i) *Les pointes tronquées $p_{D_i}(N)$, $i \in \mathbf{P}/\Gamma$, sont deux à deux disjointes, et sont disjointes de F; la réunion de F et des $p_{D_i}(N)$ est un système de représentants de X/Γ dans X.*

(ii) *Si $m \geqq N$ et $i \in \mathbf{P}/\Gamma$, le stabilisateur $\Gamma_i(m)$ de $x(m, D_i)$ dans Γ est contenu dans $\Gamma_i(m+1)$ et opère transitivement sur l'ensemble des arêtes de X d'origine $x(m, D_i)$ et d'extrémité distincte de $x(m+1, D_i)$.*

(iii) *Pour tout $i \in \mathbf{P}/\Gamma$, la réunion des $\Gamma_i(m)$ est égale à Γ_i.*

Ce résultat est analogue à ceux de Borel relatifs aux domaines fondamentaux des groupes arithmétiques (cf. [7]). Il est englobé dans les résultats bien plus généraux de G. Harder [11]. La démonstration qui en est donnée dans [22], chap. II, § 2 consiste à se ramener d'abord au cas où $\Gamma = \Gamma_A$, et à interpréter les éléments de X/Γ comme certaines classes de *fibrés vectoriels de rang* 2 sur la courbe projective définie par K; le lemme provient alors de ce

[4] Plus généralement, les *immeubles* de Bruhat-Tits constituent l'analogue ultramétrique des *espaces riemanniens symétriques* de la théorie archimédienne, cf. par exemple [21].

que presque tous ces fibrés sont décomposés en sommes de deux fibrés de rang 1.

(d) *Structure de* X/Γ.

Du fait que Γ est contenu dans $\mathbf{SL}_2(K)$, aucun élément de Γ ne transforme une arête de X en son opposée; cela permet de définir le *graphe quotient* X/Γ.

LEMME 9. *Il existe un sous-graphe fini F' de X/Γ tel que le complémentaire de F' se décompose en somme disjointe de droits chemins Δ_i, images isomorphes des pointes tronquées $p_{D_i}(N+1)$ avec $i \in \mathbf{P}/\Gamma$.*

Cela résulte du lemme 8 en prenant pour F' l'image par $X \rightarrow X/\Gamma$ de la réunion de F et des $x(N, D_i)$, $i \in \mathbf{P}/\Gamma$.

(e) *Relations entre l'homologie de* Γ *et celle de* X/Γ.

Soit M un Γ-module. Soit s un entier $\geqq 0$, et soit x un sommet de X/Γ; choisissons un représentant $\bar{x}$ de x dans X, soit $\Gamma(\bar{x})$ son stabilisateur dans Γ, et soit $H_s(\Gamma(\bar{x}), M)$ le groupe d'homologie correspondant; on voit tout de suite que ce groupe est indépendant du choix de $\bar{x}$, à isomorphisme unique près; notons le $\mathcal{H}_s(x)$. On définit de même $\mathcal{H}_s(y)$ lorsque y est une arête de X/Γ, ainsi qu'un homomorphisme Cor: $\mathcal{H}_s(y) \rightarrow \mathcal{H}_s(x)$ lorsque x est une extrémité de y. La famille

$$\mathcal{H}_s = \{\mathcal{H}_s(x), \mathcal{H}_s(y), \mathrm{Cor}\}$$

constitue ce qu'il est naturel d'appeler un *cofaisceau* sur le graphe X/Γ; les groupes d'homologie correspondants sont notés $H_r(X/\Gamma, \mathcal{H}_s)$; ils sont nuls pour $r \geqq 2$.

LEMME 10. *On a une suite exacte*:

$$0 \longrightarrow H_0(X/\Gamma, \mathcal{H}_s) \longrightarrow H_s(\Gamma, M) \longrightarrow H_1(X/\Gamma, \mathcal{H}_{s-1}) \longrightarrow 0 .$$

C'est un cas particulier de la suite spectrale associée à l'action de Γ sur X, compte tenu de ce que X est de dimension 1. On peut aussi en donner une démonstration directe en utilisant la suite exacte

$$0 \longrightarrow C_1(X, M) \longrightarrow C_0(X, M) \longrightarrow M \longrightarrow 0$$

des *chaînes* de l'arbre X à coefficients dans M.

(f) *Fin de la démonstration.*

Soit $\mathcal{C}$ la classe des groupes abéliens de type fini. Appliquons le lemme 10 avec $M = \mathbf{Z}$ et $s = 1$, de sorte que $H_1(\Gamma, M)$ s'identifie à Γ^{ab}. On obtient une suite exacte

$$0 \longrightarrow H_0(X/\Gamma, \mathcal{H}_1) \longrightarrow \Gamma^{ab} \longrightarrow H_1(X/\Gamma, \mathcal{H}_0) \longrightarrow 0 .$$

Lorsque l'on remplace X/Γ par la somme disjointe des droits chemins Δ_i, les $H_r(X/\Gamma, \mathcal{H}_s)$ ne changent pas, à un $\mathcal{C}$-isomorphisme près: cela résulte du lemme 9. On peut donc (toujours à un $\mathcal{C}$-isomorphisme près) remplacer la suite exacte précédente par:

$$0 \longrightarrow \coprod_{i \in \mathbf{P}/\Gamma} H_0(\Delta_i, \mathcal{H}_1) \longrightarrow \Gamma^{ab} \longrightarrow \coprod_{i \in \mathbf{P}/\Gamma} H_1(\Delta_i, \mathcal{H}_0) \longrightarrow 0 .$$

Mais il est facile de calculer $H_0(\Delta_i, \mathcal{H}_1)$ et $H_1(\Delta_i, \mathcal{H}_0)$. On trouve:

$$H_0(\Delta_i, \mathcal{H}_1) = \varinjlim . \Gamma_i(m) = \Gamma_i$$

$$H_1(\Delta_1, \mathcal{H}_0) = H_1(\Delta_i, \mathbf{Z}) = 0 .$$

On obtient donc en définitive un $\mathcal{C}$-*isomorphisme* de $\coprod \Gamma_i$ sur Γ^{ab}, et il ne reste plus qu'à vérifier que ce $\mathcal{C}$-isomorphisme est induit par l'homomorphisme α du n° 3.2, ce qui ne présente pas de difficulté.

Remarque

La démonstration ci-dessus donne d'autres renseignements sur les $H_s(\Gamma, M)$ et en particulier sur Γ^{ab}. Elle montre par exemple que le *rang* du groupe Coker (α) est égal au *premier nombre de Betti* du graphe X/Γ, i.e. au "nombre de circuits" de X/Γ. D'autre part, si M est fini d'ordre premier à p, le groupe $H_1(\Gamma, M)$ est fini, et les $H_s(\Gamma, M)$ sont nuls pour $s \geqq 2$.

Exemple

Soit k un corps fini à q éléments. Prenons $A = k[T]$, de sorte que $K = k(T)$ et que v est la valuation "à l'infini", i.e.

$$v(a) = -\deg(a) \qquad \text{pour tout } a \neq 0 \text{ de } A .$$

Si l'on prend pour Γ le groupe $\Gamma_A = \mathbf{SL}_2(k[T])$, le graphe X/Γ est un droit chemin, isomorphe à la pointe p_D relative à la droite $D = K \times \{0\}$ de V; cela se démontre, soit directement (cf. [22], chap. II, n° 1.6), soit en utilisant la classification des fibrés vectoriels de base une droite projective, due à Grothendieck. Ce résultat est étroitement lié à la décomposition de Γ_A comme somme amalgamée (cf. [18]):

$$\Gamma_A = \mathbf{SL}_2(k) *_{B(k)} B(k[T]) ,$$

où B désigne le sous-groupe de Borel $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ de $\mathbf{SL}_2$.

Comme sous-groupe *net*, on peut prendre le groupe de congruence Γ défini par l'idéal premier (T) de A. On trouve alors ([22], *loc. cit.*, exerc. 5) que X/Γ est réunion de $q + 1$ droits chemins d'origine commune, et que Γ est isomorphe au *produit libre* des Γ_i, lesquels sont isomorphes à A; en particulier, l'homomorphisme α: $U(\Gamma) \rightarrow \Gamma^{ab}$ est un *isomorphisme*.

