Groupes profinis et théorèmes de Sylow

Étienne AFFALOU
École Normale Supérieure de Rennes

Stage réalisé sous la direction de Benoit LOISEL
Laboratoire de Mathématiques et Applications de Poitiers

Mai-Juin 2024

Table des matières

Résumé

Dans la première partie, l'objectif est de définir les groupes profinis en tant que limite projective de groupes finis comme présentés dans [RZ10], et d'établir l'équivalence avec les groupes compacts totalement discontinus en s'appuyant sur la preuve donnée au début de [Ser94]. La deuxième partie développe une généralisation des théorèmes de Sylow au cas des groupes profinis. On se place dans le cadre des nombres surnaturels pour définir l'ordre des groupes profinis ainsi que l'indice d'un sous-groupe fermé d'un groupe profini. Enfin, la troisième et dernière partie comporte des exemples approfondis de groupes profinis et des applications des théorèmes de Sylow à des cas non-triviaux.

Remerciements

Je tiens à remercier toute l'équipe du laboratoire de mathématiques et applications de Poitiers pour leur accueil et pour m'avoir fait découvrir la vie dans un laboratoire de recherche mathématique. Je remercie particulièrement Benoit Loisel pour sa bienveillance, pour son aide pour la compréhension des concepts et pour m'avoir éclairé sur les exemples concrets. Merci également aux doctorants de m'avoir accueilli au dernier séminaire des doctorants au cours duquel j'ai pu découvrir des sujets de recherche concrets.

Introduction

Les groupes profinis apparaissent dans de nombreuses branches des mathématiques. Étant donné un groupe compact G, sa composante neutre G^0 (la composante connexe de l'identité) est un groupe de Lie compact et connexe (on sait classifier les groupes de Lie compacts et connexes). On a de plus une suite exacte

$$1 \longrightarrow G^0 \longrightarrow G \longrightarrow G/G^0 \longrightarrow 1.$$

On remarque que G/G^0 est compact et totalement discontinu, c'est-à-dire profini. Les groupes profinis se manifestent ainsi naturellement dans l'étude des groupes compacts. En théorie de Galois, si K est un corps et L/K est une extension galoisienne, alors le groupe de Galois $\mathrm{Gal}(L/K)$ est profini comme limite projective des groupes $\mathrm{Gal}(L_i/K)$ pour L_i/K une extension galoisienne finie avec $L_i \subset L$. On retrouve également les groupes profinis en théorie des nombres et en théorie de Lie p-adique.

Pour définir les groupes profinis, on commence par faire des rappels de topologie générale et on introduit la notion de groupe topologique. Les résultats que l'on prouve dans cette partie mettent en lumière les liens entre propriétés algébriques et propriétés topologiques. Après avoir établi l'équivalence avec les groupes compacts et totalement discontinus, on détaille les premiers exemples de groupes profinis commutatifs comme les entiers p-adiques ou la complétion profinie de $\mathbb{Z}$. Pour prouver les théorèmes de Sylow dans le cas profini, on choisit de voir ces théorèmes comme un corollaire du théorème de Hall. Prouver directement les théorèmes de Sylow était également possible, mais le théorème de Hall est plus général et permet notamment d'obtenir un résultat sur les groupes résolubles finis. Pour terminer, on s'intéresse aux groupes $\mathbb{Z}_p^*$ ainsi qu'aux groupes $\mathrm{SL}_2(\mathbb{Z}_p)$ en guise d'application des théorèmes de Sylow.

1 Groupes profinis

1.1 Rappels de topologie

Avant de parler de groupes topologiques, on rappelle quelques notions de topologie générale. On établit au passage des propositions très utiles dans la partie sur les groupes profinis. Sauf mention contraire, ces rappels se trouvent tous dans les trois premiers chapitres de [Bou07].

1.1.1 Connexité

Définition Soit $(X, \mathfrak{T})$ un espace topologique. Soit $A \subset X$.
On dit que l'espace $(X, \mathfrak{T})$ est **connexe** lorsque les seules parties ouvertes et fermées de X sont $\emptyset$ et X.
La partie A est une partie **connexe** de X lorsque A est connexe pour la topologie induite par $\mathfrak{T}$ sur A.

Pour montrer qu'une partie d'un espace topologique est connexe, on utilise en général la caractérisation suivante.

Proposition 1.1.1 Soit $(X, \mathfrak{T})$ un espace topologique. Soit $A \subset X$.
La partie A est connexe si et seulement si l'existence de deux ouverts disjoints U, V de $(X, \mathfrak{T})$ tels que $A \subset U \cup V$ implique $A \subset U$ ou $A \subset V$.

Remarquons que si on suppose que A s'écrit comme la réunion disjointe de deux fermés implique que l'un des deux fermés est vide, alors la condition de la proposition est vérifiée en passant au complémentaire, et donc A est connexe.

Preuve : On a $A \subset U \cup V$ avec U, V deux ouverts disjoints si et seulement si la topologie induite par $\mathfrak{T}$ sur A admet la partition d'ouverts $\{A \cap U, A \cap V\}$ par définition de la topologie induite.
Ainsi, A est connexe si et seulement si $A = A \cap U$ ou $\emptyset = A \cap U$. Si $A = A \cap U$, on a $A \subset U$.
Sinon, $\emptyset = A \cap U$ donc $A = A \cap V$ et finalement $A \subset V$.

Avant de définir les composantes connexes d'un espace topologique, on montre la proposition suivante.

Proposition 1.1.2 Soit $(X, \mathfrak{T})$ un espace topologique.
Soit $(A_i)_{i \in I}$ une famille de parties connexes de $(X, \mathfrak{T})$ telle que $\forall (i, j) \in I^2$, $A_i \cap A_j \neq \emptyset$.
Alors, la réunion des A_i est une partie connexe de $(X, \mathfrak{T})$.

Preuve : Notons A la réunion des A_i. Supposons que $A \subset O_1 \cup O_2$ où O_1 et O_2 sont deux ouverts distincts.
Soit $i \in I$. On remarque que $A_i \subset A \subset O_1 \cup O_2$ donc par connexité de A_i, on a $A_i \subset O_1$ ou $A_i \subset O_2$.
Si $A_i \subset O_1$, comme $\forall j \in I, A_i \cap A_j \neq \emptyset$, on a $\forall j \in I, A_j \cap O_1 \neq \emptyset$ et par connexité des A_j, $A_j \subset O_1$ puis $A \subset O_1$.
Sinon, $A_i \subset O_2$ et on trouve de la même façon que $A \subset O_2$. Ainsi, A est connexe par la proposition 1.1.1.

Définition Soit $(X, \mathfrak{T})$ un espace topologique. Soit $x \in X$.
La **composante connexe** de x est la réunion des connexes X contenant x. On la note C_x.
Par construction et par la proposition 1.1.2, C_x est le plus grand connexe de $(X, \mathfrak{T})$ qui contient x.

En fait, les composantes connexes d'un espace topologique forment une partition de l'ensemble sous-jacent.

Proposition 1.1.3 Soit $(X, \mathfrak{T})$ un espace topologique.
On définit la relation binaire $\mathcal{R}$ sur X définie par $\forall (x, y) \in X^2$, $x \mathcal{R} y$ si et seulement si $C_x = C_y$.
Alors, $\mathcal{R}$ est une relation d'équivalence. En particulier, les composantes connexes forment une partition de X.

Preuve : La relation d'égalité entre parties d'un ensemble est une relation d'équivalence.
Les composantes connexes sont les classes d'équivalence de cette relation car si $x \in X$ et $y \in C_x$, alors comme C_y est le plus grand connexe qui contient y, $C_x \subset C_y$ car C_x est un connexe qui contient y et donc C_y est un connexe qui contient x donc on a aussi $C_y \subset C_x$ et enfin, $x \mathcal{R} y$.

La proposition qui suit donne une autre caractérisation des parties connexes d'un espace topologique.

Proposition 1.1.4 Soit $(X, \mathfrak{T})$ un espace topologique.
L'espace $(X, \mathfrak{T})$ est connexe si et seulement si toute fonction continue de X dans $\{0,1\}$ est constante.

Preuve : L'ensemble $\{0,1\}$ est muni de la topologie discrète.
Si $(X, \mathfrak{T})$ est connexe et si $f : X \to \{0,1\}$ est continue, $\{f^{-1}(\{0\}), f^{-1}(\{1\})\}$ est une partition d'ouverts de $(X, \mathfrak{T})$ donc f est constante par connexité.
Inversement, si toute fonction continue de X dans $\{0,1\}$ est constante, si $\{A, X \setminus A\}$ est une partition d'ouverts de X, la fonction indicatrice de A est continue sur X donc est constante.
Ainsi, $A = X$ ou $A = \emptyset$ et X est connexe.

Proposition 1.1.5 Soit $(X, \mathfrak{T})$ un espace topologique. Soit A une partie connexe de X.
Alors, l'adhérence $\overline{A}$ est connexe.

Preuve : Par la proposition 1.1.4, il suffit de montrer que toute fonction continue de $\overline{A}$ dans $\{0,1\}$ est constante.
Soit $f \in \mathcal{C}^0(\overline{A}, \{0,1\})$. La partie A est connexe et f est continue sur A donc $A \subset f^{-1}(\{0\})$ ou $A \subset f^{-1}(\{1\})$ (proposition 1.1.4). Par connexité de A, $f^{-1}(\{0\})$ est fermé ou $f^{-1}(\{1\})$ est fermé donc $\overline{A} = f^{-1}(\{0\})$ ou $\overline{A} = f^{-1}(\{1\})$. Ainsi, f est constante et $\overline{A}$ est connexe.

Cette proposition permet de montrer que les composantes connexes sont fermées.

Proposition 1.1.6 Soit $(X, \mathfrak{T})$ un espace topologique. Les composantes connexes de X sont fermées.

Preuve : Les composantes connexes sont incluses dans leur adhérence, et leur adhérence est connexe par la proposition 1.1.5. Donc par maximalité des composantes connexes, les composantes connexes sont fermées.

1.1.2 Séparation et totale discontinuité

Définition Soit $(X, \mathfrak{T})$ un espace topologique.
On dit que $(X, \mathfrak{T})$ est **totalement discontinu** lorsque les composantes connexes de X sont les singletons.

Les parties des espaces totalement discontinus sont totalement discontinues.

Proposition 1.1.7 Soit $(X, \mathfrak{T})$ un espace topologique totalement discontinu. Soit $A \subset X$.
Alors, A muni de la topologie induite par $\mathfrak{T}$ est un espace topologique totalement discontinu.

Preuve : Soit B une partie de A qui contient au moins deux éléments.
Comme B n'est pas connexe pour la topologie de X, B n'est pas connexe pour la topologie induite par $\mathfrak{T}$.

Pour prouver que le produit d'espaces totalement discontinus est totalement discontinu, on montre d'abord que l'image d'un connexe par une application continue est un connexe.

Proposition 1.1.8 Soient $(X, \mathfrak{T})$ un espace topologique connexe et $(X', \mathfrak{T}')$ un espace topologique.
Soit $f : X \to X'$ une application continue. Alors, $f(X)$ est une partie connexe de X'.

Preuve : Effectivement, si $g : f(X) \to \{0,1\}$ est une application continue, $g \circ f$ est continue sur le connexe X.
Ainsi, $g \circ f$ est constante donc g est constante par définition de g.

La proposition qui suit sert à montrer la caractérisation topologique des groupes profinis (voir théorème 1.4.1).

Proposition 1.1.9 Soient $(X_i, \mathfrak{T}_i)_{i \in I}$ des espaces topologiques totalement discontinus.
Alors, $\prod_{i \in I} X_i$ muni de la topologie produit est totalement discontinu.

Preuve : Soit A une partie de $\prod_{i\in I} X_i$ qui a au moins deux éléments. Montrons que A n'est pas connexe.
Les projections canoniques $p_i : \prod_{j\in I} X_j \to X_i$ sont surjectives donc $\exists i \in I$ tel que $p_i(A)$ n'est pas un singleton.
Mais X_i est totalement discontinu donc $p_i(A)$ n'est pas connexe. Comme p_i est continue, si A était connexe, on aurait $p_i(A)$ connexe par la proposition 1.1.8. Donc A n'est pas connexe.

Définition Soit $(X, \mathfrak{T})$ un espace topologique. On dit que $(X, \mathfrak{T})$ est **séparé** lorsque $\forall (x, y) \in X^2, x \neq y$, il existe un voisinage V de x et un voisinage W de y tels que $V \cap W = \emptyset$.

Proposition 1.1.10 Soit $(X, \mathfrak{T})$ un espace topologique séparé. Alors, les singletons sont des fermés.

Preuve : Soit $x \in X$. Montrons que $O = X \setminus \{x\}$ est un ouvert. Soit $y \in O$.
Comme $y \neq x$, il existe un voisinage V de y qui ne contient par x étant donné que $(X, \mathfrak{T})$ est séparé.
On peut alors définir V_y comme la réunion des ouverts qui contiennent y et qui ne contiennent pas x.
Finalement, O est la réunion des V_y pour $y \in O$ donc O est ouvert comme réunion d'ouverts.

La proposition précédente et celle qui suit serviront à caractériser les groupes topologiques séparés (proposition 1.2.5).

Proposition 1.1.11 Soit $(X, \mathfrak{T})$ un espace topologique. On note $\Delta = \{(x, x), x \in X\}$.
L'espace $(X, \mathfrak{T})$ est séparé si et seulement si dans $X \times X$ muni de la topologie produit, Δ est fermée.

Preuve : La diagonale Δ est fermée si et seulement si l'ensemble $O = \{(x, y) \in X \times X, x \neq y\}$ est ouvert.
Mais O est ouvert si et seulement si il est voisinage de chacun de ses points.
Donc Δ est fermée si et seulement si $\forall (x, y) \in O$, il existe U et V deux ouverts tels que $(x, y) \in U \times V \subset O$.
Finalement, on a bien Δ fermée si et seulement si $(X, \mathfrak{T})$ est séparé.

De la même façon que tout produit d'espaces totalement discontinus est totalement discontinu par la proposition 1.1.9, tout produit d'espaces séparés est séparé.

Proposition 1.1.12 Soient $(X_i, \mathfrak{T}_i)_{i\in I}$ des espaces topologiques séparés.
Alors, $\prod_{i\in I} X_i$ muni de la topologie produit est séparé.

Preuve : Soient x, y deux points distincts de $\prod_{i\in I} X_i$. Comme $x \neq y$, $\exists i \in I, x_i \neq y_i$.
Comme X_i est séparé, il existe deux ouverts disjoints U et V de X_i tels que $x \in U$ et $y \in V$.
La projection canonique $p_i : \prod_{j\in I} X_j \to X_i$ étant continue, on obtient $p_i^{-1}(U)$ et $p_i^{-1}(V)$ deux ouverts disjoints tels que $x \in p_i^{-1}(U)$ et $y \in p_i^{-1}(V)$.
Finalement, muni de la topologie produit, l'espace $\prod_{i\in I} X_i$ est bien séparé.

On obtient des exemples d'espaces séparés en munissant tout ensemble de la topologie discrète.

Proposition 1.1.13 Soit X un ensemble. L'ensemble X muni de la topologie discrète est séparé.

Preuve : Si $(x, y) \in X^2$ avec $x \neq y$, alors $\{x\}$ est un voisinage ouvert de x et $\{y\}$ est un voisinage ouvert de y.

1.1.3 Compacité

Définition Soit $(X, \mathfrak{T})$ un espace topologique.
On dit que $(X, \mathfrak{T})$ est **compact** lorsque $(X, \mathfrak{T})$ est séparé et que de tout recouvrement ouvert de X, on peut extraire un sous-recouvrement fini.

On suppose connu le fait que les compacts sont fermés, et que les parties fermées d'un espace topologique compact sont compactes. Les deux résultats qui suivent nous servent à montrer le sens difficile de la caractérisation topologique des groupes profinis (voir proposition 1.4.3).

Proposition 1.1.14 Soit $(X, \mathfrak{T})$ un espace topologique compact. Soient $A, B \subset X$.
On suppose que A et B sont compactes, et que $A \cap B = \emptyset$.
Alors, il existe deux ouverts disjoints U' et V' tels que $A \subset U'$ et $B \subset V'$.

Preuve : On commence par le cas où $B = \{b\}$, avec $b \notin A$.

