UNIVERSITE KASDI MERBAH
OUARGLA
Faculte des Mathématiques et Sciences
de la Matière
Département de mathématiques

MASTER

Domaine : Mathématiques et informatique

Specialite : Mathématiques

Option : Algèbre et Géométrie

Par : Izdihar KERBOUSSA

Thème

Probléme de sous-groupe de congruence

Devant le jury composé de:

M.Amine BAHAYOU	M.A.Université KASDI Merbah-Ouargla	Président
M.Tayeb BEN MOUSSA	M.A.Université KASDI Merbah-Ouargla	Rapporteur
Yacine GUERBOUSSA	M.A.Université KASDI Merbah-Ouargla	Examinateur

Soutenu publiquement le: 2019/2020

Dédicace

Je dédie ce mémoire...

A mon très cher père ***KERBOUSSA Bachir***

Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être .

A ma très chère mère ***KENOUZ Rachida***

Aucune dédicace ne saurait êre assez éloquente pour exprimer ce que tu mérites pour tous les sacrifices que n'as cessé de me donner de puis ma naissance , durant mon enfance et même à l' âge adulte .

A mes frères ***Abd AL Madjid,Farouk,Amar,et M.said*** *.*

A ma chères sœurs ***Adila, Yamina,Dalila et Nadjah*** *.*

Pour ses soutiens moral et leurs conseils précieux tout au long de ma études.

Je n'oublie pas mes tantes,mes oncles et mes camarades

Manal,Inass,Ranai,Soria,Sara et Maumouna *.*

izdihar kerboussa

Remerciement

Avant toute chose, je tiens à remercier ***« Allah »*** *le tous puisant, pour nous avoir donné le courage,la volonté et la patience pour continuer mes études et pour réaliser ce travail.*

Je tiens à exprimer ma profonde gratitude à mon encadreur ***Mr. BEN MOUSSA Mohamed Tayeb*** *sous sa direction j'ai eu le plaisir de travailler grâce à ces conseils.*

Je tiens remercier,particulièrement ***Mr. GEURBOUSSA Yacin*** *,* ***Mr. BOUSSAID Mohamed****,* ***Mr.BAHAYOU Mohamed Amine*** *et tout les profs qui n'ont jamais cessé demesoutenir,pour l'aide qu'il m'aprocuréeet pourses précieux conseils.*

Je remercie ***Mr.CHNINI Amer****.*

Merci beaucoup à tous le promo de l'Algebre et géométrie

Zineb,Al Roumaissa,Hinda,Koutar,Iman,Ibtissam,Zineb Siham,Rbiha CHAKCHAK,BOUSSAID,ALILI et TOUNSSI *.*

les profs et mes enseignants de l'Université de Kasdi Merbah sans exception.

Table des matières

Notation

- $\varprojlim$: Limite Projective
- $(G_i; \varphi_{ij})$: Système Projective
- Hom : Homomorphisme
- $\circ(G)$: l'ordre de G
- CPS : Proprété de sous-groupe de congruence
- Γ : Sous-groupe de congruence
- Γ_m or $\Gamma(m)$: Sous-groupe de congruence prinsipal de néive m
- $\prod$: Le Produit
- $\sum$: La Somme
- $GL_n(R)$: $\{$ A$\in M_{nn}(R), detA \neq 0\}$
- $SL_n(R)$: $\{$ A $\in M_{nn}(R), det = 1\}$
- $SO_n(R)$: $\{$ A$\in M_{nn}(R), A^tA = I, detA = 1\}$

Introduction

Notre problème dans ce mémoire est destiné pour l'étude des groupe linéaire SL(n,Z), concernant une question récente connue par le problème de congruence (CSP). Historiquement la question qui précédé le(CSP)est le suivant : Soit $SL_n(A)$ ou A est l'anneau des entiers d'un corps K, avec K = Q et A = Z ou bien K est une extension quadratique de Q et A est un Z-module. Un résultat sur les groupes de Lie affirme que $SL_n(A)$ possède la propriété du sous-groupe normal pour n $\geqslant$ 3 c'est à dire que tout sous-groupe normal du réseau$SL_n(A)$ est : soit fini et contenu dans le centre, soit d'indice fini dans $SL_n(A)$. Ceci est faux dans le cas de $SL_2(A)$.

La question que l'on se pose alors est de savoir si tout sous-groupe d'indice fini de $SL_n(A)$ contient un sous-groupe de la forme :

$$Ker(SLn(A) \to SLn(A/I)) \text{ , ou I est un idéal de A}$$

Autrement dit,pour n$\geqslant$3 le groupe $SL_n(Z)$ et pour tout intègre k le sous groupe de congruence de niveau k est définie comme suit :

$$\Gamma(k) := g \in SL_n(Z) : g_{ij} - \delta_{ij} \equiv 0 mod k \forall i, j$$

Un sous-groupe H de Γ est un sous-groupe de congruence s'il contient un sous-groupe de congruence principal ,Ainsi il est évident que chaque sous-groupe de congruence de SL(3,Z)est un sous-groupe d' indice fini Il n' est pas de tout évident que l'inverse soit vrai. Beaucoup d'efforts a été fournit pour répondre à cette question sur tout par H.Baas, M.Lazard et J-P Serre (1964), et plus récent A.Lubotzky qui a donné des contre exemple très importants pour n= 2 .
La forme la plus simple du problème du sous-groupe de congruence pour $SL_n(Z)$ demande si chaque sous-groupe d'indice fini est une sous-groupe de congruence ?

On a traité ce problème dans ce mémoire que contient trois chapitres :

- 1^{er} Chapitre : les notions de base sur les groupes et le groupe libre .
- $2^{ème}$ Chapitre :les sous groupe de Congruences et les groupes pro fini .
- 3^{eme} Chapitre : sous groupe d' indice fini dans SL(n, Z) PAR H.Baas, M.Lazard et J-P.Serre .

En enfin de ce mémoire on a présenté quelques commentaires et des exemples En particulier le SL(2,Z) ..

Chapitre 1

Généralités sur les groupes

Dans cette section, nous rappelons quelques généralités sur les groupes et la notion de groupe libre .