3.4. *Propriétés de* α: $U(\Gamma) \rightarrow \Gamma^{ab}$ (*cas quadratique imaginaire*).

Nous supposons maintenant que K est un corps quadratique imaginaire $\mathbf{Q}(\sqrt{-d})$, avec $d \in \mathbf{Z}$, $d \geqq 1$. Le groupe Γ est un sous-groupe discret du groupe de Lie $G_{\mathbf{C}} = \mathbf{SL}_2(\mathbf{C})$. Soit $X \approx G_{\mathbf{C}}/\mathbf{SU}_2(\mathbf{C})$ l'espace riemannien symétrique de $G_{\mathbf{C}}$; les points de X correspondent bijectivement aux sous-groupes compacts maximaux de $G_{\mathbf{C}}$; en tant qu'espace de Riemann, X est isomorphe à *l'espace hyperbolique à trois dimensions*. Comme Γ est sans torsion, il opère librement sur X, de sorte que X/Γ est une variété de dimension 3, orientable, et non compacte. Nous noterons X_Γ la *compactification* canonique de X/Γ décrite par Borel [7], § 17 (voir aussi l'*Appendice* ci-après); c'est une *variété à bord* compacte, dont l'intérieur est égal à X/Γ[5]. Son bord ∂X_Γ est somme disjointe de tores E_i, correspondant aux éléments i de $\mathbf{P}/\Gamma$ (ce sont les "pointes" de X/Γ); si l'on note U_i le sous-groupe unipotent de $G_{\mathbf{C}}$ formé des $g \in G_{\mathbf{C}}$ tels que $gx = x$ pour tout $x \in D_i$, le tore E_i est un espace homogène de U_i, de groupe d'isotropie $\Gamma_i = \Gamma \cap U_i$, de sorte que E_i est isomorphe à U_i/Γ_i. (Noter que U_i est un espace vectoriel de dimension 1 sur $\mathbf{C}$, de sorte que U_i/Γ_i a une structure naturelle de *courbe elliptique*, admettant le corps K comme corps de multiplication complexe.)

Puisque X est *contractile*, les groupes d'homologie $H_s(\Gamma)$ du groupe Γ s'identifient aux groupes d'homologie $H_s(X/\Gamma)$ de l'espace X/Γ; nous prenons ici comme groupe de coefficients le groupe $\mathbf{Z}$, avec action triviale de Γ. Comme l'injection $X/\Gamma \to X_\Gamma$ est une équivalence d'homotopie, on peut identifier $H_s(X/\Gamma)$ à $H_s(X_\Gamma)$. On a en particulier

$$\Gamma^{ab} = H_1(\Gamma) = H_1(X/\Gamma) = H_1(X_\Gamma) .$$

Pour la même raison, on a $H_s(\Gamma_i) = H_s(E_i)$, d'où

$$U(\Gamma) = \coprod_i \Gamma_i = \coprod_i H_1(\Gamma_i) = \coprod_i H_1(E_i) = H_1(\partial X_\Gamma) .$$

Ces diverses identifications transforment l'homomorphisme

$$\alpha\colon U(\Gamma) \longrightarrow \Gamma^{ab}$$

en un homomorphisme

$$\iota\colon H_1(\partial X_\Gamma) \longrightarrow H_1(X_\Gamma) ;$$

la construction de X_Γ donnée dans [7], *loc. cit.*, montre que ι est l'homomorphisme induit par l'injection de ∂X_Γ dans X_Γ. Or nous voulons montrer que le rang de $\operatorname{Ker}(\alpha)$ est égal à $h_\Gamma = 1/2\,\mathrm{rg}.\, U(\Gamma)$. Cela va résulter du lemme suivant, bien connu en théorie du cobordisme, appliqué à $Y = X_\Gamma$ et $m = 1$:

LEMME 11. *Soit Y une variété à bord compacte et orientable, de dimension impaire $2m + 1$. Le noyau de l'homomorphisme*

[5] Le fait que X/Γ soit l'intérieur d'une variété à bord compacte est un cas particulier d'un théorème de Raghunathan [19] valable pour tous les groupes arithmétiques.

$$\iota\colon H_m(\partial Y) \longrightarrow H_m(Y)\ ,$$

induit par l'injection de ∂Y dans Y, a un rang égal à la moitié de celui de $H_m(\partial Y)$.

Rappelons la démonstration. Soient $H^s(Y)$ et $H^s(\partial Y)$ les groupes de cohomologie, à coefficients dans $\mathbf{Q}$, de Y et de ∂Y; par dualité, il suffit de prouver que l'image de l'homomorphisme de restriction

$$\rho\colon H^m(Y) \longrightarrow H^m(\partial Y)$$

est de rang égal à 1/2. rg. $H^m(\partial Y)$. Or, on a la suite exacte

$$(*) \qquad H^m(Y) \xrightarrow{\ \rho\ } H^m(\partial Y) \xrightarrow{\ \delta\ } H^{m+1}(Y, \partial Y)\ .$$

La dualité des variétés à bord (resp. la dualité de Poincaré) définit un accouplement $(\mathbf{a}, \mathbf{b}) \mapsto \langle \mathbf{a}, \mathbf{b} \rangle$ entre $H^m(Y)$ et $H^{m+1}(Y, \partial Y)$ (resp. entre $H^m(\partial Y)$ et $H^m(\partial Y)$). Si les orientations de Y et de ∂Y sont choisies de façon cohérente; les homomorphismes ρ et δ sont *transposés* l'un de l'autre par rapport à ces accouplements, i.e. on a

$$(**) \qquad \langle \delta\mathbf{a}, \mathbf{b} \rangle = \langle \mathbf{a}, \rho\mathbf{b} \rangle \qquad \text{si } \mathbf{a} \in H^m(\partial Y),\ \mathbf{b} \in H^m(Y)\ ;$$

cela résulte simplement de la formule $d(a.\,b) = d(a).\,b$, valable lorsque b est un cocycle et a une cochaîne quelconque.

Puisque ρ est le transposé de δ, $\mathrm{Im}\,(\rho)$ est l'orthogonal de $\mathrm{Ker}\,(\delta)$ dans $H^m\,(\partial Y)$. Mais la suite exacte $(*)$ montre que $\mathrm{Ker}\,(\delta) = \mathrm{Im}\,(\rho)$. On en conclut que $\mathrm{Im}\,(\rho)$ *est son propre orthogonal dans* $H^m\,(\partial Y)$, autrement dit est un *sous-espace isotrope maximal* de $H^m\,(\partial Y)$, de rang égal à la moitié de celui de $H^m(\partial Y)$. Ceci achève la démonstration du lemme 11, et, en même temps, du théorème 7.

Remarque

Si M est un Γ-module, les groupes $H_s(\Gamma, M)$ et $H^s(\Gamma, M)$ s'identifient aux groupes d'homologie et de cohomologie correspondants de la variété X_Γ, à valeurs dans le système local défini par M. On en déduit que Γ est de *dimension cohomologique* 2, et que les $H_s(\Gamma, M)$ et $H^s(\Gamma, M)$ sont *de type fini* si M l'est; ces derniers résultats sont d'ailleurs des cas particuliers de ceux démontrés par Raghunathan [19] pour tous les groupes arithmétiques sans torsion (pour leur extension aux groupes S-arithmétiques, voir [21]).

La *caractéristique d'Euler-Poincaré* $\chi(\Gamma)$ est égale à celle de X_Γ, donc à la moitié de celle de ∂X_Γ, qui est *nulle* puisque ∂X_Γ est somme disjointe de tores. Si l'on désigne par b_s le s-ième nombre de Betti de Γ, on a donc:

$$0 = \chi(\Gamma) = 1 - b_1 + b_2 \text{ et } b_1 \geqq h_\Gamma .$$

Questions

(1) *Comment peut-on déterminer* Ker (α)? Le théorème 7 dit que c'est un sous-groupe de rang h_Γ de $U(\Gamma)$ mais ne précise pas lequel. [On peut obtenir des renseignements supplémentaires sur Ker (α) en utilisant les sous-groupes de Γ qui sont intersections de Γ avec les conjugués de $\mathbf{SL}_2(\mathbf{Q})$; toutefois, j'ignore si les renseignements ainsi obtenus sont suffisants pour déterminer Ker (α).]

