LIMITES DIRECTES ET INVERSES, GROUPES PROFINIS ET THÉORIE DE GALOIS INFINIE

NICOLAS SIMARD

Abstract. Ces notes sont une introduction à la théorie de Galois infinie. Pour se faire, nous introduirons la notion de limites directe (ou injective) et inverse (ou projective). Ces outils nous permettront d'introduire plus facilement la notion de groupe profini. Nous pourrons ensuite étudier certaines des propriétés des groupes de Galois infinis. Puisque les participants de ce séminaire ont des intérêts variés, j'ai essayé de donner, autant que possible, des exemples provenant de divers domaines (topologie, algèbre commutative, géométrie, théorie des nombres, etc.)

Contents

Des exemples

Il peut être préférable d'avoir des exemples en tête avant de définir les limites directes et inverses de façon plus abstraite.

Une limite inverse. Cet exemple nous sera utile lorsque nous parlerons de théorie de Galois infinie.

Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$, i.e. $\overline{\mathbb{Q}}$ est l'ensemble de tout les éléments algébriques sur $\mathbb{Q}$. Soit $\alpha \in \overline{\mathbb{Q}}$ et soit $f(x)$ le polynôme minimal de α. Si $L/\mathbb{Q}$ est le corps de décomposition de $f(x)$,

alors $\alpha \in L$ et $L/\mathbb{Q}$ est une extension Galoisienne finie (nous ferons un rappel rapide de la théorie de Galois finie dans le prochaine section). Ceci démontre que $\overline{\mathbb{Q}} \subseteq \bigcup_{L/\mathbb{Q} \text{ Galois et finie}} L$. L'inclusion inverse est directe puisque toute extension finie est algébrique. Nous avons donc montré que

$$\overline{\mathbb{Q}} = \bigcup_{L/\mathbb{Q} \text{ Galois et finie}} L$$

Soit maintenant σ un automorphisme de $\overline{\mathbb{Q}}/\mathbb{Q}$, i.e. un automorphisme de $\overline{\mathbb{Q}}$ fixant $\mathbb{Q}$. Si $L/\mathbb{Q}$ est une extension de Galois finie, il n'est pas difficile de vérifier que $\sigma|_L \in \mathrm{Gal}(L/\mathbb{Q})$. On voit donc qu'un automorphisme de $\overline{\mathbb{Q}}/\mathbb{Q}$ donne une famille d'automorphismes $(\sigma|_L)_L$ où L parcours toutes les extensions Galoisiennes finies de $\mathbb{Q}$. De plus, cette famille d'automorphismes est *compatible*, dans le sens où $(\sigma|_{L'})|_L = \sigma|_L$ dès que $L' \supseteq L \supseteq \mathbb{Q}$ est une tour d'extensions Galoisiennes finies. Inversement, on peut voir qu'une famille compatible d'automorphismes $(\sigma_L)_L$ où $\sigma_L \in \mathrm{Gal}(L/\mathbb{Q})$ pour toute extension Galoisienne finie $L/\mathbb{Q}$ définit un unique automorphisme de $\overline{\mathbb{Q}}/\mathbb{Q}$.

Dans cet exemple, on voit bien qu'un automorphisme de l'extension infinie $\overline{\mathbb{Q}}/\mathbb{Q}$ est une limite d'automorphismes d'extensions Galoisiennes finies. Nous verrons qu'en fait le groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$ est isomorphe à la limite projective des groupes de Galois des extensions Galoisiennes finies de $\mathbb{Q}$. Un groupe obtenu de cette façon s'appelle un groupe profini.

Une limite directe. Cet exemple est inspiré de la géométrie algébrique, mais aucune connaissance de ce sujet n'est requise.

Soit z in point du plan complexe et soit V_z l'ensemble de tout les voisinages ouverts de z. On s'intéresse aux fonctions qui sont holomorphes dans un voisinage de z. Si U est un voisinage ouvert de z, on définit $\mathcal{O}(U)$ comme étant l'anneau des fonctions holomorphes sur U ($\mathcal{O}(U)$ est même une $\mathbb{C}-$algèbre). On dénote un élément de $\mathcal{O}(U)$ par (f, U).

Soit (f, U) et (g, V) deux fonctions et supposons que $f|_W = g|_W$ pour un certain voisinage ouvert W de z contenu dans $U \cap V$. Puisqu'on s'intéresse seulement aux fonctions dans un voisinage z, (f, U) et (g, V) contiennent la même information, puisqu'elles coïncident près de z. On définit alors un relation d'équivalence sur $\coprod_{U \in V_z} \mathcal{O}(U)$ (l'union disjointe des $\mathcal{O}(U)$) de la façon suivante: $(f, U) \sim (g, V)$ si et seulement si il existe $W \in V_z$ tel que $W \subseteq U \cap V$ et $f|_W = g|_W$. Le quotient de $\coprod_{U \in V_z} \mathcal{O}(U)$ par cette relation est dénoté $\mathcal{O}_z$.

On voit dans cet exemple que $\mathcal{O}_z$ contient de l'information sur les fonctions holomorphes dans un voisinage de z. On montre facilement que $\mathcal{O}_z$ est aussi une $\mathbb{C}-$algèbre. On peut aussi montrer que $\mathcal{O}_z$ est un anneau local (indice: l'évaluation en z est bien définie).

1. Limites directes et inverses

Pour simplifier les définitions au début, nous travaillerons dans des catégories connues, comme celles des ensembles, des groupes, des espaces topologiques, des anneaux, des R-modules et des R-algèbres (où R est un anneau). Nous discuterons aussi des limites dans la catégorie des groupes topologiques.

Dans les deux exemples ci-haut, nous avions une famille d'*indices* (les ouverts de V_z et les extensions Galoisiennes finies de $\mathbb{Q}$) et à chaque indice, nous avons associé un objet (la $\mathbb{C}-$algèbres $\mathcal{O}(U)$ et le groupe fini $\mathrm{Gal}(L/\mathbb{Q})$). Nous avions aussi des fonctions de restrictions qui nous permettaient des passer d'un objet à l'autre.

Avant de définir les limites, rappelons ce qu'est un ensemble partiellement ordonné:

Définition 1. *Un ensemble partiellement ordonné est un couple $(I, \leq)$ où I est un ensemble et $\leq$ est une relation réflexive, antisymétrique et transitive. $(I, \leq)$ est dit dirigé si il est partiellement ordonné et si pour toute paire d'éléments $i, j \in I$, il existe $k \in I$ tel que $i \leq k$ et $j \leq k$.*

Un ensemble dirigé $(I, \leq)$ sera simplement dénoté I.

1.1. **Limites inverses.** Pour prendre une limite inverse, il faut un système inverse sur lequel prendre la limite.

Définition 2 (système projectif)**.** *Soit I un ensemble partiellement ordonné et soit $\{X_i\}_{i \in I}$ une collection d'ensemble indicée par les éléments de I. Pour chaque $i, j \in I$, $i \leq j$, soit $f_{ij} : X_j \longrightarrow X_i$ un morphisme d'ensemble (notez bien la direction du morphisme). Supposons que la collection de morphismes satisfait les propriétés suivantes:*

- *f_{ii} est l'identité de X_i;*
- *$f_{ik} = f_{ij} \circ f_{jk}$ dès que $i \leq j \leq k$.*

Alors la collection des $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i \leq j})$ est appelée système projectif (ou inverse).