1.1 Définitions de base

1.1.1 Groupes

Définition 1.1.1. *[1] Soit G un ensemble non vide et $*$ une loi de composition interne sur G définie par :*

$$(a,b) \mapsto a * b \ .$$

On dit que $(G, *)$,(ou par abus que G) est un groupe si

i) cette loi de composition est associative : quels que soient les élément x,y,z de G ,
$x * (y * z) = (x * y) * z$,

ii) G possède un élément neutre e pour cette loi : pour tout $x \in G$,
$e * x = x * e = x$,

iii) Tout élément $x \in G$ possède un symétrique (ou inverse) $x' \in G$:
$x * x' = x' * x = e$.

1.1.2 sous-groupes

Définition 1.1.2. *[1]Soit S une partie non vide d'un groupe G . On dit que S est un sous-groupe de G si :*

i) $a,b \in S \Rightarrow ab \in S$,

ii) $a \in S \Rightarrow a^{-1} \in S$.

Ces deux conditions sont équivalentes à l'unique axiom :

$$\text{a,b} \in \text{S} \Rightarrow ab^{-1} \in S.$$

Exemple 1.1.1. *sous-groupe de (Z,+)*
pour tout entier n∈Z, nZ={nx ; x∈Z } est un sous-groupe de Z et tout sous-groupe de Z est de cette forme

Remarque 1.1.1. *Il est clair l'intersection de sous-groupes est encore un sous-groupe.*
Dès lors,si $X \subseteq G$ *alors le plus petit sous-groupe de G contenant X est l'intersection de tous les sous-groupes de G contenant X. On dit que c'est le sous-groupe engendré par X et on le note* $\langle X \rangle$.
On vérifie facilement qu'on a :
$\langle\ X\ \rangle = \{x_1^{\varepsilon_1} \circ ... x_n^{\varepsilon_n} / n \in N_0; x_i \in X \text{ et } \varepsilon_i = \pm 1 \forall i \in \{1....n\}\}$
Si $G = \langle\ X\ \rangle$ *alors on dit que X engendre G ou de façon équivalente que X est une partie génératrice de G .*

1.1.3 Homomorphisme de groupes

Définition 1.1.3. *[2] Étant donné deux groupes (G , .) et (G′ , ∗) , un homomorphisme de groupes de G dans G′ est une application f : G → G′ telle que , quels que soient x et y dans G on ait :*

$$f(x \cdot y)=f(x) * f(y) .$$

Un morphismes de groupes est aussi appelé homomorphisme de groupes .
L'ensemble des morphismes d'un groupe G dans un groupe G' sera noté Hom(G , G′).
Un morphisme d'un groupe G dans lui-même est appelé endomorphisme de groupe .
L'ensemble des endomorphismes d'un groupe G sera noté End(G) .
Selon nos conventions général , dans la suit , les groupes G et G' seront notés multiplicativement , leurs élément unités étant respectivement e et e′ .

Proposition 1.1.1. *Tout f ∈ Hom (G , G′) vérifie les propriétés suivantes :*

1) $f(e) = e'$.

2) $f(x^{-1}) = (f(x))^{-1}$ *, quel que soit x dans G .*

3) $f(x'') = (f(x))''$ *, quels que soient x dans G et n dans Z .*

4) $H \leqslant G \Rightarrow f(H) \leqslant G'$.

5) $H' \leqslant G' \Rightarrow f^{-1}(H') \leqslant G$ *, où* $f^{-1}(H') = \{x \in G; f(x) \in H\}$.

Définition 1.1.4. *Un application f : G → G' est appelé épimorphisme de groupes , si :*

a) f ∈ Hom (G , G') et

b) quel que soit le groupe Γ *, on a la propriété :*

(u et v dans Hom (G' , Γ*) et* $u \circ f = v \circ f) \Rightarrow u = v$.

.

Proposition 1.1.2. *Pour un application f d'un groupe G dans un groupe G',on a :*

a) f morphisme injectif $\Leftrightarrow$ f monomorphisme

b) f morphisme surjectif $\Leftrightarrow$ f épimorphisme .

1.1.4 Action de groupe

Définition 1.1.5. *Soit G un groupe multiplicatif d'élément unité e , Soit E un ensemble non vide . On dit que G opère à gauche sur E , si E muni d'un loi de composition externe à gauche , à opérateurs dans G ; c'est-à-dire qu'il existe une application :*

$$G \quad E \to E$$

$$(g,x) \mapsto g.x$$

satisfaisant aux deux conditions suivantes :

1) $\forall\ x \in E\ ,\ e\ .\ x = x$

2) $\forall\ (\ g_1, g_2) \in G \quad G\ ,\ \forall\ x\ \ in\ E\ ,\ g_1 g_2 \cdot\ x = g_1 \cdot (\ g_2 \cdot x\ )\ .$

Exemple 1.1.2. *:*

Le groupe des isométries G(n) agit aussi sur R^n *par l'action .*

$$(f,x) \to f\ .\ x = f\ (x)$$

1.1.5 Le stabilisateur et l'orbite

Soit G un groupe opérant sur un ensemble E grâce à l'application :

$$\mathrm{G} \quad \mathrm{E} \to \mathrm{E}$$

$$(\mathrm{g}\ ,\ \mathrm{x}) \mapsto \mathrm{g}\ .\ \mathrm{x}.$$

A tout x $\in$ E , on associe

$$G_x = \{g \in G; g.x = x\}$$

On vérifie facilement que G_x est un sous-groupe de G .

G_x est formé des élément de G que "laissent fixé " l'élément x de E .

Définition 1.1.6. *E étant un G-ensemble , le sous-groupe G_x de G , associé à tout $x \in E$ et défini ci-dessus , est appelé sous-groupe d'isotropie de x ou stabilisateur de x (nous utiliserons généralement la seconde appellation et noté $Stab_G(x)$) .*

Définition 1.1.7. *E étant G-ensemble , la classe d'équivalence modulo ρ_G (est une relation d'équivalence dans E) d'un élément x de E est appelé orbite de x suivant G ou G-orbite de x .*

La G-orbite d'un élément x de E sera noté Ω_x :

$\Omega_x = \{g.x; g \in G\}$.

