UNIVERSITÉ KASDI MERBAH OUARGLA
Faculté des Mathématiques et des Sciences de la Matière

DÉPARTEMENT DES MATHÉMATIQUES

MASTER

Spécialité : Mathématiques

Option : Algèbre et Géométrie

Par : Kaoudja Nadjat

Thème

Groupe de Golod-Shafarevich

Soutenu publiquement le : 03/06/2019

Devant le jury compose de :

Mr. M.T.Ben Moussa	Dr UKMO	Université-Ouargla	Encadreur
Mr. Y.Geurbousa	Dr UKMO	Université-Ouargla	Examinateur
Mr. A.Bahayou	Dr UKMO	Université-Ouargla	Examinateur
Mr. M.boussaid	Dr UKMO	Université-Ouargla	Examinateur
Mr. M.Kouidri	Dr UKMO	Université-Ouargla	Président

Dédicace

C'est un trés grand plaisir que je dédie ce modèste travail aux personnes les plus chères au mon coeur : A mes chers parents, première maitresse,

ma chère baba rabi yarhmek** et **ma cher mama

qui m'ont permis de continuer mes études dans les meilleurs conditions et qui m'ont appris à ne jamais baissé les bras.

Je dédie aussi cette modèste réalisation à : Mes chers frères,

Ali , Salim et Ismail.

Mes chères soeurs,

warda, Sabah, Latifa, Malika, Saida et la petite Kaouther.

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

Sabrina, Achoik, Fatiha, Masouda, koka, Fatima, Maissa, Djihad, Amel

*et à toute la famille **Kaoudja, Hacini, Bouziane.***

*A mon encadreur **M.T.Ben moussa**, en espérant qu'elle trouvre dans ce travail le témoignage de ma profonde gratitude. A tout mes enseignants de l'Université de Kasdi Merbah sans exception.*

A tous mes collègues.

A tout ceux qui m'aident, m'encouragent,et qui m'aident toujours pour continuer sur la bonne voie.

Remerciement

Je remercie d'abord et avant tout ***ALLAH*** *qui m'a 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 grace à ces conseils.*

Je tiens à remercier, particulièrement, ***Mr. BOUSSAID Mohamed Mr. GEURBOUSA Yacin, Mr. BAHAYOU Mohamed Amine Mr.AMAIER*** *et tout les profs qui n'a jamais cessé de me soutenir, pour l'aide qu'il m'a procurée et pour ses précieux conseils.*

Merci beaucoup à tous les profs de laboratoire du mathématique pour le temps et l'aide qu'ils m'ont procuré.

En enfin, je remercie tous ceux, qui de prés , ont contribué à l'accom-plissement de ce mémoire.

Table des matières

Dedicace **i**

Remerciement **ii**

Notations et Premilinaires **v**

Introduction **vi**

1 Algèbre Graduation **1**

1.1 K-Algèbre 1

1.2 Algèbre des polynômes en variables non commutent 2

1.3 Algèbre associative libre 3

1.3.1 L'ensemble monoide libre : 3

1.4 Algèbre Graduation 5

2 Théorème d'artin Wedderburn **6**

2.1 Anneaux Radicaux 6

2.2 Le monoide adjoint, et le groupe adjoint 6

2.3 Le Radical Jacobson 8

2.4 Théorème d'Artin Wedderburn 9

3 Application des groupes de Golod-Shafarevich pour répondre négativement aux problème de Burnside **12**

3.1 Limite projective 12

3.2 Groupe Topologique 14

3.3 Groupe profinis 15

3.4 Exemple de Groupe Profinis 18

3.5 Algèbre de Groupe 18

3.6 Présentation par Générateurs et Relateurs 19

3.7 Séries Hilbert 22

3.8 Groupe de Torsion 22

3.9 Groupe de Golod-Shafarevich 24

3.10 Exemple de groupe de Golod-Shafarevich 27

Conclusion **28**

Notation

- $\varprojlim$: Limite Projective
- (G_i, φ_{ij}) : Système Projective
- $\bigoplus A_s, s \in S, S$ monoide : Algèbre Gradué
- $\mathbb{F}_p[[G]]$:Algèbre de groupe
- Hom : Homomorphisme
- $\prod$: Le Produit
- $\sum$: La Somme
- $\lhd$: Normalisé

Introduction

En **1925**, Furtwängler, a posé une question dans le domaine de la théorie des nombre concernant, l'infinité des extensions [class field tower problem], cette question reste ouvert plus d'un **40 ans**.

En **1963**, Shafarevich répond négativement *à* la question précédent, par bornage supérieur de $r(G_{K,p})$ a l'aide de $d(G_{K,p})$, où $G_{K,p} = Gal(K_p/K)$.

En **1964**, Golod et Shafarevich réalise l'inégalité $r(G) > (d(G) - 1)^2/4$ est un outil pour montré q'un p-groupe est fini G un est p-groupe.

Cette dernière inégalité une conséquence immédiate de l'inégalité appelée par la suite l'inégalité de Golod-Shafarevich. Il était le temps de construire un type particulier des groupe nommé les groupe Golod-Shafarevich vérifiant l'inégalité

$$1- \mid X \mid t + H_R(t) < 0 \tag{1}$$

Cette nouvelle construction des groupe *à* aider de répondre négativement aux problem de Burnside, puisque ces groupe sont infini. Ils ont contribué aussi *à* développer le domaine combinatoire groupe theory, et la théorie des nombre puisque les groupes $Gal(\mathbb{Q}_s/\mathbb{Q})$ sont des groupes de golod-shafarevich.

Notre travail est présenter ce genre des groupes, l'essentiel de propriétés, des exemple ullustrent l'importance, et l'utilité des groupes présentés par des générateurs et relateurs

d'une part, et d'autre part les groupes soumis au conditions (1).
A titre d'exemple on a choisi le théorème de golod, qui discute l'infinité d'un groupe de torsion *à* d-générateur, utilisant dans la démonstration les groupes de Golod-Shafarevich.
Ce mémoire *à* deviser en trois chapitre :

- 1er Chapitre : contient les notions des Algèbres, Algèbre gradué, Algèbres des polynômes, Exemples.
- 2eme Chapitre : contient les Anneaux Radicaux, le Radicale de Jacobson, Le théorème d'Artin Wedderburn.
- 3eme Chapitre : contient l'essentiel de notre travail c'est l'application des groupes de Golod-Shafarevich.

Chapitre 1

Algèbre Graduation

1.1 K-Algèbre

Définition 1.1.1 [7] Soit K un anneau commutatif unitaire. Une K-algèbre A est un K-module muni d'une multiplication $A \times A \longrightarrow A$ que soit K bilinéaire, c.$\grave{a}$.d :

1. $(x_1 + x_2)y = x_1y + x_2y$
2. $(\lambda x)y = \lambda(x)y$
3. $x(y_1 + y_2) = xy_1 + xy_2$
4. $x(\lambda y) = \lambda(xy)$

Une K-algèbre A est dite associative si sa multiplication est associative, c$\bar{a}$d : pour tout $x, y, z \in A$: $(xy)z = x(yz)$, un exemple typique d'une K-algèbre associative étant l'algèbre des K-endomorphisme $End_K(M)$, où M est un K-module, les lois d'un $End_K(M)$ sont définie par :

1. $(f + g)(x) = f(x) + g(x)$

2. $(\lambda f)(x) = \lambda f(x)$

3. $(fg)(x) = f(g(x)) = f(x)g(x)$

tel que $f, g \in End_K(M) et \lambda \in$ K

1.2 Algèbre des polynômes en variables non commutent

Les k-algèbres des polynômes non commutative K$\langle X \rangle$ sur X sont toute élément f de K$\langle X \rangle$ tel que $f = \sum \lambda_w w$ où w les mots sur X et $\lambda_w = 0$ presque par tous, $w \in X^*$ (X^* l'ensemble des mots). Soient A une k-algèbre et $\phi \neq S \subseteq A$ un sous-ensemble de A.

