ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

SMA

Groupes profinis et cohomologie galoisienne

Rafael GUGLIELMETTI

Travail de semestre supervisé par la Prof. Donna TESTERMAN

Dernière modification le 3 novembre 2011

Table des matières

Résumé

Le but de ce projet est de présenter les groupes profinis et quelques unes de leurs applications, dont une courte introduction à la cohomologie galoisienne. Dans la première partie, nous commencerons par mettre en place les différents outils nécessaires (groupes topologiques ainsi que leurs propriétés, puis les limites projectives), ce qui permettra de présenter deux caractérisations des groupes profinis : l'une topologique et l'autre algébrique, comme limite projective de groupes finis. Grâce à cette deuxième caractérisation, nous verrons comment certaines propriétés des groupes finis se transmettent à la limite (groupes procycliques, par exemple).
Même si, actuellement, les groupes profinis sont utilisés dans des domaines variés, leur développement fut motivé par l'étude du groupe de Galois d'extensions infinies, ce qui sera présenté dans la quatrième section : nous verrons que les groupes de Galois sont des groupes profinis, que, sous certaines conditions, la correspondance de Galois reste correcte et que chaque groupe profini peut être réalisé commme groupe de Galois d'une extension de corps.
Dans la deuxième partie, nous étudierons quelques résultats de base de la cohomologie galoisienne non-abélienne de groupes profinis. En particulier, nous introduirons le problème de descente galoisienne et verrons comment les outils homologiques permettent d'y apporter une réponse.

Chapitre 1

Groupes profinis

1.1 Introduction

Le but de cette partie est d'introduire les différentes notions permettant la définition et l'établissement des premières propriétés des groupes profinis. La première section présente quelques résultats sur les espaces topologiques et les groupes topologiques tandis que la seconde sert à définir les systèmes projectifs et leurs limites.

1.1.1 Préliminaires topologiques

Définition 1.1.1 (Espace totalement discontinu)
Un espace topologique est totalement discontinu *si les seuls ensembles connexes sont l'ensemble vide et les singletons.*

Proposition 1.1.2
Soit X un espace topologique. On a les propriétés suivantes :

(*i*) *Si X est totalement discontinu, alors $\{x\}$ est fermé pour tout $x \in X$.*

(*ii*) *Si X est fini et muni de la topologique discrète, alors il est compact et totalement discontinu.*

Démonstration. On va prouver les différents points séparément.

(i) Soit $x \in X$ et F_x l'adhérence de $\{x\}$ et supposons que $\{x\} \subsetneq F_x$. Puisque F_x contient plus d'un seul élément, il ne peut être connexe. Ainsi, il existe deux ouverts non-vides disjoints U, V avec $x \in U$ et $F_x = U \cup V$. Puisque U est fermé dans F_x et que F_x est fermé, il l'est aussi, ce qui implique $F_x = U$, contradiction.

(ii) L'ensemble X étant fini, il est clair qu'il s'agit d'un espace compact. Soit C un ensemble contenant au moins deux points et $x \in C$. Alors $\{x\} \,|\, \big(C \setminus \{x\}\big)$ est une séparation de C. Ainsi, C n'est pas connexe et donc X est totalement discontinu.

□

Proposition 1.1.3
Soit X un espace topologique compact, de Hausdorff et totalement discontinu. Alors X admet une base d'ouverts fermés.

Démonstration. Voir [RZ00]. □

Proposition 1.1.4
Soit X un espace topologique compact et de Hausdorff ainsi que $x \in X$. La composante connexe C_x de x est l'intersection de tous les voisinages ouverts et fermés de x.

Démonstration. Voir le lemme 1.1.11 de [RZ00]. □

Les quatre propositions suivantes sont souvent utilisées. Leur preuve ne pose pas de difficulté.

Proposition 1.1.5
Soit X un espace topologique. Alors X est de Hausdorff si et seulement si la diagonale $\Delta = \{(x, y) \in X \times X : x = y\}$ est fermée dans $X \times X$.

Proposition 1.1.6

Soient X, Y deux espaces topologiques avec Y de Hausdorff ainsi que $X \overset{f}{\underset{g}{\rightrightarrows}} Y$ deux applications continues. Alors

$$\{x \in X : f(x) = g(x)\}$$

est fermé dans X.

Proposition 1.1.7
Soit X un espace de Hausdorff. Soit $C \subset X$ un sous-ensemble compact de X. Alors X est fermé.

Proposition 1.1.8
Soient X, Y deux espaces topologiques tels que X est compact, Y est de Hausdorff ainsi que $f : X \longrightarrow Y$ une application bijective continue. Alors f est un homéomorphisme.

Groupes topologiques

Définition 1.1.9 (Groupe topologique)
Un groupe $(G, \cdot)$ dont l'ensemble sous-jacent est muni d'une topolgie est dit groupe topologique *si la prise d'inverse et l'opération du groupe $\cdot : G \times G \longrightarrow G$ sont des applications continues pour la topologie sur G (dans le deuxième cas, la topologie sur $G \times G$ est la topologie du produit).*

Remarques 1.1.10 (i) Dans ce document, si on parle simplement d'un groupe, il est sous-entendu qu'il est muni de la topologie discrète. Par contre, un « groupe topologique » est donné avec sa topologie.

(ii) Si nécessaire, la loi du groupe sera notée $\mu : G \times G \longrightarrow G$.

Définition 1.1.11 (Anneau topologique)
Un anneau $(A, +, \cdot)$ est dit anneau topologique *si $(A, +)$ est un groupe topologique est si la loi multiplicative de $A \times A$ dans A est continue.*

Remarque 1.1.12
Chaque anneau considéré sera toujours muni d'un élément neutre pour la multiplication.

Exemples 1.1.13
Comme exemples typiques de groupes topologiques, on a $\mathbb{Q}$ et $\mathbb{R}^n$ qui sont munis de la topologie engendrée par la métrique euclidienne, n'importe quel groupe muni de la topologie discrète, $\mathrm{GL}_n(\mathbb{R})$ muni de la topologie de R^{n^2} (dans ce cas, montrer qu'il s'agit d'un groupe topologique demande un peu de calcul), etc.

Définition 1.1.14 (Morphisme de groupes topologiques)
Un morphisme de groupes topologiques *est un homomorphisme de groupes continu. De même, un isomorphisme de groupes topologiques est un isomorphisme de groupe continu dont l'inverse est continu.*

Proposition 1.1.15 (Propriétés de base des groupes topologiques)
Soit G un groupe topologique. On a les propriétés suivantes :

(*i*) *Soit $h \in G$. L'application $\pi_h : G \longrightarrow G$, qui envoie g sur hg, est un homéomorphisme.*

(*ii*) *Pour tout sous-groupe ouvert (respectivement fermé) H de G et pour tout élément $g \in G$, la classe à gauche gH est ouverte (respectivement fermée).*

(*iii*) *Tout sous-groupe ouvert est fermé.*

(*iv*) *Si G est compact et que $H \leq_o G$, alors H est d'indice fini dans G.*

(*v*) *Si H est un sous-groupe de G contenant un sous-ensemble ouvert U non-vide, alors H est ouvert.*

(*vi*) *Soit H un sous-groupe normal de G. Alors, G/H est un groupe topologique (muni de la topologie quotient).*

(*vii*) *Soit U un sous-ensemble ouvert de G avec $1 \in U$. Alors, il existe un sous-ensemble ouvert V de G avec $1 \in V$ et tel que $V = V^{-1}$ et $VV \subset U$.*

(*viii*) *G est de Hausdorff si et seulement si $\{1\}$ est fermé dans G.*

(*ix*) *Si H est un sous-groupe normal fermé de G, alors G/H est de Hausdorff.*

(*x*) *Si G est totalement discontinu, alors il est de Hausdorff.*

Démonstration. (i) Clair.

(ii) La classe gH est la préimage de H par l'isomorphisme $\pi_{g^{-1}}$.

(iii) Soit H un sous-groupe ouvert de G. On a alors $G \setminus H = \bigcup_{g \notin H} gH$. Puisque chaque classe gH est ouverte, $G \setminus H$ l'est aussi.

(iv) Clair.

(v) On a $H = \bigcup_{h \in H} hU$.

(vi) Le quotient G/H est un groupe et est muni de la topologie usuelle du quotient (remarquons que cette topologie peut être définie même si G/H n'est pas un groupe). L'application $p : G/H \times G/H$ qui envoie (g_1H, g_2H) sur g_1g_2H est continue puisqu'elle peut s'écrire comme composition d'applications continues $p(g_1H, g_2H) = \pi(g_1g_2)$. Le cas de l'inverse se traite de manière semblable.

(vii) Soit W le sous-ensemble de G constitué des paires (g, h) telles que $gh \in U$ (W est la préimage de U pour la loi du groupe). On a que W est ouvert et que $(1, 1) \in W$, ce qui implique l'existence de W_1, W_2 deux ouverts tels que $(1, 1) \in W_1 \times W_2 \subset W$. Alors $V = (W_1 \cap W_2) \cap (W_1^{-1} \cap W_2^{-1})$ satisfait $1 \in V$, $VV \subset U$ et $V = V^{-1}$.

(viii) Dans un espace topologique de Hausdorff, chaque singleton est fermé. Réciproquement, supposons que $\{1\}$ soit fermé dans G. Alors la diagonale Δ, qui est la préimage de $\{1\}$ par l'application continue xy^{-1}, est fermée dans $G \times G$, ce qui implique que G est de Hausdorff.

(ix) Découle directement du point précédent.

(x) Si G est totalement discontinu, $\{1\}$ est fermé (proposition 1.1.2), ce qui implique qu'il est de Hausdorff.

□

Proposition 1.1.16
Soit G un groupe topologique compact, de Hausdorff et totalement discontinu et $\mathcal{N}$ l'ensemble des sous-groupes normaux ouverts de G. Alors $\bigcap_{N\in\mathcal{N}} N = \{1\}$.

Démonstration. Voir [Oss07]. □

Remarque 1.1.17 (Premier théorème d'isomorphisme)
Soit $f : G \longrightarrow H$ un morphisme de groupes topologiques. On sait que $G/_{\ker f} \cong \operatorname{im} f$ en tant que groupes. Cependant, cet isomorphisme n'a aucune bonne raison d'être un isomorphisme de groupes topologiques : l'application induite $\hat{f} : G/_{\ker f} \longrightarrow H$ est continue et bijective mais pas forcément ouverte. Par contre, si G et H possèdent des propriétés supplémentaires (par exemple si G est compact et H est de Hausdorff) alors on aura un isomorphisme de groupes topologiques (proposition 1.1.8). En particulier, le premier théorème d'isomorphisme sera vrai si G et H sont des groupes profinis (voir 1.2.7).

Proposition 1.1.18
Soit G un groupe topologique compact, $\{H_i : i \in I\}$ une famille de sous-ensembles fermés de G telle que pour tous $i, j \in I$, il existe $k \in I$ tel que $H_k \subset H_i \cap H_j$. Alors, si H est un sous-ensemble fermé de G on a :

$$\left(\bigcap_{i\in I} H_i\right) H = \bigcap_{i\in I} H_i H.$$

Démonstration. Le fait que $\left(\bigcap_{i\in I} H_i\right) H \subset \bigcap_{i\in I} H_i H$ est clair.
Pour l'inclusion inverse, soit $g \in \bigcap_{i\in I} H_i H$ et supposons que $g \notin \left(\bigcap_{i\in I} H_i\right) H$, ce qui implique que $gH^{-1} \cap \bigcap_{i\in I} H_i = \emptyset$. Puisque tous ces ensembles sont fermés et que G est compact, il existe $i_1, \ldots, i_n \in I$ tels que

$$gH^{-1} \cap \bigcap_{j=1}^{n} H_{i_j} = \emptyset.$$

Soit $k \in I$ tel que $H_k \subset \bigcap_{j=1}^{n} H_{i_j}$, alors $gH^{-1} \cap H_k = \emptyset$ et donc $g \notin H_k H$, ce qui contredit le fait que $g \in \bigcap_{i\in I} H_i H$. □

1.1.2 Systèmes projectifs et limites projectives

L'approche qui est présentée ici est celle que l'on trouve dans les livres [RZ00] et [Wil98]. J'ai cependant choisi de présenter les définitions des systèmes projectifs et de leurs limites dans un cadre plus général. Les quelques notions de théorie des catégories utilisées peuvent être trouvées dans [Bor94] et [ML98].

Définition 1.1.19 (Ensemble ordonné filtrant)
Un ensemble $(I, \leq)$ est dit ensemble ordonné filtrant *si $(I, \leq)$ est un ensemble partiellement ordonné et si pour tous $i, j \in I$, il existe $k \in I$ tel que $i \leq k$ et $j \leq k$.*

Définition 1.1.20 (Système projectif)
Soient I un ensemble ordonné filtrant. Un système projectif *sur I est la donnée d'une famille d'objets $(X_i)_{i\in I}$ d'une catégorie $\mathscr{C}$ et, pour chaque couple $(i,j) \in I^2$ tel que $i \leq j$, d'un morphisme $\varphi_{ij} : X_j \longrightarrow X_i$. Ces morphismes doivent vérifier les propriétés suivantes :*

(*i*) $\varphi_{ii} = \mathrm{id}_{X_i}$ *pour tout* $i \in I$;

(*ii*) *pour tous* $i,j,k \in I$ *tels que* $i \leq j \leq k$, $\varphi_{ij}\,\varphi_{jk} = \varphi_{ik}$.

Un tel système est noté (X_i, φ_{ij}).

Définition 1.1.21 (Morphismes compatibles)
Soit (X_i, φ_{ij}) un système projectif dans une catégorie $\mathscr{C}$, $X \in |\mathscr{C}|$ et une famille de morphismes $\varphi_i : X \longrightarrow X_i$. La famille $(\varphi_i)_{i\in I}$ est dite compatible *avec le système (X_i, φ_{ij}) si pour tous $i,j \in I$ avec $i \leq j$, on a $\varphi_{ij}\varphi_j = \varphi_i$.*

Définition 1.1.22 (Limite projective)
Soit (X_i, φ_{ij}) un système projectif dans une catégorie $\mathscr{C}$. Une limite projective *(X, φ_i) du système est la donnée d'un couple $(X,\ \varphi_i)$, où $X \in |\mathscr{C}|$ et les φ_i forment une famille de morphismes compatibles. Ce couple doit satisfaire la condition suivante : si $\psi_i : Y \longrightarrow X_i$, $Y \in |\mathscr{C}|$, est une autre famille de morphismes compatibles, alors il existe un unique morphisme $\psi : Y \longrightarrow X$ tel que le diagramme suivant commute pour tous $i \leq j$:*

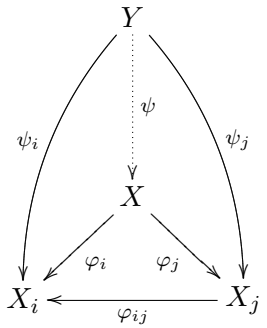


Diagramme 1.1: Limite projective

Proposition 1.1.23 (Unicité de la limite projective)
Si une limite projective (X, φ_i) d'un système projectif (X_i, φ_{ij}) existe, elle est unique à isomorphisme près.

Démonstration. Remarquons tout d'abord que si l'on prend $Y = X$ dans la définition précédente, on a l'existence d'un unique morphisme $\psi : X \longrightarrow X$ tel que le diagramme commute. Puisque id_X remplit ce rôle, il est le seul.
Supposons que (X, φ_i) et (Y, ψ_i) soient deux limites d'un même système projectif. La définition précédente nous assure l'existence d'un morphisme $\psi : Y \longrightarrow X$ faisant commuter le diagramme ci-dessus. En échangeant X et Y, on obtient un morphisme $\tilde{\psi} : X \longrightarrow Y$ avec des propriétés similaires :

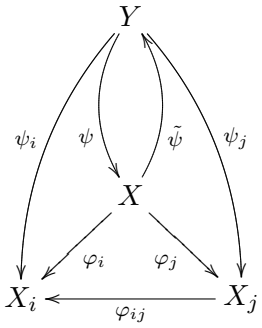


Diagramme 1.2: Unicité de la limite projective

Pour $i \leq j$, regardons :

$$\varphi_{ij}\varphi_j\psi\tilde{\psi} = \varphi_{ij}\psi_j\tilde{\psi} = \varphi_{ij}\varphi_j = \varphi_i.$$

Ainsi, si l'on prend $Y = X$ dans la définition, le morphisme $\psi\tilde{\psi}$ fait commuter le diagramme et donc $\psi\tilde{\psi} = \mathrm{id}_X$. De la même manière, on montre que $\tilde{\psi}\psi = \mathrm{id}_Y$. Ainsi, $X \cong Y$. □

On peut ainsi parler de la limite d'un système projectif et, si elle existe, on la note $\varprojlim_{i\in I} X_i$ ou encore $\varprojlim X_i$.

Proposition 1.1.24 (Existence de la limite projective)
Soit $\mathscr{C}$ une catégorie dans laquelle le produit de toute famille d'objets ainsi que l'égaliseur de toute paire de morphismes existe. Si (X_i, φ_{ij}) est un système projectif dans cette catégorie, alors sa limite projective existe.

Démonstration. Soit $P = \prod_{i\in I} X_i$ et $\pi_i : P \longrightarrow X_i$ les projections. On définit :

$$\alpha : P \longrightarrow \prod_{\substack{i,j\in I \\ i\leq j}} X_i, \quad \alpha_{kl} = \pi_k, \quad \forall k \leq l,$$

$$\beta : P \longrightarrow \prod_{\substack{i,j\in I \\ i\leq j}} X_i, \quad \beta_{kl} = \varphi_{kl}\pi_l, \quad \forall k \leq l.$$

Soit (X, f) l'égaliseur de (α, β) et $\varphi_i = \pi_i f$. Alors (X, φ_i) est la limite projective du système. La situation est la suivante :

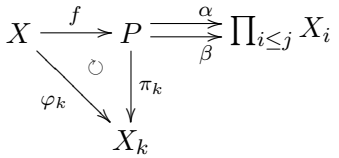


Diagramme 1.3: Existence de la limite projective

Pour vérifier que les φ_i sont bien des morphismes compatibles, soient $i \leq j$ alors :

$$\varphi_{ij}\varphi_j = \varphi_{ij}\pi_j f = \beta_{ij} f = \alpha_{ij} f = \pi_i f = \varphi_i.$$

L'universalité de X provient de celle de l'égaliseur. □

La proposition précédente nous permet d'affirmer l'existence de la limite de systèmes projectifs d'espaces topologiques, groupes topologiques, anneaux topologiques, etc. La proposition suivante explicite une telle limite dans le cas des espaces topologiques et groupes topologiques.

Proposition 1.1.25 (Description de limites projectives)
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques (respectivement groupes topologiques). On pose $P = \prod_{i\in I} X_i$, muni de la topologie usuelle du produit, les projections $\pi_i : P \longrightarrow X_i$, et on considère le sous-espace suivant

$$X = \big\{x = (x_i)_{i\in I} \in P : \forall i \leq j, x_i = \varphi_{ij}(x_j)\big\},$$

ainsi que les restrictions $\varphi_i = \pi_i\big|_X$. Alors (X, φ_i) est la limite projective du système.

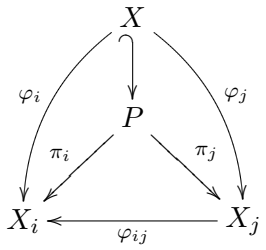


Diagramme 1.4: Description de la limite projective

Démonstration. Il est clair que les φ_i sont des applications continues (comme restriction des projections qui sont continues) et il s'agit d'applications compatibles de part la définition de X. Il reste à montrer que (X, φ_i) satisfait la propriété universelle. Pour cela, soit Y un espace topologique et $(\psi_i)_{i\in I}$ des applications continues compatibles. On pose :

$$\begin{array}{rcl} \tilde{\psi} : Y & \longrightarrow & P \\ y & \longmapsto & \big(\psi_i(y)\big)_{i\in I} \end{array}$$

et on a alors $\pi_i\tilde{\psi}(y) = \psi_i(y)$, pour tout $i \in I$. Soient $i, j \in I$ tels que $i \leq j$, alors

$$\pi_i\tilde{\psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\tilde{\psi},$$

ce qui implique que $\mathrm{im}(\tilde{\psi}) \subset X$. On peut ainsi poser $\psi = \tilde{\psi}$. Pour l'unicité, supposons que $\varphi : Y \longrightarrow X$ soit une application continue telle que $\varphi_i\varphi = \psi_i$, pour tout $i \in I$. Il faut montrer que $\psi = \varphi$, c'est-à-dire que $\pi_i\psi = \pi_i\varphi$ pour tout $i \in I$, ou encore $\varphi_i\psi = \varphi_i\varphi$, ce qui est le cas puisque les deux termes valent ψ_i.
Le fait que les φ_{ij} soient des homomorphismes de groupe implique que X est un sous-groupe de P. De plus, les φ_i sont clairement des homomorphismes de groupes. □

Notation 1.1.26
Je noterai souvent « soit (X_i, φ_{ij}) un système projectif ». Il sera alors sous-entendu :

(i) que l'ensemble filtrant est I.

(ii) que les projections sont φ_i.

Exemples 1.1.27 (i) Soit E un ensemble et $F = \{X_i : i \in I\}$ une famille de sous-ensembles de E telle que pour tous $X_i, X_j \in F$, il existe $X_k \in F$ avec $X_k \subset X_i$ et $X_k \subset X_j$. Définissons un ordre sur I par : $i \leq j \Leftrightarrow X_j \subset X_i$ et, pour $i \leq j$, $\varphi_{ij} : X_j \hookrightarrow X_i$ est l'inclusion canonique. Alors la limite $\varprojlim X_i$ peut être identifiée avec l'intersection des X_i (si $N = \bigcap_I X_i$; il s'agit de la diagonale du produit $\prod_I N$).

(ii) Soit $p \in \mathbb{P}$ et, pour $n \in \mathbb{N}$, posons $G_n = \mathbb{Z}/p^n\mathbb{Z}$. Pour $i \leq j$, on définit :

$$\begin{array}{rcl} \varphi_{ij} : G_j & \longrightarrow & G_i \\ k + p^j\mathbb{Z} & \longmapsto & k + p^i\mathbb{Z}. \end{array}$$

On voit qu'alors (G_i, φ_{ij}) est un système projectif. Ce système sera présenté plus en détails par la suite.

(iii) Soit $\{X_i\}_{i\in I}$ une collection infinie d'espaces topologiques. On va voir qu'il est possible d'exprimer le produit $P = \prod_{i\in I} X_i$ comme une limite projective de produits finis. L'ensemble $\mathcal{I} = \{F : F \subset I, |F| < \infty\}$, que l'on muni de l'ordre naturel de l'inclusion, est un ensemble filtrant. Pour $F \in \mathcal{I}$, on pose $P_F = \prod_{i\in F} X_i$. Pour $F, G \in \mathcal{I}$ avec $F \subset G$, on définit $\varphi_{FG} : P_G \longrightarrow P_F$ qui projette un élément de P_G dans P_F. On voit qu'alors (P_F, φ_{FG}) est un système projectif et on va montrer que $\varprojlim P_F = P$. Pour cela, soit φ l'application suivante :

$$\begin{array}{rcl} \varphi : P & \longrightarrow & \displaystyle\prod_{F\in\mathcal{I}} P_F \\ x & \longmapsto & \varphi(x), \text{ où } \varphi(x)_F = x_F. \end{array}$$

On va montrer les différents points :
- $\mathrm{im}(\varphi) \subset \varprojlim P_F$:
  Soit $x \in P$ et $F, G \in \mathcal{I}$ tels que $F \subset G$. On voit qu'alors $\varphi_{FG}(x_G) = x_F$, ce qui implique que $\varphi(x) \in \varprojlim P_F$.
- Injectivité de φ :
  Supposons que $\varphi(x) = \varphi(y)$, ce qui implique que $x_F = y_F$ pour tout $F \in \mathcal{I}$. En particulier, $x_{\{i\}} = y_{\{i\}}$ pour tout $i \in I$.
- Surjectivité de φ :
  Soit $y \in \varprojlim P_F$ et posons $x_i = y_{\{i\}}$. Alors $\varphi(x) = y$.
- Puisque les composantes de φ sont des projections ils s'agit d'une application continue et ouverte.

