Groupes Profinis et Théorie de Galois

Par Bruno Deschamps
Université du Maine

Table des matières

1 Nombres p-adiques **4**
- 1.1 L'anneau de entiers p-adiques . . . 4
  - 1.1.1 Propriétés élémentaires . . . 4
  - 1.1.2 Le groupe des unités p-adiques. . . . 5
  - 1.1.3 Topologie sur $\mathbb{Z}_p$ et distance p-adique. . . . 6
- 1.2 Le corps des nombres p-adiques . . . 8
  - 1.2.1 Le corps $\mathbb{Q}_p$ . . . 8
  - 1.2.2 Développement de Hensel . . . 8
- 1.3 Les sous-groupes de $\mathbb{Z}_p$ . . . 11

2 Groupes profinis **12**
- 2.1 Rappels sur les groupes topologiques . . . 12
- 2.2 Limites projectives . . . 16
- 2.3 Groupes profinis . . . 20
  - 2.3.1 Définition, propriétés topologiques . . . 20
  - 2.3.2 Caractérisation topologique . . . 22
  - 2.3.3 Le groupe $\mathbb{Z}_p^*$. . . . 26
  - 2.3.4 Le groupe $\widehat{\mathbb{Z}}$ . . . 28

3 Théorie de Sylow et groupes pronilpotents **30**
- 3.1 Théorie de Sylow . . . 30
  - 3.1.1 Nombres surnaturels . . . 30
  - 3.1.2 Indices et théorème de Lagrange . . . 31
  - 3.1.3 Sous-groupes de Sylow . . . 32
- 3.2 Groupes pronilpotents . . . 34
  - 3.2.1 Pronilpotence . . . 34
  - 3.2.2 Sous-groupe de Frattini . . . 35

4 Proliberté **37**
- 4.1 Rang . . . 37
  - 4.1.1 Groupes profinis de type fini . . . 37
  - 4.1.2 Rang topologique . . . 38
- 4.2 Complétions profinies . . . 40
- 4.3 Groupes prolibres . . . 43

5 Théorie de Galois **45**
- 5.1 Groupe de Galois . . . 45
  - 5.1.1 Clôture séparable . . . 45
  - 5.1.2 Topologie de Krull . . . 46
- 5.2 Théorie de Galois . . . 47
  - 5.2.1 Correspondances galoisiennes . . . 47
  - 5.2.2 Propriétés galoisiennes . . . 49

5.3 Le théorème de Waterhouse 56
5.3.1 La méthode de Noether 56
5.3.2 Les groupes profinis sont des groupes de Galois 57

6 Quelques exemples de groupes de Galois **58**
6.1 Le groupe des Galois absolu d'un corps fini 58
6.2 Le groupe de Galois de l'extension $\mathbb{Q}^{ab}/\mathbb{Q}$ 60
6.3 Le groupe de Galois absolu de $K((X))$ 62
6.3.1 Le corps des séries de Puiseux 62
6.3.2 Le cas $K = \overline{K}$ de caractéristique 0 64
6.3.3 Cas $\mathbb{Q}^{ab} \subset K$ 64
6.3.4 Le cas réel clos 66

Chapitre 1

Nombres p-adiques

1.1 L'anneau de entiers p-adiques

1.1.1 Propriétés élémentaires

On considère un nombre premier p et pour tout entier $n \in \mathbb{N}^*$, on note $A_n = \mathbb{Z}/p^n\mathbb{Z}$ muni de sa structure d'anneau. On désigne par $\varphi_n : A_{n+1} \longrightarrow A_n$ la surjection canonique (les φ_n sont des morphismes d'anneaux et on a $Ker\varphi_n = p^n A_{n+1}$). On considère l'anneau produit $\prod_n A_n$ et le sous-ensemble E de $\prod_n A_n$ constitué des éléments $(x_n)_n \in \prod_n A_n$ tel que

$$\forall n \in \mathbb{N}^*,\ \varphi_n(x_{n+1}) = x_n$$

Il est clair, puisque les φ_n sont des morphismes d'anneaux, que $\prod_n A_n$ confère à E une structure d'anneau.

Définition 1.— *On appelle anneau des entiers p-adiques, le sous-anneau $\mathbb{Z}_p$ de $\prod_n A_n$ constitués des éléments $(x_n)_n \in \prod_n A_n$ tel que $\forall n \in \mathbb{N}^*,\ \varphi_n(x_{n+1}) = x_n$.*

Proposition 2.— *L'anneau $\mathbb{Z}_p$ est un anneau commutatif, unitaire, de caractéristique 0.*

Preuve: $\mathbb{Z}_p$ est visiblement commutatif puisque $\prod_n A_n$ l'est. Le neutre de $\prod_n A_n$ est l'élément $(x_n)_n$ avec $x_n = 1$ pour tout n, il est visiblement dans $\mathbb{Z}_p$. Soit m un entier, il existe un entier n tel que $m < p^n$ et dans A_n on alors $m.1 \neq 0$ ce qui justifie que dans $\mathbb{Z}_p$, $m.1 \neq 0$, c'est-à-dire que $\mathbb{Z}_p$ soit de caractéristique 0.

Proposition 3.— *1/ La multiplication par p dans $\mathbb{Z}_p$ est injective.*

2/ Soit $x = (x_n)_n \in \mathbb{Z}_p$. Les propositions suivantes sont équivalentes:

i) x est divisible par p

ii) $x_1 = 0$.

Preuve: 1/ Soit $x = (x_n)_n \in \mathbb{Z}_p$ tel que $px = 0$. On a donc $px_{n+1} = 0$ pour tout n, donc $x_{n+1} = p^n y_{n+1}$ avec $y_{n+1} \in A_{n+1}$. Ainsi,

$$x_n = \varphi_n(x_{n+1}) = \varphi_n(p^n).\varphi_n(y_{n+1}) = 0$$

et par suite $x = 0$.

2/ $i) \Rightarrow ii)$ Immédiat.

ii) $\Rightarrow$ *i)* On a $x_{n+1} = py_{n+1}$ avec $y_{n+1} \in A_n$ pour tout $n \geq 1$. Il reste à voir que l'on peut choisir les éléments y_n de sorte que $(y_n)_n \in \mathbb{Z}_p$. Pour $n \geq 2$ posons :

$$\mathcal{E}_n = \{(y_k)_{k=2,\cdots,n} / \forall k = 2, \cdots, n,\ x_k = py_k \text{ et } \varphi_{k-1}(y_k) = y_{k-1}\}$$

Il est clair que pour tout $n \geq 2$, l'ensemble $\mathcal{E}_n$ est fini et non vide. Pour $n \geq 2$, posons

$$\begin{array}{rccc} f_n\ : & \mathcal{E}_{n+1} & \longrightarrow & \mathcal{E}_n \\ & (y_k)_{k=2,\cdots,n+1} & \longmapsto & (y_k)_{k=2,\cdots,n} \end{array}$$

Le système $(\mathcal{E}_n, f_n)_n$ est alors un système projectif, et, en vertu de ???, on a

$$\varprojlim \mathcal{E}_n \neq \emptyset$$

Un élément de $\varprojlim \mathcal{E}_n$ définit alors immédiatement une suite $y = (y_n)_n \in \mathbb{Z}_p$, qui vérifie bien $x = py$.

De la même manière, on obtient la caractérisation suivante :

Proposition 4.— *Soit $k \in \mathbb{N}^*$ et $x = (x_n)_n \in \mathbb{Z}_p$. Les propositions suivantes sont équivalentes:*

i) x est divisible par p^k

ii) $x_k = 0$.

On note $\epsilon_n : \mathbb{Z}_p \longrightarrow A_n$ la n-ième application coordonnée.

Corollaire 5.— *La suite*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\epsilon_n} A_n \longrightarrow 0$$

est exacte.

Preuve: La multiplication par p est injective dans $\mathbb{Z}_p$ donc la multiplication par p^n aussi. L'application ϵ_n est visiblement surjective. Il est clair que $p^n\mathbb{Z}_p \subset Ker(\epsilon_n)$, soit maintenant un élément $x = (x_n)_n \in Ker(\epsilon_n)$. On a $x_{p^n} = 0$ et par la proposition précédente, on a donc $x \in p^n\mathbb{Z}_p$.

Corollaire 6.— *Le groupe quotient $\mathbb{Z}_p/p^n\mathbb{Z}_p$ est isomorphe au groupe $\mathbb{Z}/p^n\mathbb{Z}$.*

1.1.2 Le groupe des unités p-adiques.

Posons $U = \mathbb{Z}_p^*$, on appelle ce groupe *groupes des unités p-adiques.*

Proposition 7.— *Soit $x = (x_n)_n \in \mathbb{Z}_p$, les propositions suivantes sont équivalentes:*

i) $x \in U$,

ii) x n'est pas divisible par p,

iii) $x_1 \neq 0$,

iv) $\exists n \in \mathbb{N}^*,\ x_n \in (\mathbb{Z}/p^n\mathbb{Z})^*$,

v) $\forall n \in \mathbb{N}^*,\ x_n \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

Preuve: *i)* $\Rightarrow$ *ii)* Soit $y \in \mathbb{Z}_p$ tel que $xy = 1$. Donc $x_1 \neq 0$, donc x n'est pas divisible par p.

ii) $\Rightarrow$ *iii*) Déjà fait.

iii) $\Rightarrow$ *iv*) Evident

iv) $\Rightarrow$ *v*) La restriction de φ_n à A_{n+1}^* est un homomorphisme surjectif sur A_n^*. Donc si $x_{n_0} \in A_{n_0}^*$,a lors par récurrence croissante et décroissante on en déduit bien que $x_n \in A_n^*$.

v) $\Rightarrow$ *i*) Si chaque x_n est inversible alors $(x_n^{-1})_n\mathbb{Z}_p$ et cet élément est visiblement l'inerse de x.

Proposition 8.— *Soit $x \in \mathbb{Z}_p$ non nul. Il existe un unique couple $(n, u) \in \mathbb{N} \times U$ tel que*

$$x = p^n u$$

Preuve: x étant non nul, il existe un plus grand entier $n \in \mathbb{N}$ tel que $\epsilon_n(x) = 0$. On a alors x divisible par p^n et donc $x = p^n u$. Par maximalité de n, u n'est pas divisible par p, donc $u \in U$. L'unicité de cette décomposition est evidente.

1.1.3 Topologie sur $\mathbb{Z}_p$ et distance p-adique.

Le groupe A_n est fini, la topologie discrète lui confère une structure de groupe topologique compact. On muni $\prod_n A_n$ de la topologie produit ce qui en fait un espace topologique compact (théorème de Tychonov). Cette topologie induit une topologie sur $\mathbb{Z}_p$ que nous considérerons à présent.

Proposition 9.— *L'ensemble $\mathbb{Z}_p$ est un espace compact dans lequel $\mathbb{Z}$ est dense.*

Preuve: Pour montrer que $\mathbb{Z}_p$ est compact, il faut et il suffit de prouver qu'il est fermé dans $\prod_n A_n$. Soit $x = (x_n)_n \in \prod_n A_n/\mathbb{Z}_p$. Il existe donc un entier n tel que $\varphi_n(x_{n+1}) \neq x_n$. Considérons l'ensemble

$$V = \{x_1\} \times \cdots \times \{x_n\} \times \{x_{n+1}\} \times A_{n+2} \times \cdots$$

C'est un ouvert de $\prod_n A_n$ qui voisine x. Il est clair que $V \cap \mathbb{Z}_p = \emptyset$, donc $\prod_n A_n/\mathbb{Z}_p$ est un ouvert et par suite $\mathbb{Z}_p$ est fermé dans un compact donc compact.

Une base d'ouverts de $\mathbb{Z}_p$ est donnée par les ensembles $U = \prod_n E_n \cap \mathbb{Z}_p$ avec $E_n = A_n$ pour $n \geq n_0$. Soit $x = (x_n)_n \in U$, considérons x_{n_0} comme entier naturel. Alors x_{n_0} dans $\mathbb{Z}_p$ s'écrit $(x_1, x_2, \cdots, x_{n_0}, x_{n_0}, \cdots)$ et donc $\mathbb{Z} \cap U \neq \emptyset$.

Définition 10.— *Soit $x = (x_n)_n \in \mathbb{Z}_p$. On appelle valuation p-adique de x l'entier naturel:*

$$\nu(x) = Sup(n \in \mathbb{N}^* / \ x_1 = \cdots = x_n = 0)$$

si $x \neq 0$ ($\nu(x) = 0$ si $x_1 \neq 0$). On pose $\nu(0) = +\infty$. Pour tout couple $(x, y) \in \mathbb{Z}_p$, on pose:

$$d(x, y) = e^{-\nu(x-y)}$$

On appelle la fonction d, distance p-adique.

Lemme 11.— *Soit $x \in \mathbb{Z}_p$ non nul et $(n, u) \in \mathbb{N} \times \mathbb{Z}_p^*$ l'unique couple tel que $x = p^n u$. On a*

$$\nu(x) = n$$

Preuve : Posons $u = (u_1, u_2, \cdots) \in \mathbb{Z}_p^*$. On a donc $u_1 \neq 0$ et donc $u_2 \not\equiv p \, mod(p^2)$ c'est-à-dire $pu_2 \neq 0$. Ainsi $pu = (0, pu_2, pu_3, \cdots)$ avec $pu_2 \neq 0$. Par récurrence immédiate, on trouve que

$$p^n.u = (0, \cdots, 0, p^n u_{n+1}, p^n u_{n+2}, \cdots)$$

avec $p^n u_{n+1} \neq 0$. On a donc bien $\nu(p^n u) = n$.

Si $x \in \mathbb{Z}^*$ alors il existe un unique entier n et un unique entier m premier avec p tels que $x = p^n m$. Si l'on regarde l'image de l'entier x dans $\mathbb{Z}_p$ alors ce dernier s'écrit $p^n y$ où y est l'image de m dans $\mathbb{Z}_p$. Comme m est premier à p, on en déduit que $y \in \mathbb{Z}_p^*$ et que par suite $\nu(x) = n$. C'est-à-dire que la restriction de ν à $\mathbb{Z}$ est la valuation p-adique traditionnelle sur les entiers. Ainsi ν représente l'extension naturel de la valuation p-adique sur $\mathbb{Z}$ à $\mathbb{Z}_p$.

Corollaire 12.— *L'application ν est une valuation sur l'anneau $\mathbb{Z}_p$. i.e. L'application*

$$\nu : \mathbb{Z}_p \to \mathbb{N} \cup \{+\infty\}$$

vérifie :

1/ Pour tout $x \in \mathbb{Z}_p$, $\nu(x) = 0 \Longleftrightarrow x = 0$

2/ Pour tout $x, y \in \mathbb{Z}_p$, $\nu(xy) = \nu(x) + \nu(y)$ (en convenant que $+\infty + n = +\infty$ pour tout $n \in \mathbb{N} \cup \{+\infty\}$).

3/ Pour tout $x, y \in \mathbb{Z}_p$, $\nu(x + y) = Inf(\nu(x), \nu(y))$.

Preuve : L'assertion 1/ est immédiate par définition. Soit maintenant $x, y \in \mathbb{Z}_p$. Si l'un des deux est nul l'assertion 2/ est vérifiée. Si x et y sont non nuls alors soit $u, u^{'} \in \mathbb{Z}_p^*$ et $n, n^{'}$ deux entiers tels que $x = p^n u$ et $y = p^{n^{'}} u^{'}$. On a alors

$$xy = p^n p^{n^{'}} u u^{'} = p^{n+n^{'}} u^{''}$$

avec $u^{''} = u u^{'} \in \mathbb{Z}_p^*$. On a donc bien $\nu(xy) = \nu(x) + \nu(y)$. L'assertion 3/ est immédiate.

Corollaire 13.— *L'anneau $\mathbb{Z}_p$ est intègre.*

Preuve : En effet si $x, y \in \mathbb{Z}_p$ sont tous deux non nuls alors $\nu(x)$ et $\nu(y)$ sont tous deux différents de $+\infty$ et par suite $\nu(xy) = \nu(x) + \nu(y) \neq +\infty$, donc $xy \neq 0$.

Proposition 14.— *L'application d est une distance ultramétrique sur $\mathbb{Z}_p$ compatible avec la structure d'espace topologique décrite précédemment.*

Preuve: Le fait que d soit une distance ultramétrique provient immédiatement du fait que ν est une valuation.

Soit $a = (a_n)_n \in \mathbb{Z}_p$ et $\epsilon > 0$. Dire que $x \in B(a, \epsilon)$ équivaut à dire que $\nu(x - a) > -log(\epsilon)$ c'est-à-dire $\nu(x - a) \geq n_0$ avec $n_0 = E(-log(\epsilon)) + 1$, c'est-à-dire que si $x = (x_n)_n$ alors $x_n = a_n$ pour tout $n < n_0$. On en déduit donc que:

$$B(a, \epsilon) = \left(\{a_1\} \times \cdots \times \{a_{n_0 - 1}\} \times \prod_{n \geq n_0} A_n \right) \cap \mathbb{Z}_p$$

Ces derniers ensembles forment une base de la topologie de $\mathbb{Z}_p$. D'où l'égalité des topologies.

Corollaire 15.— *L'espace métrique $\mathbb{Z}_p$ est complet, c'est le complété pour la distance p-adique de $\mathbb{Z}$.*

Preuve: L'espace $\mathbb{Z}_p$ est un espace métrique compact il donc est complet. La densité de $\mathbb{Z}$ dans $\mathbb{Z}_p$ implique bien que $\mathbb{Z}_p$ est le complété de $\mathbb{Z}$ pour d.

Corollaire 16.— *L'espace métrique $\mathbb{Z}_p$ est un anneau topologique. (i.e. les applications d'addition et de multiplication, de $\mathbb{Z}_p \times \mathbb{Z}_p$ dans $\mathbb{Z}_p$, sont continues.)*

Preuve:

1.2 Le corps des nombres p-adiques

1.2.1 Le corps $\mathbb{Q}_p$

Définition 17.— *L'anneau $\mathbb{Z}_p$ est commutatif, unitaire et intègre. On appelle corps des nombres p-adiques, le corps des fractions, noté $\mathbb{Q}_p$, de $\mathbb{Z}_p$.*

Remarque: Le corps $\mathbb{Q}_p$ est donc muni naturellement d'une valuation et d'une distance p-adique qui prolongent celles de $\mathbb{Z}_p$. On remarque alors que $\mathbb{Z}_p$ est l'ensemble des $x \in \mathbb{Q}_p$ tels que $\nu(x) \geq 0$. Remarquons aussi que les inversibles de $\mathbb{Z}_p$ sont les $x_i n\mathbb{Q}_p$ tels que $\nu(x) = 0$.

Proposition 18.— *Le corps $\mathbb{Q}_p$ est complet (c'est le complété de $\mathbb{Q}$ pour la distance p-adique), localement compact et $\mathbb{Z}_p$ est un sous-anneau ouvert de $\mathbb{Q}_p$.*

Preuve: Exercice.

1.2.2 Développement de Hensel

Théorème 19.— • *Soient $r \in \mathbb{Z}$ et $(a_n)_{n\geq r}$ une suite d'éléments dans $\{0, 1, \cdots, p-1\} \subset \mathbb{Z}_p$. La série $\sum_{n\geq r} a_n p^n$ converge dans $\mathbb{Q}_p$.*

• *Soit $x \in \mathbb{Q}_p$, il existe un unique $r \in \mathbb{Z}$ et une unique suite $(a_n)_{n\geq r}$ d'éléments dans $\{0, 1, \cdots, p-1\} \subset \mathbb{Z}_p$ telle que $a_r \neq 0$ et*

$$x = \sum_{n\geq r} a_n p^n$$

Preuve: • Soit $S_n = \sum_{k=r}^{n} a_k p^k$. La suite $(S_n)_n$ est de Cauchy, car

$$\nu(S_n - S_m) = \nu(\sum_{k=m+1}^{n} a_k p^k \geq m + 1$$

et comme $\mathbb{Q}_p$ est complet, $(S_n)_n$ converge bien.

• Si $x \neq 0$, alors $r = \nu(x) \in \mathbb{Z}$. On a alors $\nu(xp^{-r}) = 1$ et donc il existe $a_r \in \{0, 1, \cdots, p-1\}$ tel que $\nu(xp^{-r} - a_r) \geq 1$, donc

$$\nu(x - a_r p^r) \geq r + 1$$

Supposons que pour $n \geq r$, on ait trouvé des éléments $a_r, \cdots, a_n \in \{0, 1, \cdots, p-1\}$ tels que

$$\nu(x - \sum_{k=r}^{n} a_k p^k) \geq n+1$$

alors $p^{-(n+1)} \left(x - \sum_{k=r}^{n} a_k p^k\right) \geq 0$ et par suite, il existe un $a_{n+1} \in \{0, 1, \cdots, p-1\}$ tel que

$$p^{-(n+1)} \left(x - \sum_{k=r}^{n} a_k p^k\right) - a_{n+1} \geq 1$$

c'est-à-dire

$$\nu(x - \sum_{k=r}^{n+1} a_k p^k) \geq n+2$$

Il en résulte que $\sum_{n \geq r} a_n p^n$ converge vers x.

Soit $(a_n)_n$ et $(b_n)_n$ deux suites d'éléments de $\{0, 1, \cdots, p-1\} \subset \mathbb{Z}_p$ telles que

$$x = \sum_{n \geq r} a_n p^n = \sum_{n \geq r} b_n p^n$$

(on suppose par exemple que $a_r \neq 0$). Pour $n \in \mathbb{N}$, posons

$$S_n = \sum_{k=r}^{n} (a_k - b_k) p^k$$

On a $S_n \to 0$, donc $\nu(S_n) \to +\infty$. Si $(a_n)_n \neq (b_n)_n$, soit n_0 le plus petit entier tel que $a_{n_0} \neq b_{n_0}$. On a alosr pour $n \geq n_0$,

$$S_n = (a_{n_0} - b_{n_0} p^{n_0} + \sum_{n=n_0+1}^{k} (a_k - b_k) p^k$$

Comme $\nu(a_k - b_k) = 0$ ou $+\infty$, on en déduit que

$$\nu(S_n) = n_0$$

ce qui est contradiction avec le fait que $\nu(S_n) \to +infty$.

Définition 20.— *Si $x \in \mathbb{Q}_p$, l'unique série $x = \sum_{n \geq r} a_n p^n$ s'appelle le développement de Hensel de x.*

Corollaire 21.— *L'anneau $\mathbb{Z}_p$ n'est pas dénombrable (plus précisement, $\sharp \mathbb{Z}_p = 2^{\aleph_0}$).*

Preuve: $\mathbb{Z}_p$ correspond dans $\mathbb{Q}_p$ au élément dont le développement en série de Hensel est de la forme :

$$\sum_{n \geq 0} a_n p^n$$

Ce développement étant unique, il existe donc une bijection ensembliste entre $\mathbb{Z}_p$ et $\{0, 1, \cdots, p-1\}^{\mathbb{N}}$. Le cardinal de ce dernier ensemble est visiblement égal à $2^{\aleph_0}$.

Proposition 22.— *Soit $x \in \mathbb{Q}_p$. Les propositions suivantes sont équivalentes :*

i) $x \in \mathbb{Q}$,

ii) Le développement de Hensel de x est périodique à partir d'un certain rang.