Définition 1.2.1 L'algèbre des polynômes $K\langle x_s / s \in S \rangle$ est une algèbre associative libre de l'ensemble $\{x_s, s \in S\}$. L'application $\varphi : \{x_s, s \in S\} \longrightarrow A$ s'étendu à un morphisme de k-algèbre $\tilde{\varphi} : K\langle x_s / s \in S \rangle \longrightarrow A$ tel que $\tilde{\varphi}(x_s) = s$ pour tout $s \in S$.

Définition 1.2.2 $\ll S \gg$ est le plus-petit sous-algèbre de A qui contient S.

Proposition 1.2.3 L'image de $\tilde{\varphi}$ est un sous-algèbre de A inclus dans $\ll S \gg$.

Preuve. 1
Montrons que $Im\tilde{\varphi} \subseteq \ll S \gg$. Soit $\tilde{\varphi}(f) \in Im\tilde{\varphi}$ tel que $f \in K\langle x_s / s \in S \rangle$ où $f = \sum \lambda_w w, \forall\ w \in X^*$, $\tilde{\varphi}(f) = \tilde{\varphi}(\sum \lambda_w w) = \sum \lambda_w \tilde{\varphi}(w) = \lambda_w \sum \tilde{\varphi}(w)$.
Alors on montre que $\tilde{\varphi}(w) \in \ll S \gg$ pour toute mot w sur l'ensemble $\{x_s, s \in S\}$.
D'abord si $l(w) = 1$, alors $w = x_s$ pour certains $s \in S$. Ainsi $\tilde{\varphi}(w) = \tilde{\varphi}(x_s) = s \in S \subseteq \ll S \gg$. Donc $\tilde{\varphi}(w) \in \ll S \gg$.
Si pour tous les mots de longueur$<l(w)$, on peut écrire $w = w' \cdot x_s$ tel que w' est un mot de longueur $l(w) - 1$, alors $\tilde{\varphi}(w) = \tilde{\varphi}(w' \cdot x_s) = \tilde{\varphi}(w') \cdot \tilde{\varphi}(x_s)$, donc$\tilde{\varphi}(w) \cdot s^{-1} = \tilde{\varphi}(w')$
On a $\tilde{\varphi}(w) = s, s^{-1} \in \ll S \gg$, donc $\tilde{\varphi}(w') \in \ll S \gg$.
Donc $\tilde{\varphi}(f) \ll S \gg$. D'ou $Im\tilde{\varphi} \subseteq \ll S \gg$. ■

Définition 1.2.4 On dit que A est admet un nombre finis de générateurs si :

- $A = \ll S \gg$ pour S un sous-ensemble fini.

- $|S|$=n , A est n-générateurs par S.

Exemple 1.2.5 $K[x]$ est un 1-générateur par S={x} et $K[x] =\ll x \gg$

Corollaire 1.2.6 Soient A une k-algèbre n-générateurs par $\{a_1, \cdots, a_n\}$ et $K\langle x_1, \cdots, x_n\rangle$ polynômes en variables non commutes.
$\tilde{\varphi} : K\langle x_1, \cdots, x_n\rangle \longrightarrow A$ est un morphisme induit par l'application $\varphi : x_i \longrightarrow a_i$ pour $f \in K\langle x_1, \cdots, x_n\rangle$ où $f = \sum \lambda_w w \ \forall \ w \in X^*$ et $\lambda_w = 0$ ppt $w \in X^*$. On remplace chaque x_i par a_i. Alors A=$\ll a_1, \cdots, a_n \gg = \{f(a_1, \cdots, a_n)\}$.

Exemple 1.2.7 Soit $f \in K[x_1, x_2]$ tel que $f(x_1, x_2) = x_1^2 - 3x_2x_1 + x_1x_2$
Soient $a_1, a_2 \in M_2(\mathbb{Z})$ où $a_1 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right), a_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$

$$\begin{aligned} f(a_1, a_2) &= \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)^2 - 3\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) - 3\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} -3 & -3 \\ 3 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} -1 & -2 \\ 4 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 0 & -3 \\ 5 & 1 \end{smallmatrix}\right) \end{aligned}$$

1.3 Algèbre associative libre

1.3.1 L'ensemble monoide libre :

Soit X un ensemble non vide, et le mot de langueur $n \geq 0$ de X suite finie $M = x_1x_2...x_n$, où $x_i \in X$. On noté mot l'unique de langueur 0 : (le mot vide), et on noté l'ensemble de tous les mots de X^*, les parties de X^* est s'appelle *à* longe de X, si :

$$U = x_1x_2...x_n \ \ ; \ \ V = y_1y_2...y_n$$

donc $UV = x_1x_2...x_ny_1y_2...y_m$, et $U.1 = U$ et $1.U = U$. Donc : X^* est un monoide.

Définition 1.3.1 On appelle X^* monoide libre sur l'ensemble X.

Proposition 1.3.2 Le monoide libre X^* du propriété universelle suivant : pour tout application $f : X \longrightarrow M$; M est un monoide. Il existe morphisme unique de monoide

$$\tilde{\mathrm{f}} : X^* \longrightarrow M$$

par exemple : $\tilde{\mathrm{f}}$(x)= x pour $x \in X$, autre mots.

$$\begin{tikzcd} X \arrow[r, "f"'] \arrow[d, "i"'] & M \\ X^* \arrow[ur, "\tilde{\mathrm{f}}"'] & \end{tikzcd}$$

le diagramme commutative, tel que $\tilde{\mathrm{f}} \circ i = f$, $i(x) = x$.

Remarque 1.3.3 Si $U, V \in X^*$ et dénote de $l(U)$ à longueur de U et $l(V)$ à longueur de V, où :

$$l(UV) = l(U) + l(V),$$

alors le mot vide 1, est un élément unique inversible dans X^*.

Soient M est un monoide et $f : X \longrightarrow M$ est la application . Considérons l'application $\tilde{\mathrm{f}} : X^* \longrightarrow M$ d'*où* : $U = x_1 x_2 ... x_n$ et $\tilde{\mathrm{f}}(U) = f(x_1) f(x_2) ... f(x_n)$,

$$\tilde{\mathrm{f}}(U) = \tilde{\mathrm{f}}(x_1) \cdot \tilde{\mathrm{f}}(x_2) \cdot ... \cdot \tilde{\mathrm{f}}(x_n) = f(x_1) f(x_2) ... f(x_n)\,;$$

où $\tilde{\mathrm{f}}$ est un morphisme. si $g : X^* \longrightarrow M$ d'où g(x)=x pour toute $x \in X$, $g(U) = g(x_1 x_2 ... x_n) = g(x_1) g(x_2) ... g(x_n) = f(x_1) \cdot f(x_2) \cdot ... \cdot f(x_n) = \tilde{\mathrm{f}}(U)$ cette prouve montré que $\tilde{\mathrm{f}}$ est unique. □

Soit K est un anneau unitaire et commutative, et définie $K\langle x \rangle$ est un ensemble de pour toute forme : $f = \sum_{U \in X^*} K_U U$ avec $K_U = 0$ pour tout max $U \in X^*$, avec $K\langle x \rangle$ est un structure de K algèbre associative(additive)

$$\begin{aligned} (\sum K_U.U)(\sum K'_V.V) &= \sum K_U.K'_U(U.V) \\ &= \sum K''_U.U \qquad (\quad \text{où} \sum K''_U = \textstyle\sum_{U=V.W} K_V.K_W) \end{aligned}$$

si $X = \{x_1, x_2, ..., x_n\}$, dénote $K\langle X \rangle$ par $K\langle x_1, x_2, ..., x_n \rangle$ est appelons algèbre de polynôme dans non commute $x_1, x_2, ..., x_n$ indéterminé, tel que :

$$f = 1 + x_1 x_2 + x_2^2 x_1 x_3 \neq g = 1 + x_2 x_1 + x_1 x_2^2 x_3$$

1.4 Algèbre Graduation

Définition 1.4.1 [8] Soient A une K-algèbre, et $(S,+)$ un monoide, on appelle graduation de A par S toute famille $(A_s)_{s\in S}$ de sous-module de A.
Dans ce cas , on dit que A est une K-algèbre S-gradue, satisfaisant aux deux condition suivants :

1. $$A = \bigoplus_{s\in S} A_s,$$
   tel que on a : $a \in A$, donc a s'écrit unique, tel que
   $$a = \sum_{s\in S} a_s, a_s \in A_s \quad \text{et} \quad a_s = 0 \quad \text{p.p}$$
2. $A_s.A_t \subseteq A_{s+t}$,
   tel que $a \in A_s, b \in A_t : a.b \in A_{s+t}$.