Remarque: Cette définition se généralise directement à d'autres catégories que la catégorie des ensembles. Il suffit de remplacer le mot ensemble par groupe, anneau, espace topologique, etc. Rappelons que les morphismes de groupes, d'anneaux ou de R-modules sont les homomorphismes, que les morphismes d'espaces topologiques sont les fonctions continues et que les morphismes de groupes topologiques sont les homomorphismes continus.

Remarque: Pour les amateurs de théorie des catégories, on peut définir la notion de système projectif de façon plus concise. Tout d'abord, on peut voir un ensemble partiellement ordonné I comme une catégorie $\mathcal{I}$: les objets sont les éléments de I et $\mathrm{Hom}(i, j) = \{\iota_{ij}\}$ si $i \leq j$ et $\mathrm{Hom}(i, j) = \emptyset$ autrement (vérifiez que $\mathcal{I}$ est bien une catégorie). Un système inverse dans une catégorie $\mathcal{C}$ est simplement un foncteur $\mathcal{F} : \mathcal{I} \longrightarrow \mathcal{C}$ *contravariant* (vérifiez les aussi!).

Dans le contexte du premier exemple de ces notes, la deuxième propriété d'un système inverse est naturelle: elle dit que si $L'' \supseteq L' \supseteq L \supseteq \mathbb{Q}$ sont des extensions Galoisiennes, restreindre un automorphisme de L'' vers L' puis de L' vers L revient à restreindre cet automorphisme de L'' vers L.

Nous verrons après avoir défini la limite directe qu'un système projectif ou injectif peut être vu comme une sorte de graphe orienté. Cette façon de visualiser nous aidera à calculer certaines limites.

Nous sommes enfin prêt à définir la limite inverse d'ensembles:

Définition 3 (limite inverse)**.** *Soit $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i \leq j})$ un système projectif d'ensemble. Soit*

$$L = \left\{ (x_i)_i \in \prod_{i \in I} X_i | f_{ij}(x_j) = x_i \text{ pour tout } i \leq j \right\}$$

et pour chaque $i \in I$ soit $\varphi_i : L \longrightarrow X_i$ le morphisme qui envoie $(x_i)_i$ sur x_i. Alors $f_{ij} \circ \varphi_j = \varphi_i$ et $(L, \{\varphi_i\}_i)$ est la limite inverse du système $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i \leq j})$. On dénote cette limite $\varprojlim_{i \in I}(X_i, f_{ij})$.

Lorsque cela ne crée pas de confusion, on dénote la limite $L = \varprojlim X_i$.

Remarque: Les éléments de L sont des éléments du produit $\prod_{i\in I} X_i$ dont les composantes satisfont certaines conditions. De tels éléments sont parfois appelés *suites compatibles*.

Cette définition montre que la limite inverse d'ensembles existe. Avec un peu de travail, on peut montrer que la limite inverse existe dans d'autres catégories:

Theorem 1. *Soit $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i\leq j})$ un système projectif de groupes, d'anneaux, de R-modules, de R-algèbres, d'espaces topologiques ou de groupes topologiques. Alors la limite inverse de ce système existe dans la catégorie appropriée.*

Proof. Pour montrer ce théorème, il suffit de voir qu'on peut donner à l'ensemble L une structure algébrique, une topologie ou même les deux.

Supposons par exemple que les X_i sont des anneaux et que $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i\leq j})$ est un système inverse dans la catégorie des anneaux. Tout d'abord, la suite constante $(0)_i$ est dans L (elle est compatible) et si tout les X_i sont unitaires, $(1)_i$ est aussi dans L. Maintenant si $(x_i)_i, (y_i)_i \in L$, on définit $(x_i)_i + (y_i)_i = (x_i + y_i)_i$ et $(x_i)_i(y_i)_i = (x_i y_i)_i$. On vérifie facilement que les suites $(x_i + y_i)_i$ et $(x_i y_i)_i$ sont compatibles (donc les opérations sont bien définies) et que L forme un anneau sous ces opérations. On voit aussi que les $\varphi_i : L \longrightarrow X_i$ sont des morphismes d'anneaux. Tout cela montre que la limite inverse existe dans la catégorie des anneaux.

Un raisonnement presque identique montre que la limite inverse existe dans la catégorie des groupes, des R-modules et des R-algèbres.[1]

Supposons maintenant que les X_i sont des espaces topologiques.[2] On donne à L la topologie de sous-espace en considérant $L \subseteq \prod_{i\in I} X_i$ où $\prod_{i\in I} X_i$ est équipé de la topologie produit. On vérifie enfin que les fonctions $\varphi_i : L \longrightarrow X_i$ sont continues.

Finalement, supposons que les X_i sont des groupes topologiques.[3] Alors L est naturellement un groupe (comme ci-haut, on compose les éléments de L composante par composante). De plus, puisque chaque groupe est aussi un espace topologique, on peut donner à L une topologie (comme dans le paragraphe précédent). On peut alors vérifier que les fonctions multiplication $* : L \times L \longrightarrow L$ et inversion $\bullet^{-1} : L \longrightarrow L$ sont continues pour cette topologie. Ceci fait de L un groupe topologique et complète la preuve du théorème. □

Nous verrons quelques exemples de limites inverses plus tard. Pour le moment, vérifiez que le groupe des automorphismes de $\overline{\mathbb{Q}}/\mathbb{Q}$ est bien une limite inverse!

1.2. **Limite directe.** Comme dans le cas d'une limite inverse, pour prendre une limite directe, il faut un système injectif.

Définition 4 (système direct)**.** *Soit I un ensemble dirigé et soit $\{X_i\}_{i\in I}$ une collection d'ensemble indicée par les éléments de I. Pour chaque $i, j \in I$, $i \leq j$, soit $f_{ij} : X_i \longrightarrow X_j$ un morphisme*

[1] Rappelons que X_i est une R-algèbre s'il existe un homomorphisme $\rho_i : R \longrightarrow X_i$ tel que $\rho_i(R)$ est contenu dans le centre de X_i. Un morphisme de R-algèbres est un homomorphisme d'anneaux $f_{ij} : X_j \longrightarrow X_i$ tel que $\rho_i = f_{ij} \circ \rho_j$. On peut donc voir L comme une R-algèbre en définissant $\rho : R \longrightarrow L$ comme $\rho(r) = (\rho_i(r))_i$, qui est une suite compatible. On peut aussi vérifier que les $\varphi_i : L \longrightarrow X_i$ sont des morphismes de R-algèbre.

[2] Rappelons qu'un morphisme d'espaces topologiques est une fonction continue.

[3] Rappelons qu'un morphisme de groupe topologiques est un homomorphisme continue.

d'ensemble (notez bien la direction du morphisme). Supposons que la collection de morphismes satisfait les propriétés suivantes:

- f_{ii} *est l'identité de* X_i*;*
- $f_{ik} = f_{jk} \circ f_{ij}$ *dès que* $i \leq j \leq k$.

Alors la collection des $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$ *est appelée système injectif.*

Notez bien que l'ensemble I doit être *dirigé*, et non seulement partiellement ordonné, pour définir la limite directe de cette façon.

Remarque: Comme dans le cas d'un système inverse, cette définition se généralise facilement à d'autres catégories. On peut aussi voir un système directe comme un foncteur *covariant* $\mathcal{F} : \mathcal{I} \longrightarrow \mathcal{C}$ où $\mathcal{I}$ est la catégorie associée à I et $\mathcal{C}$ est une catégorie.