Définition 1.1.8. *Soient G un groupe et X un sous-ensemble non vide de G. Si tout élément de $G \setminus \{e\}$ s'écrit de façon unique sous la forme :*

$$x_1^{\varepsilon 1} \circ ..... \circ x_1^{\varepsilon n}. \tag{1.1}$$

Où n$\in N_0$;$x_i \in X$;$\varepsilon_1 = \pm 1 \forall i \in \{1...n\}$ et $x_i^{\varepsilon_i} \circ x_{i+1}^{\varepsilon^{i+1}} \neq e \ \forall i \in \{1...n-1\}$. alors X est une famille génératrice libre de G. De plus, si un élément de G\ { e} est écrit sous la forme (1.1) , on dit qu'il est écrit sous forme réduite .

Définition 1.1.9. *Si un groupe G possède une famille génératrice libre X alors G est un groupe libre. Dans ce cas, on dit que G est engendré librement par X.*

Remarque 1.1.2. *Soit G un groupe libre. Le cardinal d'une famille génératrice libre de G est appelé le rang de G.*

1.2 les groupes libres

1.2.1 construction d'un groupe libre

[2]soit X un ensemble non vide ; I étant un ensemble de même cardinal que X posons , X =$\{x_i\}_{i\in I}$
Considérons un ensemble disjoint de X et équipotent à X que nous noterons X^{-1} et dont nous écrirons les élément sous la forme x_i^{-1}, pour $i \in I$ (x_i^{-1} est ici, seulement, une notation qui sera commode par la suit) .

Définition 1.2.1. *On appelle mot sur $X \cup X^{-1}$ toute suite finie (ou ensemble fini ordonné)de n élément $X \cup X^{-1}$(n∈N)plusieurs élément de cet ensemble pouvant être égaux ; n s'appelle la longueur du mot.*

Par convention, il n'existe qu'un seul mot de longueur 0, que l'on notera 1 ,on l'appelle le mot vide, car il correspond à la partie vide de $X \cup X^{-1}$ un mot de longueur n$\geqslant$ 0 s'écrira sous la forme :

$$x_{i_1}^{\varepsilon_1}.....x_{i_n}^{\varepsilon_n}, \text{ ou } \varepsilon_j=\pm 1, \text{ pour tout j } (1\leqslant j\leqslant n) .$$

c'est-à-dire :

$$\varepsilon_j = 1 \text{ , si } x_{i_j}^{\varepsilon_j} \in X$$
$$\varepsilon_j = \text{-1, si } x_{i_j}^{\varepsilon_j} \in X^{-1}$$

On désignera par $X \cup X^{-1}$ l'ensemble des mots sur $X \cup X^{-1}$.

Exemple 1.2.1. *Si X = { x,y},x,yy^{-1},x^{-1}yyxy,x^{-1}xx^{-1},1 sont des mots sur $X \cup X^{-1}$.*

Égalité de deux mots : D' une façon général, dans $(X \cup X^{-1})$
On a $x_{i_1}^{\varepsilon_1}x_{i_2}^{\varepsilon_2}...x_{i_n}^{\varepsilon_n} = x_{j_1}^{\delta_1}x_{j_2}^{\delta_2}...x_{j_p}^{\delta_p} \Leftrightarrow n = p$
$x_{i_k}^{\varepsilon_k} = x_{j_k}^{\delta_k} \quad \forall k(1 \leqslant k \leqslant n)$

Dans l'exemple (1.2.1) tout les mots considérés sont distincte Notion de produit de mots :

Quel que soit w $\in (X \cup X^{-1})$, on pose lw=wl=w

Étant donné deux mots de longueurs non nulles dans $\in (X \cup X^{-1})$:

u= $x_{i_1}^{\varepsilon_1}...x_{i_n}^{\varepsilon_n}$, v= $x_{j_1}^{\delta_1}...x_{j_n}^{\delta_n}$

par définition, le produit uv est le mot : $x_{i_1}^{\varepsilon_1}...x_{i_n}^{\varepsilon_n}x_{j_1}^{\delta_1}...x_{j_n}^{\delta_n}$

donc long(uv)=long(u)+long(v) .

1.2.2 la propréite universelle d'un groupes libre

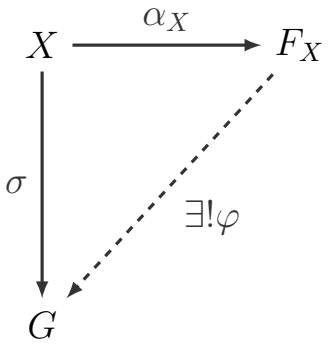
Théorème 1.2.1. *(propreté universelle)*

Soit un groupe $F \neq \{e\}$;soient X partie génératrice de F et α l'injection canonique de X dans F; alors F est libre sur X si et seulement si

quel que soient le groupe G et l' application $\sigma : X \to G$ il existe un unique morphisme $\varphi \in Hom(F, G)$ tel que $\varphi \circ \alpha = \sigma$.

Démonstration 1.2.1.

1) supposons $F = F_X$; α_X désignant l' injection canonique de X dans F_X, démontrons que le couple (F_X, α_X) vérifie la propriété énoncée.



dans le diagramme :

Ou G et σ sont donnés , définissons $\varphi : F_x \to G$ en posant pour tout u$\in F_X$, écrit sous la forme

$\varphi(u) = (\sigma(x_{i_1}))^{\varepsilon_1}(\sigma(x_{i_2}))^{\varepsilon_2}...(\sigma(x_{i_n}))^{\varepsilon_n}$ *et* $\varphi(1) = e$

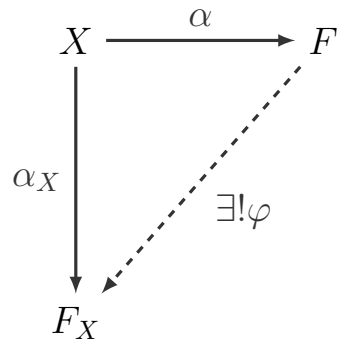
Ou e est l'élément neutre de G on définit ainsi un morphisme $\varphi \in Hom(F_X, G)$ tel

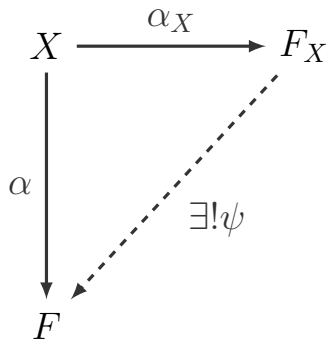
que $\varphi(x) = \sigma(x)$ *quel que soit* $x \in X$ *,donc* $\varphi \circ \alpha_X = \sigma$