1. L'espace topologique $(X, \mathfrak{T})$ étant compact, il est séparé et donc pour tout $a \in A$, il existe V_a un voisinage ouvert de a et $V_{b,a}$ un voisinage ouvert de b tels que $V_a \cap V_{b,a} = \emptyset$. La partie A vérifie
$$A \subset \bigcup_{a \in A} V_a,$$
donc par compacité de A, il existe une partie finie $\mathcal{A}$ de A telle que
$$A \subset \bigcup_{a \in \mathcal{A}} V_a.$$
On pose V_A la réunion pour $a \in \mathcal{A}$ des V_a, et V_B l'intersection pour $a \in \mathcal{A}$ des $V_{b,a}$.
La partie V_A est ouverte comme réunion d'ouverts et la partie V_B est ouverte comme intersection finie d'ouverts. De plus, on a $A \subset V_A$ et $B \subset V_B$. Les ouverts V_a et $V_{b,a}$ étant disjoints, on a $V_A \cap V_B = \emptyset$.
2. Maintenant, on ne suppose plus que la partie B est réduite un singleton, mais que B est compacte.
Par ce qui précède, si $b \in B$, on dispose d'un voisinage ouvert $V_{A,b}$ de A et d'un voisinage $V_{\{b\}}$ de b tels que $V_{A,b} \cap V_{\{b\}} = \emptyset$. Mais la partie B vérifie
$$B \subset \bigcup_{b \in B} V_{\{b\}},$$
donc par compacité de B, il existe une partie finie $\mathcal{B}$ de B telle que
$$B \subset \bigcup_{b \in \mathcal{B}} V_{\{b\}}.$$
On pose V' la réunion pour $b \in \mathcal{B}$ des $V_{\{b\}}$ et U' l'intersection pour $b \in \mathcal{B}$ des $V_{A,b}$.
La partie V' est ouverte comme réunion d'ouverts et la partie U' est ouverte comme intersection finie d'ouverts. De plus, $A \subset U'$ et $B \subset V'$. Enfin, par construction, les deux ouverts U' et V' sont disjoints.

Les deux résultats suivants proviennent de [RZ10, Lemme 1.1.11] et [RZ10, Thm. 1.1.12].

Proposition 1.1.15 Soit $(X, \mathfrak{T})$ un espace topologique compact. Soit $x \in X$.
La composante connexe de x est l'intersection de tous les voisinages ouverts et fermés de x.

Preuve : Notons $(U_t)_{t \in T}$ la famille des voisinages ouverts et fermés de x. Cette famille contient au moins X. On peut donc poser
$$A = \bigcap_{t \in T} U_t$$
Notons C la composante connexe de x. Un voisinage ouvert et fermé de x contient C par définition de la connexité. Ainsi, $C \subset A$. Pour montrer l'égalité, il suffit donc de prouver que A est connexe. Pour cela, on va utiliser la proposition 1.1.1. Soient U et V deux fermés disjoints de X tels que $A = U \cup V$. Comme X est compact, U et V sont compacts comme fermés dans un compact. Ainsi, U et V sont deux compacts disjoints et il existe U' et V' deux ouverts de X tels que $U \subset U'$ et $V \subset V'$ avec $U' \cap V' = \emptyset$ (on a utilisé la proposition 1.1.14). Ainsi, $(X \setminus (U' \cup V')) \cap A = \emptyset$ et $X \setminus (U' \cup V')$ est fermé.
Donc par compacité de X, il existe une sous-ensemble fini T' de T telle que
$$(X \setminus (U' \cup V')) \cap \left(\bigcap_{t' \in T'} U_{t'} \right) = \emptyset.$$
Notant B l'intersection des $U_{t'}$ pour $t' \in T'$, comme T' est finie, B est un voisinage ouvert et fermé de x.
Comme $x \in B = (B \cap U') \cup (B \cap V')$, on peut supposer sans perte de généralité que $x \in B \cap U'$.

La partie $B \cap U'$ est bien entendu ouverte, mais elle est aussi fermée car $B \cap U' = B \cap (X \setminus B \cap V')$ avec B fermée et $B \cap V'$ ouvert. Ainsi, $A \subset B \cap U' \subset U'$ et donc $A \cap V \subset A \cap V' = U' \cap V' = \emptyset$. Donc $A \cap V = \emptyset$ et comme $V \subset A$, $V = \emptyset$. On a donc A connexe et finalement $C = A$.

PROPOSITION 1.1.16 Soit $(X, \mathfrak{T})$ un espace topologique compact et totalement discontinu.
Alors, $(X, \mathfrak{T})$ admet une base de voisinages ouverts et fermés pour sa topologie.

PREUVE : Soit $x \in X$. Soit W un voisinage ouvert de x.
Montrons que W contient un voisinage ouvert et fermé de x.
Notons encore $(U_t)_{t \in T}$ la famille des voisinages ouverts et fermés de x. Par la proposition 1.1.15,

$$\{x\} = \bigcap_{t \in T} U_t.$$

Comme W est ouvert, $X \setminus W$ est fermé et disjoint de l'intersection des U_t pour $t \in T$.
Par compacité de X, il existe un sous-ensemble fini T' de T tel que

$$(X \setminus W) \cap \left(\bigcap_{t' \in T'} U_{t'} \right) = \emptyset.$$

Donc, comme intersection finie de voisinages ouverts et fermés de x, l'intersection des $U_{t'}$ pour $t' \in T'$ est un voisinage ouvert et fermé de x qui est inclus dans W.

Enfin, le produit d'espaces compacts est encore compact par le théorème de Tychonov.

THÉORÈME 1.1.1 Soient $(X_i, \mathfrak{T}_i)_{i \in I}$ des espaces topologiques compacts.
Alors, $\prod_{i \in I} X_i$ muni de la topologie produit est compact.

Une preuve de ce théorème repose sur l'utilisation des ultrafiltres.

1.2 Groupes topologiques

L'introduction d'une topologie compatible avec une structure de groupe permet d'obtenir des résultats topologiques et algébriques de façon assez immédiate. Dans la suite, si G est un groupe, on notera e son élément neutre.
L'intégralité des résultats sur les groupes topologiques se trouvent dans le chapitre 3 de [Bou07].

DÉFINITION Soit G un groupe muni d'une topologie $\mathfrak{T}$.
On dit que $(G, \mathfrak{T})$ est un **groupe topologique** lorsque les deux conditions suivantes sont vérifiées.

1. L'application $m : G \times G \to G$ définie par $\forall (x, y) \in G^2, m(x, y) = xy$ est continue.
2. L'application $i : G \to G$ définie par $\forall x \in G, i(x) = x^{-1}$ est continue.

Dans ce cas, on dit que la structure de groupe et la structure topologique de G sont **compatibles**.

On remarque que ces deux conditions peuvent être simplifiées en une seule, ce qui fournit la caractérisation suivante.

PROPOSITION 1.2.1 Soit G un groupe muni d'une topologie $\mathfrak{T}$.
Le groupe G muni de la topologie $\mathfrak{T}$ est un groupe topologique si et seulement si l'application $g : G \times G \to G$ définie par $\forall (x, y) \in G^2, g(x, y) = xy^{-1}$ est continue.

PREUVE : Si $(G, \mathfrak{T})$ est un groupe topologique, les applications m et i sont continues en reprenant les mêmes notations que dans la définition.
Donc en notant $d : G \times G \to G \times G$ l'application définie par $\forall (x, y) \in G^2, d(x, y) = (x, i(y))$, on obtient que d est continue car i est continue. Enfin, comme m est continue et que $g = m \circ d$, on a bien que g est continue.
Inversement, si g est continue, alors l'application $y \longmapsto ey^{-1}$ est continue par restriction donc i est continue.
Enfin, d est continue car i l'est et comme $m = g \circ d$, m est aussi continue.

EXEMPLE : Si G est un groupe quelconque, la topologie discrète est compatible avec la structure de groupe de G.

Proposition 1.2.2 Soit $(G, \mathfrak{T})$ un groupe topologique. Soient $a, b \in G$. Alors,

1. Les applications $d_a : x \longmapsto xa$ et $g_a : x \longmapsto ax$ définies sur G sont des homéomorphismes.
2. L'application $x \longmapsto axb$ définie sur G est un homéomorphisme.
3. L'application $x \longmapsto x^{-1}$ est un homéomorphisme.
4. Si A est une partie ouverte (resp. fermée) de G, les parties aA, Aa, aAa^{-1} et A^{-1} sont ouvertes (resp. fermées) dans G.

Preuve :

1. Par restriction de m, $x \longmapsto xa$ est continue. Elle est de plus bijective, d'inverse $x \longmapsto xa^{-1}$. Par restriction de m, cet inverse est également continu. On montre de même que $x \longmapsto ax$ est un homéomorphisme.
2. On obtient le résultat en composant d_b et g_a qui sont des homéomorphismes par le premier point.
3. C'est une application continue involutive de G dans G.
4. Ce sont les images d'une partie ouverte (resp. fermée) par des homéomorphismes.

Exemples : Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, alors pour tout $n \in \mathbb{N}^*$, $\mathrm{GL}_n(\mathbb{K})$ muni du produit matriciel d'une part et de la topologie induite par celle de $\mathcal{M}_n(\mathbb{K})$ d'autre part, est un groupe topologique. Il s'agit de vérifier que le produit matriciel et que l'inversion sont bien des opérations continues dans $\mathrm{GL}_n(\mathbb{K})$.
Le produit matriciel est polynômial en les coefficients des matrices donc est continu. Pour le passage à l'inverse, on remarque que si $A \in \mathrm{GL}_n(\mathbb{K})$, alors A^{-1} est la transposée de la comatrice de A divisée par le déterminant de A. Le déterminant étant polynômial, et non nul sur $\mathrm{GL}_n(\mathbb{K})$, il suffit de vérifier que le passage à la transposée de la comatrice est continu. Or, la transposition est continue et le passage à la comatrice est polynômial (car fait intervenir les mineurs) donc le passage à l'inverse est également continu. On obtient alors d'autres exemples de groupes topologiques en considérant les groupes classiques $\mathrm{SL}_n(\mathbb{K})$, $\mathrm{O}_n(\mathbb{K})$, $\mathrm{U}_n(\mathbb{C})$, $\mathrm{SO}_n(\mathbb{K})$ et $\mathrm{SU}_n(\mathbb{C})$.
Le deuxième point de la proposition précédente affirme que les automorphismes intérieurs sont des homéomorphismes.

Proposition 1.2.3 Soit $(G, \mathfrak{T})$ un groupe topologique. Soient A une partie ouverte de G et $B \subset G$.
Alors, AB et BA sont des ouverts de G.

Preuve : Par définition,

$$AB = \{ab, a \in A, b \in B\} = \bigcup_{b \in B} Ab.$$

Or, pour tout $b \in B$, Ab est un ouvert donc AB est ouvert comme réunion d'ouverts.
De même, on montre que BA est un ouvert de G.

Proposition 1.2.4 Soit $(G, \mathfrak{T})$ un groupe topologique. Soit V un voisiage de e dans G. Soit $A \subset G$.
Alors, AV et VA sont des voisinages de A.

Preuve : Si W est un ouvert tel que $e \in W \subset V$, AW et WA sont ouverts par la proposition 1.2.3 et contiennent A car $e \in W$. On conclut en remarquant que $AW \subset AV$ et que $WA \subset VA$.

On peut déjà montrer donner une caractérisation des groupes topologiques séparés.

Proposition 1.2.5 Soit $(G, \mathfrak{T})$ un groupe topologique.
L'espace topologique $(G, \mathfrak{T})$ est séparé si et seulement si $\{e\}$ est fermé.

Preuve : Si $(G, \mathfrak{T})$ est séparé, alors par la proposition 1.1.10, $\{e\}$ est fermé.
Inversement, si $\{e\}$ est fermé, $\Delta = \{(x, x), x \in G\} = g^{-1}(\{e\})$ avec $g : (x, y) \longmapsto xy^{-1}$ continue par la proposition 1.2.1, donc Δ est fermée, puis $(G, \mathfrak{T})$ est séparé par la proposition 1.1.11.

Corollaire Soit $(G, \mathfrak{T})$ un groupe topologique.
L'espace topologique $(G, \mathfrak{T})$ est séparé si et seulement si l'intersection des voisinages de $\{e\}$ vaut $\{e\}$.

PREUVE : Si $(G,\mathfrak{T})$ est séparé, $\forall x \in G \setminus \{e\}$, il existe un voisinage V de e et un voisinage W de x tels que $V \cap W = \emptyset$. Donc l'intersection des voisinages de e est réduite à $\{e\}$.
Inversement, on suppose que l'intersection des voisinages de $\{e\}$ vaut $\{e\}$. Soit $x \in G \setminus \{e\}$.
Comme $x \neq e$, $x^{-1} \neq e$ et il existe un voisinage V de e tel que $x^{-1} \notin V$ par hypothèse.
En effet, si tout voisinage de e contenait x^{-1}, l'intersection des voisinages de e contiendrait également x^{-1}.
Donc, $e \notin xV$ car si c'était le cas, il existerait $v \in V, e = xv$ et donc $x^{-1} = v \in V$ ce qui est absurde.
Montrons que $x \notin \overline{\{e\}}$. Pour cela, on suppose que $x \in \overline{\{e\}}$.
On obtient alors que tout voisinage de x rencontre $\{e\}$. Mais par la proposition 1.2.4, xV est un voisinage de x et on a montré que ce voisinage ne rencontrait pas $\{e\}$. Donc $x \notin \overline{\{e\}}$ et $\overline{\{e\}} = \{e\}$.
Ainsi, $\{e\}$ est fermé et par la proposition 1.2.5, on obtient bien que $(G,\mathfrak{T})$ est séparé.

REMARQUE : Si $(G,\mathfrak{T})$ est un groupe topologique et si H est un sous-groupe de G, alors H est un groupe topologique pour la topologie induite par $\mathfrak{T}$.

PROPOSITION 1.2.6 Soit $(G,\mathfrak{T})$ un groupe topologique. Soit H un sous-groupe de G.
Alors, l'adhérence $\overline{H}$ de H est un sous-groupe de G. Si de plus $H \trianglelefteq G$, alors $\overline{H} \trianglelefteq G$.

PREUVE : Comme $e \in H$, $e \in \overline{H}$. Bien entendu, $\overline{H} \subset G$. Soient $a, b \in \overline{H}$. Montrons que $ab^{-1} \in \overline{H}$.
Notons g l'application définie sur $G \times G$ et telle que $\forall (x,y) \in G^2$, $g(x,y) = xy^{-1}$. Par la proposition 1.2.1, g est continue. Ainsi, si V est un voisinage ouvert de ab^{-1}, alors $g^{-1}(V)$ est un voisinage ouvert de (a,b) dans $G \times G$.
En effet, $ab^{-1} \in V$ donc $(a,b) \in g^{-1}(ab^{-1}) \subset g^{-1}(V)$ avec $g^{-1}(V)$ ouvert car g est continue.
On a donc l'existence d'un voisinage ouvert V_a de a et d'un voisinage ouvert V_b de b tels que $V_a \times V_b \subset g^{-1}(V)$.
Mais $a \in \overline{H}$ et $b \in \overline{H}$ donc $(V_a \cap H) \times (V_b \cap H) \neq \emptyset$. Donc comme g stabilise les sous-groupes, $H \cap V \neq \emptyset$.
Finalement, $ab^{-1} \in \overline{H}$ et $\overline{H}$ est un sous-groupe de G.
Si $H \trianglelefteq G$, alors $\forall f \in \mathrm{Int}(G)$, comme $f(H) \subset H$, on a $f(\overline{H}) \subset \overline{f(H)} \subset \overline{H}$ par continuité de f et $\overline{H} \trianglelefteq G$.

EXEMPLE : Si $(G,\mathfrak{T})$ est un groupe topologique, alors $\overline{\{e\}} \trianglelefteq G$.

PROPOSITION 1.2.7 Soit $(G,\mathfrak{T})$ un groupe topologique séparé. Soit $M \subset G$.
Alors, le centralisateur $C_G(M) = \{g \in G, \forall m \in M, gm = mg\}$ est un sous-groupe fermé de G.

PREUVE : Le centralisateur de M est bien entendu un sous-groupe. On remarque ensuite que

$$C_G(M) = \bigcap_{m \in M} \{g \in G, gm = mg\} = \bigcap_{m \in M} f_m^{-1}(\{e\})$$

avec f_m définie sur G pour tout $m \in M$ par $\forall g \in G$, $f_m(g) = gmg^{-1}m^{-1}$ (commutateur).
Par composition et par la proposition 1.2.2, $\forall m \in M$, f_m est continue.
De plus, comme $(G,\mathfrak{T})$ est séparé, $\{e\}$ est fermé par la proposition 1.2.5. Donc $\forall m \in M$, $f_m^{-1}(\{e\})$ est un fermé.
Ainsi, $C_G(M)$ est fermé en tant qu'intersection de parties fermées.