Preuve: *ii)* $\Rightarrow$ *i)* Soit $x \in \mathbb{Q}_p^*$, on a par hypothèse :

$$x = \sum_{j=r}^{k-1} a_j p^j + p^k(\alpha_0 + \alpha_1 p + \cdots + \alpha_{s-1}p^{s-1}) \sum_{n=0}^{+\infty} p^{ns}$$

Comme

$$\sum_{n=0}^{+\infty} p^{ns} = \lim_{m \to +\infty} \frac{1 - p^{(m+1)s}}{1 - p^s} = \frac{1}{1 - p^s}$$

et par suite, $x \in \mathbb{Q}$.

i) $\Rightarrow$ *ii)* Soit $x \in \mathbb{Q}^*$. Il existe des entiers r, a, b avec $(p, b) = 1$ tels que:

$$x = p^r \frac{a}{b}$$

La périodicité du développement de Hensel de x équivaut à celle du développement de $x^{'} = a/b$. Puisque p ne divise pas b, il existe un entier positif s tel que $p^s \equiv 1[b]$ et par suite,

$$x^{'} = \frac{a^{'}}{p^s - 1}$$

pour un certain entier $a^{'}$. On suppose $a^{'} > 0$. Soit alors $k \in \mathbb{N}$ tel que

$$0 < a^{'} < p^k$$

Puisque p^k et $p^s - 1$ sont premiers entre eux, l'équation

$$\beta(p^s - 1) - \alpha p^k = a^{'}$$

admet une solution $(\alpha, \beta) \in \mathbb{Z}^2$ telle que

$$0 \leq \alpha \leq p^s - 2$$

On a alors $0 < \beta < p^k$ et par suite :

$$\begin{array}{rcl} \alpha & = & \alpha_0 + \alpha_1 p + \cdots + \alpha_{s-1}p^{s-1} \ avec \ \alpha_i \in \{0, 1, \cdots, p-1\} \\ \beta & = & a_0 + a_1 p + \cdots + a_{k-1}p^{k-1} \ avec \ a_i \in \{0, 1, \cdots, p-1\} \end{array}$$

On a alors

$$\begin{array}{rcl} x^{'} & = & \beta - p^k \frac{\alpha}{p^s - 1} \\ & = & a_0 + a_1 p + \cdots + a_{k-1}p^{k-1} \\ & & + p^k(\alpha_0 + \alpha_1 p + \cdots + \alpha_{s-1}p^{s-1}) \sum_{n=0}^{+\infty} p^{ns} \end{array}$$

donc $x^{'}$ a bien un développement de Hensel périodique. Si maintenant $a^{'} < 0$ alors $-x^{'}$ a un développement de Hensel périodique, mais comme

$$-1 = \sum_{n \geq 0} (p-1)p^n$$

on en déduit que $x^{'} = -1.(-x^{'})$ a un développement de Hensel périodique, ce qui achève la preuve.

1.3 Les sous-groupes de $\mathbb{Z}_p$

Proposition 23.— *L'anneau $\mathbb{Z}_p$ est un anneau de valuation (i.e. $\mathbb{Z}_p$ est principal et possède un unique idéal premier).*

Preuve: Soit I un idéal de $\mathbb{Z}_p$ et $n_0 \in \mathbb{N}$ et $x \in I$ tel que $\nu(x) = n_0$ soit minimal. On a alors $x = p^{n_0}u$ avec $u \in U$ et donc $x\mathbb{Z}_p = p^{n_0}\mathbb{Z}_p \subset I$. Soit maintenant, $y \in I$. On a $y = p^n v$ avec $n \geq n_0$ et $v \in U$. On a alors $y = p^{n_0}(p^{n-n_0}v) \in p^{n_0}\mathbb{Z}_p$. Donc $I = p^{n_0}\mathbb{Z}_p$ est principal.

Les idéaux de $\mathbb{Z}_p$ sont donc les $p^n\mathbb{Z}_p$, seul $p\mathbb{Z}_p$ est premier.

Théorème 24.— *Soit H un sous-groupe non nul de $\mathbb{Z}_p$. Les propositions suivantes sont équivalentes :*

i) H est un idéal de $\mathbb{Z}_p$,

ii) $\exists n \in \mathbb{N}$, $H = p^n\mathbb{Z}_p$,

iii) H est ouvert,

iv) H est fermé,

v) H est d'indice fini.

et, dans ces conditions, on a $H \simeq \mathbb{Z}_p$.

Preuve: *i*) $\Rightarrow$ *ii*) C'est une conséquence de la proposition précédente.

ii) $\Rightarrow$ *iii*) Immédiat. *iii*) $\Rightarrow$ *iv*) Immédiat.

iv) $\Rightarrow$ *i*) Soit $x \in H$ et $y = \sum_{k\geq 0} a_k p^k \in \mathbb{Z}_p$. Posons pour tout $n \in \mathbb{N}$,

$$y_n = \sum_{k=0}^{n} a_k p^k$$

On a $y_n \in \mathbb{Z}$, donc $xy_n \in H$. Par ailleurs $\lim_n y_n = y$ et comme la multiplication est continue et que H est fermé, on a $\lim_n xy_n = xy \in H$. Donc H est un idéal.

iii) $\Rightarrow$ *v*) Comme $\mathbb{Z}_p$ est compact, tout sous-groupe d'indice fini est ouvert.

v) $\Rightarrow$ *iii*) Soit $n = [\mathbb{Z}_p : H]$, on a $n(\mathbb{Z}_p/H) = 0$, donc $n\mathbb{Z}_p \subset H$. Mais $n\mathbb{Z}_p$ est un idéal de $\mathbb{Z}_p$ donc un sous-groupe ouvert. Donc H est ouvert.

Si $H = p^n\mathbb{Z}_p$, l'application $x \mapsto p^n x$ définit un isomorphisme continu de groupe topologique de $\mathbb{Z}_p$ sur H. Comme $\mathbb{Z}_p$ est compact et que H est séparé, cette application est bicontinue.

Remarque: Le sous-groupe $\{0\}$ est fermé dans $\mathbb{Z}_p$. C'est le seul sous-groupe fermé de $\mathbb{Z}_p$ qui ne soit pas d'indice fini.

Chapitre 2

Groupes profinis

2.1 Rappels sur les groupes topologiques

Définition 25.— *Soit G un groupe et Ω une toplogie sur G. On dit que (G, Ω) est un groupe topologique, si les opérations $(x, y) \mapsto xy$ et $x \mapsto x^{-1}$ sont continues.*

Si G est un groupe topologique alors les opérations $x \mapsto ax$ et $x \mapsto xa$ (pour $a \in G$ fixé) et $x \mapsto x^{-1}$ sont donc des homéomorphismes. On peut remarquer qu'un groupe muni d'une topologie est un groupe topologique si et seulement si l'application $G \times G \to G$ définie par $(x, y) \mapsto xy^{-1}$ est continue.

Proposition 26.— *Tout sous-groupe d'un groupe topologique est un groupe topologique. Tout produit de groupes topologiques est un groupe topologique. Si G est un groupe topologique et H un sous-groupe distingué de G alors l'espace quotient G/H est un groupe topologique.*

Preuve: Exercice.

Si G désigne un groupe topologique et $\mathcal{V}$ un système fondamental de voisinages de l'élément neutre alors on a :

- $\forall U \in \mathcal{V},\ \exists V \in \mathcal{V},\ V.V \subset U$,
- $\forall U \in \mathcal{V},\ \exists V \in \mathcal{V},\ V^{-1} \subset U$,
- $\forall U \in \mathcal{V},\ \forall a \in G,\ \exists V \in \mathcal{V},\ V \subset aUa^{-1}$.

Ces propriétés sont la traduction de la continuité en le neutre e de G des applications $(x, y) \mapsto xy$, $x \mapsto x^{-1}$ et $x \mapsto ax^{-1}$. En fait ces trois propriétés caractérisent la topologie de G :

Proposition 27.— *Soit G un groupe et $\mathcal{V}$ une base de filtre de parties de G telle que :*

- $\forall U \in \mathcal{V},\ \exists V \in \mathcal{V},\ V.V \subset U$,
- $\forall U \in \mathcal{V},\ \exists V \in \mathcal{V},\ V^{-1} \subset U$,
- $\forall U \in \mathcal{V},\ \forall a \in G,\ \exists V \in \mathcal{V},\ V \subset aUa^{-1}$.

Il existe une et une seule topologie sur G telle que G soit un groupe topologique et telle que $\mathcal{V}$ soit un système fondamental de voisinages de l'élément neutre.

Preuve: Rappelons le lemme de topologie générale suivant :

Lemme 28.— *Soit E un ensemble et pour tout $x \in E$, $\mathcal{F}(x)$ un filtre de partie contenant x de E. Si pour tout $x \in E$ et tout $V \in \mathcal{F}(x)$ il existe $W \in \mathcal{F}(x)$ tel que pour tout $y \in W$, $V \in \mathcal{F}(y)$ alors il existe une et une seule topolgie sur E telle que pour tout $x \in E$ $\mathcal{F}(x)$ soit le filtre des voisinages de x. (Les ouverts de la topologie en question étant les parties $\mathcal{O}$ qui voisinent tous leurs points.)*

Considérons alors le filtre $\mathcal{F}$ engendré par $\mathcal{V}$. Ce filtre vérifie :
• $\forall U \in \mathcal{F},\ \exists V \in \mathcal{F},\ V.V \subset U$,
• $\forall U \in \mathcal{F},\ U^{-1} \in \mathcal{F}$,
• $\forall U \in \mathcal{F},\ \forall a \in G,\ aUa^{-1} \in \mathcal{F}$.

Si la topologie existe alors le filtre des voisinages d'un point a de G est $a\mathcal{F} = \mathcal{F}a$ (puisqu'alors G est un groupe topologique), ce qui prouve que si la topologie existe elle unique.

Soit $a \in G$, alors :
• Toute partie X de G qui contient un élément de $a\mathcal{F}$ est dans $a\mathcal{F}$.
• Toute intersection d'élément de $a\mathcal{F}$ est un élément de $a\mathcal{F}$.
• Tout élément de $a\mathcal{F}$ contient a, car tout élément U de $\mathcal{F}$ contient e. En effet, il existe $V \in \mathcal{F}$ tel que $V.V \subset U$. Par ailleurs, il existe $W \in \mathcal{F}$ tel que $W \subset V \cap V^{-1}$ et donc $W^{-1} \subset V$ et donc $W.W^{-1} \subset V.V \subset U$ et donc $e \in U$.
• Si $V \in a\mathcal{F}$, il existe $W \in a\mathcal{F}$ tel que pour tout $b \in W$, $V \in b\mathcal{F}$. En effet, soit $V \in \mathcal{F}$ et $W \in \mathcal{F}$ tel que $W.W \subset V$. Quelque soit $b \in a.W$, on a $b.W \subset a.W.W \subset a.V$, donc $aV \in b\mathcal{F}$.

Il existe donc une unique topologie sur G telle que le filtre des voisinages de a soit $a\mathcal{F}$. Les ouverts de cette topologie, sont les sont les $V \in a\mathcal{F}$ pour un certain a tel que $\forall b \in V$, $V \in b\mathcal{F}$. Reste à voir que cette topologie confère à G la structure de groupe topologique.

Soit a et b deux points de G, posons $x = au$ et $y = bv$. On a

$$(ab^{-1})^{-1}(xy^{-1}) = buv^{-1}b^{-1}$$

Soit U un voisinage de e, on a alors $buv^{-1}b^{-1} \in U$ si $uv^{-1} \in b^{-1}Ub = V$ ($\in \mathcal{F}$ par hypothèse). Il existe donc $W \in \mathcal{F}$ tel que $W.W \subset V$ et par suite, pour tout couple $(u, v) \in W.W$, on a $xy^{-1} \in (ab^{-1})U$, ce qui montre bien que l'application $(x, y) \mapsto xy^{-1}$ est continue au point (a, b).

Un système fondamental des voisinages d'un point $a \in G$ est alors donné par les ensembles $(aV)_{V\in\mathcal{V}} = (Va)_{V\in\mathcal{V}}$. Ainsi, la donnée locale de la topologie en e, définit la topologie sur G tout entier. On fera attention au fait que les éléments de $\mathcal{V}$ n'ont aucune raison *a priori* d'être ouverts. Par exemple, considérons le groupe $G = (\mathbb{R}, +)$. Si l'on prend $\mathcal{V} = \{[-a, a],\ a > 0\}$ alors l'unique topologie associée à $\mathcal{V}$ qui confère à $(\mathbb{R}, +)$ la structure de groupe topologique et ayant $\mathcal{V}$ pour système fondamental de voisinages de 0 est la topologie usuelle, celle définie par la valeur absolue usuelle. Pourtant, aucun élément de $\mathcal{V}$ n'est ouvert.

Un cas où les hypothèse de la proposition ??? sont vérifiées est lorsque l'on prend pour $\mathcal{V}$ une base de filtre de sous-groupes distingués de G (par exemple tous). Dans ces conditions, les éléments de cette base de filtre sont nécessairement ouverts. Plus précisément, si G est un groupe topologique et si H est un sous-groupe de G voisinant e, alors H est ouvert. En effet, il existe $U \subset H$ ouvert et comme $H = \bigcup_{x\in H} xU$, on en déduit que H est une réunion d'ouverts, donc ouvert.

Nous allons maintenant essayer de caractériser simplement la propriété d'être séparé pour un groupe topologique. Rappellons à cet effet que de manière générale pour un espace topologique $(E, \mathcal{T})$ quelconque, les popositions suivantes

i) E est séparé,

ii) La diagonale $\Delta = \{(x,x)/\ x \in E\} \subset E \times E$ est un fermé de $E \times E$ (cet espace étant muni de la topologie produit),

iii) pour tout élément $x \in E$, $\bigcap_{V\ voisinage\ de\ x} V = \{x\}$,

iv) pour tout élément $x \in E$, $\bigcap_V$ voisinage fermé de $_x\, V = \{x\}$,

sont équivalentes. Dans le cas des groupes topologiques, on a plus précisément :

Proposition 29.— *Soit G un groupe topologique. Les propositions suivantes sont équivalentes:*

i) G est séparé,

ii) $\{e\}$ est fermé,

ii$'$) il existe $a \in G$ tel que $\{a\}$ soit fermé.

Preuve: L'équivalence *ii)* $\Rightarrow$ *ii$'$)* provient du fait que l'application $x \longmapsto ax$ est un homéomorphisme de G.

i) $\Rightarrow$ *ii)* C'est une propriété vraie en toute généralité : dans un espace séparé, les points forment des ensembles fermés.

ii) $\Rightarrow$ *i)* L'application $f : (x,y) \longmapsto xy^{-1}$ est continue et $\{e\}$ est fermé, donc $f^{-1}(\{e\})$ est fermé, or $f^{-1}(\{e\})$ est la diagonale Δ de l'espace $G \times G$ et, comme nous l'avons rappelé précédement, cela implique bien que G soit séparé.

Corollaire 30.— *Soit G un groupe topologique et H un sous-groupe distingué. Le groupe G/H est séparé si et seulement si H est fermé.*

Preuve: Notons $\pi : G \to G/H$ la surjection canonique, c'est une application continue par définition de la topologie quotient. Si G/H est séparé alors $\{e\} \subset G/H$ est fermé et donc $\pi^{-1}(\{e\}) = H$ est fermé.

Réciproquement, soit $\Omega = G/H - \{e\}$, on a $\pi^{-1}(\Omega) = G - H$. Si H est fermé, $\pi^{-1}(\Omega)$ est donc un ouvert de G et par suite Ω est ouvert dans G/H par définition de la topologie quotient. Ainsi, $\{e\}$ est fermé dans G/H.

Corollaire 31.— *Soit G un groupe topologique compact et H un sous-groupe distingué. Le groupe G/H est compact si et seulement si H est fermé.*

Preuve: Puisque $\pi : G \to G/H$ est continue et que G est compact, G/H est quasi-compact, donc G/H est compact si et seulement si G/H est séparé c'est-à-dire si et seulement si H est fermé dans G.

Etudions maintenant les propriétés topologiques liées aux sous-groupes d'un groupe topologique.

Proposition 32.— *Soit G un groupe topologique.*

- *Tout sous-groupe ouvert est fermé.*
- *Si H est un sous-groupe contenant un ouvert non vide alors H est ouvert.*
- *Si G est compact alors les sous-groupes ouverts de G sont exactement les sous-groupes fermés d'indice fini.*

Preuve: • Soit U un sous-groupe ouvert de G. L'ensemble des τU où $\tau \in G/U$ forment une partition de G. Le complémentaire de U dans G est une réunion d'ensembles τU qui sont ouverts, donc est ouvert. Ainsi U est aussi fermé.

• Soient H un sous-groupe de G et U un ouvert non vide tel que $U \subset H$. Considérons $x \in U$, l'ensemble $U^{'} = x^{-1}U$ est un ouvert inclus dans H et contenant e. On a alors que $H = \bigcup_{h\in H} hU^{'}$ est une réunion d'ouverts, donc est un ouvert.

• Si G est compact, comme les τU pour $\tau \in G/U$ forment un recouvrement de G, on peut en extraire un recouvrement fini. Mais comme ce recouvrement est une partition, on en déduit que G/U est en fait fini. Réciproquement si U est un fermé d'indice fini, alors le complémentaire de U dans G est une réunion finie d'ensemble τU qui, étant fermés, assure bien que ce complémentaire est aussi fermé. Ainsi U est ouvert.

Proposition 33.— *Soit G un groupe topologique compact et H un sous-groupe ouvert de G. Il existe un sous-groupe ouvert distingué $H^{'}$ de G inclus dans H.*

Preuve: Soit $\widetilde{H} = \bigcap_{g\in G} gHg^{-1}$. $\widetilde{H}$ est un sous-groupe distingué fermé de G inclus dans H. Reste à voir que $\widetilde{H}$ est d'indice fini.

Soit $n = [G : H]$, G agît sur G/H par multiplication. C'est à dire que l'on a une application φ de G sur $Perm(G/H)$ définie par:

$$\varphi(g)(\alpha H) = g\alpha H$$

Si l'on identifie $Perm(G/H)$ à S_n alors φ est un morphisme de groupe. On constate alors que :

$$\begin{aligned}
x \in Ker(\varphi) &\Leftrightarrow \forall g \in G,\ xgH = gH \\
&\Leftrightarrow \forall g \in G,\ \forall h \in H,\ \exists h^{'} \in H,\ xgh = gh^{'} \\
&\Leftrightarrow \forall g \in G,\ \forall h \in H,\ \exists h^{'} \in H,\ x = gh^{'}h^{-1}g^{-1} \\
&\Leftrightarrow \forall g \in G,\ x \in gHg^{-1} \\
&\Leftrightarrow x \in \bigcap_{g\in G} gHg^{-1} \\
&\Leftrightarrow x \in \widetilde{H}
\end{aligned}$$

Donc $Ker(\varphi) = \widetilde{H}$ et par suite $G/\widetilde{H}$ est un sous-groupe de S_n. Donc $[G : \widetilde{H}] \leq n!$.

On étudie maintenant quelques propriétés liées aux morphismes de groupes topologiques.

Définition 34.— *Soit G et H deux groupe topologique. On appelle isomorphisme de groupe topologique tout isomorphisme de G sur H qui est un homéomorphisme.*

On rappelle que si E désigne un espace topologique, $\mathcal{R}$ une relation d'équivalence sur E et $\pi : E \to E/\mathcal{R}$ la surjection canonique, alors si Y désigne un autre espace topologique et $f : E/\mathcal{R} \to Y$ une application, alors f est continue si et seulement si $f \circ \pi : E \to Y$ est continue.

Proposition 35.— *Si G et H sont deux groupes topologiques et si $s : G \to H$ désigne un homomorphisme surjectif et continu alors il existe un isomorphisme continu entre $G/Ker(s)$ et H.*

Preuve: Si l'on note $\pi : G \to G/Ker(s)$ alors on sait qu'il existe un isomorphisme canonique $\theta : G/Ker(s) \to H$. Cet isomorphisme est continu car $\theta \circ \pi = s$ est continu.

Il n'y a pas de raison *a priori* pour que cet isomorphisme soit bicontinu. On a toutefois :

Corollaire 36.— *Soit* $1 \to N \to G \to H \to 1$ *est une suite exacte de groupes topologiques. Supposons que* $G \to H$ *soit continue,* G *compact,* N *fermé et* H *séparé. Il existe alors un isomorphisme de groupe topologique entre* H *et* G/N*.*

Preuve: L'application $\theta : G/Ker(s) \to H$ est bijective et continue. Comme G est compact et N fermé, on en déduit que G/N est compact. Maintenant, H est supposé séparé, donc θ est bicontinue.

2.2 Limites projectives

Définitions

Définition 37.— *Soit* $(I, \leq)$ *un ensemble pré-ordonné. On considère une famille d'ensemble* $(E_i)_{i\in I}$ *et pour tout couple* $i, j \in I$ *tel que* $i \leq j$ *une application* $\varphi_{ji} : E_j \to E_i$*. On dit que le système* $((E_i)_i, \varphi_{ji})$ *est projectif si*

- $\forall i \in I,\ \varphi_{ii} = Id_{E_i}$,
- $\forall i, j, k \in I,\ i \leq j \leq k \Longrightarrow \varphi_{ki} = \varphi_{kj} \circ \varphi_{ji}$.

La notion de système projectif est donc duale de celle de système inductif, la dualité residant dans le changement de sens des "flêches" du système. Tout comme pour les système inductifs, nous allons associer à un système projectif un objet universel.

Proposition 38.— *Soit* $((E_i)_i, \varphi_{ji})$ *un système projectif. Il existe un ensemble* S *et une famille d'applications* $\varphi_i : S \longrightarrow E_i$ *vérifiant les propriétés suivantes :*

1/ $\forall i, j \in I,\ i \leq j \Longrightarrow \varphi_i = \varphi_j \circ \varphi_{ji}$.

2/ Si S' *est un ensemble et pour* $i \in I$, $\varphi_i' : S' \longrightarrow E_i$ *est une famille d'applications vérifiant la propriété* $\forall i, j \in I,\ i \leq j \Longrightarrow \varphi_i' = \varphi_j' \circ \varphi_{ji}$ *alors il existe une et une seule application* $\theta : S' \longrightarrow S$ *telle que* $\varphi_i' = \varphi_i \circ \theta$.