Exemple 1.4.2 La K algèbre des polynômes $\overline{k}[X]$ est $\mathbb{N}$-gradue, pour n $\in \mathbb{N}$

1. $A_n =< X^n > sous - modules$
2. $A_0 = \{\lambda.1/\lambda \in K\} = K$
3. $A_n = \{\lambda X^n./\lambda \in K\}$

- on a : $A = \bigoplus_{n\geqslant 0} A_n$ tel que :$a_n \in A$ d'où $\sum_{n\in N} a_n X^n$
- et $A_n.A_m \subseteq A_{n+m}$, $\lambda X^n \lambda' X^m = \lambda\lambda' X^{n+m} \in A_{n+m}$ tel que $\lambda\lambda' \in K$.

Chapitre 2

Théorème d'artin Wedderburn

2.1 Anneaux Radicaux

Soit A un anneau, R est un groupe abélien par une multiplication $(x, y) \longmapsto xy$ tel que :

$$\begin{cases} (x+y)z = xz + yz, \\ x(y+z) = xy + xz. \end{cases}$$

$$(xy)z = x(yz), \quad \text{(associative)}$$

donc le suppose pas une anneau est nécessairement unitaire ou commutatif

2.2 Le monoide adjoint, et le groupe adjoint

On défini l'opération par composition sur A : $x \circ y = x + y + xy$; $x, y \in A$.
Cette opération est associative admet un zéro comme un élément neutre, est appel $(A, 0)$ le monoide adjoint de A. Les éléments inversibles de $(A, 0)$ forment un groupe que désigne A^0. Ce dessus est le groupe adjoint de l'anneau A.

Remarque 2.2.1 Si A a une unité 1, alors A^0 est isomorphe au groupe A^x concéder la application

$$f : A^0 \longrightarrow A^x$$
$$x \mapsto x + 1$$

$A^x = 1 + A^0$, alors A^0 peut *être* considéré comme une extension de A^x aux anneaux unis.

Proposition 2.2.2 Chaque anneau A peut *être* inclusion un anneau unital. considérons par exemple $A \times \mathbb{Z}$ avec l'opération

$$\begin{cases} (x,n) + (y,m) = (x+y, n+m), \\ (x,n).(y,m) = (nx + my + xy, nm). \end{cases}$$

(0,1) est un neutre dans $A \times \mathbb{Z}$, A idéal de anneau $A \times \mathbb{Z}$. À={(x,0) / x ∈ A} est un idéal.

$$A \longrightarrow \grave{A}$$
$$x \mapsto (x, 0)$$

est un homomorphisme d'anneau injective.
le groupe adjoint A^0 en peut identifie avec un sous-groupe multiplicatif d'un anneau unitaire.

Définition 2.2.3 Un anneau A en dit que radical si $A = A^0$

Exemple 2.2.4 rappelons qu'un anneau A est dit nul, si chaque élément de A est nilpotent *($x^n = 0$, $\forall x$, $\exists n$),*
$\langle\langle$ *chaque anneau nul est radical* $x \circ \grave{x} = \grave{x} \circ x = 0$ *si* $x^n = 0 \Rightarrow \overline{x} = \Sigma_{i=1}(-1)^n x^i$ $\rangle\rangle$.

Exemple 2.2.5 chaque anneau nilpotent est radical, A est nilpotent si

$$A^n = 0, \forall n \in \mathbb{N}^* \Leftrightarrow x_1 x_2 ... x_n = 0 \ \forall x_1, x_2, ..., x_n \in A$$

nous avons vu pour un chaque anneau A : {A nilpotent ⇒ A nul ⇒ A radical.}

Exemple 2.2.6 Il y a un anneau nul tel que n'est pas nilpotent.

Définition 2.2.7 La classe de nilpotence d'un anneau nilpotent est le plus petit $n \in \mathbb{N}$ tels que $A^{n+1} = 0$.

l'idéal est pondre *á* un essence A_n d'anneau nilpotent (ou d' anneaux nul) tels que $cl(A_n) \longrightarrow \infty, n \longrightarrow \infty$ et prendre $A = \bigoplus_{n\geqslant 0} A_n$ (si A_n est que juste nul, on suppose :

$$\exists f(n) \in \mathbb{N}, x^{f(n)} \neq 0, \quad \text{et } f(n) \longrightarrow \infty \quad \text{comme } n \longrightarrow \infty$$

A est nul, en effet, soit $x = (x_0, x_1, ..., x_k, ...)$ un élément de A pour

$$m > cl(A_i),\ 0 \leq i \leq k. \quad \text{on a } x^m = (x_0^m, x_1^m, ..., x_k^m, 0...)$$

Si A est nilpotent alors $\exists c : A^C = 0$, alors $A^C = \bigoplus_{n\geq 0} A_n^c = 0$. Ainsi $\bigoplus A_n^c = 0 \forall n$ alors $cl(A_n) \leq c$.

Remarque 2.2.8

1. A est nil s'il y a un n tel que $r^n = 0$ pour chaque $r \in A$.
2. A est nilpotent s'il y a un n tel que $r_1 r_2 ... r_n = 0$ pour chaque $r_1, r_2, ...r_n \in A$.
3. Un anneau A est localement nilpotent si chaque sous-anneau finiment généré est nilpotent.

Le radical nil N(A) est la somme de tous les idéaux nil dans A. Où : N(A) est le plus grand idéaux nil dans A. Le radical localement nilpotent L(A), le radical est un somme de tous les idéaux localement nilpotent dans A.

Preuve. Radical nil inférieur $nil_x(A)$ est le plus petit idéal semi-premier de A, et est égale *à* l'intersection de tous les idéaux premiers de A. $Nil_x(A) = 0 \Leftrightarrow$ A a aucun des idéaux nilpotent non zéro.
Soit A un anneau s'appelle Radical Jacobson (ou quasi régulier) si $\forall\ r \in A$, $\exists \grave{r} \in A$, où $r + \grave{r} + r\grave{r} = 0$. Le radical jacobson d'anneau A est le plus grand idéal quasi régulier de A. il est note par $J(A)$, pour chaque anneau A, $Nil_x(A) \subset N(A) \subset J(A)$. ■

2.3 Le Radical Jacobson

Soit A un anneau, l'intersection des idéaux maximaux à gauche de A est appelé le radical Jacobson de R et est noté $Jac(A)$. On dit qu'un anneau est semi-simple si $Jac(A) = 0$.

2.4 Théorème d'Artin Wedderburn

Définition 2.4.1 [8] L'anneau est dit semi-semple si J(A)={0}. Soit E un ensemble, les conditions suivantes sont équivalentes.

1. chaque sérié décroissante ... $\leq x_n \leq x_{n-1}... \leq x_2 \leq x_1$ des l'éléments de E est stable.

2. chaque sous-ensemble $S \subseteq E$ non vide est des éléments minimaux.

Définition 2.4.2 Si E satisfait les conditions équivalences ci-dessus, on dit que E est un **artinien**
en duelle condition qui suivent sont équivalentes :

1. chaque séquence en cours $x_1 \leq x_2... \leq x_{n-1} \leq x_n \leq ....$

2. toute non vide $S \subseteq E$ a un max élément

Définition 2.4.3 Si les conditions ci-dessus sont remplies, on dit que E est un **noethérien**.

Définition 2.4.4 Un anneau A est un gauche artinien(droite), si le supposer des idéaux de gauche, les quelques identifions s'appliquent pour (noethérien) au lieu de (artinien).