(2) *Comment varie* b_1 *avec* Γ? Par exemple, si Γ est un groupe de congruence $\Gamma_\mathfrak{q}$, quelle est la représentation linéaire de $\Gamma_A/\Gamma = \mathbf{SL}_2(A/\mathfrak{q})$ dans l'espace vectoriel $\Gamma^{ab} \otimes \mathbf{Q}$? Une question voisine est celle de l'action des *opérateurs de Hecke*; si $x \in \mathbf{GL}_2(K)$, et si l'on pose $\Gamma_x = \Gamma \cap x^{-1}\Gamma x$, l'opérateur de Hecke T_x attaché à x est l'endomorphisme de Γ^{ab} défini par

$$\Gamma^{ab} \xrightarrow{v} (\Gamma_x)^{ab} \xrightarrow{u} \Gamma^{ab} ,$$

où v est le transfert de Γ dans Γ_x, et u est induit par l'application $\gamma \mapsto x\gamma x^{-1}$. Que peut-on dire des *valeurs propres* des T_x, par exemple? Pour certains sous-groupes Γ, les résultats récents de Weil [26] laissent penser que les valeurs propres en question sont étroitement liées aux propriétés arithmétiques des *courbes elliptiques définies sur* K; il serait très intéressant d'en avoir des exemples explicites.

3.5. *Compléments sur le cas quadratique imaginaire.*

Nous n'avons donné au n° précédent que le minimum nécessaire pour démontrer le théorème 7. La méthode employée (comparaison entre l'homologie de X_Γ et celle de son bord) permet d'obtenir d'autres résultats, que nous allons indiquer.

Soit Γ un sous-groupe arithmétique quelconque[6] de G; choisissons comme au n° 3.2 des représentants D_i des éléments de $\mathbf{P}/\Gamma$, et posons

$$\Gamma_i = \Gamma \cap B_{D_i} .$$

On notera que l'on a en général $\Gamma_i \neq \Gamma \cap U_{D_i}$; le groupe Γ_i peut même être non abélien, si K contient des racines de l'unité autres que ± 1.

Soit k un corps de caractéristique zéro et soit M un $k[\Gamma]$-module de rang fini sur k; les groupes de cohomologie $H^s(\Gamma, M)$, $H^s(\Gamma_i, M)$ sont des k-espaces vectoriels de dimension finie. Posons

[6] On pourrait même prendre pour Γ n'importe quel sous-groupe *discret* de $G_\mathbf{C}$ tel que $G_\mathbf{C}/\Gamma$ soit *de volume fini*. En effet, Garland et Raghunathan [10] ont montré que ces conditions entraînent l'existence d'une compactification de X/Γ ayant toutes les propriétés utilisées plus haut. On notera que certains de ces groupes *ne sont pas arithmétiques*; Makarov, Vinberg et Mostow en ont donné des exemples.

$$U^1(\Gamma, M) = \coprod_i H^1(\Gamma_i, M)$$

et soit $\rho: H^1(\Gamma, M) \to U^1(\Gamma, M)$ l'homomorphisme induit par les homomorphismes de restriction $\rho_i: H^1(\Gamma, M) \to H^1(\Gamma_i, M)$.

THÉORÈME 8. *Supposons M muni d'une forme k-bilinéaire non dégénérée invariante par Γ. On a alors*

$$\text{rg. Im}\,(\rho) = 1/2\,\text{rg. } U^1(\Gamma, M)\ .$$

Supposons d'abord que Γ *soit net.* Le Γ-module M définit alors un *système local* de coefficients $\mathfrak{M}$ sur la variété à bord X_Γ; ce système local est muni d'une forme bilinéaire non dégénérée, ce qui permet de l'identifier à son *dual*. On a ici encore

$$U^1(\Gamma, M) = H^1(\partial X_\Gamma, \mathfrak{M}) \quad \text{et} \quad H^1(\Gamma, M) = H^1(X_\Gamma, \mathfrak{M})\ .$$

La dualité de Poincaré définit sur $H^1(\partial X_\Gamma, \mathfrak{M})$ une forme bilinéaire non dégénérée qui est alternée (resp. symétrique) si la forme donnée sur M est symétrique (resp. alternée). La formule $(**)$ du n° précédent est encore valable, et l'on en déduit comme dans la démonstration du lemme 11 que l'image de $\rho: H^1(X_\Gamma, \mathfrak{M}) \to H^1(\partial X_\Gamma, \mathfrak{M})$ est son propre orthogonal dans $H^1(\partial X_\Gamma, \mathfrak{M})$, d'où le résultat cherché.

Passons au *cas général.* Choisissons un sous-groupe distingué Γ_1 de Γ qui soit *net* et *d'indice fini.* Posons $\mathfrak{g} = \Gamma/\Gamma_1$. On sait que l'homomorphisme de restriction

$$H^s(\Gamma, M) \longrightarrow H^s(\Gamma_1, M)$$

identifie le premier espace au sous-espace du second formé des éléments invariants par $\mathfrak{g}$. On a donc

(a) $H^1(\Gamma, M) = H^0(\mathfrak{g}, H^1(\Gamma_1, M))$.

Soit d'autre part $M^{\mathbf{P}}$ l'ensemble des applications de $\mathbf{P}$ dans M, et faisons opérer Γ sur $M^{\mathbf{P}}$ par transport de structure, i.e. par

$$(\gamma \cdot f)(D) = \gamma \cdot f(\gamma^{-1}D) \qquad \text{si } \gamma \in \Gamma,\ f \in M^{\mathbf{P}} \text{ et } D \in \mathbf{P}\ .$$

Si l'on note $\mathbf{P}(i)$, $i \in \mathbf{P}/\Gamma$, les orbites de Γ dans $\mathbf{P}$, le Γ-module $M^{\mathbf{P}}$ est produit des Γ-modules $M^{\mathbf{P}(i)}$; de plus, le *lemme de Shapiro* montre que

$$H^s(\Gamma, M^{\mathbf{P}(i)}) = H^s(\Gamma_i, M)\ .$$

On a donc

$$H^1(\Gamma, M^{\mathbf{P}}) = \coprod_i H^1(\Gamma, M^{\mathbf{P}(i)}) = \coprod_i H^1(\Gamma_i, M) = U^1(\Gamma, M)$$

et l'homomorphisme ρ correspond simplement à l'injection diagonale de M dans $M^{\mathbf{P}}$. On en déduit, comme ci-dessus

(b) $U^1(\Gamma, M) = H^1(\Gamma, M^{\mathbf{P}}) = H^0(\mathfrak{g}, H^1(\Gamma_1, M^{\mathbf{P}})) = H^0(\mathfrak{g}, U^1(\Gamma_1, M))$.

Si ρ_1 désigne l'homomorphisme de restriction $H^1(\Gamma_1, M) \to U^1(\Gamma_1, M)$, il résulte de (a) et (b) que l'on a:

(c) $\operatorname{Im}(\rho) = H^0(\mathfrak{g}, \operatorname{Im}(\rho_1))$.

Mais, d'après ce qui a été vu plus haut, $\operatorname{Im}(\rho_1)$ est son propre orthogonal dans $U^1(\Gamma_1, M)$ vis-à-vis d'une certaine forme bilinéaire non dégénérée B; le caractère canonique de B, joint au fait que $\mathfrak{g}$ *conserve l'orientation* de X_{Γ_1}, montre que B est *invariante par* $\mathfrak{g}$. Le th. 8 résulte alors du lemme élémentaire suivant:

LEMME 12. *Soit E un k-espace vectoriel de dimension finie muni d'une forme bilinéaire non dégénérée B; soit F un sous-espace de E égal à son orthogonal dans E. Soit $\mathfrak{g}$ un groupe fini opérant linéairement sur E, laissant B invariante et laissant stable F. Alors la restriction de B à $H^0(\mathfrak{g}, E)$ est non dégénérée et $H^0(\mathfrak{g}, F)$ est son propre orthogonal dans $H^0(\mathfrak{g}, E)$; on a*

$$\operatorname{rg.} H^0(\mathfrak{g}, F) = 1/2 \operatorname{rg.} H^0(\mathfrak{g}, E) .$$

La démonstration est immédiate.

Remarques

(1) L'hypothèse que k est de caractéristique 0 peut être remplacée par celle que l'ordre de $\mathfrak{g}$ est inversible dans k.