On peut maintenant définir la notion de limite directe (ou injective) pour des ensembles:

Définition 5 (limite injective)**.** *Soit* $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$ *un système injectif d'ensemble. Soit*

$$L = \left(\coprod_{i \in I} X_i \right) / \sim$$

et pour chaque $i \in I$ *soit* $\varphi_i : X_i \longrightarrow L$ *le morphisme qui envoie* x *sur* $[x]$*, la classe de* x *dans* L*, où* $\sim$ *est la relation d'équivalence suivante: si* $x_i \in X_i$ *et* $x_j \in X_j$*, alors* $x_i \sim x_j$ *si il existe* $k \in I$ *tel que* $i, j \leq k$ *et* $f_{ik}(x_i) = f_{jk}(x_j)$ *dans* X_k*. Alors* $\varphi_j \circ f_{ij} = \varphi_i$ *et* $(L, \{\varphi_i\}_i)$ *est la limite directe du système* $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$*. On dénote cette limite* $\varinjlim_{i \in I}(X_i, f_{ij})$*.*

La limite directe est parfois dénotée $L = \varinjlim X_i$.

La relation d'équivalence peut sembler arbitraire, mais elle en fait naturelle. Elle dit que x_i est équivalent à x_j si ces éléments sont éventuellement égaux, dans un ensemble plus "grand" que X_i et X_j. Dans l'exemple de limite directe au début de ces notes, on associait les éléments (f, U) et (g, V) si elles finissaient par coïncider lorsqu'on rétrécissait les voisinages de z.

Avec un peu de travail, on peut montrer que la limite directe existe dans la catégorie des groupes, des anneaux, des R-modules, des R-algèbres et des espaces topologiques. *Mais attention, la limite directe n'existe pas forcément dans la catégorie des groupes topologiques.* Le problème est de définir une topologie sur les classes d'équivalences qui rende la multiplication continue.

Theorem 2. *Soit* $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$ *un système injectif de groupes, d'anneaux, de* R*-modules, de* R*-algèbres ou d'espaces topologiques. Alors la limite directe de ce système existe dans la catégorie appropriée.*

Proof. L'idée de la preuve est essentiellement la même que dans le théorème précédent: on met une structure algébrique ou une topologie sur l'ensemble L.

Supposons que les X_i sont des anneaux et que $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$ est un système injectif d'anneaux. Tout d'abord, la classe $[0]$ est bien définie, peu importe de quel anneau 0 provient. Si les anneaux sont unitaires, la classe $[1]$ est aussi bien définie. Soit maintenant $[x_i]$, où $x_i \in X_i$, et $[x_j]$, où $x_j \in X_j$, deux classes de L. Puisque I est dirigé, on peut trouver $k \in I$ tel que $i, j \leq k$. On définit alors $[x_i] + [x_j] = [f_{ik}(x_i) + f_{jk}(x_j)]$ et $[x_i][x_j] = [f_{ik}(x_i) f_{jk}(x_j)]$. Il n'est pas difficile de vérifier que ces opérations sont bien définies (en particulier, elles ne dépendent pas de k) et qu'elles

font de L un anneau. Finalement, on voit que les fonctions $\varphi_i : X_i \longrightarrow L$ sont des morphismes d'anneaux.

Un raisonnement semblable montre qu'on peut donner à L une structure de groupe, de R-module ou de R-algèbre.[4]

Finalement, supposons que les X_i sont des espaces topologiques et que $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i\leq j})$ est une système injectif d'espaces topologiques. On met sur L la topologie finale, c'est-à-dire la plus petite topologie qui rend les applications $\varphi_i : X_i \longrightarrow L$ continues. En d'autre mots, un sous-ensemble $U \subseteq L$ est ouvert si et seulement si $\varphi_i^{-1}(U)$ est ouvert pour tout $i \in I$. Alors L est un espace topologique et les applications $\varphi_i : X_i \longrightarrow L$ sont continues par définition. □

Avant de poursuivre, notons que le fait que I soit dirigé était cruciale pour définir la limite directe dans les catégories des anneaux, des groupes, des R-algèbres et des R-modules. Cette condition n'était toutefois pas nécessaire pour définir la limite inverse. Dans la catégorie des R-modules, il est tout de même possible de définir la limite directe sur un ensemble partiellement ordonné:

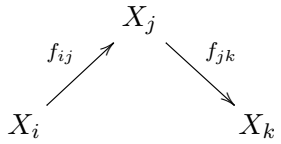
Définition 6. *Soit $(\{M_i\}_i, \{f_{ij} : M_i \longrightarrow M_j\}_{i\leq j})$ un système injectif de R-modules où I est partiellement ordonné. Soit $\lambda_i : M_i \longrightarrow \bigoplus_{i\in I} M_i$ l'inclusion et soit $W \subseteq \bigoplus_{i\in I} M_i$ le R-module généré par l'ensemble $\{\lambda_i(m_i) - \lambda_j(f_{ij}(m_i))|$ pour tout $i \leq j, m_i \in M_i\}$. Soit*

$$L = \left(\bigoplus_{i\in I} M_i\right)/W$$

et soit $\varphi_i : M_i \longrightarrow L$ la composition de λ_i avec la projection canonique $\bigoplus_{i\in I} M_i \longrightarrow L$. Alors $\varphi_j \circ f_{ij} = \varphi_i$ et $(L, \{\varphi_i\}_i)$ est la limite directe du système $(\{M_i\}_i, \{f_{ij} : M_i \longrightarrow M_j\}_{i\leq j})$. On dénote cette limite $\varinjlim_{i\in I}(M_i, f_{ij})$.

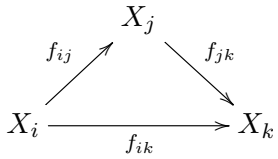
Comme nous verrons plus tard, lorsque I est dirigé, les deux limites sont isomorphes dans la catégorie des R-modules.

1.3. **Visualiser les systèmes injectifs et projectifs.** Prenons un système injectif de groupes, par exemple. On peut représenter ce système comme un graphe orienté où chaque sommet est un groupe et chaque arête (orienté) est un morphisme. Normalement, on ne représente pas les morphismes identités. Ce graphe à la propriété suivante: si on a deux morphismes



on doit avoir un troisième morphisme

[4]En utilisant la même notation que dans une note plus haut, on peut définir $\rho : R \longrightarrow L$ comme $r \longmapsto [\rho_i(r)]$ où $i \in I$ est quelconque. Bien entendu, on doit vérifier que ρ est un morphisme de R-algèbre bien défini, mais c'est le cas!



tel que $f_{ik} = f_{jk} \circ f_{ij}$.

Notons aussi qu'un diagramme comme celui-ci peut aussi être vu comme un système inverse (il suffit d'inverser la relation d'ordre). Cela fait donc du sens de parler de la limite directe ou inverse d'un diagramme, pourvu que cette limite existe. Par exemple, le diagramme suivant

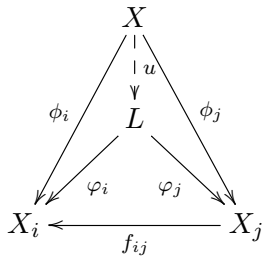
$$A \longrightarrow B$$

dans la catégorie des groupes a A pour limite inverse et B pour limite directe. Cela deviendra évident lorsque nous aurons vu la propriété universelle des limites.