De plus , si $\varphi' \in Hom(F_X, G)et\ \varphi' \circ \alpha_X = \sigma$*, alors pour tout* $u \in F_X$*, On a* $\varphi'(u) = \varphi(u)$ *; d'ou l'unicité de* φ

2) Réciproquement ,considérons un groupe F engendré par une partie non vide X, telles que si α *est l' injection canonique de X dans F , le couple (F,*α*) vérifie les condition énoncées dans le théorème*

compte tenu de l'hypothèse et de résultat précédent il existe $\varphi \in Hom(F, F_X)et$ $\psi \in Hom(F_X, F)tel$ *que les diagrammes suivants commutent :*





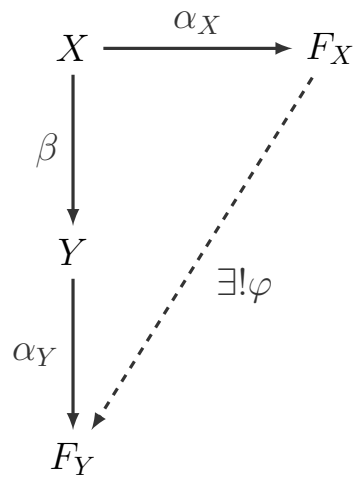
$\varphi \circ \alpha = \alpha_X$ $\qquad\qquad$ $\psi \circ \alpha_X = \alpha$

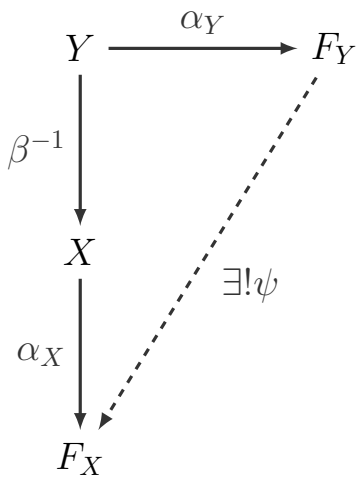
On en déduit que $\psi \circ \varphi \circ \alpha = \alpha$ *et* $\varphi \circ \psi \circ \alpha_X = \alpha_X$ *d'ou* $\psi \circ \varphi / X = id_X et$ $\varphi \circ \psi / X = id_X$ *,*$\varphi et \psi$ *sont des morphismes de groupe,F et* F_X*sont engendrés par X, par suite* $\psi \circ \varphi = id_F$ *et* $\varphi \circ \psi = id_{F_X}$ *d'ou* $F \backsimeq F_X et\ \psi(X) = X implique\ F$ *libre sur X .*

Corollaire 1.2.1. *Soient deux ensembles X et Y alors :*

X équipotent à $Y \Rightarrow F_X \backsimeq F_Y$ *.*

Démonstration 1.2.2. *La propriété étant vraie pour X=Y=0, On suppose X et Y non vides.Soit* β *une bijection de X sur Y considérons les diagrammes :*





D'aprés le théorème ,il existe un unique $\varphi \in Hom(F_{X,F_Y})$ *et un unique* $\psi \in Hom(F_X, F_Y)$*tels que :*

$\varphi \circ \alpha_X = \alpha_Y \circ \beta$ *et* $\psi \circ \alpha_X = \alpha_Y \circ \beta^{-1}$ *par suit ,*$\psi \circ \varphi \circ \alpha_X = \alpha_X$ *et* $\varphi \circ \psi \circ \alpha_Y = \alpha_Y$*. On en déduit que* $\psi \circ \varphi = id_{F_X}$ *et* $\varphi \circ \psi = id_{F_Y}$ *d'ou* $F_X \backsimeq F_Y$ *. [?]*

Remarque 1.2.1. *Nous verrons plus loin que, réciproquement* $F_X \backsimeq F_Y$ *implique X et Y équipotents .*

1.3 Indice d'un sous-groupe

Définition 1.3.1. *[2] Soit G un groupe et H un sous-groupe de G.*

1) La relation R_1 *est appelée relation de congruence à droite modulo H. L'ensemble des classes d'équivalence est noté* $(G/H)_d$*.*

2) La relation R_2 *est appelée relation de congruence à gauche modulo H. L'ensemble des classes d'équivalence est noté* $(G/H)_g$*. Le cardinal de G/H est appelé l'indice de H dans G et est noté [G : H].*

Théorème 1.3.1. *(Première formule d'indice). Si G est un groupe fini et H sous-group de G on a la formule : o (G) = o (H) [G : H] .*

Démonstration 1.3.1. *ici [G : H] = o(G)/o(H)*

Attention ; [H : G] peut être fini sans que ni G ni H le soit. Exemple : (Z ; +) et nZ, alors G/H est de cardinal n.

Théorème 1.3.2. *(Formule des indices). [2] Si H un sous-groupe de G d'indice fini dans un groupe G et si K est un sous-groupe de G contenant H, alors K est d'indice fini dans G et :*

$$[G : H] = [G : K][K : H] \tag{1.2}$$

La formule (1.2)sera appelé :formule des indices .

Démonstration 1.3.2. *Soit* $\{x_i\}_{i\in I}$ *une famille de représentants des classes à droite distinctes modulo K dans G.*

La famille des $\{Kx_i\}_{i\in I}$ *forme une partition de G :*

$G = \cup Kx_i, Kx_i \neq kx_j \Leftrightarrow i \neq j$ *et card (I)=*$[G : K]$

Soit $\{y_\lambda\}_{\lambda\in\Lambda}$ *une famille de représentants des classes à droite de H dans K. On a :*

$K = \cup Hy_\lambda, Hx_i \neq Hy_\mu \Leftrightarrow \lambda \neq \mu$ *et card* $(\Lambda) = [K : H]$.

Soit $g \in G$ *, il existe un unique* $i \in I$ *tel que* $g \in Kx_i$.

On en déduit qu'il existe un unique$a \in K$ *tel que* $g = ax_i$.

D' autre parte, il existe un unique $\lambda \in \Lambda$ *tel que* $a \in H_{y_\lambda}$.

On en déduit que $g \in H_{y_\lambda}x_i$ *; par suite,on a :* $G = \cup y_\lambda x_i$.

