L'inégalité de Golod et Shafarevich

Boughattas Elyes et Zhang Haowen
Encadré par Izquierdo Diego

Juin 2017

Résumé

On commence par introduire quelques notions sur la catégorie des groupes profinis et leur cohomologie. Ensuite, on introduit les différents termes de l'inégalité de Golod et Shafarevich, qu'on montre de deux manières : la première preuve repose sur des arguments de cohomologie et la deuxième sur des arguments algébriques sur les séries formelles non commutatives. On finit par donner un contre-exemple au problème de Burnside.

L'objet de la théorie combinatoire des groupes est d'étudier les présentations d'un groupe par générateurs et relations. Nous nous intéressons ici à un raffinement d'une inégalité montrée en 1964 par Golod et Shafarevich dans le cadre des p-groupes. Dans sa version algébrique, elle s'énonce comme suit :

Théorème 0.0.1 *Soient p un nombre premier et G un p-groupe. Si $\mathfrak{d}$ est le nombre minimal de générateurs de G et $\mathfrak{r}$ le nombre minimal de relations R telles que $< \mathfrak{d}|R >$ est une présentation de G, alors*

$$\mathfrak{r} > \frac{\mathfrak{d}^2}{4}.$$

Nous montrons en fait un énoncé topologique de cette inégalité, que nous énonçons dans la section 4. À cet effet, nous introduisons dans la section 1 une catégorie de groupes topologiques plus large que celle des p-groupes, appelée la catégorie des pro-p groupes.

Nous donnons ensuite deux preuves de cette inégalité. La première, présentée dans la section 5, utilise des arguments de cohomologie et a été trouvée par Roquette en 1967 dans [8]. La deuxième, présentée dans la section 6, repose sur des arguments algébriques sur les séries formelles non commutatives : elle est plus fidèle aux arguments utilisés par Golod et Shafarevich dans [2].

Dans leur article, Golod et Shafarevich utilisèrent cette inégalité pour construire le premier contre-exemple au *problème de Burnside*, lequel était resté un problème ouvert depuis 1902. Il s'énonce comme suit :

Question 0.0.1 *Un groupe finiment engendré dont tout élément est d'ordre fini est-il fini?*

En vue de présenter une construction plus générale du contre-exemple donné en 1964, nous suivons la démarche suggérée par Ershov dans [1] pour aboutir à un critère de finitude des pro-p groupes. Nous en déduisons ensuite dans la section 7 un contre-exemple au problème de Burnside.

Table des Matières

1 Préambule sur les groupes profinis

Cette partie introduit une classe de groupes topologiques qui sont utilisés dans la suite.

1.1 Limite projective

Commençons par introduire la notion de système projectif, puis celle de système compatible :

Définition 1.1.1 *Soit $\mathfrak{C}$ une catégorie.*

1. *La donnée d'un ensemble filtrant à droite I, d'une famille d'objets $(X_i)_{i\in I}$ et d'une famille de flèches $(X_j \xrightarrow{f_{ij}} X_i)_{i\leq j}$ est appelée **système projectif** lorsque :*

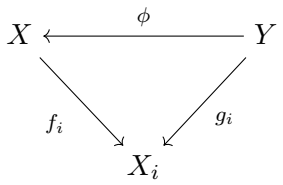
   (a) *pour $i \in I$, $f_{ii} = id_{X_i}$;*
   (b) *pour $i \leq j \leq k$, $f_{ij}f_{jk} = f_{ik}$.*

   Si tel est le cas, on note un tel système $\{X_i, f_{ij}, I\}$.

2. *Soit $\{X_i, f_{ij}, I\}$ un système projectif de $\mathfrak{C}$. La donnée d'un objet X de $\mathfrak{C}$ et d'une famille de flèches $(X \xrightarrow{f_i} X_i)_{i\in I}$ est appelée **système compatible** avec $\{X_i, f_{ij}, I\}$ lorsque pour tout $i \leq j$ on a $f_{ij}f_j = f_i$.*

On peut alors définir la limite projective d'un système projectif :

Définition 1.1.2 *Soient $\mathfrak{C}$ une catégorie et $\{X_i, f_{ij}, I\}$ un système projectif de $\mathfrak{C}$. Une **limite projective** de ce système est la donnée d'un système compatible $\{X, f_i\}$ tel que pour tout système compatible $\{Y, g_i\}$, il existe une unique flèche $Y \xrightarrow{\phi} X$ faisant commuter le diagramme suivant :*



Cette propriété universelle en assure l'unicité :

Proposition 1.1.1 *La limite projective d'un système $\{X_i, f_{ij}, I\}$ est unique à isomorphisme près. Si elle existe, elle est notée $\varprojlim X_i$.*

Donnons un exemple de système projectif :

Exemple 1.1.1 *Si p est un entier naturel, alors le système $\left\{\mathbb{Z}/p^i\mathbb{Z}, f_{ij}, \mathbb{N}\right\}$, où f_{ij} est donnée par $a + p^j\mathbb{Z} \mapsto a + p^i\mathbb{Z}$ pour $i \leq j$, est projectif.*

1.2 Espaces profinis

Dans la catégorie des espaces topologiques, la limite projective existe :

Proposition 1.2.1 *Si $\{X_i, f_{ij}, I\}$ est un système projectif d'espaces topologiques, alors sa limite projective existe.*

Démonstration : Posons $X = \left\{(x_i)_{i\in I} \in \prod_{i\in I} X_i : i \leq j \Longrightarrow x_i = f_{ij}x_j\right\}$ muni de la topologie induite par la topologie produit, et $f_i : X \longrightarrow X_i$ la restriction de la projection $\prod_{i\in I} X_i \longrightarrow X_i$. Le système $\{X, f_i\}$ est alors compatible avec le système projectif.
Si de plus $\{Y, g_i\}$ est un autre système compatible alors on vérifie aisément que $\prod_{i\in I} g_i$ est l'unique application continue qui fasse commuter le diagramme de la définition 1.1.2. □

Dans la suite, on identifiera la limite projectif d'un système projectif à celle exhibé dans la preuve précédente. Ainsi, $\varprojlim X_i$ est vu comme un sous-espace de $\prod_{i\in I} X_i : i \leq j$.

Remarque 1.2.1 *La preuve précédente fournit également l'existence de la limite projective dans la catégorie des ensembles, la catégorie des groupes, la catégorie des groupes topologiques, la catégorie des anneaux topologiques...*

Précisons l'exemple donné dans la section précédente :

Exemple 1.2.1 *Reprenons le système projectif de l'exemple* 1.1.1 *avec p premier. On peut vérifier que si chacun des $\mathbb{Z}/p^i\mathbb{Z}$ est muni de la topologie discrète, alors $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ est l'anneau topologique des entier p-adiques.*

La limite projective d'espaces topologiques vérifie les propriétés suivantes :

Proposition 1.2.2 *Soient $\{X_i, f_{ij}, I\}$ un système projectif d'espaces topologiques et $X = \varprojlim X_i$.*

1. *Si les X_i sont séparés, alors X est séparé.*
2. *Si les X_i sont totalement discontinus, alors X est totalement discontinu.*
3. *Si les X_i sont séparés, alors $\varprojlim X_i$ est fermé dans $\prod_{i\in I} X_i$.*
4. *Si les X_i sont compacts, alors X est compact.*
5. *Si les X_i sont des compacts non vides, alors X est non vide.*

Démonstration : Les points 1. et 2. découlent de ce que ces propriétés topologiques passent au produit et à la topologie induite.

Pour établir 3., prenons $x \in \prod_{k\in I} X_k - \varprojlim X_k$ et $i \leq j$ tels que $f_{ij}x_j \neq x_i$. Puisque X_i est séparé, on dispose de U et V des voisinages ouverts respectifs de x_i et $f_{ij}x_j$ qui sont disjoints. Alors, $x \in f_{ij}^{-1}(U) \times V \times \prod_{k\in I, k\neq i,j} X_k$ qui est inclus dans $\prod_{k\in I} X_k - \varprojlim X_k$ donc ce dernier est ouvert.

Le point 4. est conséquence de 3. et du théorème de Tychonoff.

Pour montrer 5., notons que $\varprojlim X_k = \bigcap_{i\leq j} \left\{x \in \prod_{k\in I} X_k : x_i = f_{ij}x_j\right\}$. Les ensembles du terme de droite sont fermés et puisque I est filtrant à droite, ces ensembles vérifient la propriété d'intersection finie : la compacité de $\prod_{k\in I} X_k$ assure donc que $\varprojlim X_i$ est non vide. □

On a la propriété suivante pour un système compatible compact :

Proposition 1.2.3 *Soient $\{X_i, f_{ij}, I\}$ un système projectif d'espaces compacts et $\{Y, g_i\}$ un système compatible compact. Si les g_i sont surjectifs, alors l'application $\phi : Y \longrightarrow \varprojlim X_i$ qui fait commuter le diagramme de la définition* 1.1.2 *est surjective.*

Démonstration : Il suffit de le montrer pour $\varprojlim X_i$. Soit donc $x \in \varprojlim X_i$ et posons $A_i := \{y \in Y : \phi(y)_i = x_i\}$. Les A_i forment une famille de fermés non vides de Y qui vérifient la propriété d'intersection finie (car I est filtrant à droite) donc $\bigcap_{i\in I} A_i \neq \emptyset$ et pour $y \in \bigcap_{i\in I} A_i$ on a bien $\phi(y) = x$. □

Nous pouvons alors définir ce qu'est un espace profini :

Définition 1.2.1 *On dit qu'un espace topologique X est profini s'il est la limite projective d'un système projectif d'espaces discrets et finis.*

On dispose de la caractérisation suivante de tels espaces :

Proposition 1.2.4 *Soit X un espace topologique. Les assertions suivantes sont équivalentes :*

(i) L'espace X est profini.

(ii) L'espace X est compact et totalement discontinu.

(iii) L'espace X est compact et admet une base d'ouverts-fermés.

Démonstration : $\underline{(i) \Longrightarrow (ii)}$: cela découle des points 2. et 4. de la proposition 1.2.2.

$\underline{(ii) \Longrightarrow (iii)}$: soit V un ouvert de X et $x \in V$. Puisque X est compact, la composante connexe de x est l'intersection de tous les ouverts-fermés qui contiennent x (voir par exemple le lemme 1.1.11 de [6]). On a donc une famille d'ouverts fermés $(U_j)_{j\in J}$ tels que $\{x\} = \bigcap_{j\in J} U_j$. Ainsi $(X - V) \cap \bigcap_{j\in J} U_j = \emptyset$. Puisque X est compact, on a donc $J' \subseteq J$ fini tel que $(X - V) \cap \bigcap_{j\in J'} U_j = \emptyset$. De là $\bigcap_{j\in J'} U_j \subseteq V$ d'où le résultat.

$\underline{(iii) \Longrightarrow (i)}$: posons I l'ensemble des partitions finies de X par des ouverts-fermés. Ordonnons I par la relation $\leq$ où $i \leq j$ si et seulement si la partition j est plus fine que i : l'ensemble I est alors filtrant à droite puisque si $i, j \in I$, la partition $\{U \cap V : (U \in i) \wedge (V \in j)\}$ est plus fine que i et j.

Si pour chaque $i \in I$ on note $\mathcal{R}_i$ la relation d'équivalence associée, on a une famille d'applications continues surjectives $g_i : X \longrightarrow X/\mathcal{R}_i$. Par la propriété universelle de la limite projective, on obtient donc une application $\phi : X \longrightarrow \varprojlim X/\mathcal{R}_i$ qui est surjective par la proposition 1.2.3.

De plus, ϕ est injective. En effet, soient $x, y \in X$ distincts : on a deux ouverts-fermés disjoints U et V contenant respectivement x et y. En prenant $i \in I$ tel que $i = \{U, V, X - (U \cup V)\}$, on a $g_i(x) \neq g_i(y)$ si bien que $\phi(x) \neq \phi(y)$.

Ainsi, ϕ est une bijection continue entre compacts et réalise donc un homéomorphisme entre X et $\varprojlim X/\mathcal{R}_i$. □

1.3 Groupes profinis et pro-$\mathcal{C}$ groupes

Dans la suite, $\mathcal{C}$ désigne une classe non vide de groupes finis close par isomorphisme et qui est :

(i) close par *quotient* au sens où si $G \in \mathcal{C}$ et $H \trianglelefteq G$ alors $G/H \in \mathcal{C}$;

(ii) close par *produit* au sens où si G et H sont dans $\mathcal{C}$, alors $G \times H \in \mathcal{C}$;

(iii) close par *sous-groupe* au sens où si $G \in \mathcal{C}$ et $H \leq G$ alors $H \in \mathcal{C}$;

On définit alors les $\mathcal{C}$-groupes et les pro-$\mathcal{C}$ groupes :

Définition 1.3.1 *On dit qu'un groupe est un* $\mathcal{C}$***-groupe*** *s'il est dans* $\mathcal{C}$ *et on dit que c'est un* ***pro-*$\mathcal{C}$ ***groupe*** *s'il est une limite projective de* $\mathcal{C}$*-groupes.*

Voici quelques exemples de telles classes :

Exemple 1.3.1
1. *La classe des groupes finis dont les limites projectives sont dites profinies.*
2. *La classe des groupes abéliens finis dont les limites projectives sont dites pro-abéliennes.*
3. *Si* p *est premier, la classe des* p*-groupes finis dont les limites projectives sont appelées pro-*p *groupes. On s'intéressera particulièrement à cette classe dans la suite.*

Pour donner une caractérisation des pro-$\mathcal{C}$ groupes, commençons par énoncer un lemme :

Lemme 1.3.1 *Soient* $\{G_i, f_{ij}, I\}$ *un système projectif de groupes finis discrets et* $\{G, f_i\}$ *leur limite projective. Alors* $\{\operatorname{Ker} f_i : i \in I\}$ *est un système fondamental de voisinages de* 1 *dans* G*.*

Démonstration : Il suffit de remarquer qu'un système fondamental de voisinages de 1 dans $\prod_{i\in I} G_i$ est donné par $\left\{\{1\}\times\cdots\times\{1\}\times\prod_{i\in I, i\neq i_1,\ldots,i_r} G_i : (r\in\mathbb{N})\wedge(i_1,\ldots,i_r\in I)\right\}$ et donc qu'un système fondamental de voisinages de 1 dans $\varprojlim G_i$ est donné par

$$\left\{\varprojlim G_i \bigcap \left(\{1\}\times\cdots\times\{1\}\times\prod_{i\in I, i\neq i_1,\ldots,i_r} G_i\right) : (r\in\mathbb{N})\wedge(i_1,\ldots,i_r\in I)\right\}.$$

Puisque I est filtrant à droite, l'ensemble précédent est inclus dans

$$\left\{\varprojlim G_i \bigcap \left(\{1\}\times\prod_{i\in I, i\neq j} G_i\right) : j\in I\right\}$$

qui n'est autre que $\{\operatorname{Ker} f_i : i \in I\}$. □

On dispose alors de la caractérisation suivante des pro-$\mathcal{C}$ groupes :

Proposition 1.3.1 *Soit* G *un groupe topologique. Les assertions suivantes sont équivalentes :*

(i) Le groupe G *est un pro-*$\mathcal{C}$ *groupe.*

(ii) Le groupe G *est compact, totalement discontinu et pour tout sous-groupe normal et ouvert* U *de* G *on a* $G/U \in \mathcal{C}$*.*

(iii) Le groupe G *est compact et il existe un système fondamental de voisinages* $\mathcal{U}$ *de* 1 *tel que* $\bigcap_{U\in\mathcal{U}} U = 1$ *et pour tout* $U \in \mathcal{U}$*, le groupe* U *est un sous-groupe normal et ouvert de* G *avec* $G/U \in \mathcal{C}$*.*

(iv) Il existe un système fondamental de voisinages $\mathcal{U}$ *de* 1 *constitué de sous-groupes normaux, ouverts et tel que* $G/U \in \mathcal{C}$ *dès que* $U \in \mathcal{U}$ *et* $G \simeq \varprojlim G/U$*.*

Démonstration : $\underline{(i) \Longrightarrow (ii)}$: si G est un pro-$\mathcal{C}$ groupe, alors G est compact et totalement discontinu par la proposition 1.2.4. De plus, soit $\{G_i, f_{ij}, I\}$ un système projectif de $\mathcal{C}$-groupes et une famille d'applications $f_i : G \longrightarrow G_i$ tels que $\{G, f_i\}$ est la limite de ce système. Soit U un sous-groupe normal et ouvert de G : par le lemme 1.3.1 il existe $i \in I$ tel que $\ker f_i \subseteq U$, si bien que $G/\ker f_i = G_i \in \mathcal{C}$. Alors, $G/U = (G/\ker f_i)/(U/\ker f_i)$ est le quotient d'un élément de $\mathcal{C}$, donc $G/U \in \mathcal{C}$.

$\underline{(ii) \Longrightarrow (iii)}$: puisque G est compact et totalement discontinu, la preuve de la proposition 1.2.4 fournit un système fondamental $\mathcal{U}$ de voisinages ouverts-fermés de 1 tels que $\bigcap\limits_{U \in \mathcal{U}} U = 1$. Il suffit donc de montrer que dans chaque ouvert-fermé $U \in \mathcal{U}$ il existe un sous-groupe normal ouvert de G.

L'ensemble U étant ouvert et les opérations sur G continues, il existe pour tout x dans U un voisinage $V_x \subseteq U$ de x et un voisinage $S_x \subseteq U$ de 1 tels que $S_x^{-1} \subseteq U$, $V_x S_x \subseteq U$ et $V_x S_x^{-1} \subseteq U$. De plus, U est un fermé de G donc il est compact et il existe $x_1, \ldots, x_n \in U$ tels que $U = V_{x_1} \cup \cdots \cup V_{x_n}$.

Posons $S = \bigcap\limits_{i=1}^{n} S_{x_i} \cap S_{x_i}^{-1}$ qui est un ouvert. Alors $SU \subseteq U$, ce qui assure que le groupe ouvert $H = \bigcup\limits_{n=1}^{\infty} S^n$ est inclus dans U. Enfin, puisque H est un ouvert du groupe compact G il est d'indice fini et admet donc un nombre fini de classes de conjugaison, ce qui fournit que le groupe $K = \bigcap\limits_{x \in G} xHx^{-1}$ est ouvert. Puisque K est normal, ouvert et $K \subseteq H \subseteq U$, il vient donc que K convient.