Lemme 2.4.5 ***(Schur)*** Soient M_1 et M_2 des R-modules a gauche simples.

1. Si $M := M_1 = M_2$, alors $End_A(M)$ est un corps.

2. Si $M_1 \ncong M_2$, alors $Hom_A(M_1; M_2) = 0$.

Preuve. Pour la preuve il suffit de se rappeler le fait que le noyau et l'image d'un morphisme sont des sous-modules et les seuls sous modules d'un module simple...

Remarque 2.4.6 Si $\phi : M_2 \cong M_1$, alors $Hom_A(M_1; M_2)$ est aussi un corps pour le produit défini par $f.g := f \circ \phi \circ g$.

■

Définition 2.4.7 Un anneau A est semi-simple *à* droite si le A-module A est semi-simple.

Remarque 2.4.8 On verra binetôt que A est semi-simple si et seulement si A est semi-simple.

Lemme 2.4.9 Soit A un anneau semi-simple *à* droite. Un module M est simple si et seulement si M est isomorphe á un idéal á droite minimal de A.

Preuve.
Un idéal *à* droite minimal est toujours simple. Réciproquement, si A est semi simple et M est simple alors il existe un idéal *à* droite maximal M de A tel que $M \cong A/M$ puisque A est semi-simple, on a $A = M \oplus I$ et I est alors un idéal *à* droite minimal de A.
On a en outre $M \cong A/M \cong I$. ■

Theoreme 2.4.10 ***(d'Artin Wedderburn)*** Soit A un anneau, les assertions suivantes sont équivalentes :

1. A est semi-simple.
2. Tout A-module simple *à* droite est semi-simple.
3. Tout idéal *à* droite de A est un facteur direct de A.
4. $A \cong \prod_{i=1}^{t} M_{n_i}(K_i)$, où les K_i sont des corps (éventuellement non commutatifs) et l'isomorphisme est un isomorphisme d'anneaux.

Preuve.
1) $\Rightarrow$ 2) Si A est semi-simple, tout A-module *à à* droite libre est semi-simple. Or tout A-module *à* droite est quotient d'un A-module droite libre. L'exercice permet alors de conclure.
2) $\Rightarrow$ 1) C'est clair .
1) $\Leftrightarrow$ 3) C'est aussi clair .
1) $\Rightarrow$ 4) A est par hypothèse une somme directe de A-module simple : $A = \bigoplus_{\lambda \in \Lambda} S_\lambda$, où

les S_λ sont simples. On peut donc écrire $1 = \Sigma_{i=1}^{t} e_{\lambda_i}$ et on a $S_\lambda = e_{\lambda_i} A$. Pour tout $a \in A$ on a alors $a = 1.a = \sum_t^{i=1} e_{\lambda_i} a$, ce qui montre que l'on a en fait

$$A = \bigoplus_{i=1}^{t} S_{\lambda_i} = \bigoplus_{i=1}^{t} (\bigoplus_{k=1}^{n_i} S_{k,i})$$

avec $\sum_t^{i=1} n_i = l$ et où l'on a regroupe les modules simples isomorphes : $S_{ki} \cong S_{ki}$, pour tout $k; ketS_{ki} \ncong S_{kJ}$ si $i \neq j$. On a en particulier $Hom_A(S_{ki}, S_{kJ}) = 0$ si $i \neq j$. En posant $M_i := \bigoplus_{k=1}^{n_i}$, on a

- $Hom_A(M_i; M_j) = 0$ si $i \neq j$, et
- $A \cong End(A) \cong End_A(\bigoplus M_i) \cong \Pi_{i=1}^{t} End_A(M_i) \cong \Pi_{i=1}^{t} M_{n_i}(End_A S_{li})$.

Le lemme de Schur montre alors que les $K_i = End_A S_{1i}$ sont des corps.
4) $\Rightarrow$ 1) Fixons $i \in \{1, ..., t\}$. On a

$$M_{ni}(K_i) = \bigoplus_{n_i}^{k=1} e_{kk}^{(i)} M_{n_i}(K_i)$$

où $e_{kk}^{(i)}$ désigne la matrice à coefficients dans K_i ayant des 0 partout sauf en position kk où elle vaut 1. On montre que $I_k := e_{kk}^{(i)} M_{n_i}(K_i)$ est un $M_{n_i}(Ki)$-module simple et on en déduit facilement que $M_{n_i}(Ki)$ est un anneau semi-simple, il est simple mais tous les anneaux simples ne sont pas semi-simples. ■

Chapitre 3

Application des groupes de Golod-Shafarevich pour répondre négativement aux problème de Burnside

3.1 Limite projective

Définition 3.1.1 [9] Soit (G_i, φ_{ij}) Un système projectif de groupe.on appelle limite projective de ce système tout groupe G avec des homomorphismes $f_i : G \longrightarrow G_i$ vérifiant :

$$\begin{tikzcd} H \arrow[r, "f_j"'] \arrow[d, "f_i"'] & G_j \arrow[dl, "\varphi_{ij}"] \\ G_i & \end{tikzcd}$$

c'est *à* dire, $\varphi_{ij} \circ f_i = f_i$, pour tous $i \leqslant j$; et vérifiant la propriété universelle : pour toute famille de morphismes de groupes $g_i : H \longrightarrow G_i$ qui vérifie le diagramme commutatif

$$\begin{tikzcd} G \arrow[r, "g_j"'] \arrow[d, "g_i"'] & G_j \arrow[dl, "\varphi_{ij}"] \\ G_i & \end{tikzcd}$$

il existe un homomorphisme de groupe unique $g : H \longrightarrow G$ tel que le diagramme suivant soit commutatif

$$\begin{tikzcd} H \arrow[r, "g"'] \arrow[d, "g_i"'] & G \arrow[dl, "f_i"] \\ G_i & \end{tikzcd}$$

la propriété universelle ci-dessus assure que si une limite projective existe alors elle est unique. On va la note par $G = \varprojlim G_i$.

Theoreme 3.1.2 La limite projective de n'importe quel système projective existe alors elle est unique.

Preuve. Soit (G_i, φ_{ij})un système projectif de groupe. Considérons G le sous-ensemble de $\prod_{i\in I} G_i$ défini par :

$$G = \{(x_i) \in \prod_{i\in I} G_i / \varphi_{ij}(x_i) = x_i, \forall i \leq j\}$$

Il résulte immédiatement que G est un sous-groupe de $\prod_{i\in I} G_i$.

Pour chaque $i \in I$ définissons $\pi_i : G \longrightarrow G_i$ par $\pi_i((x_i)_{j\in I}) = x_i$ (la projection sur G_i). Si $i \leq j$, alors :

$$\begin{tikzcd} G \arrow[r, "\pi_j"'] \arrow[d, "\pi_i"'] & G_j \arrow[dl, "\varphi_{ij}"] \\ G_i & \end{tikzcd}$$

$$\varphi_{ij}\pi_j((x_i)_{k\in I}) = \varphi_{ij}(x_j) = x_i = \pi_i((x_k)_{k\in I}).$$

Ainsi le diagramme ci-dessus est commutatif. Soit maintenant $\{g_i : H \longrightarrow G_i\}$ une famille de morphisme tels que pour tous $i \leq j$:

$$\begin{tikzcd} H \arrow[r, "g_j"'] \arrow[d, "g_i"'] & G_j \arrow[dl, "\varphi_{ij}"] \\ G_i & \end{tikzcd}$$

on définir $g : H \longrightarrow G$ par $g(x) = (g_i(x))_{i\in I}$. Cette application est bien définie car

$$\varphi_{ij}(g_j(x)) = g_i(x),\ \forall i \leq j.$$

et g est un homomorphisme de car les g_i le sont ; et par définition on a $\pi_i(g(x)) = g_i(x)$. Ile reste à démontrer l'unicité de g. Supposons que $f : H \longrightarrow G$ vérifie $\pi_i \circ f = g_i$. Alors $f(x) = (\prod_i(f(x)))_{i\in I} = (g_i(x))$. ■

Ayant un système projectif de groupe finis (G_i, φ_{ij}). On peut munir chaque G_i de la topologie discrète, et le théorème de Tychonoff assure que $\prod_i G_i$ est un groupe compact.