Preuve: Considérons le sous-ensemble S de $\prod_i E_i$ constitué des uplets $(x_i)_i$ tel que pour tout $i \leq j$, $\varphi_{ji}(x_j) = x_i$ et pour $i \in I$ l'application projection $\varphi_i : S \longrightarrow E_i$. Il est clair que l'on a pour tout $i, j \in I$

$$i \leq j \Longrightarrow \varphi_i = \varphi_j \circ \varphi_{ji}$$

Soit maintenant S' un autre ensemble et pour $i \in I$, $\varphi_i' : S' \longrightarrow E_i$ une autre famille d'applications vérifiant la propriété

$$\forall i, j \in I,\ i \leq j \Longrightarrow \varphi_i' = \varphi_j' \circ \varphi_{ji}$$

Considérons un $x' \in S'$ et pour tout $i \in I$, posons

$$x_i = \varphi_i'(x) \in E_i$$

Considérons alors $x = (x_i)_i \in \prod_i E_i$. Il est clair que pour tout $j \geq i$ on a

$$\varphi_j(x) = \varphi_{ji} \circ \varphi_i(x)$$

puisque $\varphi_i(x) = \varphi_i^{'}(x^{'})$ et que $\varphi_j(x) = \varphi_j^{'}(x^{'})$. Ainsi, $x \in S$. Considérons alors l'application θ qui à $x^{'} \in S^{'}$ associe $x \in S$. Cette application vérifie visiblement que pour tout $i \in I$,

$$\varphi_i^{'} = \varphi_i \circ \theta$$

La dernière chose à vérifier est l'unicité de θ pour cette propriété. Si $\theta^{'}$ désigne une autre application ayant ces propriétés, alors en prenant $x^{'} \in S^{'}$ et en posant $x = (x_i)_i = \theta(x^{'})$ et $y = (y_i)_i = \theta^{'}(x^{'})$, on obtient que pour tout $i \in I$,

$$\begin{array}{rcccl} x_i & = & \varphi_i(x) & = & \varphi_i \circ \theta(x^{'}) \\ & = & \varphi_i^{'}(x^{'}) & = & \varphi_i \circ \theta^{'}(x^{'}) \\ & = & \varphi_i(y) & = & y_i \end{array}$$

Ainsi $x = y$ et donc $\theta^{'} = \theta$.

Dans la suite nous dirons, pour simplifier, que θ est l'unique application qui fait commuter les diagrammes.

Définition 39.— L'ensemble S obtenu précédemment est appellé limite projective (ou inverse) du système $((E_i)_i, \varphi_{ji})$ et on le note $\varprojlim E_i$.

La limite projective est donc un objet universel qui est caractérisé de manière unique à isomorphisme près. On a, en effet

Proposition 40.— *Soit $((E_i)_i, \varphi_{ji})$ un système projectif. Soit un ensemble S et une famille d'applications $\pi_i : S \longrightarrow E_i$ telle que $\forall i, j \in I$, $i \leq j \Longrightarrow \pi_i = \pi_j \circ \varphi_{ji}$. Supposons que, pour tout ensemble $S^{'}$ muni d'applications $\pi_i^{'} : S^{'} \longrightarrow E_i$ pour tout $i \in I$ telles que $\forall i, j \in I$, $i \leq j \Longrightarrow \pi_i^{'} = \pi_j^{'} \circ \varphi_{ji}$ alors il existe une et une seule application $\theta : S^{'} \longrightarrow S$ telle que $\pi_i^{'} = \theta \circ \pi_i$. Alors il existe une unique bijection ω de S sur $\varprojlim E_i$ telle que pour tout $x \in S$ et tout $i \in I$, $\pi_i(x) = \varphi_i \circ \omega$ et pour tout $x \in \varprojlim E_i$ et tout $i \in I$, $\varphi_i(x) = \pi_i \circ \omega$.*

Preuve: Soit $\theta : S \to \varprojlim E_i$ et $\theta^{'} : \varprojlim E_i \to S$ les uniques applications faisant commuter les diagrammes. L'application $\theta \circ \theta^{'} : \varprojlim E_i \to \varprojlim E_i$ fait commuter les diagrammes, donc est unique donc vaut Id.

Il est utile de remarquer, pour la suite, que les éléments d'une limite projective sont entièrement caractérisés par leur image sur les ensembles du système projectif associé. En d'autres termes, si $((E_i)_i, \varphi_{ji})$ désigne un système projectif alors les propositions suivantes sont équivalentes :

i) $x = y$,

ii) $\varphi_i(x) = \varphi_i(y)$ pour tout $i \in I$.

Pour finir, il faut mentioner le fait que la limite projective d'un système projectif $((E_i)_i, \varphi_{ji})$ peut être vide, même dans le cas où chaque E_i est non vide et chaque application φ_{ji} est surjective.

Limites projectives de groupes

Soit $(I, \leq)$ un ensemble pré-ordonné et $(G_i)_i$ une famille de groupes et pour tout $i \leq j$, $\varphi_{ji} : G_j \to G_i$ un homomorphisme de groupe tels que (G_i, φ_{ji}) forme un système projectif. Soit $\Omega = \varprojlim G_i$ et $\pi_i : \Omega \to G_i$ les applications de projection.

Si l'on considère sur Ω la structure de groupe induite par celle de $\prod_i G_i$, alors les π_i sont des homomorphismes de groupes. On considère dans ce paragraphe Ω muni de cette structure de groupe et on étudie quelques propriétés algébriques de cette structure.

Proposition 41.— *Soit G un groupe et pour tout i, un homomorphisme $\pi_i : G \to G_i$ tels que pour tout $i \leq j$, $\pi_i = \varphi_{ji} \circ \pi_j$. L'unique application $\theta : E \to \varprojlim E_i$ faisant commuter les diagrammes est un homomorphisme.*

Preuve: Soit $x, y \in G$. Posons $u = \theta(xy)$ et $v = \theta(x).\theta(y)$. On a $\varphi_i(u) = \pi_i(xy) = \pi_i(x).\pi_i(y) = \varphi_i(v)$. Donc $u = v$.

Corollaire 42.— *Soit G un groupe et pour tout i, un homomorphisme de groupe $\pi_i : G \to G_i$ tels que pour tout $i \leq j$, $\pi_i = \varphi_{ji} \circ \pi_j$. Supposons que, pour tout groupe G' muni d'homomorphismes $\pi_i' : G' \to G_i$ tels que pour tout $i \leq j$, $\pi_i' = \varphi_{ji} \circ \pi_j'$, il existe un unique homomorphisme de groupe $\theta : G' \to G$ tel que $\pi_i' = \pi \circ \theta$ pour tout i. Alors il existe un unique isomorphisme de groupe entre G et $\varprojlim G_i$ faisant commuter les diagrammes.*

Preuve: Immédiat.

Limites projectives d'espaces topologiques.

Soit (E_i, φ_{ji}) un sytème projectif. On suppose que chaque E_i est muni d'une topologie. On considère alors la topololologie produit sur $\prod_i E_i$ et par suite la topologie induite sur $\varprojlim E_i$. Les applications φ_i sont alors continues puisqu'il s'agit alors des restrictions des applications de projections $\overline{\varphi_i} : \prod_i E_i \to E_i$ (qui sont continues par définition de la topologie produit) à $\varprojlim E_i$.

Proposition 43.— *Si chaque espace E_i est séparé et si chaque application φ_{ji} est continue, alors $\varprojlim E_i$ est un sous-espace fermé de $\prod_i E_i$.*

Preuve: Soit $z = (z_i)_i \in \prod_i E_i$ avec $z \notin \varprojlim E_i$. Il existe donc deux indices $i \leq j$ tel que $\varphi_{ji}(z_j) \neq z_i$. Soit U et V deux ouverts disjoints de E_i tels que $z_i \in U$ et $\varphi_{ji}(z_j) \in V$. Considérons

$$W = \left\{ x = (x_i)_i \in \prod_i E_i / \ x_i \in U, \ \varphi_{ji}(x_j) \in V \right\}$$

On a $z \in W$ et $W \cap \varprojlim E_i = \emptyset$. On a $W = \prod_i A_i$ avec $A_i = U$, $A_j = \varphi_{ji}^{-1}(V)$ et $A_k = E_k$ pour $k \neq i, j$. Comme φ_{ji} est continue, A_j est ouvert et par suite W aussi. On en déduit donc que le complémentaire de $\varprojlim$ dans $\prod_i E_i$ est ouvert.

Corollaire 44.— *Si chaque espace E_i est compact et si chaque application φ_{ji} est continue, alors $\varprojlim E_i$ est un espace compact.*

Preuve: Le théorème de Tychonoff affirme que $\prod_i E_i$ est compact, par la proposition précédente, $\varprojlim E_i$ est fermé dans un compact donc est compact.

On rappelle qu'un espace topologique E est dit *totalement discontinu* si la composante connexe de tout point $a \in E$ (i.e. la plus grande partie connexe contenant a) est réduite à $\{a\}$.

Proposition 45.— *Si chaque espace E_i est totalement discontinu alors $\varprojlim E_i$ est un espace totalement discontinu.*

Preuve: Notons que $\prod E_i$ est un espace topologique totalement discontinu. En effet, soit C une partie connexe de $\prod E_i$. Comme $\overline{\varphi_i}$ est continue, $\overline{\varphi_i}(C)$ est connexe dans E_i, donc est réduit à un point. Par suite, C est réduit à un point ce qui montre bien que $\prod E_i$ est totalement discontinu. Maintenant $\varprojlim E_i$ étant un sous-espace d'un espace totalement discontinu est lui-même totalement discontinu. Le cas le plus simple d'espace totalement discontinu est le cas d'un espace discret.

Proposition 46.— *Soit $(E_i, \varphi_{ji})_i$ un système projectif d'espaces topologiques tel que φ_{ji} soit continue pour tout $i \leq j$. Soit E un espace topologique et pour tout i, une application continue $\pi_i : E \to E_i$ tels que pour tout $i \leq j$, $\pi_i = \varphi_{ji} \circ \pi_j$. L'unique application $\theta : E \to \varprojlim E_i$ faisant commuter les diagrammes est continue.*

Preuve: La topologie de $\prod_i E_i$ est engendré par les ensembles $\overline{U} = \prod F_i$ avec F_i ouvert de E_i et $F_i = E_i$ pour presque tout $i \in I$. Ainsi, la topologie de $\varprojlim E_i$ est engendré par les ouverts $U = \overline{U} \cap \varprojlim E_i$ avec $\overline{U}$ Comme précédemment. Soient $i_1, \cdots, i_n$ les indices tels que $F_{i_j} \neq E_{i_j}$. On a alors $\overline{U} = \overline{\varphi_{i_1}}^{-1}(F_{i_1}) \cap \cdots \cap \overline{\varphi_{i_n}}^{-1}(F_{i_n})$. Donc

$$U = \overline{\varphi_{i_1}}^{-1}(F_{i_1}) \cap \cdots \cap \overline{\varphi_{i_n}}^{-1}(F_{i_n}) \cap S = \varphi_{i_1}^{-1}(F_{i_1}) \cap \cdots \cap \varphi_{i_n}^{-1}(F_{i_n})$$

On a alors

$$\begin{aligned} \theta^{-1}(U) &= \theta^{-1}(\varphi_{i_1}^{-1}(F_{i_1}) \cap \cdots \cap \varphi_{i_n}^{-1}(F_{i_n})) \\ &= \theta^{-1}(\varphi_{i_1}^{-1}(F_{i_1})) \cap \cdots \cap \theta^{-1}(\varphi_{i_n}^{-1}(F_{i_n})) \\ &= (\varphi_{i_1} \circ \theta)^{-1}(F_{i_1}) \cap \cdots \cap (\varphi_{i_n} \circ \theta)^{-1}(F_{i_n}) \\ &= \pi_{i_1}^{-1}(F_{i_1}) \cap \cdots \cap \pi_{i_n}^{-1}(F_{i_n}) \end{aligned}$$

donc $\theta^{-1}(U)$ est un ouvert de E et par suite θ est continue.

Corollaire 47.— *Soit E un espace topologique et pour tout i, une application continue $\pi_i : E \to E_i$ tels que pour tout $i \leq j$, $\pi_i = \varphi_{ji} \circ \pi_j$. Supposons que, pour tout espace topologique E' muni d'applications continues $\pi_i' : E' \to E_i$ tels que pour tout $i \leq j$, $\pi_i' = \varphi_{ji} \circ \pi_j'$, il existe une unique application continue $\theta : E' \to E$ tel que $\pi_i' = \pi \circ \theta$ pour tout i. Alors il existe un unique homéomorphisme de E sur $\varprojlim E_i$ faisant commuter les diagrammes.*

Preuve: Immédiat.

Si l'ensemble pré-ordonné d'indices $(I, \leq)$ est filtrant à droite, alors une base de la topologie de $\varprojlim E_i$ est donnée par la collection des ensembles $\pi_i^{-1}(V_i)$ avec $i \in I$ et V_i ouvert de E_i. En effet, les ouverts élémentaires de $\varprojlim E_i$ sont de la forme $U = \pi_{i_1}^{-1}(U_{i_1}) \cap \cdots \cap \pi_{i_n}^{-1}(U_{i_n})$. Comme I est filtrant à droite, prenons un indice i_0 tel que $i_k \leq i_0$ pour tout $k = 1, \cdots, n$ et posons

$$U_0 = \varphi_{i_0,i_1}^{-1}(U_{i_1}) \cap \cdots \cap \varphi_{i_0,i_n}^{-1}(U_{i_n})$$

U_0 est un ouvert de E_{i_0}, donc $V = \pi_{i_0}^{-1}(U_0)$ est un ouvert de $\varprojlim E_i$. Il est alors clair que $V \subset U$ et que si U est non vide, alors V l'est aussi. Le cas d'un ensemble d'indice filtrant à droite est particulièrement intéressant à cause de cela.

Soit $(I, \leq)$ un ensemble d'indices pré-ordonné filtrant à droite et $(E_i, \varphi_{ji})_{i\in I}$ un système projectif d'espaces topologiques séparés tels que φ_{ji} soit continue pour tout $i \leq j$. Soit A une partie de $\varprojlim E_i$. Pour tout $i \in I$, on note $A_i = \pi_i(A_i)$ (où $\pi : \varprojlim E_i \to E_i$ représente l'application canonique). Le système

$$(A_i, \varphi_{ji}|_{A_j})_i$$

est visiblement un système projectif et l'on peut voir de manière naturelle $\varprojlim A_i$ comme un sous-espace topologique de $\varprojlim E_i$. On a alors

Proposition 48.— *Sous les hypothèses précédentes, on a*

$$A \subset \varprojlim A_i \subset \overline{A}$$

en conséquence de quoi si $A_i = E_i$ pour tout i, alors A est dense dans $\varprojlim E_i$.

Preuve : Soit $x = (x_i)_i \in A \subset \varprojlim E_i$. Comme pour tout $i \in I$ on a $x_i \in A_i$ et pour tout $i \leq j$ on a $\varphi_{ji}(x_j) = x_i$on en déduit bien que $x \in \varprojlim A_i \subset \prod_i A_i \subset \prod_i E_i$.
Soit maintenant $x = (x_i)_i \in \varprojlim A_i$ et U un voisinage de x dans $\varprojlim E_i$. En vertu de ce qui précède, il existe un indice i_0 et un ouvert U_{i_0} de E_{i_0} contenant x_{i_0} tel $V = \pi_{i_0}^{-1}(U_{i_0})$ soit un voisinage de x inclus dans U. Maintenant, par définition des ensembles A_i, il existe $y = (y_i)_i \in A$ tel que $y_{i_0} = x_{i_0}$ et comme $\pi_{i_0}(y) \in U_{i_0}$ on en déduit donc que $y \in V$ et ainsi $U \cap A \neq \emptyset$, c'est-à-dire que $\varprojlim A_i \subset \overline{A}$.

On remarque que cette proposition nous donne aussi un critère de fermeture pour une partie d'une limite projective.

2.3 Groupes profinis

2.3.1 Définition, propriétés topologiques

Définition 49.— *Un groupe G est dit profini s'il est la limite projective d'un système projectif de groupes finis et d'homomorphismes de groupes.*

Soit $G = \varprojlim G_i$ un groupe profini. Si l'on met sur G_i la topologie discrète, alors d'après ce qui précède G est un espace compact et totalement discontinu. En fait, pour cette topologie, G est un groupe topologique. En effet, soit $U = \pi_{i_1}^{-1}(A_{i_1}) \cap \cdots \cap \pi_{i_n}^{-1}(A_{i_n})$ un ouvert fondamental de $\varprojlim G_i$. Pour tout $j = 1, \cdots, n$, prenons un $x_{i_j} \in A_{i_j}$ et arbitrairement deux éléments $a_{i_j}, b_{i_j} \in A_i$ tels que $a_{i_j} b_{i_j}^{-1} = x_{i_j}$. Posons $V_1 = \pi_{i_1}^{-1}(\{a_{i_1}\}) \cap \cdots \cap \pi_{i_n}^{-1}(\{a_{i_n}\})$ et $V_2 = \pi_{i_1}^{-1}(\{b_{i_1}\}) \cap \cdots \cap \pi_{i_n}^{-1}(\{b_{i_n}\})$. Ce sont des ouverts et par suite, $V_1 \times V_2$ est un ouvert de $G \times G$. Il est clair que l'image de $V_1 \times V_2$ par l'application $(x, y) \in G \times G \mapsto xy^{-1}$ est incluse dans U. Ce qui prouve bien de G est un groupe topologique pour cette topologie.

Proposition 50.— *Soit G un groupe profini muni de sa structure induite de groupe topologique. L'ensemble des sous-groupes ouverts distingués de G constitue une base de filtre des voisinages de l'élément neutre.*

Preuve: On note $\pi_i : G \to G_i$ les applications coordonnées. Soit U un voisinage de 1 dans G. Il existe donc des indices $i_1, \cdots, i_n$ et des parties $A_{i_j} \subset G_{i_j}$ telle que $\pi_{i_1}^{-1}(A_{i_1}) \cap \cdots \cap \pi_{i_n}^{-1}(A_{i_n}) \subset U$. Comme U contient 1, on a $1 \in A_{i_j}$. Par suite, l'ensemble $V = \pi_{i_1}^{-1}(1) \cap \cdots \cap \pi_{i_n}^{-1}(1) \subset U$. L'ensemble V est alors un sous-groupe ouvert distingué.

Exemples: • Tout groupe fini est profini. Sa structure de groupe topologique induite est celle donnée par la topologie discrète.

• Le groupe $\mathbb{Z}_p$ est profini. En effet, c'est la limite projective du système projectif

$$(\mathbb{Z}/p^n\mathbb{Z}, \varphi_{mn})_n$$

où φ_{mn} est donnée pour $m \geq n$ par la surjection canonique

$$\varphi_{mn} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$

Sa structure de groupe topologique induite est celle donnée par la distance p-adique.

• Le groupe multiplicatif $\mathbb{Z}_p^*$ est profini. En effet, nous avons vu que $\mathbb{Z}_p^*$ est le sous-ensemble de $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ composé des $(x_n)_n$ tel que pour tout n, $x_n \in (\mathbb{Z}/p^n\mathbb{Z})^*$ et pour tout $m \geq n$, $\varphi_{mn}(x_m) = x_n$. On en déduit donc que $\mathbb{Z}_p^*$ est la limite projective du système $((\mathbb{Z}/p^n\mathbb{Z})^*, \widetilde{\varphi}_{mn})_n$ où $\widetilde{\varphi_{mn}}$ est la restriction pour $m \geq n$ de $\varphi_{mn} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ (qui, étant un homomorphisme d'anneau, assure bien que $\widetilde{\varphi_{mn}}$ est un homomorphisme de groupe).

• Le groupe $\mathbb{Z}$ n'est pas profini. En fait, on a plus généralement :

Proposition 51.— *Un groupe profini G est soit fini, soit non dénombrable.*

Preuve : On sait que $\{a\}$ est une partie fermée dans G pour tout $a \in G$. S'il existait un $a \in G$ tel que $\{a\}$ soit aussi une partie ouverte, alors ce serait le cas de tous les singletons. Ainsi, la topologie serait discrète, ce qui ne peut correspondre avec la compacité que si G est fini.

On vient donc de montrer que si G n'est pas fini alors chaque singleton $\{a\}$ est un fermé d'intérieur vide. Si G était dénombrable, alors G serait une réunion dénombrable de fermé d'intérieur vide. Mais comme G est compact, G est un espace de Baire et donc G est d'intérieur vide, ce qui est bien évidement absurde.

• Le groupe $\mathbb{R}$ n'est pas profini. En fait, on a plus généralement :

Proposition 52.— *Un groupe divisible*[1] *ne peut être profini.*

Preuve : En effet, si G était un groupe profini divisible, il existerait une topologie sur G qui en ferait un groupe topologique compact où les sous-groupes distingués ouverts formeraient un système fondamental de voisinages de 0. Or dans un groupe compact un sous-groupe ouvert est d'indice fini et G ne possède pas de sous-groupe non triviaux d'indice fini car il est divisible : si H est un sous-groupe d'indice n de G, alors quelque soit $x \in G$, il existe $y \in \mathbb{R}$ tel que $x = n.y$ et donc $x = n.y \in H$ et, par suite, $H = G$.

Les isomorphismes de groupes profinis peuvent s'entendre de deux manières : soit d'une manière purement algébrique, en tant qu'isomorphisme de groupes abstraits, soit de manière topologique, en tant qu'isomorphisme de groupe topologique.

[1] Un groupe G est dit divisible si pour tout $x \in G$ et tout $n \in \mathbb{N}^*$, il existe $y \in G$ tel que $n.y = x$.

Généralement on utilise la terminologie d'isomorphisme de groupes profinis dans ce deuxièmes sens, mais on fera toutefois attention que pour parler de continuité, il faut bel et bien fixer la topologie sur le groupe. Il se peut en effet qu'un groupe abstrait G soit isomorphe (algébriquement) à deux limites projectives de groupes finis distinctes et que chacun d'elle confère à G une topologie différente. Si l'on donne effectivement des groupes profinis comme limites projectives de groupes finis (i.e. si les systèmes porjectifs associés sont fixés) on a alors un critère suffisant simple d'isomorphisme :

Proposition 53.— *Soit I un ensemble d'indice et $(G_i, \varphi_{ji})_i$ et $(G_i^{'}, \varphi_{ji}^{'})_i$ deux systèmes projectifs de groupes finis. On suppose que pour tout couple $i \in I$ il existe un isomorphisme de groupe $\psi_i : G_i \to G_i^{'}$ tel que, pour tout $i \leq j$, le diagramme suivant :*

$$\begin{array}{ccc} G_j & \xrightarrow{\psi_j} & G_j' \\ \downarrow{\scriptstyle \varphi_{ji}} & & \downarrow{\scriptstyle \varphi'_{ji}} \\ G_i & \xrightarrow{\psi_i} & G_i' \end{array}$$

soit commutatif. Les groupes profinis $G = \varprojlim G_i$ et $G^{'} = \varprojlim G_i^{'}$ sont isomorphes en tant que groupes topologiques.

Preuve : En vertu des propositions ???, il existe des uniques morphismes continus $\theta : G \longrightarrow G^{'}$ et $\theta^{'} : G^{'} \longrightarrow G$ faisant commuter les diagrammes. Par unicité, on déduit que $\theta^{'} \circ \theta$ est l'identité sur G et que $\theta \circ \theta^{'}$ est l'identité sur $G^{'}$. Les applications θ et $\theta^{'}$ sont donc des isomorphismes de groupes topologiques réciproques l'un de l'autre.