(2) Soit M un $k[\Gamma]$-module de rang fini sur k, et soit M' son dual. On peut montrer que $H^s(\Gamma, M')$ est dual de $H^{2-s}(\Gamma, M^{\mathrm{P}}/M)$; en d'autres termes, le Γ-module k^{P}/k est un *module dualisant* pour Γ.

(3) Posons $\Gamma_i^+ = \Gamma \cap U_{D_i}$ et $\mu_i = \Gamma_i/\Gamma_i^+$; l'homomorphisme ω du n° 3.2 identifie μ_i à un sous-groupe du groupe μ des racines de l'unité de K (cf. démonstration du lemme 7). On a

$$H^s(\Gamma_i, M) = H^0(\mu_i, H^s(\Gamma_i^+, M)) ,$$

ce qui ramène la détermination de $U^1(\Gamma, M)$ à celle des $H^1(\Gamma_i^+, M)$ et des actions correspondantes des μ_i. On vérifie facilement que, si Γ est *sans torsion*, ou si K est distinct de $\mathbf{Q}(\sqrt{-1})$ et de $\mathbf{Q}(\sqrt{-3})$, on a $\mu_i \subset \{\pm 1\}$ et μ_i opère trivialement sur Γ_i^+ (autrement dit Γ_i est abélien).

Donnons maintenant quelques applications du théorème 8:

COROLLAIRE 1. *Si les Γ_i sont sans torsion, on a*

$$\operatorname{rg.} \operatorname{Im}(\rho) = \textstyle\sum_i \operatorname{rg.} H^0(\Gamma_i, M) .$$

Si Γ_i est sans torsion, il est isomorphe à $\mathbf{Z} \times \mathbf{Z}$ et sa caractéristique d'Euler-Poincaré est nulle. D'où:

$$\operatorname{rg.} H^1(\Gamma_i, M) = \operatorname{rg.} H^0(\Gamma_i, M) + \operatorname{rg.} H^2(\Gamma_i, M) .$$

Mais, puisque M est isomorphe à son dual, la dualité de Poincaré montre que $H^0(\Gamma_i, M)$ et $H^2(\Gamma_i, M)$ ont même rang. On a donc

$$\mathrm{rg.}\, H^1(\Gamma_i, M) = 2\, \mathrm{rg.}\, H^0(\Gamma_i, M) ,$$

d'où le corollaire, en vertu du théorème 8.

COROLLAIRE 2. *Soit* $k = \mathbf{C}$, *et soit* Ad *la représentation adjointe de* Γ *dans l'algèbre de Lie de* G_C. *On a*

$$\mathrm{rg.}\, H^1(\Gamma, \mathrm{Ad}) = \mathrm{rg.}\, \mathrm{Im}\,(\rho) = 1/2 \sum_i \mathrm{rg.}\, H^1(\Gamma_i, \mathrm{Ad}) .$$

Si de plus les Γ_i *sont sans torsion, on a* $\mathrm{rg.}\, H^1(\Gamma, \mathrm{Ad}) = h_\Gamma$, *avec* $h_\Gamma = \mathrm{Card}\,(\mathbf{P}/\Gamma)$.

D'après Garland et Raghunathan ([10], (8.2)), l'homomorphisme ρ est *injectif*. On a donc $\mathrm{rg.}\, H^1(\Gamma, \mathrm{Ad}) = \mathrm{rg.}\, \mathrm{Im}\,(\rho)$, ce qui démontre la première égalité; la seconde résulte du th. 8 et la dernière du cor. 1, compte tenu de ce que $\mathrm{rg.}\, H^0(\Gamma_i, \mathrm{Ad}) = 1$ si Γ_i est sans torsion (ou, plus généralement, si μ_i est contenu dans $\{\pm 1\}$).

COROLLAIRE 3. *Soit* $\alpha\colon \coprod_i \Gamma_i^{ab} \to \Gamma^{ab}$ *l'homomorphisme induit par les injections* $\Gamma_i \to \Gamma$. *Le rang du groupe* $\mathrm{Im}\,(\alpha)$ *est égal au nombre d'éléments* $i \in \mathbf{P}/\Gamma$ *tels que* $\mu_i \subset \{\pm 1\}$; *en particulier, il est égal à* h_Γ *si* Γ *est sans torsion, ou si* K *est distinct de* $\mathbf{Q}(\sqrt{-1})$ *et de* $\mathbf{Q}(\sqrt{-3})$.

(Lorsque Γ est *net*, on retrouve le théorème 7.)

On applique le th. 8 au module $M = k$, avec action triviale de Γ et l'on utilise le fait que $H^1(\Gamma_i, k) = \mathrm{Hom}\,(\Gamma_i^{ab}, k)$ est de rang 2 si μ_i est contenu dans $\{\pm 1\}$, et de rang 0 sinon.

3.6. *Le groupe* $\mathbf{SL}_2(A)^{ab}$ (*cas quadratique imaginaire*).

On conserve les notations et hypothèses des n$^{\text{os}}$ 3.4 et 3.5; en particulier, on a $K = \mathbf{Q}(\sqrt{-d})$, où d est un entier $\geqq 1$; on suppose d sans facteurs carrés. On note $c(A)$ le groupe des classes d'idéaux de A, et h son ordre. On pose

$$\Gamma = \Gamma_A = \mathbf{SL}_2(A) .$$

On s'intéresse à la structure du groupe Γ^{ab}, et plus précisément, à la détermination du noyau de $\alpha\colon \coprod \Gamma_i^{ab} \to \Gamma^{ab}$. Comme les cas $d = 1$ et $d = 3$ sont bien connus (cf. Cohn [9] et Swan [23]), et quelque peu différents des autres (cf. cor. 3 au th. 8), on les écarte; on suppose donc dans tout ce qui suit que K est *distinct de* $\mathbf{Q}(\sqrt{-1})$ *et de* $\mathbf{Q}(\sqrt{-3})$. Cela entraîne que chaque Γ_i est produit de $\{\pm 1\}$ par $\Gamma_i^+ = \Gamma \cap U_{D_i}$. Nous poserons

$$U = \coprod_{i \in \mathbf{P}/\Gamma} \Gamma_i^+ ,$$

et tout revient à déterminer le noyau de $\alpha\colon U \to \Gamma^{ab}$.

Nous aurons besoin pour cela de quelques définitions préliminaires.

Structure de U.

On a vu plus haut (n° 3.2, démonstration du lemme 6) que les éléments i de $\mathbf{P}/\Gamma$ correspondent bijectivement aux *classes d'idéaux* de A. Plus précisément, soit $c \in c(A)$ une telle classe. Il existe un sous-module E de rang 1 de $L = A^2$ qui est facteur direct dans L, et dont la classe (au sens de Bourbaki, *Alg. Comm.*, chap. VII, § 4, n° 7) est égale à c. On lui associe le sous-groupe unipotent Γ_c^+ de Γ formé des éléments dont la restriction à E est l'identité. On a donc $\Gamma_c^+ = \mathrm{Hom}_A(L/E, E)$. Mais d'autre part le produit extérieur $(a, b) \mapsto a \wedge b$ définit un accouplement

$$E \otimes_A L/E \longrightarrow \bigwedge^2(L) = A ,$$

d'où un isomorphisme de E sur le module dual $(L/E)^{-1}$ de L/E. On obtient donc un isomorphisme canonique

$$\Gamma_c^+ = \mathrm{Hom}_A(L/E, E) = (L/E)^{-1} \otimes E = E \otimes E = E^{\otimes 2} .$$

On observera en outre que, si E et F sont des A-modules projectifs de rang 1 de même classe c, il n'existe que deux isomorphismes φ et $-\varphi$ de E sur F, et ces deux isomorphismes définissent *le même* isomorphisme φ^2 de $E^{\otimes 2}$ sur $F^{\otimes 2}$. Le module $E^{\otimes 2}$ associé à c est donc déterminé à isomorphisme unique près; il est licite de le noter $c^{\otimes 2}$. On a ainsi:

$$\Gamma_c^+ = c^{\otimes 2} \quad \text{et} \quad U = \coprod_{c \in c(A)} c^{\otimes 2} .$$

Si l'on choisit des idéaux fractionnaires $\mathfrak{a}(c)$ représentant les différentes classes c, on peut identifier $c^{\otimes 2}$ au *carré* $\mathfrak{a}(c)^2$ de l'idéal $\mathfrak{a}(c)$ et l'on a

$$U = \coprod_{c \in c(A)} \mathfrak{a}(c)^2 .$$

Conjugaison complexe.