$\underline{(iii) \Longrightarrow (iv)}$: si $\mathcal{U}$ est un système fondamental de voisinages de 1 avec les hypothèses de (iii), on a un morphisme continu $\phi : G \longrightarrow \varprojlim G/U$ continu et surjectif. La condition $\bigcap\limits_{U \in \mathcal{U}} U = 1$ assure l'injectivité de ϕ. Cette application réalisant une bijection continue entre compacts, c'est un homéomorphisme, ce qui conclut.

$\underline{(iv) \Longrightarrow (i)}$: cette implication est immédiate.

□

1.4 Système de générateurs d'un groupe profini

On introduit ici une définition d'un système de générateurs qui tient compte de la topologie du groupe.

Définition 1.4.1 *Soient G un groupe profini et $X \subseteq G$.*

1. *On dit que X un **système de générateurs topologiques** de G lorsque $G = \overline{< X >}$*
2. *On dit que X **converge vers** 1 lorsque tout sous-groupe ouvert U de G vérifie que $X - U$ est fini.*

*Si les deux points précédents sont vérifiés, on dit que X est un **système de générateurs de G qui converge vers** 1.*

L'existence d'un tel système de générateurs dans un groupe profini n'est pas évidente :

Proposition 1.4.1 *Si G est un groupe profini alors il admet un système de générateurs qui converge vers 1.*

Démonstration : On renvoie le lecteur à la proposition 2.4.4 de [6]. □

On dispose d'une propriété de cardinalité d'un système de générateurs qui converge vers 1 dans un groupe profini :

Proposition 1.4.2 *Soit G un groupe profini. Si X et Y sont deux parties génératrices infinies de G qui convergent vers 1 alors $|X| = |Y|$.*

Démonstration : Soit X une partie génératrice infinie de G. On va montrer que $|X| = |\mathcal{N}|$ où $\mathcal{N}$ est l'ensemble des sous-groupes ouverts normaux de G.

Tout d'abord, $X = \bigcup_{N \in \mathcal{N}} (X - N)$ d'où $|X| \leq |\mathcal{N}|$.

Ensuite si $\mathcal{A}$ désigne l'ensemble des parties finies de X et $\mathcal{N}(A) = \{N \in \mathcal{N} : X - A \subseteq N\}$ pour $A \in \mathcal{A}$, alors $\mathcal{N} = \bigcup_{A \in \mathcal{A}} \mathcal{N}(A)$. Puisque $|\mathcal{A}| = |X|$, il suffit de montrer que $|\mathcal{N}(A)| \leq \aleph_0$ pour pouvoir conclure que $|\mathcal{N}| \leq |X|$.

Soit donc $A \in \mathcal{A}$: les éléments de $\mathcal{N}(A)$ sont en bijection avec les sous-groupes normaux ouverts d'indice fini du groupe $H = G/\overline{< X - A >}$. Or les sous-groupes d'indice fini de H sont l'image de l'application qui à un morphisme $H \longrightarrow sfBij(\mathbb{N})$ (où $sfBij(\mathbb{N})$ désigne les permutations à support fini de $\mathbb{N}$) associe son noyau.

Puisque H est engendré par A, l'ensemble des morphismes $H \longrightarrow sfBij(\mathbb{N})$ est de cardinal $\aleph_0^A = \aleph_0$. On en déduit que $|\mathcal{N}(A)| \leq \aleph_0$, ce qui conclut. □

1.5 Complété d'un groupe suivant un filtre et pro-$\mathcal{C}$ complété

1.5.1 Complété d'un groupe suivant un filtre

On définit d'abord le complété d'un groupe suivant un filtre de sous-groupes normaux :

Définition 1.5.1 *Soient G un groupe abstrait et $\mathcal{N}$ une famille de sous-groupes normaux de G filtrante à gauche pour l'inclusion. On définit le* ***complété*** *de G suivant le filtre $\mathcal{N}$, noté $\hat{G}$ comme la limite projective $\varprojlim G/N$.*

Pour établir certaines propriétés des groupes libres, nous avons besoin de quelques propositions. La première établit la densité de l'image du morphisme $\theta : G \longrightarrow \hat{G}$ qui envoie g sur $(gN)_{N \in \mathcal{N}}$:

Proposition 1.5.1 *Si θ est l'application définie précédemment, alors $\theta(G)$ est dense dans $\hat{G}$.*

Démonstration : On montre de façon analogue au lemme 1.3.1 que si $f_N : \hat{G} \longrightarrow G/N$ désigne la projection dans G/N pour $N \in \mathcal{N}$, alors la famille des $\operatorname{Ker} f_N$ forme un système fondamental de voisinages de $1_{\hat{G}}$.

Pour $x \in \hat{G}$, il suffit donc de montrer que pour tout $N \in \mathcal{N}$, le groupe $\theta(G)$ rencontre $x \operatorname{Ker} f_N$. Soit donc $N \in \mathcal{N}$ et $g \in G$ tel que $gN = f_N(x)$. Alors, $f_N(\theta(g)) = gN = f_N(x)$ d'où $\theta(g) \in x \operatorname{Ker} f_N$. □

Proposition 1.5.2 *Soient G un groupe, H un group profini, et $\phi : G \longrightarrow H$ un morphisme de groupes. Soit $\mathcal{N}$ une famille de sous-groupes normaux de G filtrante à gauche pour l'inclusion telle que pour tout sous-groupe normal ouvert V de H, le groupe $\phi^{-1}(V)$ contient un élément de $\mathcal{N}$. Alors il existe un unique morphisme continu $\hat{\phi} : \hat{G} \longrightarrow H$ tel que $\hat{\phi}\theta = \phi$.*

Démonstration : Commençons par noter que l'unicité découle de la proposition 1.5.1.

Pour l'existence, notons $f_N : \hat{G} \longrightarrow G/N$ la projection pour $N \in \mathcal{N}$. Si V est un sous-groupe normal ouvert de H, prenons $N \in \mathcal{N}$ tel que $N \leq \phi^{-1}(V)$. Posons alors $g_V : \hat{G} \longrightarrow H/V$ le morphisme défini par $g_V(x) = \phi(f_N(x))V$, dont on vérifie qu'il est indépendant du choix d'un tel N.

On vérifie également que la famille des g_V forme un système compatible avec H si bien qu'ils induisent un morphisme continu $\hat{\phi} : \hat{G} \longrightarrow H$ qui vérifie $\hat{\phi}\theta = \phi$. □

1.5.2 Pro-$\mathcal{C}$ complété d'un groupe

Soit $\mathcal{C}$ une classe de groupes vérifiant les hypothèses de 1.3. On introduit ici un foncteur de complétion qui part de la catégorie des groupes discrets dans celle des $pro-\mathcal{C}$ groupes.

Si G est un groupe discret, posons $\mathcal{N}_{\mathcal{C}}(G) = \{N \trianglelefteq G : G/N \in \mathcal{C}\}$ qui est filtrante d'après les hypothèses (i) et (ii) faites sur $\mathcal{C}$: en effet, si $N_1, N_2 \in \mathcal{N}_{\mathcal{C}}(G)$ alors $G/N_1 \cap N_2$ s'injecte dans $G/N_1 \times G/N_2$, si bien que $N_1 \cap N_2 \in \mathcal{C}$.

Définition 1.5.2 *Soit G un groupe discret. On définit le pro-$\mathcal{C}$ complété de G, noté $G_{\widehat{\mathcal{C}}}$, par* $\varprojlim_{N \in \mathcal{N}_{\mathcal{C}}(G)} G/N$.

Dans la suite, si G est un groupe discret, la topologie sur engendrée par $\mathcal{N}_{\mathcal{C}}(G)$ est appelée la pro-$\mathcal{C}$ topologie de G.

À la manière du paragraphe précédent, on définit alors $\theta : G \longrightarrow G_{\widehat{\mathcal{C}}}$, dont l'image est dense dans $G_{\widehat{\mathcal{C}}}$ par la proposition 1.5.1. De plus, la proposition 1.5.2 assure que le pro-$\mathcal{C}$ complété d'un groupe vérifie la propriété universelle suivante :

Proposition 1.5.3 *Soit G un groupe discret. Il existe un unique couple $(\mathfrak{G}, \iota)$ où*

(i) $\mathfrak{G}$ est un pro-$\mathcal{C}$ groupe ;

(ii) $\iota : G \longrightarrow \mathfrak{G}$ est un morphisme continu pour la pro-$\mathcal{C}$ topologie de G ;

et tel que pour tout pro-$\mathcal{C}$ groupe H et tout morphisme continu $\phi : G \longrightarrow H$ pour la pro-$\mathcal{C}$ topologie de G, il existe un unique morphisme continu $\tilde{\phi} : \mathfrak{G} \longrightarrow H$ telle que $\phi = \tilde{\phi}\iota$.

Démonstration : Par les propositions 1.5.1 et 1.5.2, il est clair que $(G_{\widehat{\mathcal{C}}}, \theta)$ répond à ce problème universel. L'unicité relève d'arguments usuels. □

Définissons de façon constructive la pro-$\mathcal{C}$ complétion d'un morphisme entre groupes discrets.

Définition 1.5.3 *Soient G, H des groupes discrets et $\phi : G \longrightarrow H$ un morphisme de groupes.*

Posons $\mathcal{M} = \left\{\phi^{-1}(M) : M \in \mathcal{N}_{\mathcal{C}}(H)\right\}$. Puisque $\mathcal{C}$ est clos par sous-groupe, $\mathcal{M}$ est inclus dans $\mathcal{N}_{\mathcal{C}}(G)$. De plus, la clôture par sous-groupe et par produit de $\mathcal{C}$ assurent que $\mathcal{M}$ est filtrante. Pour tout $N \in \mathcal{N}_{\mathcal{C}}(H)$, on dispose alors d'un morphisme continu ϕ_N obtenu par composition

$$\left[\varprojlim_{M \in \mathcal{N}_{\mathcal{C}}(H)} G/\phi^{-1}(M)\right] \xrightarrow{\phi_N} G/\phi^{-1}(N) \longrightarrow H/N$$

où le premier morphisme est la projection et où le second morphisme est induit par ϕ. La limite projective de $(\phi_N)_{N \in \mathcal{N}_{\mathcal{C}}(H)}$ induit alors un morphisme continu $\tilde{\phi} : \varprojlim_{M \in \mathcal{N}_{\mathcal{C}}(H)} G/\phi^{-1}(M) \longrightarrow H_{\widehat{\mathcal{C}}}$.

La filtration $\mathcal{M}$ étant incluse dans $\mathcal{N}_{\mathcal{C}}(G)$, on dispose d'un morphisme surjectif

$$\psi : \ G_{\widehat{\mathcal{C}}} \longrightarrow \varprojlim_{M \in \mathcal{M}} G/M.$$

On définit alors ***le pro-$\mathcal{C}$ complété*** *de ϕ, noté $\phi_{\widehat{\mathcal{C}}}$ comme la composée $\tilde{\phi}\psi$.*

La définition précédente assure la continuité du pro-$\mathcal{C}$ complété d'un morphisme. Néanmoins, on dispose également de la description ensembliste suivante du complété, dont la vérification est laissée au lecteur :

Proposition 1.5.4 *Soient G, H des groupes discrets et $\phi : G \longrightarrow H$ un morphisme de groupes. Le pro-$\mathcal{C}$ complété de ϕ est donné par :*

$$\phi_{\widehat{\mathcal{C}}} : \quad \varprojlim_{M \in \mathcal{N}_{\mathcal{C}}(G)} G/M \longrightarrow \varprojlim_{N \in \mathcal{N}_{\mathcal{C}}(H)} H/N$$

$$(x_M)_{M \in \mathcal{N}_{\mathcal{C}}(G)} \longmapsto \left(\phi(x_{\phi^{-1}(N)})\right)_{N \in \mathcal{N}_{\mathcal{C}}(H)}$$

On a la propriété de fonctorialité suivante, dont la preuve est laissée au lecteur :

Proposition 1.5.5 *Soient G, H, K des groupes discrets ainsi que $\phi : G \longrightarrow H$ et $\psi : H \longrightarrow K$ des morphismes. Alors $(\psi\phi)_{\widehat{\mathcal{C}}} = \psi_{\widehat{\mathcal{C}}}\phi_{\widehat{\mathcal{C}}}$.*

On vient donc de définir un foncteur covariant $(\_)_{\widehat{\mathcal{C}}}$ de la catégorie des groupes discrets dans celle des pro-$\mathcal{C}$ groupes. Ainsi défini, il a la propriété d'exactitude suivante :

Proposition 1.5.6 *Le foncteur $(\_)_{\widehat{\mathcal{C}}}$ est exact à droite.*

Démonstration : Soit une suite exacte courte de groupes discrets $1 \longrightarrow G \xrightarrow{\phi} H \xrightarrow{\psi} K \longrightarrow 1$. Elle induit la suite suivante, dont nous montrons l'exactitude :

$$G_{\widehat{\mathcal{C}}} \xrightarrow{\phi_{\widehat{\mathcal{C}}}} H_{\widehat{\mathcal{C}}} \xrightarrow{\psi_{\widehat{\mathcal{C}}}} K_{\widehat{\mathcal{C}}} \longrightarrow 1.$$

Montrons la surjectivité de $\psi_{\widehat{\mathcal{C}}}$:

Le pro-$\mathcal{C}$ complété de ψ est obtenu comme la limite projective des morphismes $(\psi_N)_{N \in \mathcal{N}_{\mathcal{C}}(K)}$ où pour chaque $N \in \mathcal{N}_{\mathcal{C}}(K)$ le morphisme ψ_N est la composée des morphismes suivants :

$$\varprojlim_{M \in \mathcal{N}_{\mathcal{C}}(H)} H/M \longrightarrow \varprojlim_{L \in \mathcal{N}_{\mathcal{C}}(K)} H/\psi^{-1}(L) \longrightarrow H/\psi^{-1}(N) \longrightarrow K/N.$$

Or, le premier morphisme est surjectif par la proposition 1.2.3 ; le second l'est car c'est une projection et le troisième l'est car ψ l'est. Ainsi le morphisme $\psi_{\widehat{\mathcal{C}}}$ est surjectif comme limite projective de morphismes surjectifs et de source compacte, par la proposition 1.2.3,.

Montrons l'exactitude en $H_{\widehat{\mathcal{C}}}$:

Tout d'abord, on sait que $\psi\phi = 0$ et donc par fonctorialité $\psi_{\widehat{\mathcal{C}}}\phi_{\widehat{\mathcal{C}}} = (\psi\phi)_{\widehat{\mathcal{C}}} = 0$ d'où $\operatorname{Im}\phi_{\widehat{\mathcal{C}}} \subseteq \operatorname{Ker}\psi_{\widehat{\mathcal{C}}}$.

Ensuite, soit $(y_M)_{M \in \mathcal{N}_{\mathcal{C}}(H)} \in \operatorname{Ker}\psi_{\widehat{\mathcal{C}}}$. Soit $M \in \mathcal{N}_{\mathcal{C}}(H)$: l'exactitude de la suite initiale induit la suite exacte

$$G/\phi^{-1}(M) \xrightarrow{\overline{\phi}_M} H/M \xrightarrow{\overline{\psi}_M} K/\psi(M) \longrightarrow 1$$

où $\overline{\phi}_M$ et $\overline{\psi}_M$ sont les applications quotient respectives de ϕ et ψ. Puisque $\overline{\psi}_M(y_M) = 1$, il existe $x_{\phi^{-1}(M)} \in G/\phi^{-1}(M)$ tel que $\overline{\phi}_M(x_{\phi^{-1}(M)}) = y_M$: on dispose ainsi d'une famille $\left(x_{\phi^{-1}(M)}\right)_{M \in \mathcal{N}_{\mathcal{C}}(H)}$.

La compatibilité des applications $\overline{\phi}_M$ avec le système projectif donné par la famille $(G/\phi^{-1}(M))_{M \in \mathcal{N}_{\mathcal{C}}(H)}$ fournit que $\left(x_{\phi^{-1}(M)}\right)_{M \in \mathcal{N}_{\mathcal{C}}(H)} \in \varprojlim_{M \in \mathcal{N}_{\mathcal{C}}(H)} G/\phi^{-1}(M)$. Or, la proposition 1.2.3 assure la surjectivité du morphisme

$$\varprojlim_{L \in \mathcal{N}_{\mathcal{C}}(G)} G/L \longrightarrow \varprojlim_{M \in \mathcal{N}_{\mathcal{C}}(H)} G/\phi^{-1}(M).$$

Tout antécédent de $\left(x_{\phi^{-1}(M)}\right)_{M\in\mathcal{N}_{\mathcal{C}}(H)}$ par ce morphisme est donc un antécédent de $(y_M)_{M\in\mathcal{N}_{\mathcal{C}}(H)}$ par $\phi_{\widehat{\mathcal{C}}}$. Ainsi $\underline{\operatorname{Ker}\psi_{\widehat{\mathcal{C}}} \subseteq \operatorname{Im}\phi_{\widehat{\mathcal{C}}}}$.

On a donc $\underline{\operatorname{Im}\phi_{\widehat{\mathcal{C}}} = \operatorname{Ker}\psi_{\widehat{\mathcal{C}}}}$. □

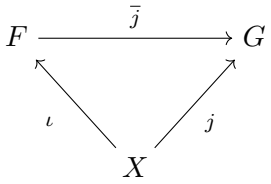
Dans le cas particulier de la classe des pro-p groupes, où p est premier, on désignera par $G_{\widehat{p}}$ le pro-p complété d'un groupe discret G.

1.6 Pro-$\mathcal{C}$ groupes libres

La notion de groupe libre est ici considérée sous un angle topologique. On développe dans cette partie les propriétés fondamentales de ces groupes qui sont utilisés dans la suite.

Définition 1.6.1 *Soit X un ensemble. Un **pro-$\mathcal{C}$ groupe libre** sur X est la donnée d'un pro-$\mathcal{C}$ groupe F et d'une application $\iota : X \longrightarrow F$ tels que :*

1. *L'ensemble $\iota(X)$ converge vers 1;*
2. *Pour tout pro-$\mathcal{C}$ groupe G et toute application $j : X \longrightarrow G$ dont l'image converge vers 1, il existe un unique morphisme $\overline{j} : F \longrightarrow G$ qui fasse commuter le diagramme suivant :*



On a alors l'existence et l'unicité d'un tel groupe :

Proposition 1.6.1 *Si X est un ensemble, alors il existe un pro-$\mathcal{C}$ groupe libre sur X. Celui-ci est unique à isomorphisme près et est noté $\mathfrak{F}_{\mathcal{C}}(X)$.*

Démonstration : Si l'unicité découle de la propriété universelle, l'existence mérite d'être précisée.