EXEMPLE : Dans un groupe topologique séparé, le centre est un sous-groupe fermé.

PROPOSITION 1.2.8 Soit $(G,\mathfrak{T})$ un groupe topologique. Soit H un sous-groupe de G.
Alors, H est ouvert si et seulement s'il est d'intérieur non vide.

PREUVE : Comme H est non vide, s'il est ouvert, son intérieur est non vide étant donné que c'est H tout entier.
Inversement, supposons H d'intérieur non vide. Il existe donc $h \in H$ tel que $h \in V \subset H$ avec V un ouvert.
Soit $x \in H$. Montrons que H est voisinage de x. Posons f_x l'application définie sur G par $\forall g \in G, f_x(g) = xh^{-1}g$.
Par la proposition 1.2.2, f_x est continue donc $f_x^{-1}(V)$ est un ouvert et $x \in f_x^{-1}(V)$ car $h \in V$.
Mais $f_x^{-1}(V) \subset H$ car si $g \in f_x^{-1}(V)$, alors $\exists v \in V, xh^{-1}g = v$ et donc $g = hx^{-1}v$ avec $h \in H$, $x \in H$ et $v \in V \subset H$ donc $g \in H$ car H est un sous-groupe de G.
On a montré que $\forall x \in H$, $x \in f_x^{-1}(V) \subset H$ donc H est voisinage de chacun de ses points. Ainsi, H est ouvert.

Dans un groupe topologique, un sous-groupe ouvert est nécessairement fermé.

Proposition 1.2.9 Soit $(G, \mathfrak{T})$ un groupe topologique. Soit H un sous-groupe ouvert de G.
Alors, H est un sous-groupe fermé de G.

Preuve : Si $H = G$, c'est évident. Sinon, on va montrer que si on pose

$$U = \bigcup_{g \in G \setminus H} gH,$$

on a $U = G \setminus H$. Si $x \in G \setminus H$, on a bien entendu $x \in U$ car $e \in H$.
Inversement, si $x \in U$, alors $\exists g \in G \setminus H$ et $\exists h \in H$ tels que $x = gh$.
Donc, si $x \in H$, on aurait $g = xh^{-1} \in H$ ce qui est faux. Donc $x \in G \setminus H$.
Par la proposition 1.2.3, $U = G \setminus H$ est ouvert comme réunion d'ouverts (H est ouvert). Ainsi, H est fermé.

Définition Soit $(G, \mathfrak{T})$ un groupe topologique.
La **composante neutre** de $(G, \mathfrak{T})$ est la composante connexe de e. On la note G^0.

Dans un groupe topologique, la composante neutre, définie topologiquement, possède en fait une structure algébrique.

Proposition 1.2.10 Soit $(G, \mathfrak{T})$ un groupe topologique. Alors, G^0 est un sous-groupe normal fermé de G.

Preuve : Par la proposition 1.1.6, G^0 est fermée. Par définition, on a bien $G^0 \subset G$.
Ensuite, $e \in G^0$ par définition de composante connexe. Si $x \in G^0$, $x^{-1}G^0$ est encore connexe par les propositions 1.1.8 et 1.2.2. Or $x \in G^0$ donc $x^{-1}G^0$ est un connexe qui contient e. Par maximalité, on a $x^{-1}G^0 \subset G^0$. Cela montre que G^0 est un sous-groupe de G.
De plus, si $x \in G$, xG^0x^{-1} est un connexe par les propositions 1.1.8 et 1.2.2 donc, de la même façon, on a $xG^0x^{-1} \subset G^0$ ($e \in xG^0x^{-1}$ car $e \in G^0$).

Exemple : Si $n \in \mathbb{N}^*$, la composante neutre de $\mathrm{GL}_n(\mathbb{R})$ est $\mathrm{GL}_n^+(\mathbb{R})$ (l'ensemble des matrices réelles de taille n dont le déterminant est strictement positif). En effet, $I_n \in \mathrm{GL}_n^+(\mathbb{R})$ et $\mathrm{GL}_n^+(\mathbb{R})$ est bien la composante connexe de I_n vu la continuité de l'application déterminant.

Proposition 1.2.11 Soit G un groupe topologique. Soit H un sous-groupe de G.
Alors, la surjection canonique $\pi : G \to G/H$ est continue et ouverte.

Preuve : Par définition de la topologie quotient, π est continue. Soit U un ouvert de G.
Montrons que $\pi(U)$ est ouvert. Pour cela, par définition de la topologie quotient, il suffit de montrer que $\pi^{-1}(\pi(U))$ est ouvert. Remarquons que

$$\pi^{-1}(\pi(U)) = \{x \in G, \pi(x) \in \pi(U)\} = \{x \in G, \exists u \in U, xH = uH\} = \{x \in G, \exists u \in U, x \in uH\} = UH.$$

Ainsi, par la proposition 1.2.3, π est bien ouverte.

Proposition 1.2.12 Soit G un groupe topologique. Soit H un sous-groupe de G.
L'ensemble G/H est discret si et seulement si H est ouvert.

Preuve : Les singletons de G/H sont de la forme xH avec $x \in G$. Ils sont ouverts si et seulement si H est ouvert par la proposition 1.2.2.

Proposition 1.2.13 Soit G un groupe topologique compact. Soit H un sous-groupe de G.
Alors, H est d'indice fini dans G si et seulement si H est ouvert dans G.

Preuve : Supposons que H est ouvert dans G. Par la proposition 1.2.12, G/H est discret.
Mais comme G est compact et comme la surjection canonique $\pi : G \to G/H$ est continue (par la proposition

1.2.11), G/H est compact (image d'un compact par une application continue). Or, un compact discret est fini (extraire un recouvrement fini du recouvrement par des singletons). Donc G/H est fini.
Inversement, supposons que G/H est fini. Par le même argument que précédemment, G/H est compact donc G/H est séparé. Ainsi, G/H étant fini et séparé, il est discret. Donc, H est ouvert par la proposition 1.2.12.

1.3 Limite projective d'un système projectif de groupes topologiques

Avant de définir les limites projectives des systèmes projectifs de groupes topologiques, on donne la définition d'ensemble ordonné filtrant et on donne deux exemples importants.
Les résultats sur les limites projectives et sur les groupes profinis proviennent des deux premiers chapitres de [RZ10].

DÉFINITION Soit I un ensemble muni d'une relation d'ordre $\leqslant$.
On dit que l'ensemble ordonné $(I, \leqslant)$ est **filtrant** (à droite) lorsque $\forall (i,j) \in I^2, \exists k \in I$ tel que $i \leqslant k$ et $j \leqslant k$.

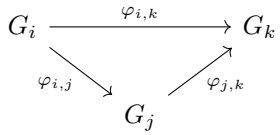
EXEMPLES : Les deux exemples suivants seront utilisés dans la suite.

1. L'ensemble $\mathbb{N}$ muni de l'ordre usuel $\leqslant$ est filtrant.
2. L'ensemble $\mathbb{N}$ muni de la divisibilité $|$ est un ensemble ordonné filtrant.

DÉFINITION Soit $(I, \leqslant)$ un ensemble ordonné filtrant.
Un **système projectif de groupes topologiques** sur I est la donnée d'une famille $(G_i)_{i\in I}$ de groupes topologiques et d'une famille $(\varphi_{i,j} : G_i \to G_j)_{(i,j)\in I^2, j\leqslant i}$ de morphismes de groupes continus qui vérifient

1. $\forall i \in I$, $\varphi_{i,i} = id_{G_i}$
2. $\forall (i,j,k) \in I^3$ tel que $k \leqslant j \leqslant i, \varphi_{i,k} = \varphi_{j,k} \circ \varphi_{i,j}$.

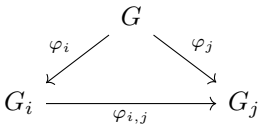
La seconde condition revient à la commutativité du diagramme suivant pour tout $(i,j,k) \in I^3$ tel que $k \leqslant j \leqslant i$.



On notera ce système projectif $((G_i)_{i\in I}, (\varphi_{i,j})_{(i,j)\in I^2, j\leqslant i})$ ou seulement $(G_i, \varphi_{i,j}, I)$ pour abréger.

EXEMPLE : On se place sur l'ensemble ordonné filtrant $(\mathbb{N}, \leqslant)$. Soit p un nombre premier
Pour tout $n \in \mathbb{N}$, on pose $G_n = \mathbb{Z}/p^n\mathbb{Z}$ et pour $(m,n) \in \mathbb{N}^2$ tel que $m \leqslant n$, on pose $\varphi_{n,m}$ la projection naturelle.
Les $\varphi_{n,m}$ sont bien entendu des morphismes de groupes qui sont continus pour la topologie discrète.
Pour tout $n \in \mathbb{N}$, on a bien sûr $\varphi_{n,n} = id_{G_n}$. La seconde condition est également vérifiée.
Le triplet $(G_n, \varphi_{n,m}, \mathbb{N})$ est donc notre premier exemple de système projectif de groupes topologiques.

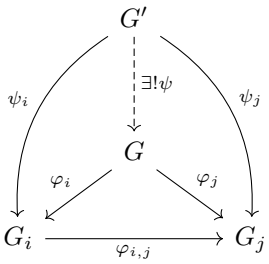
DÉFINITION Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques. Soit G un groupe topologique.
Soit $(\varphi_i : G \to G_i)_{i\in I}$ une famille de morphismes de groupes continus. On dit que les φ_i sont **compatibles** avec le système projectif $(G_i, \varphi_{i,j}, I)$ lorsque pour tout $(i,j) \in I^2$ tel que $j \leqslant i$, $\varphi_{i,j} \circ \varphi_i = \varphi_j$.
Cela revient à la commutativité du diagramme ci-dessous pour tout $(i,j) \in I^2$ tel que $j \leqslant i$.



Étant donné un système projectif de groupes topologiques, on va définir la notion de limite projective de ce système. Notons que cette limite n'a a priori aucune raison d'être unique.

DÉFINITION Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques. Soit G un groupe topologique.
Soit $(\varphi_i : G \to G_i)_{i\in I}$ une famille de morphismes de groupes continus compatibles avec $(G_i, \varphi_{i,j}, I)$.
Le groupe topologique G est une **limite projective** du système projectif $(G_i, \varphi_{i,j}, I)$ lorsque la propriété universelle suivante est vérifiée : pour tout groupe topologique G' et morphismes de groupes compatibles

$\psi_i : G' \to G_i$, il existe un unique morphisme continu $\psi : G' \to G$ tel que $\forall i \in I, \varphi_i \circ \psi = \psi_i$.
La situation est résumée par le diagramme commutatif suivant.



Si on a un système projectif de groupes topologiques, on va montrer que ce système admet une limite projective, et que cette limite est unique à *un unique* isomorphisme près.

PROPOSITION 1.3.1 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques.

1. Il existe une limite projective au système projectif $(G_i, \varphi_{i,j}, I)$.
2. On a l'unicite de la limite projective au sens suivant : si (G, φ_i) et (G', ψ_i) sont deux limites projectives du système projectif $(G_i, \varphi_{i,j}, I)$, alors G et G' sont isomorphes continument.

PREUVE : La preuve est indispensable pour mieux comprendre la structure des limites projectives.

1. Soit $G = \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid \forall (i,j) \in I^2, j \leqslant i, \varphi_{i,j}(g_i) = g_j\}$. On va montrer que G est une limite projective du système projectif $(G_i, \varphi_{i,j}, I)$. La première étape consiste à vérifier que G est bien un groupe topologique. Comme $\forall i \in I$, G_i est un groupe topologique, le produit $\prod_{i\in I} G_i$ est un groupe topologique pour la topologie produit (tout se fait composante par composante).
   Montrons que G est un sous-groupe de $\prod_{i\in I} G_i$. Le groupe G sera topologique pour la topologie induite.
   Les $\varphi_{i,j}$ étant des morphismes de groupes et les G_i étant des groupes, G contient bien l'élément neutre de $\prod_{i\in I} G_i$. De plus, si $(g_i)_{i\in I}$ et $(h_i)_{i\in I}$ sont deux éléments de G, pour tout $(i,j) \in I^2$ tel que $j \leqslant i$,
   $$\varphi_{i,j}(g_i h_i^{-1}) = \varphi_{i,j}(g_i)\varphi_{i,j}(h_i)^{-1} = g_j h_j^{-1}$$
   car les $\varphi_{i,j}$ sont des morphismes de groupes. Donc, $(g_i h_i^{-1})_{i\in I} \in G$ et G est un sous-groupe de $\prod_{i\in I} G_i$.
   On va maintenant exhiber des morphismes continus de G dans G_i.
   On pose $\forall i \in I$, $\varphi_i : G \to G_i$ la restriction de la projection canonique $\prod_{j\in I} G_j \to G_i$.
   Les φ_i sont bien entendu des morphismes de groupes. Ils sont continus par définition de la topologie produit (φ_i est égale à l'identité sur la i-ème composante et est constante sur les autres composantes).
   Par définition de G, les φ_i sont compatibles avec $(G_i, \varphi_{i,j}, I)$.
   Enfin, montrons que la propriété universelle est vérifiée. Soit G' un groupe topologique.
   Soit $(\psi_i : G' \to G_i)_{i\in I}$ une famille de morphismes compatibles avec $(G_i, \varphi_{i,j}, I)$.
   On commence par montrer $\exists \psi : G' \to G$ un morphisme continu tel que $\forall i \in I, \varphi_i \circ \psi = \psi_i$.
   Pour cela, on remarque que si $x \in G'$, on dispose de $\psi_i(x)$ pour tout $i \in I$ et on pose
   $$\forall x \in G', \quad \psi(x) = (\psi_i(x))_{i\in I}.$$
   Ainsi définie, ψ est bien un morphisme continu par continuité des ψ_i et par définition de la topologie produit. Il faut quand même montrer que ψ est à valeurs dans G. Soit $x \in G'$. Soit $(i,j) \in I^2$ tel que $j \leqslant i$. Par définition de $\psi(x)$ et par compatibilité,
   $$\varphi_{i,j}(\psi(x)_i) = \varphi_{i,j}(\psi_i(x)) = \psi_j(x) = \psi(x)_j.$$
   Donc $\psi(x) \in G$. Enfin, $\forall i \in I$, $\varphi_i \circ \psi = \psi_i$ par définition. Inversement, si un tel morphisme continu ψ existe, alors
   $$\forall x \in G', \quad \psi(x)_i = \varphi_i(\psi(x)) = \psi_i(x)$$
   et donc ce morphisme continu est unique. Le groupe G est donc une limite projective de $(G_i, \varphi_{i,j}, I)$.
2. Soient (G, φ_i) et (G', ψ_i) deux limites projectives du système projectif $(G_i, \varphi_{i,j}, I)$.
   En utilisant la propriété universelle dans les deux sens, on obtient $\exists! \varphi : G \to G'$ morphisme continu et

$\exists ! \psi : G' \to G$ morphisme continu tels que $\forall i \in I$,

$$\varphi_i \circ \psi = \psi_i \quad \text{et} \quad \psi_i \circ \varphi = \varphi_i.$$

Remarquons que $\forall i \in I$,

$$\varphi_i \circ (\psi \circ \varphi) = (\varphi_i \circ \psi) \circ \varphi = \psi_i \circ \varphi = \varphi_i.$$

Mais par la propriété universelle appliquée à la limite inverse G pour le groupe G, il existe un *unique* morphisme continu θ tel que $\forall i \in I, \varphi_i \circ \theta = \varphi_i$. Comme $\theta = id_G$ convient, $\psi \circ \varphi = id_G$. De même, on montre que $\varphi \circ \psi = id_{G'}$ et donc comme φ et ψ sont des morphismes continus, on a bien la propriété d'unicité à isomorphisme continu près voulu.

Cette preuve est importante car elle est constructive. En effet, on sait maintenant identifier la limite projective d'un système projectif à un sous-groupe du produit direct. Dans la suite, on dira **la** limite projective, mais il sera toujours sous-entendu **une** limite projective à isomorphisme continu près. On fera le plus souvent l'identification avec un sous-groupe du produit, comme dans la preuve de l'existence.

DÉFINITION Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques.
À isomorphisme près, la **limite projective** du système projectif $(G_i, \varphi_{i,j}, I)$ est notée $\varprojlim_{i \in I} G_i$ ou $\varprojlim G_i$.