2.3.2 Caractérisation topologique

Lemme 54.— *Si E est un espace topologique compact et si A et B sont deux parties fermées de E telles que $A \cap B = \emptyset$ alors il existe deux ouverts U et V tels que $A \subset U$ et $B \subset V$ et tels que $U \cap V = \emptyset$. En conséquence de quoi, l'ensemble $\bigcap V$, où V parcourt les voisinage ouvert et fermé d'un point x, est connexe.*

Preuve: • Soit $x \in A$. Pour tout $y \in B$, il existe deux ouverts disjoints U_y et V_y tels que $x \in U_x$ et $y \in V_y$. Comme E est la réunion des ouverts $E - B$ et V_y, on en déduit par compacité, qu'il existe $y_1, \cdots, y_n \in B$ tels que

$$E = (E - B) \cup V_{y_1} \cup \cdots \cup V_{y_n}$$

Posons :

$$U^x = \bigcap_{i=1}^{n} U_{y_i} \text{ et } V^x = \bigcup_{i=1}^{n} V_{y_i}$$

on a alors $U^x \cap V^x = \emptyset$, $x \in U^x$, $B \subset V^x$. Faisons varier x dans A. Comme E est la réunion de $E - A$ et des U^x, il existe $x_1, \cdots, x_m$ tels que

$$E = (E - A) \cup V^{x_1} \cup \cdots \cup V^{x_m}$$

Posons :

$$U = \bigcup_{i=1}^{m} U^{x_i} \text{ et } V = \bigcap_{i=1}^{n} V^{x_i}$$

on a alors $U \cap V = \emptyset$ et $A \subset U$ et $B \subset V$.

• Soit $(C_i)_i$ la famille des parties de E ouvertes et fermées contenant x et $A = \bigcap_i C_i$. Supposons que $A = C \cup D$ avec C et D ouverts de A et $C \cap D = \emptyset$. Comme A est fermé dans E, C et D sont fermés dans E. en appliquant le résultat établit précédemment, on prend deux ouverts U et V de E tels que $U \cap V = \emptyset$ et $C \subset U$ et $D \subset V$. Posons $B = E - (U \cup V)$, qui est fermé. L'intersection de la famille $B \cup (C_i)_i$ est vide et comme E est compact, il existe des indices $i_1, \cdots, i_n$ tels que $B \cap C_{i_1} \cap \cdots \cap C_{i_n} = \emptyset$. Ainsi l'ensemble $I = C_{i_1} \cap \cdots \cap C_{i_n}$ est inclus dans $U \cup V$, donc I est la réunion disjointe des ensembles $I \cap U$ et $I \cap V$. Chacun de ces ensembles est ouverts et fermé dans I, mais comme I est lui-même ouvert et fermé dans E, on en déduit que $I \cap U$ et $I \cap V$ sont ouverts et fermés dans E. Ainsi, si $x \in I \cap U$, alors $A \subset I \cap U$ et donc $D \subset A \cap V \subset U \cap V = \emptyset$. De même, si $x \in I \cap V$, alors $A \subset I \cap V$ et donc $C \subset U \cap A \subset U \cap V = \emptyset$. La partie A est bien connexe.

Corollaire *Si E est un espace topologique compact et totalement discontinu, alors tout ouvert de E est réunion d'une famille de parties à la fois ouvertes et fermés.*

Preuve: Soit U un ouvert de E et $x \in U$. Soit $y \in E - \{x\}$, il existe un voisinage ouvert et fermé de x, F_y tel que $y \notin F_y$, car l'intersection de tous ces voisinages vaut x d'après le lemme précédent. Maintenant, E est la réunion des ouverts $U_y = E - F_y$ et de U. Comme E est compact, on en déduit qu'il existe une famille finie $\{y_1, \cdots, y_n\}$ telle que

$$E = U \cup U_{y_1} \cup \cdots \cup U_{y_n}$$

Donc l'ensemble $F^x = F_{y_1} \cap \cdots \cap F_{y_n}$ est inclus dans U. F^x est ouvert et fermé et contient x et par suite, U est bien la réunion des F^x.

Lemme 55.— *Si G est un groupe topologique compact et si X est une partie de G contenant e à la fois ouverte et fermée, alors X contient un sous-groupe ouvert distingué.*

Preuve: Soit $x \in X$. L'ensemble $W_x = Xx^{-1}$ est un voisinage ouvert de e. Comme la multiplication dans G est continue, il existe deux ouverts L_x et R_x contenant e tels que $L_x R_x \subset W_x$, en prenant $S_x = L_x \cap R_x$, on obtient un voisinage ouvert de e tel que $S_x.S_x \subset W_x$. L'ensemble X étant fermé dans G est compact et les ensemble $X \cap S_x x$ constituent un recouvrement d'ouverts de X. Il existe donc une famille finie $\{x_1, \cdots, x_n\}$ telle que :

$$X \subset S_{x_1} x_1 \cup \cdots \cup S_{x_n} x_n$$

L'ensemble $\bigcap_{i=1}^{n} S_{x_i}$ est un voisinage ouvert de e. On a alors:

$$SX \subset \bigcup_{i=1}^{n} SS_{x_i} x_i \subset \bigcup_{i=1}^{n} W_{x_i} x_i \subset X$$

et par suite $S \subset X$ puisque e appartient à X.

Soit $T = S \cap S^{-1}$. L'ensemble T est ouvert et contient e. Soit H le sous-groupe de G engendré par T. On a $H = \bigcup_n T^n$ et comme T^n est ouvert, H est un sous-groupe ouvert de G. Comme $SX \subset X$ et que $T \subset S$, par récurrence immédiate,

on a $T^n \subset X$ et par suite $H \subset G$. D'après la partie précédente, H contient un sous-groupe ouvert distingué.

Proposition 56.— *Soit G un groupe topologique compact et totalement discontinu. Tout partie ouverte U est une réunion de classes de sous-groupes ouverts distingués de G.*

Preuve: Soit $x \in U$, l'ensemble Ux^{-1} est alors un ouvert voisinant e. D'après ce qui précéde, Ux^{-1} est la réunion de parties ouvertes et fermées. L'une d'entre elles contient e, donc d'après le lemme précédent contient un sous-groupe ouvert distingué K_x et $K_x x \subset U$ et par suite $U = \bigcup_x K_x x$.

Corollaire 57.— *Soit G un groupe topologique compact et totalement discontinu et X une partie de G. On a*

$$\overline{X} = \bigcap \{NX/\ N \text{ sous-groupe ouvert distingué de } G\}$$

Preuve: Si N est un sous-groupe ouvert distingué, alors NX représente une réunion de classe de N. Ces dernière étant en nombre fini puisque G est compact, NX est donc une réunion finie d'ensemble fermé et donc est fermé. Ainsi $\bigcap NX$ est fermé et donc

$$\overline{X} \subset \bigcap \{NX/\ N \text{ sous-groupe ouvert distingué de } G\}$$

Soit maintenant $y \notin \overline{X}$, alors y a un voisinage ouvert U disjoint de X et donc il existe un sous-groupe ouvert distingué N tel que $Ny \subset U$. Donc $Ny \cap X = \emptyset$ et par suite $y \notin NX$, donc

$$y \notin \bigcap \{NX/\ N \text{ sous-groupe ouvert distingué de } G\}$$

Corollaire 58.— *Soit G un groupe profini et H un sous-groupe de G. On a*

$$\overline{H} = \bigcap \{U/\ H \subset U \text{ sous-groupe ouvert distingué de } G\}$$

Preuve: On sait que

$$\overline{H} = \bigcap \{UH/\ U \text{ sous-groupe ouvert distingué de } G\}$$

Si $H \subset U$, alors $UH = U$. Maintenant si U est quelconque, l'ensemble $V = UH$ est ouvert puisque U l'est et $H \subset V$. Soit $x = uh$ et $y = u^{'}h^{'}$ dans V. Comme U est distingué dans G, il existe $u^{''} \in U$ tel que $hu^{'} = u^{''}h$ et par suite

$$xy = uhu^{'}h^{'} = uu^{''}hh^{'} \in V$$

On vérifie de même que $x^{-1} \in V$ et par suite, V est un sous-groupe.

Proposition 59.— *Soit G un groupe topologique compact et $\mathcal{E}$ une famille de sous-groupes ouverts distingués de G. Si $\mathcal{E}$ est une base de filtre et si $\bigcap_{N_i \in \mathcal{E}} N_i = \{e\}$ alors G est profini et*

$$G \simeq \varprojlim G/N_i$$

Preuve: Soit $N_i \in \mathcal{E}$. La surjection canonique $\pi_i : G \to G/N$ est un morphisme continue. Les applications π_i font commuter les diagrammes, donc il existe un morphisme continu θ de G dans $\varprojlim G/N_i$.

Soit $x \in Ker(\theta)$. On a $\pi_i(x) = e$ pour tout N, donc $x \in \bigcap_{N_i \in \mathcal{E}} N_i$, donc $x = e$ et θ est injective.

Soit $y = (y_i)_i \in \varprojlim G/N_i$. Soit $i_1, \cdots, i_n$ une famille finie d'indices. Les ensembles $y_{i_k} N_k$ sont fermés et $\bigcap_{i=1}^n y_{i_k} N_k \neq \emptyset$. En effet, la famille $\mathcal{E}$ étant une base de filtre, il existe un indice j_0 tel que $N_{j_0} \subset \bigcap_{i=1}^n N_k$. On a donc $\varphi_{j_0 i_k}(y_{j_0}) = y_{i_k}$ c'est à dire que si $\bar{y_{j_0}}$ désigne un représentant de y_{j_0}, alors $\bar{y_{j_0}} \in y_{i_k} N_{i_k}$ pour tout k. Comme G est compact, on en déduit que $\bigcap_i y_{i_k} N_k \neq \emptyset$. Si $x \in \bigcap_i y_{i_k} N_k$, alors $\theta(x) = y$ et par suite θ est surjective.

θ est un isomorphisme continu. Comme G est compact et $\varprojlim G/N_i$ séparé, θ est donc un homéomorphisme.

Théorème 60.— *Soit G un groupe topologique. Les propositions suivantes sont équivalentes :*

i) G est profini,

ii) G est isomorphe en tant que groupe topologique à un sous-groupe fermé d'un produit cartésien de groupes finis,

iii) G est compact et totalement discontinu,

iv) G est compact et $\bigcap N = \{e\}$ où N parcourt l'ensemble des sous-groupes ouverts distingués de G,

iv$'$) G est compact et $\bigcap N = \{e\}$ où N parcourt l'ensemble des sous-groupes ouverts de G.

Preuve: *i)* $\Rightarrow$ *ii)* Evident.

ii) $\Rightarrow$ *iii)* Immédiat.

iii) $\Rightarrow$ *iv)* On prend le corollaire établi précédemment avec $X = \{e\}$ qui est fermé puisque G est séparé.

iv) $\Rightarrow$ *i)* C'est la proposition précédente en remarquant que l'ensemble des sous-groupes ouverts distingués de G forme une base de filtre.

iv) $\Leftrightarrow$ *iv$'$)* Immédiat, compte-tenu du fait que tous sous-groupe ouvert dans un groupe topologique compact contient un sous-groupe ouvert distingué.

Corollaire 61.— • *Tout sous-groupe fermé d'un groupe profini est profini.*

• *Tout produit cartésien de groupes profinis est un groupe profini.*

• *Si $(G_i, \varphi_{ji})_i$ est un système projectif de groupes profinis et d'homomorphismes continus, alors $\varprojlim G_i$ est un groupe profini.*

Preuve: Exercice.

Remarque: Si G est profini, on vient de montrer que $G \simeq \varprojlim G/U$ où U parcourt l'ensemble des sous-groupes ouverts distingués de G. On remarque que le système projectif $(G/U, \varphi_{VU})$ est filtrant à droite et que les flèches φ_{VU} sont surjective.

Ainsi, lorsque l'on considère un groupe profini G, on peut supposer sans perte de généralité que $G = \varprojlim G_i$ avec (G_i, φ_{ji}) système projectif filtrant à droite et φ_{ji} surjective. Ceci est intéressant, en particulier, pour décrire plus siplement un système fondamentale de voisinage d'un point dans G.

Proposition 62.— *Si G est un groupe profini et H est un sous-groupe distingué fermé de G alors G/H est un groupe profini.*

Preuve : On sait que, puisque H est fermé, $H = \bigcap U$ où U parcourt les sous-groupes ouverts distingués de G contenant H. Pour un tel sous-groupe U, notons $U^{'} = \pi(U)$ où $\pi : G \to G/H$. Les $U^{'}$ forment alors une base de filtre de sous-groupes ouverts distingués de G/H et $\bigcap U^{'} = e$. Comme H est fermé, G/H est compact et donc $G/H \simeq \varprojlim (G/H)/U^{'}$. Comme les groupes $(G/H)/U^{'}$ et G/U sont isomorphes et que le système projectif $(G/H)/U^{'}$ est compatible avec celui des G/U, on a plus précisément :

$$G/H = \varprojlim G/U$$

2.3.3 Le groupe $\mathbb{Z}_p^*$.

Rappelons que la construction de $\mathbb{Z}_p$ fait de cet objet un anneau topologique. Posons $U = \mathbb{Z}_p^*$. Si l'on regarde U comme sous-ensemble de $\mathbb{Z}_p$, alors la topologie induite par $\mathbb{Z}_p$ sur U est présisément celle de groupe profini.

Pour $n \in \mathbb{N}^*$, si l'on note $U_n = Ker(\epsilon_n)$ où ϵ_n est l'application (surjective) naturelle de U vers $(\mathbb{Z}/p^n\mathbb{Z})^*$, on a précisément $U_n = 1 + p^n\mathbb{Z}_p$. Les U_n sont des sous-groupes ouverts (et distingués) d'intersection réduite à 1, on en déduit donc que :

$$U = \varprojlim U/U_n$$

Pour $n \geq 1$, l'application de U_n dans $\mathbb{Z}/p\mathbb{Z}$

$$(1 + p^n x) \longmapsto x \ mod(p)$$

est un homomorphisme surjectif de noyau U_{n+1}, on a donc l'isomorphisme

$$U_n/U_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$$

(Il est a noté que de même $U/U_1 \simeq \mathbb{Z}/p\mathbb{Z}$.) On en déduit, par récurrence immédiate, que U_1/U_n est d'ordre p^{n-1}.

Comme U_1 est fermé dans U, on a aussi

$$U_1 = \varprojlim U_1/U_n$$

(même preuve que pour U).

Proposition 63.— *Le groupe U est topologiquement isomorphe au produit cartésien $V \times U_1$ où*

$$V = \{x \in U/ \ x^{p-1} = 1\}$$

est le seul sous-groupe de U isomorphe à $\mathbb{F}_p^*$.

Preuve : Commencons par montrer qu'il n'y a qu'au plus un sous-groupe de U isomorphe à $\mathbb{F}_p^*$. Si V existe, alors pour tout $x \in V$, $x^{p-1} = 1$. Donc tout élément

de V est racine dans $\mathbb{Z}_p$ du polynôme $P(X) = X^{p-1} - 1$, or $\mathbb{Z}_p$ étant un anneau intègre et commutatif, P possède au plus $p-1$ éléments, ce qui prouve l'unicité.

Rappelons maintenant ce lemme de théorie des groupes : si

$$0 \to A \to E \to B \to 0$$

est une suite exacte de groupes commutatifs finis et que $a = ord(A)$ et $b = ord(B)$ sont premier entres eux, alors $E = A \oplus B^{'}$ où $B^{'} = \{x \in E/\ bx = 0\}$ est le seul sous-groupe de E isomorphe à B (Exercice).

Si l'on applique ce lemme à la suite :

$$1 \to U_1/U_n \to U/U_n \to \mathbb{F}_p^* \to 1$$

on a donc un isomorphisme naturel

$$\sigma_n : U/U_n \to \mathbb{F}_p^* \times U_1/U_n$$

Si maintenant, on note $\pi_n : U/U_{n+1} \to U/U_n$ et $\omega_n : U_1/U_{n+1} \to U_1/U_n$ les projections canonique, on voit facilement que le diagramme

$$\begin{array}{ccc} U/U_{n+1} & \xrightarrow{\sigma_{n+1}} & \mathbb{F}_p^* \times U_1/U_{n+1} \\ \downarrow{\scriptstyle \pi_n} & & \downarrow{\scriptstyle Id\times\omega_n} \\ U/U_n & \xrightarrow{\sigma_n} & \mathbb{F}_p^* \times U_1/U_n \end{array}$$

est commutatif. On en déduit les ismorphismes de groupes topologiques

$$U \simeq \varprojlim U/U_n \simeq \varprojlim \mathbb{F}_p^* \times U_1/U_n \simeq \mathbb{F}_p^* \times \varprojlim U_1/U_n \simeq \mathbb{F}_p^* \times U_1$$

Proposition 64.— *Si $p \neq 2$, $U_1 \simeq \mathbb{Z}_p$ et si $p = 2$, $U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2$ et $U_2 \simeq Z_2$.*

Preuve : Si $p \neq 2$, prenons $\alpha = 1 + p$. Alors $\alpha \in U_1 - U_2$. On a

$$\begin{aligned} \alpha^p &= \sum_{k=0}^{p} C_p^k p^k \\ &= 1 + p^2 + p^3 \left(\textstyle\sum_{k=2}^{p} \frac{C_p^k}{p} p^{k-2} \right) \end{aligned}$$

donc $\alpha^p \in U_2 - U_3$. Par récurrence, on montre que $\alpha^{p^n} \in U_{n+1} - U_{n+2}$. Si l'on note α_n l'image de α dans U_1/U_n, alors, d'après ce qui précède, $(\alpha_n)^{p^{n-2}} \neq 1$ et $(\alpha_n)^{p^{n-1}} = 1$. Ce qui justifie que U_1/U_n est cyclique (d'ordre p^{n-1}). Considérons l'isomorphisme

$$\theta_n : \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n$$

qui à z associe $(\alpha_n)^z$. Le diagramme suivant

$$\begin{array}{ccc} Z/p^n\mathbb{Z} & \xrightarrow{\theta_{n+1}} & U_1/U_{n+1} \\ \downarrow & & \downarrow \\ Z/p^{n-1}\mathbb{Z} & \xrightarrow{\theta_n} & U_1/U_n \end{array}$$

est alors commutatif. On en déduit donc les isomorphismes de groupes topologiques :

$$U_1 \simeq \varprojlim U_1/U_n \simeq \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \simeq \mathbb{Z}_p$$

Le cas $p = 2$ est laissé en exercice.

2.3.4 Le groupe $\widehat{\mathbb{Z}}$

Considérons le groupe $\widehat{\mathbb{Z}}$, complétion profinie de $\mathbb{Z}$. C'est donc la limite projective du système $(\mathbb{Z}/n\mathbb{Z}, \varphi_{mn})_n$ où φ_{mn} désigne (pour n divise m) la surjection canonique de $\mathbb{Z}/m\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

Proposition 65.— *Il existe un isomorphisme de groupes topologiques entre* $\widehat{\mathbb{Z}}$ *et* $\prod_p \mathbb{Z}_p$.

Preuve: Soit $n \in \mathbb{N}$ et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. On a alors un isomorphisme

$$f_n : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

qui à $x \in \mathbb{Z}/n\mathbb{Z}$ associe

$$f_n(x) = \left(\varphi_{np_1^{\alpha_1}}(x), \cdots, \varphi_{np_k^{\alpha_k}}(x)\right)$$

Pour $y \in \prod_p \mathbb{Z}_p$, posons

$$\pi_n(y) = f_n^{-1}(u_1(y), \cdots, u_k(y))$$

où $u_i : \mathbb{Z}_{p_i} \to \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ est l'application canonique. On vérifie alors (exercice) que pour tout n divise m, on a $\pi_n = \varphi_{mn} \circ \pi_m$ et que les applications π_n sont continues.

Considérons maintenant un groupe topologique G muni d'homomorphismes continues $\omega_n : G \to \mathbb{Z}/n\mathbb{Z}$ tels que $\omega_n = \varphi_{mn} \circ \omega_m$ pour tout n divisant m. Définissons l'application $\theta : G \to \prod_p \mathbb{Z}_p$ par:

$$\theta(x) = (x_2, x_3, x_5, \cdots) \in \prod_p \mathbb{Z}_p$$

avec

$$x_p = (\omega_p(x), \omega_{p^2}(x), \cdots) \in \mathbb{Z}_p$$

On a bien $\omega_n = \pi_n \circ \theta$ pour tout n (et θ est la seule application à vérifier cette propriété). L'application θ est visiblement un homomorphisme de groupe.

Les ouverts élémentaires de $\prod_p \mathbb{Z}_p$ sont les ensembles de la forme

$$U = U_2 \times U_3 \times U_5 \times U_{p_0} \times \prod_{p > p_0} \mathbb{Z}_p$$

où U_p est un ouvert élémentaire de $\mathbb{Z}_p$, c'est-à-dire un ensemble de la forme

$$u_{p_{n_p}}^{-1}(A_{p_{n_p}})$$

pour un certain entier n_p et $A_{p_{n_p}}$ une partie quelconque de $\mathbb{Z}/p^{n_p}\mathbb{Z}$. On a donc:

$$U = \pi_n^{-1}(A) \text{ avec } A = f_n^{-1}(U_2 \times \cdots \times U_{p_0}) \subset \mathbb{Z}/n\mathbb{Z}$$

On a donc $\theta^{-1}(U) = \omega_n^{-1}(A)$ qui est ouvert car ω_n est continue et A est ouvert dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi θ est continue et par suite $\prod_p \mathbb{Z}_p$ est bien isomorphe en tant que groupe topologique à $\widehat{\mathbb{Z}}$.

Chapitre 3

Théorie de Sylow et groupes pronilpotents

3.1 Théorie de Sylow

3.1.1 Nombres surnaturels

On considère l'ensemble $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$ ordonné par l'extension de l'ordre sur $\mathbb{N}$ défini par $n < +\infty$ pour tout $n \in \mathbb{N}$. Dans $\overline{\mathbb{N}}$ la notion de somme infinie a un sens.

Définition 66.— *On appelle nombre surnaturel (ou nombre de Steiniz) toute suite $s \in \overline{\mathbb{N}}^{\mathcal{P}}$. Si s désigne un nombre surnaturel, on notera plus volontier s sous la forme du produit formel $\prod_p p^{s(p)}$.*

Sur l'ensemble des nombres surnaturels, on définit une arithmétique. Pour une famille $(s_i)_i$ ($s_i = \prod_p p^{s_i(p)}$) de nombres surnaturels, on pose:

$$\prod_i s_i = \prod_p p^{s(p)} \text{ avec } s(p) = \sum_i s_i(p)$$

$$p.p.c.m.(s_i)_i = \prod_p p^s(p) \text{ avec } s(p) = sup(s_i(p))$$

$$p.g.c.d.(s_i)_i = \prod_p p^s(p) \text{ avec } s(p) = inf(s_i(p))$$

On peut donc parler de divisibilité dans l'ensemble des nombres surnaturels. Il est clair que $\mathbb{N}^*$ (muni de sa structure multiplicative) s'identifie au sous-ensemble de l'ensemble des nombres surnaturels constitué des éléments $\prod_p p^{s(p)}$ où $s(p) \in \mathbb{N}$ et $s(p) = 0$ pour presque tous p.

On remarque aussi que la relation "divise" est une relation d'ordre sur l'ensemble des nombres surnaturels et qu'en particulier si a et b sont deux nombres surnaturels tels que $a|b$ et $b|a$ alors $a = b$.

Lemme 67.— *Si $(a_i)_i$ et $(b_j)_j$ sont deux familles de nombres surnaturels alors*

$$p.p.c.m.(a_i b_j)_{i,j} = p.p.c.m.(a_i)_i . p.p.c.m.(b_j)_j$$

Preuve: Exercice.