Lemme 3.1.3 Soit (G_i, φ_{ij}) un système projective de groupe finis.Alors $\underleftarrow{lim} G_i$ est un sous-groupe fermé donc compact.

Preuve. Montrons que $\underleftarrow{lim} G_i$ est fermé dans $\prod_i G_i$ ou d'une façon équivalente que son complémentaire C dans $\prod_i G_i$ est ouvert. Soit $g = (x_i) \in C$; par définition de $\underleftarrow{lim} G_i$, il existe $i \leq j$ tel que $\varphi_{x_i} \neq x_i$. Soit $U = \prod_{k\in I} U_k$, ou $U_i = 1$ si $k = i$ et j et $U_k = G_k$ sinon. Donc U est ouvert dans $\prod_i G_i$; et ainsi gU est un voisinage de g. De plus $gU \bigcap \underleftarrow{lim} = \emptyset$. D'où $gU \subseteq G$. Ceci montre que C est ouvert.

Maintenant, comme $\prod_i G_i$ est compact et $\underleftarrow{lim} G_i$ est fermé dans $\prod_i G_i$; On a $\underleftarrow{lim} G_i$ est compact. ■

3.2 Groupe Topologique

Définition 3.2.1 [7] On appelle groupe topologique un ensemble G muni d'une structure de groupe et d'une topologie satisfaisant aux deux axiomes suivants :

1. L'application $(x, y) \longmapsto xy$ de $G \times G$ dans G est continue.

2. L'application $x \longmapsto x^{-1}$ de G dans G est continue.

Une structure de groupe et une structure topologique étant données sur un ensemble G, on dira qu'elles sont compatibles si elles satisfont *à* (1)et (2).

Exemple 3.2.2

1. sur un groupe G, la topologie discrète est compatible avec la structure du groupe ; un groupe topologique dont la topologie est discrète est appelé groupe discret.
   De même, la topologie sur G est compatible avec la structure de groupe G.

2. Si G est un groupe topologique, sa topologie est compatible avec la structure du groupe G^0 opposé *à* G ; on dit que G^0, muni de cette topologique, est le groupe topologique opposé au groupe topologique G.

3.3 Groupe profinis

Définition 3.3.1 [7] Un groupe profinis est la limite inverse des groupes finis.

Définition 3.3.2 [5]

Soit $I = (I, \leqslant)$ un ensemble partiellement ordonné tel que les conditions suivantes sont satisfaites :

- $i \leqslant i$, pour $i \in I$;
- $i \leqslant j$ et $j \leqslant k$ impliquent $i \leqslant k$, pour $i, j, k \in I$;
- $i \leqslant j$ et $j \leqslant i$ impliquent i = j, pour $i, j \in I$; et
- si $i, j \in I$, il existe des $k \in I$ tels que $i, j \leqslant k$.

Le système inverse (projectif) d'un espace topologique X (groupes topologiques) sur I, est

- la collection $\{X_i \ / \ i \in I\}$ d'espace X (groupe topologique) indice par I,

$$\varphi_i : X \to X_i$$

Exemple 3.3.3

$$f : R \to [0,1]$$
$$x \mapsto x^2$$
$$f/[-1,1] : [-1,1] \to [0,1]$$
$$x \to x^2$$

- la collection des applications continues. (homomorphismes de groupes)

$$\{\varphi_{ij} \ / \ i,j \in I\}; \quad \varphi_{ij} : X_i \longrightarrow X_j$$

$\forall i \geqslant j$, tel que le diagramme suivant commute

$$\begin{tikzcd} X_i \arrow[r, "\varphi_{ik}"'] \arrow[d, "\varphi_{ij}"'] & X_k \\ X_j \arrow[ur, "\varphi_{jk}"'] & \end{tikzcd}$$

Donc : $\varphi_{ik} = \varphi_{ik} \circ \varphi_{ij} \quad i,j,k \in I. \ \ \forall \ \ i \geqslant j \geqslant k.$

ainsi φ_{ii} est d'identité id_{X_i}

$$\varphi_{ii} : X_i \longrightarrow X_i$$

ce système se note par $\{X_i, \varphi_{ij}, I\}$. **La limite inverse (limite projective)**

$$X = \varprojlim_{i \in I} X_i$$

pour le système $\{X_i, \varphi_{ij}, I\}$ est le sous-espace (sous-groupe) X de produit directe $\prod_{i \in I} X_i$

$$X \subseteq \prod_{i \in I} X_i$$

on a : $X = \{X_i, X_j, X_k, ...\}$

Exemple 3.3.4 $\mathbb{Z}/2\mathbb{Z} \cdot \mathbb{Z}/3\mathbb{Z} \cdot .. \cdot \mathbb{Z}/p^n\mathbb{Z} = \prod_{i=2}^{p^n} \mathbb{Z}/i^n\mathbb{Z} \Longrightarrow \mathbb{Z} \subseteq \prod_{i=2}^{p^n} \mathbb{Z}/i^n\mathbb{Z}$ *telque :* $\hat{Z} = \lim\limits_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$.

$\varphi_{ij}(x_i) = x_j$, si $i \geqslant j$. on suppose que X a une topologie induit par la topologie de produit. $\forall\ i \in I \quad \varphi_i : X \longrightarrow X_i$ c'est la restriction de la projection canonique $\prod_{i \in I} X_i \longrightarrow Xi \Rightarrow \varphi_j$ est continue$\varphi_{ij}\varphi_i = \varphi_j$ et ($j < i$), d'où la propriété universelle.

Proposition 3.3.5 ***(Universelle de Limite Inverse)*** Supposons Y un espace topologie (respectivement groupe), et $\psi_i : Y \longrightarrow X_i$ $(i \in I)$ continue (respectivement homomorphismes continu) tel que $\varphi_{ij}\psi_i = \psi_j$ $(j < i)$. D'apré, il existe unique une application continue (respectivement homomorphisme) $\psi_i : Y \longrightarrow X\ \forall\ i \in I$, le diagramme suivant commute

$$\begin{tikzcd} Y \arrow[r, dotted, "\psi"] \arrow[dr, "\psi_i"'] & X \arrow[d, "\varphi_i"] \\ & X_i \end{tikzcd}$$

Soit $\mathcal{C}$ une collection non vide (de classe d'isomorphisme) de groupe fermé fini ,est appelle des sous-groupes, les images homomorphes et des produits directs finîtes (Par fois le $\mathcal{C}$ est un groupe de variété de groupe fini. Si en plus on suppose cela, chaque fois que $A, B \in \mathcal{C}$ et

$$1 \longrightarrow G \longrightarrow B \longrightarrow 1 \quad \text{est une groupe exacte}$$

, alors $G \in \mathcal{C}$, on dit que $\mathcal{C}$ est un variété d'extension fermé des groupes finis. Par exemple

1. la collection de tous les groupes finis ;
2. la collection de tous les p-groupes finis (pour un p prime fixé) ;
3. la collection de tous les groupes nilpotent fini.

Notez que (1) et (2) sont variétés d'extension fermes des groupes finis, mais (3) est une variété des groupes finis que n'est pas extension Soit $\mathcal{C}$ une variété de groupes finis ; et

soit $\{X_i, \varphi_{ij}, I\}$ est un système inverse de groupes dans $\mathcal{C}$ ouvre d'indice I, alors on dit que

$$G = \varprojlim_{i \in I} G_i$$

est un pro-$\mathcal{C}$ groupe. Si $\mathcal{C}$ est un (1), (2) ou (3) ci-dessus, donc en dit que G est, respectivement, un profinite groupe, un pro-p groupe ou un pro-nilpotente groupe.