Démontrons que la famille des $\cup y_\lambda x_i$ *, pour* $(\lambda, i) \in \Lambda I$ *forme une partition de G .*

Supposons $H_{y_\lambda x_i} = H_{y_\mu x_j}$.

$HK \subseteq K \Rightarrow KH = K$ *;*

or $H_{y_\lambda x_i} = H_{y_\mu x_j} \Rightarrow KH_{y_\lambda x_j}$.

$KH_{y_\lambda} = K_{y_\lambda} = K$ *, car* $y_\lambda \in K$ *;de même* $KH_{y_\lambda} = K$

On en définit :

$Kx_i = K_j$ *, d'ou i=j ;*

par suite , on a

$Hy_\lambda = Hy_\mu$*, d'ou* $\lambda = \mu$.

La famille $\{y_\lambda x_i\}_{\lambda,\mu\in\Lambda I}$ *est donc une famille de représentants des classes à droite distinctes de G modulo H , d'ou :[G :H]=card(*ΛI*.par hypothèse, [G :H] est fini , par suite ,* Λ *et I sont des ensemble finis , en particulier :*
$[G : K] = card(I)$ *est fini et* $card(\Lambda I) = card(\Lambda)$ *card (I) implique :*
$[G : H] = [G : K][K : H]$.

Théorème 1.3.1 (Théorème de Lagrange)**.** *[2] Soit G un groupe fini,alors l'ordre de tout sous-groupe H de G divise l'ordre de G .*

Démonstration 1.3.3. *[2] Soit H*$\leqslant$*G , considérons la famille des classe à droite ; distinctes, modulo H dans G ; cette famille forme un partition de G*
G étant fini , il n'ya qu'un nombre fini de classe à droite distinctes modulo H ; soit k ce nombre.
Si n=o(G) et m=o(H) ,alors chaque classe à droite modulo H a m éléments ,d'ou n=km et par suite m=o(H) divise n=o(G) .

Chapitre 2

Groupes profinis et sous-groupes de congruence

2.1 Notions de base sur les Congruences

2.1.1 Congruences

[3] a et b sont modulo m congrus si a − b est un multiple entier de m. Nous écrivons ce ci comme a≡ b mod m,Notez qu'il s'agit d'une relation d' équivalence pour un m donné , chaque classe de congruence n'est qu'un progression arithmétique de la forme a+km ; k ∈ Z ce sont exactement m en nombre , correspondant a=0,1,..,m − 1 En d'autres termes l'ensemble P_m de cas classes de congruence put être identifie avec le groupe Z/mZ ce point de vue fait appel aux techniques de la théorie des groupe et de la théorie des anneaux il est généralement appris un premier cours sur la théorie des groupes que les congruence comme le petit théorème de fermat,le théorème de wilson, le théorème d'Euler...etc sont facilement démontrés par des méthodes de théorie des groupe la congruence peut être définis plus généralement pour tout anneau commutatif R pour a,b,c∈ R alors on peut définir a≡ b mod c pour signifier que a − b=cd pour certains d∈ R, plus généralement pour un idéal I dans R on définit a≡ b mod I pour signifier a−b ∈ I .

2.1.2 sous-groupe de Congruences

[3] tout sous groupe $\Gamma \neq \{0\}$ de Z est de la forme mZ pour un entier positive m c'est-a-dire qu'il se compose de tous les entiers x de noyau Z→ Z/mZ. en d'autre termes ,Γ est définit par la congruence x≡0 mod m.plus généralement,considérons le groupe abélien libre Z^npour tout $n \geqslant 1$ pour un entier positive m le vecteurs m $Z^n := \{(ma_1, ..., ma_n) : a_i \in Z\}$ forme un sous groupe $\Gamma(m)$ de Z^n évidement , $\Gamma(m)$ est d'indice fini car il est égal au noyau de l'homomorphisme naturel :
$Z^n \to (Z/mZ)^n$ encore un fois ,on peut penser de$\Gamma(m)$ défini par les congruence ,si un sous groupe $x_i \equiv 0$ mod m pour $1 \leqslant i \leqslant n$. si Γ sous groupe de Z^n contient un certain $\Gamma(m)$.On l'appelons un sous groupe de congruence toute évidence,un sous groupe de congruence d'indice fini dans Z^n.

Exemple 2.1.1. *Notez que Z→Z/nZ est un homomorphisme en anneau donc :*

$$\varphi_n : SL(3, Z) \to SL(3, Z/nZ) \ .$$

est un homomorphisme de groupe,puis l'anneau Z/nZ est évidement fini,il est clair que le groupe SL(3,Z/nZ)est fini ,donc l'image de $\varphi_n$est fini ,par conséquent donc $\Gamma_n := ker\varphi_n$ est un sous-groupe (normal)d'indice fini donc $\Gamma = SL(3, Z)$ces sous-groupes sont les sous-groupe a indice fini les plus évidents de Γ .
Γ_n est un sous groupe de congruence principal de Γ par définition ,Γ_n est l'image inverse de{e},le sous-groupe trivial nous pouvons généraliser la construction ce-dessus en remplaçant {e} par un sous-groupe plus général , si X est un sous-groupe de SL(3,Z/nZ)alors $\varphi_n^{-1}(X)$ est un sous-groupe d'indice fini de Γ il s'agit d'un sous-groupe de congruence de Γ .

2.2 Les Groupes profinis

Définition 2.2.1. *[8] On appelle groupe profini un groupe topologique qui est limite projective de groupe finis .Un tel groupe est compact et totalement discontinu . Réciproquement :*

Proposition 2.2.1. *Un groupe topologique compact totalement discontinu est profini.*

Soit G un tel groupe .Comme G est totalement discontinu et localement compact, les sous-groupes ouverts de G forment une base de voisinage de 1 .Un tel sous-groupe U est d'indice fini dans G puisque G est compact ; ses conjugués gUg^{-1} sont en nombre fini et leur intersection V est un sous-groupe ouvert normal de G de tel V forment donc une base de voisinage de 1 ;
l'application canonique $G \to \varprojlim G/V$ est injective continue et d'image dense ; comme G est compacte , c'est une isomorphisme . Donc G est profini .
Les groupes profinis forment une catégorie (les morphismes étant les homomorphismes continues)ou les produits infinis et les limites projectives existent .