3.1.2 Indices et théorème de Lagrange

Définition 68.—
Soit G un groupe profini et H un sous-groupe fermé de G. On appelle indice de H dans G le nombre surnaturel, noté $[G : H]$, égal à $p.p.c.m.(a_i)_i$ où $a_i = [G : H_i]$ où $(H_i)_i$ désigne l'ensemble des sous-groupes ouverts de G contenant H.

L'ordre de G est par définition le nombre surnaturel $|G| = [G : 1]$, de même l'ordre d'un élément $x \in G$ est par définition $|x| = |\overline{< x >}|$.

Lemme 69.— *Si H est un sous-groupe fermé de G alors*

$$[G : H] = p.p.c.m.([G : NH]/\ N \text{ ouvert distingué de } G)$$

Preuve: Notons $r = p.p.c.m.([G : NH]/\ N$ ouvert distingué de $G)$. Il est clair que r divise $[G : H]$. Soit maintenant U un sous-groupe ouvert de G contenant H, il existe un sous-groupe ouvert distingué $N \subset U$. Le théorème de Lagrange affirme alors que $[G : U]$ divise $[G : NH]$ et par suite, $[G : H]$ divise r.

Proposition 70.— *Un groupe profini est un pro-p-groupe si et seulement si son ordre est p^n avec $n \in \overline{N}$.*

Preuve: Soit G un pro-p-groupe. On écrit $G = \varprojlim G_i$ ou G_i est un p-groupe et on considère $G^i = Ker(G \to G_i)$. G^i est un sous-groupe ouvert de G d'indice une puissance de p. Par ailleurs, $\bigcap G^i = \{1\}$ donc $|G| = p.p.c.m([G : G^i]$ et donc est une puissance de p.

Réciproquement, si G est un groupe profini d'ordre $r = p^n$, alors tout sous-groupe ouvert U de G est d'indice p^m avec $m \leq n$, donc si U est distingué, G/U est un p-groupe. Comme $G = \varprojlim G/U$, on en déduit bien que G est un pro-p-groupe.

Théorème 71.— *Soit H et K deux sous-groupes fermés d'un groupe profini G tels que $K \subset H$. Alors*

$$[G : K] = [G : H].[H : K]$$

Preuve: Soit N un sous-groupe ouvert distingué de G (en particulier N est d'indice fini). On a alors:

$$[G : NK] = [G : NH].[NH : NK] = [G : NH].[H : (N \cap H)K]$$

et $N \cap H$ est un sous-groupe ouvert distingué de G. Ainsi, $[G : K]$ divise $[G : H].[H : K]$. Réciproquement, si N_1 est un sous-groupe ouvert distingué de G et N_2 un sous-groupe ouvert distingué de H alors N_2 est l'intersection avec H d'un ouvert de G et donc on peut trouver un sous-groupe M ouvert distingué de G tel que $M \cap H$ soit un sous-groupe de N_2. Soit $N = M \cap N_1$, alors N est un sous-groupe ouvert distingué de G et alors $[G : N_1H].[H : N_2K]$ divise $[G : NH].[H : (N \cap H)K]$ qui vaut $[G : NK]$. Ainsi $[G : H].[H : K]$ divise $[G : K]$.

Proposition 72.— *Soit $(H_i)_i$ une base de filtre de sous-groupes fermés d'un groupe profini G. Alors,*

$$[G : \bigcap_i H_i] = p.p.c.m([G : H_i])$$

Preuve: Le théorème précédent assure que $p.p.c.m([G : H_i])$ divise $[G : \bigcap_i H_i]$. Soit U un sous-groupe ouvert de G contenant $\bigcap_i H_i$. On a

$$\bigcap_i (H_i \cap (G - U)) = \emptyset$$

et comme les ensembles $H_i \cap (G - U)$ sont fermés et que G est compact, il existe des indices i_l avec $l = 1, \cdots, l_0$ tels que :

$$\bigcap_{l=1}^{l_0} (H_{i_l} \cap (G - U)) = \emptyset$$

Ainsi, $\bigcap_{l=1}^{l_0} H_{i_l} \subset U$ et comme il existe k tel que $H_k \subset \bigcap_{l=1}^{l_0} H_{i_l}$ on a donc $H_k \subset U$ et donc $[G : U]$ divise $[G : H_k]$. Donc $[G : \bigcap_i H_i]$ divise $p.p.c.m([G : H_i])$.

Exercice. Soit G un groupe profini et $x \in G$ d'ordre $\prod_p p^{s(p)}$. Montrer que

$$\overline{< x >} = \prod_{p,\ s(p)=+\infty} \mathbb{Z}_p \times \prod_{p,\ s(p)<+\infty} \mathbb{Z}/p^{s(p)}\mathbb{Z}$$

3.1.3 Sous-groupes de Sylow

Définition 73.— *Soit G un groupe profini et p un nombre premier. On appelle p-sous-groupe de Sylow de G tout sous-groupe fermé H tel que $|H| = p^n$ et $[G : H]$ n'est pas divisible par p.*

Proposition 74.— *Les p-sous-groupes de Sylow d'un groupe profini G sont exactement les pro-p-sous-groupes maximaux de G.*

Preuve: Exercice.

Théorème 75.— *Soient G un groupe profini et p un nombre premier. Alors*

a) Le groupe G a des p-sous-groupes de Sylow.

b) Si P est un p-sous-groupe de Sylow de G et que T est un pro-p-sous-groupe de G, alors il existe $g \in G$ tel que $g^{-1}Tg \subset P$.

c) Tout pro-p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.

d) Si P_1 et P_2 sont des p-sous-groupes de Sylow de G alors il existe $g \in G$ tel que $g^{-1}P_1g = P_2$.

Preuve: a) Soit I l'ensemble des sous-groupes fermés de G d'indice premier à p. L'ensemble I est non vide puisque $G \in I$. Il est ordonné par l'inclusion. En appliquant le lemme de Zorn, il existe un élément minimal $P \in I$. On a $[G : P]$ premier à p. Si P n'est pas un pro-p-groupe, il existe un sous-groupe ouvert distingué M de P tel que P/M ne soit pas un p-groupe. Par le théorie de Sylow finie, il existe un p-Sylow $Q/M \subset P/M$ strict. L'ensemble Q est alors la réunion d'un nombre fini de classes de M qui est ouvert dans P et fermé dans P et G. Par ailleurs, on a $[G : Q] = [G : P].[P : Q]$ et donc $[G : Q]$ est premier à p, ce qui contredit la minimalité de P.

b) Soit N un sous-groupe ouvert distingué de G alors $N \cap P$ est un sous-groupe ouvert distingué de P et $NP/N \simeq P/(N \cap P)$, donc NP/N est un p-groupe. De plus, $[G : NP]$ divise $[G : P]$, donc NP/N est un p-sous-groupe de Sylow de G/N.

De manière similaire, NT/N est un p-sous-groupe de G/N. Par application de la caratérisation de la nilpotence pour les groupes finis, on sait que l'ensemble

$$R(N) = \{g/\ g^{-1}(NT)g \subset NP\}$$

est non vide et, étant une réunion de classe de N, est aussi fermé. Par ailleurs, si M et N sont deux sous-groupes ouverts distingués de G avec $M \subset N$, alors $R(M) \subset R(N)$ et donc si l'on prend $N_1, \cdots, N_n$ des sous-groupes ouverts distingués de G alors

$$\emptyset \neq R(N_1 \cap \cdots \cap N_n) \subset R(N_1) \cap \cdots \cap R(N_n)$$

donc les intersections finies de $R(N)$ ne sont pas vide, et par compacité, on en déduit qu'il existe $g \in \bigcap R(N)$. Pour tout N, on a $g^{-1}Tg \subset NP$ et donc

$$g^{-1}Tg \subset \bigcap_N NP = P$$

c) et d). Il est clair que le conjugué d'un p-sous-groupe de Sylow est un p-sous-groupe de Sylow. Ces deux assertions découlent alors immédiatement de a) et b).

On rappelle que le normalisateur $N_G(H)$ d'un sous-groupe H d'un groupe G est le sous-groupe

$$N_G(H) = \left\{g \in G/\ g^{-1}Hg = H\right\}$$

On remarque que si G est profini et H est fermé alors $N_G(H)$ est fermé. En effet, si $h \in H$, on définit $\varphi_h : G \to G$ par

$$\varphi_h(g) = g^{-1}hg$$

pour tout $g \in G$. L'application φ_h est un morphisme continu pour tout $h \in H$ et comme H est fermé, $Ker(\varphi_h)$ est fermé dans G. Maintenant,

$$N_G(H) = \bigcap_{h \in H} Ker(\varphi_h)$$

donc $N_G(H)$ est fermé.

Proposition 76.— *Soit G un groupe profini, K un sous-groupe distingué fermé de G et P un p-sous-groupe de Sylow de G.*

a) $K \cap P$ est un p-sous-groupe de Sylow de K.

b) KP/K est un p-sous-groupe de Sylow de G/K.

c) $G = N_G(Q)K$ pour tout p-sous-groupe de Sylow Q de K.

d) $H = N_G(H)$ lorsque H est un sous-groupe fermé qui contient $N_G(Q)$ pour un certain p-sous-groupe de Sylow Q de K.

Preuve: a) $K \cap P$ est un pro-p-sous-groupe de K. Il existe donc un p-sous-groupe de Sylow Q de K tel que $K \cap P \subset Q$. Maintenant, Q est un pro-p-sous-groupe de G, donc il existe $g \in G$ tel que $g^{-1}Qg \subset P$. De là,

$$Q \subset K \cap (gPg^{-1}) = g(K \cap P)g^{-1}$$

qui est un pro-p-sous-groupe de K. Il s'ensuit que $Q = g(K \cap P)g^{-1}$ et que $K \cap P = g^{-1}(K \cap P)g$ est un p-sous-groupe de Sylow de K.

b) Comme KP/K est isomorphe en tant que groupe topologique à $P/(K \cap P)$, on en déduit que c'est un pro-p-sous-groupe de G/K. Maintenant comme $[G : KP]$

divise $[G : P]$ qui est premier à p par hypothèse, on en déduit bien que $[(G/K) : (KP/K)] = [G : KP]$ est premier à p, et que donc KP/K est un p-sous-groupe de Sylow de G/K.

c) Soit $g \in G$, alors $g^{-1}Qg$ est un p-sous-groupe de Sylow de K et donc qu'il existe $k \in K$ tel que

$$k^{-1}(g^{-1}Qg)k = Q$$

Ainsi, $x = gk \in N_G(Q)$ et $g = xk^{-1} \in N_G(Q)K$.

d) Soit $u \in N_G(H)$. Comme Q est un p-sous-groupe de Sylow de $K \cap H$, $u^{-1}Qu$ est un p-sous-groupe de Sylow de $u^{-1}(K \cap H)u = K \cap H$. Ainsi, il existe $h \in K \cap H$ tel que

$$h^{-1}(u^{-1}Qu)h = Q$$

et donc $uh \in N_G(Q) \subset H$ et par suite $u \in H$.

3.2 Groupes pronilpotents

3.2.1 Pronilpotence

On rappelle que si G désigne un groupe et que $x, y \in G$, on appelle commutateur de x et de y l'élément $[x, y] = xyx^{-1}y^{-1}$. Si A et B sont deux sous-groupes de G, on note $[A, B]$ le sous-groupe de G engendré par les commutateurs $[a, b]$ avec $a \in A$ et $b \in B$. On rappelle que la suite centrale descendante d'un groupe G est la suite de sous-groupes $(C^n(G))_n$ définie par:

$$C^1(G) = G,\ C^{n+1}(G) = [G, C^n(G)]$$

Un groupe G est alors dit *nilpotent* s'il existe un entier n tel que $C^{n+1}(G) = e$. On a alors la caractérisation des groupes nilpotents finis suivante :

Théorème 77.— *Soit G un groupe fini. Les propositions suivantes sont équivalentes :*

i) G est nilpotent,

ii) tout sous-groupe de Sylow de G est distingué,

iii) G est isomorphe au produit direct de ses sous-groupes de Sylow,

iv) $N_G(U) \neq U$ pour tout sous-groupe propre de G.

On va maintenant s'intéresser au cas des groupes pronilpotents (qui sont, par définition, les limites projectives de groupes nilpotents.)

Lemme 78.— *Soit $(H_i)_i$ une famille de sous-groupes fermés d'un groupe profini G telle que $G = \overline{< \bigcup_i H_i >}$. Pour tout i, on note*

$$K_i = \overline{< \bigcup_{j \neq i} H_j >}$$

Si $\bigcap_i K_i = 1$, alors G est isomorphe à $\prod_i H_i$.

Preuve: Pour tout i, K_i est distingué dans G. De plus $K_iH_i = G$ et $K_i \cap H_i = 1$ donc $G/K_i \simeq H_i$. Définissons $\varphi : G \to \prod_i H_i$ par $\varphi(g) = (gK_i)_i$. On a $Ker(\varphi) = \bigcap_i K_i = 1$, donc φ est injectif. Il est clair que φ est continu. Montrons que

$\varphi(G)$ est dense dans $\prod_i H_i$. Le sous-groupe $\varphi(H_j)$ eszt constitué des éléments $(x_i)_i \in \prod_i G/K_i$ tel que $x_i = 1$ pour $i = j$. Ainsi, $\varphi(G)$ contient le sous-groupe

$$D = \{(x_i)_i / \ x_i = 1 \text{ pour presque tout } i\}$$

Maintenant, une base de la topologie est donnée par les ensemble

$$U = \prod_{j \in J \ fini} U_j \times \prod_{i \notin J} G/K_i$$

où U_j est un ouvert de G/K_j. Il est clair que $D \cap U \neq \emptyset$. L'ensemble $\varphi(G)$ est donc dense dans $\prod_i H_i$ et par suite puisque φ est continu et que les groupes sont profinis, c'est un isomorphisme de groupes profinis.

Théorème 79.— *Soit G un groupe profini. Les propositions suivantes sont équivalentes :*

i) G est pronilpotent,

ii) tout p-sous-groupe de Sylow de G est distingué,

iii) G est isomorphe (en tant que groupe topologique) au produit direct de ses p-sous-groupes de Sylow,

iv) $N_G(U) \neq U$ pour tout sous-groupe ouvert propre de G.

Preuve: $i) \Rightarrow iv)$ Soit U un sous-groupe ouvert strict de G et N l'intersection de ses conjugués. On sait que N est un sous-groupe ouvert distingué de G et donc G/N est nilpotent (en effet G/N est le quotient d'un des groupes G_i où les G_i sont des groupes nilpotents finis tels que $G = \varprojlim G_i$). Si $N_G(U) = U$ alors $N_{G/N}(\pi(U)) = \pi(U)$ (avec $\pi : G \to G/N$) ce qui est contraire au résultat sur les groupes nilpotents finis.

$iv) \Rightarrow ii)$ Soit P un sous-groupe de Sylow de G et U un sous-groupe ouvert contenant $N_G(P)$. Par le d) de la prop???, on a $N_G(U) = U$ et donc, par hypothèse, $N_G(U) = U$. Comme $N_G(P)$ est fermé, il est l'intersection des U ouvert le contenant. Donc $N_G(P) = G$ et P est bien distingué.

$ii) \Rightarrow iii)$ Soit I l'ensemble des nombres premiers qui divise $|G|$ et $(P_i)_i$ l'ensemble des sous-groupes de Sylow de G. Pour tout $i \in I$, notons $K_i = \overline{\bigcup_{j \neq i} P_j}$. On remarque que $|K_i|$ est premier à i (exercice). Il s'ensuit que $K_i \cap P_i = 1$ et que $\bigcap_i K_i = 1$. Maintenant, on a bien $\overline{\bigcup_j P_j} = G$ puisque ce groupe est d'indice 1 dans G. On applique alors le lemme précédent pour conclure.

$iii) \Rightarrow i)$ Puisque les p-groupes finis sont nilpotents, les pro-p-groupes sont pronilpotents. Enfin, un produit cartésien de pronilpotents est aussi pronilpotent.

3.2.2 Sous-groupe de Frattini

Définition 80.— *Soit G un groupe profini. On appelle sous-groupe de Frattini de G, le sous-groupe $\Phi(G) = \bigcap U$ où U parcourt l'ensemble des sous-groupes ouverts maximaux.*

$\Phi(G)$ est donc un sous-groupe fermé distingué.

Proposition 81.— *Soit G un groupe profini, H et K deux sous-groupes fermés de G. On a*

a) Si $H\Phi(G) = G$ alors $H = G$.

b) Si K est distingué alors $K\Phi(G)/K \subset \Phi(G/K)$.

c) Si K est distingué et $K \subset \Phi(H)$ alors $K \subset \Phi(G)$.

d) Si K est distingué, $\Phi(G) \subset K$ et $K/\Phi(G)$ pronilpotent alors K est pronilpotent. En particulier, $\Phi(G)$ est un groupe pronilpotent.

e) G est pronilpotent ssi $G/\Phi(G)$ est abélien.

Preuve: a) Comme H est fermé, H est l'intersection des sous-groupes ouverts contenant H. Si $H \neq G$, il existe un sous-groupe ouvert maximal U contenant H. On a alors $H\Phi(G) \subset U \neq G$.

b) On a $\Phi(G/K) = T/K$ où T est l'intersection des sous-groupes ouverts maximaux de G contenant K. Ainsi $\Phi(G) \subset T$.

c) Supposons que $K \not\subset \Phi(G)$, donc il existe un sous-groupe ouvert U maximal tel que $K \not\subset U$. La maximalité de U assure que $KU = G$ et comme $K \subset H$ on a $H = K(U \cap H)$. Comme $K \subset \Phi(H) \subset H$, on a $\Phi(H)(U \cap H) = H$ et donc, d'après a), $H = M \cap H$. Ainsi $K \subset H \subset U$ et donc $G = KU = U$ ce qui est absurde.

d) Soit Q un sous-groupe de Sylow de K. On sait que $\Phi(G)Q/\Phi(G)$ est un sous-groupe de Sylow de $K/\Phi(G)$, il est distingué puisque $K/\Phi(G)$ est supposé pronilpotent. De plus, on sait que

$$G/\Phi(G) = (K/\Phi(G))N_{G/\Phi(G)}(\Phi(G)Q/\Phi(G))$$

et donc, $\Phi(G)Q$ est distingué dans G. Comme Q est un sous-groupe de Sylow de $\Phi(G)Q$, on sait que $G = (\Phi(G)Q)N_G(Q)$. Ainsi, par le a), on a $G = N_G(Q)$, ceci assurent que les sous-groupes de sylow de K sont distingués et donc que K est pronilpotents.

e) $G/\Phi(G)$ est abélien, donc, par d), G est pronilpotent. Réciproquement, si G est pronilpotent, $N_G(U) \neq U$ pour tout sous-groupe ouvert propre de G, donc pour tout sous-groupe ouvert maximal M de G, on a $N_G(M) = G$ et donc M est distingué dans G. De plus, comme M est maximal, G/M est un groupe cyclique d'ordre premier. Ainsi, si $x, y \in G$, alors $x^{-1}y^{-1}xy \in M$ pour tout M et par suite $x^{-1}y^{-1}xy \in \bigcap M = \Phi(G)$. Ceci assure que $G/\Phi(G)$ est abélien.

Chapitre 4

Proliberté

4.1 Rang

4.1.1 Groupes profinis de type fini

Soit G un groupe profini et X une partie de G. On note $< X >$ l'adhérence dans G du sous-groupe engendré par X dans G.

Définition 82.— *On dit qu'une partie X de G engendre (topologiquement) G, si $< X >= G$. On parle alors de système de générateurs.*

S'il existe une partie X finie de G qui engendre G on dit alors que G est de rang fini et l'on appelle rang (topologique) de G le cardinal minimal d'une famille X qui engendre G. On note $\mathrm{rg}(G)$ *cet entier.*

Exemples : • Si G est fini, il est profini et sa topologie est la topologie discrête. On voit alors sans mal que la notion de rang topologique correspond à la notion classique de rang algébrique.
• Les groupes $\mathbb{Z}_p$ et $\widehat{\mathbb{Z}}$ sont de rang 1 puisque la partie $X = \{1\}$ engendre ces groupes.
• Si $G \to H$ est un morphisme surjectif et continu de groupes profinis, alors si G est de rang fini, H l'est aussi et $\mathrm{rg}(H) \leq \mathrm{rg}(G)$. On peut en déduire, par exemple, que $\mathrm{rg}(\mathbb{Z}_p^n) = n$. En effet, la famille $\{(1,0,\cdots,0);(0,1,0,\cdots,0);\cdots;(0,\cdots,0,1)\}$ engendre bien $\mathbb{Z}_p^n$ et donc $\mathrm{rg}(\mathbb{Z}_p^n) \leq n$. Maintenant, le groupe $\mathbb{Z}_p^n$ se surjecte continument sur le groupe $(\mathbb{Z}/p)^n$. Ce groupe est de rang n (c'est un $\mathbb{F}_p$-e.v. de dimension n), donc $\mathrm{rg}(\mathbb{Z}_p^n) \geq n$.

Proposition 83.— *Soit G un groupe profini de rang fini. Pour tout entier n, il n'y a qu'un nombre fini de sous-groupes ouverts d'indice n dans G.*

Preuve : Comme tout sous-groupe ouvert contient un sous-groupe ouvert distingué, il suffit de montrer cette propriété pour les sous-groupes ouverts distingué. Si N est un sous-groupe distingué ouvert d'indice n, alors $\Gamma \simeq G/N$ est un groupe d'ordre n. Il y a un nombre fini de sous-groupes ouverts distingués N tels que $G/N \simeq \Gamma$, car si X désigne une famille finie d'élément de G engendrant G, alors un morphisme surjectif continu de G sur Γ est entièrement déterminé par ses valeurs en X. Donc il y a exactement autant de tels sous-groupes N que de morphismes continus surjectifs de G sur Γ. Maintenant, il n'y a qu'un nombre fini de groupe Γ d'ordre n, ce qui achève la preuve.

Si G est de rang fini, alors pour tout entier $n \geq 1$, le nombre de sous-groupes ouverts d'indice $\leq n$ est fini, donc leur intersection G_n est un sous-groupe ouvert

(et distingué). La suite $(G_n)_n$ est alors décroissante et d'intersection réduite à $\{1\}$. Ils forment donc une "filtration" profinie naturelle, et l'on a

$$G \simeq \varprojlim G/G_n$$

4.1.2 Rang topologique

Soit G un groupe profini et X un système de générateurs de G. On dit que X converge vers 1 si pour tou sous-groupe ouvert distingué N de G, l'ensemble $X - N$ est fini. Par exemple, si G est de rang fini, alors G possède un système de générateurs convergeant vers 1. De manière générale,

Proposition 84.— (Douady) *Tout groupe profini possède un système de générateurs qui converge vers* 1.