L'application $a \mapsto \bar{a}$ définit, par transport de structure, des automorphismes de Γ, Γ^{ab}, $c(A)$ et U, que nous noterons par la même lettre σ.

Action de σ sur $c(A)$ et sur U.

Tout d'abord, si $\mathfrak{a}$ est un idéal fractionnaire de K, le produit $\mathfrak{a}\cdot\bar{\mathfrak{a}}$ est l'idéal principal engendré par la *norme* $N(\mathfrak{a})$ de $\mathfrak{a}$; on en conclut que la classe de $\bar{\mathfrak{a}}$ est *l'inverse* de la classe de $\mathfrak{a}$, autrement dit que l'on a

$$\sigma(c) = c^{-1} \qquad \text{pour tout } c \in c(A) .$$

Supposons que $\sigma(c) = c$, i.e. que $c^2 = 1$, et soit $\mathfrak{a}$ un idéal de classe c. Puisque $\mathfrak{a}$ et $\bar{\mathfrak{a}}$ sont dans la même classe, il existe $\lambda \in K^*$ tel que $\bar{\mathfrak{a}} = \lambda\mathfrak{a}$. On a alors $\lambda\bar{\lambda} = \pm 1$, d'où $\lambda\bar{\lambda} = 1$ puisque $\lambda\bar{\lambda}$ est > 0; le "théorème 90" montre qu'il existe $\mu \in K^*$ tel que $\lambda = \mu^{-1}\bar{\mu}$ et l'idéal $\mathfrak{a}' = \mu^{-1}\mathfrak{a}$ vérifie la relation $\bar{\mathfrak{a}}' = \mathfrak{a}'$. Si r est le nombre d'éléments $c \in c(A)$ tels que $c^2 = 1$, on en conclut que l'on peut trouver des représentants

$$\mathfrak{a}_1, \cdots, \mathfrak{a}_r, \mathfrak{b}_1, \cdots, \mathfrak{b}_s, \mathfrak{c}_1, \cdots, \mathfrak{c}_s \qquad (r + 2s = h)$$

des éléments de $c(A)$ tels que $\bar{\mathfrak{a}}_i = \mathfrak{a}_i$ pour $1 \leqq i \leqq r$ et $\bar{\mathfrak{b}}_j = \mathfrak{c}_j$ pour $1 \leqq j \leqq s$. Le A-module U se décompose en $U = V \oplus W$, avec

$$V = \coprod_i \mathfrak{a}_i^2 \text{ et } W = \coprod_j (\mathfrak{b}_j^2 \oplus \mathfrak{c}_j^2) .$$

L'application σ est un *anti-automorphisme* de U, donné par:

$$\sigma(x) = \bar{x} \qquad \text{si } x \in \mathfrak{a}_i^2$$
$$\sigma(y, z) = (\bar{z}, \bar{y}) \qquad \text{si } (y, z) \in \mathfrak{b}_j^2 \oplus \mathfrak{c}_j^2 .$$

Nous noterons U_{R}, V_{R} et W_{R} l'ensemble des éléments de U, V et W invariants par σ, et nous noterons U'_{R} l'ensemble des $u + \sigma(u)$, où u parcourt U. On a:

$$U_{\mathrm{R}} = V_{\mathrm{R}} \oplus W_{\mathrm{R}} , \quad U'_{\mathrm{R}} = 2V_{\mathrm{R}} \oplus W_{\mathrm{R}}$$

et

$$U_{\mathrm{R}} \supset U'_{\mathrm{R}} \supset 2U_{\mathrm{R}} .$$

Les groupes U_{R}, U'_{R}, V_{R} et W_{R} sont des groupes abéliens libres de rang h, h, r et $2s$ respectivement. Leur relation avec le noyau de α est donnée par le théorème suivant:

THÉORÈME 9. *Le noyau N de l'homomorphisme α: $U \to \mathbf{SL}_2(A)^{ab}$ vérifie les inclusions $6U'_{\mathrm{R}} \subset N \subset U_{\mathrm{R}}$.*

(En particulier, N est compris entre U_{R} et $12U_{\mathrm{R}}$, autrement dit N coincide avec U_{R} à un groupe d'exposant 12 près.)

COROLLAIRE 1. *Soit x un produit d'éléments unipotents de $\mathbf{SL}_2(A)$, et soit $\bar{x} = \sigma(x)$ son image par la conjugaison complexe. L'élément $(x.\bar{x})^6$ appartient au groupe dérivé de $\mathbf{SL}_2(A)$.*

Cela exprime le fait que $6U'_{\mathrm{R}}$ est contenu dans N.

COROLLAIRE 2. *Soit $u \in U$. Pour que $\alpha(u)$ soit un élément de torsion de $\mathbf{SL}_2(A)^{ab}$, il faut et il suffit que u appartienne à U_{R}.*

Si $u \in U_{\mathrm{R}}$, on a $2u \in U'_{\mathrm{R}}$ et le théorème montre que $\alpha(u)^{12} = 1$. D'autre part, si u n'appartient pas à U_{R}, il en est de même de nu pour tout $n \geqq 1$, et le théorème montre que $\alpha(u)$ est d'ordre infini.

(En particulier, si $a \in A$ n'appartient pas à $\mathbf{Z}$, l'image de $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ dans $\mathbf{SL}_2(A)^{ab}$ est *d'ordre infini*, comme l'avait observé Swan ([23], n° 17) dans divers cas particuliers.)

Démonstration du théorème 9.

Observons d'abord que l'inclusion $N \subset U_{\mathrm{R}}$ est une *conséquence* de l'inclusion $6U'_{\mathrm{R}} \subset N$. En effet, supposons que l'on ait $6U'_{\mathrm{R}} \subset N$ et qu'il existe un élément $u \in N$ non contenu dans U_{R}; le sous-groupe de N engendré par $6U'_{\mathrm{R}}$

et u serait alors de rang $h+1$, ce qui contredirait le cor. 3 au th. 8.

Reste à prouver que $6U'_{\mathrm{R}}$ est contenu dans N. Cela va résulter de la proposition suivante, qui sera démontrée au n° 3.7:

PROPOSITION 6. *Soit* $\mathfrak{q}$ *un idéal fractionnaire de* K *et soit* $H(\mathfrak{q})$ *le sous-groupe de* $\mathbf{SL}_2(K)$ *formé des matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *telles que* $a \in A$, $b \in \mathfrak{q}$, $c \in \mathfrak{q}^{-1}$ *et* $d \in A$. *Soient* $t \in \mathfrak{q}$ *et* $t' = \bar{t}/N(\mathfrak{q})$; *on a* $t' \in \mathfrak{q}^{-1}$. *Posons*

$$x_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \quad et \quad y_t = \begin{pmatrix} 0 & 0 \\ -t' & 1 \end{pmatrix}.$$

L'élément $(x_t \cdot y_t)^6$ *appartient alors au groupe dérivé de* $H(\mathfrak{q})$.

(Le groupe $H(\mathfrak{q})$ est un sous-groupe arithmétique de G; c'est le stabilisateur du réseau $\mathfrak{m} \oplus \mathfrak{n}$, où $\mathfrak{m}$ et $\mathfrak{n}$ sont deux idéaux tels que $\mathfrak{m} \cdot \mathfrak{n}^{-1} = \mathfrak{q}$; c'est un groupe de même genre que $\mathbf{SL}_2(A)$. Lorsque la classe de $\mathfrak{q}$ est un *carré*, $H(\mathfrak{q})$ et $\mathbf{SL}_2(A)$ sont isomorphes; c'est le cas que nous allons utiliser.)