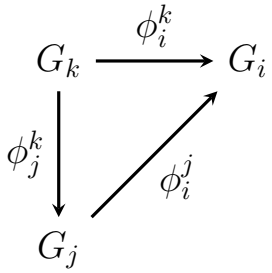
Définition 2.2.2. *Tout sous-groupe fermé H d'un groupe profini G est profini .De plus , l'espace homogène G/H est compact totalement discontinu.*

L'importance de groupe profinit réside dans le fait que le problème de sous-groupe de congruence sera formulé dans le langage des groupes pro finis.

2.2.1 Système projectif

Définition 2.2.3. *Les groupes pro finis sont définit de la manière suivante.*
Supposons que nous avons un ensemble d'indexation partiellement ordonné I et des groupes finis G_i ,pour $i \in I$ supposons que nous avons des homomorphismes :

$$\phi_i^j : G_j \to G_i \text{ pour } i \leqslant j \text{ , } \phi_i^i = id,$$



le diagramme est commute alors $\phi_i^k = \phi_i^j \circ \phi_j^k$ *,* $i,j,k \in I$ *,* $i \leqslant j \leqslant k$ *.*

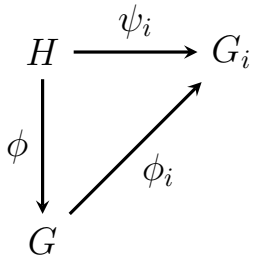
2.2.2 Limite projective

Soit G un groupe $\phi_i^j \circ \phi_j^k = \phi_i^k$ pour $i \leqslant j \leqslant k$, et $\phi_i : G \to G_i$sont des homomorphismes satisfaisant :

i) les condition de compatibilité $\phi_i = \phi_i^j \circ \phi_j$ pour tout $i \leqslant j$.

ii) **la propriété universelle suivante**

On appelle le couple $(G, \{\phi_i\})$ une limite projective de $(\{G_i, \phi_i^j\})$ la propriété universelle suivante : pour tout couple $(H, \{\psi_i\})$ avec $\psi_i : H \to G_i$ homomorphismes compatibles , on a un homomorphisme unique : $\phi : H \to G$ tel que $\psi_i = \phi_i \circ \phi \forall i \in I$.



En fait, on peut définir G comme étant le sous-ensemble de produit direct $\prod_{i \in I} G_i$ constitué de tous les couples compatibles ;c'est à dire :

$$\text{G}=\{\ (x_i)_{i \in I} \in \prod_i G_i \mid \forall\ \text{i,j}\ \ \forall \phi_i^j x_i = \phi_i^j(x_j)\}$$

$\phi_i : G \to G_i$ est la projection naturelle sont les projections pour simplifier , on écrit $G = \varprojlim G_i$ [3] .

Définition 2.2.4. *Soit G un groupe ,p un nombre premier .On dit que G est un p-groupe si tout élément de G est d' ordre une puissance de p ;*
G p-groupe$\Leftrightarrow \forall x \in G, \exists k \in N$ *tel que l'ordre de* $x = p^k$.

Définition 2.2.5. *[4] Soit p un nombre premier. Un pro-p-groupe est un groupe topologique qui est limite projective de p-groupes finis , c'e st un groupe compact totalement discontinu.*

Exemple 2.2.1. *Soit n un entier, soit L(n) le groupe libre engendré par n éléments, et soit F(n) la limite projective des quotients finis de L(n) qui sont des p-groupes. Le groupe F(n) s'appelle le pro-p-groupe libre de rang n .*
On a F(0) = 1 , F(1) = Z_p *(groupe additif des entiers p-adiques).*

La notion des groupes profinis se lié aux groupes finis et aussi des majorité des groupes infinis . [3]

Définition 2.2.6. *:*

i) un groupe profini est une limite projective de groupe finis ,
ii) Si tous les G,sont des groupe soluble, nilpotents,p- leur limite projective est appelée un groupe pro-soluble, pro-nilpotent, pro-p .

2.2.3 Exemple de Groupe Profinis

1) Fixer p premier ,soit $G_n = Z/p^nZ$, et pour m $\geqslant$ n ,
soit $\phi_n^m = Z/p^mZ \to Z/p^nZ$ l'homomorphisme naturel. la limite projective $\varprojlim Z/p^nZ$ est le groupe Z_p d'entier p-adic c'est un pro-p groupe.

2) Soit G =Z/nZ , et pour m divisant n ,Soit $\phi_m^n : Z/nZ \to Z/mZ$ le projection.En suit $\hat{\mathrm{Z}}= \varprojlim Z/nZ \cong \prod Z_p$.

Chapitre 3

Le problème de sous-groupe de congruence

3.1 Sous groupe d' indice fini dans SL(n, Z) par H.Baas, M.Lazard et J-P.Serre

3.1.1 Enoncé du théorème et schéma de démonstration

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

$$\mathrm{SL(n,Z)}\rightarrow\mathrm{SL(n,Z/qZ)}.$$

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

Théorème 3.1.1. *si $n \geqq 3$,tout sous-groupe d'indice fini de SL(n, Z) est un groupe de congruence.*

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

Soit $\hat{\mathrm{G}}$(n) (resp. A(n)) le complété de G(n) pour la topologie des sous-groupes d'indice fini (resp. des sous-groupes de congruence). Les groupes $\hat{\mathrm{G}}$(n) et A(n) sont des groupes profinis .

On notera que,d'après le théorème d'approximation dans le groupe SL_n, le groupe A(n) s'identifie au produit des groupes SL(n,Z_p), pour tous les nombre premiers p (on

note Z_p l'anneau des entiers p-adiques). Il est clair que A(n) s'identifie au quotient de $\hat{\mathrm{G}}$(n) par un sous-groupe distingué fermé C(n). La suite exacte correspondante :

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

Sera notée (X_n). Le Théorème 1 équivaut à dire que C(n) = 1 pour n $\geqq$3.
L'étude des groupes C(n) utilise la méthode de "suspension" . De façon précise, soit S : G(n) $\to$ G(n + l) l'homomorphisme défini par la formule :

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

Cet homomorphisme se prolonge par continuité en un homomorphisme (encore noté S) de la suite exacte (X_n) dans la suite exacte (X_{n+1}) ; en particulier
S : C(n) $\to$ C(n + l) est bien défini. Les trois propriétés suivantes seront démontrées dans les n^{os} 2 et 3 :

1) Pour n$\geqq$3, l'homomorphisme S : C(n—l)$\to$ C(n) est surjectif.
2) Pour n $\geqq$3, C(n) est contenu dans le centre de $\hat{\mathrm{G}}$(n).
3) On a H^1(A(2), Q/Z)= Z/12Z et H^2(A(2), Q/Z)=0.