3.4 Exemple de Groupe Profinis

1. Au lieu de considérer tous les sous-groupes normaux d'indice fini de G, on peut considérer seulement les sous-groupes U de G dont l'indice est une puissance d'un nombre premier fixé p. Le groupe profinite $\varprojlim G/U$ (U parcourt l'ensemble des sous-groupes de G tels que $\mid G : U \mid = p^u, u \in \mathbb{N}$) s'appelle la pro-$p$ complétion de G. L'exexmple typique ici étant $\mathbb{Z}_p = \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}$, la pro-$p$ complétion de $\mathbb{Z}$. En fait $\mathbb{Z}_p$ est un anneau, qui s'appelle l'anneau des entiers p-adiques. le corps des fraction de $\mathbb{Z}_p$ est noté $\mathbb{Q}_p$ et est appelé le corps des nombres p-adiques.

2. Soit G un groupe. Considérez la collection

$$\mathcal{N} = \{N \triangleleft G \mid G/N \in \mathcal{C}\}$$

et on dit que le pro-$\mathcal{C}$ groupe

$$G_{\hat{\mathcal{C}}} = \varprojlim_{N \in \mathcal{N}} G/N$$

est un pro-$\mathcal{C}$ completion de G. En particulier, nous utilisons les termes profinis completion, le pro-p completion. Le profinis et pro-p completion de groupe de G apparaissent assez fréquemment, et ils seront généralement désignés par $\hat{\mathrm{G}}$, et $G_{\hat{p}}$ respectivement.

3.5 Algèbre de Groupe

Définition 3.5.1 [1] Soit G un groupe fini. On défini F[G] comme un ensemble de formule somme :

$$u = \sum_{g \in G} \lambda_g g, \ \lambda_g \in F$$

Donné de deux opérations : addition et produit définies comme suit :

$$\sum_{g\in G}\lambda_g g+\sum_{g\in G}\mu_g g=\sum_{g\in G}(\lambda_g+\mu_g)g$$

et

$$\sum_{g\in G}\lambda_g g\times\sum_{g\in G}\mu_g g=\sum_{g\in G,h\in G}(\lambda_g\mu_{h^{-1}g})g$$

Noter que la produit est un induit par produit dans G, F et linéarités.

La proposition suivante est gauche au lecteur.

Proposition 3.5.2 L'ensemble $(F[G],+,\times)$ est un anneau et est un F-espace de vecteur de dimension |G| avec la produit scalaire compatible avec le groupe opération. Donc F[G] est un F-algèbre.

L'algèbre F[G] est non commutative si le groupe G est commutative. Il est clair que les éléments de base (les éléments de G) sont inversibles dans F[G].

3.6 Présentation par Générateurs et Relateurs

Définition 3.6.1 [2] Soient G un groupe, et X élément de G est appelé générateur de G et dénoté $G=\langle X\rangle$, tel que chaque élément de G est un produit des éléments de X et leur inverses :

$$g=x_1^{\varepsilon_1}.x_2^{\varepsilon_2}...x_d^{\varepsilon_d},\ g^{-1}=x_d^{-\varepsilon_d}...x_2^{-\varepsilon_2}.x_1^{-\varepsilon_1}.\quad \textit{tel que } g,g^{-1}\in G$$

Le nombre majeure d'éléments pour le produire de G s'appelle parfois le rang de G et est dénoté par le $d(G)$, et écrire : $d(G)=Rang(G)$. En particulier, soit G un groupe abélien

$$Rang(G)=d(G/H)$$

tel que : H sous-groupe de torsion $(h\in H,h^{\alpha}=0)$.

Soient $G=\langle X\rangle$ et $\hat{X}$ un système des caractères tel que il y a **un bijection** de $\hat{X}\to X$, les caractères $X,Y,Z,A,B,C,..$ des éléments de $\hat{X}$ et les caractères $x,y,z,a,b,c,..$ des éléments de X, tel que :

$$\hat{X} \to X$$
$$X \to x$$
$$Y \to y$$
$$Z \to z$$
$$\vdots$$
$$\vdots$$

Un mot (ouvre $\hat{X}$) est expression de la formule

$$W \equiv W(\hat{X}) \equiv X_1^{\varepsilon_1} X_2^{\varepsilon_2} ... X_k^{\varepsilon_k} \equiv \prod_{j=1}^{k} X_j^{\varepsilon_j}$$

tel que $X_1, ..., X_k \in \hat{X}$, et $\varepsilon_1, .., \varepsilon_k \in \{-1, 1\}$, tel que :

$$X_k^{\varepsilon_k} = \begin{cases} X_k \\ X_k^{-1} \end{cases}$$

tel que k : est la longueur de mot W, dénoté comme $k = |W|$.

Exemple 3.6.2 • Soit $W = ABC^{-1}DEF^{-1}C = g \in G$ tel que : $|W| = 7$

- $g = W(X) = \prod_{j=1}^{k} x_j^{\varepsilon_j}$ $\varepsilon_j = \begin{cases} +1 \\ -1 \end{cases}$
- $h = V(\hat{X})$, d'où : $h = C^{-1}BDEF^{-1}$, tel que : $|V| = 5$

$$\begin{aligned} W(\hat{X})V(\hat{X}) \equiv WV &= ABC^{-1}DEF^{-1}CC^{-1}BDEF^{-1} \\ &= ABC^{-1}DEF^{-1}BDEF^{-1} \end{aligned}$$

$|WV| = 10$.

Le mot inverse de $W(\hat{X})$ est un mot $W(\hat{X})^{-1} \equiv X_k^{-\varepsilon_k} ... X_2^{-\varepsilon_2} X_1^{-\varepsilon_1}$ et dénoté g^{-1}. Le mot vide ne se composant d'aucune caractère et dénoter par 1 ; il a la longueur 0 et définit l'élément neutre de G. Deux des mots V et W s'appellent librement équivalents si $W = ABB^{-1}E$ et $V = AE$, et écrit $V \equiv W$.

Un mot $R(\hat{X}) = X_1^{\varepsilon_1} ... X^{\varepsilon_k}$ s'appelle un relateur si $x_1^{\varepsilon_1} ... x^{\varepsilon_k} = 1$ dans G. Un relateur trivial est libre l'équivalent au mot vide, on a s'écrit : l(ϕ)=$|\phi| = 0$. Comme indiqué, la notion

d'un relateur dépend du groupe G et du système des générateurs. Donné un système se générateurs X pour G, il est souvent commode d'identifier $\hat{X}$ avec $\hat{X}$.
Si X est un générateur du groupe G et R est un relateur, donc $\langle X|R\rangle$ s'appelle par une **présentation** de G et il écrire

$$G = \langle X|R\rangle$$

.

D'autres formes sont également employées :

- $G = \langle (x_i)_{j\in J}|(R_k(\hat{X}))_{k\in K}\rangle$
- $G = \langle S_1, ..., S_n|R_1, ..., R_q\rangle$
- $G = \langle s_1, ..., s_n|-\rangle$: de relateur d'un l'ensemble vide.

Le groupe G s'appelle présentation avec de générateur et de relateur.

Exemple 3.6.3

1. Soit $G = (\mathbb{Z}, +)$, avec le générateur simple 1. Soit X se composer d'une caractère A. Puis que les mots possibles sont des formes

$$W \equiv A^{\varepsilon_1} \cdot A^{\varepsilon_2} \cdot ... \cdot A^{\varepsilon_k} \equiv A^{n_1} \cdot A^{n_2} \cdot ... \cdot A^{n_k} \quad \text{tel que} \;\; \varepsilon_j = \pm 1, n_j \in \mathbb{Z};$$

   dans cette dernière forme, nous rassemblons toutes les caractère consécutives avec le même indice ε, c'est $n_j \cdot n_{j+1} < 0$, (exemple : $-9 = 1^{-5}.1^{14}$). Clairement, W est librement équivalent au mot A^n où $n = \sum_{j=1}^{q} n^j$. Deux mots A^n et A^m, tel que $n, m \in \mathbb{Z}$, sont librement équivalents $\Leftrightarrow$ si $m = n$. Maintenant, A^n représente l'entier $n \in \mathbb{Z}$, et donc un mot $A^n = 1$ est un relateur $\Leftrightarrow n = 0$; $(A^0 = 1 \notin R,\ R$: est un le relateur) d'où il n'ya pas un relateur, donc le relateur est trivial. Donc $\mathbb{Z} = \langle A|-\rangle$.