Soit F_0 le groupe libre sur X et $\mathcal{U}$ l'ensemble des sous-groupes normaux U de F_0 tels que $F_0/U \in \mathcal{C}$ et $X - U$ est fini, muni de la filtration à gauche naturelle.

On pose alors $F = \varprojlim F_0/U$ le complété de F_0 suivant $\mathcal{U}$ et $\iota : X \longrightarrow F$ l'application obtenue par la composition de l'inclusion $X \longrightarrow F_0$ par le morphisme $\theta : F_0 \longrightarrow F$. On affirme que (F, ι) est un pro-$\mathcal{C}$ groupe libre sur X.

Tout d'abord, $\iota(X)$ converge vers 1. En effet, d'après le lemme 1.3.1, il suffit de prendre comme ouvert un sous-groupe de F de la forme $\operatorname{Ker} f_U$ (où $U \in \mathcal{U}$ et f_U désigne la projection $\varprojlim F_0/V \longrightarrow F_0/U$). Or, $\iota(X) - \operatorname{Ker} f_U$ est fini car $\iota^{-1}\left(\iota(X) - \operatorname{Ker} f_U\right)$ est inclus dans $X - U$ lequel est fini.

Ensuite, soit G un pro-$\mathcal{C}$ groupe et $j : X \longrightarrow G$ d'image convergeant vers 1. Par la propriété universelle du groupe libre, il existe un morphisme $\widetilde{j} : F_0 \longrightarrow G$ qui étend j. Enfin, par la proposition 1.5.2, il existe $\overline{j} : F \longrightarrow G$ telle que $\overline{j}\theta = \widetilde{j}$. Ainsi, $\overline{j}\iota = \overline{j}\theta{\restriction_X} = \widetilde{j}{\restriction_X} = j$ si bien que $\overline{j}$ fait commuter le diagramme de la propriété universelle.

Notons enfin que $\iota(X)$ engendre F d'après la proposition 1.5.1, si bien que $\overline{j}$ est unique. □

Remarque 1.6.1 *La preuve précédente assure que $\iota(X)$ est une partie génératrice de $\mathfrak{F}_{\mathcal{C}}(X)$ et que ι est injective.*

Dans la suite, si p désigne un nombre premier et X un ensemble, on note $\mathfrak{F}_p(X)$ le pro-p groupe libre sur X.

1.7 Présentation topologique d'un pro-C groupe

On définit le pendant topologique de la présentation algébrique d'un groupe :

Définition 1.7.1 *Soient G un pro-$\mathcal{C}$ groupe, $X \subseteq G$ et $R \subseteq \mathfrak{F}_{\mathcal{C}}(X)$. On dit que $< X|R >$ est une **présentation topologique** de G si X est un système de générateurs de G qui converge vers 1 et si on a une suite exacte courte*

$$0 \longrightarrow \overline{< R >^{\mathfrak{N}}} \longrightarrow \mathfrak{F}_{\mathcal{C}}(X) \longrightarrow G \longrightarrow 0$$

où $\overline{< R >^{\mathfrak{N}}}$ désigne l'adhérence du sous-groupe normal engendré par R dans $\mathfrak{F}_{\mathcal{C}}(X)$ et où les flèches sont supposées continues.

1.8 Sous-groupe de Frattini d'un groupe profini

Le groupe de Frattini permet de ramener l'étude des systèmes de générateurs d'un groupe à celui d'un groupe plus simple à étudier :

Définition 1.8.1 *Soit G un groupe profini. Le sous-groupe de Frattini de G, noté $\Phi(G)$, est l'intersection de tous les sous-groupes ouverts maximaux de G.*

Notons d'emblée que $\Phi(G)$ est un sous-groupe normal strict de G. On a besoin de quelques propriétés supplémentaires pour la suite.

Proposition 1.8.1 *Soient G un groupe profini et H un sous-groupe fermé de G. Si $G = H\Phi(G)$ alors $G = H$.*

Démonstration : Puisque H est fermé, il est l'intersection de tous les sous-groupes ouverts de G qui le contiennent (voir par exemple la proposition 2.1.4 de [6]) et soit M un sous-groupe ouvert maximal de G qui contient H. Alors $M = G$, sans quoi $M\Phi(G) = M$ serait un sous-groupe strict de G. □

Enfin, nous disposons d'une description du sous-groupe de Frattini pour les pro-p groupes :

Proposition 1.8.2 *Si G est un pro-p groupe, alors $\Phi(G) = \overline{G^p[G,G]}$.*

Démonstration : On renvoie le lecteur à la proposition 2.8.7 de [6]. □

1.9 Dualité de Pontryagin

Un outil puissant lors de l'étude des groupes topologiques est le dual de Pontryagin :

Définition 1.9.1 *Soit G un groupe topologique. Le **dual de Pontryagin** de G, noté $\widehat{G}$, est le groupe des morphismes continus de G dans $\mathbb{R}/\mathbb{Z}$ muni de la topologie compacte-ouverte.*

On admet le théorème suivant, dû à Lev Pontryagin, qui est utilisé dans la suite :

Théorème 1.9.1 *Soit G un groupe topologique abélien et localement compact. Alors, l'application $G \longrightarrow \widehat{\widehat{G}}$ qui à $g \in G$ associe le morphisme d'évaluation $\phi_g : \widehat{G} \longrightarrow \mathbb{R}/\mathbb{Z}$, donné par $f \mapsto f(g)$, est un isomorphisme de groupes topologiques.*

2 Préambule sur la cohomologie des groupes profinis

Dans cette section, on définit la cohomologie d'un groupe profini et on montre quelques propriétés fondamentales qui sont utiles dans la suite. À cet effet, considérons un groupe profini G.

2.1 Premières définitions

On note $\mathfrak{C}_G$ la catégorie des groupes abéliens discrets sur lesquels G opère continûment. Autrement dit, un objet de $\mathfrak{C}_G$ est un groupe abélien discret A muni d'une application continue $G \times A \to A$, qui envoie $(g, x) \in G \times A$ sur gx, et telle que :

(i) pour tout $x \in A$ on a $ex = x$ où e désigne l'élément neutre de G ;

(ii) pour tout $g, h \in G$ et $x \in A$ on a $(gh)x = g(h(x))$;

(iii) pour tout $g \in G$ et $x, y \in A$ on a $g(x + y) = gx + gy$.

Sauf mention du contraire, tout module considéré par la suite sera supposé dans $\mathfrak{C}_G$. Commençons par donner un nom aux objets de cette catégorie :

Définition 2.1.1 *Tout élément A de la catégorie $\mathfrak{C}_G$ est appelé un G-module.*

Pour chaque G-module A, on note $\mathcal{C}^n(G, A)$ l'ensemble des applications continues de G^n dans A. Pour $n \geq 0$, on définit alors le **morphisme de cobord**

$$d_n : \mathcal{C}^n(G, A) \longrightarrow \mathcal{C}^{n+1}(G, A)$$

par la formule

$$\begin{aligned} d_n(f)(g_1, \ldots, g_{n+1}) =& g_1 \cdot f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{i=n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \ldots, g_n) \end{aligned}$$

et on pose $d_{-1} = 0$.

On dispose alors de la propriété suivante, dont la vérification est laissée au lecteur :

Proposition 2.1.1 *Pour tout $n \geq 0$, on a $d_n \circ d_{n-1} = 0$.*

On obtient donc un complexe de cochaînes $\mathcal{C}^\bullet(G, A)$ donné par :

$$0 \xrightarrow{d_{-1}} \mathcal{C}^0(G, A) \xrightarrow{d_0} \mathcal{C}^1(G, A) \xrightarrow{d_1} \mathcal{C}^2(G, A) \xrightarrow{d_2} \ldots$$

Ce complexe induit alors des groupes de cohomologie :

Définition 2.1.2 *Soit $n \geq 0$. On définit le n-ième groupe de cohomologie de G à valeurs dans A, noté $H^n(G, A)$, par* $\mathrm{Ker}(d_n)/\mathrm{Im}\, d_{n-1}$.

Fixons également les termes qui seront utilisés dans la suite :

Définition 2.1.3 *Soit $n \geq 0$. On appelle :*

*(i) une n-**cochaîne** tout élément de $C^n(G, A)$;*

*(ii) un n-**cocycle** tout élément de $Z^n(G, A) := \mathrm{Ker}\, d_n$;*

*(iii) un n-**cobord** tout élément de $B^n(G, A) := \mathrm{Im}\, d_{n-1}$.*

De plus, pour simplifier les notations :

Remarque 2.1.1 *Dans la suite, s'il n'y a pas d'ambiguïté, on notera d au lieu de d_n.*

Soit A un G-module. Commençons par donner une caractérisation de ses premiers groupes de cohomologie :

Exemple 2.1.1 *Caractérisation de $H^0(G,A)$.*
Le 0-ième groupe de cohomologie $H^0(G,A)$ est l'ensemble des éléments dans A fixés par l'action de G, à savoir l'ensemble $A^G = \{a \in A | ga = a, \forall g \in G\}$.

Exemple 2.1.2 *Caractérisation de $H^1(G,A)$.*
Un 1-cocycle est une fonction continue $x : G \longrightarrow A$ telle que pour tout $(\sigma,\tau) \in G^2$ on ait :

$$x(\sigma\tau) = x(\sigma) + \sigma x(\tau).$$

Un 1-cobord est une fonction continue $x : G \longrightarrow A$ telle qu'il existe $a \in A$ tel que pour tout $\sigma \in G$ on ait

$$x(\sigma) = \sigma a - a.$$

Notons que si l'action de G sur A est triviale, alors $H^1(G,A)$ est l'ensemble des morphismes continus de G dans A.

2.2 Suite exacte longue de cohomologie

Dans cette section, on introduit la suite exacte longue de cohomologie associée à une suite exacte courte : elle est très utile pour calculer certains groupes de cohomologie.

Commençons par énoncer un premier lemme, plus connu sous le nom de **lemme du serpent** :

Lemme 2.2.1 *Soit un diagramme commutatif*

$$\begin{array}{ccccccc} & & A & \xrightarrow{i} & B & \xrightarrow{j} & C \longrightarrow 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' \end{array}$$

où les lignes sont exactes. On dispose alors d'une suite exacte canonique

$$\begin{array}{l} \mathrm{Ker}(i) \longrightarrow \mathrm{Ker}(\alpha) \xrightarrow{i} \mathrm{Ker}(\beta) \xrightarrow{j} \mathrm{Ker}(\gamma) \xrightarrow{\delta} \\ \quad \mathrm{Coker}(\alpha) \xrightarrow{i'} \mathrm{Coker}(\beta) \xrightarrow{j'} \mathrm{Coker}(\gamma) \longrightarrow \mathrm{Coker}(j'). \end{array}$$

Démonstration : L'existence et l'exactitude des lignes du haut et du bas sont faciles à vérifier. On va maintenant construire un morphisme

$$\delta : \mathrm{Ker}(\gamma) \to \mathrm{Coker}(\alpha)$$

qui convient. Soit $c \in \mathrm{Ker}(\gamma)$. Il existe $b \in B$ tel que $j(b) = c$ puisque j est surjectif. Comme $j'(\beta(b)) = \gamma(j(b)) = \gamma(c) = 0$, il existe un unique $a' \in A'$ tel que $i'(a') = \beta(b)$. On définit

$$\delta(c) := a' \mod \alpha(A).$$

Cette définition ne dépend pas du choix de b : en fait, si $\tilde{b}$ est un autre élément de B tel que $j(\tilde{b}) = c$ et si $a' \in A'$ est tel que $i'(\tilde{a}') = \beta(\tilde{b})$, alors $j(\tilde{b} - b) = 0$, c'est-à-dire $\tilde{b} - b = i(a)$ pour un $a \in A$. Donc $i'(\tilde{a}' - a' = \beta(\tilde{b} - b) = \beta(i(a)) = i'(\alpha(a))$, et par conséquent $\tilde{a}' - a' = \alpha(a)$, c'est-à-dire $\tilde{a}' \equiv a' \mod \alpha(A)$.

Exactitude en $\mathrm{Ker}(\gamma)$: si $\delta(c) = 0$, il existe un $a \in A$ tel que $a' = \alpha(a)$, où a' est défini comme ci-dessus, et donc $\beta(b - i(a)) = i'(a') - i'(\alpha(a)) = 0$, c'est-à-dire $b - i(a) \in \mathrm{Ker}(\beta)$ et $j(b - i(a)) = c \in \mathrm{Im}(j)$.

Exactitude en $\mathrm{Coker}\,\alpha$: Soit $a' \in A'$ tel que $i'(a') \equiv 0 \mod (\beta(B))$, il existe un $b \in B$ tel que $i'(a') = \beta(b)$. Soit $c = j(b)$, et on a donc $\delta(c) \equiv a' \mod \alpha(A)$ par la définition de δ. □

Une suite exacte de G-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

induit le diagramme commutatif suivant où les lignes sont exactes

$$\begin{array}{ccccccc} & & \bar{\mathcal{C}}^n(G,A) & \longrightarrow & \bar{\mathcal{C}}^n(G,B) & \longrightarrow & \bar{\mathcal{C}}^n(G,C) \longrightarrow 0 \\ & & \downarrow{\scriptstyle d_n^A} & & \downarrow{\scriptstyle d_n^B} & & \downarrow{\scriptstyle d_n^C} \\ 0 \longrightarrow & Z^{n+1}(G,A) & \longrightarrow & Z^{n+1}(G,B) & \longrightarrow & Z^{n+1}(G,C) & \end{array}$$

où $\bar{\mathcal{C}}^n(G,\bullet) := \mathcal{C}^n(G,\bullet)/\,\mathrm{Im}(d_n)$, $Z^n(G,\bullet) := \mathrm{Ker}(d_{n+1})$. Notons que $\mathrm{Ker}(d_n^\bullet) = H^n(G,\bullet)$ et $\mathrm{Coker}(d_n) = H^{n+1}(G,\bullet)$. D'après le lemme 2.2.1 on obtient donc pour tout $n \geq 0$ la suite exacte

$$H^n(G,A) \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \xrightarrow{\delta} H^{n+1}(G,A) \longrightarrow H^{n+1}(G,B) \longrightarrow H^{n+1}(G,C)$$

On vient donc de prouver le théorème suivant :

Théorème 2.2.1 *Tout suite exacte de G-modules $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ induit une suite exacte longue*

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G,A) \longrightarrow \dots$$

$$\dots \longrightarrow H^n(G,A) \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \xrightarrow{\delta} H^{n+1}(G,A) \longrightarrow \dots$$

2.3 Quelques morphismes entre groupes de cohomologie

On va introduire des morphismes entre certains groupes de cohomologie qui seront utiles par la suite.

Étant donnés deux groupes profinis G et G', un G-module A et un G'-module A', on appelle paire compatible un couple (φ, f) où φ est un morphisme $G' \to G$ et f est un morphisme $A \to A'$ vérifiant la relation $f(\varphi(\sigma')a) = \sigma' f(a)$ pour tous $\sigma' \in G'$ et $a \in A$.

Une telle paire induit naturellement un morphisme :

$$\begin{aligned} \mathcal{C}^n(G,A) &\longrightarrow \mathcal{C}^n(G',A') \\ a &\longmapsto f \circ a \circ \varphi \end{aligned}$$

On vérifie aisément que ce morphisme commute avec le cobord d, si bien qu'il induit un morphisme :

$$H^n(G,A) \longrightarrow H^n(G',A').$$

Dans la suite, nous allons appliquer ce procédé pour construire trois morphismes entre des groupes de cohomologie.

2.3.1 Morphisme d'inflation

Soient H un sous-groupe distingué fermé d'un groupe profini G et A un G-module, alors A^H est un G/H-module.

Le couple formé de la projection $G \longrightarrow H$ et de l'injection $A^H \hookrightarrow A$ forme une paire compatible de morphismes, qui induit un morphisme

$$inf_G^{G/H} : H^n(G/H, A^H) \to H^n(G, A)$$

appelé **inflation**. Par définition, on voit que l'inflation est transitive au sens où pour deux sous-groupes distingués fermés $H \subseteq F$ de G, on a

$$inf_G^{G/H} \circ inf_{G/H}^{G/F} = inf_G^{G/F}.$$

2.3.2 Morphisme de restriction

Soient H un sous-groupe fermé d'un groupe profini G et A un G-module. Commençons par remarquer que A possède également une structure de H-module.

L'inclusion $H \hookrightarrow G$ et le morphisme identité $A \longrightarrow A$ forment une paire compatible, d'où un morphisme induit en cohomologie

$$res_H^G : H^n(G, A) \to H^n(H, A)$$

qui l'on appelle **restriction**. Il est clair que la restriction est transitive, au sens où pour deux sous-groupes $F \subseteq H$ de G, on a

$$res_F^H \circ res_H^G = res_F^G.$$

2.3.3 Lemme de Shapiro

Soit H un sous-groupe fermé de G. Pour chaque H-module A, on considère le G-module

$$M = \mathrm{Ind}_G^H(A)$$

qui est l'ensemble de toutes applications continues $x : G \to A$ telles que $x(\tau\sigma) = \tau x(\sigma)$ pour tout $\tau \in H$. L'action de $\rho \in G$ sur M est donnée par $x(\sigma) \mapsto (\rho x)(\sigma) = x(\sigma\rho)$. Les G-modules ainsi obtenus sont dit **induits**.

On a un morphisme π de $\mathrm{Ind}_G^H(A)$ dans A défini par $x \longmapsto x(1)$.

L'inclusion $H \hookrightarrow G$ et π forment une paire compatible. On en déduit donc un morphisme entre $H^n(G, \mathrm{Ind}_G^H(A))$ et $H^n(H, A)$. En fait, par une construction explicite (voir par exemple la proposition 1.6.4 de [5]), on peut trouver un inverse de ce morphisme, ce qui fournit la propriété suivante :

Proposition 2.3.1 *(Lemme de Shapiro) Il y a un isomorphisme $H^n(G, Ind_G^H(A)) \xrightarrow{\sim} H^n(H, A)$ pour chaque $n \geq 0$.*

2.3.4 Morphisme de transgression

On construit ici un morphisme dans un cas particulier qui suffira pour la suite.

Proposition 2.3.2 *Soient H un sous-groupe distingué et fermé de G et A un G-module.*

Si un 1-cocycle $x : H \longrightarrow A$ est un représentant pour un élément $[x] \in H^1(H, A)^{G/H}$, alors il existe une 1-cochaîne $y : G \to A$ telle que $y|_H = x$ et que $d(y)(\sigma_1, \sigma_2)$ est contenu dans A^H et ne dépend que des classes $\sigma_1 H$, $\sigma_2 H$.