Montrons comment la proposition précédente entraîne l'inclusion $6U'_{\mathrm{R}} \subset N$. Soit $c \in c(A)$ et soit $u \in \Gamma_c^+$. Il faut prouver que l'image de $6\big(u + \sigma(u)\big)$ dans $\mathbf{SL}_2(A)^{ab}$ est triviale. Soit $\mathfrak{a}$ un idéal appartenant à la classe c; si l'on identifie Γ_c^+ à $\mathfrak{a}^2$ comme on l'a expliqué plus haut, u correspond à un certain élément t de $\mathfrak{a}^2$ et $\sigma(u)$ correspond à l'élément $\bar{t}$ de $\Gamma^+_{\sigma(c)} = \bar{\mathfrak{a}}^2$; mais, puisque $\mathfrak{a}^{-1} = N(\mathfrak{a})^{-1} \cdot \bar{\mathfrak{a}}$ est dans la même classe que $\bar{\mathfrak{a}}$, on peut aussi identifier $\Gamma^+_{\sigma(c)}$ à $\mathfrak{a}^{-2}$ et cela transforme $\sigma(u)$ en l'élément $t' = N(\mathfrak{a})^{-2} \cdot \bar{t}$ de $\mathfrak{a}^{-2}$. On va maintenant expliciter des éléments unipotents de $\mathbf{SL}_2(A)$ dont les classes de conjugaison sont u et $\sigma(u)$. Choisissons un isomorphisme

$$\theta \colon L \longrightarrow \mathfrak{a} \oplus \mathfrak{a}^{-1}$$

qui soit *de déterminant* 1, autrement dit tel que sa puissance extérieure seconde

$$\textstyle\bigwedge^2 \theta \colon A = \bigwedge^2 L \longrightarrow \bigwedge^2(\mathfrak{a} \oplus \mathfrak{a}^{-1}) = \mathfrak{a} \otimes \mathfrak{a}^{-1} = A$$

soit l'identité. Le groupe $\mathbf{SL}(\mathfrak{a} \oplus \mathfrak{a}^{-1})$ s'identifie de façon évidente au groupe $H(\mathfrak{q})$ de la prop. 6, avec $\mathfrak{q} = \mathfrak{a}^2$. En particulier, l'élément t de $\mathfrak{a}^2$ définit un élément unipotent $x_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ de $\mathbf{SL}(\mathfrak{a} \oplus \mathfrak{a}^{-1})$ et $\theta^{-1} x_t \theta$ est un *représentant* de u. De même, si l'on choisit un isomorphisme

$$\theta' \colon L \longrightarrow \mathfrak{a}^{-1} \oplus \mathfrak{a}$$

de déterminant 1, l'élément $\theta'^{-1}\begin{pmatrix} 1 & t' \\ 0 & 1 \end{pmatrix}\theta'$ est un représentant de $\sigma(u)$. Mais on peut prendre pour θ' le composé de θ et de l'isomorphisme

$$w \colon (x, y) \longmapsto (y, -x)$$

de $\mathfrak{a} \oplus \mathfrak{a}^{-1}$ sur $\mathfrak{a}^{-1} \oplus \mathfrak{a}$ (noter le signe "moins" qui est nécessaire pour que det $(w) = 1$). On a alors

$$\theta'^{-1}\begin{pmatrix}1 & t'\\0 & 1\end{pmatrix}\theta' = \theta^{-1}w^{-1}\begin{pmatrix}1 & t'\\0 & 1\end{pmatrix}w\theta = \theta^{-1}\begin{pmatrix}1 & 0\\-t' & 1\end{pmatrix}\theta\ .$$

Avec les notations de la prop. 6, ce qui précède montre que $\theta^{-1}x_t\theta$ est un représentant de u et $\theta^{-1}y_t\theta$ un représentant de $\sigma(u)$. D'où le résultat cherché puisque $(x_ty_t)^6$ appartient au groupe dérivé de $H(\mathfrak{q})$.

Remarques

(1) En utilisant une variante de la prop. 6, on peut démontrer le résultat suivant, plus précis que le cor. 2: si $u \in U_{\mathbf{R}}$, il existe des éléments x_i de $\mathbf{SL}_2(A)$, d'ordre 3 ou d'ordre 4, tels que $\alpha(u)$ soit égal à l'image du produit des x_i dans $\mathbf{SL}_2(A)^{ab}$.

(2) Signalons quelques résultats, obtenables par une méthode analogue à celle suivie ci-dessus, et qui précisent un peu l'inclusion $12U_{\mathbf{R}} \subset N$:

si $d \equiv 1 \pmod 3$, on a $4V_{\mathbf{R}} \subset N$
si $d \equiv 2 \pmod 4$,, $6V_{\mathbf{R}} \subset N$
si $d \equiv 3 \pmod 8$,, $3V_{\mathbf{R}} \subset N$.

En particulier, si $d \equiv 19 \pmod{24}$, on a $V_{\mathbf{R}} \subset N$, et l'élément $\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$ appartient au groupe dérivé de $\mathbf{SL}_2(A)$. Ainsi, pour $d = 19, 43, 67, 163$, où $h = 1$, on a $N = U_{\mathbf{R}} = V_{\mathbf{R}}$ et l'image de U dans $\mathbf{SL}_2(A)^{ab}$ est un groupe cyclique infini, engendré par l'image de $\begin{pmatrix}1 & \omega\\0 & 1\end{pmatrix}$, où $\omega = (1 + \sqrt{-d})/2$.

Par contre, si $d \equiv 15, 23 \pmod{24}$, l'image de $\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$ dans $\mathbf{SL}_2(A)^{ab}$ est d'ordre 12. Cela se voit en utilisant le fait que $\mathbf{SL}_2(\mathbf{Z}/4\mathbf{Z}) \times \mathbf{SL}_2(\mathbf{Z}/3\mathbf{Z})$ est quotient de $\mathbf{SL}_2(A)$ par un groupe de congruence convenable.

(3) Pour un certain nombre de valeurs de d, on dispose de résultats beaucoup plus précis que le th. 9. En effet, Bianchi ([6], voir aussi [27]) a déterminé un domaine fondamental de $\Gamma = \mathbf{SL}_2(A)$[7] dans l'espace hyperbolique; pour certaines valeurs de d, on peut en déduire une *présentation* de Γ par générateurs et relations, d'où *a fortiori* la structure de Γ^{ab} (et non pas seulement, comme ici, de la partie de Γ^{ab} engendrée par les éléments unipotents). Une méthode voisine a été utilisée récemment par Swan [23], qui donne un procédé général permettant de déterminer une présentation de Γ, et explicite le résultat pour $d = 2, 5, 6, 7, 11, 15, 19$ (ainsi que pour $d = 1$ et 3, que nous avons convenu d'exclure). D'autres valeurs de d ont été traitées par Mennicke (non publié), en particulier $d = 10$ qui est la plus petite valeur pour laquelle on ait rg. $\Gamma^{ab} > h$. Les méthodes de Swan et Mennicke sont topologi-

[7] En fait, Bianchi considère, non pas le groupe Γ, mais le groupe $\tilde{\Gamma}$ des automorphismes et anti-automorphismes du réseau A^2; on a $(\tilde{\Gamma} : \Gamma) = 4$ et l'on passe facilement d'une présentation de $\tilde{\Gamma}$ à une présentation de Γ.

ques; lorsque K est euclidien ($d = 1, 2, 3, 7, 11$), on dispose également d'une méthode algébrique, due à P. M. Cohn [9].

3.7. *Démonstration de la proposition* 6.

Elle utilise les trois lemmes suivants:

LEMME 13. *Soit* $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. *La matrice* $-x^6 = \begin{pmatrix} -1 & -6 \\ 0 & -1 \end{pmatrix}$ *appartient au groupe dérivé de* $\mathbf{SL}_2(\mathbf{Z})$.

Soit $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Posons

$$u = xwx^{-1}w^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ et } v = x^{-1}wxw^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} .$$

On constate alors que $uvu^{-1}v^{-1} = -x^6$, ce qui montre bien que $-x^6$ appartient au groupe dérivé de $\mathbf{SL}_2(\mathbf{Z})$ (et même au *second* groupe dérivé).

LEMME 14. *Soit p un nombre premier $\neq 2$ et soit $\Gamma_0(p)$ le sous-groupe de* $\mathbf{SL}_2(\mathbf{Z})$ *formé des matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *telles que* $c \equiv 0 \pmod p$. *Soient x et y les éléments de $\Gamma_0(p)$ définis par* $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 0 \\ -p & 1 \end{pmatrix}$. *L'élément* $(xy)^6$ *appartient au groupe dérivé de* $\Gamma_0(p)$.