Les points précédents impliquent que φ est un homéomorphisme entre P et $\varprojlim P_F$.

1.1.3 Propriétés des limites projectives

Les propositions ci-dessous concernent les propriétés dont hérite la limite d'un système projectif.

Proposition 1.1.28
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques de Hausdorff et $P = \prod_{i\in I} X_i$. Alors $\varprojlim X_i$ est fermé dans P.

Démonstration. Soit $x \in P \setminus \varprojlim X_i$, ce qui implique l'existence de $k, l \in I$ avec $k \leq l$ et tels que $x_k \neq \varphi_{kl}(x_l)$. Puisque X_k est de Hausdorff, il existe V_1, V_2 deux ouverts

tels que $x_k \in V_1$, $\varphi_{kl}(x_l) \in V_2$ et $V_1 \cap V_2 = \emptyset$. L'application φ_{kl} étant continue, il existe un voisinage ouvert $W \subset X_l$ de x_l tel que $\varphi_{kl}(W) \subset V_2$. Posons, pour $i \neq k$ et $i \neq l$, $W_i = X_i$, $W_k = V_1$ et $W_l = W$. Alors $\prod_{i \in I} W_i$ est un voisinage de x contenu dans $P \setminus \varprojlim X_i$. □

Remarque 1.1.29
La condition de Hausdorff dans la proposition ci-dessus est nécessaire. Par exemple, si l'on prend le système constitué de deux espaces topologiques $X_1 = X_2$, où X_1 est un espace qui n'est pas de Hausdorff et $\varphi_{12} : X_2 \longrightarrow X_1$ l'identité, alors $\varprojlim X_i$ n'est pas fermé dans $X_1 \times X_1$. En effet, on a que $\varprojlim X_i = \Delta$, la diagonale du produit, et l'on sait que Δ est fermée si et seulement si X_1 est de Hausdorff (proposition 1.1.5).

Corollaire 1.1.30
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques compacts de Hausdorff. Alors, $\varprojlim X_i$ est compact.

Démonstration. Le théorème de Tychonov nous assure que $P = \prod_{i \in I} X_i$ est un espace compact. Puisque $\varprojlim X_i$ est fermé dans P, il est compact. □

Proposition 1.1.31
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques. Alors :

(i) si chaque X_i est de Hausdorff, la limite l'est aussi ;

(ii) si chaque X_i est totalement discontinu, la limite l'est aussi.

Démonstration. (i) Clair.

(ii) Soit C un sous-ensemble connexe de $\varprojlim X_i$. Puisque chaque projection φ_i est continue, $\varphi_i(C)$ est un sous-ensemble connexe de X_i et donc est un singleton. Il s'ensuit que C est un singleton.

□

Proposition 1.1.32
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques et X sa limite projective. Alors

$$\mathcal{B} = \{\varphi_i^{-1}(U) : i \in I, U \text{ ouvert dans } X_i\}$$

est une base pour la topologie de X.

Démonstration. Les ouverts de base de $P = \prod_{i \in I} X_i$ sont des unions d'ouverts du type $\prod_{i \in I} W_i$, où l'ouvert W_j est tel que $W_j \neq X_j$ pour au plus un nombre fini d'indice. Ainsi, un ouvert de X est une union d'ouverts de la forme

$$O = X \cap \pi_{i_1}^{-1}(U_{i_1}) \cap \ldots \cap \pi_{i_n}^{-1}(U_{i_n}),$$

où chaque U_{i_j} est ouvert dans X_{i_j}. Ainsi, il suffit de montrer que pour tout $x \in O$, il existe $l \in I$ et un ouvert U_l de X_l tel que $x \in \varphi_l^{-1}(U_l) \subset O$.
Soit donc O comme ci-dessus et $x \in O$. Puisque I est un ensemble filtrant, il existe $l \in I$ tel que $i_j \leq l$ pour $j = 1, \ldots, n$. Pour chaque j, posons $W_j = {\varphi_{i_j l}}^{-1}(U_{i_j})$, qui est un ouvert de X_l, et $U_l = \bigcap_{j=1}^n W_j$. Puisque $x_l \in U_l$, $\pi_l^{-1}(U_l)$ est un voisinage ouvert de x. Il reste à voir que $\pi_l^{-1}(U_l) \subset O$. Pour cela, soit $y \in \pi_l^{-1}(U_l)$. On a alors, $y_l \in U_l$ et il faut voir que $y_{i_j} \in U_{i_j}$ pour tout j, ce qui est le cas car $y_{i_j} = \varphi_{i_j k}(y_k)$.
On vérifie alors que la topologie engendrée par $\mathcal{B}$ n'est pas plus fine que celle du produit. □

Proposition 1.1.33
Soit (G_i, φ_{ij}) un système projectif de groupes topologiques, G sa limite projective et H un sous-groupe ouvert de G. Alors il existe $l \in I$ tel que $\ker \varphi_l \leq H$.

Démonstration. Puisque $1 \in H$ et que H est ouvert, la proposition précédente nous assure l'existence de $l \in I$ et d'un ouvert U_l de G_l tel que $1 \in \varphi_l^{-1}(U_l) \subset H$. De plus, puisque $1_l \in U_l$, on a $\ker \varphi_l \subset \varphi_l^{-1}(U_l) \subset H$, comme désiré. □

Proposition 1.1.34
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques compacts de Hausdorff, X sa limite et Y un sous-espace fermé de X. Alors, $Y = \varprojlim \varphi_i(Y)$.

Démonstration. Voir [RZ00]. □

Proposition 1.1.35
Soit (X_i, φ_{ij}) un système projectif d'espaces topologiques non-vides compacts et de Hausdorff. Alors $\varprojlim X_i \neq \emptyset$.

Démonstration. Pour $i \leq j$, on définit

$$C_{ij} = \{x \in \prod_{i \in I} X_i : x_i = \varphi_{ij}(x_j)\},$$

et l'on voit que

$$X = \varprojlim X_i = \bigcap_{k \leq l} C_{kl}.$$

Puisque X_i est de Hausdorff, C_{kl} est fermé dans le produit (proposition 1.1.6), pour tout $k \leq l$. Si la limite X est vide, cela implique l'existence de $i_1, \ldots, i_n$ et $j_1, \ldots, j_n$, avec $i_k \leq j_l$ pour tout k, tels que $\bigcap_{k=1}^n C_{i_k j_k} = \emptyset$ (X est compact). Puisque I est un ensemble filtrant, il existe $m \geq j_1, \ldots, j_n$. On choisit x_m dans X_m, qui n'est pas vide et on pose $x_{j_k} = \varphi_{j_k m}(x_m)$, pour $k = 1, \ldots, n$. Pour les autres indices, on choisit x_i de manière arbitraire. On a ainsi un élément $x \in \prod_{i \in I} X_i$ qui appartient à $\bigcap_{k=1}^n C_{i_k j_k}$, contradiction. □

Proposition 1.1.36
Soit (X_i, φ_{ij}) un système projectif surjectif (c'est-à-dire que les φ_{ij} sont surjectifs) d'espaces topologiques non-vides compacts de Hausdorff. Alors, pour chaque $i \in I$, la projection $\varphi_i : \varprojlim X_i \longrightarrow X_i$ est surjective.

Démonstration. Voir [RZ00]. □

1.2 Pro-$\mathcal{C}$ groupes

1.2.1 Caractérisations des groupes profinis

Remarque 1.2.1
Dans ce qui suit, une *classe* $\mathcal{C}$, par exemple la classe des groupes finis, désignera toujours une classe fermée par rapport aux isomorphismes. C'est-à-dire que si $F \in \mathcal{C}$ et $G \cong F$, alors $G \in \mathcal{C}$.

Définition 1.2.2 (Pro-$\mathcal{C}$ groupe)
Soit $\mathcal{C}$ une classe de groupes finis. Un pro-$\mathcal{C}$ groupe *est la limite d'un système projectif surjectif de groupes (G_i, φ_{ij}), où $G_i \in \mathcal{C}$ est muni de la topologie discrète. La limite est un groupe topologique muni de la topologie de sous-espace du produit.*

Définition 1.2.3 (Produit sous-direct)
Soit G_i, $i \in I$, une collection de groupes et G un groupe. On dit que G est le produit sous-direct *des G_i s'il existe une collection de sous-groupes normaux N_i, $N_i \trianglelefteq G$, tels que $\bigcap_{i\in I} N_i = \{1\}$ et $G/_{N_i} \cong G_i$.*

Remarque 1.2.4
Supposons qu'un groupe G soit le produit sous-direct d'une collection $\{N_i\}$, comme ci-dessus. Alors G est isomorphe à un sous-groupe du produit $\prod G_i$. En effet, on considère :

$$\varphi : G \longrightarrow \prod_i G/_{N_i} \cong \prod_i G_i,$$

qui envoie $g \in G$ sur sa classe pour chacune des composantes. La condition $\bigcap_i N_i = \{1\}$ nous assure l'injectivité de φ.

Définition 1.2.5 (Formation)
Une formation *est une classe $\mathcal{C}$ de groupes finis telle que $\mathcal{C}$ est fermée par passage au quotient et telle que si G est un groupe possédant deux sous-groupes normaux N_1, N_2 tels que $G/_{N_1}, G/_{N_2} \in \mathcal{C}$ alors $G/_{N_1 \cap N_2} \in \mathcal{C}$. Cette dernière condition est équivalente à dire que $\mathcal{C}$ est fermée pour les produits sous-directs finis.*

Définition 1.2.6 (Cas particuliers de pro-$\mathcal{C}$ groupes)
Selon la classe $\mathcal{C}$ de groupes considérés, les pro-$\mathcal{C}$ groupes prennent un nom particulier. Par exemple, si la classe $\mathcal{C}$ est :

(*i*) *la classe des groupes finis, alors un pro-$\mathcal{C}$ groupe est un groupe* profini *;*

(*ii*) *la classe des groupes abéliens finis, alors un pro-$\mathcal{C}$ groupe est un groupe* pro-abélien.

Théorème 1.2.7
Soit $\mathcal{C}$ une formation de groupes finis fermée par prise de sous-groupes et G un groupe topologique. Alors les conditions suivantes sont équivalentes :

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

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

(*iii*) *G est compact, 1 admet un système fondamental de voisinages ouverts $\mathcal{I}$ tel que $\bigcap_{N\in\mathcal{I}} N = \{1\}$ et tout $N \in \mathcal{I}$ est un sous-groupe normal de G avec $G/_N \in \mathcal{C}$.*

(*iv*) *L'élément neutre de G admet un système fondamental de voisinages ouverts $\mathcal{I}$ tel que $\bigcap_{N\in\mathcal{I}} N = \{1\}$ et tout $N \in \mathcal{I}$ est un sous-groupe normal de G avec $G/_N \in \mathcal{C}$ et $G \cong \varprojlim_{N\in\mathcal{I}} G/_N$.*

Démonstration. $(i) \Rightarrow (ii)$ Puisque G est la limite d'un système projectif (G_i, φ_{ij}) de groupes finis (chaque G_i est compact, de Hausdorff, totalement discontinu), le corollaire 1.1.30 et la proposition 1.1.31 impliquent que G hérite de ces propriétés.

Soit maintenant $N \trianglelefteq_o G$. La proposition 1.1.33 nous assure l'existence de $l \in I$ tel que $\ker \varphi_l \leq N \leq G$. Puisque $G/\ker \varphi_l \cong \operatorname{im} \varphi_l \leq G_l$ et que la classe $\mathcal{C}$ est fermée pour les sous-groupes, $G/\ker \varphi_l \in \mathcal{C}$. De plus, le fait que la classe soit fermée par passage au quotient et que

$$G/N \cong \left(G/\ker \varphi_l\right) / \left(N/\ker \varphi_l\right)$$

implique que $G/N \in \mathcal{C}$.

$(ii) \Rightarrow (iii)$ La proposition 1.1.3 (et sa démonstration) nous assure l'existence d'un système fondamental $\mathcal{I}$ de voisinages de l'unité tel que $\bigcap_{I \in \mathcal{I}} I = \{1\}$. Il reste à montrer que tout $I \in \mathcal{I}$ contient un sous-groupe normal ouvert N. Pour $I \in \mathcal{I}$, posons $F = (G \setminus I) \cap I^2$, qui est fermé car I^2 est fermé par la proposition 1.1.7. Soit $x \in I$. Puisque G est de Hausdorff et compact, et que I est ouvert et fermé, I est compact. Ainsi, il existe des voisinages ouverts V_x, W_x de x et de 1, respectivement, tels que $V_x, W_x \subset I$ et $V_x W_x \subset G \setminus F$. En effet, le fait que $1, x \in I$ implique l'existence d'ouverts $V, W \subset I$ avec $1 \in W$ et $x \in V$. La continuité de la loi du groupe et le fait que $G \setminus F$ soit ouvert implique l'existence de deux ouverts V', W' tels que $(1, x) \in W' \times V' \subset \mu^{-1}(G \setminus F)$ (μ désigne la loi du groupe). On peut alors prendre $V_x = V \cap V'$ et $W_x = W \cap W'$.

La collection $\{V_x : x \in I\}$ est un recouvrement d'ouverts de I et, par compacité de I, il existe $n \in \mathbb{N}$ ainsi que $x_1, \ldots, x_n$ tels que $I \subset \bigcup_{i=1}^n V_{x_i}$.

Posons $W = \bigcap_{i=1}^n W_{x_i}$ et $Z = W \cap W^{-1}$. L'ouvert Z est donc un voisinage ouvert de 1 qui est fermé par prise d'inverse. Il lui reste encore deux défauts : il n'est pas fermé pour le produit d'éléments et, à fortiori, n'est pas normal dans G.

Pour « fermer » Z par rapport aux produits d'éléments, considérons l'ensemble suivant : $H = \bigcup_{k \in \mathbb{N}} Z^k$, où Z^k est l'ensemble des produits de k éléments de Z. Il faut vérifier que le sous-groupe H de G est inclus dans I. Pour commencer, montrons que $IZ \subset I$. Soit $x \in IZ$, alors $x \in G \setminus F$ (cela provient de la condition $V_x W_x \subset G \setminus F$ ci-dessus et de la définition de Z), ce qui implique que $x \notin G \setminus I$ ou $x \notin I^2$. Puisque $x \in I^2$, alors, $x \in I$. Ainsi, $IZ \subset I$. Par récurrence, on a que $IZ^k \subset I$ pour tout $k \in \mathbb{N}$ et, en particulier, $Z^k \subset I$, ce qui implique que $H \subset I$.

Il reste à normaliser le H ; pour cela, on pose $N = \bigcap_{g \in G} gHg^{-1}$ qui est normal dans G. Puisque G est compact et que H est ouvert, il est d'indice fini (proposition 1.1.15 (iv)) et donc ne possède qu'un nombre fini de conjugués, ce qui implique que N est ouvert. Comme $N \leq H$, il satisfait aux propriétés demandées.

$(iii) \Rightarrow (iv)$ On va mettre un ordre $\leq_{\mathcal{I}}$ sur $\mathcal{I}$: pour $I, J \in \mathcal{I}$, $I \leq_{\mathcal{I}} J$ si et seulement si $J \leq I$. Ainsi, $\mathcal{I}$ devient un ensemble filtrant, car si $I, J \in \mathcal{I}$, alors $I \cap J$ est un voisinage de 1 et donc il existe $K \in \mathcal{I}$ tel que $K \subset I \cap J$, ce qui implique $I \leq_{\mathcal{I}} K$ et $J \leq_{\mathcal{I}} K$.

Pour $I \in \mathcal{I}$, on définit $G_I = G/I$ et pour $I \leq_{\mathcal{I}} J$ on pose :

$$\begin{aligned} \varphi_{IJ} : G_J &\longrightarrow G_I \\ gJ &\longmapsto gI, \end{aligned}$$

qui est bien défini car $J \leq I$. On voit qu'alors (G_I, φ_{IJ}) est un système projectif de groupes topologiques. Soit $\tilde{G}$ sa limite. Il reste à montrer que $\tilde{G} \cong G$. Pour cela, on définit l'application suivante :

$$\begin{aligned} \varphi : G &\longrightarrow \tilde{G} \\ g &\longmapsto \varphi(g), \text{ où } \varphi(g)_I = gI. \end{aligned}$$

Par définition des φ_{IJ}, on remarque que φ est bien définie, c'est-à-dire que $\operatorname{im}\varphi \subset \tilde{G}$. Puisque φ est constituée de projections, elle est continue. Puisque G est compact et que $\tilde{G}$ est de Hausdorff (chaque G_I est de Hausdorff, puisque I est fermé dans G, voir point (ix) de 1.1.15), le fait que φ soit continue et bijective entraînera que φ soit un homéomorphisme (proposition 1.1.8).
Pour l'injectivité, supposons que $\varphi(g) = \varphi(h)$, ce qui implique que pour tout $I \in \mathcal{I}$, $gI = hI$ et donc que $gh^{-1} \in I$. Puisque l'intersection de tous les sous-groupes de $\mathcal{I}$ est triviale, on a $g = h$.
La surjectivité de φ provient de celle des φ_I.

$(iv) \Rightarrow (i)$ Clair.

$(ii) \Rightarrow (i)$ Même si cette étape n'est pas nécessaire puisque les équivalences ont déjà été démontrées, il peut être intéressant de voir comment réaliser la preuve. L'idée est de considérer le système projectif constitué des G/H, où H est un sous-groupe normal ouvert de G. On montre qu'alors G est la limite de ce système projectif.
Remarque :
On utilise pour cela la proposition 1.1.16.

□

Remarque 1.2.8
Au point (iii) de la caractérisation ci-dessus, l'ensemble $\mathcal{I}$, constitué de sous-groupes ouverts est une base de filtres. Puisque chaque $I \in \mathcal{I}$ est normal, cela permet de définir une unique topologie compatible sur G (voir [Bou07]). Puisque $\bigcap_{N \in \mathcal{I}} N = \{1\}$, la topologie définie sera de Hausdorff. Le fait que l'espace ainsi créé soit totalement discontinu provient de la proposition 1.1.4.

Remarque 1.2.9
La classe des groupes finis, celle des groupe cycliques, celle des groupes abéliens finis, sont des classes qui satisfont toutes les bonnes propriétés demandées dans le théorème ci-dessus.

Définition 1.2.10 (Anneau profini)
Un anneau profini *est un anneau obtenu comme limite d'un système projectif d'anneaux finis (munis de la topologie discrète).*

On a alors une caractérisation des anneaux profinis semblable à celle des groupes profinis. La preuve du théorème suivant peut être trouvée dans [RZ00].

Théorème 1.2.11
Soit R un anneau topologique. Alors les conditions suivantes sont équivalentes :

- (i) *R est un anneau profini.*
- (ii) *R est compact et de Hausdorff.*
- (iii) *R est compact, de Hausdorff et totalement discontinu.*

(*iv*) *R est compact et l'élément 0 possède un système fondamental de voisinages consistant d'idéaux ouverts de R.*

(*v*) *Il existe un système projectif surjectif (R_i, φ_{ij}) d'anneaux finis tel que $R = \varprojlim R_i$.*

Exemples 1.2.12 (i) Soit R un anneau profini. Alors R^* est profini. Le fait que R^* soit de Hausdorff et totalement discontinu est clair. Pour ce qui est de la compacité, on considère le sous ensemble A de $R \times R$ constitué des préimages de 1 pour la loi multiplicative de l'anneau. Comme $R \times R$ est compact et que A est fermé, il est compact. Ensuite, R^* est compact.

(ii) Soit R un anneau profini. Alors le groupe $\mathrm{GL}_n(R)$ est profini. Cela découle du point précédent et du fait que $\mathrm{M}_n(R) \cong R^{n^2}$ est profini (caractérisation (*ii*)).

Proposition 1.2.13
Soit $G = \varprojlim_i G_i$ un groupe profini. Alors les $\ker \varphi_i$ forment un système fondamental de voisinages ouverts pour 1.

Démonstration. Puisque G est profini, l'unité possède un système fondamental de voisinage consitué de sous-groupes normaux ouverts. On conclut en utilisant la proposition 1.1.33. □

Définition 1.2.14 (Pro-$\mathcal{C}$ complétion d'un groupe)
Soit $\mathcal{C}$ une formation non-vide de groupes finis et G un groupe. Soit la collection

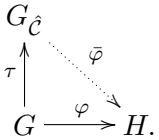
$$\mathcal{I} = \{I \trianglelefteq_f G : G/_I \in \mathcal{C}\},$$

qui n'est pas vide, puisque $G \in \mathcal{I}$. On suppose que $\mathcal{I}$ vérifie la propriété suivante : pour tous $I, J \in \mathcal{I}$, il existe $K \in \mathcal{I}$ tel que $K \leq I \cap J$.
On définit alors un ordre sur $\mathcal{I}$ par $I \leq_{\mathcal{I}} J$ si et seulement si $J \leq I$, ce qui fait de $\mathcal{I}$ un ensemble filtrant. On peut alors considérer le système projectif $(G/_I, \varphi_{IJ})$, où $\varphi_{IJ} : G/_J \longrightarrow G/_I$ envoie gJ sur gI. La pro-$\mathcal{C}$ complétion *de G, notée $G_{\hat{\mathcal{C}}}$ est :*

$$G_{\hat{\mathcal{C}}} = \varprojlim_{I \in \mathcal{I}} G/_I.$$

Selon les cas, il peut être plus facile de travailler avec une autre définition de la pro-$\mathcal{C}$ complétion d'un groupe. Cela repose sur le lemme suivant :

Lemme 1.2.15
Soit $\mathcal{C}$ une formation de groupes finis et G un groupe. Alors, la pro-$\mathcal{C}$ complétion de G est la donnée d'un pro-$\mathcal{C}$ groupe $G_{\hat{\mathcal{C}}}$ et d'un homomorphisme continu $\tau : G \longrightarrow G_{\hat{\mathcal{C}}}$ tel que $\mathrm{im}\,\tau$ est dense dans $G_{\hat{\mathcal{C}}}$ et telle que la propriété universelle suivante soit satisfaite : pour tout pro-$\mathcal{C}$ groupe H et tout homomorphisme continu $\varphi : G \longrightarrow H$, il existe un unique morphisme de groupes topologiques $\bar{\varphi} : G_{\hat{\mathcal{C}}} \longrightarrow H$ tel que le diagramme suivant commute



De plus, il suffit de vérifier la condition ci-dessus pour $H \in \mathcal{C}$.

Démonstration. Voir lemme 3.2.1 de [RZ00]. □

Dans le cas où $\mathcal{C}$ est la classe de groupes finis (respectivement la classe des p-groupes), on l'appellera *complétion profinie* (respectivement *p-complétion*), que l'on notera $\hat{G}$ (respectivement $G_{\hat{p}}$). Les deux premiers exemples, qui seront étudiés plus en détails ci-dessous, sont :

$$\begin{aligned}\hat{\mathbb{Z}} &= \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} \\ \mathbb{Z}_{\hat{p}} &= \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.\end{aligned}$$

Remarque : le complété $\mathbb{Z}_{\hat{p}}$ est usuellement noté $\mathbb{Z}_p$ et est appelé groupe des entiers p-adiques (et cette convention sera utilisée dans ce document).