2. Considérons le groupe

$$SL(2, \mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) / a, b, c, d \in \mathbb{Z}, ad - bc = 1\},$$

   soit

- $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$,
- $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$,
- $AB = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$,
- $BA = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$
- $det(BA) = 1$, $det(AB) = 1$, $A = B^3$,

alors A et B engendré de $SL(2, \mathbb{Z})$,
$AB^{-3} = 1$, $A^4 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 1$ que vérifie la propriété que si relateur.

- $B^3 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = -Id$,
- $det(B^3) = 1$.

Alors les relateurs sont : $A^2 = B^3, A^4$, donc la présentation $SL(2, \mathbb{Z}) = \langle AB/A^2B^{-3}, A^4 \rangle$.

3.7 Séries Hilbert

D'après les précédons. Soient $a_n = dim_k A_n, \quad \forall n \in \mathbb{N}$ et r_n le nombre d'éléments de R où ont le longeur n.

Définition 3.7.1 Soit A une algèbre graduée associative sur l'anneau K. A est localement finie si seulement si A_n est un espace vectoriel de dimension finie sur K.
Pour $K\langle X \rangle_n$ est un sous-espace de dimension finie, on peut être supposer que $r_n < \infty$ (finie) $\forall n \in \mathbb{N}$

Définition 3.7.2 $\{a_n\}, \{r_n\}$ sont des série correspondance des séries Hilbert

$$\sum_{\infty}^{n=0} a_n t^n, \ \sum_{\infty}^{n=0} r_n t^n, \ \forall t \in R$$

.

3.8 Groupe de Torsion

- **Définition 3.8.1** [3]

- Dans un groupe, un élément est dit **de torsion** s'il est d'ordre fini, c'est-*à*-dire si l'une de ses puissances est l'**élément neutre**, i.e. : ($x^n = e$ ou $x^n = 0$), où :e : élément neutre, et x : élément de torsion.
- Un groupe est dit **sans torsion** si sa torsion ne contient que le neutre, c'est-*à*-dire si tout élément différent du neutre est d'ordre infini.

- **Définition 3.8.2** Un groupe abélien G est dit **de torsion** si tout élément de G est d'ordre fini (i.e. $\forall x \in G, \exists n \in \mathbb{Z}$ tel que $nx = 0$). Il dit **sans torsion** si tout élément, différent de l'élément neutre, est d'ordre infini (i.e. $\forall x \in G, x \neq 0,\ nx = 0$ implique $n = 0$).

- **Exemple 3.8.3**

  1. ($\mathbb{Z}$) est sans torsion. Plus généralement, un groupe abélien libre est sans torsion.
  2. tout groupe fini est de torsion.
  3. $(\mathbb{Q}/\mathbb{Z}, +)$ est de torsion.

3.9 Groupe de Golod-Shafarevich

Définition 3.9.1 [6] Soient $X = \{x_1, ..., x_d\}$ et $U = \{u_1, ..., u_d\}$ des ensembles finies de la même cardinale. Soient $F = F_{\hat{p}}(X)$ le pro-p groupe libre sur X, tel que :$F = \langle x_1 ... x_d \rangle$ et $\mathbb{F}_p\langle\langle U \rangle\rangle = \{\sum_{n=0}^{\infty} \lambda u_i^n\}$

$$i : F \to F_p\langle\langle U \rangle\rangle^{\times}$$
$$x_i \mapsto 1 + u_i$$

l'**Inclusion de Magnus**, i.e. : on a $(F \hookrightarrow \mathbb{F}_p\langle\langle u_1, \cdots, u_d \rangle\rangle^{\times})$. Et $\mathbb{F}_p\langle\langle u_1, \cdots, u_d \rangle\rangle^{\times}$ le groupe multiplication de $\mathbb{F}_p\langle\langle u_1, \cdots, u_d \rangle\rangle$, par exemple : W est un mot de F ; où :

$$W = x_1x_2x_3x_4 \mapsto (1 + u_1)(1 + u_2)(1 + u_3)(1 + u_3)(1 + u_4).$$

On définie la fonction degré de Zassenhaus par :

$$D : F \to \mathbb{N} \bigcup \{\infty\}$$
$$D(f) = deg(i(f) - 1),$$

- pour tout $f \in F(X)$ un ensemble, $D(f) = deg(i(f) - 1)$.

  $\star$**La Propriétés de base de la fonction degré D :**

- $D(f) \geqslant 1$ pour tout $f \in F(X)$
- $D([f, g]) \geq D(f) + D(g)$ où $[f, g] = f^{-1}g^{-1}fg$
- $D(f^p) = p.D(f)$ pour tout $f \in F(X)$.

où : deg est un degré habituel de série de puissance dans $u_1, ..., u_d$.

Définition 3.9.2 *1.* Un groupe G finiment généré est un groupe GS (Golod-Shafarevich) s'il a une présentation $\langle X/R \rangle$ avec la propriété suivante : il existe $0 < t < 1$ tel que :

$$1 - \mid X \mid t + H_R(t) < 0$$

où : $H_R(t) = \sum_{n=1}^{\infty} r_n t^n$ et $r_n = \mid \{r \in R : \quad \text{degré}(r) = n\} \mid$ où : $R = \cup_{n \geqslant 1} r_n$.

2. Un pro-p groupe G est un groupe Golod-Shafarevich (GS) s'il a une présentation satisfaire la condition de GS.

Exemple 3.9.3 $G = \langle a, b, c, d, f, g | ab = c, bc = d, cd = f, df = g, fg = a, ga = b \rangle$
Il facile de montrer qu'il existe un homomorphisme $\varphi : G \to Sym(Z)$ où : on remarque qu'il existe 6 relateurs et 6 générateurs, l'inégalité $r < (d^2)/4$ est versifier,

$$(6 < ((6^2)/4) = 9) \quad \text{danc est infini}$$

ce qui implique que G est de golod-shafarevich (d'après le corollaire 2.3 de [2])

$$\Rightarrow G \quad \text{est infini.}$$

Theoreme 3.9.4 ***(Golod)*** pour chaque p premier, et $d \geq 2$, il existe un groupe infini, d-générateur, p-torsion.

première preuve : Soit $K = \mathbb{F}_p$ un corps fini d'ordre p, et considérons l'algèbre A^+ est nil, et prenons A^+ l'image de $k\langle X \rangle^+$ dans A.

$$\varphi : K\langle X \rangle \to A$$
$$K\langle X \rangle^+ \mapsto A^+$$

Comme l'algèbre A^+ est un d-générée et nil, et K a la caractéristique p, l'ensemble $1 + A^+ = \{1 + a : a \in A^+\}$ est un groupe de p-torsion. Nous montrons le sous-groupe Γ de $1 + A^+$ engendré par $1 + u_1, 1 + u_2, ..., 1 + u_d$ est infini, tel que $U = \{u_1, u_2, ..., u_d\}$ et $K\langle X \rangle^+ = \{f_1, f_2, ..\}$, et (donc satisfait toutes les propriétés requises).
l'application d'inclusion $i : \Gamma \to A^+$ induit un homomorphisme $i_* : \mathbb{F}_p[\Gamma] \to A$ (où $\mathbb{F}_p[\Gamma]$ est un $\mathbb{F}_p$-algèbre de groupe de Γ). l'image de i_* contient 1 et $1 + u_i$. pour tout i, alors i_* est surjective. Comme, A est de dimension infini, alors forcément $\mathbb{F}_p[\Gamma]$ est infini, d'où Γ est infini.
Deuxième preuve : Cette fois-ci on a introduit la notion des groupes de Golod-Shafarevich. Soient X un ensemble fini avec $|X| = d$ et $F = F(X)$ le groupe libre sur X, tel que F est dénombrable, où $F = \{f_1, f_2, ...\}$. Maintenant prendre un séquence de entiers $n_1, n_2, ...,$, et

considérer un groupe $G\langle X/R\rangle$ où $R = \{f_1^{p^{n_1}}, f_2^{p^{n_2}}, ...\}$. Par construction, G est p-torsion. Il est facile de voir que $D(f^{p^k}) = D(f)^{p^k}$ pour tout $f \in F$, pour tout $\tau \in (0,1)$ on a

$$1 - |X|\tau + H_R(\tau) \leqslant 1 - |X|\tau + \sum_{i=1}^{\infty} \tau^{p^{n_i}}$$