Démonstration : Soit $s : G/H \to G, \gamma \mapsto s\gamma$ une section continue de la projection $G \to G/H$ telle que $s1 = 1$ (pour l'existence, voir par exemple l'exercice 4 de la section 1.1 dans [5] : l'idée est de considérer l'ensemble X des paires (S, s) telles que s est une section continue $G/H \to G/S$; l'ordre naturel sur X rend X inductif et on déduit le résultat par le lemme de Zorn). Puisque $[x]$ est invariant par chaque $\gamma \in G/H$, on a

$$s\gamma((s\gamma)^{-1}\tau s\gamma) - x(\tau) = \tau y(s\gamma) - y(s\gamma) \tag{1}$$

pour un élément $y(s\gamma) \in A$. On peut supposer que $y(1) = 0$ et que $\gamma \mapsto y(s\gamma)$ est continue. En fait, il existe un sous-groupe distingué ouvert U de G tel que $x(\tau)$ ne dépend que des classes $\tau(H \cap U)$ et est contenu dans A^U. Donc le membre de gauche de l'équation (1) prend la même valeur pour tous les éléments $s\gamma$ dans une classes modulo U. Donc on peut choisir pour $y(s\gamma)$ la même valeur dans une classe de G/U, c'est à dire que $y(s\gamma)$ est une fonction continue de γ. Pour un $\sigma = s\gamma\tau \in G$ arbitraire, on pose

$$y(\sigma) = y(s\gamma) + s\gamma(\tau).$$

Soient $\sigma, \sigma_i \in G, \tau \in H$. Une série de calculs (qui sont détaillés par exemple dans la proposition 1.6.6 de [5]) montre que pour σ, σ_1, $\sigma_2 \in G$ et $\tau \in H$:

1. $y|_H = x$
2. $y(\sigma\tau) = y(\sigma) + \sigma y(\tau)$
3. $y(\tau\sigma) = y(\tau) + \tau y(\sigma)$
4. $d(y)(\sigma_1, \sigma_2\tau) = d(y)(\sigma_1\tau, \sigma_2) = d(y)(\sigma_1, \sigma_2)$
5. $\tau d(y)(\sigma_1, \sigma_2) = d(y)(\sigma_1, \sigma_2)$

Donc y est une 1-cochaîne qui convient. □

Considérons maintenant x et y comme dans la proposition précédente. Alors la classe $[d(y)]$ de $d(y)$ peut être vue dans $H^2(G/H, A^H)$. On peut ainsi définir une application dite de **transgression** par

$$tg : H^1(H, A)^{G/H} \longrightarrow H^2(G/H, A^H)$$

$$[x] \longmapsto [d(y)]$$

avec les notations de la proposition 2.3.2.

2.3.5 Suite exacte à cinq termes

Proposition 2.3.3 *Soient H un sous-groupe distingué fermé de G et A un G-module. La suite suivante est exacte :*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{inf} H^1(G, A) \xrightarrow{res} H^1(H, A)^{G/H} \xrightarrow{tg} H^2(G/H, A^H) \xrightarrow{inf} H^2(G, A).$$

Démonstration : Exactitude en $H^1(G, A)$.

Soit $x : G/H \to A^H$ un 1-cocycle dans $Z^1(G/H, A^H)$ tel que $inf(x) : G \to G/H \to A$ est un cobord dans $B^1(G, A)$, c'est-à-dire qu'il existe $a \in A$ tel que pour tout $\sigma \in G$ on a $inf(x)(\sigma) = \sigma a - a$. Pour tout $\tau \in H$ et $\sigma \in G$, on a $inf(x)(\sigma) = inf(x)(\sigma\tau)$ et donc $\sigma a - a = \sigma\tau a - a$. On en déduit que $a \in A^H$ et que $x(\sigma H) = inf(x)(\sigma) = \sigma a - a = \sigma H a - a$. Par conséquent, x est un 1-cobord.

Exactitude en $H^1(G, A)$.

Soit $x : G/H \to A^H$ un 1-cocycle dans $Z^1(G/H, A^H)$, alors

$$(res \circ inf)(x)(\tau) = inf(x)(\tau) = x(\tau H) = x(H) = x(1) = 0$$

si bien que $\underline{\mathrm{Im}(inf) \subseteq \mathrm{Ker}(res)}$.

Réciproquement, soit $x : G \to A$ un 1-cocycle dans $Z^1(G, A)$ tel que $res(x)$ est un cobord dans $B^1(H, A)^{G/H}$, c'est-à-dire $x(\tau) = \tau a - a$ pour tout $\tau \in H$. Le 1-cocyle $x'(\sigma) = x(\sigma) - (\sigma a - a)$ de G définit la même classes de cohomologie que x et satisfait $x'(\tau) = 0$ pour tout $\tau \in H$. Donc

$$x'(\sigma\tau) = x'(\sigma) + \sigma x'(\tau) = x'(\sigma),$$

et

$$x'(\tau\sigma) = x'(\tau) + \tau x'(\sigma) = \tau x'(\sigma)$$

On définit $y : G/H \to A$ par $y(\sigma H) = x'(\sigma)$. Alors $y(\sigma H) \in A^H$, car $y(\sigma H) = y(\tau\sigma H) = \tau y(\sigma H)$ pour tout $\tau \in H$, et on obtient un 1-cocycle avec $inf(y) = x'$ qui montre que $\underline{\mathrm{Ker}(res) \subseteq \mathrm{Im}(inf)}$.

$\underline{\text{Exactitude en } H^1(H, A)^{G/H}.}$

Si $y \in Z^1(G, A)$ et $x = res(y)$ représente une classe $[x]$ dans $H^1(H, A)^{G/H}$, alors $tg[x] = [d(y)] = 0$, si bien que $\underline{\mathrm{Im}(res) \subseteq \mathrm{Ker}(tg)}$.

Réciproquement, soit $x \in Z^1(H, A)$ représentant une classe $[x] \in H^1(H, A)^{G/H}$ tel que $tg[x] = 0$. Soit $y \in \mathcal{C}^1(G, A)$ une cochaîne comme dans la proposition 2.3.2. L'élément $d(y)$ peut être vu comme un 2-cocycle de G/H : ainsi $[d(y)] = tg[x] = 0$ et donc $d(y) = d(z)$ où $z \in \mathcal{C}^1(G/H, A^H)$. Voyant y et z comme des fonctions sur G, on a $y - z \in Z^1(G, A)$. Comme $res(y - z)$ et $res(y) = x$ sont des 1-cocycles de H, $res(z)$ l'est aussi, et puisque z est constant sur H, on a $res(z) = 0$. Donc $res(y - z) = res(y) = x$, c'est-à-dire $[x] = res[y - z]$, ce qui montre que $\underline{\mathrm{Ker}(tg) \subseteq \mathrm{Im}(res)}$.

$\underline{\text{Exactitude en } H^2(G/H, A^H).}$

Soit $x \in Z^1(H, A)$ un cocycle qui représente une classe $[x] \in H^1(H, A)^{G/A}$. Par la proposition 2.3.2, il y a un cocycle $z \in Z^2(G/H, A^H)$ tel que $inf(z) = d(y)$ et $tg[x] = [z]$. Donc $inf(z) \in B^2(G, A)$ et $inf(tg[x]) = [inf(z)] = 0$, ce qui montre que $\underline{\mathrm{Im}(tg) \subseteq \mathrm{Ker}(inf)}$.

Réciproquement, soit $z \in Z^2(G/H, A^H)$ tel que $z(1, \sigma) = z(\sigma, 1) = 0$ et $inf[z] = [inf(z)] = 0$. Alors $inf(z) = d(y)$ avec $y \in \mathcal{C}^1(G, A)$. On pose $x = res(y)$ et on a $d(x) = res(d(y)) = res(inf(z)) = 0$. En voyant $d(y)$ comme un 2-cocycle z de G/H, $tg[x] = [d(y)] = [z]$, ce qui montre que $\underline{\mathrm{Ker}(inf) \subseteq \mathrm{Im}(tg)}$. □

3 Préambule sur l'algèbre complétée d'un groupe profini

Dans cette partie nous introduisons la structure universelle d'algèbre complétée d'un groupe profini suivant un anneau profini.

3.1 Anneaux profinis

Il s'agit de définir la notion d'anneau profini :

Définition 3.1.1 *Un **anneau profini** est un anneau topologique qui est limite projective d'anneaux finis et discrets.*

Les propriétés montrées dans le cadre des groupes profinis demeurent et nous laissons au lecteur le soin d'adapter les preuves précédentes :

Proposition 3.1.1 *Soit A un anneau topologique. Les assertions suivantes sont équivalentes :*

(i) *L'anneau A est un anneau profini.*

(ii) *L'anneau A est compact.*

(iii) *L'anneau A est compact et totalement discontinu.*

(iv) *L'anneau A est compact et il existe un système fondamental de voisinages de 0 constitué d'idéaux ouverts de A.*

(v) *L'élément 0 a un système fondamental de voisinages $\mathfrak{I}$ constitué d'idéaux ouverts I et tels que $A \simeq \varprojlim A/I$.*

Nous pouvons alors définir la notion d'algèbre profinie sur un anneau profini :

Définition 3.1.2 *Soient A un anneau profini et $\mathfrak{A}$ une A-algèbre topologique. On dit que $\mathfrak{A}$ est une A-algèbre profinie si elle est limite projective de A-algèbres finiment engendrées et libres comme A-modules.*

Notons alors que :

Remarque 3.1.1 *La caractérisation de la proposition* 3.1.1 *demeure vraie pour les algèbres topologiques sur un anneau profini A, à condition de remplacer le terme "anneau" par "algèbre".*

3.2 Algèbre d'un groupe fini sur un anneau profini

On donne ici une structure topologique à l'algèbre d'un groupe fini, pourvu que l'anneau de base soit profini.

Définition 3.2.1 *Soient A un anneau profini et G est un groupe fini. L'algèbre du groupe G sur l'anneau A est l'ensemble des combinaisons formelles $\sum_{g\in G} r_g g$ à coefficients dans A, muni de la topologie produit.*

La remarque 3.1.1 assure alors que :

Proposition 3.2.1 *Si A est un anneau profini et G est un groupe fini, alors l'algèbre de groupe $A[G]$ est une A-algèbre profinie.*

3.3 Algèbre complétée d'un groupe profini

Nous sommes maintenant en mesure de définir l'algèbre d'un groupe profini :

Définition 3.3.1 *Soient A un anneau profini et G un groupe profini. La A-algèbre complétée de G, notée $A[\![G]\!]$, est définie comme étant la limite projective $\varprojlim A[G/U]$ où la filtration porte sur les sous-groupes ouverts et normaux de G.*

La proposition suivante est alors conséquence de la remarque 3.1.1 :

Proposition 3.3.1 *Si A est un anneau profini et G est un groupe profini, alors $A[\![G]\!]$ est une A-algèbre profinie.*

Si $\mathcal{U}$ désigne l'ensemble des sous-groupes ouverts et distingués de G, posons $\theta : G \longrightarrow A[\![G]\!]^\times$ l'application qui envoie $g \in G$ sur $(g \bmod U)_{U\in\mathcal{U}}$: elle est continue car pour $U \in \mathcal{U}$, l'application $G \longrightarrow A[G/U]$ qui envoie g sur sa classe modulo U l'est. L'application θ est alors une injection continue de source compacte d'où :

Proposition 3.3.2 *L'application θ est un plongement de G dans $A[\![G]\!]^\times$.*

La proposition précédente permet d'identifier un groupe profini à son plongement dans son algèbre complétée. On définit alors l'algèbre du groupe G suivant l'anneau A par :

Définition 3.3.2 *L'algèbre du groupe profini G suivant l'anneau A, notée $A[G]$, est définie comme étant la sous-algèbre de $A[\![G]\!]$ engendrée par $\theta(G)$.*

Notons que cette définition coïncide bien avec 3.2.1 lorsque G est fini puisque dans ce cas, l'algèbre complétée est confondue avec l'algèbre de groupe.

On dispose enfin de la propriété suivante sur l'algèbre d'un groupe profini, la preuve étant analogue à celle de la proposition 1.5.1 :

Proposition 3.3.3 *Si G est un groupe profini et A est un anneau profini, alors l'algèbre de groupe $A[G]$ est dense dans l'algèbre complétée $A[\![G]\!]$.*

3.4 Propriété universelle de l'algèbre complétée

Avant d'exhiber la propriété universelle vérifiée par l'algèbre complétée, nous avons besoin d'un premier lemme d'uniforme continuité sur un groupe compact:

Lemme 3.4.1 *Soient G un groupe compact et H un groupe topologique tel que 1_H a un système fondamental de voisinages formé de sous-groupes.*

Si $f : G \longrightarrow H$ est une application continue alors pour tout voisinage V de 1_H, il existe un voisinage U de 1_G tel que pour tout $(x, y) \in G^2$, si $x^{-1}y \in U$ alors $f(x)^{-1}f(y) \in V$.

Démonstration : Soit $f : G \longrightarrow H$ une application continue et V un voisinage de 1_H : par hypothèse, on peut supposer que V est un sous-groupe de H. La continuité de f assure que pour tout $x \in G$ il existe un voisinage U_x de 1_G tel que :

(i) $f(U_x) \subseteq V$

(ii) $f(xU_x) \subseteq f(x)V$

(iii) Pour tout $y \in G$, si $y \in xU_x$ alors $f(x)^{-1}f(y) \subseteq V$.

Puisque G est compact et que les xU_x (pour $x \in G$) recouvrent G, on a $(x_i)_{1\leq i\leq n} \in G^n$ tels que $G = x_1U_{x_1} \cup \cdots \cup x_nU_{x_n}$. Posons alors $U = U_{x_1} \cap \cdots \cap U_{x_n}$.

Soit $(x, y) \in G^2$ tel que $x^{-1}y \in U$. Le recouvrement de G par les $x_iU_{x_i}$ assure alors l'existence de $i, j \in \{1, \ldots, n\}$ tels que $x \in x_iU_{x_i}$ et $y \in x_jU_{x_j}$: on dispose donc de $(u_i, u_j) \in U_{x_i} \times U_{x_j}$ tel que $x = x_iu_i$ et $y = x_ju_j$.

Alors, $f(x)^{-1}f(y) = \left[f(x)^{-1}f(x_i)\right]\left[f(x_i)^{-1}f(x_j)\right]\left[f(x_j)^{-1}f(y)\right]$. Le choix de x_i et x_j assure alors que $f(x)^{-1}f(x_i) \in V$ et $f(x_j)^{-1}f(y) \in V$. De plus, puisque $x^{-1}y \in U$, on a $x_i^{-1}x_ju_j \in u_iU \subseteq U_{x_i}$ d'où $f(x_i)^{-1}f(x_ju_j) \in V$. Mais puisque $f(x_ju_j) \in f(x_j)V$, il vient que $f(x_i)^{-1}f(x_j) \in V$ car V est un groupe.
Ainsi, $f(x)^{-1}f(y) \in V$ si bien que U convient. □

L'algèbre complétée d'un groupe profini vérifie la propriété universelle suivante :

Proposition 3.4.1 *Soient A un anneau profini, $\mathfrak{A}$ une A-algèbre profinie et G un groupe profini. Tout morphisme continu $f : G \longrightarrow \mathfrak{A}^\times$ se prolonge de façon unique en un morphisme continu d'algèbres $\tilde{f} : A[\![G]\!] \longrightarrow \mathfrak{A}$.*

Démonstration : Pour l'unicité, remarquons que f se prolonge en un unique morphisme continu $A[G] \longrightarrow \mathfrak{A}$. La densité de $A[G]$ dans $A[\![G]\!]$ assure alors l'unicité d'un prolongement de f à $A[\![G]\!]$.

Pour l'existence, donnons-nous un système fondamental de voisinages de 0 dans $\mathfrak{A}$ constitué d'idéaux ouverts I et tels que $\mathfrak{A} \simeq \varprojlim \mathfrak{A}/I$. Soit I un tel idéal : le lemme 3.4.1 assure l'existence d'un sous-groupe ouvert et normal U de G tel que pour $x, y \in G$, si $x^{-1}y \in U$ alors $f(x) - f(y) \in I$.

L'application f passe donc au quotient en une application $f_{U,I} : G/U \longrightarrow \mathfrak{A}/I$ et induit un morphisme d'algèbres $\tilde{f}_{U,I} : A[G/U] \longrightarrow \mathfrak{A}/I$. En composant par la projection $A[\![G]\!] \longrightarrow A[G/U]$, on obtient alors une application $f_I : A[\![G]\!] \longrightarrow \mathfrak{A}/I$ dont on vérifie qu'elle est indépendante du choix initial de U. Enfin, la famille des application (f_I) induit un morphisme continu $\tilde{f} : A[\![G]\!] \longrightarrow \mathfrak{A}$ qui prolonge f, si bien que $\tilde{f}$ convient. □

3.5 Fonctorialité de l'algèbre complétée

Un anneau profini A étant donné, nous venons d'associer à chaque groupe profini une algèbre profinie. Il s'agit maintenant de vérifier que cette opération définit bien un foncteur, c'est à dire qu'elle est compatible avec les morphismes de groupes profinis.

Proposition 3.5.1 *Soient A un anneau profini et G,H des groupes profinis.*
Tout morphisme continu de groupes $\phi : G \longrightarrow H$ se prolonge de façon unique en un morphisme d'algèbres complétées $\Phi : A[\![G]\!] \longrightarrow A[\![H]\!]$, dont le noyau est l'idéal topologique engendré à gauche par les $(x - 1)$ pour $x \in \operatorname{Ker}\phi$. De plus, si ϕ est surjective, alors Φ l'est aussi.

Démonstration : Soit $\phi : G \longrightarrow H$ un morphisme continu et $N = \operatorname{Ker}\phi$. L'existence et l'unicité d'un prolongement de ϕ en un morphisme d'algèbres complétées $\Phi : A[\![G]\!] \longrightarrow A[\![H]\!]$ sont une conséquence de la proposition 3.4.1.

Pour déterminer le noyau de Φ on peut supposer que ϕ est surjective, quitte à prendre sa corestriction sur son image. Notons $I(N)$ l'adhérence de l'idéal à gauche engendré par $\{(h - 1) : h \in N\}$.