1.2.2 Complété profini et p-complétion de $\mathbb{Z}$

Dans cette section, on va présenter plus en détails les groupes $\mathbb{Z}_p$ et $\hat{\mathbb{Z}}$ mentionnés ci-dessus. Soit $G_n = \mathbb{Z}/n\mathbb{Z}$. Afin de définir un système projectif sur les G_n, il faut décider d'un ordre $\leq'$ sur $\mathbb{N}$ (on rappelle que l'on considère $0 \notin \mathbb{N}$).
Pour $n \leq' m$, on aimerait pouvoir définir un morphisme $\varphi_{nm} : G_m \longrightarrow G_n$ qui envoie $k + m\mathbb{Z}$ sur $k + n\mathbb{Z}$. Cependant, celui-ci n'est bien défini que si $n \mid m$. Ainsi, l'ordre convenable sur $\mathbb{N}$ est $n \leq' m$ si et seulement si $n \mid m$. Dans ce cas, si $a \in \hat{\mathbb{Z}}$, on doit avoir

$$a_n \equiv a_m \pmod{n}, \quad \forall n \mid m.$$

Le complété $\hat{\mathbb{Z}}$ hérite des structures d'anneaux des G_n (les opérations sont définies composantes par composante) et on peut identifier $\mathbb{Z}$ à un sous-anneau de $\hat{\mathbb{Z}}$ en associant à chaque $z \in \mathbb{Z}$ l'élément $\varphi(z)$ dont toutes les composantes sont z.
Dans le cas des groupes $H_n = \mathbb{Z}/p^n\mathbb{Z}$, l'ordre sur $\mathbb{N}$ est l'ordre usuel et, pour $n \leq m$, on définit l'application surjective φ_{nm} de manière évidente :

$$\varphi_{nm}\big(k + \mathbb{Z}/p^m\mathbb{Z}\big) = k + \mathbb{Z}/p^n\mathbb{Z}.$$

Ainsi, si $a \in \mathbb{Z}_p$, on doit avoir

$$a_n \equiv a_m \pmod{p^n}, \quad \forall n \leq m.$$

Proposition 1.2.16 (Identification de $\mathbb{Z}_p$ avec des séries formelles)
On peut identifier $\mathbb{Z}_p$ avec l'ensemble des séries entières

$$A = \Big\{a = \sum_{n=0}^{\infty} a_n p^n : a_n \in \mathbb{N}_0, 0 \leq a_n < p\Big\}.$$

Démonstration. Pour cela, définissons $\varphi : A \longrightarrow \mathbb{Z}_p$, qui envoie a sur $\varphi(a)$, où

$$\varphi(a)_n = \left(\sum_{j=0}^{n-1} a_j p^j\right) + p^n\mathbb{Z}.$$

L'injectivité de φ provient du fait que pour $a \in A$, chaque a_i est strictement inférieur à p. Pour la surjectivité, soit $b \in \mathbb{Z}_p$ et posons $a_0 = b_1$. Pour $n \geq 1$, le fait que $b \in \mathbb{Z}_p$ implique que $b_n \equiv b_{n+1} \pmod{p^n}$. Ainsi, il existe $a_n \in \mathbb{N}$ tel que $b_{n+1} - b_n = a_n p^n$. Vérifions que $\varphi(a) = b$:

$$\varphi(a)_n = a_0 + \sum_{i=1}^{n-1}(b_{i+1} - b_i) + p^n\mathbb{Z} = a_0 - b_1 + b_n + p^n\mathbb{Z} = b_n + p^n\mathbb{Z}.$$

On a envie que la bijection entre les deux ensembles devienne un isomorphisme d'anneaux. Pour cela, on définit pour $a, b \in A$ leur somme et leur produit :

$$\begin{aligned} a+b &= \varphi^{-1}\big(\varphi(a)+\varphi(b)\big) \\ a\cdot b &= \varphi^{-1}\big(\varphi(a)\cdot\varphi(b)\big). \end{aligned}$$

De la même manière, on peut définir une topologie sur A à partir de celle de $\mathbb{Z}_p$.
On aimerait voir comment on peut injecter $\mathbb{Z}$ dans l'anneau A. Pour $z \in \mathbb{Z}$, on sait que l'on peut voir z dans $\mathbb{Z}_p$ en prenant la suite constante. Pour lui faire correspondre un élément $a \in A$, on trouve, avec le même raisonnement que ci-dessus que $a_n p^n = z_{n+1} - z_n$. Ainsi, si $N \in \mathbb{N}$ est tel que $p^N > z$, on aura que $a_n = 0$, pour tout $n > N$. Tout élément de $\mathbb{Z}$ vu dans A est donc tel que seul un nombre fini de ses composantes dans A seront non-nulles. Réciproquement, soit $a = \sum_{i=0}^{n} a_i p^i \in A$. On peut alors lui associer l'élément de $\mathbb{Z}$ inférieur à p^n qui est $\sum_{i=0}^{n-1} a_i p^i$. Ainsi, $\mathbb{Z}$ peut être indentifié au sous ensemble de A qui possède au plus un nombre fini de composantes non-nulles. □

Proposition 1.2.17 (Caractérisation des éléments inversibles de $\mathbb{Z}_p$)
Soit $b \in \mathbb{Z}_p$ un élément inversible et a sa représentation en série entière. Alors b est inversible si et seulement si $a_0 \neq 0$.

Démonstration. Soit $b \in \mathbb{Z}_p$ et a sa représentation en série entière. Ainsi, il existe $b' \in \mathbb{Z}_p$ tels que $bb' = 1$. En particulier, $b_1 b'_1 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$ et donc $a_0 \neq 0$.
Réciproquement, supposons que la représentation en série entière a de $b \in \mathbb{Z}_p$ soit telle que $a_0 \neq 0$. Alors, b_1 possède un inverse dans $\mathbb{Z}/p\mathbb{Z}$. Supposons que b_n soit inversible dans $\mathbb{Z}/p^n\mathbb{Z}$, c'est-à-dire qu'il existe b'_n tel que $b_n b'_n = 1$. Puisque $b_n \equiv b_{n+1} \pmod{p^n}$, on trouve que b_{n+1} possède un inverse dans $\mathbb{Z}/p^{n+1}\mathbb{Z}$. □

Proposition 1.2.18
On a

$$\hat{\mathbb{Z}} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p.$$

Démonstration. Utilise la caractérisation du complété donnée dans le lemme 1.2.15. □

1.2.3 Propriétés de base des pro-$\mathcal{C}$ groupes

Proposition 1.2.19
Soit $\mathcal{C}$ une formation de groupes finis.

(*i*) *Soit G un pro-$\mathcal{C}$ groupe et $N \trianglelefteq_c G$. Alors, G/N est un pro-$\mathcal{C}$ groupe. Si, de plus, $\mathcal{C}$ est fermée pour les sous-groupes, alors tout sous-groupe fermé d'un pro-$\mathcal{C}$ groupe est un pro-$\mathcal{C}$ groupe.*

(*ii*) *Le produit direct de toute collection de pro-$\mathcal{C}$ groupe est un pro-$\mathcal{C}$ groupe.*

(*iii*) *La limite d'un système projectif surjectif de pro-$\mathcal{C}$ groupes est un pro-$\mathcal{C}$ groupe.*

Démonstration. (i) Le fait que N soit fermé dans G entraine que $\bar{G} = G/N$ est de Hausdorff. Puisque G est compact et totalement discontinu, $\bar{G}$ l'est aussi. De plus, pour tout sous-groupe normal ouvert $\bar{H}$ de G/N, on a $\bar{G}/\bar{H} \in \mathcal{C}$ (par le troisième théorème d'isomorphisme), ce qui implique que G/N est pro-$\mathcal{C}$ (caractérisation (*ii*) du théorème 1.2.7).
Si H est un sous-groupe fermé de G, alors on a $H = \varprojlim \varphi_i(H)$, par la proposition 1.1.34.

(ii) Le fait que le produit d'une famille de pro-$\mathcal{C}$ groupes soit compact, de Hausdorff et totalement discontinu est clair. Si $G = \prod_{i\in I} G_i$, où chaque G_i est un pro-$\mathcal{C}$ groupe, il reste à voir que $G/_N \in \mathcal{C}$ pour tout $N \trianglelefteq_o G$. Puisque N est un ouvert de G, il contient un ouvert de base U, c'est-à-dire qu'il existe $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$ et U_{i_j} un ouvert de G_{i_j} pour chaque j tel qu'en posant $W_i = G_i$ si $i \neq i_1, \ldots, i_n$ et $W_{i_j} = U_j$ on ait :

$$U = \prod_{i\in I} W_i \subset N.$$

En utilisant un argument semblable à la preuve du théorème 1.2.7, on peut constuire, pour $j = 1, \ldots, n$, un sous-groupe normal $N_{i_j} \subset W_{i_j}$ de G_{i_j}. Pour les autres indices, on prend $N_i = G_i$. On a donc :

$$G/_{\prod_{i\in I} N_i} \cong \prod_{i\in I} G_i/_{N_i} \cong \prod_{j=1}^{n} G_{i_j}/_{N_{i_j}}.$$

Puisque $\mathcal{C}$ est une formation et que $G_{i_j}/_{N_{i_j}} \in \mathcal{C}$ pour tout j, le dernier produit appartient à $\mathcal{C}$. En effet, en posant, pour $k = 1, \ldots, n$:

$$\pi_k : \prod_{j=1}^{n} G_{i_j}/_{N_{i_j}} \longrightarrow G_{i_k}/_{N_{i_k}}$$

comme étant la projection canonique. Les sous-groupes normaux $\ker \pi_k$ sont ceux demandés par la définition de produit sous-direct. Le troisième théorème d'isomorphisme permet de conclure.

(iii) Provient des deux points précédents et de la caractérisation (*iii*) de 1.2.7 (les voisinages choisis sont les noyaux des projections).

□

1.3 Groupes profinis

1.3.1 Ordre des groupes profinis

Un groupe profini étant construit à partir d'une collection de groupes finis, on aimerait pouvoir transposer certains concepts tels les p-sous-groupes, les p-sylows, etc. Le problème est que la notion de l'ordre usuel d'un groupe fini n'est pas très utile dans le cas des groupes profinis. En effet, dans le cas d'un groupe profini infini (qui n'est alors pas dénombrable, comme le montre [RZ00]) son cardinal n'apporte que peu d'informations. On retrouve certaines des propriétés voulues en généralisant la notion de nombre naturel comme suit.

Définition 1.3.1 (Nombre surnaturel)
Un nombre surnaturel *est un produit formel*

$$n = \prod_{p \in \mathbb{P}} p^{n(p)},$$

où $n : \mathbb{P} \longrightarrow \mathbb{N}_0 \cup \{\infty\}$.

Remarque 1.3.2
Soit $n \in \mathbb{N}_0$. On adopte les conventions suivantes :

$$n < \infty, \quad n + \infty = \infty + n = \infty + \infty = \infty.$$

Soit

$$\Big\{ n_i = \prod_{p \in \mathbb{P}} p^{n_i(n)} : i \in I \Big\}$$

une collection de nombres surnaturel. On peut alors généraliser les notions de divisibilité, produit, pgdc, ppmc de la manière suivante :

(i) On dit que n_i divise n_j si $n_i(p) \leq n_j(p)$ pour tout premier p.

(ii) Le produit des n_i est

$$\prod_{i \in I} n_i = \prod_{p \in \mathbb{P}} p^{n(p)},$$

où $n(p) = \sum_{i \in I} n_i(p)$.

(iii) Le pgdc (respectivement le ppmc) des n_i est défini de la manière suivante :

$$\prod_{p \in \mathbb{P}} p^{n(p)},$$

où $n(p) = \min_{i \in I}\{n_i(p)\}$ (respectivement $n(p) = \sup_{i \in I}\{n_i(p)\}$).

Définition 1.3.3 (Indice d'un sous-groupe)
*Soit G un groupe profini, $H \leq_c G$ et $\mathcal{N}$ l'ensemble des sous-groupes normaux ouverts de G. On définit l'*indice *de H dans G par*

$$|G : H| = \text{ppmc}\Big\{ \big|G/_N : HN/_N\big| : N \in \mathcal{N} \Big\}.$$

Remarquons que le fait que G soit compact et $N \in \mathcal{N}$ ouvert implique que $|G : N|$ est fini.
On définit alors l'ordre de G par $|G : \{1\}|$.

Remarque 1.3.4
Dans le cas d'un groupe fini, cette définition de l'indice d'un sous-groupe coïncide avec la définition habituelle. En effet, le troisième théorème d'isomorphisme nous donne

$$|G : H| = \text{ppmc}\Big\{\big|G : HN\big| : N \in \mathcal{N}\Big\},$$

qui atteint son maximum lorsque $N = H$. Comme $|G : HN|_c$ (le c sert à désigner l'indice « classique » pour éviter les confusions) divise $|G : H|_c$ pour tout N, le ppmc est ainsi $|G : H|_c$.

Exemple 1.3.5
Intuitivement, on a l'impression que l'ordre de $\mathbb{Z}_p$ est p^∞. On verra plus bas que c'est le cas. De même, puisque $\hat{\mathbb{Z}} = \prod_{p\in\mathbb{P}} \mathbb{Z}_p$, on a $|\hat{\mathbb{Z}}| = \prod_{p\in\mathbb{P}} p^\infty$.

Proposition 1.3.6
Soit G un groupe profini.

(*i*) *Soit $H \leq_c G$ et $\mathcal{V}$ un système fondamental de voisinages de l'unité constitué de sous-groupes normaux ouverts. Alors*

$$|G : H| = \text{ppmc}\Big\{\big|G/_N : HN/_N\big| : N \in \mathcal{V}\Big\}.$$

(*ii*) *Si $H \leq_c G$, alors*

$$|G : H| = \text{ppmc}\big\{|G : U| : H \leq U \leq_o G\big\}.$$

(*iii*) *Supposons que $I \leq_c J \leq_c G$, alors*

$$|G : I| = |G : J||J : I|.$$

(*iv*) *Soit (G_i, φ_{ij}) un système projectif surjectif de groupes profinis. Alors*

$$\big|\varprojlim G_i\big| = \text{ppmc}\{|G_i| : i \in I\}.$$

(*v*) *Pour toute collection $\{G_i\}_{i\in I}$ de groupes profinis,*

$$\Big|\prod_{i\in I} G_i\Big| = \prod_{i\in I} |G_i|.$$

Démonstration. Voir [RZ00]. □

Remarque 1.3.7
La propriété (*ii*) de la proposition ci-dessus permet de montrer que si $N \trianglelefteq_c G$, alors $|G/_N| = |G : N|$.

Il est possible de généraliser la notion de p-groupe pour un ensemble quelconque de premiers. Pour cela, il est nécessaire de définir les π-nombres.

Définition 1.3.8 (π-nombre, pro-π groupe)
Soit n un nombre surnaturel et $\pi \subset \mathbb{P}$. On dit que n est un π-nombre *si chaque fois que $n(p) \neq 0$, alors $p \in \pi$. Un groupe profini G est un* pro-π groupe *si son ordre est un π-nombre (si $\pi = \{p\}$, on parle plutôt de pro-p groupe).*

Remarques 1.3.9 (i) Le point (*iv*) de la proposition ci-dessus entraîne qu'un groupe profini $G = \varprojlim G_i$ est un π-groupe si les premiers divisant l'ordre des G_i sont uniquement ceux de π. On voit déjà que les notions qui viennent d'être définies apportent des résultats intéressants : certaines propriétés de l'ordre d'un groupe profini sont liées à celles des éléments de la limite (et inversément).

(ii) Si $\pi = \{p\}$, on a que que $G = \varprojlim G_i$ est un pro-p groupe si le seul premier divisant l'ordre des G_i est p. Ainsi, un pro-p groupe est une limite de p-groupes.

1.3.2 π-sous-groupes de Hall

Définition 1.3.10 (π-sous-groupe de Hall)
Soit $\pi \subset \mathbb{P}$ et $\pi' = \mathbb{P} \setminus \pi$. Un sous-groupe fermé H d'un groupe profini G est appelé un π-sous-groupe de Hall *si H est un pro-π groupe et si $|G : H|$ est un π'-nombre.*

Remarque 1.3.11
En choisissant $\pi = \{p\}$ dans la définition ci-dessus, on voit que la notion de p-sous-groupe de Hall prolonge celle de p-Sylow.

Proposition 1.3.12
Soit $\pi \subset \mathbb{P}$, $\varphi : G \longrightarrow K$ un morphisme de groupes profinis et $H \leq_c G$. Alors :

(*i*) *Si H est un π-groupe, $\varphi(H)$ en est un aussi.*

(*ii*) *Si H est un π-sous-groupe de Hall de G, alors $\varphi(H)$ est un π-sous-groupe de Hall de $\varphi(G)$.*

Démonstration. Supposons que K soit la limite du système (K_i, ψ_{ij}).

(i) Soit p divisant l'ordre de $\varphi(H)$. Il faut montrer que $p \in \pi$.
Puisque G, K sont compacts et que H est fermé dans G, on a par la proposition 1.1.34
$$\varphi(H) = \varprojlim \psi_i \varphi(H).$$
Ainsi, il existe $j \in I$ tel que p divise l'ordre de $\psi_j \varphi(H)$, ce qui implique que p divise $|H|$ (ici, p est identifié au nombre surnaturel n pour lequel seul $n(p) \neq 0$ et $n(p) = 1$), et donc que $p \in \pi$.

(ii) Arguments similaires.

□

Proposition 1.3.13
Soit $\pi \subset \mathbb{P}$, $G = \varprojlim G_i$, où (G_i, φ_{ij}) est un système projectif surjectif de groupes finis, et $H \leq_c G$. Alors H est π-sous-groupe de Hall de G si et seulement si $\varphi_i(H)$ est un π-sous-groupe de Hall de G_i pour tout $i \in I$.

Démonstration. Le sens direct provient de la proposition précédente.
Pour le sens réciproque, puisque le système projectif est surjectif, il est clair que si chaque $\varphi_i(H)$ est un π-groupe, H le sera aussi. Il reste à montrer que si chaque $|G_i : \varphi_i(H)|$ est un π'-nombre, $|G : H|$ l'est aussi. La proposition 1.2.13 combiné avec le point (i) de la proposition 1.3.6 impliquent que

$$|G : H| = \text{ppmc}\left\{ \left| G/_{\ker \varphi_i} : (H \ker \varphi_i)/_{\ker \varphi_i} \right| : i \in I \right\}.$$

Puisque chaque morphisme φ_i est surjectif (proposition 1.1.36), on obtient par le premier et le deuxième théorème d'isomorphisme :

$$|G : H| = \text{ppmc}\left\{ \left| G_i : \varphi_i(H) \right| : i \in I \right\},$$

ce qui conclut la preuve. □

Un exemple de l'utilisation de cette proposition est donné dans la section 1.3.3.

Remarque 1.3.14
La condition de surjectivité dans la proposition précédente est importante. En effet, si l'on prend $G_2 = S_3$, $G_1 = S_4$ et $\varphi_{12} : S_3 \hookrightarrow S_4$, alors $G = \varprojlim G_i = S_3$. Or, l'image par φ_1 d'un 2-Sylow de S_3 n'est pas un 2-Sylow de S_4.

Théorème 1.3.15
Soit (G_i, φ_{ij}) un système projectif surjectif de groupes finis, G sa limite projective et $\pi \subset \mathbb{P}$.

(*i*) *Si chaque G_i contient un π-sous-groupe de Hall, G contient un π-sous-groupe de Hall.*

(*ii*) *Si, pour tout i, chaque π-sous-groupe de G_i est contenu dans un π-sous-groupe de Hall, alors chaque π-sous-groupe fermé de G est contenu dans un π-sous-groupe de Hall.*

(*iii*) *Si, pour tout i, chaque paire de π-sous-groupes de Hall de G_i sont conjugués, alors chaque paire de π-sous-groupes de Hall de G sont conjugués.*

Démonstration. (i) L'idée est de construire une « sous limite » constituée d'ensembles de π-sous-groupes de Hall. Pour cela, soit $\mathcal{G}_i$ l'ensemble des π-sous-groupes de Hall de G_i. Pour voir que les $\mathcal{G}_i$ forment bien un système projectif, il faut s'assurer que $\varphi_{ij}\big|_{\mathcal{G}_j} \subset \mathcal{G}_i$, ce qui est le cas, puisque chaque φ_{ij} est surjectif. Considérons $\mathcal{G} = \varprojlim \mathcal{G}_i$, qui n'est pas vide, par la proposition 1.1.35 (chaque ensemble fini $\mathcal{G}_i$ est muni de la topologie discrète). Soit $\tilde{H} \in \mathcal{G}$, c'est-à-dire que $\tilde{H}_i$ est un π-sous-groupe de Hall de G_i pour chaque i et posons $H = \varprojlim \tilde{H}_i$. La proposition précédente implique que H est un π-sous-groupe de Hall de G.

(ii) Soit H un π-sous-groupe fermé de G. L'idée est de considérer pour chaque i

$$\mathcal{G}_i = \big\{\varphi_i(H) \leq H_i \leq G_i : H_i \text{ est un } \pi\text{-sous-groupe de Hall}\big\},$$

qui n'est pas vide par hypothèse. La suite est semblable au point précédent.

(iii) Soient $H, \tilde{H}$ deux π-sous-groupes de Hall de G. On considère

$$\mathcal{G}_i = \big\{g \in G_i : g\varphi_i(H)g^{-1} = \varphi_i(\tilde{H})\big\},$$

qui n'est pas vide par hypothèse. La suite est semblable au point (*i*).

□

Théorème 1.3.16 (Théorème de Sylow pour les groupes profinis)
Soit (G_i, φ_{ij}) un système projectif surjectif de groupes finis, G sa limite projective et $p \in \mathbb{P}$. Alors :

(*i*) *G contient un p-Sylow.*

(*ii*) *Chaque p-sous-groupe fermé de G est contenu dans un p-Sylow.*

(*iii*) *Chaque paire de p-Sylows de G sont conjugués.*

Démonstration. Provient du théorème précédent et des théorèmes de Sylow classiques (voir par exemple [Lan02]). □

Exemple 1.3.17
On trouve directement que $|\mathbb{Z}_p| = p^\infty$. De même, puisque l'on peut injecter $\mathbb{Z}_p$ dans $\hat{\mathbb{Z}}$, on trouve en utilisant la caractérisation de $\hat{\mathbb{Z}}$ vue dans la proposition 1.2.18 que $\mathbb{Z}_p$ est un p-Sylow de $\hat{\mathbb{Z}}$.

Remarque 1.3.18
Bien que très pratique, cette manière d'étendre la notion d'ordre à des groupes infinis possède quelques limitations et certains résultats qui sont vrais dans le cas fini ne le restent pas forcément.