PROPOSITION 1.3.2 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques abéliens.
Alors, $\varprojlim G_i$ est un groupe abélien.

PREUVE : Comme tous les G_i sont abéliens, le produit $\prod_{i \in I} G_i$ est un groupe abélien. Ainsi, $\varprojlim G_i$, vu comme sous-groupe du produit des G_i, est abélien.

EXEMPLE : On garde l'exemple $(G_n, \varphi_{n,m}, \mathbb{N})$ où $G_n = \mathbb{Z}/p^n\mathbb{Z}$.
La proposition 1.3.1 assure l'existence d'une limite projective, et la preuve affirme que l'on peut écrire

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \mid \forall (m,n) \in \mathbb{N}^2, m \leqslant n, x_n \equiv x_m \ [p^m]\}$$

à isomorphisme continu près. Ce groupe, qui est abélien en vertu de la proposition 1.3.2, est noté $\mathbb{Z}_p$ et est appelé groupe des entiers p-adiques. Remarquons que les morphismes $\varphi_{n,m}$ sont en fait des morphismes d'anneaux, de sorte que $\mathbb{Z}_p$ possède une structure d'anneau topologique.

PROPOSITION 1.3.3 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques séparés.
Alors, $\varprojlim G_i$ est fermé dans $\prod_{i \in I} G_i$ muni de la topologie produit.

PREUVE : On va montrer que $O = \left(\prod_{i \in I} G_i\right) \setminus \varprojlim G_i$ est voisinage de chacun de ses points.
Soit $(x_i)_{i \in I} \in O$. Comme $(x_i)_{i \in I}$ n'est pas dans la limite projective,

$$\exists (r,s) \in I^2, s \leqslant r, \quad \varphi_{r,s}(x_s) \neq x_r.$$

Le groupe topologique G_s est séparé donc il existe un voisinage ouvert U de $\varphi_{r,s}(x_r)$ et V un voisinage ouvert de x_s tels que $U \cap V = \emptyset$. Donc $\varphi_{r,s}^{-1}(U)$ est un ouvert contenant x_r et il existe un voisinage U' de x_r tel que $U' \subset \varphi_{r,s}^{-1}(U)$, de sorte que $\varphi_{r,s}(U') \subset \varphi_{r,s}(\varphi_{r,s}^{-1}(U)) \subset U$.
On pose $W = \prod_{i \in I} V_i$ où $\forall i \in I \setminus \{r,s\}$, $V_i = G_i$,$V_r = U'$ et $V_s = V$. Clairement, W est un voisinage ouvert de $(x_i)_{i \in I}$ qui ne rencontre pas la limite projective. Donc O est voisinage de chacun de ses points.

On va montrer que le fait d'être compact et totalement discontinu passe à la limite projective.

PROPOSITION 1.3.4 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes topologiques.
On suppose que $\forall i \in I$, G_i est un groupe compact et totalement discontinu.
Alors, le groupe $\varprojlim G_i$ est compact et totalement discontinu.

Preuve : Par le théorème de Tychonov, $\prod_{i\in I} G_i$ est compact car les G_i sont tous compacts.
Donc, en tant que fermé dans un compact par la proposition 1.3.3, $\varprojlim G_i$ est compact.
De plus, comme les G_i sont totalement discontinus, par la proposition 1.1.9, $\prod_{i\in I} G_i$ l'est aussi.
Enfin, en utilisant la proposition 1.1.7, on obtient que $\varprojlim G_i$ est totalement discontinu.

En fait, on peut définir les systèmes projectifs et les limites projectifs dans un cadre plus général. En particulier, on peut parler d'un système projectif d'espaces topologiques. Cela nous sera utile pour généraliser les théorèmes de Sylow au cas des groupes profinis.

Définition Soit $(I, \leqslant)$ un ensemble ordonné filtrant.
Un **système projectif d'espaces topologiques** sur I est la donnée d'une famille $(X_i)_{i\in I}$ d'espaces topologiques et d'une famille $(\varphi_{i,j} : X_i \to X_j)_{(i,j)\in I^2, j\leqslant i}$ d'applications continues qui vérifient

1. $\forall i \in I$, $\varphi_{i,i} = id_{X_i}$
2. $\forall (i,j,k) \in I^3$ tel que $k \leqslant j \leqslant i, \varphi_{i,k} = \varphi_{j,k} \circ \varphi_{i,j}$.

On notera ce système projectif $((X_i)_{i\in I}, (\varphi_{i,j})_{(i,j)\in I^2, j\leqslant i})$ ou seulement $(X_i, \varphi_{i,j}, I)$ pour abréger.

On définit de la même façon les applications compatibles. La preuve de la proposition 1.3.1 tient toujours dans le cadre des espaces topologiques, donc on peut définir les limites projectives de systèmes projectifs d'espaces topologiques.

Proposition 1.3.5 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces topologiques séparés.
Alors, $\varprojlim X_i$ est un sous-espace fermé de $\prod_{i\in I} X_i$ muni de la topologie produit.

Preuve : Là encore, la preuve de la proposition 1.3.3 s'adapte au cadre des espaces topologiques.

Dans le cas des groupes topologiques, une limite projective d'un système projectif de groupes topologiques contient au moins l'élément neutre. Dans le cas des espaces topologiques, on montre que la limite projective est non vide.

Proposition 1.3.6 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces topologiques compacts non vides.
Alors, $\varprojlim X_i$ est un espace topologique non vide.

Preuve : Pour tout $j \in I$, on pose Y_j l'ensemble des $(x_i)_{i\in I} \in \prod_{i\in I} X_i$ telles que $\forall k \in I, k \leqslant j$, $\varphi_{j,k}(x_j) = x_k$.
En utilisant l'axiome du choix et un argument similaire à celui utilisé dans la preuve de la proposition 1.3.3, on obtient que Y_j est un fermé non vide de $\prod_{i\in I} X_i$. Ainsi, les Y_j sont des compacts non vides par le théorème de Tychonov (et car les Y_j sont fermés dans un compact). De plus, si $j \leqslant j'$, alors $Y'_j \subset Y_j$.
Donc toute intersection finie de Y_j est non vide (I est filtrant). Ainsi, par compacité,

$$\bigcap_{j\in I} Y_j \neq \emptyset.$$

Or l'intersection de tous les Y_j vaut exactement la limite projective des X_i par définition.

Proposition 1.3.7 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces topologiques compacts.
Soit X un espace topologique compact. Soit $(\varphi_i : X \to X_i)_{i\in I}$ une famille d'applications surjectives continues compatibles. Alors, l'application induite $\varphi : X \to \varprojlim X_i$ est surjective.

Preuve : Soit $(x_i)_{i\in I} \in \varprojlim X_i$. Soit $i \in I$. On pose $Y_i = \varphi_i^{-1}(\{x_i\})$.
Comme φ_i est surjective, $Y_i \neq \emptyset$. Mais X_i est séparé, donc $\{x_i\}$ est fermé par la proposition 1.1.10.
Ainsi, Y_i est fermé par continuité de φ_i. Or X est compact, Y_i est également un compact.
Montrons que (Y_i, id, I) est un système projectif d'espaces topologiques.
Par définition, il suffit de vérifier que si $j, k \in I$ vérifient $k \leqslant j$, $Y_j \subset Y_k$.
Soit $y_j \in Y_j$. On a donc $\varphi_j(y_j) = x_j$. Montrons que $\varphi_k(y_j) = x_k$.
Par compatibilité et par définition de la limite projective, on a bien

$$\varphi_k(y_j) = (\varphi_{j,k} \circ \varphi_j)(y_j) = \varphi_{j,k}(x_j) = x_k.$$

On dispose donc d'un système projectif d'espaces compacts non vides donc par 1.3.6, la limite projective des Y_i notée Y est non vide. De plus, par construction, si $y \in Y$, on a bien $\varphi(y) = (x_i)_{i\in I}$. Ainsi, φ est bien surjective.

PROPOSITION 1.3.8 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces topologiques. Soit X un espace topologique. Soit $(\rho_i : X \to X_i)_{i\in I}$ une famille d'applications continues surjectives compatibles.
Notons $\rho : X \to \varprojlim X_i$ l'application induite par les ρ_i. Alors, on a l'alternative suivante :

1. $\varprojlim X_i = \emptyset$.
2. $\varphi(X)$ est dense dans $\varprojlim X_i$.

PREUVE : Supposons que $\varprojlim X_i = \emptyset$ et montrons que $\varphi(X)$ est dense dans $\varprojlim X_i$.
Pour cela, on montre que l'intersection de $\varphi(X)$ avec un ouvert fondamental de $\varprojlim X_i$, de la forme

$$V = \varprojlim X_i \cap \left(\prod_{i\in I} V_i\right)$$

avec V_i qui vaut toujours X_i sauf un nombre fini de fois où V_i est un ouvert de X_i, est non vide quand $V \neq \emptyset$.
Soit $i' \in I$ tel que i' est plus grand que tous les indices qui correspondent aux $V_i \neq X_i$ (i' exite car I est filtrant).
Si $(y_i)_{i\in I} \in V$, comme $\rho_{i'}$ est surjective, $\exists x \in X$ tel que $\rho_{i'}(x) = y_{i'}$. Par construction, on a bien $\rho(x) \in V$.

PROPOSITION 1.3.9 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces compacts.
On note $X = \varprojlim X_i$ et pour tout $i \in I$, $\varphi_i : X \to X_i$ la projection sur X_i. Alors,

1. Si Y est un sous-espace fermé de X, alors Y et $\varprojlim \varphi_i(Y)$ sont isomorphes.
2. Si Y est un sous-espace de X, alors $\overline{Y}$ et $\varprojlim \varphi_i(Y)$ sont isomorphes.

PREUVE : On prouve les deux points successivement.

1. Tout d'abord, Y s'injecte naturellement dans la limite projective des $\varphi_i(Y)$. En effet, si y et y' sont deux éléments de Y qui s'envoient sur le même élément de $\varprojlim \varphi_i(Y)$, c'est que $\forall i \in I$, on a $\varphi_i(y) = \varphi_i(y')$.
   Ainsi, $y = y'$ étant donné que y et y' coïncident sur toutes les coordonnées.
   Ce morphisme est de plus surjectif par la proposition 1.3.7 (Y est compact comme fermé dans un compact).
2. Si Y est vide, l'égalité est vérifiée. Sinon, Y est non vide et par la proposition 1.3.8, Y s'envoie sur un sous-ensemble dense de $\varprojlim \varphi_i(Y)$.
   Mais comme dans la preuve de la proposition 1.3.5, $\varprojlim \varphi_i(Y)$ est fermé dans X. Ainsi, on a bien

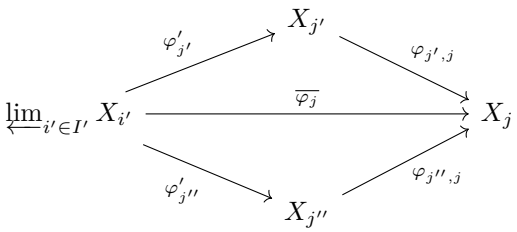
$$\overline{Y} \cong \overline{\varprojlim \varphi_i(Y)} = \varprojlim \varphi_i(Y).$$

Pour montrer une propriété utile dans la suite, on définit les parties cofinales d'un ensemble ordonné filtrant.

DÉFINITION Soit $(I, \leqslant)$ un ensemble ordonné filtrant. Soit I' une partie de I.
On dit que I' est **cofinale** dans I lorsque $\forall i \in I, \exists i' \in I'$ tel que $i \leqslant i'$.

PROPOSITION 1.3.10 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces topologiques compacts.
Soit I' une partie cofinale de I. Alors, $\varprojlim_{i'\in I'} X_{i'}$ et $\varprojlim_{i\in I} X_i$ sont homéomorphes.

PREUVE : Pour tout $i \in I$, notons $\varphi_i : \varprojlim_{j\in I} X_j \to X_i$ et $\varphi'_i : \varprojlim_{j'\in I'} X_{j'} \to X_i$.
On veut construire une bijection de $\varprojlim_{i'\in I'} X_{i'}$ dans $\varprojlim_{i\in I} X_i$. Soit $j \in I$. Soit $j' \in I'$ tel que $j \leqslant j'$.
Posons $\overline{\varphi_j} = \varphi_{j',j} \circ \varphi'_{j'}$. Remarquons que $\overline{\varphi_j}$ est bien définie sur $\varprojlim_{i'\in I'} X_{i'}$, est à valeurs dans X_j et ne dépend pas du choix de j'. En effet, si $j'' \in I$ vérifie aussi $j \leqslant j''$, alors le diagramme suivant commute, ce qui assure que la définition de $\overline{\varphi_j}$ ne dépend pas du choix de j'.



De plus, les $\overline{\varphi_j}$ sont compatibles car si $(i,j) \in I^2$ vérifient $j \leqslant i$, les relations qui proviennent de la définition du système projectif assurent que

$$\varphi_{i,j} \circ \overline{\varphi_i} = \varphi_{i,j} \circ \varphi_{j',i} \circ \varphi'_{j'} = \varphi_{j',j} \circ \varphi'_{j'} = \overline{\varphi_j}.$$

Ainsi, par la propriété universelle, on dispose d'une unique application continue $\overline{\varphi} : \varprojlim_{i'\in I'} X_{i'} \to \varprojlim_{i\in I} X_i$ et qui vérifie $\forall j \in I$, $\varphi_j \circ \overline{\varphi} = \overline{\varphi_j}$. Montrons que $\overline{\varphi}$ est bijective. Montrons tout d'abord l'injectivité de $\overline{\varphi}$.
Soit $(x_i)_{i\in I} \in \varprojlim_{i\in I} X_i$. Soient $(y_i)_{i\in I'}, (z_i)_{i\in I'} \in \varprojlim_{i'\in I'} X_{i'}$ tels que $\overline{\varphi}((y_i)_{i\in I'}) = \overline{\varphi}((z_i)_{i\in I'}) = (x_i)_{i\in I}$.
Remarquons que si $j \in I'$, $\varphi_j(\overline{\varphi}((y_{i'})_{i\in I'})) = \overline{\varphi_j}((y_{i'})_{i\in I'})$ et donc $\varphi_j((x_i)_{i\in I}) = \varphi_{j',j}(\varphi'_{j'}((y_{i'})_{i\in I'}))$.
Ainsi, $x_j = \varphi_{j',j}(y_{j'}) = y_j$. De même, on a $\forall j \in I'$, $x_j = z_j$. Donc comme I' est cofinale dans I, $\overline{\varphi}$ est injective.
De plus, par restriction d'un élément de $\varprojlim_{j\in I} X_j$ à un élément de $\varprojlim_{j'\in I'} X_{j'}$, $\overline{\varphi}$ est bien surjective.
En effet, si $(y_i)_{i\in I} \in \varprojlim_{j\in I} X_j$, en posant $(y_i)_{i\in I'} \in \varprojlim_{j'\in I'} X_{j'}$ tel que $\forall j' \in I', y_{j'} = x_{j'}$, on obtient bien $\forall i \in I', y_i = \overline{\varphi_i}((x_j)_{j\in I}) = \overline{\varphi}(x_i)$ par la propriété universelle.
Il reste à montrer que $\overline{\varphi}$ est continue et que son inverse est continue aussi. On sait déjà que $\overline{\varphi}$ est continue.
Mais les espaces de départ et d'arrivée sont compacts dont $\overline{\varphi}$ est fermée. En effet, l'image d'un fermé par $\overline{\varphi}$ est en fait l'image d'un compact par une application continue (l'espace de départ est compact donc on obtient l'image continue d'un fermé dans un compact), donc on obtient un compact dans l'espace d'arrivée, donc un fermé étant donné que l'espace d'arrivée est séparé.
On en déduit que $\overline{\varphi}$ est un homéomorphisme (c'est une bijection continue fermée).

PROPOSITION 1.3.11 Soit $(X_i, \varphi_{i,j}, I)$ un système projectif d'espaces topologiques compacts non vides.
On suppose que $\forall (i,j) \in I^2$ tel que $j \leqslant i$, $\varphi_{i,j}$ est surjective. Alors, $\forall j \in I, \varphi_j : \varprojlim_{i\in I} X_i \to X_j$ est surjective.