Il est d'emblée clair que $I(N) \subseteq \operatorname{Ker}\Phi$, si bien que Φ passe au quotient en une application $\tilde{\Phi} : A[\![G]\!]/I(N) \longrightarrow A[\![H]\!]$.
Notons enfin que $G+I(N)/I(N)$ est un groupe pour la multiplication de $A[\![G]\!]$ (car pour tout $g \in G$, on a $gI(N)g^{-1} \subseteq I(N)$). Ainsi, $\tilde{\Phi}$ se restreint en une application continue $\Psi : G + I(N)/I(N) \longrightarrow H$

qui est clairement bijective. La séparation de H et le caractère quasi-compact de $G + I(N)/I(N)$ assurent alors que Ψ est un homéomorphisme. On peut donc étendre Ψ^{-1} en un morphisme continu d'algèbres $A[\![H]\!] \longrightarrow A[\![G + I(N)/I(N)]\!] = A[\![G]\!]/I(N)$.

De plus, $\Psi^{-1}\tilde{\Phi} = id_{A[\![G]\!]}$ et $\tilde{\Phi}^{-1}\Psi = id_{A[\![H]\!]}$ car elles prolongent respectivement id_G et id_H. On en déduit donc que $\tilde{\Phi}$ est un homéomorphisme d'algèbres, ce qui fournit bien que $I(N) = \operatorname{Ker}\Phi$.

Le dernier point est conséquence des arguments qui viennent d'être utilisés. □

4 L'inégalité de Golod et Shafarevich

Dans cette section, nous énonçons le théorème de Golod et Shafarevich que nous prouvons dans les sections suivantes de deux façons.

La première preuve repose sur des arguments de cohomologie. Celle-ci est suivie d'une seconde preuve reposant quant à elle sur des arguments algébriques sur les séries formelles non commutatives.

4.1 Un énoncé topologique

Si p est un nombre premier et G est un pro-p groupe, nous appellerons dans la suite :

(i) $d(G)$ le cardinal minimal d'un ensemble de générateurs de G qui converge vers 1 ;

(ii) $r(G)$ le cardinal minimal d'une partie R de $\mathfrak{F}_p\left(d(G)\right)$ qui converge vers 1 et telle que $< d(G)|R >$ soit une présentation topologique de G au sens de la définition 1.7.1.

Si on pose $\mathfrak{C}$ l'ensemble des cardinaux inférieurs à $\max(|G|, \aleph_0)$, alors $(d(G), r(G))$ est le plus petit élément pour l'ordre lexicographique sur le sous-ensemble de $\mathfrak{C} \times \mathfrak{C}$ formé des couples (d, r) tels qu'il existe une partie R de $\mathfrak{F}_p(d)$ qui converge vers 1 et de cardinal r, ainsi que des morphismes continus s'insérant dans une suite exacte courte

$$0 \longrightarrow \overline{< R >^{\mathfrak{N}}} \longrightarrow \mathfrak{F}_p(d) \longrightarrow G \longrightarrow 0$$

où $\overline{< R >^{\mathfrak{N}}}$ désigne l'adhérence du sous-groupe normal de $\mathfrak{F}_p(d)$ engendré par R.

En 1964, Golod et Shafarevich ont établi dans [2] l'inégalité suivante :

Théorème 4.1.1 (Golod et Shafarevich) *Si G est un p-groupe, alors $r(G) > \dfrac{(d(G)-1)^2}{4}$.*

Une amélioration a été apportée indépendamment par Gaschütz et Vinberg par la suite :

Théorème 4.1.2 *Si G est un p-groupe, alors $r(G) > \dfrac{d(G)^2}{4}$.*

C'est la version améliorée de l'inégalité qui fait l'objet du présent mémoire.

4.2 Un énoncé algébrique

Si G est un groupe discret, posons :

(i) $\mathfrak{d}(G)$ le cardinal minimal d'un ensemble de générateurs de G ;

(ii) $\mathfrak{r}(G)$ le cardinal minimal d'une partie R de $\mathfrak{L}(X)$ telle qu'il existe une suite exacte courte

$$1 \longrightarrow < R >^{\mathfrak{N}} \longrightarrow \mathfrak{L}(X) \longrightarrow G \longrightarrow 1$$

où X désigne un ensemble à $\mathfrak{d}(G)$ éléments, $\mathfrak{L}(X)$ le groupe libre sur X et $< R >^{\mathfrak{N}}$ le sous-groupe normal de $\mathfrak{L}(X)$ engendré par R.

Si p est un nombre premier on dispose du corollaire suivant au théorème 4.1.2 :

Théorème 4.2.1 *Si G est un p-groupe, alors $\mathfrak{r}(G) > \dfrac{\mathfrak{d}(G)^2}{4}$.*

Démonstration : Soit G un p-groupe : pour simplifier les notations, on pose $d = d(G)$, $r = r(G)$, $\mathfrak{d} = \mathfrak{d}(G)$ et $\mathfrak{r} = \mathfrak{r}(G)$. Puisque d est fini, il est évident que $d = \mathfrak{d}$. Écartons d'emblée le cas évident où $\mathfrak{r} = \infty$.

D'après le théorème 1.4.2, il suffit de montrer que $\mathfrak{r} \geq r$. Considérons alors une suite exacte courte

$$1 \longrightarrow < R >^{\mathfrak{N}} \xrightarrow{\phi} \mathfrak{L}(X) \xrightarrow{\psi} G \longrightarrow 1$$

où X est de cardinal $d = \mathfrak{d}$ et R est une partie de $\mathfrak{L}(X)$ de cardinal $\mathfrak{r}$. Le foncteur de pro-p complétion étant exact à droite par la proposition 1.5.6, on obtient une suite exacte

$$\left(< R >^{\mathfrak{N}}\right)_{\widehat{p}} \xrightarrow{\phi_{\widehat{p}}} \mathfrak{L}(X)_{\widehat{p}} \xrightarrow{\psi_{\widehat{p}}} G_{\widehat{p}} \longrightarrow 1.$$

Or par construction du pro-p groupe libre sur X, on a $\mathfrak{L}(X)_{\widehat{p}} = \mathfrak{F}_p(X)$ et puisque G est un p-groupe fini $G_{\widehat{p}} \simeq G$. On obtient donc une suite exacte

$$\left(< R >^{\mathfrak{N}}\right)_{\widehat{p}} \xrightarrow{\phi_{\widehat{p}}} \mathfrak{F}_p(X) \longrightarrow G \longrightarrow 1.$$

En passant au quotient par le noyau N de $\phi_{\widehat{p}}$, on obtient finalement une suite exacte courte

$$1 \longrightarrow \left(< R >^{\mathfrak{N}}\right)_{\widehat{p}}/N \longrightarrow \mathfrak{F}_p(X) \longrightarrow G \longrightarrow 1$$

où les morphismes sont continus. Puisque le morphisme $\theta :< R >^{\mathfrak{N}} \longrightarrow \left(< R >^{\mathfrak{N}}\right)_{\widehat{p}}$ de la proposition 1.5.1 est d'image dense, on en déduit que le sous-groupe normal engendré par l'image de R par ce morphisme est un sous-groupe normal dense de $\left(< R >^{\mathfrak{N}}\right)_{\widehat{p}}$, donc que le sous-groupe normal engendré par les classes de $\theta(R)$ modulo N est dense dans $\left(< R >^{\mathfrak{N}}\right)_{\widehat{p}}/N$. Il vient donc que le nombre minimal de générateurs de $\left(< R >^{\mathfrak{N}}\right)_{\widehat{p}}/N$ comme sous-groupe normal de $\mathfrak{F}_p(X)$ est inférieur à $\mathfrak{r} = |R|$ et donc que $\mathfrak{r} \geq r$. □

5 Une preuve cohomologique de l'inégalité

La preuve présentée ici repose sur des arguments de cohomologie et utilise les notations du préambule et les résultats qui y sont montrés. Elle a été trouvée par Roquette qui la développe dans [8] et elle repose sur des arguments différents de ceux qu'avaient utilisés Golod et Shafarevich dans [2].

Il s'agit de caractériser $d(G)$ et $r(G)$ par les dimensions des premiers groupes de cohomologie de G puis d'utiliser des arguments cohomologiques pour conclure. La démarche qui suit respecte néanmoins la présentation plus moderne qui est faite dans [5].

Nous fixons dans la suite un nombre premier p et un pro-p groupe G.

5.1 Caractérisation cohomologique de $d(G)$

Dans ce qui suit, les groupes de cohomologie seront considérés pour le G-module trivial $\mathbb{F}_p$.

Théorème 5.1.1 *On a* $d(G) = dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$.

Si H et K sont des groupes topologiques, on pose dans la suite $Hom_{\mathcal{C}}(H, K)$ l'ensemble des morphismes continus de H dans K.

Avant d'entamer la preuve rappelons que $H^1(G, \mathbb{F}_p) = Hom_{\mathcal{C}}(G, \mathbb{F}_p)$ puis montrons quelques lemmes pour pouvoir nous ramener à $G/\Phi(G)$ où $\Phi(G)$ est le sous-groupe de Frattini de G.

Lemme 5.1.1 *On a* $d(G) = d(G/\Phi(G))$.

Démonstration : Soit X un système de générateurs de G qui converge vers 1. En notant $\tilde{X}$ le réduit modulo $\Phi(G)$ de X, on obtient que $\tilde{X}$ est un système de générateurs de $G/\Phi(G)$ qui converge vers 1. Ainsi $d(G) \geq d(G/\Phi(G))$.

Si Y est un système de générateurs de $G/\Phi(G)$ qui converge vers 1 et $\tilde{Y}$ un ensemble de représentants uniques des éléments de Y, alors $G = \overline{< \tilde{Y} >}\Phi(G)$ et par la proposition 1.8.1 on obtient que $G = \overline{< \tilde{Y} >}$. Enfin, comme Y converge vers 1 et comme la projection $G \longrightarrow G/\Phi(G)$ est ouverte, il vient que $\tilde{Y}$ converge également vers 1. Ainsi, $\tilde{Y}$ est un système de générateurs de G qui converge vers 1 d'où $d(G) \leq d(G/\Phi(G))$. □

On relie également la dimension du premier groupe de cohomologie de G et celle de $G/\Phi(G)$:

Lemme 5.1.2 *On a* $dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = dim_{\mathbb{F}_p} H^1(G/\Phi(G), \mathbb{F}_p)$.

Démonstration : Soient ϕ la projection $G \longrightarrow G/\Phi(G)$ et $H^1(\phi) : H^1(G/\Phi(G), \mathbb{F}_p) \longrightarrow H^1(G, \mathbb{F}_p)$ le morphisme de groupes de cohomologie induit. L'injectivité de $H^1(\phi)$ est évidente.

Pour montrer la surjectivité, soit $f \in H^1(G, \mathbb{F}_p)$. Puisque $\mathbb{F}_p$ est abélien et d'ordre p, le groupe $\overline{G^p[G, G]}$ est un sous-groupe de $\mathrm{Ker}\, f$. Par la proposition 1.8.2, il vient donc que $\Phi(G)$ est dans le noyau de f, si bien que la factorisation $\tilde{f}$ de f modulo $\Phi(G)$ est un antécédent de f par $H^1(\phi)$.

Ainsi $H^1(G, \mathbb{F}_p)$ et $H^1(G/\Phi(G), \mathbb{F}_p)$ sont isomorphes, ce qui conclut. □

Pour établir le théorème 5.1.1, il suffit alors de montrer la proposition suivante :

Proposition 5.1.1 *On a* $d(G/\Phi(G)) = dim_{\mathbb{F}_p} H^1(G/\Phi(G), \mathbb{F}_p)$.

Démonstration : Puisque $\Phi(G)$ est fermé, $G/\Phi(G)$ est un pro-p groupe : il est alors compact et donc localement compact. Il est de plus abélien puisque $[G,G]$ est un sous-groupe de $\Phi(G)$. On peut donc appliquer le théorème de dualité de Pontryagin.

Notons κ la dimension de l'espace vectoriel $\widehat{G/\Phi(G)} = H^1(G/\Phi(G),\mathbb{F}_p) = Hom_{\mathcal{C}}(G/\Phi(G),\mathbb{F}_p)$. Puisque $Hom_{\mathcal{C}}(G/\Phi(G),\mathbb{F}_p)$ est muni de la topologie compacte-ouverte et puisque $\mathbb{F}_p$ est discret et $G/\Phi(G)$ compact, on obtient que $Hom_{\mathcal{C}}(G/\Phi(G),\mathbb{F}_p)$ est discret et donc que $\widehat{G/\Phi(G)}$ est l'espace discret $\mathbb{F}_p^{(\kappa)}$.

Alors, par le théorème de dualité de Pontryagin, il vient que

$$G/\Phi(G) \simeq Hom_{\mathcal{C}}(\widehat{G/\Phi(G)},\mathbb{F}_p) = Hom_{\mathcal{C}}(\mathbb{F}_p^{(\kappa)},\mathbb{F}_p) = \prod_{\kappa}\mathbb{F}_p$$

ce dernier étant muni de la topologie de la convergence simple car $\mathbb{F}_p^{(\kappa)}$ est discret.

Distinguons maintenant deux cas :

• Si $d(G/\Phi(G))$ est fini, il est clair que $d(G/\Phi(G)) = \kappa = dim_{\mathbb{F}_p}H^1(G/\Phi(G),\mathbb{F}_p)$, ce qui conclut.

• Si $d(G/\Phi(G))$ est infini, l'homéomorphisme de groupes $G/\Phi(G) \simeq \prod_{\kappa}\mathbb{F}_p$ assure qu'il existe dans $G/\Phi(G)$ une partie génératrice convergeant vers 1 de cardinal κ, puisqu'il en est ainsi dans $\prod_{\kappa}\mathbb{F}_p$ avec la partie $\{(\delta_{i,j})_{j\in\kappa} : i \in \kappa\}$. On en déduit par la proposition 1.4.2 que $d(G/\Phi(G)) = \kappa$ et donc que $d(G/\Phi(G)) = dim_{\mathbb{F}_p}H^1(G/\Phi(G),\mathbb{F}_p)$ ce qui conclut. □

Le théorème 5.1.1 est donc conséquence de la combinaison des lemmes 5.1.1 et 5.1.2 ainsi que de la propositon précédente.

5.2 Caractérisation cohomologique de $r(G)$

Donnons-nous une présentation topologique $< X|R >$ de G et une suite exacte courte associée

$$1 \longrightarrow \overline{< R >^{\mathfrak{N}}} \longrightarrow \mathfrak{F}_p(X) \longrightarrow G \longrightarrow 1$$

où $|X| = d(G)$ et $|R| = r(G)$ avec R qui converge vers 1.

On se contente de montrer les propositions de cette section dans le cas où $r(G)$ est fini, ce qui suffit pour la suite. Les résultats restent vrais dans le cas général et nous invitons le lecteur intéressé à se référer aux corollaires 3.9.3. et 3.9.5 de [5].

Commençons par donner une première caractérisation de $r(G)$:

Proposition 5.2.1 *On a* $r(G) = dim_{\mathbb{F}_p} H^1(R, \mathbb{F}_p)^G$.

Démonstration : Rappelons que le premier paragraphe de la preuve du lemme 5.1.2 fournit un isomorphisme $H^1(R, \mathbb{F}_p) = Hom_{\mathcal{C}}(R, \mathbb{F}_p) \simeq Hom_{\mathcal{C}}(R/\Phi(R), \mathbb{F}_p)$.

Si $\{r_1, \cdots, r_{r(G)}\}$ est un ensemble de générateurs de R, les conjugués des r_i engendrent (au sens algébrique) un sous-groupe dense de R. Pour tout $\pi \in H^1(R, \mathbb{F}_p)^G$, on a $\pi(gxg^{-1}) = \pi x$ pour $g \in \mathfrak{F}_p(X)$ car π est invariant par $G = \mathfrak{F}_p(X)/R$. Si π s'annule sur tous les r_i, il s'annule aussi sur les gr_ig^{-1} et donc sur R, d'où π=0. La dualité entre $H^1(R, \mathbb{F}_p)$ et $R/\Phi(R)$ fournit alors que $r(G) \geq \dim_{\mathbb{F}_p} H^1(R, \mathbb{F}_p)^G$.

Réciproquement on procède de façon similaire par la dualité entre $H^1(R, \mathbb{F}_p)$ et $R/\Phi(R)$. Si $n = \dim_{\mathbb{F}_p} H^1(R, \mathbb{F}_p)^G$, on peut trouver n éléments $r_1, \cdots, r_n$ dans R tel que $< r_i, \pi >= 0$ pour tout i entraîne $\pi = 0$ pour $\pi \in H^1(R, \mathbb{F}_p)^G$. Donc les r_i engendrent R et on a $r(G) \leq \dim_{\mathbb{F}_p} H^1(R, \mathbb{F}_p)^G$ □

Théorème 5.2.1 *On a* $r(G) = dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$

Démonstration : Comme R est un sous-groupe distingué fermé de $\mathfrak{F}_p(X)$ la proposition 2.3.3 fournit la suite exacte à cinq termes

$$0 \longrightarrow H^1(G, \mathbb{F}_p) \longrightarrow H^1(\mathfrak{F}_p(X), \mathbb{F}_p) \longrightarrow H^1(R, \mathbb{F}_p)^G \longrightarrow H^2(G, \mathbb{F}_p) \longrightarrow H^2(\mathfrak{F}_p(X), \mathbb{F}_p).$$

Puisque $\mathfrak{F}_p(X)$ est libre on a $H^2(\mathfrak{F}_p(X), \mathbb{F}_p) = 0$ (voir par exemple le théorème 7.7.4 de [6]). En calculant les dimensions on en déduit donc

$$\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = \dim_{\mathbb{F}_p} H^1(R, \mathbb{F}_p)^G + \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) - \dim_{\mathbb{F}_p} H^1(\mathfrak{F}_p(X), \mathbb{F}_p).$$

Or le théorème 5.1.1 assure que $\dim_{\mathbb{F}_p} H^1(\mathfrak{F}_p(X), \mathbb{F}_p) = d(G)$ et $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = d(G)$.

En utilisant la proposition 5.2.1, on en déduit donc que

$$\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = \dim_{\mathbb{F}_p} H^1(R, \mathbb{F}_p)^G = r(G)$$

ce qui constitue le résultat souhaité. □

5.3 Une première preuve de l'inégalité

Supposons dorénavant que G est un p-groupe et commençons par rappeler l'inégalité que nous allons montrer :

Théorème 5.3.1 *On a* $r(G) > \dfrac{d(G)^2}{4}$.