Soit (x) le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ engendré par x. L'ensemble

$$(x)\backslash\mathbf{SL}_2(\mathbf{Z})/\Gamma_0(p)$$

des doubles classes de $\mathbf{SL}_2(\mathbf{Z})$ modulo $\Gamma_0(p)$ et (x) a deux éléments; on peut les représenter par 1 et $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On en conclut que l'image de x par le *transfert* $v\colon \mathbf{SL}_2(\mathbf{Z})^{ab} \to \Gamma_0(p)^{ab}$ est égale à $x.wx^pw^{-1} = xy$. D'autre part, on a $v(-1) = (-1)^{p+1} = 1$, puisque p est impair. D'où:

$$v(-x^6) = (xy)^6 .$$

D'après le lemme précédent, $-x^6$ appartient au groupe dérivé de $\mathbf{SL}_2(\mathbf{Z})$; il en résulte que $v(-x^6)$ est l'élément neutre de $\Gamma_0(p)^{ab}$; d'où le lemme.

Remarque. Si p est congru à -1 mod. 3 (resp. mod. 4, resp. mod. 12), l'exposant 6 du lemme précédent peut être remplacé par 2 (resp. par 3, resp. par 1).

LEMME 15. *Soit $\mathfrak{q}$ un idéal fractionnaire de K. En tant que groupe abélien, $\mathfrak{q}$ est engendré par les éléments $t \in \mathfrak{q}$ jouissant de la propriété suivante*:

(P)—*L'entier $t\bar{t}/N(\mathfrak{q})$ est un nombre premier* $\neq 2$.

Il suffit de montrer que, pour tout nombre premier l, et tout élément non nul ν de $\mathfrak{q}/l\mathfrak{q}$, il existe $t \in \mathfrak{q}$, tel que t jouisse de la propriété (P) et que l'image de t dans $\mathfrak{q}/l\mathfrak{q}$ soit égale à ν.

Soit n un représentant de ν dans $\mathfrak{q}$. Soit Ω l'ensemble des idéaux premiers $\mathfrak{p}$ de A dont la classe mod. l est égale à celle de $n\mathfrak{q}^{-1}$; d'après le théorème de la progression arithmétique, la *densité* de Ω est > 0. On peut donc trouver un élément $\mathfrak{p}$ de Ω qui soit de degré 1, et dont la norme p soit $\neq 2$. Le fait que $\mathfrak{p}$ appartienne à Ω signifie qu'il existe un élément z de K^*, congru à 1 mod. l (multiplicativement), tel que $\mathfrak{p} = zn\mathfrak{q}^{-1}$. L'élément $t = zn$ répond alors à la question: on a $t \in \mathfrak{q}$, l'image de t dans $\mathfrak{q}/l\mathfrak{q}$ est la même que celle de n, et $t\bar{t}/N(\mathfrak{q}) = p$ est un nombre premier $\neq 2$.

Démonstration de la proposition 6.

Il s'agit de montrer que, si $t \in \mathfrak{q}$, $t' = \bar{t}/N(\mathfrak{q})$, et si $x_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $y_t = \begin{pmatrix} 1 & 0 \\ -t' & 1 \end{pmatrix}$, l'élément $(x_t y_t)^6$ a une image triviale dans $H(\mathfrak{q})^{ab}$.

Soit $a(t)$ cette image. L'application $t \mapsto a(t)$ est un homomorphisme de $\mathfrak{q}$ dans $H(\mathfrak{q})^{ab}$. Vu le lemme 15, il suffit donc de prouver que $a(t) = 1$ lorsque $t\bar{t}/N(\mathfrak{q})$ est égal à un nombre premier $p \neq 2$. Supposons que ce soit le cas. Soit φ l'homomorphisme de $\Gamma_0(p)$ dans $\mathbf{SL}_2(K)$ défini par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & bt \\ ct^{-1} & d \end{pmatrix}.$$

L'image de φ est *contenue dans* $H(\mathfrak{q})$. En effet, puisque b appartient à $\mathbf{Z}$, on a $bt \in \mathfrak{q}$; d'autre part, puisque c appartient à $p\mathbf{Z}$, on a $ct^{-1} \in pt^{-1}A$, et comme $pt^{-1} = \bar{t}.N(\mathfrak{q})^{-1} = t'$ appartient à $\mathfrak{q}^{-1}$, on a bien $ct^{-1} \in \mathfrak{q}^{-1}$.

De plus, si $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $y = \begin{pmatrix} 1 & 0 \\ -p & 1 \end{pmatrix}$, on a $\varphi(x) = x_t$, $\varphi(y) = y_t$. Mais, d'après le lemme 14, $(xy)^6$ appartient au groupe dérivé de $\Gamma_0(p)$; son image par φ, qui est $(x_t y_t)^6$, appartient donc au groupe dérivé $H(\mathfrak{q})$, ce qui achève la démonstration.

Appendice

Adjonction de bords aux espaces symétriques de rang 1

Notations (celles des §§ 1, 2, 3 ne s'appliquent plus).

Le lettre G désigne un groupe algébrique linéaire *simple* sur $\mathbf{R}$, *de* $\mathbf{R}$-*rang égal à* 1 (cf. [7], n° 11.3); on note également G l'ensemble de ses points réels et l'on fait une convention analogue pour les autres groupes algébriques définis ci-dessous.

On note X l'*espace symétrique* attaché à G. On fait opérer G à droite sur X. L'action de G est transitive et les stabilisateurs des points de X sont les sous-groupes compacts maximaux de G. Si K est un tel sous-groupe, on note (K) le point de X de stabilisateur K.

On note bX la *frontière de Satake* de X. C'est un espace homogène de G. Si $D \in bX$, le stabilisateur Q_D de D est un sous-groupe parabolique minimal de G; son radical unipotent est noté N_D. Le quotient Q_D/N_D contient un unique tore déployé de rang 1; son image réciproque B_D dans Q_D est un sous-groupe trigonalisable maximal de G. Le point D est déterminé de manière unique par N_D, B_D ou Q_D; on pourrait donc, par exemple, *définir* bX comme l'espace homogène des sous-groupes paraboliques minimaux de G.

Adjonction d'un bord correspondant à un point frontière de X.

Soit $D \in bX$. Notons Y_D l'ensemble des sous-tores déployés de rang 1 de Q_D (ou de B_D, cela revient au même), et soit X_D *l'ensemble somme de X et de Y_D*. Nous allons munir X_D d'une structure de *variété à bord d'intérieur X et de bord Y_D*.

Soit K un sous-groupe compact maximal de G. On vérifie facilement qu'il existe un unique élément S_K de Y_D qui soit stable par l'involution de Cartan définie par K. Si A_K désigne la composante neutre de S_K (pour la topologie usuelle), on a la *décomposition d'Iwasawa* $G = K.A_K.N_D$, cf. [7], n° 11.18. On identifie A_K au groupe $\mathbf{R}_+^*$ des nombres réels > 0 au moyen de la *racine positive* de S_K, pour la relation d'ordre associée à N_D; si $t \in \mathbf{R}_+^*$, on note t_K l'élément correspondant de A_K (l'ensemble des $(K).t_K$, $0 < t \leqq 1$, est la demi-géodésique de X issue de (K) et tendant vers le point frontière D). Soit maintenant

$$f_K\colon \mathbf{R}_+ \times N_D \longrightarrow X_D$$

l'application définie par:

$$\begin{aligned} f_K(t, n) &= (K).t_K.n \in X && \text{si } t > 0,\ n \in N_D \\ f_K(t, n) &= n^{-1}.S_K.n \in Y_D && \text{si } t = 0,\ n \in N_D\,. \end{aligned}$$

C'est une *bijection*.

Soit K' un autre sous-groupe compact maximal de G, et soient $\theta \in \mathbf{R}_+^*$, $\nu \in N_D$ tels que $(K') = (K).\theta_K.\nu$. Posons:

$$\varphi(t, n) = (\theta t, \nu n) \qquad \text{si } (t, n) \in \mathbf{R}_+ \times N_D.$$

Un calcul immédiat montre que le diagramme

$$\begin{tikzcd} \mathbf{R}_+ \times N_D \arrow[d, "\varphi"'] \arrow[dr, "f_{K'}"] & \\ & X_D \\ \mathbf{R}_+ \times N_D \arrow[ur, "f_K"'] & \end{tikzcd}$$

est commutatif. Mais φ respecte la structure de variété à bord de $\mathbf{R}_+ \times N_D$, produit de celle de $\mathbf{R}_+$ (de bord $\{0\}$) par celle de N_D (de bord vide). On en conclut qu'il existe sur X_D une structure de *variété à bord analytique réelle* et une seule telle que les bijections f_K soient des *isomorphismes*; c'est la structure que nous voulions définir; son bord est Y_D.