Proposition 85.— *Soit G un groupe profini de rang infini et $\mathcal{N}$ l'ensemble des sous-groupes ouverts distingués de G. Si X est un système de générateurs de G convergeant vers* 1*, alors $\sharp X = \sharp\mathcal{N}$.*

Preuve : Puisque X peut s'écrire

$$X = \bigcup_{N\in\mathcal{N}} (X - N)$$

et que $X - N$ est fini par hypothèse, on a donc $\sharp X \leq \sharp\mathcal{N}$. Considérons maintenant pour toute partie A de X, l'ensemble

$$\mathcal{N}(A) = \{N \in \mathcal{N}/\ X - A \subset N\}$$

On a alors

$$\mathcal{N} = \bigcup_A \mathcal{N}(A)$$

Pour A donné, considérons $G(A)$ le plus petit sous-groupe distingué fermé de G contenant $X - A$. Le groupe quotient $G/G(A)$ est alors de rang fini (une classe de générateurs de ce groupe est donnée par l'image de A par la surjection canonique $G \mapsto G/G(A)$) et il y a une bijection entre $\mathcal{N}(A)$ et les sous-groupes ouverts distingués de $G/G(A)$. On sait qu'il n'y a qu'un nombre fini de sous-groupes ouverts d'indice donné dans $G/G(A)$, on en déduit donc que $\mathcal{N}(A)$ est dénombrable.

Puisque X est infinie, l'ensemble des parties finies de X est de même cardinal que X, on en déduit donc que $\mathcal{N}$ est une réunion de $\sharp X$ ensembles dénombrables, ce qui implique $\sharp\mathcal{N} \leq \sharp X$.

Définition 86.— *Si G est un groupe profini de rang infini, on appelle rang de G le cardinal d'un système de générateurs de G convergeant vers* 1.

Exemples.— • Soit $(G_i)_{i\in I}$ une famille infinie de groupes finis. On sait que $G = \prod_i G_i$ est un groupe profini. On a alors $rg(G) = \sharp I$. En effet, considérons l'ensemble

$$X = \bigcup_{i\in I} G_i \subset G$$

Cet ensemble est visiblement un système de générateurs (puisqu'il est dense) qui a pour cardinal $\sharp I$. Maintenant soit N un sous-groupe ouvert distingué. Du fait de la définition de la topologie produit, il existe une partie finie $J \subset I$ telle que

$$\prod_{j\notin J} G_j \subset N$$

On a alors

$$X - N \subset X - \prod_{j \notin J} G_j \subset \bigcup_{j \in J} G_j$$

ce qui assure que $X - N$ est fini et donc que X converge bien vers 1.

• Si K est un corps dénombrable, alors G_K est un groupe profini de rang $\leq \aleph_0$. En effet, on sait que $rg(G_K)$ est précisément égal au cardinal de l'ensemble de ses sous-groupes ouverts distingués, qui correspondent, pour la topologie de Krull, aux extensions galoisiennes finies de K. Le corps K étant dénombrable, il n'y a qu'un nombre dénombrable de polynômes à coefficients dans K et donc, au plus un nombre dénombrable d'extensions galoisiennes finies de K.

On peut caractériser finement, pour un groupe profini, le fait d'être de rang $\leq \aleph_0$:

Proposition 87.— *Pour un groupe profini G, les propositions suivantes*

i) G est de rang $\leq \aleph_0$,

ii) il existe une suite décroissantes de sous-groupes ouverts distingués $(U_n)_n$ de G telle que $\bigcap_n U_n = \{e\}$,

iii) il existe un système projectif $\cdots \mapsto G_{n+1} \mapsto G_n \mapsto \cdots$ indexé par $\mathbb{N}$ avec des morphismes surjectifs tels que $G = \varprojlim G_n$,

iv) G est métrisable.

sont équivalentes.

Preuve : *i)* $\Rightarrow$ *ii)* Puisque G est de rang $\leq \aleph_0$ il y a au plus $\aleph_0$ sous-groupes ouverts distingués dans G. On les indice en une suite $(S_n)_n$. Pour tout n entier, on pose

$$U_n = \bigcap_{k=0}^{n} S_k$$

La suite $(U_n)_n$ est donc une suite décroissante de sous-groupes ouverts distingués et l'on a

$$\bigcap_n S_n = \bigcap_n U_n$$

par ailleurs, on sait que $\bigcap_n S_n = \{e\}$.

ii) $\Rightarrow$ *i)* Puisque $\bigcap_n U_n = \{e\}$ il s'ensuit que G et $\varprojlim G/U_n$ sont topologiquement isomorphe et par suite que la famille $(U_n)_n$ forme un système fondamental de voisinages de e. Tout sous-groupe ouvert contient donc un U_n pour un certain n, or U_n étant d'indice fini, il n'y a donc qu'un nombre fini de sous-groupes contenant U_n et par suite G ne contient qu'un nombre dénombrable de sous-groupes ouverts distingués.

ii) $\Rightarrow$ *iii)* Il suffit de prendre $G_n = U_n/U_{n+1}$.

iii) $\Rightarrow$ *ii)* Il suffit de prendre $U_n = Ker(\varphi_n)$, où $\varphi_n : G \to G_n$ désigne l'application de projection.

ii) $\Rightarrow$ *iv)* Pour $x \in G$, $x \neq e$, on pose :

$$\nu(x) = Inf\{n \in \mathbb{N} / \ x \in U_n\}$$

et l'on convient que $\nu(e) = +\infty$. On pose alors pour tout couple $(x, y) \in G^2$:

$$d(x, y) = e^{\nu(xy^{-1})}$$

(avec la convention $e^{-\infty} = 0$). L'application d est alors une distance sur G : la seule chose non immédiate est l'inégalité triangulaire. Soit $x, y, z \in G$, posons

$$\nu(xy^{-1}) = n$$
$$\nu(yz^{-1}) = m$$

et $k = Inf(n, m)$. On a donc $xy^{-1} \in U_k$ et $yz^{-1} \in U_k$, donc $xz^{-1} \in U_k$ et par suite

$$\nu(xz^{-1}) =\geq k$$

l'inégalité triangulaire découle alors de cette dernière inégalité.

Montrons que d est compatible avec la topologie de G. Pour commencer, remarquons que pour $x \in G$ et $\epsilon > 0$ donnés, on a

$$B(x, \epsilon) = xU_{[\log \epsilon + 1]} = xB(e, \epsilon)$$

et donc que la donnée locale des voisinages de e définit tous les voisinages de x. Ainsi pour montrer que la distance d est compatible avec la topologie profinie de G, il suffit de vérifier que les filtres des voisinages de e pour ces deux topologies coincident.

La famille $(U_n)_n$ forme un système fondamental de voisinages de e. Par ailleurs, on a pour tout n

$$U_n = B(e, e^{-n})$$

et la famille $(B(e, e^{-n}))_n$ forme un système fondamental de voisinages de e pour d. Ce qui prouve bien l'équivalence des deux topologies.

iv) $\Rightarrow$ *ii)* Soit d une distance sur G compatible. Pour tout entier n, la boule $B(e, 1/n + 1)$ est un voisinage ourvert de e et donc il existe un sous-groupe ouvert distingué S_n de G tel que $S_n \subset B(e, 1/n + 1)$. On pose alors pour tout entier n

$$U_n = \bigcap_{k=0}^{n} S_k$$

ce qui nous donne bien une suite décroissante de sous-groupes ouverts distingués $(U_n)_n$ qui vérifie :

$$\bigcap_n U_n = \bigcap_n S_n \subset \bigcap_n B(e, 1/n + 1) = \{e\}$$

4.2 Complétions profinies

On considère un groupe G et une famille $\mathcal{N}$ de sous-groupes distingués d'indices finis de G vérifiant les deux propriétés suivantes:

• si $N \in \mathcal{N}$ et si M est un sous-groupe distingué de G contenant N alors $M \in \mathcal{N}$,

• si $N_1, N_2 \in \mathcal{N}$ alors $N_1 \cap N_2 \in \mathcal{N}$.

A toute paire $N_1, N_2 \in \mathcal{N}$, telle que $N_1 \subset N_2$, on associe l'homomorphisme canonique $\varphi_{N_1 N_2} : G/N_1 \to G/N_2$.

Lemme 88.— *Le système* $(G/N, \varphi_{N_1 N_2})_{\mathcal{N}}$ *est projectif.*

Preuve: Immédiat

Définition 89.— *La limite projective du système $(G/N, \varphi_{N_1N_2})_{\mathcal{N}}$ est un groupe profini que l'on note $\widehat{G}_{\mathcal{N}}$ et que l'on appelle complétion profinie respectivement à l'ensemble $\mathcal{N}$ de G. Si $\mathcal{N}$ désigne l'ensemble de tous les sous-groupes distingués d'indices finis de G, on note plus simplement ce groupe $\widehat{G}$ et on l'appelle complétion profinie de G.*

Pour tout $N \in \mathcal{N}$, on note $\varphi_N : \widehat{G}_{\mathcal{N}} \to G/N$ l'application de projection et $\pi_N : G \to G/N$ la surjection canonique. Il est clair que pour tout $N \subset M$, on a $\pi_M = \varphi_{NM} \circ \pi_N$. Il s'ensuit qu'il existe un unique homomorphisme $\theta : G \to \widehat{G}_{\mathcal{N}}$ faisant commuter les diagrammes.

Exercice : a) Montrer que l'ensemble des réunions de classes gN pour $N \in \mathcal{N}$ définit une topologie qui fait de G un groupe topologique.

b) Montrer que si l'on muni G de cet topologie, alors θ est continue.

Proposition 90.— *Le groupe $\theta(G)$ est dense dans $\widehat{G}_{\mathcal{N}}$ et le noyau de l'homomorphisme θ est le sous-groupe $N_\infty = \bigcap_{N\in\mathcal{N}} N$.*

Preuve: • Comme $\varphi_N \circ \theta(G) = \pi_N(G) = G/N$ pour tout N, on en déduit , par l'exercice ???, que $\theta(G)$ est dense dans $\varprojlim G/N = \widehat{G}_{\mathcal{N}}$.

• Soit $x \in N_\infty$, alors pour tout $N \in \mathcal{N}$, on a $\varphi_N(\theta(x)) = \pi_N(x) = 1$. Donc $\theta(x) = 1$. Réciproquement, si $\theta(x) = 1$, alors $\pi_N(x) = \varphi_N(\theta(x)) = 1$ ce qui montre que $x \in N$ pour tout $N \in \mathcal{N}$.

Remarque: Si G est profini, alors G s'injecte dans $\widehat{G}$. Il n'est pas toujours vrai qu'alors $G = \widehat{G}$. En fait, on a $G = \widehat{G}$ si et seulement si les sous-groupes d'indice fini de G sont ouverts. En effet, si c'est le cas, on sait qu'alors l'ensemble de tous les sous-groupes ouverts distingués N forment une base de filtre et que $G \simeq \varprojlim G/N$, or ici $\widehat{G} = \varprojlim G/N$. Réciproquement, si θ est un isomorphisme, alors à cause de la compacité des groupes, c'est un homéomorphisme. Les sous-groupes d'indices finis N de G sont des sous-groupes ouverts de $\widehat{G} = G$ donc des sous-groupes ouverts de G.

En particulier, si $G = \mathbb{Z}_p$, alors on a $\widehat{\mathbb{Z}_p} = \mathbb{Z}_p$. En effet, nous avons montré précédemment que les sous-groupes ouverts de $\mathbb{Z}_p$ sont exactement les sous-groupes d'indice fini (qui sont précisement les $p^n\mathbb{Z}_p$).

Proposition 91.— *Pour tout $M \subset G$, notons $\widehat{M} = \overline{\theta(M)}$. On a alors pour tout $N \in \mathcal{N}$, $\widehat{N} = Ker(\varphi_N)$ et par suite on a l'isomorphisme*

$$G/N \simeq \widehat{G}_{\mathcal{N}}/\widehat{N}$$

En particulier, l'ensemble $\{\widehat{N}/\ N \in \mathcal{N}\}$ est une base de voisinage de e dans $\widehat{G}_{\mathcal{N}}$.

De plus, si $\mathcal{M}$ est la famille de tous les sous-groupes de G qui contiennent des éléments de $\mathcal{N}$, alors l'application $M \mapsto \widehat{M}$ est une bijection de $\mathcal{M}$ dans l'ensemble des sous-groupes ouverts de $\widehat{G}_{\mathcal{N}}$. On a alors pour tout $M \in \mathcal{M}$, $[G : M] = [\widehat{G} : \widehat{M}]$.

Preuve: Soit $N \in \mathcal{N}$, on a $\theta(N) \subset Ker(\varphi_N)$ et puisque ce groupe est fermé, on a donc

$$\widehat{N} = \overline{\theta(N)} \subset Ker(\varphi_N)$$

Réciproquement, considérons un élément $x \in Ker(\varphi_N)$. Prenons un ouvert du système fondamental de voisinages de x, c'est-à-dire un ensemble de la forme

$x.Ker(\varphi_{N'})$ pour un certain $N^{'} \in \mathcal{N}$. Il existe $y \in G$ tel que

$$\varphi_{N\cap N'}(x) = y(N \cap N^{'})$$

On a alors

$$\begin{array}{rcl} yN & = & \varphi_N(x) \\ yN^{'} & = & \varphi_{N'}(x) \end{array}$$

il s'ensuit que

$$\theta(y) \in \theta(N) \cap x.Ker(\varphi_{N'})$$

et par suite, tout voisinage de tout point de $Ker(\varphi_N)$ rencontre $\theta(N)$, c'est-à-dire que $\theta(N)$ est dense dans $Ker(\varphi_N)$.

Soit maintenant $g \in G$, on a

$$gN = \varphi_N(\theta(g))$$

mais comme $\widehat{N} = Ker(\varphi_N)$, on a

$$\theta(G) \cap \widehat{N} = \theta(N)$$

Par ailleurs, pour tout $x \in \widehat{G}$, il existe $g \in G$ tel que

$$\varphi_N(x) = gN = \varphi_N(\theta(g))$$

et donc $x \in \theta(g).\widehat{N}$ et, par suite

$$\widehat{G} = \theta(G).\widehat{N}$$

On en déduit donc que

$$G/N \simeq \theta(G)/\theta(N) \simeq \widehat{G}/\widehat{N}$$

Soit $M^{'}$ un sous-groupe de $\widehat{G}$. Il existe donc $N \in \mathcal{N}$ tel que $\widehat{N} \subset M^{'}$. L'isomorphisme précédent, assure alors qu'il existe un sous-groupe M de G contenant N tel que

$$M^{'} = \theta(M)\widehat{N} \text{ et } \theta(G) \cap M^{'} = \theta(M)$$

En particulier, on a $M^{'} = \widehat{M}$ et $(G : M) = (\widehat{G} : \widehat{M})$.

Définition 92.— *Une famille $\mathcal{C}$ de groupes finis est dite "presque pleine" si :*

a/ $\mathcal{C}$ contient des groupes non triviaux,

b/ si $G \in \mathcal{C}$, tout quotient de G est dans $\mathcal{C}$,

c/ si $G \in \mathcal{C}$, tout sous-groupe de G est dans $\mathcal{C}$,

d/ si $G_1, G_2 \in \mathcal{C}$,alors $G_1 \times G_2 \in \mathcal{C}$.

On dit que la famille $\mathcal{C}$ est "pleine" si elle vérifie en plus :

e/ si $1 \to A \to B \to C \to 1$ est une suite exacte de groupe et si $A, C \in \mathcal{C}$, alors $B \in \mathcal{C}$.

Une limite inverse de groupes dans $\mathcal{C}$ est alors appellée pro-$\mathcal{C}$-groupe.

Exemples: • si $\mathcal{C}$ contient tous les groupes finis, alors $\mathcal{C}$ est pleine et les pro-$\mathcal{C}$-groupes sont exactement les groupes profinis.

• Si $\mathcal{C}$ est l'ensemble des p-groupes, alors $\mathcal{C}$ est pleine et on appelle les pro-$\mathcal{C}$-groupes des pro-p-groupes. Par exemple $\mathbb{Z}_p$ est un pro-p-groupe.

• Si $\mathcal{C}$ est l'ensemble des groupes finis abéliens (resp. nilpotents, résolubles) alors $\mathcal{C}$ est presque pleine mais pas pleine. Les pro-$\mathcal{C}$-groupes sont appellés groupes abélien profini (resp. pro-nilpotents, pro-résolubles).

4.3 Groupes prolibres

Définition 93.— *Soit $\mathcal{C}$ une classe presque pleine de groupes finis. Un pro-$\mathcal{C}$-groupe F est dit pro-$\mathcal{C}$-libre s'il possède un système de générateurs convergeant vers* 1 *ayant la propriété suivante : si, pour une application $\varphi_0 : X \mapsto G$ de X dans un pro-$\mathcal{C}$-groupe G, l'ensemble $\varphi_0(X)$ converge vers* 1*, alors il existe un homomorphisme continu*

$$\varphi : F \longrightarrow G$$

qui étend φ_0 (i.e. $\varphi_{|X} = \varphi_0$). Dans ces conditions, l'ensemble X est appelé "base de F".

On remarque, pour des raisons évidentes, que si φ existe, il est alors unique. Par ailleurs, si F et G sont deux groupes pro-$\mathcal{C}$-libres de même rang, alors ils sont isomorphes. C'est pour cela que nous parlerons dans la suite du groupe pro-$\mathcal{C}$-libre de rang α pour désigner un représentant, noté $\widehat{F}_\alpha(\mathcal{C})$, dans la classe de ces groupes.

Lorsque $\mathcal{C}$ désigne la classe de tous les groupes finis, on parlera plus simplement de groupes prolibres que l'on notera $\widehat{F}_\alpha$ s'ils sont de cardinal α.

Théorème 94.— *Pour tout classe $\mathcal{C}$ presque pleine de groupes finis et tout cardinal α, il existe un groupe pro-$\mathcal{C}$-libre de rang α.*

Preuve : On considère le groupe libre F sur un ensemble de lettres

$$X^{'} = \{x_i^{'}/\ i \in I\}$$

de cardinal α. Notons $\mathcal{N}$, l'ensemble des sous-groupes distingués N de F tels que

- $F/N \in \mathcal{C}$
- N contienne presque tous les éléments de $X^{'}$

L'ensemble $\mathcal{N}$ satisfait les propriétés qui permettent de définir une pro-$\mathcal{C}$-complétion de F que nous noterons

$$\widehat{F} = \varprojlim F/N$$

(c'est un pro-$\mathcal{C}$-groupe). On considère

$$\theta : F \longrightarrow \widehat{F}$$

le morphisme canonique et pour tout $i \in I$, on pose

$$x_i = \theta(x_i^{'}) \text{ et } X = \{x_i/\ i \in I\}$$

Il est clair que X est un système de générateurs de $\widehat{F}$ convergeant vers 1 puisque d'après la proposition ???, tout sous-groupe distingué ouvert de $\widehat{F}$ est de la forme $\widehat{N}$ avec $N \in \mathcal{N}$.

Considérons maintenant un pro-$\mathcal{C}$-groupe G et une application

$$\varphi_0 : X \longrightarrow G$$

telle que $\varphi_0(X)$ converge vers 1 dans G. Pour tout $i \in I$, posons

$$y_i = \varphi_0(x_i)$$

Si M est un sous-groupe ouvert distingué de G, alors l'application $x_i^{'} \mapsto y_i M$ s'éntend un un homomorphisme

$$\varphi_M : F \longrightarrow G/M$$

donc le noyau $Ker(\varphi_M)$ est un sous-groupe distingué N qui contient presque tous les $x_i^{'}$ (puisque G/M est fini) et comme F/N est isomorphe à un sous-groupe de G/M, on en déduit que $F/N \in \mathcal{C}$ et par suite que $N \in \mathcal{N}$. Notons maintenant $\overline{\varphi}_M$ le morphisme composé

$$\widehat{F} \longrightarrow F/N \longrightarrow G/M$$

Il satisfait $\overline{\varphi}_M(x_i) = y_i$, et par suite, comme la collection des $\overline{\varphi}_M$ fait commuter les diagrammes, elle définit un morphisme

$$\overline{\varphi} : \widehat{F} \longrightarrow G$$

tel que $\overline{\varphi}(x_i) = y_i$ pour tout i. Ainsi le groupe $widehatF$ est bien pro-$\mathcal{C}$-libre. Reste à voir que son rang est bien α.

Pour montrer cela, il suffit de montrer que $x_i \neq x_j$ pour $i \neq j$. Prenons un élément $C \in \mathcal{C}$ non trivial, $i \neq j$ et $c_i \neq c_j$ dans C. L'argument du paragraphe précédent montre que l'application

$$\begin{array}{ccc} x_i^{'} & \longmapsto & c_i \\ x_j^{'} & \longmapsto & c_j \end{array}$$

s'étend un morphisme

$$\overline{\varphi} : \widehat{F} \longrightarrow C$$

qui vérifie $\overline{\varphi}(x_i) = c_i \neq c_j = \overline{\varphi}(x_j)$.

Exemples.— • Si $\mathcal{C}$ est la classe des p-groupes finis, alors $\widehat{F}_1(\mathcal{C}) = \mathbb{Z}_p$. Si maintenant, $\mathcal{C}$ désigne la classe de tous les groupes finis alors $\widehat{F}_1(\mathcal{C}) = \widehat{\mathbb{Z}}$.
• Si G désigne un pro-$\mathcal{C}$-groupe de rang α, alors G est un quotient de $\widehat{F}_\beta(\mathcal{C})$ pour tout cardinal $\beta \geq \alpha$.
• Si $\alpha \leq \beta$ sont deux cardinaux, alors $\widehat{F}_\alpha(\mathcal{C})$ peut-être vu comme quotient et comme sous-groupe fermé de $\widehat{F}_\beta(\mathcal{C})$.

Chapitre 5

Théorie de Galois

5.1 Groupe de Galois

5.1.1 Clôture séparable

Lemme 95.— *Soit K un corps et $\overline{K}$ sa clôture algébrique. L'ensemble E des éléments de $\overline{K}$ séparables sur K est un sous-corps de $\overline{K}$.*

Preuve: Soit $x, y \in \overline{K}$ des éléments séparables. L'extension $K(x,y)/K$ est séparable, donc $x-y$ et xy^{-1} sont des éléments séparables.

Définition 96.— *L'ensemble des éléments séparable sur K s'appelle la clôture séparable de K et se note K^{sep}.*

Proposition *L'extension K^{sep}/K est galoisienne, c'est la plus grande extension galoisienne de K.*

Preuve: Par hypothèse, K^{sep}/K est séparable. Reste à montrer qu'elle est normale. Soit $x \in K^{sep}$, les conjugués de x sont aussi séparbale, donc vivent dans K^{sep}. Soit L/K galoisienne, L/K est en particulier séparable donc $L \subset K^{sep}$.

Exemple: • Si K est de caractéristique 0, alors $K^{sep} = \overline{K}$.

• Si K est fini, alors $K^{sep} = \overline{K}$.

• Soit K un corps de caractéristique p. Considérons dans $K(X)[T]$ le polynôme $P(T) = T^p - X$. P est irréductible (Eisenstein) et $P' = 0$, donc P n'est pas séparable et par suite $K(X)^{sep} \neq \overline{K(X)}$.

Définition 97.— *Un corps K est dit parfait si $K^{sep} = \overline{K}$.*

Proposition *Soit K un corps de caractéristique p. Les propositions suivantes sont équivalentes:*

i) K est parfait,

ii) l'endomorphisme $x \mapsto x^p$ est surjectif.