PREUVE : Soit $j \in I$. Soit $I_j = \{i \in I, j \leqslant i\}$. Remarquons que I_j est cofinale dans I.
En effet, si $i \in I$, comme I est filtrant, il existe $i' \in I$ tel que $i \leqslant i'$ et $j \leqslant i'$ et donc $i' \in I_j$ et $i \leqslant i'$.
Ainsi, par la proposition 1.3.10, $\varprojlim_{i'\in I'} X_{i'}$ et $\varprojlim_{i\in I} X_i$ sont homéomorphes.
Quitte à passer par cet homéomorphisme, on peut supposer que $\forall i \in I, j \leqslant i$.
Soit $x_j \in X_j$. On cherche $(y_r)_{r\in I} \in \varprojlim X_i$ telle que $\varphi_j((y_r)_{r\in I}) = x_j$. Pour tout $r \in I$, on pose $Y_r = \varphi_{r,j}^{-1}(\{x_j\})$.
Notons que pour tout $r \in I$, $\varphi_{r,j}$ existe, est surjective et est continue donc Y_r est un compact, comme fermé (image réciproque d'un fermé par une application continue car c'est un singleton dans un espace séparé par la proposition 1.1.10) dans le compact X_r et $Y_r \neq \emptyset$ par surjectivité.
De plus, si $r \in I$, $\varphi_{r,s}(Y_r) \subset Y_s$. Effectivement, si $y \in \varphi_{r,s}(Y_r)$, il existe $x \in Y_r$ tel que $y = \varphi_{r,s}(x)$.
Mais alors, par compatibilité et en se souvenant que $x \in Y_r$, on a $\varphi_{s,j}(y) = \varphi_{s,j}(\varphi_{r,s}(x)) = \varphi_{r,j}(x) = x_j$.
Ainsi, $y \in Y_s$ et $\varphi_{r,s}(Y_r) \subset Y_s$. Donc $(Y_r, \varphi_{r,s}, I)$ est un système projectif d'espaces compacts non vides.
Par la proposition 1.3.6, la limite projective $\varprojlim Y_r$ est non vide. Soit $(y_r)_{r\in I} \in \varprojlim Y_r \subset \varprojlim X_i$.
Par construction, on a bien $\varphi_j((y_r)_{r\in I}) = x_j$.

1.4 Groupes profinis, caractérisation

DÉFINITION Un groupe est dit **profini** lorsqu'il est la limite projective d'un système projectif de groupes finis munis de la topologie discrète.

Les groupes profinis sont compacts et totalement discontinus.

PROPOSITION 1.4.1 Soit G un groupe profini.
On suppose que G est limite projective du système projectif de groupes finis discrets $(G_i, \varphi_{i,j}, I)$.

Alors, G est compact et totalement discontinu.

PREUVE : Soit $i \in I$. Le groupe G_i étant muni de la topologie discrète, il est totalement discontinu par définition. De plus, par la proposition 1.1.13, G_i est séparé. Comme G_i est fini, tout recouvrement ouvert de G_i est fini. Ainsi, G_i est compact. Il suffit d'utiliser la proposition 1.3.4 pour conclure.

En fait, les groupes compacts et totalement discontinus sont profinis. Pour prouver cela, on commence par montrer la proposition suivante.

PROPOSITION 1.4.2 Soit G un groupe topologique. On suppose que G est compact et totalement discontinu. Alors, les sous-groupes ouverts de G forment une base de voisinages de e.

PREUVE : Remarquons tout d'abord que les sous-groupes ouverts contiennent e donc sont des voisinages de e.
Ensuite, il s'agit de montrer que pour tout voisinage ouvert V de e, il existe un sous-groupe ouvert H de G tel que $e \in H \subset V$. Par la proposition 1.1.16, il suffit de faire le cas où V est un voisinage ouvert et fermé de e.
Dans cette preuve, si A est une partie de X et si $n \in \mathbb{N}$, on notera A^n l'ensemble de tous les produits $a_1 \cdots a_n$ pour $a_1, \cdots, a_n \in A$. Soit $F = (G \setminus V) \cap V^2$. En tant qu'image d'un compact par une application continue, V^2 est compact (V est compact en tant que fermé dans un compact donc $V \times V$ est compact).
Donc, V^2 est fermé et comme V est ouvert, F est fermé dans un compact donc F est compact.
Soit $x \in V$. Comme $x \in G \setminus F$ par continuité de la multiplication, il existe un voisinage V_x de x et un voisinage S_x de e tels que $V_x \subset V$ et $S_x \subset V$ avec $V_x S_x \subset G \setminus F$.
Par compacité de V, il existe un nombre fini de x_i tels que les V_{x_i} recouvrent V. Notons S l'intersection des S_{x_i}.
Alors, $W = S \cup S^{-1}$ est un voisinage symétrique (si $w \in W$, alors $w^{-1} \in W$) de e, $W \subset V$ et $VW \subset G \setminus F$.
Ainsi, $VW \cap F = \emptyset$. Mais $VW \subset V^2$ car $W \subset V$ donc $VW \cap (G \setminus V) = \emptyset$. Donc, $VW \subset V$.
On en déduit que $\forall n \in \mathbb{N}, VW^n \subset V$. Notons R la réunion des W^n pour $n \in \mathbb{N}$.
Comme W est symétrique, R est un sous-groupe ouvert de G, contenu dans V (car V contient l'élément neutre).

PROPOSITION 1.4.3 Soit G un groupe compact et totalement discontinu. Alors G est un groupe profini.

PREUVE : Par la proposition 1.4.2, les sous-groupes ouverts de G forment une base de voisinages de e, et ces sous-groupes sont d'indice fini par la proposition 1.2.13.
Si U est un sous-groupe de G ouvert, les gU pour $g \in G$ sont en nombre fini, donc les gUg^{-1} pour $g \in G$ sont aussi en nombre fini. Ainsi, l'intersection notée V des gUg^{-1} pour $g \in G$ est un sous-groupe de G comme intersection de sous-groupes, V est ouvert car l'intersection est finie et par la proposition 1.2.2.
De plus, $U \subset V$ car $e \in G$ et V est normal dans G par construction.
En effet, si $v \in V$, alors $\exists g \in G, \exists u \in U$ tels que $v = gug^{-1}$. Ainsi, pour tout $x \in G$,

$$xvx^{-1} = xgug^{-1}x^{-1} = (xg)u(xg)^{-1} \in V.$$

Donc on dispose d'une base $\mathcal{N}$ de voisinages de e formée de sous-groupes normaux ouverts d'indice fini de G.
On va donner à $\mathcal{N}$ une structure d'ensemble ordonné filtrant. Si V et W sont deux éléments de $\mathcal{N}$, on notera $W \lesssim V$ lorsque V est un sous-groupe de W. Notons que la relation $\lesssim$ est bien une relation d'ordre, et que cet ordre est filtrant. En effet, si V et W sont deux éléments de $\mathcal{N}$, alors $V \lesssim V \cap W$ et $W \lesssim V \cap W$ avec $V \cap W$ un sous-groupe ouvert normal dans G.
Pour tout $(V, W) \in \mathcal{N}^2$ tel que $W \lesssim V$, on pose $\varphi_{V,W} : G/V \to G/W$ l'application qui associe gW à gV pour tout $g \in G$. Vérifions que $\varphi_{V,W}$ est bien définie. Si $gV = g'V$, alors $\exists v \in V, g' = gv$ et donc $g'W = gvW = gW$ car $V \subset W$ par hypothèse. Ainsi, $\varphi_{V,W}$ est bien définie. De plus, les G/V pour $V \in \mathcal{N}$ sont bien des groupes topologiques. Ensuite, on voit facilement que les $\varphi_{V,W}$ sont des morphismes de groupes.
Montrons qu'ils sont continus. On remarque que si on note $\pi_V : G \to G/V$ et $\pi_W : G \to G/W$ les projections canoniques, on a $\pi_W = \varphi_{V,W} \circ \pi_V$. Ainsi, si O est un ouvert de G/W, $\pi_W^{-1}(O)$ est un ouvert par la proposition 1.2.11, et donc $\pi_V(\pi_W^{-1}(O))$ est encore un ouvert par la proposition 1.2.11. Mais $\pi_V(\pi_W^{-1}(O)) = \varphi_{V,W}^{-1}(O)$ car si $\varphi_{V,W}(gV) \in O$, c'est que $gW \in O$ donc que $gV \in \pi_V(\pi_W^{-1}(O))$ et inversement, si $gV \in \pi_V(\pi_W^{-1}(O))$, alors $\varphi_{V,W}(gV) = gW \in O$ et $gV \in \varphi_{V,W}^{-1}(O)$. Donc, $\varphi_{V,W}$ est continue.
Enfin, on remarque que si $X \lesssim W \lesssim V$, alors on a bien $\varphi_{V,X} = \varphi_{W,X} \circ \varphi_{V,W}$.
Donc, $(G/V, \varphi_{V,W}, \mathcal{N})$ est un système projectif de groupes topologiques finis. Ainsi, $\varprojlim_{V \in \mathcal{N}} G/V$ est profini.
Montrons que G est isomorphe à $\varprojlim_{V \in \mathcal{N}} G/V$. On aura bien montré que G est profini.

Pour tout $V \in \mathcal{N}$, on dispose d'un morphisme continu surjectif π_V. On a remarqué plus tôt que les π_V étaient des morphismes compatibles. Ainsi, on dispose d'un morphisme continu surjectif $\pi : G \to \varprojlim_{V \in \mathcal{N}} G/V$.
Montrons que π est injectif. Soit $(g, g') \in G^2$ tel que $g \neq g'$.
Comme G est totalement discontinu, il existe un voisinage ouvert et fermé U de g tel que $g' \notin U$.
Montrons que $\pi(g) \neq \pi(g')$. Supposons que $\pi(g) = \pi(g')$. On a alors $\forall V \in \mathcal{N}$, $gV = gV'$.
Par la proposition 1.2.4, les gV forment une base de voisinages de g. Ainsi, il existe un voisinage V de e tel que $gV \subset U$ car U est un voisinage ouvert de g. Donc, $g'V \subset U$ avec $g'V$ un voisinage de g' par la proposition 1.2.4.
C'est absurde car $g' \notin U$ et $e \in V$. Finalement, $\exists V \in \mathcal{N}$, $gV \neq gV'$ et $\pi(g) \neq \pi(g')$.
Le groupe G est donc bien isomorphe de façon continue à un groupe profini.

On a donc montré le théorème suivant.

THÉORÈME 1.4.1 Soit G un groupe topologique.
Le groupe G est profini si et seulement si il est compact et totalement discontinu.

PREUVE : On a déjà fait les deux implications dans les propositions 1.4.1 et 1.4.3.

On peut maintenant montrer sans difficulté la proposition qui suit.

PROPOSITION 1.4.4 Soit G un groupe profini. Soit H un sous-groupe fermé de G. Alors, H est profini.

PREUVE : Comme G est profini, il est compact et totalement discontinu par la proposition 1.4.1.
Le groupe H est fermé dans un compact donc est compact, et c'est une partie d'un groupe totalement discontinu donc H est aussi totalement discontinu par la proposition 1.1.7.
Ainsi, par la proposition 1.4.3, H est profini.

Le groupe profini que l'on a construit dans la preuve de la proposition 1.4.3 est le complété profini de G. On a donc prouvé que dans le cas où G est compact et totalement discontinu, G est isomorphe à son complété profini.

DÉFINITION Soit G un groupe.
Le **complété profini** de G est la limite projective des G/V pour V un sous-groupe normal d'indice fini de G.
On note $\hat{G}$ le complété profini de G.

EXEMPLE : Tous les sous-groupes de $\mathbb{Z}$ différents de $\{0\}$ sont normaux et d'indice fini. Ainsi, on a

$$\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}^*} \mathbb{Z}/n\mathbb{Z}$$

avec la relation de divisibilité sur les entiers naturels non nuls n. On peut donc identifier $\hat{\mathbb{Z}}$ de la façon suivante.

$$\hat{\mathbb{Z}} = \{(x_n)_{n \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \mid \forall (m, n) \in \mathbb{N}^2, m \mid n, x_n \equiv x_m \ [m]\}.$$

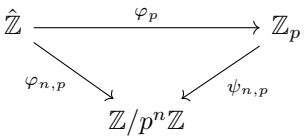
DÉFINITION Soit G un groupe. Soit p un nombre premier.
Le **complété pro-p** de G est la limite projective des G/V pour V un sous-groupe normal de G qui est d'indice fini égal à une puissance de p.

Les groupes $\mathbb{Z}_p$ construits en 1.3 sont les complétés pro-p de $\mathbb{Z}$. On a une relation entre $\hat{\mathbb{Z}}$ et les $\mathbb{Z}_p$.

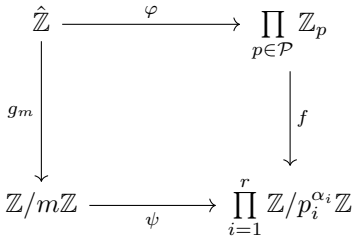
PROPOSITION 1.4.5 Notons $\mathcal{P}$ l'ensemble des nombres premiers. Alors, on a l'isomorphisme de groupes

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

PREUVE : Soit $p \in \mathcal{P}$. On commence par remarquer qu'on dispose de morphismes de groupes continus compatibles $g_n : \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ pour tout $n \in \mathbb{N}$ donc on dispose des morphismes de groupes continus $\varphi_{n,p} : \hat{\mathbb{Z}} \to \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \in \mathbb{N}$. Par la propriété universelle des groupes profinis, il existe un unique morphisme de groupes continu $\varphi_p : \hat{\mathbb{Z}} \to \mathbb{Z}_p$ tel que pour tout $n \in \mathbb{N}$, le diagramme suivant commute.



Les φ_p pour $p \in \mathcal{P}$ induisent un morphisme de groupes continu $\varphi : \hat{\mathbb{Z}} \to \prod_{p\in\mathcal{P}} \mathbb{Z}_p$. Montrons que φ est bijectif.
On va d'abord montrer que φ est surjectif. Pour cela, on remarque que $\hat{\mathbb{Z}}$ est compact car profini par la proposition 1.4.1, et donc que $\mathrm{Im}(\varphi)$ est fermée dans $\prod_{p\in\mathcal{P}} \mathbb{Z}_p$ car φ est continue.
Pour montrer que φ est surjective, il suffit donc de montrer que $\mathrm{Im}(\varphi)$ est dense dans $\prod_{p\in\mathcal{P}} \mathbb{Z}_p$.
On se donne donc un ouvert fondamental O de $\prod_{p\in\mathcal{P}} \mathbb{Z}_p$, et on cherche à montrer que $\mathrm{Im}(\varphi) \cap O \neq \emptyset$.
Par définition de la topologie produit, l'ouvert O s'écrit sous la forme $f^{-1}(x_1, \cdots, x_r)$ où $f : \prod_{p\in\mathcal{P}} \mathbb{Z}_p \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ est la projection avec p_i des nombres premiers et α_i des entiers naturels non nuls.
Si $m \in \mathbb{N}^* \setminus \{1\}$ s'écrit $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors on va montrer que le diagramme suivant commute.



Notons d'abord ψ est un isomorphisme par le lemme chinois. Soit $x \in \hat{\mathbb{Z}}$. Montrons que $\psi(g_m(x)) = f(\varphi(x))$.
D'une part, l'élément $g_m(x)$ de $\mathbb{Z}/m\mathbb{Z}$ correspond à la m-ième coordonnée de x et donc l'image par ψ de cet élément est la décomposition de la m-ième coordonée de x selon les $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.
D'autre part, l'image par φ de x est la projection de x dans tous les $\mathbb{Z}/p^n\mathbb{Z}$ et l'image par f de $\varphi(x)$ est la restriction de la projection de x dans les $\mathbb{Z}/p^n\mathbb{Z}$ aux $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.
Vu la décomposition en produit de facteurs premiers de m, le diagramme est bien commutatif.
Mais comme $\mathrm{Im}(f \circ \varphi) \neq \emptyset$ et comme le diagramme commute, si $(x_1, \cdots, x_r) \in \mathrm{Im}(f \circ \varphi)$, alors $\mathrm{Im}(\varphi) \cap f^{-1}(x_1, \cdots, x_r) \neq \emptyset$. Donc, φ est surjective.
Maintenant, φ est injective car si $x \in \hat{\mathbb{Z}} \setminus \{0\}$, alors $\exists m \in \mathbb{N}^* \setminus \{1\}$ tel que $g_m(x) \neq 0$ dans $\mathbb{Z}/m\mathbb{Z}$.
Ainsi, pour un tel m, on obtient $(f \circ \varphi)(x) \neq 0$ et donc $\varphi(x) \neq 0$. Le noyau de φ est réduit à l'élément neutre, donc φ est injectif. Finalement, φ est un isomorphisme continu.