1.4. **La propriété universelle des limites.** Les limites directes et inverses peuvent être caractérisées par leur propriété universelle. Commençons par une définition:

Définition 7. *Soit $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i \leq j})$ un système projectif sur un ensemble partiellement ordonné I dans une catégorie $\mathcal{C}$ (la catégorie $\mathcal{C}$ peut être une des catégories usuelles). Un cône $(X, \{\phi_i\}_i)$ sur ce système est un objet X de $\mathcal{C}$ et une famille de morphismes $\phi_i : X \longrightarrow X_i$ tels que $f_{ij} \circ \phi_j = \phi_i$ pour tout $i \leq j$.*

Theorem 3 (propriété universelle de la limite projective)**.** *Soit $(L, \{\varphi_i\}_i)$ la limite projective du système $(\{X_i\}_i, \{f_{ij} : X_j \longrightarrow X_i\}_{i \leq j})$ dans une catégorie $\mathcal{C}$ et soit $(X, \{\phi_i\}_i)$ un cône sur ce système projectif. Alors il existe un unique morphisme $u : X \longrightarrow L$ tel que le diagramme suivant commute:*



Proof. Commençons par le cas d'une limite projective d'ensembles.

Définissons $u : X \longrightarrow L$ de la façons suivante. Pour un $x \in X$ donné, on définit $u(x) = (\phi_i(x))_i \in \prod_{i \in I} X_i$. Puisque $(X, \{\phi_i\}_i)$ est un cône sur le système, on vérifie directement que $u(x)$ est une suite compatible, i.e. $u(x) \in L$. La commutativité du diagramme du théorème est facile à vérifier puisque les $\varphi_i : L \longrightarrow X_i$ sont des projections. L'unicité de u découle de sa définition et de la commutativité du diagramme.

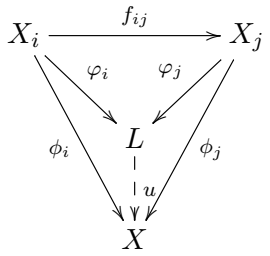
Dans le cas où la limite est prise dans une autre catégorie, il suffit de vérifier que la fonction $u : X \longrightarrow L$ définie pour les ensembles est une homomorphisme, une fonction continue ou les deux, selon le cas. □

D'une certaine façon, la limite projective sur un système projectif est le cône le plus près possible du système. Si on visualise les système comme une graphe dans le plan et le cône $(L, \{\varphi_i\}_i)$ comme un véritable cône, l'image est claire!

Avec tout le travail accompli jusqu'à présent, la propriété universelle de la limite injective devrait être relativement simple à deviner.

Définition 8. *Soit $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$ un système injectif sur un ensemble dirigé I dans une catégorie $\mathcal{C}$ (la catégorie $\mathcal{C}$ peut être une des catégories usuelles, sauf peut-être la catégorie des groupes topologiques). Un co-cône $(X, \{\phi_i\}_i)$ sur ce système est un objet X de $\mathcal{C}$ et une famille de morphismes $\phi_i : X_i \longrightarrow X$ tels que $\phi_i \circ f_{ij} = \phi_j$ pour tout $i \leq j$.*

Theorem 4 (propriété universelle de la limite injective)**.** *Soit $(L, \{\varphi_i\}_i)$ la limite injective du système $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i \leq j})$ dans une catégorie $\mathcal{C}$ et soit $(X, \{\phi_i\}_i)$ un co-cône sur ce système. Alors il existe un unique morphisme $u : L \longrightarrow X$ tel que le diagramme suivant commute:*



Proof. Commençons par le cas d'une limite injective d'ensembles.

Définissons $u : L \longrightarrow X$ de la façon suivante. Soit l une classe d'équivalence dans L. Alors $l = \varphi_i(x_i) = [x_i]$ pour un certain $x_i \in X_i$ par définition de φ_i. On définit alors $u(x) = \phi_i(x_i)$. Il faut maintenant montrer que cette fonction est bien définie. Supposons que $x_i \sim x_j$, où $x_j \in X_j$, de telle sorte que $[x_i] = [x_j]$. Alors il existe $k \in I$, tel que $i, j \leq k$ et $f_{ik}(x_i) = f_{jk}(x_j)$. En appliquant ϕ_k à cette équation et en utilisant le fait que $(X, \{\phi_i\}_i)$ est un co-cône sur le système, on voit que $\phi_i(x_i) = \phi_k(f_{ik}(x_i)) = \phi_k(f_{jk}(x_j)) = \phi_k(x_j)$. La commutativité du diagrame du théorème est aussi simple à vérifier. L'unicité de u découle de sa définition et de la commutativité du diagramme.

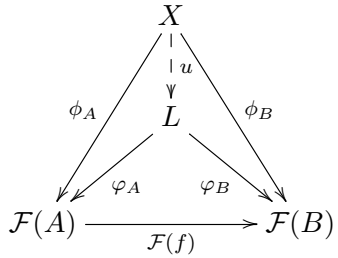
Dans le cas où la limite est prise dans une autre catégorie, il suffit de vérifier que $u : L \longrightarrow X$ définit pour les ensembles est un homomorphisme ou une fonction continue, selon le cas. □

Comme pour la limite projective, on peut visualiser la limite injective comme étant le cône *sous* le graphe qui est le plus près possible du graphe.

1.5. **Limites dans des catégories arbitraires.** En théorie des catégories, on utilise la propriété universelle des limites pour les définir. Dans ces notes, nous avons plutôt fait le contraire: nous avons défini un objet que nous avons appelé limite et nous avons démontré qu'il satisfaisait une propriété universelle. Il peut être instructif de voir les limites de façon plus abstraite.

Soient $\mathcal{I}$ et $\mathcal{C}$ des catégories et $\mathcal{F} : \mathcal{I} \longrightarrow \mathcal{C}$ un foncteur covariant. La limite de ce diagramme $\mathcal{F} : \mathcal{I} \longrightarrow \mathcal{C}$, si elle existe, est un cône (L, φ) tel que pour tout cône (X, ψ) il existe un unique

morphisme $u : X \longrightarrow L$ tel que le diagramme suivant commute



La limite en théorie des catégories correspond à ce que nous appelons limite inverse ou projective. Il découle directement de la propriété universelle que la limite, si elle existe, est unique à isomorphisme près.

La co-limite est définie de façon analogue en utilisant la notion de co-cône. Elle correspond à ce que nous appelions limite directe ou injective et elle aussi unique à isomorphisme près lorsqu'elle existe.

En terminant, notons que tout ce que nous avons fait dans cette section fut de montrer que les limites et les co-limites existent dans la catégorie des ensembles, des groupes, des anneaux, des R-modules et des R-algèbres. Pour ce faire, nous avons exhibé un objet qui satisfaisait la propriété universelle adéquate. L'unicité des limites nous permet de conclure que ces objets sont bel et bien les limites recherchés.

Remarque: Il est maintenant possible de montrer que les deux limites injectives que nous avons définies dans la catégorie des R-modules sont isomorphes lorsque I est dirigé. Pour ce faire, il suffit de montrer que la seconde définition (lorsque I n'est pas nécessairement dirigé) satisfait la propriété universelle de la limite injective (cet exercise est laissé au lecteur). L'isomorphisme entre les deux limites est alors donné gratuitement par l'unicité de la limite!