Établissons d'abord quelques propriétés purement algébriques.

5.3.1 Quelques propriétés préalables

Commençons par montrer, avec un argument élémentaire, une version plus faible de l'inégalité précédente, dont nous aurons besoin ensuite :

Lemme 5.3.1 *On a* $r(G) \geq d(G)$.

Démonstration : La suite exacte courte $0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \mathbb{F}_p \longrightarrow 0$ fournit une suite exacte longue de cohomologie

$$\ldots \longrightarrow H^1(G,\mathbb{Z}) \longrightarrow H^1(G,\mathbb{F}_p) \longrightarrow H^2(G,\mathbb{Z}) \xrightarrow{H^2(p)} H^2(G,\mathbb{Z}) \longrightarrow H^2(G,\mathbb{F}_p) \longrightarrow \ldots$$

où $H^1(G,\mathbb{Z}) = Hom(G,\mathbb{Z}) = 0$ car G est fini.
On obtient donc une suite exacte

$$0 \longrightarrow H^1(G,\mathbb{F}_p) \longrightarrow H^2(G,\mathbb{Z}) \xrightarrow{H^2(p)} H^2(G,\mathbb{Z}) \longrightarrow H^2(G,\mathbb{F}_p)$$

qui donne donc que $dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p) \geq dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p)$ ce qui conclut à l'aide des caractérisations des théorèmes 5.1.1 et 5.2.1. □

Énonçons un premier fait qui relève de considérations usuelles sur l'action d'un p-groupe :

Fait 5.3.1 *Soit A un G-module fini où $pA = 0$. Si $A^G = 0$, alors $A = 0$.*

Nous avons également besoin du lemme suivant :

Lemme 5.3.2 *Soit $R = \mathbb{F}_p[G]$ l'algèbre du groupe G et A un G-module fini discret tel que $pA = 0$. Si on pose $b_i = dim_{\mathbb{F}_p} H^i(G,A)$ (pour $i \geq 0$), alors il existe une suite exacte longue de G-modules*

$$0 \longrightarrow A \longrightarrow R^{b_0} \xrightarrow{\partial} R^{b_1} \xrightarrow{\partial} R^{b_2} \xrightarrow{\partial} \ldots$$

telle que pour tout $n \geq 0$ on ait $\partial\left((R^{b_n})^G\right) = 0$.

Démonstration : Notons d'emblée que le module A dispose d'une structure de $\mathbb{F}_p$-espace vectoriel car $pA = 0$.

Puisque $dim_{\mathbb{F}_p} A^G = b_0 = dim_{\mathbb{F}_p} \mathbb{F}_p^{b_0} = dim_{\mathbb{F}_p} \left(R^{b_0}\right)^G$ on dispose d'un isomorphisme de $\mathbb{F}_p$ espaces vectoriels $i : A^G \longrightarrow \left(R^{b_0}\right)^G$. Ce dernier s'étend en un morphisme de G-modules $j : A \longrightarrow R^{b_0}$: en effet, le morphisme $Hom_G(A, R^{b_0}) \longrightarrow Hom(A^G, R^{b_0})$ est surjectif car la suite exacte courte de morphismes de $\mathbb{F}_p$-espaces vectoriels

$$0 \longrightarrow Hom(A/A^G, R^{b_0}) \longrightarrow Hom(A, R^{b_0}) \longrightarrow Hom(A^G, R^{b_0}) \longrightarrow 0$$

fournit une suite exacte longue

$$\ldots \longrightarrow Hom_G(A, R^{b_0}) \longrightarrow Hom_G(A^G, R^{b_0}) \longrightarrow H^1(G, Hom(A/A^G, R^{b_0})) \longrightarrow \ldots$$

où $H^1(G, Hom(A/A^G, R^{b_0})) = 0$.

De plus, j est injectif par le fait 5.3.1 car $(\operatorname{Ker} j)^G = \operatorname{Ker} j\restriction A^G = \operatorname{Ker} i = 0$. On dispose donc d'une suite exacte courte

$$0 \longrightarrow A \xrightarrow{j} R^{b_0} \xrightarrow{k} B \longrightarrow 0$$

où $B = R^{b_0}/j(A)$ et k est le morphisme de projection modulo $j(A)$.

Enfin, puisque R^{b_0} est G-isomorphe à $\operatorname{Ind}_G^{\{1\}}\left(\mathbb{F}_p^{b_0}\right)$, la proposition 2.3.1 assure que pour $i \geq 1$ on a $H^i(G, R^{b_0}) \simeq H^i(\{1\}, \mathbb{F}_p^{b_0}) = 0$. La suite exacte longue associée à la suite exacte courte précédente fournit alors que $H^i(G, B) \simeq H^{i+1}(G, A)$ pour $i \geq 1$. Le résultat reste vrai pour $i = 0$ car dans la suite exacte longue

$$0 \longrightarrow A^G \longrightarrow (R^{b_0})^G \longrightarrow H^0(G, B) \longrightarrow H^1(G, A) \longrightarrow H^1(G, R^{b_0}) \longrightarrow \dots$$

on a $H^1(G, R^{b_0}) = 0$ et le morphisme de G-modules $A^G \longrightarrow (R^{b_0})^G$ est un morphisme injectif entre $\mathbb{F}_p$ espaces vectoriels de même dimension, donc un isomorphisme.

Ainsi, puisque $dim_{\mathbb{F}_p} H^0(G, B) = b_1$, on construit de façon analogue un morphisme injectif de G-modules $l : B \longrightarrow R^{b_1}$ et un G-module C tels qu'on ait une suite exacte

$$0 \longrightarrow B \xrightarrow{l} R^{b_1} \longrightarrow C \longrightarrow 0$$

où $\left(dim_{\mathbb{F}_p} H^i(G, C)\right)_{i\geq 0} = \left(dim_{\mathbb{F}_p} H^{i+1}(G, B)\right)_{i\geq 0} = \left(dim_{\mathbb{F}_p} H^{i+2}(G, A)\right)_{i\geq 0}$. Puisque k et l sont respectivement surjectif et injectif, en posant $\partial = lk$, on a une suite exacte

$$0 \longrightarrow A \xrightarrow{j} R^{b_0} \xrightarrow{\partial} R^{b_1} \longrightarrow C$$

où $\partial\left(\left(R^{b_0}\right)^G\right) = lk(j(A)) = l(0) = 0$. On itère alors la construction par récurrence. □

Définissons ensuite la notion de suite centrale ascendante d'un G-module ainsi que son polynôme de Poincaré:

Définition 5.3.1 *Soit A un G-module. En posant $A_0 = 0$, on définit une suite de G-modules A_n par récurrence en imposant que A_{n+1} soit le plus grand sous-module de A contenant A_n tel que $A_{n+1}/A_n = (A/A_n)^G$. La suite $(A_n)_{n\in\mathbb{N}}$ est appelée la* ***suite centrale ascendante*** *associée à A.*

Si A est fini, on pose $c_n(A) = dim_{\mathbb{F}_p}(A_{n+1}/A_n)$ et $s_n(A) = dim_{\mathbb{F}_p} A_{n+1}$. On définit alors le ***polynôme de Poincaré*** *de A par $P_A = \sum_{n\geq 0} c_n(A)X^n$ si bien que $\frac{1}{1-X}P_A = \sum_{n\geq 0} s_n(A)X^n$.*

On dispose du lemme suivant sur les suites centrales ascendantes :

Lemme 5.3.3 *Soient A et B des G-modules et $\phi : A \longrightarrow B$ un morphisme injectif de G-modules. Si $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ désignent les suites centrales ascendantes respectives de A et B, alors on a l'égalité $A_n = \phi^{-1}(B_n)$.*

Démonstration : On le montre par récurrence sur n. L'injectivité de ϕ assure que le résultat est vrai pour $n = 0$.

Soit donc $n \geq 0$ tel que le résultat est vrai en n. On sait alors que $\phi(A_n) \subseteq B_n$ et donc ϕ fournit un morphisme $A/A_n \longrightarrow B/B_n$. Ce dernier induit alors un morphisme $(A/A_n)^G \longrightarrow (B/B_n)^G$ et donc un morphisme $A_{n+1}/A_n \longrightarrow B_{n+1}/B_n$ qui envoie la classe de $x \in A_{n+1}$ sur celle de $\phi(x)$. Le

caractère maximal de B_{n+1} assure alors que $\phi(A_{n+1}) \subseteq B_{n+1}$.

De plus, si $b \in B_{n+1}$ est dans $\phi(A)$, donnons nous $a \in A$ tel que $b = \phi(a)$. Comme la classe de b modulo B_n est fixe par G il s'ensuit que pour tout $g \in G$ on a $gb - b \in B_n$ et donc que $\phi(ga - a) \in B_n$. Par hypothèse de récurrence, il suit que pour tout $g \in G$ on a $ga - a \in A_n$ si bien que la classe de a mod A_n est G-invariante et donc $a \in A_{n+1}$. Ainsi, $\phi^{-1}(B_{n+1}) \subseteq A_{n+1}$. Finalement on a bien $A_n = \partial^{-1}(B_n)$. □

Le lemme précédent permet de montrer la propriété suivante :

Proposition 5.3.1 *Soit une suite exacte de G-modules*

$$0 \longrightarrow A \xrightarrow{\partial} B \xrightarrow{\partial} C.$$

Si $\partial\left(B^G\right) = 0$, alors elle induit, par restriction sur les termes des suites ascendantes respectives, les suites exactes

$$0 \longrightarrow A_n \xrightarrow{\partial} B_n \xrightarrow{\partial} C_{n-1}$$

pour tout $n \geq 0$.

Démonstration : Montrons d'abord par récurrence sur n que $\partial(B_n) \subseteq C_{n-1}$. Le résultat est vrai pour $n = 1$ puisque par hypothèse $\partial(B_1) = \partial\left(B^G\right) = 0 = C_0$.

Supposons le résultat vrai pour $n \geq 1$. Soit $b \in B_{n+1}$: par définition de B_{n+1}, on sait que pour tout $g \in G$ on a $gb - b \in B_n$. Or, $\partial(B_n) \subseteq C_{n-1}$ si bien que pour tout $g \in G$ on a $\partial(gb - b) \in C_{n-1}$ et donc la classe de ∂b modulo C_{n-1} est G-invariante. Par définition de C_n, il suit que $\partial b \in C_n$ d'où $\partial(B_{n+1}) \subseteq C_n$.

Ensuite, puisque $A \xrightarrow{\partial} B$ est injective, le lemme 5.3.3 fournit que la suite $0 \longrightarrow A_n \xrightarrow{\partial} B_n$ est définie et exacte. On obtient donc la suite

$$0 \longrightarrow A_n \xrightarrow{\partial} B_n \xrightarrow{\partial} C_{n-1}$$

dont l'exactitude en B_n provient de celle de la suite $0 \longrightarrow A \xrightarrow{\partial} B \xrightarrow{\partial} C$ en B et de ce que $A_n = \phi^{-1}(B_n)$ par le lemme 5.3.3. □

5.3.2 Preuve de l'inégalité

Les propriétés précédentes permettent de donner une preuve du théorème 5.3.1.

Par commodité, on notera dans la suite $d = d(G)$ et $r = r(G)$.

En appliquant le lemme 5.3.1 au G-module $\mathbb{F}_p$ et en utilisant les caractérisations des théorèmes 5.1.1 et 5.2.1 on obtient une suite exacte de G-modules

$$0 \longrightarrow \mathbb{F}_p \longrightarrow R \xrightarrow{\partial} R^d \xrightarrow{\partial} R^r$$

où $\partial\left((R^d)^G\right) = 0$. Puisque $\mathbb{F}_p$ s'envoie sur R^G, la suite précédente se factorise en une nouvelle suite exacte

$$0 \longrightarrow R/R^G \xrightarrow{\partial} R^d \xrightarrow{\partial} R^r$$

où on a encore $\partial\left((R^d)^G\right) = 0$.

En posant $M = R/R^G$, $B = R^d$ et $C = R^r$, on peut alors appliquer la proposition 5.3.1 et on obtient donc les suites exactes associées aux suites centrales ascendantes respectives de M, B et C

$$0 \longrightarrow M_n \xrightarrow{\partial} B_n \xrightarrow{\partial} C_{n-1}.$$

Cette suite exacte fournit alors la relation

$$s_n(B) \leq s_n(M) + s_{n-1}(C)$$

pour $n \geq 0$ (où $s_{-1}(C) = 0$).

On en déduit que coefficient par coefficient on a $\dfrac{1}{1-X}P_B \leq \dfrac{1}{1-X}P_M + \dfrac{X}{1-X}P_C$. Or, les définitions de M, B et C assurent que $P_M = \dfrac{P_R - 1}{X}$, $P_B = dP_R$ et $P_C = rP_R$ si bien qu'on obtient l'inégalité suivante coefficient par coefficient :

$$\frac{1}{1-X}dP_R \leq \frac{1}{1-X}\left(\frac{P_R - 1}{X} + rXP_R\right).$$

On obtient donc pour $0 < t < 1$ que $dP_R(t) \leq \dfrac{P_R(t) - 1}{t} + rtP_R(t)$ et donc $1 \leq P_R(t)\left(rt^2 - dt + 1\right)$, d'où $0 < rt^2 - dt + 1$.

Or le minimum du polynôme $rX^2 - dX + 1$ est atteint en $\dfrac{d}{2r}$, qui appartient à $]0, 1[$ par le lemme 5.3.1. En évaluant $rX^2 - dX + 1$ en $\dfrac{d}{2r}$ on trouve finalement $r > \dfrac{d^2}{4}$, ce qui constitue l'inégalité de Golod et Shafarevich.

6 Une preuve via des séries formelles non commutatives

La preuve présentée dans cette section est plus fidèle aux arguments employés par Golod et Shafarevich dans [2], reposant sur des considérations d'algèbre non commutative. Ce sont des arguments analogues qui ont permis à Gaschütz et Vinberg de montrer la version améliorée à laquelle nous nous intéressons. Néanmoins, nous suivons ici la démarche que présente Ershov dans [1] et qui reprend les arguments que développe Koch dans [3].

La preuve repose sur l'étude de l'algèbre complétée d'un pro-p groupe qu'on peut en fait voir comme un quotient d'une algèbre de séries formelles à variables non commutatives, grâce à un résultat qu'a démontré Lazard dans [4].

On fixe dans la suite un nombre premier p et un pro-p groupe G. Donnons au préalable la définition d'une valuation sur une algèbre :

Définition 6.0.1 *Soit $\mathfrak{A}$ une algèbre abstraite. Une **valuation** sur $\mathfrak{A}$ est la donnée d'une application $v : \mathfrak{A} \longrightarrow \mathbb{N} \cup \{\infty\}$ telle que :*

(i) $v(0) = \infty$;

(ii) pour tout $(a, b) \in \mathfrak{A}^2$ *on a* $v(ab) = v(a) + v(b)$;

(iii) pour tout $(a, b) \in \mathfrak{A}^2$ *on a* $v(a + b) \geq \min\{v(a), v(b)\}$.

6.1 L'isomorphisme de Lazard

Commençons pas définir une topologie sur l'algèbre des séries formelles non commutatives sur $\mathbb{F}_p$:

Définition 6.1.1 *Pour $d \geq 1$ on note $\mathbb{F}_p[\![x_1, \ldots, x_d]\!]$ l'algèbre des séries formelles sur les indéterminées non commutatives $x_1, \ldots, x_d$.*

Elle est munie de la valuation $v : \mathbb{F}_p[\![x_1, \ldots, x_d]\!] \longrightarrow \mathbb{N} \cup \{\infty\}$ qui envoie $f \in \mathbb{F}_p[\![x_1, \ldots, x_d]\!]$ sur le degré de sa plus petite composante homogène non nulle.

On la munit de la topologie donnée par le système fondamental de voisinages de 0 constitué des idéaux I_n (pour $n \geq 0$) avec $I_n = \{f \in \mathbb{F}_p[\![x_1, \ldots, x_d]\!] : v(f) \geq n\}$.

En vertu de la remarque 3.1.1 et de la proposition 3.1.1, nous avons donc la proposition suivante :

Proposition 6.1.1 *Pour $d \geq 1$ l'algèbre des séries formelles à d indéterminées non commutatives, munie de la topologie précédente, est une algèbre profinie.*

L'isomorphisme de Lazard permet d'identifier l'algèbre complétée d'un pro-p groupe libre à d générateurs à l'algèbre des séries formelles non commutatives à d indéterminées. Avant de le construire, nous avons besoin d'un lemme :

Lemme 6.1.1 *Soient H un p-groupe et $I(H)$ l'idéal bilatère de $\mathbb{F}_p[H]$ engendré par $\{h - 1 : h \in H\}$, appelé l'**idéal augmenté** de H. Alors il existe $n > 0$ tel que $I^n(H) = 0$.*

Démonstration : Le caractère fini de G assure l'existence d'une suite strictement décroissante de G-modules $\{0\} = A_s \subseteq \cdots \subseteq A_0 = I(H)$ tels que A_i/A_{i+1} n'a pas de sous-G-module propre non trivial. Comme A_i/A_{i+1} vérifie les conditions du fait 5.3.1 et qu'il est non nul, $(A_i/A_{i+1})^G$ est un sous-module non trivial de A_i/A_{i+1}. Or A_i/A_{i+1} est simple, d'où on en déduit que $A_i/A_{i+1} = (A_i/A_{i+1})^G$ si bien que tout point de A_i/A_{i+1} est fixe sous l'action de G.

Ainsi, avec $i = 0$, on sait que pour tout $a \in I(H)$ et $g \in G$, on a $ga - a \in A_1$ et donc que $(g-1)a \in A_1$ d'où $I^2(H) \subseteq A_1$. On obtient donc par récurrence que $I^{s+1}(G) \subseteq A_s = \{0\}$, ce qui conclut. □

On peut donc montrer le théorème de Lazard qui s'énonce comme suit :

Théorème 6.1.1 *Soient $d \geq 1$ et F le pro-p groupe libre engendré par une famille $\{s_1, \ldots, s_d\}$. Il existe un unique homéomorphisme d'algèbres profinies de $\mathbb{F}_p[\![F]\!]$ dans $\mathbb{F}_p[\![x_1, \ldots, x_d]\!]$, noté ι, qui envoie s_i sur $1 + x_i$ pour $i \in \{1, \ldots, d\}$.*

Démonstration : Commençons par remarquer que le groupe multiplicatif $1 + I_1$, muni de la topologie induite par $\mathbb{F}_p[\![x_1, \ldots, x_d]\!]$, est un pro-$p$ groupe : en effet, puisque I_1 est compact, $1 + I_1$ l'est aussi. De plus la famille des $1 + I_n$ $(n \geq 1)$ est un système fondamental de voisinages de 1 formé de sous-groupes ouverts et distingués de $1 + I_1$ vérifiant $\bigcap_{n \geq 1} (1 + I_n) = \{1\}$. Enfin, pour tout $n \geq 1$, le groupe quotient $(1 + I_1)/(1 + I_n)$ est un p-groupe. Le point *(iii)* de la proposition 1.3.1 assure donc que $1 + I_1$ est un pro-p groupe.