Premièrement, le fait de ne rajouter qu'un seul infini ne permet pas forcément suffisament de précisions. Par exemple, l'ordre de $\hat{\mathbb{Z}}$ est $\prod_{p\in\mathbb{P}} p^\infty$, l'ordre « maximal », alors que l'on peut construire des groupes profinis « plus grands » (dans le sens où l'ensemble filtrant sur lequel on travaille pour $\hat{\mathbb{Z}}$ n'est que de cardinalité $\aleph_0$).
Deuxièmement, un groupe profini dont l'ordre est divisible par un premier p ne possède pas forcément d'élément d'ordre p. En effet, si $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ possède un élément d'ordre p, il n'est pas dans $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

1.3.3 Le groupe général linéaire des p-adiques

On a vu plus haut (exemple 1.2.12) sans donner d'exemple concret que si R est un anneau profini, alors $\mathrm{GL}_n(R)$ est un groupe profini. Le but de cette section est de discuter du cas de $\mathrm{GL}_n(\mathbb{Z}_p)$. On rappelle que $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ et que l'homomorphisme d'anneaux $\varphi_i : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^i\mathbb{Z}$ désigne la projection naturelle.
On aimerait montrer que

$$\mathrm{GL}_n(\mathbb{Z}_p) = \varprojlim_{i\in\mathbb{N}} \mathrm{GL}_n\left(\mathbb{Z}/p^i\mathbb{Z}\right).$$

On fixe $k \in \mathbb{N}$ (pour toute cette section) et on considère :

$$\begin{array}{rcl} \phi_k : \mathrm{GL}_n(\mathbb{Z}_p) & \longrightarrow & \mathrm{M}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right) \\ (M_{ij}) & \longmapsto & \left(\varphi_k(M_{ij})\right), \end{array}$$

ainsi que $K_k = I_n + \mathrm{M}_n(p^k\mathbb{Z})$. On aimerait montrer qu'il existe une suite exacte

$$I_n \longrightarrow K_k \xrightarrow{\psi} \mathrm{GL}_n(\mathbb{Z}_p) \xrightarrow{\phi_k} \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right) \longrightarrow I_n.$$

Pour commencer, montrons que $\operatorname{im}\phi_k \subset \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)$. On va pour cela utiliser la proposition suivante :

Proposition 1.3.19
Soit $b \in \mathbb{Z}_p$ et $k \in \mathbb{N}$. Alors b est inversible si et seulement si $\varphi_k(b) \in \mathbb{Z}/p^k\mathbb{Z}$ est inversible.

Démonstration. Le sens direct est clair.
Supposons que $\varphi_k(b)$ soit inversible, ce qui implique que p ne divise pas b_k. On montre alors par récurrence que p ne peut diviser b_j pour tout $j \leq k$, ce qui implique que b_1 est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Si a est la représentation de b en série entière, on a $a_0 = b_1$, et donc $a_0 \neq 0$, ce qui implique que b est inversible (proposition 1.2.17). □

Remarque 1.3.20
On rappelle que si A est un anneau et $M \in \mathrm{M}_n(A)$, alors

$$M \in \mathrm{GL}_n(A) \Leftrightarrow \det M \in A^*.$$

Puisque φ_k est un homomorphisme d'anneau, que ϕ_k est définie composante par composante et que le déterminant d'une matrice se calcule via une somme de produits, on a, pour $M \in \mathrm{GL}_n(\mathbb{Z}_p)$:

$$\det \phi_k M = \varphi_k \det M,$$

ce qui implique que $\operatorname{im}\phi_k \subset \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)$. Le fait que ϕ_k soit un homomorphisme de groupes est clair.
On aimerait montrer que ϕ_k est une application surjective. Soit $B \in \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)$. Pour tout couple $1 \leq i, j \leq n$, posons $A_{ij} \in \mathbb{Z}_p$ comme étant la suite constante avec $(A_{ij})_l = B_{ij}$, pour tout $l \in \mathbb{N}$. Si A est la matrice dont les coefficients sont A_{ij}, on a $\phi_k(A) = B$ et

$$\det A \in {\mathbb{Z}_p}^* \Leftrightarrow \varphi_k \det A \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^* \Leftrightarrow \det \phi_k A = \det B \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*.$$

Ainsi, $A \in \mathrm{GL}_n(\mathbb{Z}_p)$.
L'application $\psi : K_k \longrightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ est définie componsante par componsante via l'injection habituelle de $\mathbb{Z}$ dans $\mathbb{Z}_p$. Il faut encore voir que si $A \in K_k$, alors $\psi(A)$ est bien une matrice inversible. Comme ψ « commute avec le déterminant » et qu'un élément de $\mathbb{Z}_p$ est inversible si et seulement si sa première composante est non-nulle, cela revient à montrer que le déterminant de A est non nul modulo p. On calcule :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} A_{i\sigma(i)} \equiv \prod_{i=1}^{n} A_{ii} = \prod_{i=1}^{n} (1 + \alpha_i p^k) \equiv 1 \pmod{p}.$$

L'exactitude de la suite exacte en $\mathrm{GL}_n(\mathbb{Z}_p)$ ne pose pas de problème. On a donc

$$\mathrm{GL}_n(\mathbb{Z}_p)/\psi(K_k) \cong \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right),$$

en tant que groupes topologiques (voir remarque 1.1.17).
En tant que noyaux de l'application ϕ_k, les $\psi(K_k)$ sont des voisinages fermés (proposition 1.1.6) de l'unité et sont ouverts (puisque la cardinalité de $\mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)$ est finie). On remarque de plus que $\bigcap_{k\in\mathbb{N}} \psi(K_k) = \{I_n\}$ et la proposition 1.1.33 nous permet d'affirmer que les $\psi(K_k)$ forment un système fondamental de voisinages ouverts de l'unité dans $\mathrm{GL}_n(\mathbb{Z}_p)$. On a alors, par le théorème 1.2.7

$$\mathrm{GL}_n(\mathbb{Z}_p) \cong \varprojlim_{k\in K} \mathrm{GL}_n(\mathbb{Z}_p)/\psi(K_k) \cong \varprojlim_{k\in\mathbb{N}} \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right).$$

Un p-Sylow de $\mathrm{GL}_n(\mathbb{Z}_p)$

On sait que la cardinalité de $\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right)$ est

$$(p^n - 1) \cdot (p^n - p) \cdot \ldots \cdot \left(p^n - p^{n-1}\right).$$

Si on pose

$$K_k = I_n + \mathrm{M}_n\left(p\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right),$$

on peut montrer qu'il existe une suite exacte

$$I_n \longrightarrow K_k \longrightarrow \mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right) \longrightarrow \mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right) \longrightarrow I_n.$$

L'application du premier théorème d'isomorphisme implique alors

$$\begin{aligned}\left|\mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right| &= p^{(k-1)n^2}\prod_{i=0}^{n-1}\left(p^n-p^i\right)\\ &= p^{(k-1)n^2}\prod_{i=0}^{n-1}p^i\left(p^{n-i}-1\right)\\ &= p^{(k-1)n^2+\frac{n(n-1)}{2}}\prod_{i=1}^{n}\left(p^i-1\right).\end{aligned}$$

Ainsi, pour tout $k\in\mathbb{N}$, $\mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)$ possède un p-Sylow d'indice $\prod_{i=1}^{n}\left(p^i-1\right)$. Le fait que $\mathrm{GL}_n(\mathbb{Z}_p)$ s'écrive comme une limite de $\mathrm{GL}_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)$ implique qu'il possède un p-Sylow H. On aura alors $H=\varprojlim_{k\in\mathbb{N}}\phi_k(H)$ et donc H est d'indice $\prod_{i=0}^{n-1}\left(p^i-1\right)$ dans $\mathrm{GL}_n(\mathbb{Z}_p)$ (voir démonstration de la proposition 1.3.13).

Le cas de SL_n

On a vu ci-dessus que $\mathrm{GL}_n(\mathbb{Z}_p)$ se « comporte bien » par rapport à $\mathbb{Z}_p$. On aimerait montrer maintenant le lien entre $\mathrm{SL}_n(\hat{\mathbb{Z}})$ et les $\mathrm{SL}_n(\mathbb{Z}_p)$. Si l'on prend l'isomorphisme $\varphi:\hat{\mathbb{Z}}\longrightarrow\prod_{p\in\mathbb{P}}\mathbb{Z}_p$, on peut l'utiliser afin de définir un isomorphisme ϕ de la manière suivante :

$$\begin{aligned}\phi:\mathrm{SL}_n(\hat{\mathbb{Z}}) &\longrightarrow \prod_{p\in\mathbb{P}}\mathrm{SL}_n(\mathbb{Z}_p)\\ A &\longmapsto \phi(A),\quad \text{où } \left(\phi(A)_p\right)_{ij}=\varphi(A_{ij})_p.\end{aligned}$$

Montrer que cette application est bien définie et est un isomorphisme se fait avec quelques jeux d'écriture, comme ci-dessus avec GL_n.

1.3.4 Groupes procycliques

Le but de cette section est de transposer certains résultats s'appliquant aux groupes cycliques finis. Notamment l'unicité de groupes profinis cycliques et l'existence de leurs sous-groupes.

Définition 1.3.21 (Ensemble générateur)
Soit G un groupe profini et X un sous-ensemble de G. On dit que X engendre *(ou engendre topologiquement) G si $\langle X\rangle$ est dense dans G, c'est-à-dire $G=\overline{\langle X\rangle}$*

Proposition 1.3.22
Soient X,Y deux espaces topologiques et $f:X\longrightarrow Y$ une application continue. Alors, pour tout $A\subset X$, on a

$$f\left(\overline{A}\right)\subset\overline{f(A)}.$$

Démonstration. Puisque f est continue, $f^{-1}\left(\overline{f(A)}\right)$ est un fermé de X qui contient A, on a donc

$$\overline{A}\subset f^{-1}\left(\overline{f(A)}\right),$$

ce qui implique

$$f(\overline{A})\subset f\left(f^{-1}\left(\overline{f(A)}\right)\right)\subset\overline{f(A)}.$$

□

Proposition 1.3.23
Soit X un espace topologique, $A \subset X$ et $f : X^n \longrightarrow X$ une application continue. Si $f(A \times \ldots \times A) \subset A$, alors $f\big(\bar{A} \times \ldots \times \bar{A}\big) \subset \bar{A}$.

Démonstration. On calcule :

$$\begin{array}{rcl} f(\bar{A} \times \ldots \times \bar{A}) & = & f\big(\overline{A \times \ldots \times A}\big) \\ & \overset{1.3.22}{\subset} & \overline{f(A \times \ldots \times A)} \subset \bar{A}. \end{array}$$

□

Corollaire 1.3.24
Soit G un groupe topologique, $H \leq G$ et $N \trianglelefteq G$. Alors $\bar{H} \leq G$ et $\bar{N} \trianglelefteq G$.

Démonstration. Découle de la proposition et du fait que la multiplication à gauche (et à droite) par un élément de G est une opération continue. □

Définition 1.3.25 (Groupe procyclique)
Un groupe profini G est dit procyclique *s'il existe $x \in G$ tel que $G = \overline{\langle x \rangle}$.*

Proposition 1.3.26
Un groupe profini est procyclique si et seulement s'il est une limite projective d'un système de groupes cycliques.

Démonstration. Soit $G = \varprojlim G_i$, où (G_i, φ_{ij}) est un système projectif surjectif de groupes finis.
Supposons que $G = \overline{\langle x \rangle}$. Alors, $\varphi_i(x)$ engendre G_i pour tout $i \in I$ (cela provient de la proposition 1.3.22).
Réciproquement, supposons que chaque G_i soit cyclique. Pour chaque i, posons

$$\mathcal{G}_i = \{g \in G_i : \langle g \rangle = G_i\}.$$

Puisque φ_{ij} est surjectif, $\varphi_{ij}\big|_{\mathcal{G}_j} \subset \mathcal{G}_i$. Ainsi, les $\mathcal{G}_i$ forment un système projectif qui a une limite non-vide. Un élément de cette limite sera le générateur cherché. En effet, si g est un tel élément :

$$\overline{\langle g \rangle} = \varprojlim \varphi_i\big(\overline{\langle g \rangle}\big) \supset \varprojlim \varphi_i(\langle g \rangle) = \varprojlim \langle \varphi_i(g) \rangle = \varprojlim G_i = G.$$

□

Remarque 1.3.27
En particulier, un groupe procyclique est abélien (comme limite projective de groupes abéliens).

Proposition 1.3.28
Soit $p \in \mathbb{P}$ et p^n un nombre surnaturel.

(*i*) *Il existe un unique groupe procyclique C d'ordre p^n à isomorphisme près. Si $n < \infty$, $C \cong \mathbb{Z}/p^n\mathbb{Z}$ sinon, on a $C \cong \mathbb{Z}_p$.*

(*ii*) *Le groupe $\mathbb{Z}_p$ a un unique sous-groupe fermé H d'indice p^n. De plus, $H = p^n\mathbb{Z}_p \cong \mathbb{Z}_p$ si n est fini et $H = \{1\}$ sinon.*

(*iii*) *Chaque groupe procyclique d'ordre p^n s'écrit comme un quotient de $\mathbb{Z}_p$ d'une manière unique.*

Démonstration. (i) Si $n < \infty$, le résultat est clair. Supposons donc que C soit un groupe procyclique d'ordre p^∞. On aimerait montrer que

$$C \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z}.$$

Pour cela, on va utiliser la caractérisation (iv) du théorème 1.2.7. Si N est un sous-groupe (normal) ouvert de C tel que C/N est fini (ici, $\mathcal{C}$ est la classe des groupes finis), alors on a $|C : N| = p^i$ pour un certain i. Soient N_1, N_2 deux sous-groupes de C d'indice p^i. On aimerait voir que $N_1 = N_2$. Cela provient du fait que $N_1/N_1 \cap N_2$ et $N_2/N_1 \cap N_2$ sont deux sous-groupes de même indice du groupe cyclique *fini* $C/N_1 \cap N_2$, ce qui implique que $N_1 = N_2$. Pour l'existence, le fait que $|C| = p^\infty$ implique l'existence de sous-groupes ouverts d'indice arbitrairement grand. Etant donné un sous-groupe d'indice p^i, on déduit l'existence des sous-groupes d'ordre p^k, $k < i$ avec un résultat sur les groupes finis et le théorème de correspondance. Ainsi, pour chaque $i \in \mathbb{N}$, C possède un unique sous-groupe H_i ouvert d'indice p^i. On a donc :

$$C \cong \varprojlim G/H_i \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z} \cong \mathbb{Z}_p.$$

(ii) Considérons $\mathbb{Z}_p$ comme l'anneau A de séries formelles (voir proposition 1.2.16) et, pour $n \in \mathbb{N}$ non-nul, posons :

$$\begin{aligned} \varphi_n : A &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ \sum_{i=0}^{\infty} a_i p^i &\longmapsto \sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z}. \end{aligned}$$

On constate que cette application est surjective et que son noyau est $p^n A$, ainsi on a que $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, ce qui implique que $p^n\mathbb{Z}_p$ est un sous-groupe d'indice p^n de $\mathbb{Z}_p$. Puisque $p^n\mathbb{Z}_p$ est le noyau de φ_n, il est fermé (proposition 1.1.6). Le même raisonnement que ci-dessus implique qu'il est le seul sous-groupe d'indice p^n.
Soit maintenant H un sous-groupe fermé d'indice p^∞ de $\mathbb{Z}_p$. Puisque

$$|\mathbb{Z}_p : H| = p^\infty = \text{ppmc}\left\{ \left|\mathbb{Z}_p/p^i\mathbb{Z}_p : H(p^i\mathbb{Z}_p)/p^i\mathbb{Z}_p\right| : i \in \mathbb{N} \right\},$$

il existe pour tout $i \in \mathbb{N}$ un entier $j(i)$ tel que $H(p^{j(i)}\mathbb{Z}_p) \leq p^i\mathbb{Z}_p$. En effet, pour tout i, il existe un entier un sous-groupe normal ouvert N_i de $\mathbb{Z}_p$ tel que

$$p^i = \left|\mathbb{Z}_p/N_i : HN_i/N_i\right|,$$

c'est-à-dire qu'il existe k tel que

$$p^i = \left|\mathbb{Z}_p/p^k\mathbb{Z}_p : H(p^k\mathbb{Z}_p)/p^k\mathbb{Z}_p\right|.$$

En utilisant le point (iii) de la proposition 1.3.6 et la remarque 1.3.7 on trouve que $H(p^k\mathbb{Z}_p)$ est un sous-groupe d'indice p^i de $\mathbb{Z}_p$. Comme ce sous-groupe est fermé (il est l'image du compact $H \times (p^k\mathbb{Z}_p)$ par la loi du groupe), ce qui précède implique que $H(p^k\mathbb{Z}_p) = p^i\mathbb{Z}_p$, pour un certain i. On pose alors $j(i) = k$.
Ainsi,

$$H = H\{1\} = H \bigcap_{i \in N} p^i\mathbb{Z}_p \leq H \bigcap_{i \in \mathbb{N}} p^{j(i)}\mathbb{Z}_p \overset{1.1.18}{=} \bigcap_{i \in \mathbb{N}} H\left(p^{j(i)}\mathbb{Z}_p\right) \leq \bigcap_{i \in \mathbb{N}} p^i\mathbb{Z}_p = \{1\}.$$

(iii) Provient des deux points précédents.

□

Proposition 1.3.29
Soit G un groupe abélien fini. Alors G est isomorphe au produit de ses p-Sylows.

Démonstration. Soit $P = \{p_1, \ldots, p_r\} \subset \mathbb{P}$ l'ensemble des premiers divisant l'ordre de G et, pour chaque $p_i \in P$, notons N_i l'unique p_i-Sylow de G. Le théorème de Lagrange implique que $|G : N_1 \cdot \ldots \cdot N_r| = 1$ et donc que $G = N_1 \cdot \ldots \cdot N_r$. Le fait que $|N_i \cap \prod_{j \neq i} N_j| = 1$ pour tout i implique que

$$G \cong \prod_{i=1}^{r} P_i.$$

□

Cette proposition et son utilisation pour la classification des groupes procyclique provient de [Rib70].

Proposition 1.3.30
Soit G un groupe profini abélien et pour chaque $p \in \mathbb{P}$, notons G_p son unique p-Sylow (quitte à prendre G_p trivial). Alors

$$G \cong \prod_{p \in \mathbb{P}} G_p.$$

Démonstration. Soit N un sous-groupe (normal) ouvert de G et pour $p \in \mathbb{P}$ notons N_p l'unique p-Sylow de G/N. Puisque G/N est fini, la proposition précédente nous permet d'écrire

$$G/N \cong \prod_{p \in \mathbb{P}} N_p.$$

On sait de plus que $G = \varprojlim_N G/N$, où N parcourt l'ensemble des sous-groupes (normaux) ouverts de G. Les morphismes de ce système se restreignent pour former, pour chaque p, un système projectif constitué des N_p. Posons $H_p = \varprojlim_N N_p$, qui est un p-sous-groupe de G. Par le même raisonnement que celui de la preuve de la proposition 1.3.13, on trouve que H_p est un p-Sylow de G, et donc que $H_p = G_p$ par unicité. On obtient alors

$$G = \varprojlim_N G/N \cong \varprojlim_N \prod_{p \in \mathbb{P}} N_p \cong \prod_{p \in \mathbb{P}} \varprojlim_N N_p \cong \prod_{p \in \mathbb{P}} G_p.$$

Pour montrer l'avant dernier isomorphisme, on utilise la propriété universelle de la limite projective. □

Proposition 1.3.31
Soit $n = \prod_{p \in \mathbb{P}} p^{n(p)}$ un nombre surnaturel.

(*i*) *Il existe un unique groupe procyclique d'ordre n à isomorphisme près.*

(*ii*) *Le groupe $\hat{\mathbb{Z}}$ a un unique sous-groupe H fermé d'indice n. De plus,*

$$H \cong \prod_{p \in S} \mathbb{Z}_p,$$

où $S = \{p \in \mathbb{P} : n(p) < \infty\}$.

(*iii*) *Toute groupe procyclique d'ordre n s'écrit comme un quotient de $\hat{\mathbb{Z}}$ de manière unique.*

Démonstration. (i) Pour chaque $p \in \mathbb{P}$ posons G_p comme étant l'unique groupe procyclique d'ordre $p^{n(p)}$ (voir 1.3.28). Le point (v) de la proposition 1.3.6 implique que l'ordre de $G = \prod_{p\in P} G_p$ est n. Le fait que G soit procyclique provient de la proposition 1.2.19 et l'unicité de la proposition précédente.

(ii) Soit $P = \prod_{p\in S} \mathbb{Z}_p$ qui est d'indice n dans $\hat{\mathbb{Z}}$. Soit maintenant H un sous-groupe d'indice n de $\hat{\mathbb{Z}}$. La proposition précédente implique que $H = \prod_{p\in\mathbb{P}} H_p$ où H_p est l'unique p-Sylow de H. On a alors :

$$n = |\hat{\mathbb{Z}} : H| = \left|\hat{\mathbb{Z}}/_H\right| = \prod_{p\in\mathbb{P}} \left|\mathbb{Z}_p/_{H_p}\right|.$$

Ainsi, pour tout p, $\left|\mathbb{Z}_p/_{H_p}\right| = n(p)$. La proposition 1.3.28 implique que $H_p = \{1\}$ pour tous les $p \notin S$ et $H_p \cong \mathbb{Z}_p$ dans les autres cas.

(iii) Provient des deux points précédents.

□

Remarque 1.3.32
Dans (i) on n'utilise pas le fait que C soit cyclique mais seulement le fait qu'il soit abélien. En fait, ce résultat reste correct sous l'hypothèse que C soit pronilpotent (voir [Wil98]).

1.3.5 Coup d'œil catégorique

Le but de cette section est de voir quelques relations que l'on peut effectuer entre les catégories et les groupes profinis.

Définition 1.3.33 (Morphisme de systèmes projectifs)
Soit $\mathscr{C}$ une catégorie et (G_i, φ_{ij}), (G'_i, φ'_{ij}) deux systèmes projectifs d'objets de $\mathscr{C}$ sur un même ensemble filtrant I. Un morphisme de systèmes projectifs Θ *:*

$$\Theta : (G_i, \varphi_{ij}) \longrightarrow (G'_i, \varphi'_{ij})$$

est la donnée pour chaque $i \in I$ d'un morphisme $\theta_i : G_i \longrightarrow G'_i$ tel que pour tous $i \leq j$ le diagramme suivant commute :

$$\begin{array}{ccc} G_i & \xleftarrow{\varphi_{ij}} & G_j \\ {\scriptstyle\theta_i}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\theta_j} \\ G'_i & \xleftarrow[\varphi'_{ij}]{} & G'_j \end{array}$$

On peut composer de manière naturelle deux morphismes de systèmes projectifs $\Theta : (G_i, \varphi_{ij}) \longrightarrow (G'_i, \varphi'_{ij})$ et $\Psi : (G'_i, \varphi'_{ij}) \longrightarrow (G''_i, \varphi''_{ij})$ afin de donner le morphisme $\Psi\Theta : (G_i, \varphi_{ij}) \longrightarrow (G''_i, \varphi''_{ij})$ dont les composantes sont :

$$(\Psi\Theta)_i = \psi_i\theta_i.$$

On définit ainsi la catégorie des systèmes projectifs d'objets de $\mathscr{C}$, que l'on note $\mathbf{Proj}_{\mathscr{C}}$.

Dans ce qui suit, on suppose que $\mathscr{C}$ est une catégorie dans laquelle le produit de toute famille d'objets ainsi que l'égaliseur de toute paire de morphismes existe, ce qui implique l'existence des limites projectives (proposition 1.1.24).

Soit $\Theta : (G_i, \varphi_{ij}) \longrightarrow (G'_i, \varphi'_{ij})$ un morphisme d'objets de $\mathbf{Proj}_{\mathscr{C}}$, $G = \varprojlim G_i$ et $G' = \varprojlim G'_i$. Pour tout $l \in I$, on peut définir un morphisme de $\varprojlim G_i$ dans G'_l en faisant $\theta_l \varphi_l$. Ces morphismes induisent un autre morphisme, noté $\varprojlim \theta_i$ ou $\varprojlim \Theta$, de G dans G'. Pour voir cela, considérons le diagramme commutatif suivant, pour $k \leq l$:

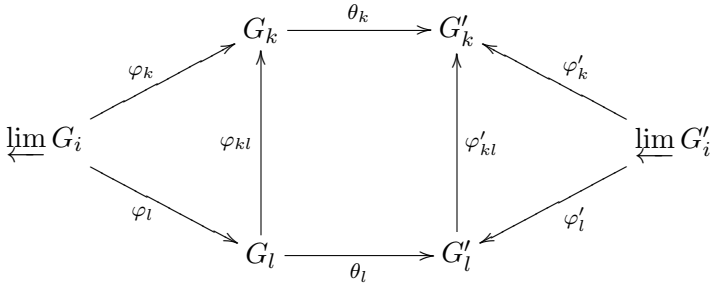


Diagramme 1.5: Extension d'un morphisme de systèmes projectifs à leurs limites

Ainsi, les morphismes $\theta_i \varphi_i$ sont compatibles pour le système (G'_i, φ'_{ij}). La propriété universelle de la limite nous assure donc l'existence d'un unique morphisme $\varprojlim \Theta : G \longrightarrow G'$, comme désiré.