[Il y a peut-être intérêt à changer la structure analytique réelle de X_D le long de Y_D en prenant pour coordonnée locale "normale", non t_K comme nous l'avons fait, mais une puissance $(t_K)^\lambda$ de t_K, où λ est un nombre réel > 0 convenable. Cela peut avoir de l'importance pour l'étude de X_D et de ses quotients du point de vue de la géométrie différentielle.]

On notera que le groupe Q_D opère sur X_D (par transport de structure). Le stabilisateur dans Q_D d'un élément S du bord Y_D est le *centralisateur* $Z(S)$ de S dans G; on a $Q_D = Z(S).N_D$ et $Z(S) \cap B_D = S$. D'autre part, Y_D est un *espace homogène principal* de N_D.

Adjonction de plusieurs bords.

Soit P une partie *dénombrable* de bX, et soit $X(P)$ l'ensemble somme de X et des Y_D pour $D \in P$. Si $D \in P$, X_D s'identifie à un sous-ensemble de $X(P)$. Il existe sur $X(P)$ une structure de variété à bord et une seule telle que les X_D (munis des structures définies ci-dessus) en soient des sous-variétés ouvertes. On l'obtient simplement en *recollant* les X_D, $D \in P$, suivant leur intersection commune X; le fait que $X(P)$ soit *séparée* résulte de [7], 12.6.

Le bord de $X(P)$ est somme disjointe des Y_D, $D \in P$. La variété $X(P)$ est *dénombrable à l'infini*, du fait que P est supposé dénombrable (sinon, on obtient une variété non paracompacte); elle est *contractile* puisque son intérieur l'est.

Le caractère "intrinsèque" de $X(P)$ montre que tout automorphisme de l'espace de Riemann X qui laisse P invariant se prolonge en un automorphisme de la variété à bord $X(P)$.

Action d'un groupe discret.

Soit Γ un sous-groupe *discret* de G. Soit P l'ensemble des *pointes* de Γ, autrement dit l'ensemble des $D \in bX$ tels que $N_D/(\Gamma \cap N_D)$ soit compact. L'ensemble P est dénombrable et invariant par Γ. Le groupe Γ opère donc sur la variété à bord $X(P)$.

THÉORÈME. *Supposons que* Γ *soit arithmétique* (cf. Borel [7], § 17). *Le groupe* Γ *opère alors proprement sur l'espace* $X(P)$ *et le quotient* $X(P)/\Gamma$ *est compact.*

Ce théorème n'est qu'une reformulation, dans un langage un peu différent, de résultats établis par Borel dans [7], *loc. cit.* On notera que, d'après Garland-Raghunathan [10], on peut remplacer l'hypothèse que Γ est arithmétique par celle que G/Γ est *de volume fini.*

COROLLAIRE. *Supposons en outre que* Γ *soit sans torsion. Alors* Γ *opère librement sur* $X(P)$ *et le quotient* $X(P)/\Gamma$ *est une variété à bord compacte*;

son bord est $(\coprod_{D\in P} Y_D)/\Gamma$ *et son intérieur est* X/Γ.

Si l'on choisit des représentants $D_i \in P$ des éléments de P/Γ, le bord de $X(P)/\Gamma$ est réunion disjointe des $E_i = Y_{D_i}/(Q_{D_i} \cap \Gamma)$; lorsqu'en outre Γ est net, on a $Q_{D_i} \cap \Gamma = N_{D_i} \cap \Gamma$ et E_i a une structure naturelle de "nilvariété". On retrouve l'énoncé de Borel [7], 17.10 (dans le cas particulier du rang réel 1).

COLLÈGE DE FRANCE

BIBLIOGRAPHIE

[1] E. ARTIN et J. TATE, Class Field Theory, Benjamin, New York, 1967.
[2] H. BASS, *K-theory and stable algebra*, Publ. Math. I.H.E.S. **22** (1964), 5-60.
[3] ———, M. LAZARD et J-P. SERRE, *Sous-groupes d'indice fini dans* $\mathbf{SL}(n, \mathbf{Z})$, Bull. Amer. Math. Soc. **70** (1964), 385-392.
[4] ———, J. MILNOR et J-P. SERRE, *Solution of the congruence subgroup problem for* $\mathbf{SL}_n (n \geqq 3)$ *and* $\mathbf{Sp}_{2n} (n \geqq 2)$, Publ. Math. I.H.E.S. **33** (1967), 59-137.
[5] H. BEHR, *Über die endliche Definierbarkeit verallgemeinerter Einheitengruppen*, II, Invent. math. **4** (1967), 265-274.
[6] L. BIANCHI, *Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari*, Math. Ann. **40** (1892), 332-412 [Opere Matematiche, Vol. 1, pt. 1, p. 270-373].
[7] A. BOREL, Introduction aux groupes arithmétiques, Hermann, Paris, 1969.
[8] J. CASSELS et A. FRÖHLICH, Algebraic Number Theory, Acad. Press, 1967.
[9] P. M. COHN, *A presentation of* $\mathbf{SL}_2$ *for Euclidean imaginary quadratic number fields*, Mathematika, **15** (1968), 156-163.
[10] H. GARLAND et M. S. RAGHUNATHAN, *Fundamental domains for lattices in (R-) rank one semi-simple Lie groups*, Ann. of Math. **92** (1970), 279-326.
[11] G. HARDER, *Minkowskische Reduktionstheorie über Funktionenkörpern*, Invent. math. **7** (1969), 33-54.
[12] Y. IHARA, *On discrete subgroups of the two by two projective linear group over* $\mathfrak{p}$*-adic fields*, J. Math. Soc. Japan **18** (1966), 219-235.
[13] F. KLEIN, *Zur Theorie der elliptischen Modulfunktionen*, Math. Ann. **17** (1880), 62-70 [Gesamm. Math. Abh., Bd. 3, p. 169-178].
[14] M. KNESER, *Normal subgroups of integral orthogonal groups*, Lecture Notes in Maths. 108 (*Algebraic K-theory and its geometric applications*), p. 67-71, Springer-Verlag, 1969.
[15] J. MENNICKE, *On Ihara's modular group*, Invent. math. **4** (1967), 202-228.
[16] C. MOORE, *Group extensions of p-adic and adelic linear groups*, Publ. Math. I.H.E.S. **35** (1969), 5-70.
[17] O. T. O'MEARA, *On the finite generation of linear groups over Hasse domains*, Journ. Crelle **217** (1965), 79-108.
[18] H. NAGAO, *On* $\mathbf{GL}(2, K[x])$, J. Inst. Poly. Osaka Univ. **10** (1959), 117-121.
[19] M. S. RAGHUNATHAN, *A note on quotients of real algebraic groups by arithmetic subgroups*, Invent. math. **4** (1968), 318-335.
[20] J-P. SERRE, *Groupes de congruence (d'après H. Bass, H. Matsumoto, J. Mennicke, J. Milnor, C. Moore)*, Séminaire BOURBAKI, 1966/67, exposé 330, Benjamin, New York, 1968.
[21] ———, *Cohomologie des groupes discrets*, C. R. Acad. Sci. Paris **268** (1969), 268-271.
[22] ———, *Arbres, amalgames et* $\mathbf{SL}_2$, Collège de France, 1968/69 (notes polycopiées, rédigées avec la collaboration de H. BASS), à paraître aux Lect. Notes.
[23] R. SWAN, *Generators and relations for certain special linear groups*, à paraître prochainement (voir aussi Bull. Amer. Math. Soc. **74** (1968), 576-581).

[24] A. WEIL, Adèles and algebraic groups (notes by M. DEMAZURE and T. ONO), Inst. Adv. Study, Princeton, 1961.
[25] ———, Basic Number Theory, Springer-Verlag, 1967.
[26] ———, "*Zeta-functions and Mellin transforms*," in Algebraic Geometry (Bombay Coll., 1968), p. 409-426, Oxford Univ. Press, 1969.
[27] W. WOODRUFF, The singular points of the fundamental domains for the groups of Bianchi, Dissert., Univ. Arizona, 1967.

(Received January 26, 1970)