1.6. **Quelques exemple de limites.**

1.6.1. *Limites triviales de R-modules.* Soit $\{M_i\}_{i\in I}$ une collection de R-modules et dotons I de l'ordre partiel trivial, i.e. les seules relations d'ordre sont $i \leq i$. Notons que I n'est pas dirigé et qu'il n'y a aucune fonction de transition f_{ij} à part les fonctions identité. Dans ce cas, on voit que $\varinjlim M_i = \bigoplus_{i\in I} M_i$ et $\varprojlim_{i\in I} M_i = \prod_{i\in I} M_i$.

1.6.2. *Un exemple abstrait.* Considérons à nouveau le diagramme

$$A \longrightarrow B$$

Alors A est la limite projective et B est la limite injective. En effet, les objets A et B satisfont la propriété universelle des limites projectives et injectives respectivement. Plus généralement, si I est un ensemble partiellement ordonné qui possède un élément maximal m, i.e. un élément tel que $i \leq m$ pour tout $i \in I$, alors $\varinjlim_{i\in I} X_i = X_m$ si $(\{X_i\}_i, \{f_{ij} : X_i \longrightarrow X_j\}_{i\leq j})$ est un système injectif sur I. Un résultat similaire vaut pour les limites projectives.

1.6.3. *Le produit libre.* Prenons l'ensemble $I = \{1, 2\}$ et dotons le de l'ordre partiel trivial: $1 \leq 1$ et $2 \leq 2$. Un système injectif de groupes sur I est simplement une paire de groupes G_1 et G_2. Nous montrerons que la limite injective de ce système est $G_1 * G_2$, le produit libre de G_1 et G_2.[5] Notons au passage que l'ensemble I n'est pas dirigé, alors la limite injective n'existe pas nécessairement.

Tout d'abord, on peut définir de façon naturelle des fonctions $\varphi_i : G_i \longrightarrow G_1 * G_2$ en envoyant un élément x de G_i sur le mot x dans le produit libre. Pour montrer que $G_1 * G_2$ est bien la limite injective du système, il faut montrer que $G_1 * G_2$ satisfait la propriété universelle de la limite injective. Supposons alors qu'on ait un groupe X et deux morphismes $\phi_i : G_i \longrightarrow X$. On définit alors $u : G_1 * G_2 \longrightarrow X$ comme $u(x_1 \dots x_n) = u(x_1) \dots u(x_n)$ où $u(x_i) = \phi_1(x_i)$ si $x_i \in G_1$ et $u(x_i) = \phi_2(x_i)$ si $x_i \in G_2$. Cette fonction est bien définie, ce qui termine la démonstration.

Notons en terminant que la limite projective de ce même système est simplement $G_1 \times G_2$, le produit direct de G_1 et de G_2.

1.6.4. *Le produit fibré (ou* pullback*).* Considérons maintenant le diagramme suivant

$$\begin{array}{ccc} & & X \\ & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow[g]{} & Z \end{array}$$

Lorsqu'elle existe, la limite projective de ce diagramme s'appelle le produit fibré. Selon la catégorie dans laquelle cette limite est prise, elle peut avoir diverses interprétations. Dans la catégorie des schémas, par exemple, le produit fibré de X et Y sur Z et est dénoté $X \times_Z Y$ et il est très important en géométrie algébrique. Il joue un rôle analogue au produit tensoriel.

Notons que la limite directe de ce diagramme est simplement Z.

1.6.5. *Le produit amalgamé (ou* pushout*).* Considérons maintenant le diagramme suivant

$$\begin{array}{ccc} Z & \xrightarrow{f} & X \\ {\scriptstyle g}\downarrow & & \\ Y & & \end{array}$$

Lorsqu'elle existe, la limite directe de ce diagramme s'appelle le produit amalgamé. Une telle limite intervient en topologie dans la formulation du théorème de Van Kampen sous la forme suivante: Z est un sous-groupe de X et Y et les fonctions f et g sont les inclusions. Dans ce cas précis, la limite directe peut être décrite comme $X * Y/N$ où N est le sous-groupe normal engendré par les éléments $f(z)g(z)^{-1}$ où $z \in Z$. Cette définition ressemble à celle que nous avons donné de la limite injective. Toutefois, nous ne pouvions pas appliquer cette définition directement puisque l'ensemble d'indices n'est pas dirigé.

Finalement, on voit que la limite projective de ce système est Z.

---

[5]Rappelons que le produit libre de G_1 et de G_2 est l'ensemble des mots $x_1 x_2 \dots x_n$, où $x_i \in G_1$ ou G_2, modulo les relations $x_1 \dots x_i x_{i+1} \dots x_n \sim x_1 \dots (x_i x_{i+1}) \dots x_n$ si x_i et x_{i+1} appartiennent au même groupe et $x_1 \dots x_{i-1} e x_{i+1} \dots x_n \sim x_1 \dots x_{i-1} x_{i+1} \dots x_n$. La multiplication dans ce groupe est simplement la juxtaposition des mots.

1.6.6. *Les entiers $p-$adiques.* Pour chaque $n \geq 1$, on peut considérer la fonction surjective suivante

$$a \pmod{p^{n+1}} \longmapsto a \pmod{p^n} : \mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

La limite projective du système obtenu

$$\ldots \longrightarrow \mathbb{Z}/p^3\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

est isomorphe aux entiers $p-$adiques, i.e. $\mathbb{Z}_p$.

2. Théorie de Galois infinie

Les extensions de Galois infinies surgissent à plusieurs endroits en mathématiques. En géométrie algébrique, par exemple, il est souvent plus pratique de travailler sur des corps algébriquement clos. Parfois on veut faire agir les automorphismes de ce corps sur des variétés, des polynômes ou des morphismes. Mais comment comprendre le groupe de ces automorphismes, si l'extension est de dégrée infinie?

Nous verrons dans cette section la définition d'une extension de Galois infinie. Nous étudierons ensuite certaine de leur propriétés, puis nous parlerons d'une classe importante des groupes: les groupes profinis. Finalement, nous présenterons le théorème fondamental de la théorie de Galois pour les extensions infinies et nous donnerons quelques exemples de groupes de Galois infinis.

2.1. **Extension de Galois: définition.** Avant de parler d'extensions infinies, revenons rapidement sur les extensions Galoisiennes finies. Il existe plusieurs définitions d'une extension de Galois. La plus connue est peut-être la suivante:

Définition 9 (extension de Galois finie)**.** *Soit K/F une extension finie. Alors K/F est une extension de Galois si elle est le corps de décomposition d'un polynôme séparable sur F.*

Cette définition est très élégante. Il existe toutefois d'autre caractérisations équivalentes des extensions de Galois finies:

Theorem 5. *Soit K/F une extension finie. Alors les propriétés suivantes sont équivalentes:*

(1) *K/F est une extension de Galois*
(2) *K/F est le corps de décomposition d'une collection de polynômes séparables sur F*
(3) *Le corps fixé de* $\mathrm{Aut}(K/F)$ *est F*
(4) $|\mathrm{Aut}(K/F)| = [K : F]$
(5) *K/F est normale et séparable.*

Rappelons qu'une extension algébrique K/F est dite *normale* si elle est le corps de décomposition d'une collection de polynômes sur F et qu'elle est dite *séparable* si le polynôme minimal de tout élément de K est séparable.

Si on désire généraliser la définition d'extension Galoisienne aux extensions infinies, la dernière caractérisation semble un bon choix. Ceci nous mène à la définition suivante:

Définition 10 (extension de Galois)**.** *Soit K/F une extension algébrique. Alors K/F est une extension de Galois si elle est normale et séparable.*

Notons qu'avec cette définition généralise la définition précédente, puisque toute extension finie est algébrique.