On remarque que si $\Theta' : (G_i, \varphi_{ij}) \longrightarrow (G_i, \varphi_{ij})$ est l'identité, alors $\varprojlim \theta'_i = \mathrm{id}_{\varprojlim G_i}$. De plus, sous les mêmes notations que ci-dessus, on a que $\varprojlim(\Psi\Theta) = \varprojlim \Psi \circ \varprojlim \Theta$, ce qui implique que $\varprojlim$ est un foncteur de $\mathbf{Proj}_{\mathscr{C}}$ dans $\mathscr{C}$.

Proposition 1.3.34
Soit $\Theta : (G_i, \varphi_{ij}) \longrightarrow (H_i, \psi_{ij})$ un morphisme de systèmes projectifs de groupes topologiques tel que pour chaque $i \in I$, $\theta_i : G_i \longrightarrow H_i$ est injectif. Alors $\varprojlim \Theta$ est injectif.

Démonstration. Supposons que $g \in \varprojlim G_i$ soit tel que $\varprojlim \Theta(g) = 1$, ce qui implique que $\theta_j \varphi_j(g) = 1$, pour tout $j \in I$. Puisque chaque θ_j est injectif, on trouve que $g_j = 1$ pour tout j, et donc que $\ker \varprojlim \Theta = \{1\}$. □

Proposition 1.3.35
Soit $\Theta : (X_i, \varphi_{ij}) \longrightarrow (Y_i, \psi_{ij})$ un morphisme de systèmes projectifs d'espaces topologiques compacts et de Hausdorff tel que pour chaque $i \in I$, $\theta_i : X_i \longrightarrow Y_i$ est surjectif. Alors $\varprojlim \Theta$ est surjectif.

Démonstration. Soit $y \in \varprojlim Y_i$ et posons, pour chaque $i \in I$, $A_i = {\theta_i}^{-1}(\{y_i\})$. Puisque chaque Y_i est de Hausdorff et que chaque X_i est compact, $A_i \subset G_i$ est compact.
Pour que les A_i forment un système projectif, il faut voir que $\mathrm{im}\, \varphi_{ij}\big|_{A_j} \subset A_i$. Pour cela, soit $g \in A_j$. On a

$$\theta_i \varphi_{ij}(g) = \psi_{ij} \theta_j(g) = \psi_{ij} y_j = y_i,$$

comme désiré.
Puisque les A_i sont compacts et de Hausdorff, la proposition 1.1.35 implique qu'il existe $x \in \varprojlim A_i$ et $\varprojlim \Theta(x) = y$. □

Proposition 1.3.36
Le foncteur $\varprojlim$ *de la catégorie des systèmes projectifs des groupes profinis dans la catégorie des groupes profinis est exact.*

Démonstration. Soient (G_i, φ_{ij}), (H_i, λ_{ij}) et (K_i, η_{ij}) des systèmes projectifs de groupes finis sur le même ensemble filtrant I ainsi que G, H et K leur limite respective. Supposons que pour chaque $i \in I$ la suite suivante soit exacte :

$$1 \longrightarrow G_i \xrightarrow{\theta_i} H_i \xrightarrow{\psi_i} K_i \longrightarrow 1$$

(les θ_i et les ψ_i sont les composantes de deux morphismes de systèmes projectifs Θ et Ψ). Il faut voir que la suite induite suivante est exacte :

$$1 \longrightarrow G \xrightarrow{\varprojlim \Theta} H \xrightarrow{\varprojlim \Psi} K \longrightarrow 1.$$

Le fait que $\varprojlim \Theta$ soit injectif et $\varprojlim \Psi$ soit surjectif provient des deux propositions précédentes. Il reste donc à voir que $\ker \varprojlim \Psi = \operatorname{im} \varprojlim \Theta$.
Soit $h \in \ker \varprojlim \Psi$. On a donc, pour tout $i \in I$, $\psi_i(h_i) = \psi_i\lambda_i(h) = 1$. Par hypothèse. il existe un unique $g_i \in G_i$ tel que $h_i = \theta_i(g_i)$. Il reste à voir que $g \in \varprojlim G_i$. Calculons, pour $i \leq j$:

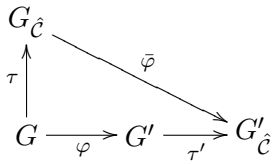
$$\theta_i\varphi_{ij}(g_j) = \lambda_{ij}\theta_j(g_j) = \lambda_{ij}(h_j) = \theta_i(g_i).$$

Comme θ_i est injectif, on a $g_i = \varphi_{ij}(g_j)$. Ainsi, $h \in \operatorname{im} \varprojlim \Theta$.
Réciproquement, soit $h \in \operatorname{im} \varprojlim \Theta$ et $g \in G$ tel que $\varprojlim \Theta(g) = h$. On a donc $h_i \in \ker \psi_i$ pour tout i, et donc $h \in \ker \varprojlim \Psi$. □

Propriétés de la complétion

Proposition 1.3.37
Soit $\mathcal{C}$ *une formation non-vide de groupes finis. L'application* F *qui à chaque groupe topologique associe sa pro-*$\mathcal{C}$ *complétion, c'est-à-dire* $F(G) = G_{\hat{\mathcal{C}}}$ *est un foncteur de la catégorie des groupes profinis.*

Démonstration. (i) Soient G, G' deux groupes topologiques, $(G_{\hat{\mathcal{C}}}, \tau)$, $(G'_{\hat{\mathcal{C}}}, \tau')$ leurs pro-$\mathcal{C}$ complétion (en reprenant les notations du lemme 1.2.15) ainsi que $\varphi : G \longrightarrow G'$ un homomorphisme de groupes continu. On aimerait montrer que l'on peut assigner à φ un morphisme $F(\varphi) : G_{\hat{\mathcal{C}}} \longrightarrow G'_{\hat{\mathcal{C}}}$. Or, par définition de la pro-$\mathcal{C}$ complétion (lemme 1.2.15), on a l'existence de $\bar{\phi} : G_{\hat{\mathcal{C}}} \longrightarrow G'_{\hat{\mathcal{C}}}$ tel que le diagramme suivant commute :



Il suffit donc de prendre $F(\varphi) = \bar{\varphi}$.

(ii) On aimerait montrer que pour tout groupe topologique G, $F(\mathrm{id}_G) = \mathrm{id}_{G_{\hat{\mathcal{C}}}}$. On voit que c'est le cas en prenant $H = G_{\hat{\mathcal{C}}}$ dans la définition de la pro-$\mathcal{C}$ complétion et $\varphi = \tau$: l'unicité du morphisme $\bar{\varphi}$ entraîne que $\bar{\varphi} = \mathrm{id}$.

(iii) Soit G'' un groupe topologique et $\varphi : G \longrightarrow G'$ ainsi que $\varphi' : G' \longrightarrow G''$ deux morphismes. Le fait que $F(\varphi'\varphi) = F(\varphi')F(\varphi)$ se montre en utilisant l'unicité du morphisme induit.

□

1.3.6 Propriétés supplémentaires

Définition 1.3.38 (Sous-ensemble cofinal)
Soit I un ensemble filtrant et $J \subset I$. J est dit cofinal *dans I si pour tout $i \in I$, il existe $j \in J$ tel que $i \leq j$.*

Proposition 1.3.39
Soit I un ensemble filtrant, $G = \varprojlim_I G_i$ un groupe profini et J un sous-ensemble cofinal de I. Alors

$$\varprojlim_{j \in J} G_j \cong G.$$

Démonstration. Soit $f : I \longrightarrow J$ la fonction qui associe à chaque $i \in I$ un élément $j \in J$ avec $i \leq j$. Soit π_J la projection de G dans $\prod_{j \in J} G_j$. En fait, il est clair que $\operatorname{im} \pi_J \subset \varprojlim_J$. Puisque π_J est une projection, elle est ouverte et continue.
La surjectivité est claire. Pour l'injectivité, supposons que $\pi_J(x) = \pi_J(y)$ et soit $i \in I$, alors :

$$x_i = \varphi_i(x) = \varphi_{f(i)i}\,\varphi_{f(i)}(x) = \varphi_{f(i)i}\,\varphi_{f(i)}(y) = y_i,$$

ce qui implique que

$$G \cong \varprojlim_{j \in J} G_j.$$

□

1.4 Groupes profinis et théorie de Galois

Bien qu'actuellement les groupes profinis soient étudiés pour eux-mêmes et utilisés dans plusieurs domaines des mathématiques[1], leur théorie a été initialement mise au point afin de pouvoir généraliser certains résultats de théorie de Galois des extensions finies.

1.4.1 Théorie de Galois finie - Rappels et notations

Le but de cette section est de présenter quelques notations et de rappeler le théorème principal de la théorie de Galois finie.

Notation 1.4.1
Soit G un groupe agissant sur un ensemble X. On note alors

$$X^G = \{x \in X : gx = x, \forall g \in G\}.$$

Définition 1.4.2 (Groupe de Galois)
Soit K un corps et F une extension galoisienne (c'est-à-dire normale et séparable) finie de K. Le groupe de Galois *de F sur K, noté $\mathcal{G}\mathrm{al}(F,K)$ est*

$$\mathcal{G}\mathrm{al}(F,K) = \left\{\sigma \in \mathrm{Aut}(F) : \sigma\big|_K = \mathrm{id}_K\right\}.$$

Théorème 1.4.3 (Théorème fondamental de la théorie de Galois)
Soit K un corps et F une extension galoisienne finie de K. Posons $G = \mathcal{G}\mathrm{al}(F,K)$.

(*i*) *Considérons les applications suivantes :*

$$\begin{array}{rcl} \{K \subset E \subset F : E \text{ sous corps de } F\} & \longleftrightarrow & \{H \leq \mathcal{G}\mathrm{al}(F,K)\} \\ E & \longmapsto & \mathcal{G}\mathrm{al}(F,E) \\ F^H & \longleftarrow\!\shortmid & H. \end{array}$$

Ces deux applications sont bijectives et inverses l'une de l'autre.

(*ii*) *Si le sous-corps E de F correspond au sous-groupe H, alors $[F:E] = |H|$ et $[E:K] = |G:H|$.*

(*iii*) *Si le sous-corps E de F correspond à H, alors E est normale sur K si et seulement si $H \trianglelefteq G$.*

(*iv*) *Si $K \subset E \subset F$ est une extension normale de K, alors*

$$\mathcal{G}\mathrm{al}(F,K)\,/\mathcal{G}\mathrm{al}(F,E) \cong \mathcal{G}\mathrm{al}(E,K).$$

Démonstration. On trouve la preuve de ce théorème dans de nombreux livres traitant de la théorie de Galois ou de l'algèbre (par exemple dans [Lan02]). □

Un problème surgit déjà si l'on tente de généraliser le point (*i*) à une extension infinie. Si la première composition est l'identité :

$$F^{\mathcal{G}\mathrm{al}(F,E)} = E,$$

1. Sous prétexte de présenter 4 livres traitant des groupes profinis, Alexander Lubotzky (voir [Lub07]) présente quelques thèmes liés à la recherche dans des domaines touchants les groupes profinis.

cela n'est pas forcément le cas de l'autre (voir exemple ci-dessous). On verra que l'autre composée est l'identité si l'on se restreint aux sous-groupes H de G qui sont fermés pour une certaine topologie, appelée topologie de Krull.

Exemple 1.4.4
Considérons l'extension de $\mathbb{Q}$ suivante :

$$F = \mathbb{Q}(\sqrt{p}, p \in \mathbb{P}).$$

Puisque F est une extension de $\mathbb{Q}$ elle est séparable et elle est normale car le polynôme minimal de chaque $\sqrt{p}$ est de degré 2. Pour tout $p \in \mathbb{P}$, considérons maintenant les $\mathbb{Q}$-automorphismes de F suivants :

$$\begin{aligned} \sigma_p : \sqrt{p} &\longmapsto -\sqrt{p} \\ \sqrt{q} &\longmapsto \sqrt{q}, \quad q \in \mathbb{P}, q \neq p, \end{aligned}$$

et le sous-groupe de $\mathcal{G}\mathrm{al}\,(F, \mathbb{Q})$ qu'ils engendrent :

$$H = \langle \sigma_o, p \in \mathbb{P} \rangle.$$

On remarque qu'un élément $\varphi \in H$ permute le signe d'un nombre fini de $\sqrt{p}$, ce qui implique que l'isomorphisme qui envoie tout $\sqrt{p}$ sur $-\sqrt{p}$ n'appartient pas à H. Ainsi, H est un sous-groupe propre de $\mathcal{G}\mathrm{al}\,(F, \mathbb{Q})$. Pourtant

$$F^H = \mathbb{Q} = \mathbb{Q}^{\mathcal{G}\mathrm{al}(F,\mathbb{Q})},$$

ce qui exclut l'injectivité de la composée.

1.4.2 Théorie de Galois - Cas infini

Définition 1.4.5 (Topologie de Krull)
Soit K un corps et F une extension galoisienne (éventuellement infinie) de K. Le but est d'exhiber un système fondamental de voisinages de l'unité constitué de sous-groupes normaux, ce qui permettra la définition d'une topologie sur G.
Considérons l'ensemble suivant

$$\mathcal{F} = \{E : K \subset E \subset F, E \text{ extension galoisienne finie de } K\}$$

et notons $G = \mathcal{G}\mathrm{al}\,(F, K)$ ainsi que $G'_E = \mathcal{G}\mathrm{al}\,(F, E)$ et $G_E = \mathcal{G}\mathrm{al}\,(E, K)$ pour tout $E \in \mathcal{F}$. On a alors les propriétés suivantes :

(*i*) *$G'_E \trianglelefteq G$ pour tout $E \in \mathcal{F}$ (malgré que G'_E puisse être infini, la démonstration est la même que dans le cas fini).*

(*ii*) *Soient $A, B \in \mathcal{F}$ et considérons G'_A ainsi que G'_B. On a alors :*

$$G'_A \cap G'_B = G'_{A \vee B},$$

où $A \vee B$ désigne le plus petit corps contenant A et B. Puisque $A \vee B$ est finie et galoisienne sur K, on a $A \vee B \in \mathcal{F}$.

Ces deux propriétés entraînent que $\{G'_E : E \in \mathcal{F}\}$ forme une base de filtre constituée de sous-groupes normaux. Ainsi, par la proposition 1 du chapitre 3 de [Bou07], il existe une et une seule topologie sur G qui soit compatible avec la structure de groupes. Cette topologie est appelée topologie de Krull.

Remarque 1.4.6
Si F est une extension finie de K, alors $F \in \mathcal{F}$. Dans ce cas $G'_F = \mathcal{G}\mathrm{al}\,(F,F) = \{\mathrm{id}\}$, ce qui implique que la topologie de Krull est la topologie discrète.

Théorème 1.4.7
Soit K un corps et F une extension galoisienne de K. Alors, si $G = \mathcal{G}\mathrm{al}\,(F,K)$ est muni de la topologie de Krull, on a, avec les mêmes notations que ci-dessus

$$G = \varprojlim_{E \in \mathcal{F}} \mathcal{G}\mathrm{al}\,(E,K)\,.$$

En particulier G est un groupe profini.

Démonstration. Pour commencer, montrons que cette limite projective a un sens. Il est clair que $(\mathcal{F}, \subset)$ est un ensemble partiellement ordonné. Le fait qu'il s'agisse d'un ensemble filtrant provient du fait que si $E_1, E_2 \in \mathcal{F}$ alors $E_1 \vee E_2 \in \mathcal{F}$.
Soient $E_1, E_2 \in \mathcal{F}$ des corps intermédiaires tels que $E_1 \subset E_2$. On définit :

$$\begin{aligned} \varphi_{E_1E_2} : \mathcal{G}\mathrm{al}\,(E_2,K) &\longrightarrow \mathcal{G}\mathrm{al}\,(E_1,K) \\ \sigma &\longmapsto \sigma\big|_{E_1}. \end{aligned}$$

Remarquons que puisque E_1 est normale sur K, cette application est bien définie, c'est-à-dire $\mathrm{im}\,\sigma\big|_{E_1} \subset E_1$.
Puisque tous les corps considérés sont normaux et algébriques sur K, cette application est surjective : un isomorphisme $\sigma : E_1 \longrightarrow E_1$ peut être prolongé en un isomorphisme de E_2, ce qui implique que $\varphi_{E_1E_2}$ est un homomorphisme de groupes surjectif. Si $E_1 \subset E_2 \subset E_3$ on a pour $\sigma \in \mathcal{G}\mathrm{al}\,(E_3,K)$

$$\varphi_{E_1E_2}\,\varphi_{E_2E_3}(\sigma) = \varphi_{E_1E_2}\,\sigma\big|_{E_2} = \sigma\big|_{E_1} = \varphi_{E_3E_1}(\sigma).$$

Ainsi, $\left(\mathcal{G}\mathrm{al}\,(E,K)\,,\varphi_{EE'}\right)$ forme un système projectif surjectif de groupes finis.
Définissons maintenant :

$$\begin{aligned} \varphi : G &\longrightarrow \prod_{E \in \mathcal{F}} \mathcal{G}\mathrm{al}\,(E,K) \\ \sigma &\longmapsto \varphi(\sigma),\ \text{où } \varphi(\sigma)_E = \sigma\big|_E\,. \end{aligned}$$

Soient $E_1 \subset E_2$ deux éléments de $\mathcal{F}$ et $\sigma \in G$, alors :

$$\varphi_{E_1E_2}\,\varphi(\sigma)_{E_2} = \varphi_{E_1E_2}\,\sigma\big|_{E_2} = \sigma\big|_{E_1} = \varphi(\sigma)_{E_1},$$

ce qui implique que $\mathrm{im}\,\varphi \subset \varprojlim \mathcal{G}\mathrm{al}\,(E,K) \subset \prod_E \mathcal{G}\mathrm{al}\,(E,K)$.
Montrons que φ est injective. Pour cela, supposons que $\varphi(\sigma) = \mathrm{id}$. Si $\sigma \neq \mathrm{id}$, il existe $\alpha \in F$ tel que $\sigma(\alpha) \neq \alpha$. Considérons $E = K[\alpha]$, que l'on peut inclure dans une extension finie et normale $\tilde{E}$. Ainsi, $\tilde{E} \in \mathcal{F}$ et donc $\sigma\big|_{\tilde{E}} = \mathrm{id}_{\tilde{E}}$, ce qui implique que $\sigma(\alpha) = \alpha$, contradiction. Ainsi, σ est l'identité sur F et φ est injective.
Pour la surjectivité, soit $\rho \in \varprojlim \mathcal{G}\mathrm{al}\,(E,K)$. De la même manière que ci-dessus, on peut construire pour chaque $\alpha \in F$ une extension F_α normale finie de K telle que $\alpha \in F_\alpha$. On pose alors $\sigma(\alpha) = \rho_{F_\alpha}(\alpha)$, qui est bien définie (puisque ρ appartient à la limite projective, on sait que pour toute extension finie E de K contenant α, $\rho_E(\alpha)$ a la même valeur). Alors, $\varphi(\sigma) = \rho$.
Soit $E \in \mathcal{F}$, on a alors

$$\varphi_E^{-1}(\{\mathrm{id}\}) = \{\sigma \in G : \sigma\big|_E = \mathrm{id}_E\} = G'_E.$$

Puisque les G'_E sont des voisinages ouverts de id, il s'ensuit que φ_E est continue et donc que φ est continue.
Montrons maintenant qu'il s'agit d'une application ouverte. Pour cela, soit $G'_E = \mathcal{G}\mathrm{al}(F,E)$ un voisinage ouvert de l'identité, on a alors :

$$\varphi(G'_E) = \varprojlim_A G_A \bigcap \Big(\prod_{A \subset E} \{\mathrm{id}\} \times \prod_{A \not\subset E} G_A \Big).$$

Ainsi, un ouvert de base de G est envoyé sur un ouvert de base de $\varprojlim G_A$, ce qui implique que φ est une application ouverte, comme désiré. Il s'ensuit que φ est isomorphisme de groupes topologiques. □

Proposition 1.4.8
Soit p un premier impair et $n \in \mathbb{N}$. Alors $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$ est cyclique.

Démonstration. Voir les articles 82 à 89 de [Gau86] ou le corollaire 13 du chapitre 19 de [Chi08]. □

Exemples 1.4.9 (i) Soit p un nombre premier. Alors, le groupe de Galois $\mathcal{G}\mathrm{al}\left(\bar{\mathbb{F}}_p, \mathbb{F}_p\right)$ est isomorphe à $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. Tout d'abord, remarquons que pour tout $n \in \mathbb{N}$, $\mathbb{F}_p$ possède une extension galoisienne de degré n, à savoir $\mathbb{F}_{p^n}$. On montre que $\mathcal{G}\mathrm{al}(\mathbb{F}_{p^n}, \mathbb{F}_p)$ est cyclique d'ordre n en considérant l'automorphisme

$$\begin{array}{rcl} \sigma : \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ x & \longmapsto & x^p \end{array}$$

qui engendre le groupe de Galois. Le fait que $\mathcal{G}\mathrm{al}(\mathbb{F}_{p^m}, \mathbb{F}_p)$ soit cyclique d'ordre m pour tout m implique l'uncité du corps intermédiaire de degré n pour chaque n.

(ii) Soit K un corps fini, alors $\mathcal{G}\mathrm{al}\left(\bar{K}, K\right) \cong \hat{\mathbb{Z}}$. On a $K = \mathbb{F}_{p^n}$ pour un certain $p \in \mathbb{P}$ et un $n \in \mathbb{N}$ et on fait ensuite comme au point (i).

(iii) Soit p un premier impair. Pour $m \in \mathbb{N}$, on note ζ_m une racine primitive m-ème de l'unité dans $\bar{\mathbb{Q}}$. Alors, en posant $F = \bigcup_{n\in\mathbb{N}} \mathbb{Q}[\zeta_{p^n}]$ et $K = \mathbb{Q}[\zeta_p]$, on a :

$$\mathcal{G}\mathrm{al}(F,K) \cong \mathbb{Z}_p.$$

En effet, on note, pour $n \in \mathbb{N}$, $E_n = \mathbb{Q}[\zeta_{p^n}]$ (c'est-à-dire $E_1 = K$) et, comme précédemment

$$\mathcal{F} = \{K \subset E \subset F : E \text{ extensions galoisienne finie de } K\}.$$

Remarquons que $\{E_n : n \in \mathbb{N}\}$ est cofinal dans $\mathcal{F}$, ce qui implique que

$$\varprojlim_{E\in\mathcal{F}} \mathcal{G}\mathrm{al}(E,K) \cong \varprojlim_{n\in\mathbb{N}} \mathcal{G}\mathrm{al}(E_n,K),$$

par la proposition 1.3.39. On sait par la théorie de Galois classique que pour tout $m \in \mathbb{N}$ on a $\mathcal{G}\mathrm{al}(\mathbb{Q}[\zeta_m], \mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ et

$$\mathcal{G}\mathrm{al}(E_n, \mathbb{Q}) / \mathcal{G}\mathrm{al}(E_n, K) \cong \mathcal{G}\mathrm{al}(K, \mathbb{Q}).$$

Ainsi, $\mathcal{G}\mathrm{al}(E_n, E_1)$ est un sous-groupe d'ordre p^{n-1} du groupe cyclique $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$, ce qui implique que

$$\mathcal{G}\mathrm{al}(F,K) \cong \varprojlim_{n\in\mathbb{N}} \mathcal{G}\mathrm{al}(E_n,E_1) \cong \varprojlim_{n\in\mathbb{N}} C_{p^{n-1}} = \mathbb{Z}_p.$$

Théorème 1.4.10 (Théorème fondamental de la théorie de Galois)
Soit K un corps et F une extension galoisienne de K. Posons $G = \mathcal{G}\mathrm{al}(F,K)$, muni de la topologie de Krull.