PROPOSITION 1.4.6 Soit $n \in \mathbb{N}$. Soit p un nombre premier. Alors, $\mathbb{Z}/p^n\mathbb{Z}$ et $\mathbb{Z}_p/p^n\mathbb{Z}_p$ sont isomorphes.

PREUVE : On dispose d'un morphisme de projection $\psi_{n,p} : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ qui envoie un élément de $\mathbb{Z}_p$ sur sa coordonnée en $\mathbb{Z}/p^n\mathbb{Z}$. Ce morphisme est surjectif par définition, et on va montrer que son noyau est $p^n\mathbb{Z}_p$.
Tout d'abord, si $x \in p^n\mathbb{Z}_p$, alors la coordonnée de x en $\mathbb{Z}/p^n\mathbb{Z}$ vaut bien 0 et $x \in \ker(\psi_{n,p})$.
Inversement, si $x \in \ker(\psi_{n,p})$, alors sa coordonnée en $\mathbb{Z}/p^n\mathbb{Z}$ vaut 0, et donc par les relations de compatibilités, les coordonnées précédentes de x sont également nulles. Ainsi, $x \in p^n\mathbb{Z}_p$ et finalement, $\ker(\psi_{n,p}) = p^n\mathbb{Z}_p$.
Par le premier théorème d'isomorphisme appliqué à $\psi_{n,p}$, les groupes $\mathbb{Z}_p/p^n\mathbb{Z}_p$ et $\mathbb{Z}/p^n\mathbb{Z}$ sont isomorphes.

On donne un autre exemple, celui des séries formelles sur un corps fini.

PROPOSITION 1.4.7 Soit $q \in \mathbb{N}$. On suppose que $q = p^n$ avec p un nombre premier et $n \in \mathbb{N}^*$.
Alors, l'anneau des séries formelles $\mathbb{F}_q[[t]]$ sur le corps fini $\mathbb{F}_q$ est un groupe profini.

PREUVE : Pour tout $n \in \mathbb{N}^*$, le sous-groupe additif associé à l'idéal (t^n) de $\mathbb{F}_q[t]$ est normal d'indice fini car $\mathbb{F}_q$ est fini. On peut donc considérer la limite projective $\mathcal{F} = \varprojlim \mathbb{F}_q[t]/(t^n)$ qui est un groupe profini par définition.
Montrons que $\mathbb{F}_q[[t]]$ est isomorphe à $\mathcal{F}$. Si $\sum a_k t^k \in \mathbb{F}_q[[t]]$, on pose

$$\varphi\left(\sum a_k t^k\right) = \left(\sum_{k=0}^{n-1} a_k t^k \ [t^n]\right)_{n\in\mathbb{N}^*}.$$

De cette façon, φ est à valeurs dans $\mathcal{F}$ et est un morphisme de groupes additifs.
Dans l'autre sens, si $(P_k\ [t^k])_{k\in\mathbb{N}^*} \in \mathcal{F}$, on pose

$$\psi((P_k\ [t^k])_{k\in\mathbb{N}^*}) = \sum_{k=1}^{+\infty} \mathrm{coeff}_{k-1}(P_k)t^{k-1}$$

où pour tout $k \in \mathbb{N}^*$, $\mathrm{coeff}_{k-1}(P_k)$ est le coefficient de degré $k-1$ du polynôme P_k.
L'application ψ est à valeurs dans $\mathbb{F}_q[[t]]$ et est un morphisme de groupes additifs. De plus, si $(P_k\ [t^k])_{k\in\mathbb{N}^*} \in \mathcal{F}$,

$$\varphi \circ \psi((P_k\ [t^k])_{k\in\mathbb{N}}) = \varphi\left(\sum_{k=0}^{+\infty} \mathrm{coeff}_k(P_{k+1})t^k\right) = \left(\sum_{k=0}^{n-1} \mathrm{coeff}_k(P_{k+1})t^k\ [t^n]\right)_{n\in\mathbb{N}} = (P_k\ [t^k])_{k\in\mathbb{N}}$$

par les relations de compatibilités, et si $\sum a_k t^k \in \mathbb{F}_q[[t]]$,

$$\psi\left(\varphi\left(\sum a_k t^k\right)\right) = \psi\left(\left(\sum_{k=0}^{n-1} a_k t^k\ [t^n]\right)_{n\in\mathbb{N}}\right) = \sum_{k=1}^{+\infty} a_{k-1}t^{k-1} = \sum a_k t^k.$$

Ainsi, φ et ψ sont inverses l'une de l'autre et on a bien $\mathbb{F}_q[[t]] \cong \mathcal{F}$.
On remarque que cet isomorphisme est continu en considérant la topologie usuelle sur les séries formelles.

On montre maintenant une proposition qui servira à démontrer les théorèmes de Hall.

PROPOSITION 1.4.8 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes finis. Notons $G = \varprojlim G_i$.
Pour tout $i \in I$, on note $\varphi_i : G \to G_i$ le morphisme de projection sur la coordonnée i.
Alors, $(\ker(\varphi_i))_{i\in I}$ est une base de voisinages de l'élément neutre $e_G \in G$.

PREUVE : Par définition de la topologie produit, les voisinages de e_G la forme

$$V_{\{i_1,\cdots,i_n\}} = \left(\prod_{i\neq i_1,\cdots,i_n} G_i\right) \times \{e_{G_{i_1}}\} \times \cdots \times \{e_{G_{i_n}}\}$$

donnent une base de voisinages avec $\{i_1, \cdots, i_n\} \subset I$ où $n \in \mathbb{N}^*$. Mais en utilisant les relations de compatibilités, on remarque que si $i_1, \cdots, i_n \leqslant i_0$, on a

$$G \cap V_{\{i_1,\cdots,i_n\}} = G \cap \left(\left(\prod_{i\neq i_0} G_i\right) \times \{e_{G_{i_0}}\}\right).$$

Ainsi, les $\ker(\varphi_{i_0}) = G \cap V_{\{i_1,\cdots,i_n\}}$ forment bien une base de voisinages de e_G.

2 Théorie de Sylow dans les groupes profinis

2.1 Ordre d'un groupe profini

On commence par montrer qu'un groupe profini est soit fini, soit non dénombrable.
La présentation des théorèmes de Sylow pour les groupes profinis provient de la partie 2.3 de [RZ10].

PROPOSITION 2.1.1 Soit G un groupe profini. Alors, G est fini ou non dénombrable.

PREUVE : Si il existe $a \in G$ tel que $\{a\}$ est ouvert, alors par la proposition 1.2.2, tous les singletons sont ouverts. Or, par la proposition 1.4.1, G est compact donc on doit pouvoir extraire du recouvrement par les singletons un recouvrement fini et donc G est fini.
Supposons que G n'est pas fini. Par ce qui précède, tous les singletons sont d'intérieur vide.
Les singletons sont fermés car ce sont des composantes connexes (par la proposition 1.1.6) étant donné que G est totalement discontinu par la proposition 1.4.1.

Si G est dénombrable, alors il est réunion dénombrable de fermés d'intérieur vide.
Mais G est compact donc c'est un espace de Baire et G est d'intérieur vide.
On obtient une contradiction car G n'est pas vide.

Si un groupe profini est fini, les théorèmes de Sylow classiques s'y appliquent naturellement. Par contre, si un tel groupe est non dénombrable, on veut définir les sous-groupes de Sylow et avoir un énoncé qui se rapproche des théorèmes de Sylow dans le cas fini. On définit pour cela la notion de nombre surnaturel.
Dans ce qui va suivre, on note $\mathcal{P}$ l'ensemble des nombres premiers.

Définition Un **nombre surnaturel** est une suite d'éléments de $\mathbb{N} \cup \{\infty\}$ indexée par l'ensemble $\mathcal{P}$.
Si $n = (k_p)_{p\in\mathcal{P}} \in (\mathbb{N} \cup \{\infty\})^{\mathcal{P}}$, on notera plutôt n sous la forme du produit formel suivant

$$n = \prod_{p\in\mathcal{P}} p^{k_p}.$$

On note $\mathcal{S}$ l'ensemble des nombres surnaturels.

On étend l'addition et l'ordre de $\mathbb{N}$ à $\mathbb{N} \cup \{+\infty\}$ en posant $\forall n \in \mathbb{N}$, $n < \infty$, $\infty + \infty = \infty$ et $\infty + n = n + \infty = \infty$.

Définition Soit $(n, m) \in \mathcal{S}$. On suppose que n et m s'écrivent respectivement

$$n = \prod_{p\in\mathcal{P}} p^{n(p)} \quad \text{et} \quad m = \prod_{p\in\mathcal{P}} p^{m(p)}.$$

On dit que m **divise** n et on note $m \mid n$ lorsque pour tout $p \in \mathcal{P}$, $m(p) \leqslant n(p)$.

On s'attend à ce que la relation divise soit une relation d'ordre.

Proposition 2.1.2 La relation de divisibilité sur l'ensemble $\mathcal{S}$ est une relation d'ordre.

Preuve : Tout provient du fait que la relation $\leqslant$ est une relation d'ordre sur $\mathbb{N} \cup \{\infty\}$.

À défaut de pouvoir définir une addition raisonnable sur $\mathcal{S}$, on généralise facilement et de façon naturelle le produit, le plus grand commun diviseur et le plus petit commun multiple d'une famille de nombres surnaturels.

Définition Soit $(n_i)_{i\in I}$ une famille d'éléments de $\mathcal{S}$ qui s'écrivent

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

Le **produit** des n_i pour $i \in I$ est le nombre surnaturel

$$\prod_{i\in I} n_i = \prod_{p\in\mathcal{P}} p^{n(p)} \quad \text{avec} \quad \forall p \in \mathcal{P}, n(p) = \sum_{i\in I} n(p, i).$$

Le **plus grand commun diviseur** des n_i pour $i \in I$ est le nombre surnaturel

$$\operatorname{pgcd}((n_i)_{i\in I}) = \prod_{p\in\mathcal{P}} p^{n(p)} \quad \text{avec} \quad \forall p \in \mathcal{P}, n(p) = \inf_{i\in I} n(p, i).$$

Le **plus petit commun multiple** des n_i pour $i \in I$ est le nombre surnaturel

$$\operatorname{ppcm}((n_i)_{i\in I}) = \prod_{p\in\mathcal{P}} p^{n(p)} \quad \text{avec} \quad \forall p \in \mathcal{P}, n(p) = \sup_{i\in I} n(p, i).$$

On peut maintenant définir l'indice d'un sous-groupe fermé d'un groupe profini.
Remarquons que par la proposition 1.4.4, un tel sous-groupe est également profini.

Définition Soit G un groupe profini. Soit H un sous-groupe fermé de G.
Notons $\mathcal{N}$ l'ensemble des sous-groupes ouverts et normaux de G. L'**indice** de H dans G est

$$[G : H] = \text{ppcm}(([G/N : HN/N])_{N\in\mathcal{N}}) \in \mathcal{S}.$$

L'**ordre** de G est $[G : \{e\}]$ et se réécrit $\text{ppcm}((|G/N|)_{N\in\mathcal{N}})$ (notons que le sous-groupe $\{e\}$ est fermé par les propositions 1.1.10 et 1.4.1). On le note $\#G$.

Remarque : La proposition 1.2.13 assure que notre définition de l'indice d'un sous-groupe fermé d'un groupe profini fait intervenir un ppcm d'entiers naturels.

Proposition 2.1.3 Soit G un groupe profini. Soit H un sous-groupe fermé de G.
Notons $\mathcal{N}'$ une base de voisinages de e_G qui sont des sous-groupes ouverts et normaux de G. Alors,

$$[G : H] = \text{ppcm}(([G/N : HN/N])_{N\in\mathcal{N}'}).$$

On peut donc se restreindre à une base de voisinages de e_G qui sont des sous-groupes ouverts et normaux.

Preuve : Tout d'abord, comme $\mathcal{N}' \subset \mathcal{N}$, on a l'inégalité

$$\text{ppcm}(([G/N : HN/N])_{N\in\mathcal{N}'}) \leqslant [G : H].$$

Pour montrer l'autre inégalité, il suffit de prouver que si $N \in \mathcal{N}$, il existe $N' \in \mathcal{N}'$ tel que $N' \subset N$.
Mais c'est bien sûr le cas par définition d'une base de voisinages, et on a bien l'égalité annoncée.

La formule des indices est toujours vraie dans le cadre des groupes profinis.

Proposition 2.1.4 Soient G un groupe profini. Soient H un sous-groupe de G et K un sous-groupe de H.
On suppose que H est fermé dans G et que K est fermé dans H. Alors, $[G : K] = [G : H][H : K]$.

Preuve : La formule des indices est toujours vraie dans le cas fini donc

$$[G : K] = \text{ppcm}(([G/N : KN/N])_{N\in\mathcal{N}}) = \text{ppcm}(([G/N : HN/N][HN/N : KN/N])_{N\in\mathcal{N}}).$$

Or, la famille des $H \cap N$ pour $N \in \mathcal{N}$ est un système fondamental de voisinages de e dans H donc par la proposition 2.1.3,

$$[H : K] = \text{ppcm}(([H/(H \cap N) : K(H \cap N)/(H \cap N)])_{N\in\mathcal{N}})$$

et donc par le deuxième théorème d'isomorphisme, on obtient

$$[H : K] = \text{ppcm}(([HN/N : KN/N])_{N\in\mathcal{N}}).$$

Vu l'égalité qui provient de la formule des indices du cas fini, il suffit de montrer que

$$\text{ppcm}(([G/N : HN/N][HN/N : KN/N])_{N\in\mathcal{N}}) = \text{ppcm}(([G/N : HN/N])_{N\in\mathcal{N}})\text{ppcm}(([HN/N : KN/N])_{N\in\mathcal{N}}).$$

Soit p un nombre premier. Notons n, n_1 et n_2 les plus grands entiers naturels tels que

$$p^n \mid \text{ppcm}(([G/N : HN/N][HN/N : KN/N])_{N\in\mathcal{N}}),$$

$$p^{n_1} \mid \text{ppcm}(([G/N : HN/N])_{N\in\mathcal{N}}) \text{ et } p^{n_2} \mid \text{ppcm}(([HN/N : KN/N])_{N\in\mathcal{N}}).$$

Montrons que $n = n_1 + n_2$. On aura bien fini par définition du ppcm et du produit de nombres surnaturels.
Tout d'abord, par définition de n_1 et n_2, $n \leqslant n_1 + n_2$, $n \geqslant n_1$ et $n \geqslant n_2$. Ainsi, si $n = \infty$, l'égalité est vraie et si $n \neq \infty$, alors $n_1 \neq \infty$ et $n_2 \neq \infty$. On se place donc dans le cas où $n \neq \infty$ et on veut montrer que $n \geqslant n_1 + n_2$.
On a l'existence de $N_1, N_2 \in \mathcal{N}$ tels que $p^{n_1} \mid [G/N_1 : HN_1/N_1]$ et $p^{n_2} \mid [G/N_2 : HN_2/N_2]$.
En posant $N = N_1 \cap N_2$, on remarque que $N \in \mathcal{N}$ et que

$$p^{n_1+n_2} \mid [G/N : HN/N][HN/N : KN/N]$$

étant donné que $N_1 \subset N$ et que $N_2 \subset N$. Donc, par définition de n, $n \geqslant n_1 + n_2$ et on a bien montré l'égalité.

La propriété suivante permet de calculer l'ordre d'un groupe profini en pratique.

PROPOSITION 2.1.5 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes finis. Notons $G = \varprojlim G_i$.
On suppose que les $\varphi_{i,j}$ sont surjectifs. Alors, G est un groupe profini et $\#G = \text{ppcm}((\#G_i)_{i\in I})$.

PREUVE : Pour tout $i \in I$, on pose $G_i' = \ker(\varphi_i)$ où $\varphi_i : G \to G_i$ est la projection canonique.
Le premier théorème d'isomorphisme et la proposition 1.3.11 permettent d'assurer que $\forall i \in I, \#G_i = \#G/G_i'$.
Montrons que $\#G = \text{ppcm}((\#G/G_i')_{i\in I})$. On aura fini d'après la remarque que l'on vient de faire.
Comme les G_i sont tous finis, les propositions 1.4.8 et 2.1.3 permettent de conclure.