Preuve: $i) \Rightarrow ii)$: Soit $a \in K$. Considérons le polynôme $P(X) = x^p - a$ et L son corps de décomposition sur K. Comme K est parfait, L/K est séparable et par suite galoisienne. Soit $b \in L$ une racine de P. Comme $P(b) = 0$, son polynôme minimal divise donc $P(X) = (X-b)^p$ et comme b est séparable, ce polynôme est $X - b$ ce qui prouve que $b \in K$.

ii) $\Rightarrow$ *i)* : Soit $P \in K[X]$ un polynôme irréductible et inséparable. On a alors $P(X) = \sum_{i=0}^{n} a_i X^{ip}$. Soit $b_i \in K$ tel que $a_i = b_i^p$, on a donc:

$$P(X) = \sum_{i=0}^{n} (b_i X^i)^p = \left(\sum_{i=0}^{n} b_i X^i \right)^p$$

ce qui est contraire à l'irréductibilité de P.

Définition 98.— *Le groupe de Galois de l'extension K^{sep}/K s'appelle le groupe de Galois absolu de K et se note $G(K)$ ou G_K.*

5.1.2 Topologie de Krull

Soit L/K une extension galoisienne. On considère un ensemble $\mathcal{E}$ d'extensions galoisiennes finies L_i/K tel que $L = \bigcup_i L_i$ (il existe de tels ensembles, par exemple celui constitué de toute les extensions galoisiennes finies). On ordonne $\mathcal{E}$ par inclusion, c'est alors un ordre filtrant à droite. En effet, si L_i et L_j sont dans $\mathcal{E}$ alors $L_i.L_j/K$ est galoisienne et par suite il existe $\alpha \in L$ tel que $L_i.L_j = K(\alpha)$. Mais par hypothèse, il existe $L_k \in \mathcal{E}$ tel que $\alpha \in L_k$. On a alors $L_i \subset L_k$ et $L_j \subset L_k$.

Pour tout $L_i \subset L_j$ si on appelle $\varepsilon_{ij} : L_i \to L_j$ l'injection canonique, alors, on a:

$$L = \varinjlim L_i$$

Comme L_i/K est galoisienne, le groupe $G^i = Gal(L/L_i)$ est un sous-groupe normal de $Gal(L/K)$. Considérons l'ensemble $\mathcal{V} = \{G^i\}$.

Lemme 99.— *$\mathcal{V}$ est une base de filtre.*

Preuve: Soit G^i et G^j dans $\mathcal{V}$. Le sous-groupe $G^i \cap G^j$ est visiblement normale dans $Gal(L/K)$. Maintenant considérons le compositum $L_i.L_j$. C'est une extension galoisienne de K de degré fini. Il est clair que $G^i \cap G^j = Gal(L/L_i.L_j)$. Soit $\alpha \in L$ un élément primitif de $L_i.L_j/L$. Par hypothèse, il existe k tel que $\alpha \in L_k$. On a alors $G^k \subset Gal(L/L_i.L_j) = G^i \cap G^j$.

Maintenant, il est clair que

- $\forall U \in \mathcal{V},\ \exists V \in \mathcal{V},\ V.V \subset U$ (prendre $V = U$).
- $\forall U \in \mathcal{V},\ \exists V \in \mathcal{V},\ V^{-1} \subset U$ (prendre $V = U$).
- $\forall U \in \mathcal{V},\ \forall a \in Gal(L/K),\ \exists V \in \mathcal{V},\ V \subset aUa^{-a}$ (prendre $V = U$). On en déduit donc qu'il existe une unique topologie sur $Gal(L/K)$ compatible avec la structure de groupe topologique pour laquelle $\mathcal{V}$ est une base de filtre de voisinages de l'élément neutre.

Proposition-Définition 100.— *La topologie ainsi décrite sur $Gal(L/K)$ est indépendante du choix de $\mathcal{E}$. On l'appelle topologie de Krull.*

Preuve: Soit $\mathcal{V}$ et $\mathcal{V}'$ les bases de voisinages de l'élément neutre de $Gal(L/K)$ associée aux deux familles $\mathcal{E}$ et $\mathcal{E}'$ d"extensions galoisiennes finies engendrants L. Soit $G = Gal(L/L_i) \in \mathcal{V}$ et α un élément primitif de L_i/K. Il existe $L_i' \in \mathcal{E}'$ tel que $\alpha \in L_i'$, on a alors $G' \subset G$ avec $G' = Gal(L/L_i') \in \mathcal{V}'$. Les topologies définies sont donc les mêmes.

Exemple: Soit L/K une extension galoisienne finie. Considérons pour $\mathcal{E}$ l'ensemble $\{L\}$. On a donc $\mathcal{V} = \{1 = Gal(L/L)\}$ et par suite, 1 est un ouvert, donc la topologie sur $Gal(L/K)$ est la topologie discrète.

On considère un ensemble $\mathcal{E}$ d'extensions galoisiennes finies L_i/K tel que $L = \bigcup_i L_i$. Pour tout i, on note $\pi_i : Gal(L/K) \to Gal(L_i/K)$ la surjection canonique. L'application π est visiblement un homomorphisme de groupe. Cet homomorphisme est continu si l'on considère sur $Gal(L/K)$ la topologie de Krull et sur $Gal(L_i/K)$ la topologie discrète. Pour montrer ce fait, il suffit de montrer que $\pi^{-1}(\{\sigma\})$ est ouvert dans $Gal(L/K)$ pour tout $\sigma \in Gal(L_i/K)$ (puisque ce dernier ensemble est discrêt et fini), ce qui équivaut à montrer que $\pi^{-1}(\{Id\})$ est ouvert puisque l'application $\psi_\sigma : \mu \to \sigma.\mu$ est un homéomorphisme de $Gal(L_i/K)$. Maintenant, $\pi^{-1}(\{Id\}) = Gal(L/L_i) = G^i$ qui est ouvert par définition.

Pour tout i, on note $G_i = Gal(L_i/K)$. Si $L_i \subset L_j$, on note $\varphi_{ji} : G_j \to G_i$ la surjection canonique. Il est immédiat que le système (G_i, φ_{ji}) est un système projectif de groupes finis. Si l'on muni les G_i de la topologie discrète, alors φ_{ji} est continue. On considère le groupe profini $\varprojlim G_i$ muni de sa structure de groupe toplogique naturelle. On a alors:

Théorème 101.— *Il existe un isomorphisme de groupe topologique entre $Gal(L/K)$ (muni de la topologie de Krull) et $\varprojlim G_i$.*

Preuve: Soit G un groupe topologique et pour tout i, $\varphi_i : G \to G_i$ un homomorphisme continu de groupe tel que pour tout $i \leq j$, $\varphi_i = \varphi_{ji} \circ \varphi_j$. Pour tout $\sigma \in G$, désignons par $\theta(\sigma) : L \to L$ l'application définie, pour $x \in L$, par:

$$\theta(\sigma)(x) = \varphi_i(\sigma)(x) \; lorsque \; x \in L_i$$

L'application $\theta(\sigma)$ est bien définie car si $x \in L_j$ et si $L_i.L_j \subset L_k$, alors

$$\begin{aligned} \varphi_i(\sigma)(x) &= \varphi_{ki} \circ \varphi_k(\sigma)(x) \\ &= \varphi_k(\sigma)(x) \\ &= \varphi_{kj} \circ \varphi_k(\sigma)(x) \\ &= \varphi_j(\sigma)(x) \end{aligned}$$

L'application $\theta(\sigma)$ est visiblement un K-automorphisme de L et $\theta : G \to Gal(L/K)$ vérifie bien que c'est la seule application à vérifier $\varphi_i = \pi_i \circ \theta$. L'application θ est homomorphisme de groupe. Elle est bien continue car $\theta^{-1}(G^i) = \varphi_i^{-1}(\{Id\})$. D'où l'isomorphisme de groupe topologique.

Le groupe de Galois d'une extension galoisienne est donc un groupe profini. En particulier, muni de la topologie de Krull (qui est compatible avec la topologie de groupe profini), ce groupe est compact et totalement discontinu.

5.2 Théorie de Galois

5.2.1 Correspondances galoisiennes

On considère une extension L/K galoisienne. Pour fixer les idées, comme base de voisinages de l'unité de $Gal(L/K)$ pour la topologie de Krull, on prend les sous-groupes $G^i = Gal(L/L_i)$ pour toutes les extensions galoisiennes finies L_i/K avec $L_i \subset L$.

Pour tout corps intermédiaire M, on note $gr(M) = Gal(L/M)$ le sous-groupe

de $Gal(L/K)$ constitué des M-automorphismes de L. De même, pour tout sous-groupe H de $Gal(L/K)$, on note $inv(H) = L^H$ le sous-corps de L constitué des éléments invariants par H.

Lemme 102.— *Pour tout corps intermédiaire M de l'extension L/K, l'extension L/M est galoisienne et on a $inv(gr(M)) = M$.*

Preuve: Soit $\alpha \in L$ et $Min_K(\alpha)$ (resp. $Min_M(\alpha)$) le polynôme minimal de α sur K (resp. sur M). Comme L/K est galoisienne, $Min_K(\alpha)$ est scindé à racines simples dans L. Comme $Min_M(\alpha)$ divise $Min_K(\alpha)$, on en déduit que ce polynôme est aussi scindé à racines simples dans L.

Le fait que $inv(gr(M)) = M$ si L/K est fini est bien connu. De manière générale, il est clair que $M \subset inv(gr(M))$. Soit $\alpha \in inv(gr(M))$. Si $\alpha \notin M$, alors α possède un conjugué $\beta \neq \alpha$ dans K^{sep} et il existe un M-isomorphisme σ tel que $\sigma(\alpha) = \beta$. La restriction de σ à L est un élément de $Gal(L/M) = gr(M)$, ce qui est en contradiction avec le fait que $\alpha \in inv(gr(M))$.

Lemme 103.— *Si M un corps intermédiaire de l'extension L/K, alors le groupe $Gal(L/M)$ est un sous-groupe fermé de $Gal(L/K)$.*

Preuve: Soit $\sigma \in Gal(L/K)$ tel que $\sigma \notin Gal(L/M)$. Il existe donc $x \in M$ tel que $\sigma(x) \neq x$. Considérons la clôture galoisienne $L_i = \widetilde{K(x)}$ de l'extension $K(x)/K$ dans L. L'extension L_i/K est galoisienne et finie. Le groupe G^i est un sous-groupe ouvert de $Gal(L/K)$ donc l'ensemble

$$U = \sigma.G^i = \left\{\mu \in Gal(L/K)/\ \mu_{|L_i} = \sigma_{|L_i}\right\}$$

est un ouvert qui voisine σ. Par ailleurs, pour tout $\mu \in U$, $\mu(x) \neq x$, ce qui prouve que $U \cap Gal(L/M) = \emptyset$ et par suite que le complémentaire de $Gal(L/M)$ dans $Gal(L/K)$ est ouvert.

Théorème 104.— (Krull) *Soit H un sous-groupe de $Gal(L/K)$. On a*

$$gr(inv(H)) = \overline{H}$$

Preuve: Grace au lemme précédent, il nous reste à vérifier que H est dense dans $gr(inv(H))$, c'est-à-dire que si un ouvert de $Gal(L/K)$ rencontre $gr(inv(H))$, il rencontre aussi H. Soit donc $\sigma \in gr(inv(H))$ et U un ouvert de $Gal(L/K)$ voisinant σ. Comme les G^i constitue une base de voisinage de l'unité, on peut supposer que $U = \sigma.G^i$.

Soit $M = inv(H)$. L'extension L_i/K étant galoisienne et finie, l'extension $L_i.M/M$ est galoisienne et finie. Soit $H^{'}$ l'ensemble des restrictions des éléments de H à $L_i.M$. $H^{'}$ est donc un sous-groupe de $Gal(L_i.M/M)$ dont le corps des invariants est égal à M. Le théorème de Galois affirme alors que $H^{'} = Gal(L_i.M/M)$. Soit $\tau^{'}$ la restriction de σ à $L_i.M$ alors $\tau^{'} \in Gal(L_i.M/M)$ et par suite, il existe $\tau \in H$ tel que $\tau^{'}$ soit la restriction de τ à $L_i.M$. Comme $\sigma^{-1}.\tau_{|L_i.M} = Id$, on a $\sigma^{-1}.\tau_{|L_i} = Id$ et par suite $\tau \in \sigma.G^i = U$. Ainsi $\tau \in U \cap H \neq \emptyset$.

Corollaire 105.— *Les correspondances galosiennes gr et inv constituent donc des bijections réciproques l'une de l'autre (et renversant les inclusions) entre les corps intermédiaires de l'extension L/K et les sous-groupes fermés de $Gal(L/K)$.*

5.2.2 Propriétés galoisiennes

Extensions intermédiaires

Théorème 106.— *Soit L/K une extension galoisienne et M un corps intermédiaire. Les propositions suivantes sont équivalentes:*

i) M/K est galoisienne,

ii) $Gal(L/M)$ est un sous-groupe dinstingué dans $Gal(L/K)$.

Dans ces conditions, il y a un isomorphisme de groupes topologiques entre $Gal(M/K)$ et $Gal(L/K)/Gal(L/M)$.

Preuve: $i) \Rightarrow ii)$ Si M/K est galoisienne, alors la surjection canonique $Gal(L/K) \rightarrow Gal(M/K)$ a pour noyau $Gal(L/M)$ qui est donc un sous-groupe distingué de $Gal(L/K)$.

$ii) \Rightarrow i)$ Si $\sigma \in Gal(L/K)$, alors $inv(\sigma Gal(L/M)\sigma^{-1}) = \sigma(M)$. Comme $Gal(L/M)$ est distingué, on a $\sigma(M) = inv(Gal(L/M)) = M$ pour tout $\sigma \in Gal(L/K)$ et par suite, $Isom_K(M) = Aut_K(M)$. L'extension M/K est donc normale, elle est séparable puisque L/K l'est.

Dans ces conditions, on a la suite exacte:

$$1 \rightarrow Gal(L/M) \rightarrow Gal(L/K) \rightarrow Gal(M/K) \rightarrow 1$$

La surjection $\varphi : Gal(L/K) \rightarrow Gal(M/K)$ est surjective. En effet, les groupes étant topologiques, il suffit de montrer que cette surjection est continue en Id. Une base de voisinage de Id dans $Gal(M/K)$ est donné par les $Gal(M/L_i)$ pour L_i/K galoisienne finie ($L_i \subset M$), or $\varphi^{-1}(Gal(M/L_i)) = Gal(L/L_i)$ qui est ouvert par définition.

Le groupe G est bien compact, le groupe $Gal(L/M)$ est fermé dans $Gal(L/K)$ et $Gal(M/K)$ est séparé. L'isomorphisme de groupes topologiques annoncé en découle alors.

Proposition 107.— *Soit $L/M/K$ une extension telle que L/M et M/K soient galoisiennes. Les propositions suivantes sont équivalentes:*

i) L/K est galoisienne,

ii) Tout K-automorphisme de M/K se relève en un K-automorphisme de L/K. (i.e. L'application de restriction $r : Aut_K(L) \rightarrow Gal(M/K)$ est surjective.)

Preuve: $i) \Rightarrow ii)$ Evident.

$ii) \Rightarrow i)$ Traitons pour commencer le cas où L/K est finie. Par hypothèse, on a une surjection $Aut_K(L) \rightarrow Gal(M/K)$. Son noyau est clairement $Gal(L/M)$. Donc $\sharp Aut_K(L) = \sharp Gal(L/M).\sharp Gal(M/K) = [L : K]$ ce qui prouve bien que L/K est galoisienne.

Revenons au cas général. L'extension L/K étant séparable, nous avons juste à vérifier que tous les conjugués sur K de tous les éléments de L sont dans L. Soit donc $\alpha \in L$ et $P(X) = X^n + a_{n-1}X^{n-1} + \widetilde{\cdots} + a_0$ le polynôme minimal de α sur M. Considérons le corps $K^{'} = K(a_0, \widetilde{\cdots}, a_{n-1})$ (clôture galoisienne de $K(a_0, \widetilde{\cdots}, a_{n-1})$ dans M qui existe car M/K est galoisienne) qui est une extension finie de K incluse dans M. Soit $\sigma \in Gal(K^{'}/K)$, on peut relever σ en un élément de $Gal(M/K)$ puisque M/K est galoisienne et par suite en un élément de $Aut(L/K)$ (par hypothèse). Notons $\alpha_1^{\sigma}, \cdots, \alpha_{n_\sigma}^{\sigma}$ les racines de

$$P^{\sigma}(X) = X^n + \sigma(a_{n-1})X^{n-1} + \cdots + \sigma(a_0)$$

Elles sont toutes dans L puisque L/M est galoisienne, $P^\sigma(X)$ est irréductible et que $\sigma(\alpha) \in L$ est racine de $P^\sigma(X)$.

Comme il y a un nombre fini de P^σ (puisqu'il y a un nombre fini de conjugué de a_i pour tout i), il y a un nombre fini de α_i^σ. Considérons le corps $N = K^{'}(\alpha_i^\sigma)_{\sigma,i}$. C'est un corps de dimension finie sur K et galoisien sur $K^{'}$. Soit $\mu \in Gal(K^{'}/K)$, on relève μ à M puis à L. La restriction de μ à N est un K-automorphisme. En effet, μ laisse globalement invariant $K^{'}$ et comme $\mu(P^\sigma(\alpha_i^\sigma)) = 0 = P^{\mu\sigma}(\mu(\alpha_i^\sigma))$ on en déduit que $\mu(\alpha_i^\sigma) = \alpha_j^{\mu\sigma} \in N$ pour un certain j. On a donc relevé tout élément de $Gal(K^{'}/K)$ à $Aut(N/K)$. On en déduit donc que N/K est galoisienne et par suite que les conjugués de α sur K sont dans N et donc dans L.

Remarque: Si $L/M/K$ une extension telle que L/M et M/K soient galoisiennes et si $Gal(M/K)$ se relève en un sous-groupe de $Gal(K/L)$, alors

$$Gal(L/K) \sim Gal(M/K) \times_s Gal(L/M)$$

l'action de $Gal(M/K)$ sur $Gal(L/M)$ étant, via le relèvement, l'action de conjugaison.

Extensions linéairement disjointes

Lemme 108.— *Soient L/K et M/K deux extensions d'un même corps, les propositions suivantes sont équivalentes:*

i) Toute famille d'éléments de L linéairement indépendante sur K est linéairement sur M.

ii) Toute famille d'éléments de M linéairement indépendante sur K est linéairement sur L.

Preuve: Exercice.

Définition 109.— *Deux extensions L/K et M/K sont dites linéairement disjointes (sur K) si elles satisfont les propriétés équivalentes du lemme précédent.*

Proposition 110.— *Soit L/K et M/K deux extensions. Si $[L : K] < +\infty$, alors les propositions suivantes sont équivalentes:*

i) L et M sont linéairement disjointes,

ii) $[L : K] = [LM : M]$.

Si, de plus, $[M : K] < +\infty$, alors ces propositions équivalent à :

ii$^{'}$) $[LM : K] = [L : K].[M.K]$.

Preuve: *i)* $\Rightarrow$ *ii)* Soit $e_1, \cdots, e_n$ une base de L comme K-espace vectoriel. L'espace vectoriel $L.M$ est engendré sur M par la famille $(e_1, \cdots, e_n)$. Par hypothèse, les éléments $e_1, \cdots, e_n$ sont linéairement indépendants sur K et donc sur M. ainsi, $(e_1, \cdots, e_n)$ est une base de $L.M$ en tant que M-espace vectoriel. Donc $[L : K] = [LM : M]$.

ii) $\Rightarrow$ *i)* Par hypothèse, $[L : K] = [LM : M] = n$. Soit $(e_1, \cdots, e_m)$ une famille d'éléments de L linéairement indépendantes sur K. Soit $(e_1, \cdots, e_n)$ une base de L qui complète $(e_1, \cdots, e_m)$.
La famille $(e_1, \cdots, e_n)$ engendre L sur K, donc engendre $L.M$ sur M, par suite c'est une base de $L.M$ donc est linéairement indépendante sur M, ce qui prouve bien que $(e_1, \cdots, e_m)$ est une famille d'éléments de L linéairement indépendants sur M.

$ii) \Rightarrow ii^{'})$ Si $[M:K] < +\infty$, alors on a

$$[L.M:K] = [L.M:M].[M:K] = [L:K].[M:K]$$

$ii^{'}) \Rightarrow i)$ Supposons $[L.M:K] = [L:K].[M:K] = p.q = n$. Soit $(e_1, \cdots, e_m)$ une famille libre de L que l'on complète en une base $(e_1, \cdots, e_p)$. Alors $(e_1, \cdots, e_p)$ engendre $L.M$ sur M donc est une base et par suite $(e_1, \cdots, e_m)$ est libre sur M.

Il est clair que si L et M sont linéairement disjoints sur K, alors $L \cap M = K$. La réciproque n'est pas vraie, par exemple soit $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ et $M = \mathbb{Q}(j\sqrt[3]{2})$. On a bien $L \cap M = \mathbb{Q}$ et pourtant $L.M = \mathbb{Q}(j, \sqrt[3]{2})$ qui est de degré 6 sur $\mathbb{Q}$ alors que M et L sont de degré 3. On a toutefois:

Théorème 111.— *Soient L/K et M/K deux extensions dont l'une est galoisienne. Les propositions suivantes sont équivalentes:*

i) L et M sont linéairement disjointes,

ii) $L \cap M = K$.

Dans ces conditions, si les deux extensions sont galoisiennes alors le groupe de Galois de l'extension $Gal(L.M/K)$ est isomorphe (en tant que groupe topologique) au groupe $Gal(L/K) \times Gal(M/K)$.

Preuve: $i) \Rightarrow ii)$ Evident.

$ii) \Rightarrow i)$ Supposons L/K galoisienne. On peut supposer que $[L:K] < +\infty$. En effet, si $(e_1, \cdots, e_m)$ est une famille K-libre d'éléments de L, alors la clôture galoisienne $\widetilde{L}$ de $K(e_1, \cdots, e_m)$ vérifie bien $\widetilde{L} \cap M = K$.

Posons $[L:K] = n$ et considérons $\alpha \in L$ un élément primitif de L/K. Soit $P(X) = \prod_{i=1}^{n}(X - \alpha_i) = Min_K(\alpha)(X)$ et $Q(X) = Min_M(\alpha)(X)$. Le polynôme Q est un diviseur de P totalement décomposé sur L. Si $Q \neq P$, alors les coefficients de Q sont dans $L \cap M$ et pas dans K ce qui est absurde. Donc $Q = P$ et par suite α est de degré n sur M, donc $[L.M:M] = [L.K]$.

Montrons l'isomorphisme dans le cas fini. Soit $\theta : Gal(L.M/K) \to Gal(L/K) \times Gal(M/K)$ définie par $\theta(\sigma) = (\sigma_{|L}, \sigma_{|M})$.