(*i*) *Considérons les applications suivantes :*

$$\begin{aligned} \mathcal{C} = \{K \subset E \subset F : E \text{ sous corps de } F\} &\longleftrightarrow \{H \leq_c G\} \\ \Phi : E &\longmapsto \mathcal{G}\mathrm{al}(F,E) \\ F^H &\longleftarrow\!\shortmid H : \Psi. \end{aligned}$$

Ces deux applications sont bijectives et inverses l'une de l'autre.

(*ii*) *Si le sous-corps E de F correspond à H, alors E est normale sur K si et seulement si $H \trianglelefteq G$.*

(*iii*) *Si $K \subset E \subset F$ est une extension normale de K, alors*

$$\mathcal{G}\mathrm{al}(F,K)\,/\mathcal{G}\mathrm{al}(F,E) \cong \mathcal{G}\mathrm{al}(E,K).$$

Démonstration. (i) Remarquons tout d'abord que l'application Φ est bien définie : pour un corps intermédiaire E, $\mathcal{G}\mathrm{al}(F,E)$ est un sous-groupe profini de G, qui est donc fermé.
On va montrer que $\Psi\Phi = \mathrm{id}_{\mathcal{C}}$. Pour cela, soit E une extension intermédiaire. On a clairement, $E \subset \Psi\Phi(E)$. Pour l'autre inclusion, soit $\alpha \in F^{\mathcal{G}\mathrm{al}(F,E)}$ et f le polynôme minimal de α sur E. Puisque $\sigma(\alpha) = \alpha$ pour tout $\sigma \in \mathcal{G}\mathrm{al}(F,E)$ et que $\sigma(\alpha)$ est une racine de f, alors $\deg f = 1$ (par la séparabilité), ce qui implique que $E[\alpha] = E$ et donc $\alpha \in E$.
Montrons maintenant que $\Phi\Psi = \mathrm{id}_{\{H \leq_c G\}}$. Soit H un sous-groupe fermé de G. On doit montrer que $H = \mathcal{G}\mathrm{al}\left(F, F^H\right)$. L'inclusion $H \subset \mathcal{G}\mathrm{al}\left(F, F^H\right)$ est claire. Puisque H est fermé, il suffit alors de montrer que H est dense dans $H' = \mathcal{G}\mathrm{al}\left(F, F^H\right)$ ou, de manière équivalente, que chaque élément de H' est adhérent à H. Soit donc $\tau \in H'$. Il faut voir que $V \cap H \neq \emptyset$ pour tout voisinage V de τ ou, de manière équivalente, que $\tau W \cap H \neq \emptyset$ pour tout voisinage W de l'unité. Supposons donc que $N \subset P$ est une extension galoisienne finie de K telle que $N \supset F^H$. On doit alors montrer que

$$\tau\mathcal{G}\mathrm{al}(F,N) \cap H \neq \emptyset.$$

Soit $I = \{\sigma\big|_N : \sigma \in H\}$, qui est un groupe fini de K-automorphismes de N. Le théorème d'Artin (voir [Lan02]) implique que $I = \mathcal{G}\mathrm{al}\left(N, N^I\right)$, ce qui implique que $I = \mathcal{G}\mathrm{al}\left(N, F^H\right)$. Ainsi, il existe $\sigma \in H$ tel que $\tau\big|_N = \sigma\big|_N$ et donc

$$\sigma \in \tau\mathcal{G}\mathrm{al}(F,N) \cap H,$$

comme désiré.

(ii) Semblable au cas fini.

(iii) Soit $K \subset E \subset F$ une extension normale de K et considérons l'application :

$$\begin{aligned} \varphi : \mathcal{G}\mathrm{al}(F,K) &\longrightarrow \mathcal{G}\mathrm{al}(E,K) \\ \sigma &\longmapsto \sigma\big|_E, \end{aligned}$$

qui est bien définie car E est normale sur K. On constate alors que $\ker\varphi = \mathcal{G}\mathrm{al}(F,E)$, et donc

$$\mathcal{G}\mathrm{al}(F,K)\,/\mathcal{G}\mathrm{al}(F,E) \cong \mathcal{G}\mathrm{al}(E,K),$$

en tant que groupes topologiques (voir 1.1.17).

□

Théorème 1.4.11 (Tout groupe profini est un groupe de Galois)
Soit G un groupe profini. Alors il existe un corps K et une extension galoisienne F de K telle que $G = \mathcal{G}\mathrm{al}\,(F, K)$.

Démonstration. Cette preuve est analogue à celle de la théorie de Galois finie où l'on fait agir S_n sur $K(x_1, \ldots, x_n)$ par permutation des variables pour montrer que S_n peut être réalisé comme groupe de Galois.
Soit E un corps et considérons T comme étant l'union disjointe des ensembles quotients G/N, où N est un sous-groupe normal ouvert de G. On associe à chaque élément $t \in T$ une indéterminée X_t et on considère le corps des fractions rationnelles $F = E\big(X_t : t \in T\big)$. Un élément $g \in G$ agit naturellement sur une classe nN, par $g \cdot nN = (gn)N$, ce qui induit un E-automorphisme sur F par permutation des indéterminées. Ainsi, G agit sur F par groupes d'automorphismes. Le but est alors de montrer que le groupe de Galois de F sur $K = F^G$ est G.
Soit $f \in F$ et supposons que les indéterminées apparaissant dans f sont $x_{t_1}, \ldots, x_{t_n}$, où $t_i = g_i N_i \in G/N_i$. Alors, le stabilisateur G_f de f satisfait

$$G_f \supset \bigcap_{i=1}^{n} N_i,$$

ce qui implique, par la propriété (v) de 1.1.15, que G_f est ouvert et donc d'indice fini, puisque G est compact. Ainsi, l'orbite d'un élément de F est finie.
Montrons que F est une extension galoisienne de K. Pour cela, soit $f \in F$ et $f_1 = f, \ldots, f_n$ l'orbite de f sous l'action de G. Considérons le polynôme

$$\tilde{f}(x) = \prod_{i=1}^{n} (x - f_i).$$

Puisque $g \cdot \tilde{f} = \tilde{f}$ pour tout $g \in G$, on a que $\tilde{f} \in K[x]$. L'extension est donc algébrique. Par construction, les racines de $\tilde{f}$ sont toutes distinctes, ce qui implique que les racines de $\min(f, K)$ le seront aussi et donc que l'extension est séparable (on aurait aussi pu choisir le corps E de caractéristique 0). On constate que toutes les racines de $\min(f, K)$ seront dans F, ce qui implique qu'il s'agit d'une extension normale.
On a vu que tout élément de g induit un K-isomorphisme sur F, c'est-à-dire que G est (identifié à) un sous-groupe de $G' = \mathcal{G}\mathrm{al}\,(F, K)$. Puisque $F^G = F^{\mathcal{G}\mathrm{al}(F,K)}$, on aura, par le théorème fondamental, que $G = \mathcal{G}\mathrm{al}\,(F, K)$ pour autant que G soit fermé dans G'. Or, puisque G est compact et que G' est de Hausdorff, G est fermé dans G'. □

Chapitre 2

Cohomologie galoisienne

2.1 Motivation

Avant de commencer à définir les bases de la cohomologie galoisienne, nous allons voir une motivation à l'étude de ces outils. Cette motivation sera introduite dans un cadre précis au départ puis sera généralisée afin de conduire au problème de descente galoisienne. Cette approche est celle suivie par Grégory Berhuy dans ses notes de cours d'introduction à la cohomologie galoisienne (voir [Ber10]).

2.1.1 La conjuguaison de matrices

Considérons les deux matrices suivantes

$$M_0 = \begin{pmatrix} 1 & 4 \\ \frac{3}{2} & 4 \end{pmatrix}, \quad M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

On constate qu'elles sont conjuguées par la matrice suivante

$$\begin{pmatrix} 2i & 0 \\ 0 & i \end{pmatrix}.$$

Puisque les deux matrices M_0 et M sont réelles, il est légitime de se demander si elles ne sont pas conjuguées par une matrice réelle. On trouve facilement que c'est effectivement le cas. Ainsi, si deux matrices réelles sont conjuguées par un élément de $\mathrm{GL}_n(\mathbb{C})$ elles peuvent être conjuguées (ce résultat peut être montré avec des outils d'algèbre linéaire et nous le verrons plus tard dans un cadre plus général) par un élément de $\mathrm{GL}_n(\mathbb{R})$. Par contre, deux matrices réelles peuvent être conjuguées par un élément de $\mathrm{SL}_n(\mathbb{C})$ sans qu'il soit possible de trouver un élément de $\mathrm{GL}_n(\mathbb{R})$ qui remplisse le même rôle.

Notation 2.1.1
Soit K un corps, $n \in \mathbb{N}$. On note $G(K)$ pour $\mathrm{GL}_n(K)$ ou $\mathrm{SL}_n(K)$.

On peut maintenant généraliser le problème comme suit :

Problème 2.1.2 (Problème de descente galoisienne pour les matrices)
Soit K un corps, Ω une extension galoisienne de K et $M_0, M \in \mathrm{M}_n(K)$. S'il existe $Q \in G(\Omega)$ telle que $M_0 = QMQ^{-1}$, existe-t-il $P \in G(K)$ telle que $M_0 = PMP^{-1}$.

On verra comment les ensembles de cohomologie permettent de répondre à ces questions.

2.2 Ensembles de cohomologie

Définition 2.2.1 (Ensemble pointé)
Un ensemble pointé *est un couple (X, x_0), où X est un ensemble et $x_0 \in X$. L'élément x_0 est alors appelé* point de base.

Définition 2.2.2 (Morphisme d'ensembles pointés)
Si (X, x_0) et (Y, y_0) sont deux ensembles pointés, une application $f : X \longrightarrow Y$ est un morphisme d'ensemble pointés si $f(x_0) = y_0$.

Exemples 2.2.3 (i) Un groupe est un ensemble pointé (dont le point de base est l'élément neutre) et les homomorphismes de groupes sont des morphismes d'ensembles pointés.

(ii) Quand on parle du groupe fondamental d'un espace topologique, on considère souvent l'espace comme un ensemble pointé : le point de base est le point de base des lacets.

Définition 2.2.4 (Noyau d'un morphisme d'ensembles pointés)
Si $f : (X, x_0) \longrightarrow (Y, y_0)$ est un morphisme d'ensembles pointés, le noyau *de f est*

$$\ker f = \{x \in X : f(x) = y_0\}.$$

Définition 2.2.5 (G-groupe (cas fini))
Soit G un groupe fini. Un groupe A est appelé G-groupe *si G agit sur A par automorphismes de groupe, c'est-à-dire si*

$$\sigma \cdot (a_1 a_2) = (\sigma \cdot a_1)(\sigma \cdot a_2).$$

Définition 2.2.6 (Action continue)
Soit A un G-groupe, muni de la topologie discrète. On dit que G agit continûment *sur A si l'application de $G \times A$ dans A est continue.*

Dans ce qui suit, l'énoncé « soit A un G-groupe » signifiera toujours que G est fini et muni de la topologie discrète ou bien qu'il est profini. De plus, l'action sera toujours considérée comme continue.

Proposition 2.2.7
Soit G un groupe profini et A un G-groupe. Alors les conditions suivantes sont équivalentes :

(i) $A = \bigcup A^U$, *où U parcourt l'ensemble des sous-groupes ouverts de G.*

(ii) Pour tout $a \in A$ son stabilisateur S_a est un sous-groupe ouvert de G.

(iii) L'action est continue (au sens de la définition ci-dessus).

Démonstration. On note $\varphi : G \times A \longrightarrow A$ l'action de G sur A.

$(i) \Rightarrow (ii)$ Soit $a \in A$ et $U \trianglelefteq_o G$ tel que $a \in A^U$. On a alors $U \subset S_a$ ce qui implique que S_a est ouvert dans G (point (v) de la proposition 1.1.15).

$(ii) \Rightarrow (iii)$ Si a est un élément de A et si $(g, b) \in \varphi^{-1}(\{a\})$, alors $g\,S_b \times \{b\}$ est un ouvert du produit qui est envoyé sur $g \cdot b = a$. En effet, si $(gx, b) \in g\,S_b \times \{b\}$, alors

$$\varphi(gx, b) = (gx)b = g(xb) = gb = b.$$

$(iii) \Rightarrow (ii)$ Si l'on choisit $a \in A$ et que l'on définit $i : G \longrightarrow G \times A$ par $i(g) = (g, a)$, on trouve $S_a = (\varphi i)^{-1}\big(\{a\}\big)$ (l'inclusion i est continue).

$(ii) \Rightarrow (i)$ Une des inclusions est claire. Maintenant, si $a \in A$, alors $a \in A^{S_a}$ et, par hypothèse, S_a est ouvert.

□

Définition 2.2.8 (0-ème ensemble de cohomologie)
Si A est un G-ensemble, on note

$$H^0(G, A) := A^G,$$

que l'on appelle 0-ème ensemble de cohomologie de G à coefficient dans A.

Remarque 2.2.9
Si A est un G-groupe, $H^0(G, A)$ est un sous-groupe de A.

Définition 2.2.10 (1-cocycle)
Soit A un G-groupe. Un 1-cocycle (qui sera noté cocycle dans la suite de ce document, puisque qu'aucun cocycle de dimension supérieure ne sera utilisé) de G à valeurs dans A est une application continue

$$\begin{array}{rcl} \alpha : G & \longrightarrow & A \\ \sigma & \longmapsto & \alpha_\sigma, \end{array}$$

telle que

$$\alpha_{\sigma\tau} = \alpha_\sigma \, \sigma \cdot \alpha_\tau, \quad \forall \sigma, \tau \in G.$$

Notation 2.2.11
On note $Z^1(G, A)$ l'ensemble des cocycles de G à valeurs dans A.

Exemples 2.2.12 (i) L'application qui envoie tout élément de g sur $1 \in A$ est un cocycle appelé cocycle trivial.

(ii) Si G agit trivialement sur A (c'est-à-dire si $\sigma \cdot a = a$ pour tout $\sigma \in G$ et tout $a \in A$), alors la condition donne :

$$\alpha_{\sigma\tau} = \alpha_\sigma \alpha_\tau,$$

qui est vérifiée si et seulement si α est un homomorphisme de groupes.

Lemme 2.2.13
Soit A un G-groupe et $\alpha \in Z^1(G, A)$. Pour tout $a \in A$, l'application

$$\begin{array}{rcl} \alpha' : G & \longrightarrow & A \\ \sigma & \longmapsto & a \, \alpha_\sigma \, \sigma \cdot a^{-1} \end{array}$$

est un cocycle.

Démonstration. Calcul. □

Définition 2.2.14 (Cocycles cohomologues)
Deux cocycles $G \overset{\alpha}{\underset{\alpha'}{\rightrightarrows}} A$ sont dits cohomologues, *ce que l'on note $\alpha \sim \alpha'$, s'il existe $a \in A$ tel que*

$$\alpha'_\sigma = a \, \alpha_\sigma \, \sigma \cdot a^{-1}, \quad \forall \sigma \in G.$$

On vérifie que le fait d'être cohomologue est une relation d'équivalence, ce qui motive la définition suivante.

Définition 2.2.15 (Premier ensemble de cohomologie)
L'ensemble quotient $H^1(G,A) = Z^1(G,A)/_\sim$ *est appelé* premier ensemble de cohomologie de G à coefficient dans A. *La classe d'un élément* α *est notée* $[\alpha]$ *ou* $\bar{\alpha}$.

Lien avec la cohomologie de groupes classique

Si G, A sont comme ci-dessus, on aimerait bien que $Z^1(G,A)$ hérite d'une structure de groupe, ce qui permettrait, éventuellement, que $H^1(G,A)$ soit, lui aussi, un groupe. Malheureusement, on ne peut définir une loi de groupe sur $Z^1(G,A)$ que si A est abélien. Dans ce cas, on pose, pour $\alpha, \beta \in Z^1(G,A)$

$$(\alpha\beta)_\sigma = \alpha_\sigma \, \beta_\sigma, \quad \forall \sigma \in G.$$

On constate alors que cette loi est compatible avec la relation $\sim$ et qu'ainsi $H^1(G,A)$ hérite d'une structure de groupe. On peut alors définir facilement (voir plus bas) les groupes de cohomologie $H^2(G,A)$, $H^3(G,A)$, etc. Dans le cas non-abélien, il est possible de définir H^2 mais c'est un peu délicat (voir [Gir71]). Nous allons présenter maintenant la définition classique des groupes de cohomologie afin de déterminer quel est le lien avec la définition présentée ci-dessus. La définition utilisée ici est celle proposée dans [Rib70].

Définition 2.2.16 (Groupes de cohomologie)
Soit A *un* G*-groupe avec* A *abélien. Soit* $n \in \mathbb{N}_0$. *On considère* $C^n(G,A)$ *le groupe des applications continues (pas des homomorphismes !) de* G^n *dans* A *(*G^n *est muni de la topologie du produit), dont les éléments sont appelés* n-cochaînes. *Pour* $n \in \mathbb{N}$, *on définit le* cobord *:*

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

de la manière suivante :

$$\begin{aligned}(d^n\alpha)(\sigma_1,\ldots,\sigma_{n+1}) &= \sigma_1\alpha(\sigma_2,\ldots,\sigma_{n+1}) + \sum_{i=1}^{n}(-1)^i\alpha(\sigma_1,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_{n+1}) \\ &\quad +(-1)^{n+1}\alpha(\sigma_1,\ldots,\sigma_n).\end{aligned}$$

On vérifie que $d^{n+1}d^n = 0$ *pour tout* $n \in \mathbb{N}$, *ce qui implique que* $\left(C^\bullet, d^\bullet\right)$ *est un complexe de cochaîne. On pose alors :*

$$\begin{aligned} Z^n(G,A) &= \ker d^n, \quad n \in \mathbb{N}_0, \\ B^n(G,A) &= \operatorname{im} d^{n-1}, \quad n \in \mathbb{N}, \\ B^0 &= 0 \end{aligned}$$

et pour finir

$$H^n(G,A) = Z^n(G,A)/_{B^n(G,A)}.$$

On cherche à expliciter $H^0(G,A)$ et $H^1(G,A)$ dans la définition ci-dessus. Par convention $G^0 = \{1\}$, ce qui implique que $C^0(G,A)$ peut être identifié à A. On trouve alors que $\ker d^0 = A^G$, et donc $H^0(G,A)$ est (identifié à) A^G. Pour $n = 1$, on trouve

$$B^1(G,A) = \operatorname{im} d^0 = \left\{\sigma \cdot a - a : \sigma \in G, a \in A\right\},$$

et

$$(d^1\alpha)(\sigma_1, \sigma_2) = \sigma_1\alpha(\sigma_2) - \alpha(\sigma_1\sigma_2) + \alpha(\sigma_1),$$

ce qui implique

$$Z^1(G, A) = \ker d^1 = \Big\{\alpha \in C^1(G, A) : \alpha(\sigma_1\sigma_2) = \alpha(\sigma_1) + \sigma_1\alpha(\sigma_2)\Big\}.$$

On remarque alors que cela correspond à ce que l'on a défini plus haut dans le cas non commutatif. On aimerait voir si la relation d'équivalence modulo $B^1(G, A)$ correspond à la notion de cocycles cohomologues. Pour cela, supposons que $\alpha, \alpha' \in Z^1(G, A)$ soient deux cocycles tels que $\overline{\alpha} = \overline{\alpha'}$, ce qui implique qu'il existe $a \in A$ tel que

$$\alpha(\sigma) - \alpha'(\sigma) = \sigma \cdot a - a, \quad \forall \sigma \in G,$$

c'est-à-dire

$$\alpha'(\sigma) = a + \alpha(\sigma) + \sigma \cdot (-a),$$

comme désiré. On constate donc que ce qui a été fait (définitions 2.2.10 et 2.2.14) est cohérent avec ce qui se fait dans le cas abélien.

2.3 Suites exactes

On rappelle que les H^0 et les H^1 sont vus comme des ensembles pointés. Le point de base du premier est l'élément neutre du groupe et celui du second est la classe du cocycle trivial.

Définition 2.3.1 (Morphismes compatibles)
Soit A un G-groupe, A' un G'-groupe ainsi que $\varphi : G' \longrightarrow G$ et $f : A \longrightarrow A'$ deux morphismes de groupes continus. On dit que f et φ sont compatibles *si*

$$f\big(\varphi(\sigma') \cdot a\big) = \sigma' \cdot f(a), \quad \forall \sigma' \in G', a \in A.$$

Proposition 2.3.2
Soient A, A' ainsi que f, φ comme ci-dessus. Alors f induit deux morphismes :

$$\begin{array}{rcl} f_* : H^0(G, A) & \longrightarrow & H^0(G', A') \\ a & \longmapsto & f(a), \end{array}$$

et

$$f_* : H^1(G, A) \longrightarrow H^1(G', A').$$

Démonstration. La flèche induite entre les H^0 ne pose pas de problème. Pour la deuxième partie, commençons par définir une application

$$\begin{array}{rcl} f_* : Z^1(G, A) & \longrightarrow & Z^1(G'A') \\ \alpha & \longmapsto & \beta, \quad \beta_{\sigma'} = f\big(\alpha_{\varphi(\sigma')}\big), \quad \forall \sigma' \in G'. \end{array}$$

Le fait que β soit un cocycle découle d'un simple calcul. La continuité de β provient du fait que l'on a la composition d'applications continues suivante :

$$G' \xrightarrow{\varphi} G \xrightarrow{\alpha} A \xrightarrow{\qquad f \qquad} A'$$

$$\sigma' \longmapsto \varphi(\sigma') \longmapsto \alpha_{\varphi(\sigma')} \longmapsto f\big(\alpha_{\varphi(\sigma')}\big) = \beta_{\sigma'}.$$

Un calcul direct montre que l'application f_* est compatible avec la relation d'équivalence des cocycles, ce qui implique qu'elle passe au quotient en un morphisme d'ensembles pointés $f_* : H^1(G, A) \longrightarrow H^1(G', A')$. □

Exemple 2.3.3
En prenant $G = G'$ et $\varphi = \mathrm{id}_G$, on trouve qu'un morphisme compatible $f : A \longrightarrow A'$ est juste un morphisme de G-groupes. Dans ce cas, pour $[\alpha] \in H^1(G, A)$, on a $f_*([\alpha]) = [f\alpha]$.
En fait, si on se fixe un groupe profini G, on a un foncteur $H^1(G, -)$ de la catégorie des G-groupes dans la catégorie des ensembles pointés.