(Il s'agit ici de cohomologie des groupes profinis de plus, le groupe A(2) opère trivialement sur le groupe de coefficients Q/Z.)
Montrons comment ces propriétés entraînent le Théorème 1 :
La suite spectrale des extensions de groupes, appliquée à (X_2) et au groupe de coefficients I= Q/Z, donne la suite exacte :

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

D'après (3), on a H^1(A(2), I)=Z/12Z. D'autre part, le groupe $H^1(\hat{\mathrm{G}}(2), \mathrm{I})$ s'identifie à Hom(G (2), I), qui est aussi cyclique d'ordre 12 (cela se voit, par exemple, sur la présentation standard de G(2) au moyen de deux générateurs x, y liés par les

relations $x^4 = 1$, $x^2 = y^3$).

Il suit de là que

H^1(A(2), I)$\rightarrow$ H^1 $\hat{\mathrm{G}}$(2), I) est bijectif. La suite exacte écrite plus haut, jointe à la propriété (3), montre alors que $H^1(C(2), I)^{A(2)} = 0$. Mais ce groupe est dual du quotient C(2)/D(2),où D(2) désigne l'adhérence du groupe de commutateurs ($\hat{\mathrm{G}}$(2), C(2)). Ainsi, ($\hat{\mathrm{G}}$(2), C2)) est dense dans C(2). La propriété (1), appliquée au cas n = 3, montre alors que (S($\hat{\mathrm{G}}$(2)), C(3)) est dense dans C(3) ; d'après la propriété (2), on a donc C(3) = 1, d'où C(n) = 1 pour tout n$\geqq$3 d'après la propriété (1).

3.1.2 Démonstration des propriétés (1)et(2)

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

Lemme 3.1.1. *Soit x= $(x_1, ..., x_m)$ un élément unimodulaire de R^m. Si l'anneau R est semi-local il existe une famille $(y_2, ..., y_m)$ d'éléments de R telle que $x_1 + y_2x_2 + ... + x_my_m$ soit inversible dans R.*

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

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

Lemme 3.1.2. *Soient x=$(x_1, ..., x_n)$ et x'= $(x'_1, ..., x'_n)$ deux éléments de Z^n. Soit I une partie de [1, n] telle que $x_i = x'_i$ pour $i \in I$, et soit a l'idéal de Z engendre par les x_i , $i \in I$. Supposons que l'on ait :*

$$x'_j \equiv x_j mod\ qa \quad pour\ tout\ j \notin I.$$

Il existe alors $s \in E_q(n)$ qui transforme x en x'. Par hypothèse, on a $x'_j = x_j + \Sigma_{i \in I} q t_{ij} x_i$, avec $t_{ij} \in Z$. On prend alors pour s le produit des matrices $1 + q t_{ij} E_{ji}$, pour tous les couples(i,j) tels que $i \in I$, $j \notin I$.

Proposition 3.1.1. *Supposons $n \geqq 3$, et $q \geqq 1$. Soient $a = (a_1, ..., a_n)$ et a' = $(a'_1, ..., a'_n)$ deux éléments unimodulaires de Z^n tels que $a \equiv a'$ mod q .Il existe alors $s \in E_q$ (n) qui transforme a en a'.*

Il est clair que le groupe $E_1(n)$=G(n) opère transitivement sur l'ensemble des éléments unimodulaires de Z^n. On peut donc supposer que a'est égal au vecteur coordonnée e_1= (1, 0,..., 0) et que $q > 1$. Posons $a_1 = 1^- r$, avec $r \in qZ$. L'image de $(a_2, ra_3, ..., ra_n)$ dans le (Z/a_1Z)-module $(Z/a_1Z)^{n-1}$ est unimodulaire. Comme Z/ a_1 Z est semi-local, le Lemme 1 montre qu'il existe des entiers $t_3, ..., t_n$ tels que l'élément $b = a_2 + \Sigma_{i \geqq 3} t_i r a_i$ soit inversible mod a_1.

En appliquant le Lemme 2 avec I= [3, n], on voit qu'il existe $s_1 \in E_q(n)$ tel que s_1 (a) soit égal à l'élément c'=($a_1, b, a_3, ..., a_n$).

Comme a_1 et b sont premiers entre eux, le Lemme 2 (appliqué avec I= [1, 2] cette fois) montre qu'il existe $s_2 \in E_q(n)$ transformant c' en a" = $(a_1, b, r, 0, ..., 0)$. Soit maintenant 0 l'élément de SL(n, Z) qui laisse fixes les vecteurs coordonnées $e_i (i \neq 3)$ et transforme e_3 en $e_3 + e_1$. On a 0 $e_1 = e_1$, et 0 a" = (1 , b, r, 0,..., 0). Le Lemme 2, appliqué avec I=l,montre qu'il existe $s_3 \in E_q(n)$ transformant 0 a" en e_i. L'élément $0^{-1} S_3 0 . s_2 s_1$ transforme alors a en e_1, ce qui achève de démontrer la proposition.

Corollaire 3.1.1. *Pour $n \geqq 3$, $G_q(n) = E_q(n).G_q(n^-1)$. (On convient d'identifier G(n — 1) à un sous-groupe de G(n) au moyen de l'homomorphisme de suspension S.)*

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

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

Avec $A \in G_q(n^-1)$ *et* $x \in qZ^{n-1}$ *. Soit* $y = -xA^{-1}$ *; en multipliant à gauche*

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

on obtient

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

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

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

cela montre bien que t appartient à $E_n.G_q(n-1)$ *.*

Corollaire 3.1.2. *Pour* $n \geqq 3$*, on a* $(G(n), G_q(n)) \subset E_q(n)$*. Il suffit de prouver que, si* $s \in G_q(n)$*, et si t est élémentaire, le commutateur* $(s,t) = s^{-1}t^{-1}st$ *appartient à* $E_q(n)$*. Après conjugaison, on peut supposer t de la forme*

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

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

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

avec $A \in G_q(n^-l)$ *. On a alors :*

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

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

Corollaire 3.1.3. *Pour $n \geqq 3$, les sous-groupes $E_q(n)$ sont d'indice fini dans $G(n)$. On utilise le lemme suivant, qui est bien connu :*

Lemme 3.1.3. *Soit $1 \to H \to G \to \pi \to 1$ une suite exacte de groupes . Si π et $G/(G\ ,\ G)$ sont finis, $G/(G\ ,\ H)$ l'est aussi.*
(Rappelons la démonstration : il suffit de prouver que $H/(G,\ H)$ est fini ; cela résulte de la suite exacte :

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

et du fait que $H_2(\pi, Z)$ est fini.)
En appliquant ce lemme au groupe $G = G(n)$ et au sous-groupe distingué $H = G_q(n)$, on voit que $(G(n),\ G_q(n))$ est d'indice fini dans $G(n)$, et il en est donc de même de $E_q(n)$, d'après le Corollaire 2.