Maintenant fixer $\tau \in (1/|X|, 1)$. Ensuite $1 - |X|\tau < 0$, donc on peut choisir la séquence $\{n_i\}$ tel que $\sum_{i=1}^{\infty} \tau^{p^{n_i}} < -(1 - |X|\tau)$. Alors G est Golod-Shafarevich et donc infini. □

Theoreme 3.9.5 ***(Golod)*** Pour tout nombre premier p, et un entier $d \geqslant 2$, il existe un groupe infini, d-générateur, p-torsion, tel que les sous groupes à $(d-1)$ générateurs sont finis.

i.e. On a $(H \subseteq G)$:

$$g^p = e \ (e : \quad \text{est neutre}), \ \infty = |G| = | < g_1, ..., g_d > |$$
$$\bigcup$$
$$\infty > |H| = | < h_1, ..., h_{d-1} > |$$

Preuve. Prenez n'importe quel ensemble X avec $|X| = d$, et construit un groupe p-torsion G de Golod-Shafarevich avec l'exigence supplémentaire que $1 - |X|\tau + H_R(\tau) < 0$ pour certain $\tau \in (1/d, 1/d - 1)$. Soit $\varepsilon = -(1 - |X|\tau + H_R(\tau))$ et $\delta = \tau(d-1)$. Depuis $\delta < 1$ On peut trouver une suite entière $\{m_i\}$ tel que $\sum_{i=1}^{\infty} \delta^{m_i} \preceq \varepsilon$.

Soit $\Omega = \{\omega^{(1)}, \omega^{(2)}, ...\}$ l'ensemble de tous les ordres $(d-1)$ d'éléments de $F(X)$ (le groupe libre sur X). Si $\omega^{(i)} = (f_1^{(i)}, ..., f_{(d-1)}^{(i)})$, soit R_i l'ensemble de tous les commutateur normal à gauche de longueur m_i impliquant $f_1^{(i)}, ..., f_{(d-1)}^{(i)}$. Nous dire ce le groupe $G' = \langle X | R \cup \bigcup_{i \geqslant 1} R_i \rangle$ a le propriétés indépendant. Par la construction, chaque (d-1)-généré sous-groupe de G' est nilpotent et p-torsion (puisque G' est un quotient de G) et d'où fini. Si $c = [y_1, ..., y_m]$ est un normal à gauche et commutateur de longueur m, $D(c) \geqslant D(y_1) + ... + D(y_m)$. Dons, si $S_i = \{(y_1, ..., y_{m_i}) : y_j \in \{f_1^{(i)}, ..., f_{d-1}^{(i)}\}\}$, puis

$$H_{R_i}(\tau) \leqslant \sum_{(y_1,...,y_{m_i}) \in S_i} \tau^{D(y_1)+...+D(y_{m_i})} \leqslant (\sum_{j=1}^{d-1} \tau^{D_j^{f^{(i)}}})^{m_i} \leqslant (\tau(d-1))^{m_i} = \delta^{m_i}.$$

Dons, si $1 - |X|\tau + H_R(\tau) + \sum_{i \geqslant 1} H_{R_i}(\tau) < 0$, ainsi G' est Golod Shafarevich infini. ■

3.10 Exemple de groupe de Golod-Shafarevich

- **Proposition :[4]** Soit S un ensemble fini des nombres premier.

$$G_S = \langle x_1, ..., x_m | x_i^{p^{K_i}} = [x_i, a_i], 1 \leqslant i < m \rangle \quad m = |S|$$

Alors : G_S est un groupe de Golod-Shafarevich, $\forall\ m \geqslant 4$

- **Preuve.** pour montrer que G_S est G-S, il suffit de vérifier que :

$$1 - |X|\tau + H_R(\tau) < 0 \qquad \dashrightarrow (*)$$

où $|X| = m$, et $H_R(\tau) = \sum_{n=1}^{\infty} r_n t^n$, d'après G_S, on a :

$$x_i^{p^{k_i}}.a_i.x_i.a_i^{-1}.x_i^{-1} = e, \quad \text{d'où } (*).$$

Alors G_S est G-S ■

Conclusion

La naissance des groupes appelés groupe des Golod-Shafarevich, en 1964 a donné un grand horizon pour la théorie combinatoire des groupes, ainsi la théorie des nombres, en particulier $\langle\langle$ Class field tower problem $\rangle\rangle$.
A l'aide de cette catégorie des groupes on a répondu négativement *à* la conjecture de Burnside, utilisant le théorème de Golod avec deux versions, et trois de démonstrations.
Notre espoir au future c'est à répondre *à* la question ouverte suivante :
Établir des nouvelles résultat concernant les groupes de Golod-Shafarevich de caractéristique zéro.

Bibliographie

[1] Joseph J. Rotman, Advanced Modern Algebra, Prentice Hall ; 1st edition (2002) ; 2nd printing (2003), page(521).

[2] A.N.Parshin I.R.Shafarevich, Algebra VIII Combinatorial Group Theory Applications to Geometry, Title of the Russian edition : Itogi nauki i tekhniki, Sovremennye problemy matematiki, Fundamental'nye napravleniya, Vol. 58, Algebra 7 Publisher VINITI. Moscow 1990.

[3] Daniel Guin et Thomas Hausberger, Algebre I, october 2008- N d'imprimeur :807088, Imprimé en france.

[4] Efim Zelmanov, SOME OPEN PROBLEMS IN THE THEORY OF INFINITE DIMENSIONAL ALGEBRAS, (2007), No. 5, pp. 1185-1195.

[5] Luis Ribes Introduction to Profinite Groupe,School of Mathematics and Statistics, Carleton University, Ottawa ON K1V 8N2 Canada, Volume 22 (2013), 179-230.

[6] MIKHAIL ERSHOV, GOLOD-SHAFAREVICH GROUPE : A SURVEY, Received 14, January 2012, Accepted 2 April 2012, Department of Mathematics, University of Virginia, Published 29 May 2012.

[7] N.Bourbaki Elemente de Mathématique, Topologie Générale, Chapitre 1 *á* 4 ; N. Bourbaki, Réimpression inchangée de l'édition originale de 1959, Springer-Verlag Berlin Heidelberg 2007.

[8] N. Bourbaki Algèbre Chapitres 1-3, 2éme ed. Réimpression inchangée de l'édition originale de 1970, Masson, Paris 1970, N.Bourbaki, 1981 N.Bourbaki et Spring-Verlag Berlin H eidelberg 2007.

[9] Supervisé par laprof. Eva Bayer Fluckiger, Assistant responsable. Daniel Arnold MOLDOVAN, Introduction *à* la géométrie algébrique, Ecole polytechnique federale de lausanne (SMA), (1er novembre 2011)

ملخص

و بفضل زمر قولود-شافارفيش تحصلنا على إجابة للسؤال الذي ظل عالقا منذ أمد بعيد و هو :

أ صحيح وجود زمرة غير منتهية لها عدد منته

من المولدات و قابلة للفتل بمقاس P ؟

Résumé

A l'aide des groupes de

Golod-Shafarevich on a obtenu la réponse de question dit que :

Est-il-vrai qu'il existe un groupe infini, a

d-générateurs, p-torsion ?

Abstract

Thanks to Golod-Shafarevich groups wich have given us the :

Is-it-true that exists infinite

d-generated p-torsion group?