Remarque 2.3.4
Si $1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$ est une suite exacte de G-groupes, alors

$$g(b) = g(b') \Leftrightarrow \exists a \in A,\ b' = bf(a).$$

En fait, cette équivalence reste vraie dans le cas suivant : A est un sous-groupe (pas forcément normal) de B, f est l'inclusion, $C = B/A$ et g est l'application de passage au quotient. En effet, on a

$$g(b) = g(b') \Leftrightarrow b' \equiv b \pmod{A} \Leftrightarrow b' = ba \Leftrightarrow b' = bf(a).$$

2.3.1 Premier morphisme de connexion

Pour cette section, on va considérer la suite exacte de G-groupes suivante :

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

Le but est de montrer que cette suite exacte va induire un morphisme d'ensembles pointés $\delta^0 : H^0(G,C) \longrightarrow H^1(G,A)$, appelé *premier morphisme de connexion*, tel que la suite suivante soit exacte

$$1 \longrightarrow A^G \xrightarrow{f_*} B^G \xrightarrow{g_*} C^G \xrightarrow{\delta^0} H^1(G,A) \xrightarrow{f_*} H^1(G,B) \xrightarrow{g_*} H^1(G,C).$$

Diagramme 2.1: Suite exacte induite

Le fait que la première partie $1 \longrightarrow A^G \xrightarrow{f_*} B^G \xrightarrow{g_*} C^G$ de la suite soit exacte est clair vu la définition de f_*, g_* pour les ensembles H^0.

Définition du morphisme de connexion

Soit $c \in C^G$. Puisque g est surjectif, il existe $b \in B$ tel que $g(b) = c$. On a alors

$$g(\sigma \cdot b) = \sigma \cdot g(b) = \sigma \cdot c = c = g(b), \quad \forall \sigma \in G.$$

La remarque 2.3.4 et l'injectivité de f impliquent l'existence d'un unique élément $\alpha_\sigma \in A$ tel que

$$\sigma \cdot b = bf(\alpha_\sigma).$$

On aimerait donc poser $\delta^0(c) = [\alpha]$. Il faut voir maintenant que α est un cocycle continu et que sa définition ne dépend pas du choix de b. Si $b' \in B$ est une autre préimage de c, on obtient une autre application $\alpha' : G \longrightarrow A$. On a alors, pour $\sigma \in G$

$$\begin{aligned} f(\alpha'_\sigma) &= b'^{-1}\sigma \cdot b' \overset{2.3.4}{=} \big(bf(a)\big)^{-1}\sigma \cdot \big(bf(a)\big) \\ &= f(a)^{-1}f(\alpha_\sigma)\,\sigma \cdot f(a), \end{aligned}$$

ce qui implique, puisque f est un morphisme injectif, que α et α' satisfont la relation de cohomologie (pour autant que α soit un cocycle). Ainsi, l'application δ^0 est bien définie. Pour montrer que α est bien un cocycle, on effectue le calcul direct. Pour la continuité, on a

$$\begin{aligned} \alpha^{-1}\big(\{1\}\big) &= \{\sigma \in G : \alpha_\sigma = 1\} \\ &= \{\sigma \in G : f(\alpha_\sigma) = 1\} \\ &= \{\sigma \in G : b^{-1}\sigma \cdot b = 1\} \\ &= S_b, \end{aligned}$$

qui est ouvert, puisque l'action de G sur B est continue (proposition 2.2.7).

Notation 2.3.5
Pour $c \in C^G$, $d^0(c)$ désignera le cocycle α construit ci-dessus (de telle sorte que $\pi d^0 = \delta^0$, où π est l'application de passage au quotient).

Exactitude en C^G

Le fait que $\operatorname{im} g_* \subset \ker \delta^0$ découle d'un simple calcul. Réciproquement, soit $c \in \ker \delta^0$, c'est-à-dire que $\alpha = d^0(c)$ est cohomologue au cocycle trivial : il existe $a \in A$ tel que

$$a\,\alpha_\sigma\,\sigma \cdot a^{-1} = 1, \quad \forall \sigma \in G.$$

Soit de plus $b \in B$ tel que $g(b) = c$. On trouve, en appliquant f à l'équation ci-dessus :

$$\begin{aligned} f(1) &= f(a)f(\alpha_\sigma)f(\sigma \cdot a^{-1}) \\ &= f(a)b^{-1}\,\sigma \cdot b\, f(\sigma \cdot a^{-1}), \end{aligned}$$

ce qui implique

$$bf(a^{-1}) = \sigma \cdot \big(bf(a^{-1})\big),$$

et donc $bf(a^{-1}) \in B^G$. Ainsi,

$$c = g(b) = g\big(bf(a^{-1})\big) = g_*\big(bf(a^{-1})\big),$$

comme désiré.

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

Soit $[\alpha] = \delta^0(c)$, pour un $c \in C^G$ dont l'une des préimages est b, et supposons que cette classe soit représentée par le cocycle α. On trouve alors pour $\sigma \in G$

$$f_*(\alpha)_\sigma = f(\alpha_\sigma) = b^{-1}\,\sigma \cdot b,$$

ce qui implique que $f_*(\alpha)$ est cohomologue au cocycle trivial et donc $[\alpha] \in \ker f_*$. Réciproquement, soit $[\alpha] \in \ker f_*$, ce qui implique qu'il existe $b \in B$ tel que

$$1 = b\, f(\alpha_\sigma)\, \sigma \cdot b^{-1}, \quad \forall \sigma \in G.$$

En posant, $c = g(b)$, on aura $\delta^0(c) = [\alpha]$ pour autant que $c \in C^G$. Pour vérifier cela, on calcule :

$$\sigma \cdot c = \sigma \cdot g(b) = g(\sigma \cdot b) = g\big(bf(\alpha_\sigma)\big) = g(b)g\big(f(\alpha_\sigma)\big) = g(b) = c.$$

Exactitude en $H^1(G, B)$

Un calcul direct montre que $\operatorname{im} f_* \subset \ker g_*$. Pour l'autre inclusion, soit $[\beta] \in \ker g_*$, c'est-à-dire qu'il existe $c \in C$ tel que

$$1 = c g_*(\beta)_\sigma\, \sigma \cdot c^{-1}, \quad \forall \sigma \in G$$

ce qui est équivalent à

$$g(\beta_\sigma) = c^{-1}\sigma \cdot c.$$

Si b est une préimage de c par g, on a

$$g(\beta_\sigma) = g(b^{-1}\,\sigma \cdot b).$$

La remarque 2.3.4 implique que pour tout $\sigma \in G$, il existe $\alpha_\sigma \in A$ tel que

$$\beta_\sigma = b^{-1}\,\sigma \cdot bf(\alpha_\sigma) \Leftrightarrow f(\alpha_\sigma) = \sigma \cdot b^{-1}\, b\, \beta_\sigma.$$

On écrit maintenant :

$$\begin{aligned}\beta_\sigma &= b^{-1}\,\sigma\cdot bf(\alpha_\sigma)\\ &= b^{-1}\,\sigma\cdot bf(\alpha_\sigma)\sigma\cdot b^{-1}\,\sigma\cdot b\\ &= b^{-1}f(\alpha'_\sigma)\sigma\cdot b,\end{aligned}$$

où l'on a utilisé le fait que $f(A)$ est normal dans B. La dernière égalité implique que

$$f(\alpha'_\sigma) = b\,\beta_\sigma\,\sigma\cdot b^{-1}.$$

Pour voir que α' est un cocycle, on calcule

$$\begin{aligned}f(\alpha'_{\sigma\tau}) &= b\,\beta_{\sigma\tau}\,(\sigma\tau)\cdot b^{-1}\\ &= b\,\beta_\sigma\sigma\cdot\beta_\tau\,(\sigma\tau)\cdot b^{-1}\\ &= b\,\beta_\sigma\,\sigma\cdot b^{-1}\sigma\cdot b\,\sigma\cdot(\beta_\tau\,\tau\cdot b^{-1})\\ &= b\,\beta_\sigma\,\sigma\cdot b^{-1}\sigma\cdot(b\,\beta_\tau\,\tau\cdot b^{-1})\\ &= f(\alpha'_\sigma)\sigma\cdot f(\alpha'_\tau) = f(\alpha'_\sigma\,\sigma\cdot\alpha'_\tau)\end{aligned}$$

et l'injectivité de f permet de conclure.

Remarque 2.3.6
Dans certains cas particuliers, il est possible de rajouter $H^2(G,A)$ et un deuxième morphisme de connexion à la suite exacte de la figure 2.1. C'est le cas si, par exemple, A se trouve dans le centre de B (voir section 5.7 de [Ser94]).

Proposition 2.3.7
En gardant les mêmes hypothèses (la même suite exacte) que précédemment, il est possible de définir une action de B^G sur C^G de telle manière à ce que l'on ait une bijection d'ensembles pointés entre l'ensemble des orbites et le noyau de l'application $f_* : H^1(G,A)\longrightarrow H^1(G,B)$.

Démonstration. On va procéder en plusieurs étapes.

Définition de l'action Soit $(b,c)\in B^G\times C^G$ et b' tel que $g(b')=c$. On pose alors : $b\cdot c = g(bb')$ et la remarque 2.3.4 permet de vérifier que l'action est bien définie (c'est-à-dire ne dépend pas du choix de la préimage de c). On vérifie maintenant que $b\cdot c$ appartient bien à C^G :

$$\sigma\cdot(b\cdot c) = \sigma\cdot g(bb') = g(b\,\sigma\cdot b') = g(bb') = b\cdot c,\quad \forall\sigma\in G,$$

où l'on utilise le fait que $g(\sigma b') = g(b')$, puisque b' est une préimage de c.

Application Le fait que la longue suite soit exacte implique que le noyau de l'application $f_* : H^1(G,A)\longrightarrow H^1(G,B)$ soit égal à $\operatorname{im}\delta^0$. Il suffit donc de constuire une bijection entre l'ensemble pointé des orbites C^G/B^G et $\operatorname{im}\delta^0$. Pour cela, on construit une application

$$\varphi : C^G/B^G\longrightarrow \operatorname{im}\delta^0$$

qui envoie une classe $[c]$ sur $\delta^0(c)$. Supposons que $c'\in[c]$, c'est-à-dire qu'il existe $d\in B^G$ tel que $c' = d\cdot c$. Choisissons une préimage b de c (ce qui implique $c' = g(db)$) et notons α ainsi que α' les cocycles obtenus respectivement par c et c'. Alors :

$$f(\alpha'_\sigma) = (db)^{-1}\,\sigma(db) = b^{-1}d^{-1}\,\sigma\cdot d\,\sigma\cdot b = b^{-1}\,\sigma\cdot b = f(\alpha_\sigma),\quad\forall\sigma\in G,$$

ce qui implique que les cocycles α et α' sont égaux et donc que l'application φ est bien définie.
On vérifie facilement que la classe de l'élément neutre de C est bien envoyée sur le cocycle trivial.

Injectivité Supposons que $c, c' \in C^G$ soient tels que $\delta^0(c) = \delta^0(c')$. Si l'on note α et α' des représentants de leurs classes, il existe $a \in A$ tel que

$$\alpha'_\sigma = a\,\alpha_\sigma\,\sigma\cdot a^{-1}, \quad \forall\sigma \operatorname{im} G,$$

ce qui implique, si b est une préimage de c et b' une préimage de c' :

$$\begin{aligned} & b'^{-1}\,\sigma\cdot b' = f(a)b^{-1}\,\sigma\cdot b\,\sigma\cdot f(a)^{-1} \\ \Leftrightarrow\quad & b\,f(a)^{-1}b'^{-1} = \sigma\cdot\big(b\,f(a)^{-1}\,b'^{-1}\big). \end{aligned}$$

Ainsi, $d := b\,f(a)^{-1}\,b'^{-1} \in B^G$. On constate alors que $c = d\cdot c'$ et l'application φ est bien injective.

Surjectivité Evidente, vu la définition de φ.

□

Remarque 2.3.8
On a l'impression que la définition de cette action pourrait être simplifiée en posant : $b\cdot c = g(b)c$. L'intérêt de la version ci-dessus est que la proposition reste vraie sous les hypothèses plus faibles de la remarque 2.3.4.

2.4 Limite inductive

Dans cette section, nous allons présenter le concept de *limite directe* qui est une construction duale à celle des limites projectives.

Définition 2.4.1 (Système inductif)
Soient I un ensemble ordonné filtrant. Un système inductif *sur I est la donnée d'une famille d'objets $(X_i)_{i\in I}$ d'une catégorie $\mathscr{C}$ et, pour chaque couple $(i,j) \in I^2$ tel que $i \leq j$, d'un morphisme $\varphi_{ij} : X_i \longrightarrow X_j$. Ces morphismes doivent vérifier les propriétés suivantes :*

(i) $\varphi_{ii} = \mathrm{id}_{X_i}$ *pour tout* $i \in I$;

(ii) pour tous $i,j,k \in I$ *tels que* $i \leq j \leq k$, $\varphi_{jk}\varphi_{ij} = \varphi_{ik}$.

Un tel système est noté (X_i, φ_{ij}).

Définition 2.4.2 (Morphismes compatibles)
Soit (X_i, φ_{ij}) un système inductif dans une catégorie $\mathscr{C}$, $X \in |\mathscr{C}|$ et une famille de morphismes $\varphi_i : X_i \longrightarrow X$. La famille $(\varphi_i)_{i\in I}$ est dite compatible *avec le système (X_i, φ_{ij}) si pour tous $i,j \in I$ avec $i \leq j$, on a $\varphi_j\varphi_{ij} = \varphi_i$.*

Définition 2.4.3 (Limite inductive)
Soit (X_i, φ_{ij}) un système inductif dans une catégorie $\mathscr{C}$. Une limite inductive *(X, φ_i) du système est la donnée d'un couple (X, φ_i), où $X \in |\mathscr{C}|$ et les φ_i forment une famille de morphismes compatibles. Ce couple doit satisfaire la condition suivante : si $\psi_i : X_i \longrightarrow Y$ est une autre famille de morphismes compatibles, alors il existe un unique morphisme $\psi : X \longrightarrow Y$ tel que le diagramme suivant commute pour tous $i \leq j$:*

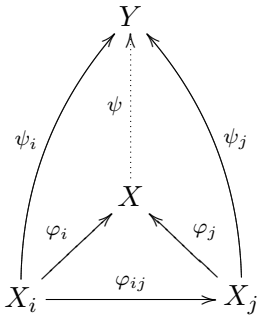


Diagramme 2.2: Limite inductive

La limite inductive, si elle existe, est notée $\varinjlim_{i\in I} X_i$.

Remarque 2.4.4
On procède comme dans le cas de la limite projective pour montrer l'unicité, à isomorphisme près, de la limite inductive.

2.4.1 Description de la limite inductive dans le cas de groupes

Soit (G_i, φ_{ij}) un système inductif de groupes et considérons l'union disjointe

$$G' = \coprod_{i\in I} G_i.$$

On définit alors une relation $\sim$ sur G' de la manière suivante : si $x \in G_i$ et $y \in G_j$, alors

$$x \sim y \Leftrightarrow \exists k \in I, \varphi_{ik}(x) = \varphi_{jk}(y).$$

Le fait que I soit un ensemble filtrant implique que $\sim$ est une relation d'équivalence et l'on écrit $G = G'/_{\sim}$. Il faut vérifier que l'on puisse mettre une structure de groupe sur G et qu'il s'agit bien de la limite inductive du système.

Structure de groupe et morphismes compatibles

Soient $[g], [h] \in G$ ainsi que $g \in G_i$, $h \in G_j$ des représentants de ces classes. Puisque I est un ensemble filtrant, il existe k tel que $i, j \leq k$. On pose alors

$$[g][h] = \left[\varphi_{ik}(g)\varphi_{jk}(h)\right]$$

et on vérifie que c'est bien défini (cela ne dépend pas des représentants choisis ni de l'indice k). On définit pour chaque $i \in I$ l'application $\varphi_i : G_i \longrightarrow G$ qui envoie g sur $[g]$, qui est un homomorphisme de groupes. Si $g \in G_i$ et $i, j \in I$ sont tels que $i \leq j$, alors $g \sim \varphi_{ij}(g)$, et donc $\varphi_i(g) = \varphi_j\varphi_{ij}(g)$, ce qui implique qu'il s'agit de morphismes compatibles.

Universalité

Soit H un groupe et $\psi_i : G_i \longrightarrow H$ une collection de morphismes compatibles. On aimerait définir un homomorphisme de groupes $\psi : G \longrightarrow H$. Pour cela, soit $[g] \in G$ et supposons que $g \in G_k$. On pose alors

$$\psi([g]) = \psi_k(g).$$

Il faut vérifier que cette application est bien définie. Soit donc $h \in G_l$ tel que $g \sim h$. Puisque les ψ_i sont des morphismes compatibles et que $g \sim h$, il existe $m \in I$ tel que $\varphi_{lm}(h) = \varphi_{km}(g)$ et tel que le diagramme suivant commute

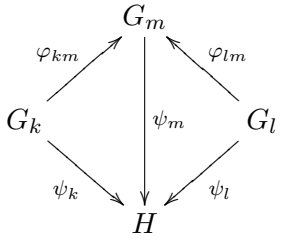


Diagramme 2.3: Universalité de la limite inductive de groupes

Ainsi, on a

$$\psi_l(h) = \psi_m\varphi_{lm}(h) = \psi_m\varphi_{km}(g) = \psi_k(g),$$

ce qui implique que l'application ψ est bien définie. Une telle application doit satisfaire $\psi\varphi_i = \psi_i$; son comportement est ainsi entièrement déterminé par les φ_i et les ψ_i, ce qui entraîne l'unicité.

Remarque 2.4.5
Dans le cas où les G_i sont juste des ensembles pointés, la limite est un ensemble pointé de point de base $[x_0]$, où x_0 est le point de base de n'importe quel élément de la limite.

Exemple 2.4.6
Soit G un groupe et supposons que $G = \bigcup_{i\in I} G_i$. Alors

$$G = \varinjlim_{i\in I} G_i,$$

où chaque G_i est un sous-groupe de G. On muni l'ensemble des G_i de l'ordre lié à l'inclusion et les φ_{ij} sont les inclusions. De même, les morphismes compatibles $\varphi_i : G_i \longrightarrow G$ sont des inclusions. Si (H, ψ_i) est un autre groupe et sa collection de morphismes, compatibles, on définit $\psi : G \longrightarrow H$ de la manière suivante : pour $g \in G$, il existe $j \in I$ tel que $g \in G_j$ et l'on a

$$\psi(g) := \psi_i(g).$$

On a alors clairement, pour tout $i \in I$ que $\psi\varphi_i = \psi_i$ et cette condition détermine de manière unique tout morphisme de groupes entre G et H.

2.5 Théorème 90 de Hilbert

Dans toute cette section K désigne un corps et Ω une extension galoisienne de K.

Le théorème 90 de Hilbert est un énoncé que l'on trouve sous des formes diverses. La version la plus simple concerne les extensions galoisiennes cycliques (dont le groupes de Galois est cyclique). Une deuxième version de cet énoncé est la suivante : si Ω est une extension galoisienne d'un corps K, alors

$$H^1\big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,,\Omega^*\big)=\{1\}.$$

L'énoncé qui est présenté ici est la généralisation suivante :

$$H^1\big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,,\mathrm{GL}_n(\Omega)\big)=\{1\}$$

(il s'agit d'une généralisation car Ω^* est identifiable à $\mathrm{GL}_1(\Omega)$).

Théorème 2.5.1 (Hilbert 90 (cas fini))
Soit Ω/K est une extension galoisienne finie. Alors $H^1\big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,,\mathrm{GL}_n(\Omega)\big)=\{1\}$.

Démonstration. Voir [Ber10]. □

Avant de montrer le théorème Hilbert 90 pour le cas infini, nous avons besoin d'introduire quelques outils.

2.5.1 Extension des scalaires

Dans le cas des matrices, on considère pour chaque extension E d'un corps K l'ensemble des matrices $\mathrm{M}_n(E)$. On peut généraliser cela avec la définition suivante.

Définition-Notation 2.5.2
On note **Field** : K *la catégorie constituée de toutes les extensions de corps de K.*

Définition 2.5.3 (Foncteur d'extension des scalaires)
Un foncteur d'extension des scalaires *est un foncteur de* **Field** : K *dans une autre catégorie.*

Exemple 2.5.4
L'application qui assigne à chaque extension E de K l'ensemble des matrices $\mathrm{M}_n(E)$ est un foncteur de la catégorie **Field** : K dans **Rng** (un morphisme $\sigma : E \longrightarrow E'$ entre deux corps est appliqué composante par compostante à la matrice).

Remarque 2.5.5
Si Φ : **Field** : $\Omega/K \longrightarrow$ **Grp** est un foncteur, alors pour toute extension galoisienne intermédiaire F, $\mathcal{G}\mathrm{al}\,(F,K)$ agit naturellement sur $\Phi(F)$:

$$\sigma\cdot x=\Phi\big(\sigma\big)(x),\quad \forall\sigma\in\mathcal{G}\mathrm{al}\,(F,K)\,,\forall x\in\Phi(F).$$

Convention 2.5.6
Dans ce qui suit, un foncteur Φ en groupe pour l'extension Ω/K *désigne un foncteur* Φ : **Field** : $\Omega/K \longrightarrow$ **Grp** *dont les corps de la catégorie de départ sont les sous-corps de Ω contenant K. On suppose de plus qu'il possède les propriétés suivantes :*

(*i*) *L'action de $\mathcal{G}\mathrm{al}\,(\Omega,K)$ sur $\Phi(\Omega)$ est continue.*

(*ii*) *Pour toute extension galoisienne intermédiaire finie F, $\Phi(F)\cong\Phi(\Omega)^{\mathcal{G}\mathrm{al}(\Omega,F)}$.*

(*iii*) *Si $K\subset E\subset F\subset\Omega$ sont deux extensions intermédiaires et si $i_F^E : E\longrightarrow F$ est l'inclusion, alors l'application $\Phi(i_F^E)$ est injective.*

2.5.2 Théorème 90 de Hilbert (cas général)

Dans un premier temps, on aimerait montrer la proposition suivante :

Proposition 2.5.7
Soit Φ un foncteur en groupe pour Ω/K. Alors

$$H^1\big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,,\Phi(\Omega)\big)\cong\varinjlim_{F}H^1\big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(F)\big),$$

où F parcourt l'ensemble des extensions galoisiennes intermédiaires.

On va réaliser cela en plusieurs étapes.

Proposition 2.5.8
Si $\mathcal{F}$ désigne l'ensemble des extensions galoisiennes finis de K contenue dans Ω, alors

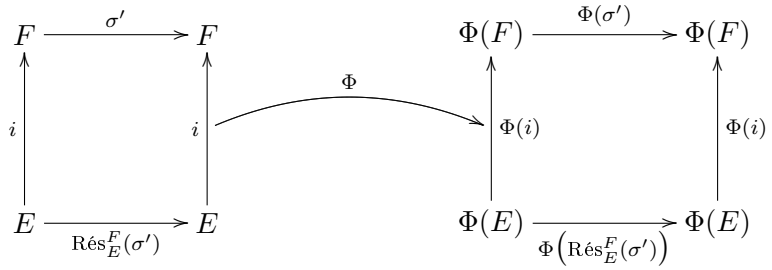
$$\big\{H^1\big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(F)\big):F\in\mathcal{F}\big\}$$

est un système inductif.