EXEMPLE : Si $p \in \mathcal{P}$, alors $\#\mathbb{Z}_p = p^\infty$ en utilisant la définition de $\mathbb{Z}_p$ et la proposition 2.1.5.

2.2 Sous-groupes de Hall d'un groupe profini

DÉFINITION Soit $\pi \subset \mathcal{P}$ un ensemble de nombres premiers. Notons π' l'ensemble $\mathcal{P} \setminus \pi$.
Soit $n \in \mathcal{S}$. On suppose que n s'écrit

$$n = \prod_{p\in\mathcal{P}} p^{n(p)}.$$

On dit que n est un **π-nombre** lorsque π contient au moins tous les $p \in \mathcal{P}$ tels que $n(p) \neq 0$.

EXEMPLE : Le nombre $2^\infty 3^{16} 7^{94}$ est un $\{2,3,7\}$-nombre, mais aussi un $\{2,3,5,7,11\}$-nombre.

DÉFINITION Soit G un groupe profini. Soit $\pi \subset \mathcal{P}$.
On dit que G est un **groupe pro-π** ou un **π-groupe** lorsque le nombre surnaturel $\#G$ est un π-nombre.
Si π ne contient qu'un seul nombre premier p, on dira **groupe pro-p** plutôt que groupe pro-$\{p\}$.

EXEMPLE : Soit p un nombre premier. Le groupe $\mathbb{Z}_p$ est un groupe pro-p car $\#\mathbb{Z}_p = p^\infty$.

PROPOSITION 2.2.1 Soit G un groupe. Soit $p \in \mathcal{P}$. Alors, le complété pro-p de G est un pro-p groupe.

PREUVE : Par définition du complété pro-p et de l'ordre d'un groupe profini, l'ordre de G est un ppcm de puissances de p. C'est donc une puissance de p et le complété pro-p de G est un bien un pro-p groupe.

Nous allons maintenant définir les π-sous-groupes de Hall des groupes profinis.

DÉFINITION Soit G un groupe profini. Soit H un sous-groupe fermé de G. Soit $\pi \subset \mathcal{P}$. Posons $\pi' = \mathcal{P} \setminus \pi$.
On dit que le groupe profini H est un **π-sous-groupe de Hall** de G lorsque H est un groupe pro-π et que l'indice $[G : H]$ est un π'-nombre.

REMARQUE : Dans la suite, on écrira π-Hall plutôt que π-sous-groupe de Hall. C'est le même raccourci que quand on se permet de parle de p-Sylow d'un groupe fini.

PROPOSITION 2.2.2 Soit $\pi \subset \mathcal{P}$. Soient G et G' deux groupes profinis.
Soit $\varphi : G \to G'$ un morphisme de groupes continu. Soit H un sous-groupe fermé de G. Alors,

1. Si H est un π-groupe, alors $\varphi(H)$ est un π-groupe.
2. Si H est un π-Hall de G, alors $\varphi(H)$ est un π-Hall de $\varphi(G)$.

PREUVE : On utilise le premier point dans la preuve du second point.

1. Supposons que H est un π-groupe. Montrons que $\#\varphi(H)$ est un π-nombre.
   On introduit pour cela l'application $\psi : H \to G'$ défini par $\forall h \in H, \psi(h) = \varphi(h)$.
   Comme φ est un morphisme continu, ψ est un morphisme continu aussi.
   Le premier théorème d'isomorphisme assure alors que $H/\ker(\psi)$ et $\psi(H)$ sont isomorphes.
   Mais $\psi(H) = \varphi(H)$ par construction de ψ et donc $\#H/\ker(\psi) = \#\varphi(H)$.

Or, la proposition 2.1.4 fournit l'égalité

$$\#H = [H : \{e_G\}] = [H : \ker(\psi)][\ker(\psi) : \{e_G\}] = [H : \ker(\psi)]\#\ker(\psi)$$

en remarquant que le groupe $\ker(\psi)$ est fermé comme image réciproque du fermé $\{e_{G'}\}$ par l'application continue ψ (on a utilisé les propositions 1.2.5 et 1.4.1).
On montre aisément que $\#H/\ker(\psi) = [H : \ker(\psi)]$ par définition de $[H : \ker(\psi)]$.
On a donc prouvé l'égalité suivante

$$\#H = \#(H/\ker(\psi))\#\ker(\psi) = \#\varphi(H)\#\ker(\psi).$$

Ainsi, si $p \in \mathcal{P}$ est tel que la puissance de p qui apparaît dans le produit formel $\#\varphi(H)$ notée $\#\varphi(H)(p)$ est non nulle, alors cette puissance est également non nulle dans $\#H$ et comme $\#H$ est un π-nombre, $p \in \pi$. Cela prouve que $\#\varphi(H)$ est un π-nombre et que $\varphi(H)$ est un π-groupe.

2. Tout d'abord, comme H est un π-Hall de G, $\varphi(H)$ est un π-groupe par le premier point.
Montrons que $[\varphi(G) : \varphi(H)]$ est un π' nombre où on a posé $\pi' = \mathcal{P} \setminus \pi$.
Tout d'abord, $\varphi(H)$ est un sous-groupe fermé de $\varphi(G)$ car H est compact et φ est continue. Donc

$$\#\varphi(G) = [\varphi(G) : \varphi(H)]\#\varphi(H)$$

en utilisant la proposition 2.1.4. On peut multiplier par $\#\ker(\varphi)$ pour obtenir

$$\#\varphi(G)\#\ker(\varphi) = [\varphi(G) : \varphi(H)]\#\varphi(H)\#\ker(\varphi).$$

Mais par le premier théorème d'isomorphisme, $\#G = \#\varphi(G)\#\ker(\varphi)$ donc

$$\#G = [\varphi(G) : \varphi(H)]\#\varphi(H)\#\ker(\varphi).$$

Or, $\#G = [G : H]\#H$ par la proposition 2.1.4 donc

$$[G : H]\#H = [\varphi(G) : \varphi(H)]\#\varphi(H)\#\ker(\varphi).$$

Mais en notant ψ la restriction de φ à H, le premier théorème d'isomorphisme nous fournit $\#H = \#\varphi(H)\#\ker(\psi)$ et la proposition 2.1.4 donne également $\#\ker(\varphi) = [\ker(\varphi) : \ker(\psi)]\#\ker(\psi)$ donc

$$[G : H]\#\varphi(H)\#\ker(\psi) = [\varphi(G) : \varphi(H)]\#\varphi(H)[\ker(\varphi) : \ker(\psi)]\#\ker(\psi).$$

Les simplifications étant possibles dans $\mathbb{N}$, en passant à la limite pour obtenir des nombres surnaturels, on obtient

$$[G : H] = [\varphi(G) : \varphi(H)][\ker(\varphi) : \ker(\psi)].$$

Ainsi, si $p \in \mathcal{P}$ est tel que la puissance de p qui apparaît dans le produit formel $[\varphi(G) : \varphi(H)]$ est non nulle, alors cette puissance est également non nulle dans le produit formel de $[G : H]$.
Mais H est un π-Hall de G donc $[G : H]$ est un π'-nombre et donc $p \in \pi'$.
Ainsi, $[\varphi(G) : \varphi(H)]$ est un π'-nombre. Finalement, $\varphi(H)$ est un π-Hall de $\varphi(G)$.

On montre une dernière proposition qui nous servira pour prouver le théorème de Hall.

PROPOSITION 2.2.3 Soit G un groupe profini. Soit H un sous-groupe fermé de G. Soit $\pi \subset \mathcal{P}$.
On suppose que G est la limite projective des G_i avec $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes finis tel que les $\varphi_{i,j}$ sont surjectifs. Pour tout $i \in I$, notons $\varphi_i : G \to G_i$ la projection canonique.
Alors, H est un π-Hall de G si et seulement si $\forall i \in I, \varphi_i(H)$ est un π-Hall de G_i.

PREUVE : Par la proposition 1.3.9, on a l'isomorphisme suivant

$$H \cong \varprojlim \varphi_i(H).$$

Ainsi, par les propositions 2.1.5 et 2.2.2, H est un π-groupe si et seulement si $\forall i \in I$, $\varphi_i(H)$ est un π-groupe.
En notant $\pi' = \mathcal{P} \setminus \pi$, on va montrer que $[G : H]$ est un π'-nombre si et seulement si $\forall i \in I$, $[G_i : \varphi_i(H)]$ est un π'-nombre. On aura fini en utilisant ce qu'on vient de montrer sur les π-groupes.
Tout d'abord, par la proposition 1.4.8, en notant $S_i = \ker(\varphi_i)$ pour $i \in I$, les S_i forment une base de voisinages

de l'élément neutre de G. Ces voisinages sont ouverts car ce sont des images réciproques des singletons $\{e_{G_i}\}$ (qui sont ouverts car G_i est fini et muni de la topologie discrète) par des applications continues.
Ainsi, par la proposition 2.1.3, on a l'égalité suivante

$$[G : H] = \text{ppcm}(([G/S_i : HS_i/S_i])_{i\in I}).$$

Les φ_i sont surjectifs en vertu de la proposition 1.3.11, donc par le premier théorème d'isomorphisme, si $i \in I$,

$$[G/S_i : HS_i/S_i] = [G_i : \varphi_i(H)].$$

Cela montre que $[G : H]$ est un π'-nombre si et seulement si $\forall i \in I$, $[G_i : \varphi_i(H)]$ est un π'-nombre.

Avant de prouver le théorème de Hall dans le cadre des groupes profinis, nous allons expliciter la définition des sous-groupes de Hall dans le cas fini. Dans ce cas plus simple, il n'est pas question de nombre surnaturel.

DÉFINITION Soit G un groupe fini. Soit H un sous-groupe de G. Soit $\pi \subset \mathcal{P}$.
On dit que H est un **π-sous-groupe de Hall** de G lorsque les nombres premiers qui divisent l'ordre de H sont des éléments de π et que l'ordre de H est premier avec l'indice de H dans G.

REMARQUE : Cette définition n'est qu'une adaptation au cas fini de la définition donnée précédemment.

2.3 Théorème de Hall pour les groupes profinis

Le théorème qui suit nous permet dans la suite de généraliser les théorèmes de Sylow au cas profini.

THÉORÈME 2.3.1 Soit $(G_i, \varphi_{i,j}, I)$ un système projectif de groupes finis tel que les $\varphi_{i,j}$ sont surjectifs.
Soit $\pi \subset \mathcal{P}$. On note G la limite projective des G_i. On suppose que pour tout $i \in I$,

a. G_i contient un π-Hall.

b. Tout π-sous-groupe de G_i est contenu dans un π-Hall.

c. Deux π-Hall de G_i sont conjugués.

Alors,

1. G contient un π-Hall.
2. Tout π-sous-groupe de G est contenu dans un π-Hall.
3. Deux π-Hall de G sont conjugués.

PREUVE : La stratégie est similaire pour les trois points.

1. Pour tout $i \in I$, notons $\mathcal{H}_i$ l'ensemble des π-Hall de G_i. Par l'hypothèse a., les $\mathcal{H}_i$ sont tous non vides.
Soient $i, j \in I$ tels que $j \leqslant i$. Montrons que $\varphi_{i,j}(\mathcal{H}_i) \subset \mathcal{H}_j$.
Si $H_i \in \mathcal{H}_i$, la proposition 2.2.2 assure que $\varphi_{i,j}(H_i)$ est un π-Hall de $\varphi_{i,j}(G_i)$, avec $\varphi_{i,j}(G_i) = G_j$ par surjectivité. Ainsi, $\varphi_{i,j}(H_i)$ est un π-Hall de G_j comme voulu.
On dispose donc d'un système projectif $(\mathcal{H}_i, \varphi_{i,j}, I)$ d'espaces topologiques non vides et finis (sous-groupes d'un groupe fini). Ces espaces topologiques munis de la topologie discrète sont finis donc compacts ; donc par la proposition 1.3.6, la limite projective des $\mathcal{H}_i$ est non vide. Notons $\mathcal{H}$ cette limite.
Si $(H_i)_{i\in I} \in \mathcal{H}$, la proposition 2.2.3 assure que $\varprojlim H_i$ est un π-Hall de G.
2. Soit H un π-sous-groupe de G. Si $i \in I$, $\varphi_i(H)$ est un π-sous-groupe de G_i par la proposition 2.2.2.
Pour tout $i \in I$, on pose $\mathcal{S}_i$ l'ensemble des π-Hall de G_i qui contiennent $\varphi_i(H)$.
L'hypothèse b. assure que $\forall i \in I, \mathcal{S}_i \neq \emptyset$. Soient $i, j \in I$ tels que $j \leqslant i$. Montrons que $\varphi_{i,j}(\mathcal{S}_i) \subset \mathcal{S}_j$.
Si S_i est un π-Hall de G_i qui contient $\varphi_i(H)$. Par la proposition 2.2.2, $\varphi_{i,j}(S_i)$ est un π-Hall de $\varphi_{i,j}(G_i) = G_j$ par surjectivité. De plus, comme S_i contient $\varphi_i(H)$, $\varphi_{i,j}(S_i)$ contient $\varphi_{i,j}(\varphi_i(H)) = \varphi_j(H)$ par compatibilité. Ainsi, $\varphi_{i,j}(S_i) \in \mathcal{S}_j$ comme voulu.
On a donc un système projectif $(\mathcal{S}_i, \varphi_{i,j}, I)$ d'espaces topologiques compacts et non vides par le même argument que dans la preuve du 1. et donc la limite projective des $\mathcal{S}_i$, notée $\mathcal{S}'$ pour éviter la confusion avec l'ensemble $\mathcal{S}$ des nombres surnaturels, est non vide par la proposition 1.3.6.
Soit $(S_i)_{i\in I} \in \mathcal{S}'$. Par construction, $H = \varprojlim \varphi_i(H)$ est un sous-groupe de la limite projective des S_i et cette limite projective est un π-Hall de G par la proposition 2.2.3.

3. Soient H et K deux π-Hall de G. Par la proposition 2.2.3, si $i \in I$, $\varphi_i(H)$ et $\varphi_i(K)$ sont des π-Hall de G_i. Ainsi, si $i \in I$, en posant $Q_i = \{q_i \in G_i, q_i^{-1}\varphi_i(H)q_i = \varphi_i(K)\}$, l'hypothèse c. assure que $Q_i \neq \emptyset$.
Soient $i, j \in I$ tels que $j \leqslant i$. Montrons que $\varphi_{i,j}(Q_i) \subset Q_j$. Si $q_i \in Q_i$, alors

$$\varphi_{i,j}(q_i)^{-1}(\varphi_{i,j} \circ \varphi_i)(H)\varphi_{i,j}(q_i) = (\varphi_{i,j} \circ \varphi_i)(K)$$

et donc $\varphi_{i,j}(q_i) \in Q_j$ par compatibilité. Ainsi, $(Q_i, \varphi_{i,j}, I)$ est un système projectif d'espaces topologiques compacts et non vides. Par la proposition 1.3.6, la limite projective des Q_i notée Q est non vide.
Enfin, par construction, si $q \in Q$, on a bien $q^{-1}Hq = K$ et H et K sont conjugués.

C'est à l'aide de ce théorème 2.3.1 que l'on va prouver les théorèmes de Sylow. On aurait pu montrer ces théorèmes directement comme dans [Ser94] mais le théorème de Hall est plus général et permet de montrer notamment un résultat sur les groupes résolubles finis.

2.4 Application aux théorèmes de Sylow

Commencons par définir les sous-groupes de Sylow d'un groupe profini de la façon la plus naturelle possible.

DÉFINITION Soit G un groupe profini. Soit H un sous-groupe de G. Soit $p \in \mathcal{P}$.
On dit que H est un **p-sous-groupe de Sylow** de G lorsque H est un $\{p\}$-sous-groupe de Hall de G.

REMARQUE : Cette définition correspond bien à la définition que l'on connaît déjà dans le cas fini.
EXEMPLE : Si p un nombre premier, on déduit de la proposition 1.4.5 que $\hat{\mathbb{Z}}$ admet un p-sous-groupe de Sylow isomorphe à $\mathbb{Z}_p$.
REMARQUE : Comme dans le cas fini, on se permet de parler de p-Sylow plutôt que de p-sous-groupe de Sylow.

THÉORÈME 2.4.1 Soit G un groupe profini. Soit p un nombre premier. Alors,

1. G contient un p-Sylow.
2. Tout sous-groupe fermé de G est contenu dans un p-Sylow.
3. Les p-Sylow de G sont conjugués.