2.2. **Extension de Galois: propriétés.** Soit K/F une extension algébrique. On définit

$$I = \{L/F | K \supseteq L \supseteq F, [L:F] < \infty \text{ et } L/F \text{ Galois}\}$$

Nous avons alors les caractérisations suivantes des extensions Galoisiennes:

Theorem 6. *Soit K/F une extension algébrique. Alors K/F est une extension de Galois si et seulement si*

$$K = \bigcup_{L/F \in I} L$$

.

Proof. $\Longrightarrow$) Par définition de I, $\bigcup_{L/F\in I} L \subseteq K$. Pour l'inclusion opposée, prenons un élément $x \in K$. Alors x est inclus dans le corps de décomposition de son polynôme minimal sur F, qui est séparable (car K/F est séparable). Par définition, cette extension est Galoisienne et finie, donc $x \in \bigcup_{L/F\in I} L$.

$\Longleftarrow$) tout d'abord, K/F est séparable. En effet, si x est un élément de K, alors x est contenu dans une extension $L/F \in I$, donc son polynôme minimal sur F est séparable. Maintenant chaque $L/F \in I$ est le corps de décomposition d'un certain polynôme $f_L(x) \in F[x]$. Soit K' le corps de décomposition de la collection de polynômes $\{f_L(x) : L/F \in I\}$. Clairement, $K' \subseteq K$. Pour l'inclusion opposée, prenons x dans K. Alors x est contenu dans le corps de décomposition de son polynôme minimal, qui est contenu dans K'. □

Theorem 7. *Soit K/F une extension algébrique. Alors K/F est une extension de Galois si et seulement si K/F est séparable et tout polynôme irréductible sur F qui admet une racine dans K se factorise complètement dans K.*

Proof. $\Longrightarrow$) Par définition K/F est séparable. Soit maintenant $f(x) \in F[x]$ un polynôme irréductible admettant une racine dans K. Alors par le théorème précédent, cette racine appartient à une certaine extension Galoisienne finie L/F. Puisque les éléments de $\mathrm{Gal}(L/F)$ agissent transitivement sur les racines de $f(x)$, on voit que $f(x)$ se factorise complètement dans L, donc dans K.

$\Longleftarrow$) Soit α un élément de K. Alors le polynôme minimal de α sur F, disons $m_\alpha(x)$, est séparable et admet toutes ses racines dans K par hypothèse. En d'autre mots, le corps de décomposition L_α de $m_\alpha(x)$ est contenu dans K. Cela implique que $K = \bigcup_{\alpha\in K} L_\alpha$. Puisque L_α est une extension de Galois finie, on voit que $K = \bigcup_{\alpha\in K} L_\alpha = \bigcup_{L/F\in I} L$, ce qui complète la preuve. □

Nous allons maintenant nous servir des outils que nous avons développé dans la première section. Pour cela, on place une relation d'ordre partielle sur I en définissant $L_1 \leq L_2$ si et seulement si $L_1 \subseteq L_2$. L'ensemble I muni de cette relation est même dirigé. En effet, si L_1 et L_2 sont des extensions Galoisiennes finies, alors L_1L_2 (leur compositum) l'est aussi et $L_1, L_2 \subseteq L_1L_2$.

Si K/F est Galoisienne, on voit que

$$K = \varinjlim_{L/F\in I} L$$

Prenons maintenant deux extensions Galoisiennes finies L_1/F et L_2/F et supposons que $L_1 \subseteq L_2$. On a alors une fonction

$$\rho_{L_2/L_1} : \mathrm{Gal}(L_2/F) \longrightarrow \mathrm{Gal}(L_1/F)$$

qui envoie $\sigma \in \mathrm{Gal}(L_2/F)$ sur $\sigma|_{L_1} \in \mathrm{Gal}(L_1/F)$. Le noyau de cette fonction est $\mathrm{Gal}(L_2/L_1)$ et on peut montrer qu'elle est surjective.

Comme dans le cas d'une extension de Galois finie, $\mathrm{Gal}(K/F)$ est défini comme l'ensemble des automorphismes de K qui fixent les éléments de F. On a alors le résultat suivant:

Theorem 8. *Soit K/F une extension de Galois. Alors*

$$\mathrm{Gal}(K/F) \cong \varprojlim_{L/F \in I} \mathrm{Gal}(L/F)$$

Ce théorème généralise les remarque faites au début de ces notes à propos des automorphismes de $\overline{\mathbb{Q}}/\mathbb{Q}$. En effet, on voit que l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ est Galoisienne (puisqu'elle est égale à l'union de toutes les extensions de Galois de $\mathbb{Q}$) et nous avons remarqué que ses automorphismes pouvaient être vu comme des suites compatibles d'automorphismes d'extensions de Galois finies. Avec tout ce qui as été dit jusqu'à présent, le lecteur devrait être en mesure de fournir la preuve de ce théorème.

Proof. Exercice! □

D'une certaine façon, la limite projective nous permet de recoller les automorphismes des extensions qui composent K/F.

2.3. **Les groupes profinis.** À ce stade-ci, on peut se demander si tout les théorèmes de la théorie de Galois finie restent valide dans le cas infini. En particulier, y a-t-il une correspondance bijective entre les sous-extensions d'une extension Galoisienne infinie K/F et les sous-groupes de $\mathrm{Gal}(K/F)$? Malheureusement, ce n'est pas tout à fait le cas. Heureusement, on peut rétablir la bijection en ne considérant pas tout les sous-groupes de $\mathrm{Gal}(K/F)$, mais seulement ceux qui sont fermés dans une certaine topologie. Pour définir cette topologie, nous étudierons la classe des groupes profinis.

Définition 11. *Un groupe est dit profini s'il est isomorphe à la limite projective d'un système projectif de groupes $(\{G_i\}_i, \{f_{ij} : G_j \longrightarrow G_i\}_{i \leq j})$ ayant les propriétés suivantes:*

1. *l'ensemble d'indices I est dirigé*
2. *les groupes G_i sont fini pour tout $i \in I$*
3. *les fonctions de transition f_{ij} sont surjectives pour tout $i \leq j$.*

Les résultats de la sous-section précédente nous permettent de voir que:

Theorem 9. *Soit K/F une extension de Galois infinie. Alors $\mathrm{Gal}(K/F)$ est un groupe profini.*

Soit G un groupe profini, disons $G \cong \varprojlim G_i$. Chacun des G_i peut être vu comme un groupe topologique si on le dote de la topologie discrète. Comme nous l'avons vu dans la première section, les limites projectives de groupes topologique existent. Ceci montre que les groupes profinis sont donc des groupes topologiques. Le théorème suivant donne une charactérisation alternative des groupes profinis:

Theorem 10. *Soit G un groupe topologique. Alors G est profini si et seulement si il est compact et totalement disconnexe.*

Un espace topologique est dit totalement disconnexe si ses seules parties connexes sont les singletons.

Proof. Voir *Algebraic Number Theory* de Cassels et Fröhlich, Ch.V, Th1. □

Ce théorème nous donne une meilleur idée de la nature topologique des groupes profini. On peut tout de même en dire davantage sur la topologie d'un tel groupe:

Proposition 1. *Soit $G = \varprojlim_{i\in I} G_i$ un groupe profini. Alors*

(1) *Pour tout sous-ensemble fini $J \subseteq I$, on définit*

$$N_J = \left(\prod_{i\in J}\{1_{G_i}\} \times \prod_{i\in I\setminus J} G_i\right) \cap G$$

Alors N_J est un sous-groupe normal ouvert d'indice fini dans G.