Démonstration. Soient $K\subset E\subset F\subset\Omega$ deux extensions galoisiennes intermédiaires (on ne suppose pas qu'elles sont finies et on n'exclut pas $F=\Omega$). Puisque les extensions considérées sont normales, on peut définir de matière naturelle des homomorphismes de restriction :

$$\begin{array}{rcl}\mathrm{Rés}^F_E:\mathcal{G}\mathrm{al}\,(F,K) & \longrightarrow & \mathcal{G}\mathrm{al}\,(E,K)\\ \sigma & \longmapsto & \sigma\big|_E.\end{array}$$

Le but est de définir un morphisme d'ensembles pointés entre $H^1\big(\mathcal{G}\mathrm{al}\,(E,K)\,,\Phi(F)\big)$ et $H^1\big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(F)\big)$. Pour cela, on va utiliser la proposition 2.3.2 : l'un des morphisme sera le morphisme de restriction et l'autre sera l'image par Φ du morphisme d'inclusion $i:E\hookrightarrow F$. Il est nécessaire de vérifier que ces deux morphismes sont compatibles. Pour cela, on considère le carré commutatif de gauche, qui est envoyé sur un carré commutatif par Φ :



On constate que le fait que le carré de droite commute est équivalent à la condition de compatibilité. Ainsi, le morphisme $\Phi(i):\Phi(E)\longrightarrow\Phi(F)$ se prolonge en un morphisme d'ensembles pointés $\varphi_{EF}:H^1\big(\mathcal{G}\mathrm{al}\,(E,K)\,,\Phi(E)\big)\longrightarrow H^1\big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(F)\big)$. On aimerait expliciter ce que fait cette application induite. Pour cela, on identifie nos morphismes avec ceux de la proposition 2.3.2 et l'on constate que la classe d'un cocycle $\alpha:\mathcal{G}\mathrm{al}\,(E,K)\longrightarrow\Phi(E)$ est envoyé sur la classe $[\beta]$ où $\beta:\mathcal{G}\mathrm{al}\,(F,K)\longrightarrow\Phi(F)$ est tel que

$$\beta_{\sigma'}=\Phi(i)\big(\alpha_{\mathrm{Rés}^F_E(\sigma')}\big),\quad\forall\sigma'\in\mathcal{G}\mathrm{al}\,(F,K)\,.$$

Un calcul direct permet de vérifier que si $K \subset D \subset E \subset F \subset \Omega$ sont des extensions galoisiennes intermédiaires, alors

$$\big(\varphi_{EF}\,\varphi_{DE}([\alpha])\big)(\sigma) = \varphi_{DF}\big([\alpha]\big)(\sigma),\ \forall \alpha \in Z^1(\mathcal{G}\mathrm{al}\,(D,K)\,,\Phi(D)), \forall \sigma \in \mathcal{G}\mathrm{al}\,(F,K)\,.$$

Ainsi, on peut considérer le système inductif $\big(H^1\big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(F)\big),\varphi_{EF}\big)$ et sa limite. □

Lemme 2.5.9
Soit $\alpha \in Z^1(G,A)$. Alors, il existe un sous-groupe normal ouvert N de G et une application $\bar{\alpha} : G/_N \longrightarrow A$ tel que $\alpha = \bar{\alpha}\pi$, où π est l'application de passage au quotient.

Démonstration. Soit $a \in A$ l'image de 1 par α. Puisque A est muni de la topologie discrète, l'ensemble $I = \alpha^{-1}(\{1\})$ est un ouvert fermé contenant 1. En procédant comme dans la démonstration du théorème 1.2.7, on peut trouver un sous-groupe normal ouvert N de G tel que α est constante sur les classes à gauche de N (on utilise le fait que α est un cocycle). Ainsi, on peut définir une application $\bar{\alpha} : G/_N \longrightarrow A$ avec les propriétés voulues. □

Proposition 2.5.10
On a une bijection

$$Z^1(G,A) \cong \varinjlim Z^1\big(G/_N, A^N\big),$$

où N parcourt les sous-groupes normaux ouverts de G.

Démonstration. Il est facile de montrer que l'action de G sur A se restreint en une action continue de $G/_N$ sur A^N pour tout sous-groupe normal N de G et que l'on est en présence d'un système projectif $\big(G/_N, \varphi_N\big)$, où N parcourt l'ensemble des sous-groupes normaux ouverts de G. De plus, en exhibant des morphismes compatibles $\psi_N : Z^1\big(G/_N, A^N\big) \longrightarrow Z^1(G,A)$, on obtient un morphisme $\psi : \varinjlim Z^1\big(G/_N, A^N\big) \longrightarrow Z^1(G,A)$.

Injectivité de ψ On montre sans difficulté que les applications ψ_N sont injectives et que cela entraîne l'injectivité de ψ.

Surjectivité de ψ Soit $\alpha \in Z^1(G,A)$ un cocycle et $\bar{\alpha}$ ainsi que $N_1 \trianglelefteq_o G$ comme dans le lemme ci-dessus. Remarquons que puisque α est continue, que G est profini et que A est muni de la topologie discrète, il existe un $N_2 \trianglelefteq_o G$ tel que $\mathrm{im}\,\alpha \subset A^{N_2}$. En effet, les hypothèses implique que l'image de α est finie, disons $\mathrm{im}\,\alpha = \{a_1, \ldots, a_n\}$. Puisque l'action de G sur A est continue, les stabilisateurs $S_{a_1}, \ldots, S_{a_n}$ sont ouverts dans G (et donc fermés). Ainsi, $I = \bigcap_{i=1}^n S_{a_i}$ est un ouvert fermé contenant 1, ce qui implique l'existence de $N_2 \trianglelefteq_o G$ avec $N_2 \subset I$ et $\mathrm{im}\,\alpha \subset A^{N_2}$. On pose $N = N_1 \cap N_2$, qui est un sous-groupe normal ouvert de G, et on définit une application (un coycle, en fait) $\beta : G/_N \longrightarrow A$, qui est telle que $\beta\pi = \alpha$ (si π est l'application de passage au quotient) et $\mathrm{im}\,\beta \subset A^N$. On constate alors que $\psi_N(\beta) = \alpha$, c'est-à-dire $\psi([\beta]) = \alpha$.

□

Le schéma de la preuve précédente provient de la section *Profinite groups* du livre [CF].

Proposition 2.5.11
On a une bijection

$$H^1(G,A) \cong \varinjlim H^1\big(G/_N, A^N\big),$$

où N parcourt les sous-groupes normaux ouverts de G.

Démonstration. De la même manière que ci-dessus, on obtient un morphisme induit $\bar{\psi} : \varinjlim H^1\big(G/_N, A^N\big) \longrightarrow H^1(G,A)$.

Surjectivité La surjectivité de $\bar{\psi}$ provient de celle du morphisme ψ de la proposition ci-dessus.

Injectivité Pour montrer l'injectivité du morphisme $\bar{\psi}$, il suffit de montrer celle des morphismes $\bar{\psi}_N : H^1\big(G/_N, A^N\big) \longrightarrow H^1(G,A)$. Supposons que $[\alpha], [\alpha']$ soient des classes telles que $\bar{\psi}_N([\alpha]) = \bar{\psi}_N([\alpha'])$. Ainsi, il existe $a \in A$ tel que

$$\alpha'_{\pi(\sigma)} = a\,\alpha_{\pi(\sigma)}\,\sigma \cdot a^{-1}, \quad \forall \sigma \in G.$$

Puisque $\beta_1 = 1$ pour tout cocycle β, on a, pour $\tau \in N$

$$\alpha'_{\overline{1}} = a\,\alpha_{\overline{1}}\,\tau \cdot a^{-1} \Leftrightarrow a = \tau a,$$

c'est-à-dire $a \in A^N$, et donc $[\alpha] = [\alpha']$.

□

On peut maintenant montrer la proposition 2.5.7.

Preuve de la proposition 2.5.7. Maintenant que les différents points ont été mis en place, la preuve se fait de manière facile :

$$\begin{aligned}
\varinjlim_F H^1\big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(F)\big) &\underset{(i)}{\cong} \varinjlim_F H^1\Big(\mathcal{G}\mathrm{al}\,(F,K)\,,\Phi(\Omega)^{\mathcal{G}\mathrm{al}(\Omega,F)}\Big)\\
&\underset{(ii)}{\cong} \varinjlim_F H^1\Big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,/_{\mathcal{G}\mathrm{al}\,(\Omega,F)},\Phi(\Omega)^{\mathcal{G}\mathrm{al}(\Omega,F)}\Big)\\
&\underset{(iii)}{\cong} H^1\big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,,\Phi(\Omega)\big).
\end{aligned}$$

Les isomorphismes se justifient de la manière suivante :

(i) Hypothèse sur le foncteur en groupe (voir convention 2.5.6).

(ii) Point (iv) du théorème 1.4.3.

(iii) Provient de la proposition précédente et du fait que lorsque F parcourt l'ensemble des extensions galoisiennes finies intermédiaires, $\mathcal{G}\mathrm{al}\,(\Omega,F)$ parcourt l'ensemble des sous-groupes normaux ouverts de $\mathcal{G}\mathrm{al}\,(\Omega,K)$.

□

Théorème 2.5.12 (Théorème 90 de Hilbert (cas général))
Soit Ω/K est une extension galoisienne. Alors $H^1\big(\mathcal{G}\mathrm{al}\,(\Omega,K)\,,\mathrm{GL}_n(\Omega)\big) = \{1\}$.

Démonstration. Pour commencer, remarquons que le foncteur qui associe à chaque extension intermédiaire F le groupe $\mathrm{GL}_n(F)$ satisfait les hypothèses de la convention 2.5.6 : les points (ii) et (iii) sont clair. En ce qui concerne la continuité de l'action de groupe, remarquons que puisqu'elle est définie de la manière suivante

$$\begin{aligned}
\mathcal{G}\mathrm{al}\,(\Omega,K) \times G(\Omega) &\longrightarrow G(\Omega),\\
(\sigma,R) &\longmapsto \sigma R, \quad (\sigma R)_{ij} = \sigma(R_{ij}),
\end{aligned}$$

le stabilisateur S_M d'un élément $M \in G(\Omega)$ contient $\mathcal{G}\mathrm{al}\,(\Omega, F)$, où F est une extension galoisienne finie intermédiaire telle que $M \in \mathrm{M}_n(F)$, et donc est ouvert (point (v) de la proposition 1.1.15). Ainsi, la proposition 2.5.7 et le théorème 90 de Hilbert du cas fini nous donnent

$$H^1\big(\mathcal{G}\mathrm{al}\,(\Omega, K)\,, \mathrm{GL}_n(\Omega)\big) = \varinjlim H^1\big(\mathcal{G}\mathrm{al}\,(F, K)\,, \mathrm{GL}_n(F)\big) = \varinjlim\{1\} = \{1\}.$$

□

Corollaire 2.5.13
Soit Ω/K est une extension galoisienne. Alors $H^1\big(\mathcal{G}\mathrm{al}\,(\Omega, K)\,, \mathrm{SL}_n(\Omega)\big) = 1$.

Démonstration. On considère la suite exacte suivante :

$$1 \longrightarrow \mathrm{SL}_n(\Omega) \xhookrightarrow{i} \mathrm{GL}_n(\Omega) \xrightarrow{\det} \Omega^* \longrightarrow 1.$$

La section 2.3.1, implique l'existence d'un morphisme δ tel que la suite suivante soit exacte :

$$\mathrm{GL}_n(\Omega)^G \xrightarrow{\det_*} (\Omega^*)^G \xrightarrow{\delta^0} H^1\big(G, \mathrm{SL}_n(\Omega)\big) \xrightarrow{i_*} H^1\big(G, \mathrm{GL}_n(\Omega)\big),$$

où $G = \mathcal{G}\mathrm{al}\,(\Omega, K)$. Ainsi, on a

$$\mathrm{GL}_n(K) \xrightarrow{\det_*} K^* \xrightarrow{\delta^0} H^1\big(G, \mathrm{SL}_n(\Omega)\big) \xrightarrow{i_*} 1,$$

ce qui implique que $H^1\big(G, \mathrm{SL}_n(\Omega)\big) = \{1\}$, puisque le morphisme δ^0 est surjectif et que $\ker \delta^0 = \operatorname{im} \det_* = K^*$. □

2.6 Problème de descente galoisienne pour les matrices

On rappelle l'énoncé du problème :

Problème 2.6.1 (Problème de descente galoisienne pour les matrices)
Soit K un corps, Ω une extension galoisienne de K et $M_0, M \in \mathrm{M}_n(K)$. S'il existe $Q \in G(\Omega)$ (on rappelle que $G(\Omega)$ désigne aussi bien $\mathrm{GL}_n(\Omega)$ que $\mathrm{SL}_n(\Omega)$) telle que $M_0 = QMQ^{-1}$, existe-t-il $P \in G(K)$ telle que $M_0 = PMP^{-1}$.

Dans cette section K, Ω, M, M_0, P et Q sont comme dans l'énoncé ci-dessus et $G = \mathcal{G}\mathrm{al}\,(\Omega, K)$.
Pour la suite, on considère l'action, continue, de $\mathcal{G}\mathrm{al}\,(\Omega, K)$ sur $G(\Omega)$ comme dans le théorème ci-dessus :

$$\begin{array}{rcl} \mathcal{G}\mathrm{al}\,(\Omega, K) \times G(\Omega) & \longrightarrow & G(\Omega), \\ (\sigma, R) & \longmapsto & \sigma R, \quad (\sigma R)_{ij} = \sigma(R_{ij}). \end{array}$$

Pour commencer, remarquons que pour tout élément $\sigma \in G$, on a $Q(\sigma Q)^{-1} \in \mathrm{Z}_G(M_0)(\Omega)$, l'ensemble des matrices des $G(\Omega)$ commutant avec M_0. Ainsi, on peut définir une application

$$\begin{array}{rcl} \alpha^Q : G & \longrightarrow & \mathrm{Z}_G(M_0)(\Omega) \\ \sigma & \longmapsto & \alpha^Q_\sigma = Q(\sigma Q)^{-1}, \end{array}$$

et l'on remarque que cette application est un cocycle. Une question que l'on peut se poser est l'importance du choix de Q parmi les matrices qui conjuguent M à M_0. Si $R \in G(\Omega)$ est une autre matrice telle que $M_0 = RMR^{-1}$, on vérifie que la magie opère et que

$$\alpha^R_\sigma = \left(RQ^{-1}\right) \alpha^Q_\sigma \, \sigma \cdot \left(RQ^{-1}\right)^{-1},$$

ce qui correspond à deux cocycles cohomologues, car $RQ^{-1} \in \mathrm{Z}_G(M_0)(\Omega)$. On aimerait maintenant exprimer une condition sur ces coycles pour que la matrice M_0 soit conjuguée à M sur $G(K)$. Cette condition est la suivante :

$$\exists P \in G(K), M_0 = PMP^{-1} \Leftrightarrow \exists C \in \mathrm{Z}_G(M_0)(\Omega), \alpha^Q = \alpha^C.$$

En effet, supposons qu'un tel P existe. On a alors :

$$QP^{-1}M_0 = QMP^{-1} = M_0QP^{-1},$$

ce qui implique l'existence de $C \in \mathrm{Z}_G(M_0)(\Omega)$ tel que $Q = CP$ et l'on vérifie que $\alpha^Q = \alpha^C$. Réciproquement, si un tel C existe, alors $C^{-1}Q \in G(K)$ et remplit le rôle de P. Ce que l'on a vu nous permet d'affirmer :

Proposition 2.6.2
L'ensemble des classes de $G(K)$-conjugaison de matrices $M \in \mathrm{M}_n(K)$ qui sont conjuguées à M_0 par un élément de $G(\Omega)$ est en bijection avec l'ensemble des classes de cocycles $[\alpha] \in H^1\big(G, \mathrm{Z}_G(M_0)(\Omega)\big)$ telles que $\alpha = \alpha^Q$ pour un élément $Q \in G(\Omega)$.

Démonstration. Soit $[\alpha]$ une classe de cocycles telle que $\alpha = \alpha^Q$, pour un élément Q de $G(\Omega)$. On associe à cette classe la matrice $M_\alpha = Q^{-1}M_0Q$ et on vérifie que $M_\alpha \in \mathrm{M}_n(K)$ (penser à multiplier par $Q^{-1}Q$). On remarque que la classe $[\alpha]$ ne détermine pas une seule matrice : si $\alpha' = \alpha^{Q'} \sim \alpha = \alpha^Q$, on obtient une matrice

$M_{\alpha'}$, qui est telle que $PM_{\alpha'}P^{-1} = M_\alpha$ pour $P = Q^{-1}C^{-1}Q' \in G(K)$, où C est l'élément rendant les cocycles cohomologues.

Réciproquement, soient $M \in \mathrm{M}_n(K)$ et $Q \in G(\Omega)$ des matrices telles que $M_0 = QMQ^{-1}$. On associe à M la classe du cocycle $[\alpha^Q]$. Il a été montré ci-dessus que cette application est bien définie : si Q' est un autre élément de $G(\Omega)$ conjuguant nos matrices, alors $\alpha^Q \sim \alpha^{Q'}$. Si, maintenant, M' est une autre matrice de la classe, c'est-à-dire $M' = PMP^{-1}$, pour $P \in G(K)$, on a

$$M_0 = QMQ^{-1} = QP^{-1}M'PQ^{-1}$$

et on constate que $\alpha^{QP^{-1}} = \alpha^Q$, ce qui implique que deux matrices de la même classes de $G(K)$-conjugaison sont envoyées sur la même classe de cohomologie. Avec cela, on constate que ces associations sont bijectives. □

Corollaire 2.6.3
L'inclusion $f : \mathrm{Z}_G(M_0)(\Omega) \longrightarrow G(\Omega)$ induit une application

$$f_* : H^1\big(G, \mathrm{Z}_G(M_0)(\Omega)\big) \longrightarrow H^1\big(G, G(\Omega)\big).$$

Alors, l'ensemble des classes de cocycles $[\alpha]$ de $H^1\big(G, \mathrm{Z}_G(M_0)(\Omega)\big)$ qui peuvent s'écrire $\alpha \sim \alpha^Q$ pour un $Q \in G(\Omega)$ est le noyau de f_*.

Démonstration. Le fait qu'un cocycle soit cohomologue au cocycle trivial par un élément de $G(\Omega)$ est exactement la condition voulue. □

La bijection entre l'ensemble des classes de conjugaison et le noyau de l'application f_* peut être prouvée en utilisant les outils de cohomologie mis au point plus haut. Pour cela, on définit l'action de groupe

$$\begin{array}{rcl} G(\Omega) \times \mathrm{M}_n(\Omega) & \longrightarrow & \mathrm{M}_n(\Omega) \\ (Q, M) & \longmapsto & Q \star M = QMQ^{-1}, \end{array}$$

et l'on constate que

$$S_{M_0} = \{Q \in G(\Omega) : QM_0Q^{-1} = M_0\} = \mathrm{Z}_G(M_0)(\Omega).$$

Puisque l'on a $G(\Omega)/\mathrm{Z}_G(M_0)(\Omega) = G(\Omega)/S_{M_0} \cong G(\Omega) \star M_0$, on a une suite exacte

$$1 \longrightarrow \mathrm{Z}_G(M_0)(\Omega) \hookrightarrow G(\Omega) \longrightarrow G(\Omega) \star M_0 \longrightarrow 1$$

et la proposition 2.3.7 implique qu'il existe une bijection entre le noyau de l'application $f_* : H^1\big(G, \mathrm{Z}_G(M_0)(\Omega)\big) \longrightarrow H^1\big(G, G(\Omega)\big)$ et l'ensemble des orbites de l'action de B^G sur C^G. On constate alors que B^G est $G(K)$ et que C^G est l'ensemble des matrices de $\mathrm{M}_n(K)$ qui sont conjuguées à M_0 par un élément de $G(\Omega)$.

Ce que nous avons vu ci-dessus et le fait que $H^1\big(G, G(\Omega)\big)$ est trivial (voir théorème 90 de Hilbert et son corollaire) impliquent que l'on a une bijection entre l'ensemble des classes de $G(K)$-conjugaison de matrices $M \in \mathrm{M}_n(K)$ qui sont conjuguées à M_0 par un élément de $G(\Omega)$ et $H^1\big(G, \mathrm{Z}_G(M_0)(\Omega)\big)$.

2.7 Perspective

Dans ce que l'on a fait plus haut, les concepts mis en place semblent un peu disproportionnés par rapport aux résultats obtenus. L'intérêt de ce formalisme est la généralisation à des problèmes plus conceptuels qui ressemblent à celui des matrices. Il s'agit de structures mathématiques que l'on peut associer à une série d'extensions de corps via un foncteur d'extension des scalaires (par exemple les K-algèbres). On remplace alors la relation de conjuguaison sur K par le fait d'appartenir à une même orbite pour une bonne action de groupe (dans le cas des algèbres, il s'agit de l'isomorphisme sur K, et la question est de savoir quand deux K-algèbres isomorphes sur Ω le sont sur K). Sous certaines hypothèses on retrouve alors un résultat semblable : pour un objet a défini sur le corps de base K, l'ensemble des K-classes d'équivalence d'objets définis sur K qui sont équivalents à a sur Ω est en bijection avec le noyau d'une application entre deux ensembles de cohomologie. Cette généralisation est disponible dans les notes de cours de Grégory Berhuy (voir [Ber10]).

Table des notations

A^G	Ensembles des éléments de A fixés par G
$E \vee F$	Plus petit corps contenant E et F (quand cela a un sens)
F/K	F est une extension du corps K
Field : K	Catégorie des extensions de corps de K
Field : Ω/K	Catégorie des extensions de corps de K contenues dans Ω
$H \leq G$	H est un sous-groupe de G
$H \leq_c G$	H est un sous-groupe fermé de G
$H \trianglelefteq G$	H est un sous-groupe normal de G
$H \trianglelefteq_f G$	H est un sous-groupe normal d'indice fini de G
$H \trianglelefteq_o G$	H est un sous-groupe normal ouvert de G
$\mathbb{F}_n$	Corps fini à n éléments
$\mathcal{G}\mathrm{al}\,(F, K)$	Groupe de Galois de F sur K
Grp	Catégorie des groupes
I_n	Matrice identité de taille $n \times n$
$\mathrm{M}_n(A)$	Matrices $n \times n$ à coefficient dans l'anneau A
$\mathbb{N}$	Ensemble des entiers positifs (sans le 0)
$\mathbb{N}_0$	Ensemble des entiers positifs (avec le 0)
$\mathbb{P}$	Ensemble des nombres premiers
Rng	Catégorie des anneaux
$\mathbb{Z}$	Anneau des entiers relatifs
$Z^1(G, A)$	Ensemble des cocycles de G à valeurs dans A
ζ_n	Racine primitive n-ème de l'unité

Bibliographie

[Ber10] Grégory Berhuy, *An introduction to galois cohomology and its applications*, Disponible à l'adresse `http://www-fourier.ujf-grenoble.fr/~berhuy/`, 2010.

[Bor94] Francis Borceux, *Handbook of categorical algebra*, Cambridge University Press, 1994.

[Bou07] Nicolas Bourbaki, *Topologie générale*, Springer, 2007.

[CF] JWS Cassels and A. Fröhlich, *Algebraic number theory*, Proceedings of an Instructional Conference organized by the London Mathematical Society (A Nato Advanced Study Institute) with Support of the International Mathematical Union.

[Chi08] L. Childs, *A concrete introduction to higher algebra*, Springer Verlag, 2008.

[Gau86] C. F. Gauss, *Disquisitiones Arithmeticae, 1801. English translation by Arthur A. Clarke*, Springer-Verlag, New York, 1986.

[Gir71] J. Giraud, *Cohomologie non abélienne*, Springer, 1971.

[Lan02] S. Lang, *Algebra, volume 211 of Graduate Texts in Mathematics*, Springer-Verlag, New York, 2002.

[Lub07] Alexander Lubotzky, *Book reviews - profinite groups*, Disponible à l'adresse `http://www.ams.org/bull/2001-38-04/S0273-0979-01-00914-4/S0273-0979-01-00914-4.pdf`, 2007, pp. 475–479.

[ML98] S. Mac Lane, *Categories for the working mathematician*, Springer verlag, 1998.

[Oss07] Brian Osserman, *Inverse limits and profinite groups*, Disponible à l'adresse `http://www.math.ucdavis.edu/~osserman/classes/250C/`, 2007.

[Rib70] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's University, 1970.

[RZ00] L. Ribes and P. Zalesskii, *Profinite groups*, Profinite Groups (2000).

[Ser94] J.P. Serre, *Cohomologie galoisienne*, Springer, 1994.

[Wil98] J.S. Wilson, *Profinite groups*, Oxford University Press, USA, 1998.