PREUVE : Le groupe G est profini donc il s'écrit $\varprojlim G_i$ où $(G_i, \varphi_{i,j}, I)$ est un système projectif de groupes finis.
Si G est fini, le résultat est bien connu. Sinon, les projections $G \to G_i$ sont surjectives.
Ainsi, si $(i, j) \in I^2$ vérifie $j \leqslant i$, comme $\varphi_{i,j} \circ \varphi_i = \varphi_j$, si $g_j \in G_j, \exists g \in G, \varphi_j(g) = g_j$ et donc $\varphi_{i,j}(\varphi_i(g)) = g_j$.
On a donc montré que les $\varphi_{i,j}$ sont surjectifs.
Enfin, les théorèmes de Sylow étant vérifiés pour tous les G_i, le théorème 2.3.1 permet de conclure.

Insistons sur le fait qu'utiliser le théorème de Hall pour prouver les théorèmes de Sylow permet de raccourcir la preuve, mais que l'on peut tout à fait démontrer le résultat directement par des méthodes analogues à celles utilisées dans la preuve du théorème 2.3.1.

3 Exemples

3.1 Le groupe multiplicatif de l'anneau des entiers p-adiques

Dans cette partie, on fixe $p \in \mathcal{P}$ un nombre premier et on s'intéresse au groupe des inversibles des entiers p-adiques.

PROPOSITION 3.1.1 L'anneau des entiers p-adiques $\mathbb{Z}_p$ est intègre.

PREUVE : Bien entendu, $\mathbb{Z}_p$ n'est pas l'anneau nul (l'élément neutre additif est l'image de 0 par la projection $\mathbb{Z} \to \mathbb{Z}_p$ et l'élément neutre multiplicatif est l'image de 1 par cette projection).
Soient x et y deux éléments de $\mathbb{Z}_p$ qui sont non nuls. Comme x et y sont non nuls, ils ont une coordonnée non nulle et donc les suivantes sont non nulles par compatibilités. Ainsi, xy a également une coordonnée non nulle (en effet, la suite $(p^n)_{n\in\mathbb{N}}$ est strictement croissante donc on a bien la non nullité d'une coordonnée de xy quitte à regarder une coordonnée plus lointaine), ce qui prouve que $xy \neq 0$.

On donne maintenant la structure du groupe multiplicatif de $\mathbb{Z}_p$ noté $\mathbb{Z}_p^*$.

PROPOSITION 3.1.2 Le groupe des inversibles de $\mathbb{Z}_p$ vérifie $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

PREUVE : Tout d'abord, un élément $x \in \mathbb{Z}_p$ dont la première coordonnée est non nulle est inversible.
En effet, comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, la première coordonnée x_0 de x est inversible donc $\exists y_0 \in \mathbb{Z}/p\mathbb{Z}$ tel que $x_0 y_0 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. Maintenant, xy_0 est inversible car xy_0 s'écrit $1 + pa$ avec $a \in \mathbb{Z}_p$ et

$$(1 + pa) \sum_{k=0}^{+\infty} (-pa)^k = 1$$

la série étant convergente au sens de la distance p-adique classique. Ainsi, $\mathbb{Z}_p \setminus p\mathbb{Z}_p \subset \mathbb{Z}_p^*$.
Inversement, un élément de $\mathbb{Z}_p^*$ a nécessairement sa première coordonnée non nulle étant donné que l'élément neutre de $\mathbb{Z}_p^*$ est $(1, 1, \cdots)$. Donc $\mathbb{Z}_p^* \subset \mathbb{Z}_p \setminus p\mathbb{Z}_p$ et finalement, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

REMARQUE : La proposition 3.1.2 permet au passage d'affirmer que $\mathbb{Z}_p^*$ est un groupe profini car $\mathbb{Z}_p^*$ peut se voir comme la limite projective des $(\mathbb{Z}/p^m\mathbb{Z})^*$. À ce titre, les théorèmes de Sylow affirment que $\mathbb{Z}_p$ (resp. $\mathbb{Z}_p^*$) a un unique p-Sylow étant donné que $\mathbb{Z}_p$ est un groupe abélien (resp. anneau commutatif).

PROPOSITION 3.1.3 Le groupe $\mathbb{Z}_p^*$ a pour seul p-Sylow le sous-groupe $1 + p\mathbb{Z}_p$.

PREUVE : Le groupe $\mathbb{Z}_p^*$ est abélien donc par le théorème 2.4.1, $\mathbb{Z}_p^*$ a un unique p-Sylow.
Introduisons la projection $f : \mathbb{Z}_p^* \to (\mathbb{Z}/p\mathbb{Z})^*$ qui envoie une suite de $\mathbb{Z}_p^*$ sur sa première coordonnée.
Tout d'abord, f est bien définie par la proposition 3.1.2 et est un morphisme de groupes (multiplicatifs).
L'application f est bien entendu surjective, et son noyau est égal à $1 + \mathbb{Z}_p$. Effectivement, si $x \in \ker(f)$, la première coordonnée de x vaut 1 et donc $x \in 1 + \mathbb{Z}_p$. Inversement, on a $1 + \mathbb{Z}_p \subset \ker(f)$.
Le premier théorème d'isomorphisme assure alors que $\mathbb{Z}_p/(1 + p\mathbb{Z}_p)$ et $(\mathbb{Z}/p\mathbb{Z})^*$ sont isomorphes.
Or on sait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$ (voir [Per96]) et donc $\mathbb{Z}_p/(1+p\mathbb{Z}_p)$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.
Mais $1 + p\mathbb{Z}_p$ est d'ordre p^∞ car $\mathbb{Z}_p$ est d'ordre p^∞ et donc par définition, $1 + p\mathbb{Z}_p$ est un p-Sylow de $\mathbb{Z}_p^*$.

REMARQUE : On peut montrer que pour $p \neq 2$, le groupe $\mathbb{Z}_p^*$ est isomorphe au produit direct $(\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p$. Pour $p = 2$, on a $\mathbb{Z}_2^*$ qui est isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_2$.

3.2 Le groupe spécial linéaire d'indice 2 sur l'anneau des entiers p-adiques

Commençons par rappeler que si A est un anneau intègre et commutatif, la formule qui donne l'inverse d'une matrice à coefficient dans A en fonction de la transposée de sa comatrice et de son déterminant est toujours vraie. Ainsi, les matrices inversibles de taille $n \times n$ à coefficients dans A où $n \in \mathbb{N}^*$ forment bien un groupe, appelé groupe linéaire d'indice n sur A et noté $\mathrm{GL}_n(A)$. De plus, le noyau du déterminant est un sous-groupe distingué de $\mathrm{GL}_n(A)$ appelé groupe spécial linéaire d'indice n sur A et noté $\mathrm{SL}_n(A)$. Dans cette partie, on pose $p \in \mathcal{P}$ et on va s'intéresser au groupe $\mathrm{SL}_2(\mathbb{Z}_p)$, où $\mathbb{Z}_p$ est un anneau intègre et commutatif en vertu de la proposition 3.1.1.

PROPOSITION 3.2.1 Soit $n \in \mathbb{N}^*$. Notons $\varphi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ le morphisme de projection.
Soit $\varphi : \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ l'application induite par φ_n.
Alors, φ est bien définie, est un morphisme de groupes et est surjective.

PREUVE : Soit $A \in \mathrm{SL}_2(\mathbb{Z}_p)$. On écrit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } \varphi(A) = \begin{pmatrix} \varphi_n(a) & \varphi_n(b) \\ \varphi_n(c) & \varphi_n(d) \end{pmatrix}$$

où a, b, c et d sont des éléments de $\mathbb{Z}_p$. On a bien

$$\det(\varphi(A)) = \varphi_n(a)\varphi_n(d) - \varphi_n(b)\varphi_n(c) = \varphi_n(ad - bc) = \varphi_n(1_{\mathbb{Z}_p}) = 1_{\mathbb{Z}/p^n\mathbb{Z}}$$

étant donné que φ_n est un morphisme d'anneaux. Donc φ est bien définie et comme φ_n est un morphisme d'anneaux, φ est un morphisme de groupes. Montrons que φ est surjective. Soit $M_0 \in \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Écrivons

$$M_0 = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \text{ où } (x, y, z, t) \in (\mathbb{Z}/p^n\mathbb{Z})^4.$$

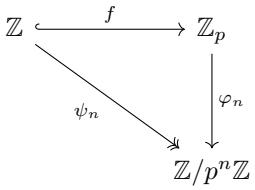
Remarquons que l'on a une surjection $\psi_n : \mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ et donc $\exists (a,b,c,d) \in \mathbb{Z}^4$ tel que $\psi(a) = x, \psi(b) = y, \psi(c) = z$ et $\psi(d) = t$, de sorte que $ad - bc \equiv 1\ [p^n]$. Posons $\delta = ad - bc$.
Mais en projetant un élément de $\mathbb{Z}$ dans toutes les coordonnées, on obtient une injection $f : \mathbb{Z} \to \mathbb{Z}_p$.
De cette façon, $f(\delta) \in 1 + p^n\mathbb{Z}_p$ avec $1 + p^n\mathbb{Z}_p \subset \mathbb{Z}_p^*$ vu la proposition 3.1.2.
Ainsi, $\exists \varepsilon \in 1 + p^n\mathbb{Z}_p$ ($1 + p^n\mathbb{Z}_p$ est un sous-groupe) tel que $\varepsilon f(\delta) = 1_{\mathbb{Z}_p^*}$. On pose

$$M = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} f(a) & f(b) \\ f(c) & f(d) \end{pmatrix} = \begin{pmatrix} \varepsilon f(a) & \varepsilon f(b) \\ f(c) & f(d) \end{pmatrix}$$

On vérifie tout d'abord que comme f est un morphisme d'anneaux,

$$\det(M) = \varepsilon f(a) f(d) - \varepsilon f(b) f(c) = \varepsilon f(\delta) = 1_{\mathbb{Z}_p^*}$$

donc $M \in \mathrm{SL}_2(\mathbb{Z}_p)$. Remarquons que le diagramme suivant commute par définition des morphismes mis en jeu.



Enfin, on remarque que

$$\begin{aligned}
\varphi(M) &= \varphi\left(\begin{pmatrix} \varepsilon f(a) & \varepsilon f(b) \\ f(c) & f(d) \end{pmatrix}\right) \\
&= \begin{pmatrix} \varphi_n(\varepsilon f(a)) & \varphi_n(\varepsilon f(b)) \\ \varphi_n(f(c)) & \varphi_n(f(d)) \end{pmatrix} \\
&= \begin{pmatrix} \varphi_n(\varepsilon)\varphi_n(f(a)) & \varphi_n(\varepsilon)\varphi_n(f(b)) \\ \varphi_n(f(c)) & \varphi_n(f(d)) \end{pmatrix} \\
&= \begin{pmatrix} \varphi_n(f(a)) & \varphi_n(f(b)) \\ \varphi_n(f(c)) & \varphi_n(f(d)) \end{pmatrix} \\
&= \begin{pmatrix} \psi(a) & \psi(b) \\ \psi(c) & \psi(d) \end{pmatrix} \\
&= \begin{pmatrix} x & y \\ z & t \end{pmatrix} \\
&= M_0.
\end{aligned}$$

Ainsi, φ est bien surjective car $M \in \mathrm{SL}_2(\mathbb{Z}_p)$ et $\varphi(M) = M_0$.

Remarque : On peut montrer que $\mathrm{GL}_2(\mathbb{Z}_p)$ est profini en tant que limite projective des $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ (voir [RZ10]). Ainsi, en tant que sous-groupe fermé de $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{SL}_2(\mathbb{Z}_p)$ est également profini (on utilise la proposition 1.4.4 et le fait que $\mathrm{SL}_2(\mathbb{Z}_p)$ est l'image réciproque d'un fermé par l'application continue déterminant). La différence avec l'exemple du groupe des inversibles de $\mathbb{Z}_p$ réside dans le fait que $\mathrm{SL}_2(\mathbb{Z}_p)$ n'est pas abélien. Dans la suite, on va donner des p-Sylow de $\mathrm{SL}_2(\mathbb{Z}_p)$.

Proposition 3.2.2 Soit P_0 un p-Sylow du groupe $\mathrm{SL}_2(\mathbb{F}_p)$. Notons $\varphi : \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ l'application définie dans la proposition 3.2.1. Alors, $\varphi^{-1}(P_0)$ est un p-Sylow de $\mathrm{SL}_2(\mathbb{Z}_p)$.

Preuve : En notant $P = \varphi^{-1}(P_0)$, P est fermé (image réciproque d'un fermé par une application continue).
Par la proposition 3.2.1, φ est surjective et donc $\varphi(P) = P_0$. En particulier, les éléments de P sont tous d'ordre une puissance de p étant donné que P_0 est un p-groupe. Ainsi, P est un groupe pro-p.
Par les théorèmes de Sylow 2.4.1, P est inclus dans un p-Sylow de $\mathrm{SL}_2(\mathbb{Z}_p)$ que nous notons Q.
Supposons que $P \neq Q$. Dans ce cas, $\varphi(Q)$ est un sous-groupe de $\mathrm{SL}_2(\mathbb{F}_p)$ qui est un p-groupe et qui contient strictement P_0. C'est impossible par définition d'un p-Sylow de $\mathrm{SL}_2(\mathbb{F}_p)$.
Donc $P = Q$ et P est bien un p-Sylow de $\mathrm{SL}_2(\mathbb{Z}_p)$.

En comptant le nombre de bases de $(\mathbb{F}_p)^2$ comme dans [Per96], on obtient que l'ordre de $\mathrm{GL}_2(\mathbb{F}_p)$ est $(p^2-p)(p^2-1) = p(p-1)(p^2-1)$. En utilisant le premier théorème d'isomorphisme sur le morphisme déterminant, comme l'image de $\mathrm{GL}_2(\mathbb{F}_p)$ par det est $\mathbb{F}_p^*$ qui est d'ordre $p-1$ et donc l'ordre de $\mathrm{SL}_2(\mathbb{F}_p)$ vaut $p(p-1)(p^2-1)/(p-1) = p(p^2-1)$. Le troisième théorème de Sylow dans le cas fini assure que le nombre n_p de p-Sylow de $\mathrm{SL}_2(\mathbb{F}_p)$ vérifie $n_p \equiv 1\ [p]$. Ainsi, on a nécessairement $n_p = 1 + kp$ où $k \in \mathbb{N}$. Mais $k \neq 0$ étant donné qu'on connait déjà deux p-Sylow de $\mathrm{SL}_2(\mathbb{F}_p)$, les sous-groupes $\langle\{A\}\rangle$ et $\langle\{B\}\rangle$ engendrés par

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Pour connaître la valeur exacte de n_p, on utilise également le fait que $n_p \mid p^2 - 1$. Montrons que $k = 1$.
Supposons que $k \geqslant 2$. On introduit $d = \mathrm{pgcd}(1+p, 1+kp)$.
Par définition du pgcd, $d \mid 1+p$ et $d \mid 1+kp$ donc $d \mid k+kp$ puis $d \mid k+kp-1-kp$. Ainsi,

$$d \mid k-1.$$

Comme $1+kp \mid p^2-1$ et $1+p \mid p^2-1$, $\mathrm{ppcm}(1+kp, 1+p) \mid p^2-1$ donc en multipliant par d, on obtient

$$(1+kp)(1+p) \mid d(p^2-1).$$

Mais $d \mid k-1$ donc $d(p^2-1) \mid (k-1)(p^2-1)$ et donc par transitivité de la relation divise, on a

$$(1+kp)(1+p) \mid (k-1)(p^2-1).$$

En particulier, en développant et en observant que le terme de droite est non nul étant donné que $k \neq 1$, on obtient $1+p+kp+kp^2 \leqslant 1-k-p^2+kp^2$ ou encore $p+kp \leqslant -k-p^2$ ce qui est impossible.
On a montré que $k \leqslant 1$ et comme $k \neq 0$ par la remarque précédente, on a bien $k = 1$.
Nous avons trouvé autant de p-Sylow dans $\mathrm{SL}_2(\mathbb{Z}_p)$ qu'il y en a dans $\mathrm{SL}_2(\mathbb{F}_p)$, c'est-à-dire exactement $p+1$.

Bibliographie

[Ser94] Jean-Pierre Serre. *Cohomologie Galoisienne*. Springer-Verlag Berlin, 1994.

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.

[Bou07] N. Bourbaki. *Topologie générale*. Springer-Verlag Berlin, 2007.

[RZ10] Luis Ribes et Pavel Zalesskii. *Profinite groups*. Springer-Verlag Berlin, 2010.