Posons $j : \{s_1, \ldots, s_d\} \longrightarrow \mathbb{F}_p[\![x_1, \ldots, x_d]\!]^\times$ l'application qui envoie s_i sur $1 + x_i$ pour $i \in \{1, \ldots, d\}$. Puisque $1 + I_1$ est un pro-p groupe, la propriété universelle des pro-p groupes libres fournit un *unique* morphisme continu de pro-p groupes $\tilde{j} : F \longrightarrow 1 + I_1$ qui prolonge j. Comme $1 + I_1 \subseteq \mathbb{F}_p[\![x_1, \ldots, x_d]\!]^\times$, la fonctorialité de l'algèbre complétée permet d'étendre $\tilde{j}$ en un *unique* morphisme d'algèbres complétées $\iota : \mathbb{F}_p[\![F]\!] \longrightarrow \mathbb{F}_p[\![x_1, \ldots, x_d]\!]$ et l'unicité en découle.

Pour tout sous-groupe ouvert distingué U de F, posons $\tau_U : \mathbb{F}_p[\![x_1, \ldots, x_d]\!] \longrightarrow \mathbb{F}_p[F/U]$ qui envoie $f(x_1, \ldots, x_d)$ sur $f(s_1 - 1, \ldots, s_d - 1)$: grâce au lemme 6.1.1, cette application est bien définie et continue car F/U est un p-groupe. Elle induit alors un morphisme continu $\tau : \mathbb{F}_p[\![x_1, \ldots, x_d]\!] \longrightarrow \mathbb{F}_p[\![F]\!]$.

De plus, on a $\tau\iota = id_{\mathbb{F}_p[\![F]\!]}$ et $\iota\tau = id_{\mathbb{F}_p[\![x_1, \ldots, x_d]\!]}$: en effet, il suffit de remarquer que $\tau\iota$ restreinte à F est l'identité et donc $\tau\iota = id_{\mathbb{F}_p[\![F]\!]}$ par l'unicité de la proposition 3.5.1 ; de plus, $\iota\tau$ restreinte à $\{x_1, \ldots, x_d\}$ est l'identité donc $\iota\tau$ induit l'identité sur les polynômes de $\mathbb{F}_p[\![x_1, \ldots, x_d]\!]$: ceux-ci étant denses dans $\mathbb{F}_p[\![x_1, \ldots, x_d]\!]$ on obtient que $\iota\tau = id_{\mathbb{F}_p[\![x_1, \ldots, x_d]\!]}$.

De là, ι est un homéomorphisme d'algèbres profinies et convient. □

Cet isomorphisme d'algèbres permet alors de définir une valuation sur l'algèbre complétée d'un pro-p groupe libre :

Définition 6.1.2 *Soient $d \geq 1$ et F le pro-p groupe libre à d générateurs $\{s_1, \ldots, s_d\}$. On définit sur $\mathbb{F}_p[\![F]\!]$ une valuation w par $w = v\iota$ où ι est le morphisme de Lazard.*

6.2 Un critère de finitude des pro-p groupes

Dans cette partie, on montre un critère de finitude des pro-p groupes à l'aide d'une présentation de ceux-ci. Donnons-nous, au sens de la définition 1.7.1, une présentation topologique $< X|R >$ de G, c'est-à-dire une suite exacte où s'insèrent des morphismes continus

$$0 \longrightarrow \overline{< R >^{\mathfrak{N}}} \longrightarrow \mathfrak{F}_p(X) \xrightarrow{\phi} G \longrightarrow 0$$

avec $R \subseteq \mathfrak{F}_p(X)$ et $\overline{< R >^{\mathfrak{N}}}$ qui désigne l'adhérence du sous-groupe normal engendré par R dans $\mathfrak{F}_p(X)$.

Supposons de plus que :

(i) L'ensemble X est fini et posons $d = |X|$ et $F = \mathfrak{F}_p(X)$;

(ii) L'ensemble R converge vers 1, ce qui équivaut à supposer que pour tout $n \geq 0$, l'ensemble $\{r \in R : w(r-1) = n\}$ est fini, où w désigne la valuation de $\mathbb{F}_p[\![F]\!]$ définie en 6.1.2 ;

(iii) L'ensemble R ne contient aucune relation triviale, au sens où $1 \notin R$.

Posons alors la série formelle $H_R = \sum_{r \in R} X^{w(r-1)}$.

6.2.1 Énoncé du critère et quelques notations

Il s'agit de montrer le critère suivant :

Théorème 6.2.1 *Si G est un p-groupe fini, alors pour tout $t \in]0,1[$ on a $1 - dt + H_R(t) > 0$.*

En vue de montrer le critère précédent, supposons dans la suite que G est fini, donc un p-groupe. Pour en donner une preuve, nous avons besoin d'introduire quelques notations :

Notations 6.2.1 *(i) Posons $R = \bigcup_{n \geq 0} R_n$ où $R_n = \{r \in R : w(r-1) = n\}$ et $r_n = |R_n|$ pour $n \geq 0$. Notons que puisque ι envoie F dans $1 + I_1$ où I_1 est l'idéal fermé des séries formelles de valuation supérieure à 1, alors $R_0 = 0$;*

(ii) On ordonne les relations $R = \{\rho_i : i \geq 1\}$ de sorte que pour tout $n \geq 1$ on ait une description de R_n par $R_n = \left\{\rho_{r_1+\cdots+r_{n-1}+1}, \ldots, \rho_{r_1+\cdots+r_n}\right\}$;

(iii) On pose également $A = \mathbb{F}_p[\![F]\!]$ et $B = \mathbb{F}_p[\![G]\!] = \mathbb{F}_p[G]$, la dernière égalité étant justifiée par le fait que G est fini. Soient $\iota : A \longrightarrow \mathbb{F}_p[\![x_1, \ldots, x_d]\!]$ l'isomorphisme de Lazard et $\tau : \mathbb{F}_p[\![x_1, \ldots, x_d]\!] \longrightarrow A$ sa réciproque ;

(iv) Par la proposition 3.5.1, le morphisme $F \xrightarrow{\phi} G$ induit un morphisme surjectif $\phi' : A \longrightarrow B$ dont le noyau est l'idéal topologique engendré à gauche par les $\rho - 1$ pour $\rho \in R$;

(v) On définit sur B une valuation, notée ν, par $\nu(b) = \max\{w(a) : a \in A, \phi'(a) = b\}$;

(vi) Enfin, on pose pour simplifier les notations :

- *$y_i = \phi'\tau(x_i) = \phi'(s_i - 1)$ pour $i \in \{1, \ldots, d\}$;*
- *$I_n = \{b \in B : \nu(b) \geq n\}$ pour $n \geq 0$;*
- *$c_n = dim_{\mathbb{F}_p} B/I_n$ pour $n \geq 0$.*

La preuve du théorème 6.2.1 utilise la propriété suivante :

Proposition 6.2.1 *Pour tout $n \geq 1$, on a $\sum_{i=1}^{n} r_i c_{n-i} - dc_{n-1} + c_n \geq 1$.*

Pour la montrer, on transite par quelques résultats préalables.

6.2.2 Quelques lemmes intermédiaires

Établissons une première suite exacte :

Lemme 6.2.1 *On dispose d'une suite exacte*

$$B^{(R)} \xrightarrow{\phi_1} B^d \xrightarrow{\phi_0} B \xrightarrow{\epsilon} \mathbb{F}_p \longrightarrow 0$$

où les morphismes sont définis de la façon suivante :

(i) Pour $(b_1, \dots, b_d) \in B^d$ *on pose* $\phi_0(b_1, \dots, b_d) = \sum_{i=1}^{d} b_i y_i$ *;*

(ii) Pour $(b_i)_{i\geq 1} \in B^{(R)}$ *on pose* $\phi_1(b_1, b_2, \dots) = \left(\sum_{i\geq 1} b_i \phi' \tau(z_{i1}), \dots, \sum_{i\geq 1} b_i \phi' \tau(z_{id}) \right)$ *où pour tout entier* $i \in \{1, \dots, r\}$*, les* $z_{ij} \in \mathbb{F}_p[\![x_1, \dots, x_d]\!]$ *sont définis par l'écriture unique de* $\iota(\rho_i) - 1$ *dans* $\mathbb{F}_p[\![x_1, \dots, x_d]\!]$ *sous la forme* $\iota(\rho_i) - 1 = \sum_{j=1}^{d} z_{ij} x_j$ *;*

(iii) Le morphisme ϵ *est le morphisme d'augmentation qui donne la somme des coefficients d'un élément de l'algèbre* B*.*

Démonstration : Montrons que la suite est exacte en $\mathbb{F}_p$:

Ceci est évident puisque le morphisme d'évaluation est surjectif.

Montrons ensuite l'exactitude de la suite en B :

Tout d'abord, $\epsilon\phi_0 = 0$ car pour $b \in B$ et $i \in \{1, \dots, d\}$ on obtient en décomposant b que $\epsilon\left(b(s_i - 1)\right) = 0$. Ainsi, $\operatorname{Im}\phi_0 \subseteq \operatorname{Ker}\epsilon$.

Ensuite, notons que si $b = \sum_{g\in G} \lambda_g g \in \operatorname{Ker}\epsilon$, alors $b = \sum_{g\in G} \lambda_g (g - 1 + 1) = \sum_{g\in G} \lambda_g (g-1) + \left(\sum_{g\in G} \lambda_g\right) 1 = \sum_{g\in G} \lambda_g (g-1)$. Pour montrer que $\operatorname{Ker}\epsilon \subseteq \operatorname{Im}\phi_0$, il suffit donc de montrer que pour tout $g \in G$, l'élément $g - 1$ est dans l'image de ϕ_0. Or, ceci découle directement par récurrence de ce que $\{s_1, \dots, s_d\}$ engendre G et de ce que pour $g, h \in G$, on a $gh-1 = g(h-1)+g-1$ et $g^{-1}-1 = -g^{-1}(g-1)$.

Il suit donc que $\operatorname{Im}\phi_0 = \operatorname{Ker}\epsilon$.

Montrons enfin l'exactitude de la suite en B^d :

Commençons par remarquer que $\operatorname{Im}\phi_1 \subseteq \operatorname{Ker}\phi_0$. En effet, si $(b_i)_{i\geq 1} \in B^{(R)}$, on a

$$\phi_0\phi_1(b_1, b_2, \dots) = \sum_{j=1}^{d} \sum_{i\geq 1} b_i \phi' \tau(z_{ij}) y_j = \sum_{j=1}^{d} \sum_{i\geq 1} b_i \phi' \tau(z_{ij}) \phi' \tau(x_j) = \sum_{j=1}^{d} \sum_{i\geq 1} b_i \phi' \tau(z_{ij} x_j)$$
$$= \sum_{i\geq 1} b_i \phi'\left(\rho_i - 1\right) = 0$$

où la dernière égalité découle du fait que pour tout $\rho \in R$, on a $\rho - 1$ dans $\operatorname{Ker}\phi'$ par le point *(iv)* des notations 6.2.1.

Pour montrer que $\underline{\operatorname{Ker}\phi_0 \subseteq \operatorname{Im}\phi_1}$, donnons-nous $(b_1,\dots,b_d) \in \operatorname{Ker}\phi_0$. Notons que pour tout $i \in \{1,\dots,d\}$ la topologie discrète de B et la continuité de ϕ' assurent que $\phi'^{-1}(b_i)$ est un ouvert de l'algèbre A.

Puisque $\sum_{i=1}^{d} b_i y_i = \sum_{i=1}^{d} b_i \phi'\tau(x_i) = 0$, on obtient que $\phi'^{-1}(b_1)\tau(x_1)+\cdots+\phi'^{-1}(b_d)\tau(x_d)$ est un ouvert inclus dans $\operatorname{Ker}\phi'$. Or $\operatorname{Ker}\phi' = \overline{<\lambda(\rho-1) : \rho \in R>}$: ainsi, on dispose de $(a_1,\dots,a_d) \in \prod_{i=1}^{d} \phi'^{-1}(b_i)$ et $(a'_i)_{i\geq 1} \in A^{(R)}$ tels que $\sum_{i=1}^{d} a_i\tau(x_i) = \sum_{i\geq 1} a'_i(\rho_i - 1)$.

En écrivant que $\iota(\rho_i)-1 = \sum_{j=1}^{d} z_{ij}x_j$ pour $i \geq 1$, on obtient alors que $\sum_{i=1}^{d} \iota(a_i)x_i = \sum_{i=1}^{d} \left(\sum_{k\geq 1} \iota(a'_k)z_{ki}\right) x_i$. Il en découle que pour $i \in \{1,\dots,d\}$ on a $\iota(a_i) = \sum_{k\geq 1} \iota(a'_k)z_{ki}$ et donc que $a_i = \sum_{k\geq 1} a'_k\tau(z_{ki})$.

Finalement, on obtient

$$\phi_1(\phi'(a'_1),\dots,\phi'(a'_d)) = \left(\sum_{i\geq 1} \phi'(a'_i)\phi'\tau(z_{i1}),\dots,\sum_{i\geq 1} \phi'(a'_i)\phi'\tau(z_{id})\right)$$

$$= \left(\sum_{i\geq 1} \phi'(a'_i\tau(z_{i1})),\dots,\sum_{i\geq 1} \phi'(a'_i\tau(z_{id}))\right) = \left(\phi'\left(\sum_{i\geq 1} a'_i\tau(z_{i1})\right),\dots,\phi'\left(\sum_{i\geq 1} a'_i\tau(z_{id})\right)\right)$$

$$= \big(\phi'(a_1),\dots,\phi'(a_d)\big) = (b_1,\dots,b_d)$$

ce qui montre que $(b_1,\dots,b_d) \in \operatorname{Im}\phi_1$ et donc que $\operatorname{Ker}\phi_0 \subseteq \operatorname{Im}\phi_1$.

On a ainsi $\underline{\operatorname{Im}\phi_1 = \operatorname{Ker}\phi_0}$. □

Avant d'aller plus loin, remarquons que $\operatorname{Im}\phi_1$ est un sous-espace de B^d : il est alors de dimension finie. On dispose donc de $S \subseteq R$ fini tel que la suite $B^S \xrightarrow{\phi_1} B^d \xrightarrow{\phi_0} B \xrightarrow{\epsilon} \mathbb{F}_p \longrightarrow 0$ est encore exacte.

Partitionnons alors S par les $S_n = \{s \in S : w(s-1) = n\}$ pour $n \geq 0$ et posons $s_n = |S_n|$ et $s = |S|$, si bien que $S_n \subseteq R_n$ et $s_n \leq r_n$. Nous avons alors la suite exacte suivante :

Lemme 6.2.2 *Soit $n \geq 1$. La suite exacte du lemme 6.2.1 induit une suite*

$$\prod_{i=1}^{\infty} I_{n-i}^{s_i} \xrightarrow{\psi_1} I_{n-1}^{d} \xrightarrow{\psi_0} I_n \longrightarrow 0$$

où les flèches ψ_1 et ψ_0 sont respectivement les restrictions de ϕ_1 et ϕ_0. De plus ψ_0 est surjective.

Démonstration : Il s'agit de montrer que la suite est bien définie, puis que ψ_0 est surjective.

Montrons que $\phi_1\left(\prod_{i=1}^{\infty} I_{n-i}^{s_i}\right) \subseteq I_{n-1}^d$:

Commençons par remarquer que le produit de gauche est fini car S est fini. Soit donc un élément $(h_1,\dots,h_s) \in \prod_{i=1}^{\infty} I_{n-i}^{s_i}$: on sait que $\phi_1(h_1,\dots,h_s) = \left(\sum_{k=1}^{s} h_k\phi'\tau(z_{k1}),\dots,\sum_{k=1}^{s} h_k\phi'\tau(z_{kd})\right)$.

Soit $j \in \{1,\dots,d\}$: on a $\nu\left(\sum_{k=1}^{s} h_k\phi'\tau(z_{kj})\right) \geq \min\{\nu(h_k)+v(z_{kj}) : 1\leq k\leq s\}$. Considérons ensuite $k \in \{1,\dots,s\}$: on dispose alors de $i \geq 1$ tel que $h_k \in I_{n-i}$ et $w(\rho_k - 1) = i$. Puisque $\iota(\rho_k)-1 = \sum_{l=1}^{d} z_{kl}x_l$, on a que $v(z_{kj}) \geq w(\rho_k-1)-1 = i-1$. Ainsi, on obtient que $\nu(h_k)+v(z_{kj}) \geq n-1$ d'où on déduit que $\nu\left(\sum_{k=1}^{s} h_k\phi'\tau(z_{kj})\right) \geq n-1$.

On a ainsi que $\phi_1(h_1,\dots,h_s) \in I_{n-1}^d$.

Montrons que $\phi_0\left(I_{n-1}^d\right) \subseteq I_n$:

Ceci découle clairement du fait que $I_1 I_{n-1} \subseteq I_n$.

Montrons ensuite que ψ_0 est surjective :

Soit $h \in I_n$ et $g \in A$ tel que $\phi'(g) = h$ avec $w(g) \geq n$: un tel g existe puisqu'on a posé $\nu(h) = \max\{w(x) : x \in A, \phi'(x) = h\}$.

Décomposons $\iota(g)$ sous la forme $\iota(g) = \sum_{i=1}^{d} g_i x_i$. Si on note pour $f \in \mathbb{F}_p[\![x_1\dots,x_d]\!]$ et $m \geq 0$ la composante homogène de degré m de f par $f^{(m)}$, on a alors $\iota(g)^{(m)} = \sum_{i=1}^{d} g_i^{(m-1)} x_i$.

Puisque $v(\iota(g)) = w(g) \geq n$, on obtient pour $m < n$ que $g^{(m)} = 0$: en particulier, $g^{(n-1)} = 0$ et donc $v(g_i) \geq n-1$.