(2) *Soit U un sous-ensemble ouvert de G contenant l'identité de G. Alors $N_J \subseteq U$ pour un certain J. De plus, tout sous-groupe ouvert de G est une réunion de translatés de sous-groupes N_J.*

(3) *Tout sous-groupe ouvert de G est fermé et d'indice fini.*

(4) *Tout sous-groupe fermé de G d'indice fini est ouvert.*

(5) *Toute intersection de sous-groupes ouverts est un sous-groupe fermé. Tout sous-groupe fermé est une intersection de sous-groupes ouverts.*

Proof. Nous avons défini la limite projective comme le sous-groupe des suites compatibles dans $\prod_{i\in I} G_i$. La topologie est la topologie de sous-espace et l'opération de groupe est la multiplication composante par composante des suites.

1) Les sous-groupes N_J sont clairement normaux dans G. On voit ensuite que $\prod_{i\in J}\{1_{G_i}\} \times \prod_{i\in I\setminus J} G_i$ est ouvert dans $\prod_{i\in I} G_i$ car $\{1_{G_i}\}$ est ouvert dans G_i pour tout $i \in I$ (les G_i sont doté de la topologie discrète), donc N_J est ouvert dans G par définition de la topologie de sous-espace. Finalement, l'indice de $\prod_{i\in J}\{1_{G_i}\} \times \prod_{i\in I\setminus J} G_i$ dans $\prod_{i\in I} G_i$ est $\prod_{i\in J} |G_i| < \infty$, donc les N_J sont d'indice fini dans G.

2) Soit U un ouvert de G contenant 1_G, l'identité de G. Par définition de la topologie sur G, il existe un ouvert V de $\prod_{i\in I} G_i$ tel que $U = V \cap G$. En utilisant la base d'ouverts autour de 1_G dans $\prod_{i\in I} G_i$, on voit qu'il existe un ouvert un ensemble fini d'indices $J \subseteq I$ et un ouvert $\prod_{i\in J} V_i \times \prod_{i\in I\setminus J} G_i$ de $\prod_{i\in I} G_i$ tel que

$$1_G \in \prod_{i\in J} V_i \times \prod_{i\in I\setminus J} G_i \subseteq V$$

Mais alors

$$\prod_{i\in J}\{1_{G_i}\} \times \prod_{i\in I\setminus J} G_i \subseteq V$$

d'où $N_J \subseteq U$.

Soit maintenant U un ouvert quelconque de G. Si x appartient à U, alors $x^{-1}U$ est un ouvert contenant 1_G (notez que la multiplication et l'inversion sont des opérations continues et inversibles, donc $x^{-1}U$ est homéomorphe à U, qui est ouvert). Par le raisonnement précédent, il existe un ensemble fini d'indices $J_x \subseteq I$ tel que $G_{J_x} \subseteq x^{-1}U$, d'où $x \in xG_{J_x} \subseteq U$. On voit alors que $U = \bigcup_{x\in U} xG_{J_x}$.

3) Si U est un sous-groupe ouvert de G, $G \setminus U$ est la réunion des translatés de U. Puisque les translatées sont ouvertes, $G \setminus U$ est ouvert, donc U est fermé. De plus, puisque G est compact, seul un nombre fini de translatés suffisent à recouvrir G, ce qui implique que U est d'indice fini. On peut aussi voir que U est d'indice fini en remarquant qu'il contient un sous-groupe de la forme N_J.

4) Si U est un sous-groupe fermé d'indice fini dans G, alors $G \setminus U$ est une réunion fini de fermés, donc U est ouvert.

5) Soit $\{U_\lambda\}_\lambda$ une collection de sous-groupes ouverts de G. Alors chaque U_λ est fermé et donc $\bigcap_\lambda U_\lambda$ est fermé.

Inversement, soit U un sous-groupe fermé. Pour tout ensemble fini $J \subseteq I$, UN_J est un sous-groupe (car N_J est normal) ouvert (car $UN_J = \bigcup_{x \in U} xN_J$). Nous montrerons que

$$U = \bigcap_{J \subseteq I, J \text{ fini}} UN_J$$

Tout d'abord, il est clair que U est contenu dans cette intersection. Supposons que $x \notin U$. Nous montrerons que x n'est pas dans l'intersection en question. Puisque x n'est pas dans U, 1_G n'est pas dans Ux. Puisque Ux est fermé, $G \setminus Ux$ est un ouvert qui contient 1_G. Il existe donc un ensemble fini $J \subseteq I$ tel que $N_J \subseteq G \setminus Ux$. En particulier, $N_J \cap Ux = \emptyset$. Alors $x \notin UN_J$. En effet, si $x = ug$, où $u \in U$ et $g \in N_J$, alors $g = u^{-1}x \in N_J \cap Ux$, ce qui est contradictoire. Ceci termine la preuve. □

Ce théorème montre que dans un groupe profini G, les sous-groupes ouverts normaux forment une base d'ouverts autour de 1_G. Puisque l'espace topologique G est homogène[6], ce résultat nous donne une base d'ouverts autour de n'importe que point de G.

2.3.1. *Retour sur les nombres $p-$adiques.* Nous avons vu plus haut que les entiers $p-$adiques étaient isomorphes à une limite projective de groupes cycliques finis. Cela implique que $\mathbb{Z}_p$ est un groupe profini sous l'addition. On peut aussi montrer que l'opération de multiplication est continue, ce qui fait même de $\mathbb{Z}_p$ un anneau topologique.

2.4. **Le théorème fondamental de la théorie de Galois.** Nous sommes maintenant en mesure d'énoncer le théorème fondamental de la théorie de Galois.

Theorem 11 (Théorème fondamental de la théorie de Galois)**.** *Soit K/F une extension Galoisienne et soit $G = \mathrm{Gal}(K/F)$ son groupe de Galois. Alors pour tout sous-corps M de K contenant F, l'extension K/M est Galoisienne. De plus, il existe une correspondance bijective*

$$\{\textit{Sous-corps } M \textit{ de } K \textit{ contenant } F, K \supseteq M \supseteq F\} \leftrightarrow \{\textit{Sous-groupe fermé } H \textit{ de } G\}$$

donnée par $M \longmapsto \mathrm{Gal}(K/M)$ et $H \longmapsto K^H = \{x \in K : \sigma(x) = x \text{ pour tout } \sigma \in H\}$. Cette correspondance a les propriétés suivantes:

1. *Si H_1 et H_2 sont des sous-groupes fermés de G, alors $H_1 \subseteq H_2$ si et seulement si $K^{H_1} \supseteq K^{H_2}$.*
2. *M/F est une extension finie si et seulement $\mathrm{Gal}(K/M)$ est ouvert.*

[6]Un espace topologique X est dit homogène si pour toute paire d'éléments $x, y \in X$, il existe un homéomorphisme $\varphi : X \longrightarrow X$ tel que $\varphi(x) = y$. Dans le cas d'un groupe topologique, la multiplication par yx^{-1} est une tel homéomorphisme.