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

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

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

3.2 Sous-groupes non de congruence dans $SL_2(Z)$

[6]Dans cette section, nous allons tout d'abord prouver de maniére relativement théorique que SL2(Z) ne posséde pas la propriété des sous-groupes de congruence, puis nous énoncerons le critére de Wohlfahrt imposant une condition nécessaire sur les sous-groupes de congruence, ce qui nous permettra de conclure sur un exemple de sous-groupe non de congruence dans SL2(Z).

3.2.1 Contre-exemples plus systématiques

Appliquons ceci à un exemple de sous-groupe d'indice fini non de congruence dans $SL_2(Z)$. Pour tout mot g appartenant au groupe libre .
$\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \rangle = \langle A; B \rangle$ On définit $E_A(g)$ comme la somme des exposants de A apparaissant dans g, et on définit de même $E_B(g)$ en remplaçant A par B. E_A définit un morphisme de $\langle A; B \rangle$ dans Z. Pour tout entier strictement positif l, on pose $\Gamma_l = \mathrm{g} \in \langle A; B \rangle | E_A(g) \equiv E_B(g) \equiv 0 mod l$. Comme c'est le noyau du morphisme $\langle A; B \rangle \to Z^2(Z/lZ)^2$composé du morphisme abéliani sant et de la restriction modulo l, il est normal d'indice l^2. Nous allons montrer que si l a un diviseur premier impair p, alors Γ_l n'est pas un sous-groupe de congruence.

Démonstration 3.2.1. *En effet, si Γ_l était de congruence, $\Gamma_p \geqslant \Gamma_l$ le serait. Or*
$A^p = \begin{pmatrix} 1 & 2p \\ 0 & 1 \end{pmatrix} \in \Gamma_p$
donc, par le critére de Wohlfahrt, on aurait $\Gamma_p \geqslant \Gamma(2p)$. Or ceci n'est pas possible compte tenu de leurs indices respectifs dans $SL_2(Z)$: $[SL_2(Z) : \Gamma_p] = p^2[SL_2(Z) : \langle A; B \rangle] = 12p^2 3p(p^2 - 1) = [SL_2(Z) : \Gamma(2p)]$.

3.3 Commentaire sur$SL_n(Z)$

1) On soit que $SL_n(Z) = \langle I_n + E_{ij} | 1 \leqslant i, j \leqslant n, i \neq j \rangle$ où I_n est l'identité et E_{ij} est la matrice n.n dans tout les compostes sont nuls , sauf la composante $e_{ij} = 1$.
2) Soit l'homomorphisme naturel $\varphi : SL_n(Z) \to SL_n(Z/mZ)$ pour m = 1,2,.....
3) $\Gamma_n(m) = Ker(SL_n(Z) \to SL_n(Z/mZ)$, pour n fixé . Notons $\aleph$ la collection des sous groupes de congruence de $\Gamma_n(m)$ alors $\aleph$ est un système fondamental de voisinages pour une topologie de housdrff sur $SL_n(Z)$(C.S.T) .utilisant (2), où peut voire que
$$\kappa_{\aleph}(SL_n(Z)) = \varprojlim SL_n(Z/mZ) \cong SL_n(\hat{\mathrm{Z}}) \cong \prod_p SL_n(Z_p).$$
4) On peut comparer la topologie de congruence sur $SL_n(Z)$ avec sa topologie profinie .Considérez l'épimorphisme continu naturel .
$$\varphi : \widehat{SL_n(Z)} \to SL_n(\hat{\mathrm{Z}}) \ .$$
alors le (CSP) est le problème de décider si le noyau de φ est trivial .Dans Bass ,Lazard et Serre (1964) et Mennicke(1965) on montre que si n $\geqslant$ 3 alors Ker(φ) = 1 , c'est à dire les topologies de sous-groupes profini et congruence sur $SL_n(Z)$ coïncidant .[7]

Conclusion

Le problème de sous-groupe de congruence a été developer récement ,apres les travaux de Bass ,Lazard et Serre et par suite A.lubotski (n=2 des contres-exemple).Est-ce que tous sous-groupe d'idice fini de Aut (F_n) est un sous-groupe de congruence ?

Résumé

Tout sous-groupe d'indice fini de SL(n, Z) contient un sous-groupe de congruence
$\forall$ n $\geqq$ 3 , si n = 2 , c'est faux .

Abstract

Any finite index subgroup of SL(n, Z) contains a Congruence subgroup
$\forall$ n $\geqq$ 3, if n = 2 , it is false .

ملخص

كل زمرة جزئية ذات مؤشر منتهي من $SL(n, Z)$ **هي زمرة جزئية توافقية**
$\forall 3 \leqslant n$ ، **خطا في حالة** $n = 2$.

Bibliographie

[1] GROUPE Herman .

[2] JOSETTE calais , Éléments de théorie des groupes , 09/1984

[3] B-SURY ,the congruence subgroup problem

[4] JEAN-PIERRE SERRE , Structure de certains pro-p-groupes Séminaire N. Bourbaki, 1964

[5] H.BASS M.LAZARD et J-B.SERRE , Sous-groupe d'indice fini dans SL(n,Z) , 18/11/1963

[6] BULOS MICHAL , le problème des sous-groupes de congruence , 11/12/2004

[7] PAVEL ZALIESSKII , Profinite Groups

[8] J-P Serre, Cohomologie galoisienne ,cour au Collège de France 1963