En posant $h_i = \phi'\tau(g_i)$ pour $i \in \{1,\dots,d\}$, on a alors que $(h_1,\dots,h_d) \in I_{n-1}^d$ et

$$\psi_0(h_1,\dots,h_d) = \sum_{i=1}^{d} h_i y_i = \phi'\tau\left(\sum_{i=1}^{d} g_i x_i\right) = \phi'(g) = h$$

ce qui montre la surjectivité de ψ_0. □

6.2.3 Preuve du théorème 6.2.1

Commençons par énoncer un lemme dont la preuve est laissée au lecteur :

Lemme 6.2.3 *Supposons qu'on ait une suite exacte de $\mathbb{F}_p$-espaces vectoriels*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D \longrightarrow 0$$

qui induit une suite

$$A' \xrightarrow{\alpha'} B' \xrightarrow{\beta'} C' \xrightarrow{\gamma'} 0$$

où $A' \subseteq A$, $B' \subseteq B$, $C' \subseteq C$, $\alpha' = \alpha\big|_{A'}$, $\beta' = \beta\big|_{B'}$ et $\gamma' = \gamma\big|_{C'}$, avec β' qui est surjective. Alors, la suite induite

$$A/A' \longrightarrow B/B' \longrightarrow C/C' \longrightarrow D \longrightarrow 0$$

est exacte.

Comme évoqué à la partie 6.2.1, nous allons commencer par montrer la propriété suivante :

Proposition 6.2.2 *Pour tout $n \geq 1$, on a $\sum_{i=1}^{n} r_i c_{n-i} - dc_{n-1} + c_n \geq 1$.*

Démonstration : Soit $n \geq 1$. En appliquant le lemme 6.2.3 aux suites considérées aux lemmes 6.2.1 et 6.2.2, nous obtenons une suite exacte

$$B^S/\prod_{i=1}^{\infty} I_{n-i}^{s_i} \xrightarrow{\alpha} B^d/I_{n-1}^d \xrightarrow{\beta} B/I_n \xrightarrow{\gamma} \mathbb{F}_p \longrightarrow 0$$

d'où on déduit que $dim_{\mathbb{F}_p} B^S/\prod_{i=1}^{\infty} I_{n-i}^{s_i} - dim_{\mathbb{F}_p} B^d/I_{n-1}^d + dim_{\mathbb{F}_p} B/I_n - 1 \geq 0$.

En remarquant que $B^S/\prod_{i=1}^{\infty} I_{n-i}^{s_i} = \prod_{i=1}^{\infty} (B/I_{n-i})^{s_i}$ et $B^d/I_{n-1}^d = (B/I_{n-1})^d$, on en déduit que $\sum_{i=1}^{n} s_i c_{n-i} - dc_{n-1} + c_n \geq 1$. Or pour tout $i \geq 1$, on a $r_i \geq s_i$, d'où on déduit l'inégalité souhaitée. □

Le critère découle de la propriété précédente, en notant que celle-ci n'est autre qu'une condition sur les coefficients d'une certaine série formelle :

Théorème 6.2.2 *Si G est un p-groupe fini, alors pour tout $t \in]0,1[$ on a $1 - dt + H_R(t) > 0$.*

Démonstration : Il suffit de remarquer que l'inégalité de la proposition 6.2.2 équivaut à l'inégalité coefficient par coefficient des séries formelles suivantes :

$$(1 - dX + H_R) \sum_{i \geq 1} c_i X^i \geq \frac{1}{1 - X}.$$

Puisque G est fini, l'algèbre B l'est aussi et donc la suite $(c_i)_{i \geq 1}$ est bornée si bien que $\sum_{i \geq 1} c_i X^i$ est de rayon supérieur à 1. En particulier, pour tout $t \in]0,1[$

$$(1 - dt + H_R(t)) \sum_{i \geq 1} c_i t^i \geq \frac{1}{1 - t}$$

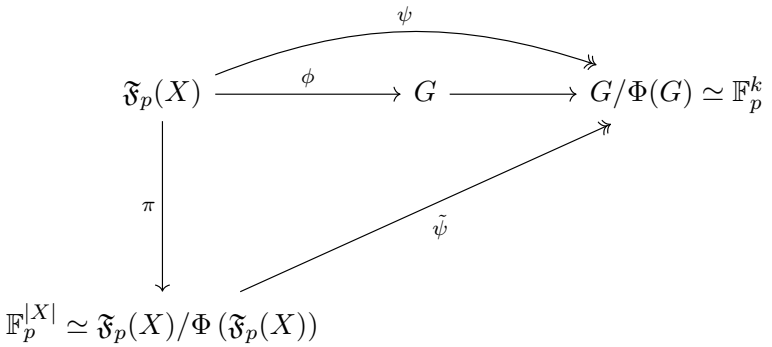
d'où il vient que pour tout $t \in]0,1[$, on a $1 - dt + H_R(t) > 0$, qui constitue le critère annoncé. □

6.3 Une preuve de l'inégalité

Pour établir l'inégalité de Golod et Shafarevich, il faut au préalable obtenir quelques informations supplémentaires sur les valuations des relations, pourvu que le nombre de générateurs soit minimal.

Lemme 6.3.1 *Soit G un p-groupe et $< X|R >$ une présentation topologique de G, où $d = |X|$ est pris minimal. Alors, $R \subseteq \Phi(\mathfrak{F}_p(X))$, où $\Phi(\mathfrak{F}_p(X))$ est le sous-groupe de Frattini de $\mathfrak{F}_p(X)$.*

Démonstration : Soit $\phi : \mathfrak{F}_p(X) \longrightarrow G$ une application continue surjective telle qu'on ait $\operatorname{Ker}\phi = \overline{< R >}$ et $k \in \mathbb{N}$ tel que $G/\Phi(G) \simeq \mathbb{F}_p^k$. On dispose alors du diagramme commutatif suivant :



Supposons par l'absurde que R n'est pas inclus dans $\Phi(\mathfrak{F}_p(X))$. Puisque $R \subseteq \operatorname{Ker}\psi$, il vient donc que $\pi(R) \subseteq \operatorname{Ker}\tilde{\psi}$. Or $\pi(R) \neq 0$ si bien que $\tilde{\psi}$ n'est pas injective et donc que $|X| > k$. Or, par minimalité de X et le lemme 5.1.1, on a $|X| = d(G) = d(G/\Phi(G)) \leq k$, ce qui aboutit à une contradiction.

Finalement, on a donc bien $R \subseteq \Phi(\mathfrak{F}_p(X))$, ce qui conclut. □

Le lemme précédent fournit alors la propriété suivante sur les valuations des relations :

Proposition 6.3.1 *Si G un p-groupe et $< X|R >$ une présentation topologique de G, où $d = |X|$ est pris minimal, alors pour tout $r \in R$, on a $w(r-1) \geq 2$.*

Démonstration : Par le lemme 6.3.1, il suffit de montrer que pour tout élément α de $\Phi(\mathfrak{F}_p(X))$ on a $w(\alpha - 1) \geq 2$. Pour simplifier les notations, posons $F = \mathfrak{F}_p(X)$.

Tout d'abord, tout élément de $[F, F]$ a une valuation supérieure à 2. En effet, si x_i et x_j sont deux indéterminées non commutatives, on a

$$(1+x_i)(1+x_j)(1+x_i)^{-1}(1+x_j)^{-1} = (1+x_i+x_j+f)(1-x_i+g)(1-x_j+h)$$

où f, g, h sont des séries formelles de valuation supérieure à 2. En développant, il s'ensuit donc que $(1+x_i)(1+x_j)(1+x_i)^{-1}(1+x_j)^{-1} - 1$ est de valuation supérieure à 2.

Ensuite, tout élément de F^p est de valuation supérieure à 2, car si x est une indéterminée, alors $(1+x)^p = 1 + x^p$.

On en déduit que tout élément de $\Phi(F) = \overline{F^p[F,F]}$ est de valuation supérieure à 2. En effet, si on note I_2 l'idéal des séries formelles à d indéterminées de valuation supérieure à 2, on vient de montrer que $\iota^{-1}(F^p[F,F]) \subseteq 1 + I_2$ où ι est le morphisme de Lazard. Or I_2 est fermé et il s'ensuit donc que $\iota^{-1}\left(\overline{F^p[F,F]}\right) \subseteq 1 + I_2$, si bien que $w(\Phi(F) - 1) \subseteq [\![2, \infty[\![$, ce qui conclut. □

Donnons une nouvelle démonstration du lemme 5.3.1 dont nous aurons encore besoin :

Lemme 6.3.2 *Si G est un p-groupe, alors $r(G) \geq d(G)$.*

Démonstration : Considérons une présentation topologique $< X|R >$ de G telle que $|X| = d(G)$ et $|R| = r(G)$, que nous noterons respectivement d et r. Écartons d'emblée le cas évident où $r = \infty$.

Dans ce cas, puisque G est un p-groupe et R est fini, le théorème 6.2.1 assure que pour tout $t \in]0,1[$, on a $1 - dt + H_R(t) > 0$. Or $H_R(t) \geq rt$ car aucune relation n'est de valuation nulle, d'après le numéro *(i)* des notations 6.2.1. Ainsi, sur $]0,1[$, on a $1 + (r-d)t > 0$ et donc $r > d$. □

L'inégalité de Golod et Shafarevich est alors une conséquence du théorème 6.2.1 et de la proposition 6.3.1 :

Théorème 6.3.1 *Si G est un p-groupe, alors $r(G) > \dfrac{d(G)^2}{4}$.*

Démonstration : Donnons-nous une présentation topologique $< X, R >$ de G telle que $|X| = d(G)$ et $|R| = r(G)$, que nous noterons respectivement d et r. Écartons d'emblée le cas évident où $r = \infty$.

Dans ce cas, puisque G est un p-groupe et que R est fini, le théorème 6.2.1 fournit que sur $]0,1[$, on a $1 - dt + H_R(t) > 0$. Or, $H_R(t) \geq rt^2$ car d'après la proposition 6.3.1, toute relation est de valuation supérieure ou égale à 2. On en déduit que pour tout $t \in]0,1[$, on a $rt^2 - dt + 1 > 0$.

Or, le minimum de ce trinôme est atteint en $\dfrac{d}{2r}$, lequel appartient à $]0,1[$ d'après le lemme 6.3.2. En évaluant en $\dfrac{d}{2r}$, on trouve finalement que $r > \dfrac{d^2}{4}$, ce qui constitue l'inégalité de Golod et Shafarevich.

□

7 Un contre-exemple au problème de Burnside

Dans cette section, on donne un contre-exemple au problème de Burnside, à l'aide du théorème 6.2.1.

7.1 Énoncé du problème de Burnside

Le problème que souleva Burnside en 1902 s'exprime comme suit :

Question 7.1.1 *Un groupe finiment engendré dont tout élément est d'ordre fini est-il fini?*

La première réponse à cette question a été apportée par Golod et Shafarevich en 1964, dans l'article [2], où un contre-exemple a été exhibé. Une version plus précise du problème est la suivante :

Question 7.1.2 *Un groupe finiment engendré et d'exposant fini est-il fini?*

La réponse est encore négative et la réponse à cette question a été apportée par Novikov et Adjan en 1968 dans une série d'articles.

Nous proposons ici un contre-exemple à la question 7.1.1, la question 7.1.2 étant plus délicate.

7.2 Construction d'un premier contre-exemple

Le contre-exemple au problème de Burnside que nous présentons est donné par sa présentation et repose sur le critère donné par le théorème 6.2.1. Plus précisément, on montre :

Théorème 7.2.1 *Soient p un nombre premier et $d \geq 2$. Il existe un groupe infini engendré par d éléments et tel que tout élément du groupe soit de torsion p-primaire.*

Démonstration : Soit X un ensemble à d éléments. Par la construction donnée en 1.6.1, le pro-p groupe libre sur X est dénombrable : on peut donc énumérer ses éléments différents du neutre par une suite $(f_i)_{i\geq 1}$. Considérons une suite $(n_i)_{\imath\geq 1}$ d'entiers qui sera adaptée par la suite, et considérons les relations $R = \left\{ f_i^{p^{n_i}} : i \geq 1 \right\}$.

Posons G le pro-p groupe de présentation topologique $< X|R >$. Fixons $\tau \in]\frac{1}{d}, 1[$, si bien que $1 - d\tau < 0$. En considérant la suite $(n_i)_{i\geq 1}$ composée de termes suffisamment grands, on a alors :

$$1 - d\tau + H_R(\tau) = 1 - d\tau + \sum_{r\in R} \tau^{w\left(f_i^{p^{n_i}}-1\right)} = 1 - d\tau + \sum_{r\in R} \tau^{w((f_i-1)^{p^{n_i}})} \leq 1 - d\tau + \sum_{r\in R} \tau^{w(f_i-1)p^{n_i}}$$
$$\leq 1 - d\tau + \sum_{r\in R} \tau^{p^{n_i}} < 0.$$

Le théorème 6.2.1 fournit donc que G est infini : puisqu'il est engendré par d éléments et que tout élément est de torsion p-primaire, G convient. □

7.3 Construction d'un second contre-exemple

Nous montrons ici une version plus forte du théorème 7.2.1. Donnons au préalable une définition :

Définition 7.3.1 *Si G est un groupe et $X \subseteq G$, on définit par récurrence les commutateurs à droite de longueur $n \geq 2$ et à termes dans X par :*

- *les commutateurs à droite de longueur 2 sont les commutateurs $[x, y]$ où $x, y \in X$;*
- *les commutateurs à droite de longueurs $n \geq 2$ et à termes dans X étant construits, ceux de longueurs $n + 1$ sont les éléments de la forme $[g, x]$ où $x \in X$ et g est un commutateur de longueur n et à termes dans X.*

On en déduit le lemme suivant, qui n'est autre qu'une reformulation de la définition d'un groupe nilpotent :

Lemme 7.3.1 *Soit $m \geq 1$. Si G est un groupe engendré par $\{g_1, \dots, g_d\}$ dont tous les commutateurs à droite d'ordre m et à termes dans $\{g_1, \dots, g_d\}$ sont nuls, alors G est nilpotent d'ordre inférieur à m.*

Rappelons au préalable une proposition sur les groupes nilpotents (pour une preuve, on pourra se reporter à la remarque qui suit la proposition 5.2.18 de [7]) :

Proposition 7.3.1 *Si G est un groupe nilpotent et finiment engendré qui est de torsion, alors G est fini.*

L'énoncé de la version forte du théorème 7.2.1 est le suivant :

Théorème 7.3.1 *Soient p un nombre premier et $d \geq 2$. Il existe un groupe infini engendré par d éléments, tel que tout élément du groupe soit de torsion p-primaire et tel que tout sous-groupe engendré par $d-1$ éléments soit fini.*

Démonstration : Soit X un ensemble à d éléments. Reprenons la présentation $< X|R >$ donnée dans la preuve du théorème 7.2.1 mais supposons τ pris dans $]\frac{1}{d}, \frac{1}{d-1}[$. Puisque $1 - d\tau + H_R(\tau) < 0$, considérons également $\delta = \tau(d-1)$ et une suite $(m_i)_{i\geq 1}$ d'entiers tels que $1 - d\tau + H_R(\tau) + \sum_{i\geq 1} \delta^{m_i} < 0$.

Comme le pro-p groupe libre sur X est dénombrable, le produit $\prod_{i=1}^{d-1} \mathfrak{F}_p(X)$ l'est également : on peut donc énumérer ses éléments par une famille $\left(f_1^{(i)}, \dots, f_{d-1}^{(i)}\right)_{i\geq 1}$. Pour tout $i \geq 1$, posons alors R_i l'ensemble des commutateurs à droite non triviaux, de longueur m_i et à termes dans $\left\{f_1^{(i)}, \dots, f_{d-1}^{(i)}\right\}$.

Posons également $R' = R \cup \bigcup_{i\geq 1} R_i$ et G' le pro-p groupe de présentation topologique $< X|R' >$.

Commençons par noter que si $x, y \in \mathfrak{F}_p(X)$ alors

$$[x, y] - 1 = (x-1)(y-1)x^{-1}y^{-1} - (y-1)(x-1)x^{-1}y^{-1}$$

si bien que $w([x, y] - 1) \geq w(x-1) + w(y-1)$. On en déduit par récurrence que pour tout $c \in \mathfrak{F}_p(X)$ qui est un commutateur à droite de longueur m sur une famille $(x_i)_{1\leq i\leq m}$, on a

$$w(c-1) \geq w(x_1 - 1) + \cdots + w(x_m - 1).$$

En écrivant $S_i = \left\{(y_1, \dots, y_{m_i}) : y_k \in \left\{f_1^{(i)}, \dots, f_{d-1}^{(i)}\right\}\right\}$ pour $i \geq 1$, on a alors

$$H_{R_i}(\tau) \leq \sum_{(y_1,\dots,y_{m_i})\in S_i} \tau^{w(y_1-1)+\cdots+w(y_{m_i}-1)} = \left(\sum_{k=1}^{d-1} \tau^{w\left(f_k^{(i)}-1\right)}\right)^{m_i} \leq (\tau(d-1))^{m_i} = \delta^{m_i}$$

d'où on déduit que

$$1 - d\tau + H_{R'}(\tau) = 1 - d\tau + H_R(\tau) + \sum_{i\geq 1} H_{R_i}(\tau) \leq 1 - d\tau + H_R(\tau) + \sum_{i\geq 1} \delta^{m_i} < 0.$$

Le théorème 6.2.1 fournit donc que G est infini : de plus, G est engendré par d éléments et tout élément est de torsion p-primaire.

Enfin, si H est un sous-groupe de G et s'il existe $i \geq 1$ tel que H est engendré par $\left\{f_1^{(i)}, \dots, f_{d-1}^{(i)}\right\}$ alors tous ses commutateurs à droite d'ordre m_i et à termes dans $\left\{f_1^{(i)}, \dots, f_{d-1}^{(i)}\right\}$ sont nuls. Le lemme 7.3.1 et la proposition 7.3.1 assurent donc que H est fini : il s'ensuit que G convient. □

8 Références

[1] Mikhail Ershov. Golod-Shafarevich groups: a survey. *Internat. J. Algebra Comput.*, 22(5):1230001, 68, 2012.

[2] Evgenii S. Golod and Igor R. Šafarevič. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

[3] Klaus Haberland. *Galois cohomology of algebraic number fields*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1978. With two appendices by Helmut Koch and Thomas Zink.

[4] Michel Lazard. Groupes analytiques p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (26):389–603, 1965.

[5] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[6] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2000.

[7] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[8] Peter Roquette. On class field towers. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 231–249. Thompson, Washington, D.C., 1967.

[9] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[10] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1998.