(3) *M/F est une extension Galoisienne si et seulement si* $\mathrm{Gal}(K/M)$ *est normal dans* G*, auquel cas* $\mathrm{Gal}(M/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/M)$.
(4) *Si* M_1 *et* M_2 *sont deux sous-corps de* K *contenant* F*, alors* $M_1 \cap M_2$ *correspond à* $\overline{\langle \mathrm{Gal}(K/M_1), \mathrm{Gal}(K/M_2)\rangle}$ *et* M_1M_2 *correspond à* $\mathrm{Gal}(K/M_1) \cap \mathrm{Gal}(K/M_2)$*, où la barre dénote la clôture topologique du groupe.*

Proof. Tout d'abord, il n'est pas difficile de se convaincre que K/M est une extension Galoisienne.

La preuve du reste de ce théorème se divise en deux parties. On établi d'abord la bijection, puis on vérifie les propriétés.

Avant tout, rappelons que pour toute extension Galoisienne finie L/F, les fonctions de restriction

$$\rho_L : G \longrightarrow \mathrm{Gal}(L/F)$$

sont continues. Une application du lemme de Zorn nous permet aussi de montrer que tout plongement $\varphi : M \longrightarrow K$ fixant F s'étend à un automorphisme de K fixant F. En particulier, cela implique que les projections ρ_L sont surjectives.

Supposons maintenant que M/F est une extension finie et montrons que $\mathrm{Gal}(K/M)$ est fermé dans G. Pour se faire, nous montrerons que le complément de $\mathrm{Gal}(K/M)$ dans G est ouvert. Soit $\sigma \in \mathrm{Gal}(K/M)^c$. Alors il existe un élément $m \in M$ tel que $\sigma(m) \neq m$. Soit L une extension galoisienne finie de F contenant M, i.e. $L \supseteq M \supseteq F$ (une telle extension existe, par la théorie de Galois finie). Alors $\sigma|_L \in \mathrm{Gal}(L/F)$ et $U = \rho_L^{-1}(\{\sigma|_L\})$ est un ouvert non-vide de G (par la continuité et la surjectivité des projections et puisque les $\mathrm{Gal}(L/F)$ sont muni de la topologie discrète). De plus $\mathrm{Gal}(K/M) \cap U = \emptyset$, ce qui montre que $\mathrm{Gal}(K/M)$ est fermé lorsque M/F est finie.

Dans le cas où M/F est de degré quelconque, on note que $M = \bigcup_{F \subseteq M_i \subseteq M, [M_i:F] < \infty} M_i$. De plus, on voit que $\mathrm{Gal}(K/M) = \bigcap_{F \subseteq M_i \subseteq M, [M_i:F] < \infty} \mathrm{Gal}(K/M_i)$. Puisque chaque $\mathrm{Gal}(K/M_i)$ est fermé, $\mathrm{Gal}(K/M)$ est fermé.

On peut maintenant montrer que

$$K^{\mathrm{Gal}(K/M)} = M$$

L'inclusion $\supseteq$ est simple à voir. De l'autre côté, supposons que $x \notin M$. Alors x est contenu dans une extension Galoisienne finie L/M (le polynôme minimal de x sur F peut être vu comme un polynôme à coefficient dans M). Puisque x n'est pas dans M, le polynôme minimal de x sur M est de degré > 1, donc il existe un automorphisme $\sigma \in \mathrm{Gal}(L/M)$ tel que $\sigma(x) \neq x$. Par la remarque précédente, cet automorphisme s'étend à un automorphisme de K/M. Mais alors $x \notin K^{\mathrm{Gal}(K/M)}$ puisqu'il n'est pas fixé par cette extension de σ. Ceci termine la preuve que $K^{\mathrm{Gal}(K/M)} = M$.

Pour terminer la preuve de la première partie, il ne reste plus qu'à montrer que

$$\mathrm{Gal}(K/K^H) = H$$

pour tout sous-groupe H fermé de G. Soit donc H un sous-groupe fermé de G. Posons $M = K^H$ et $H' = \mathrm{Gal}(K/K^H)$. On remarque tout d'abord que $H \subseteq H'$. De plus, par le résultat du paragraphe précédent, $K^{H'} = K^H$. Soit maintenant N un sous-groupe normal ouvert de H' et posons $L = K^N$. Alors $L^{H'/N} = L^{HN/N} = M$ (si un élément de K est fixé par N et par H'/N, il est fixé par H', etc.). Puisque N est normal et ouvert dans H', il est d'indice fini dans H'. Par le lemme d'Artin, on a $|H'/N| = [L : L^{H'/N}] = |HN/N|$, d'où $H' = HN$ puisque $N \subseteq HN \subseteq H'$. Par la preuve du

théorème 1, on en déduit que H est dense dans H'. Or nous avons montré que H est fermé, d'où $H = H' = \mathrm{Gal}(K/K^H)$. Ceci prouve que la bijection est bien une.

La seconde partie de la preuve ressemble à la preuve du théorème fondamental de la théorie de Galois pour les extensions finies et les détails seront laissé au lecteur. Par exemple, on peut montrer que si $\sigma \in G$, alors $\mathrm{Gal}(K/\sigma(M)) = \sigma\mathrm{Gal}(K/M)\sigma^{-1}$. On peut ensuite utiliser ce résultat pour montrer que M/F est une extension Galoisienne si et seulement si $\mathrm{Gal}(M/F)$ est normal dans G. □

En terminant, notons que plusieurs théorèmes en théorie de Galois finie se généralisent en théorie de Galois infinie.

2.5. **Exemples de groupes de Galois infini.**

2.5.1. *Le groupe de Galois absolu de* $\mathbb{Q}$. Avec la théorie que nous avons développée, on peut aborder le problème inverse de Galois d'une nouvelle façon. En effet, le théorème fondamental de la théorie de Galois nous indique que les extensions galoisiennes finies de $\mathbb{Q}$ sont en bijection avec les sous-groupes ouverts normaux de $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Le problème revient alors à étudier la topologie de $G_{\mathbb{Q}}$. Je laisse à François le soin de nous en dire davantage à ce sujet!

2.5.2. *Groupe de Galois de* $\overline{\mathbb{F}_p}/\mathbb{F}_p$. On sait que $\mathrm{Gal}(\mathbb{F}_{p^m}) \cong C_m$, le groupe cyclique à m éléments. On sait aussi que lorsque $m|n$, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ et on a un homomorphisme naturel $a \pmod n \longmapsto a \pmod m : C_n \longrightarrow C_m$. En d'autre mots, les groupes de Galois des corps finis de caractéristique p forment un système projectif sur les entiers positifs. La limite projective de ce système est dénotée

$$\hat{\mathbb{Z}} = \varprojlim_n C_n$$

d'où $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}$.

2.5.3. *Une* $\mathbb{Z}_p-$*extension.* Une $\mathbb{Z}_p$-extension est une extension Galoisienne dont le groupe de Galois est isomorphe à $\mathbb{Z}_p$, le groupe (additif) des entiers $p-$adiques. On peut construire une $\mathbb{Z}_p$-extension de la façon suivante. Soit $K = \bigcup_{n\geq 1} \mathbb{F}_{p^{p^n}}$. Alors $K/\mathbb{F}_p$ est une extension de Galois dont le groupe de Galois est

$$\varprojlim_{n\geq 0} \mathrm{Gal}(\mathbb{F}_{p^{p^n}}/\mathbb{F}_p) = \varprojlim_{n\geq 0} C_{p^n} = \mathbb{Z}_p$$

En terminant, notons qu'il faut travailler plus fort pour trouver une $\mathbb{Z}_p-$extensions de $\mathbb{Q}$.