Soit $(e_1, \cdots, e_n)$ une base de L sur K et $(f_1, \cdots, f_m)$ une base de M sur K. Alors la famille $(e_i f_j)_{i,j}$ est une base de $L.M$ sur K. Soient σ et $\sigma^{'}$ dans $Gal(L.M/K)$ tels que $\theta(\sigma) = \theta(\sigma^{'})$ alors pour tout

$$x = \sum_i \sum_j \lambda_{ij} e_i e_j \in L.M \quad (\lambda_{ij} \in K)$$

on a

$$\begin{aligned}
\sigma(x) &= \sigma\left(\sum_i \sum_j \lambda_{ij} e_i e_j\right) &&= \sum_i \sum_j \lambda_{ij} \sigma(e_i e_j) \\
&= \sum_i \sum_j \lambda_{ij} \sigma_{|L}(e_i)\sigma_{|M}(e_j) &&= \sum_i \sum_j \lambda_{ij} \sigma^{'}_{|L}(e_i)\sigma^{'}_{|M}(e_j) \\
&= \sigma^{'}\left(\sum_i \sum_j \lambda_{ij} e_i e_j\right) &&= \sigma^{'}(x)
\end{aligned}$$

Donc $\sigma = \sigma^{'}$ et par suite θ est injective. Comme $\sharp Gal(L.M/K) = [L.M:K] = [L:K].[M:K] = \sharp Gal(L/K).\sharp Gal(M/K)$, on en déduit que θ est bijective.

Revenons au cas général. Soit $(L_i)_i$ (resp. $(M_j)_j$) une famille d'extensions galoisiennes finies dont la réunion vaut L (resp. M). Les extensions $(L_i.M_j)_{ij}$ sont galoisiennes et $\bigcup_{ij} L_i.M_j = L.M$.

Remarquons que $L_{i_0}.M_{j_0} \subset L_{i_1}M_{j_1}$ si et seulement si $L_{i_0} \subset L_{i_1}$ et $M_{j_0} \subset M_{j_1}$. En effet, on a

$$L_{i_0}.M_{j_0} \subset L_{i_1}.M_{j_1} \Longleftrightarrow \left\{ \begin{array}{ccc} L_{i_0} & \subset & L_{i_1}.M_{j_1} \\ M_{j_0} & \subset & L_{i_1}.M_{j_1} \end{array} \right.$$

et par hypothèse, $L_{i_0}.L_{i_1} \subset L$ est linéairement de M_{j_1}. Si $L_{i_0}.L_{i_1} \neq L_{i_1}$, alors $[(L_{i_0}.L_{i_1}).M_{j_1} : K] > [L_{i_1}.M_{j_1} : K]$, ce qui est absurde car $L_{i_0}.L_{i_1}.M_{j_1} = L_{i_1}.M_{j_1}$. Donc $L_{i_0} \subset L_{i_1}$ et de la même manière, $M_{j_0} \subset M_{j_1}$.

Le groupe $Gal(L/K)$ est la limite projective du système

$$((Gal(L_i/K))_i, \pi_{i_1,i_0})_{i_1 i_0}$$

où

$$\pi_{i_1,i_0} : Gal(L_{i_1}/K) \longrightarrow Gal(L_{i_0}/K)$$

est l'application de restriction donnée pour $L_{i_0} \subset L_{i_1}$. Pour tout indice i, notons $\pi_i : Gal(L/K) \to Gal(L_i/K)$ la surjection canonique. De même, le groupe $Gal(M/K)$ est la limite projective du système

$$((Gal(M_j/K))_j, \varepsilon_{j_1,j_0})_{j_1 j_0}$$

où

$$\varepsilon_{j_1,j_0} : Gal(M_{j_1}/K) \longrightarrow Gal(M_{j_0}/K)$$

est l'application de restriction donnée pour $M_{i_0} \subset M_{j_1}$. Pour tout indice j, notons $\varepsilon_j : Gal(M/K) \to Gal(M_j/K)$ la surjection canonique. Notons

$$\pi_{i_1 i_0} \times \varepsilon_{j_1 j_0} : Gal(L_{i_1}/K) \times Gal(M_{j_1}/K) \longrightarrow Gal(L_{i_0}/K) \times Gal(M_{j_0}/K)$$

l'application coordonnée par coordonnée. Pour tout couple (i_0, j_0) notons

$$\theta_{i_0 j_0} : Gal(L_{i_0}.M_{j_0}/K) \longrightarrow Gal(L_{i_0}/K) \times Gal(M_{j_0}/K)$$

décrite précédemment. On déduit alors que $Gal(L.M/K)$ est la limite projective du sytème

$$((Gal(L_i.M_j/K))_{ij}, \varphi_{i_1 j_1, i_0 j_0})_{ij}$$

avec

$$\varphi_{i_1 j_1, i_0 j_0} : Gal(L_{i_1}.M_{j_1}/K) \longrightarrow Gal(L_{i_0}.M_{j_0}/K)$$

donné pour $L_{i_0} \subset L_{i_1}$ et $M_{j_0} \subset M_{j_1}$ par

$$\varphi_{i_1 j_1, i_0 j_0}(\sigma) = \theta^{-1}_{i_0 j_0} \circ \pi_{i_1 i_0} \times \varepsilon_{j_1 j_0} \circ \theta_{i_1 j_1}(\sigma)$$

En effet, le diagramme

$$\begin{array}{ccc} Gal(L_{i_1}.M_{j_1}/K) & \xrightarrow{\theta_{i_1 j_1}} & Gal(L_{i_1}/K) \times Gal(M_{j_1}/K) \\ \Big\downarrow{\scriptstyle \varphi_{i_1 j_1, i_0 j_0}} & & \Big\downarrow{\scriptstyle \pi_{i_1 i_0} \times \varepsilon_{j_1 j_0}} \\ Gal(L_{i_0}.M_{j_0}/K) & \xrightarrow{\theta_{i_0 j_0}} & Gal(L_{i_0}/K) \times Gal(M_{j_0}/K) \end{array}$$

est commutatif. Notons $\varphi_{ij} : Gal(L.M/K) \to Gal(L_iM_j/K)$ la surjection canonique.

Pour tout couple d'indice i, j posons $\psi_{ij} : Gal(L/K)\times Gal(M/K) \to Gal(L_iM_j/K)$ définie par:

$$\psi_{ij}(\sigma,\tau)\theta_{ij}^{-1}(\pi_i(\sigma),\varepsilon_j(\tau))$$

Les applications ψ_{ij} sont des homomorphismes continus. Il est clair que pour tout $(i_0, j_0) \leq (i_1, j_1)$, on a

$$\psi_{i_0,j_0}\varphi_{i_1j_1,i_0j_0} \circ \psi_{i_1,j_1}$$

Il existe donc une unique application $\omega : Gal(L/K) \times Gal(M/K) \to Gal(L.M/K)$ qui fait commuter les diagramme. Cette application est un homomorphisme continu.

Notons maintenant $\theta : Gal(L.M/K) \to Gal(L/K) \times Gal(M/K)$ l'application définie par:

$$\theta(\sigma) = (\sigma_{|L}, \sigma_{|M})$$

L'application $\omega \circ \theta$ est une application de $Gal(L.M/K)$ dans lui-même qui fait commuter les diagrammes, donc $\omega \circ \theta = Id$. On établit sans peine que $\theta \circ \omega = Id$. Ainsi, ω est un isomorphisme continu. Comme les groupes considérés sont compact, on en déduit que ω est un homéomorphisme.

Remarque 112.— Dans cette situation, on a $Gal(L.M/M) = Gal(L/K)$ et $Gal(L.M/L) = Gal(M/K)$ (exercice).

Corollaire 113.— *Soit L/K une extension galoisienne et L_n/K une famille d'extensions galoisiennes vérifiant :*

- *Pour tout $n \in \mathbb{N}$, $L_n \subset L$.*
- *Le compositum $\bullet_n L_n$ est égal à L.*
- *Pour tout $n_0 \in \mathbb{N}$, on a $L_{n_0} \cap \bullet_{n\neq n_0} L_n = K$.*

Il existe un isomorphisme de groupe topologique entre les groupes $Gal(L/K)$ et $\prod_n Gal(L_n/L)$.

Preuve: Considérons l'application

$$\theta : Gal(L/K) \longrightarrow \prod_n Gal(L_n/K)$$

qui à $\sigma \in Gal(L/K)$ associe $(\sigma_n)_n \in \prod_n Gal(L_n/K)$ où $\sigma_n = \sigma|_{L_n}$. L'application θ est visiblement un homomorphisme de groupe. Soit $(K_n)_n$ la suite de corps définie par $K_n = \bullet_{k\leq n} L_k$. Il est clair que $(K_n)_n$ est croissante et que $\bigcup_n K_n = L$.

Montrons que θ est injectif. Soit σ et σ' dans $Gal(L/K)$ tel que $\theta(\sigma) = \theta(\sigma')$. Si $x \in L$, il existe un entier n_0 tel que $x \in K_{n_0}$. Il existe donc des familles $(a_i^k)_{i\in I}$ (I fini, $k \leq n_0$) d'éléments de L_k tels que :

$$x = \sum_{i\in I} \prod_{k=1}^{n_0} a_i^k$$

On a alors :

$$\begin{aligned}\sigma(x) &= \sigma\left(\sum_{i\in I}\prod_{k=1}^{n_0} a_i^k\right) = \sum_{i\in I}\prod_{k=1}^{n_0}\sigma(a_i^k) = \sum_{i\in I}\prod_{k=1}^{n_0}\theta(\sigma)(a_i^k)\\ &= \sum_{i\in I}\prod_{k=1}^{n_0}\theta(\sigma')(a_i^k) = \sum_{i\in I}\prod_{k=1}^{n_0}\sigma'(a_i^k) = \sigma'\left(\sum_{i\in I}\prod_{k=1}^{n_0} a_i^k\right)\\ &= \sigma'(x)\end{aligned}$$

Donc $\sigma = \sigma'$.

Montrons que θ est surjective. Soit $(\sigma_n)_n \in \prod_n Gal(L_n/K)$. Le théorème précédent montre, par une récurrence immédiate, que le groupe $Gal(K_n/K) = \prod_{k=1}^n Gal(L_k/K)$. Ainsi pour tout entier n, il existe un K-automorphisme τ^n de L tel que $\tau^n_{|K_n} = (\sigma_1, \cdots, \sigma_n)$ c'est-à-dire, en particulier, que $\tau^n_{|L_k} = \sigma_k$. En posant pour $x \in K_n$,

$$\sigma(x) = \tau^n(x)$$

on définit bien un K-automorphisme de L tel que $\sigma_{|L_n} = \sigma_n$ pour tout n. Donc θ est surjective.

Montrons que θ est bicontinue. Comme $Gal(L/K)$ et $\prod_n Gal(L_n/L)$ sont des groupes profinis, il suffit de montrer que θ est continue en e ($e = Id$). Soit V un voisinage fondamentale de e dans $\prod_n Gal(L_n/K)$. On a alors

$$V = V_1 \times V_{n_0} \times \prod_{n\geq n_0} Gal(L_n/K)$$

avec V_i un voisinage fondamental de e dans $Gal(L_i/K)$. L'ouvert V_i correspond alors a $Gal(L_i/L^i)$ avec L^i/K galoisienne finie et $L^i \subset L_i$. Considérons alors le corps $F = L^1 \bullet \cdots \bullet L^{n_0}$. C'est une extension galoisienne finie de K. Ainsi $U = Gal(L/F)$ est un voisinage de e dans $Gal(L/K)$. Mais alors, $\theta(U) \subset V$ car si $\sigma \in U$ alors la restriction de σ à L^i est l'identité donc appartient à $Gal(L_i/L^i)$. Donc θ est continue en e.

En application de ce résultat, cherchons à calculer le groupe de Galois $Gal(L/K)$ où L désigne le compositum de toutes les extensions quadratiques de $\mathbb{Q}$. Il est clair que $L = \mathbb{Q}(i, \sqrt{2}, \cdots, \sqrt{p}, \cdots)$ où p parcourt l'ensemble des nombres premiers.

Etablissons pour commencer le résultat suivant :

Lemme 114.— *Soit $(p_n)_n$ une suite de nombres premiers distincts deux à deux. La suite de corps $K_n = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ est strictement croissante. Les extensions $K_n/\mathbb{Q}$ sont galoisiennes de groupes $(\mathbb{Z}/2\mathbb{Z})^n$.*

Preuve: La proposition est vraie au rang $n = 1$. Supposons qu'elle le soit à un rang $n \geq 1$, alors au rang $n+1$, comme $\mathbb{Q}(\sqrt{p_{n+1}})$ est de degré deux on a soit $K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$, soit $\mathbb{Q}(\sqrt{p_{n+1}}) \subset K_n$. Supposons que l'on soit dans la deuxième cituation. Comme $Gal(K_n/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^n$ est abélien, tout quotient de $Gal(K_n/\mathbb{Q})$ est un sous-groupe et réciproquement. Pour dénombrer les quotients d'ordre 2, il nous faut donc dénombrer les sous-groupes 2, c'est-à-dire les éléments d'ordre 2. Tous les éléments sont d'ordre 2 dans $(\mathbb{Z}/2\mathbb{Z})^n$ sauf 0. Il y a donc $2^n - 1$ quotients de $Gal(K_n/\mathbb{Q})$ isomorphes à $\mathbb{Z}/2\mathbb{Z}$ c'est-à-dire qu'il y a exactement $2^n - 1$ extensions quadratiques dans K_n. Maintenant, si a et b sont deux nombres rationnels tels que a/b ne soit pas un carré dans $\mathbb{Q}$, alors $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}(\sqrt{b})$. On en déduit donc qu'il existe une injection de $\mathcal{P}(p_1, \cdots, p_n) - \{\emptyset\}$ dans l'ensemble des

sous-extensions quadratiques de $K_n/\mathbb{Q}$ qui à un élément $P \in \mathcal{P}(p_1, \cdots, p_n)$ associe le corps $\mathbb{Q}(\sqrt{\prod_{p\in P} p})$. Or le cardinal de $\mathcal{P}(p_1, \cdots, p_n)/\emptyset$ vaut $2^n - 1$, donc cette injection est une bijection. Mais, par hypothèse, $p_{n+1} \in K_n$, donc $\mathbb{Q}(\sqrt{p_{n+1}})$ est une sous-extension quadratique de $K_n/\mathbb{Q}$ qui ne figure pas dans l'énumération faite précédemment de ces extensions, ce qui est absurde.

Donc $K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$ et comme $K_{n+1} = K_n \bullet \mathbb{Q}(\sqrt{p_{n+1}})$ on en déduit par la proposition précédente que $Gal(K_{n+1}/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^n \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^{n+1}$.

Une fois établi ce lemme, posons $M = \mathbb{Q}(\sqrt{2}, \cdots, \sqrt{p_n}, \cdots)$ où $(p_n)_n$ désigne la suite des nombres premiers. Il est clair que $M \bullet \mathbb{Q}(i) = L$ et que $M \cap \mathbb{Q}(i) = \mathbb{Q}$. Par application de la proposition, on a $Gal(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times Gal(M/\mathbb{Q})$. Reste à déterminer $Gal(M/\mathbb{Q})$. Pour tout $n \in \mathbb{N}^*$, posons $L_n = \mathbb{Q}(\sqrt{p_n})$. On a bien $L = \bullet_n L_n$. S'il existe un entier n_0 tel que $L_{n_0} \cap \bullet_{n\neq n_0} L_n \neq \mathbb{Q}$, alors $L_{n_0} \subset \mathbb{Q}(\sqrt{m_1}, \cdots, \sqrt{m_k}$ où $m_1, \cdots, m_k$ est une famille de nombres premiers distincts deux à deux et tous distincts de p_{n_0}, ce qu n'est pas possible d'après le lemme. On en déduit, par apllication de la proposition, que $Gal(M/\mathbb{Q}) = \prod_n \mathbb{Z}/2\mathbb{Z}$ et par suite que

$$Gal(L/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$$

Clôture abélienne

Définition 115.— *On dit qu'une extension galoisienne L/K est abélienne si les groupe $Gal(L/K)$ est abélien. Si l'on considère l'ensemble $(L_i)_i$ des extensions abéliennes finies de K, on appelle la réunion des $(N_i)_i$* clôture abélienne de K *et on la note K^{ab}.*

Proposition 116.— *L'ensemble K^{ab} est un corps. L'extension K^{ab}/K est une extension abélienne et si L/K désigne une extension abélienne, alors $L \subset K^{ab}$.*

Preuve: Si N_i et N_j sont deux extensions abéliennes finies de K, alors le compositum $N_i.N_j$ en est une aussi. En effet, si $z = \sum_{k=1}^n x_k^i y_k^j \in N_i.N_j$ et si $\sigma, \mu \in Gal(N_i.N_j/K)$, alors

$$\begin{aligned}
\sigma(\mu(z)) &= \sum_{k=1}^n \sigma(\mu(x_k^i))\sigma(\mu(y_k^j)) \\
&= \sum_{k=1}^n \sigma_{|N_i}(\mu_{|N_i}(x_k^i))\sigma_{|N_j}(\mu_{|N_j}(y_k^j)) \\
&= sum_{k=1}^n \mu_{|N_i}(\sigma_{|N_i}(x_k^i))\mu_{|N_j}(\sigma_{|N_j}((y_k^j)) \\
&= \sum_{k=1}^n \mu(\sigma(x_k^i))\mu(\sigma((y_k^j)) \\
&= \mu(\sigma(z))
\end{aligned}$$

L'extension K^{ab}/K est bien galoisienne puisque c'est la réunion d'extensions galoisiennes. Par définition $Gal(K^{ab}/K)$ est la limite projective de groupe abélien, donc est abélien. Si $Gal(L/K)$ est abélien, alors tout sous-groupe et tout quotient de $Gal(L/K)$ est abélien. Donc toute extension galoisienne finie de K incluse dans L est abélienne et comme L est la réunion de ces extensions, on a bien $L \subset K^{ab}$.

Théorème 117.— *Si G désigne le sous-groupe de $Gal(K^{sep}/K)$ engendré par les commutateurs $[\sigma,\tau]=\sigma\tau\sigma^{-1}\tau^{-1}$ pour $\sigma,\tau\in Gal(K^{sep}/K)$, alors $Gal(K^{sep}/K^{ab})=\overline{G}$.*

Preuve: On rappelle que G est un sous-groupe distingué de G_K, que G_K/G est abélien et que si H est un sous-groupe distingué de G_K tel que G_K/H soit abélien alors $G\subset H$ (propriétés générales au sous-groupe engendré par les commutateurs d'un groupe). Comme

$$Gal(K^{sep}/K)/Gal(K^{sep}/K^{ab})\simeq Gal(K^{ab}/K)$$

est abélien, on a $G\subset Gal(K^{sep}/K^{ab})$ et comme $Gal(K^{sep}/K^{ab})$ est fermé, on a $\overline{G}\subset Gal(K^{sep}/K^{ab})$.

Soit $L=inv(\overline{G})$. Comme G est distingué, $\overline{G}$ l'est aussi. Donc L/K est galoisienne et $Gal(L/K)=Gal(K^{sep}/K)/\overline{G}$ est abélien puisque $G\subset\overline{G}$. Donc L/K est une extension abélienne et par suite $L\subset K^{ab}$. Ainsi, $Gal(K^{sep}/K^{ab})\subset Gal(K^{sep}/L)=\overline{G}$.

5.3 Le théorème de Waterhouse

5.3.1 La méthode de Noether

Théorème.— (Noether) *Soit G un groupe fini. Il existe une extension galoisienne L/K telle que $Gal(L/K)=G$.*

Preuve: Soit $n=\sharp G$. On considère un plongement de G dans le groupe des permutations S_n. Le groupe S_n agit comme groupe de permutation sur $F(X_1,\cdots,X_n)$ (où F est un corps commutatif quelconque) par permutation des variables. Explicitement, si $R\in F(X_1,\cdots,X_n)$ et $\sigma\in S_n$ alors:

$$\sigma(R(X_1,\cdots,X_n))=R(X_{\sigma(1)},\cdots,X_{\sigma(n)})$$

Donc G agit comme groupe d'automorphisme de $F(X_1,\cdots,X_n)$. Le théorème d'Artin affirme alors que $F(X_1,\cdots,X_n)/F(X_1,\cdots,X_n)^G$ est une extension galoisienne de groupe G.

Remarque: La méthode de Noether permet d'arriver à un résultat plus précis : *pour tout groupe fini G, il existe une extension galoisienne de corps de nombre L/K tel que $Gal(L/K)$.* Cela utilise la propriété suivante (conséquence d'un théorème de Hilbert) : *si $L/\mathbb{Q}(X_1,\cdots,X_n)$ est une extension galoisienne de groupe G, alors il existe une extension galoisienne $\widetilde{L}/\mathbb{Q}$ de groupe de Galois G.*

Le méthode Noether appliquée au groupe $G=S_n$ montre que

$$F(X_1,\cdots,X_n)/F(X_1,\cdots,X_n)^{S_n}$$

est galoisienne de groupe S_n. Maintenant,

$$F(X_1,\cdots,X_n)^{S_n}=F(\sigma_1,\cdots,\sigma_n)$$

où les σ_i sont les fonctions symétriques élémentaires. Il est célèbres que ces dernière sont algébriquement indépendantes, donc $F(X_1,\cdots,X_n)\simeq F(\sigma_1,\cdots,\sigma_n)$ et par suite, il existe une extension $L/F(X_1,\cdots,X_n)$ de groupe de Galois S_n. En prenant $F=\mathbb{Q}$ et en appliquant Hilbert on en déduit que S_n est groupe de Galois d'une extension $M/\mathbb{Q}$. En plongeant maintenant un groupe G d'ordre n dans S_n et en prenant le corps des invariants de M par G, on en déduit ce que nous anoncions.

5.3.2 Les groupes profinis sont des groupes de Galois

Nous savons que les groupes de Galois d'extensions galoisiennes sont des groupes profinis. Réciproquement :

Théorème.— (Waterhouse, 1974) *Soit G un groupe profini. Il existe une extension galoisienne L/K telle que $Gal(L/K) = G$.*

La construction de L/K est une généralisation de la méthode de Noether au cas infini. Pour montrer ce théorème commençons par établir une généralisation du théorème d'Artin :

Proposition.— *Soit G un groupe profini d'automorphismes d'un corps F tel que pour tout $x \in L$,*

$$S(x) = \{\sigma \in G/\ \sigma(x) = x\}$$

soit un sous-groupe ouvert de G. Alors l'extension F/F^G est galoisienne et $Gal(F/F^G) = G$.

Preuve: Posons $K = F^G$ et considérons $x_1, \cdots, x_n \in L$. Le groupe

$$H = S(x_1) \cap \cdots \cap S(x_n)$$

est un sous-groupe ouvert de G. Soit N l'intersection des conjugués de H. C'est un sous-groupe fermé de G

Soit $n = [G : H]$, G agît sur G/H par multiplication et induit donc un homomorphisme de G sur S_n dont le noyau est N. Donc G/N est isomorphe à un sous-groupe de S_n, donc $[G : N] \leq n!$ et N est donc d'indice fini dans G et par suite N est un sous-groupe ouvert de G.

Le groupe G/N est fini et agit comme groupe d'automorphismes sur le corps $L = K(Gx_1, \cdots, Gx_n)$. Le corps des invariants est alors égal à K donc, d'après le théorème d'Artin, L/K est galoisienne finie de groupe G/N.

Le corps F est la réunion des extensions L/K, donc est galoisien. L'intersection des N vaut bien 1, donc

$$Gal(F/K) = \varprojlim Gal(L/K) = \varprojlim G/N = G$$

Considérons un groupe profini G et $\mathcal{N}$ l'ensemble des sous-groupes ouverts distingués de G. Soit $\Omega \bigsqcup_{N \in \mathcal{N}} G/N$ et $L = F(X_\omega)_{\omega \in \Omega}$ le corps des fractions rationnelles en les variables X_ω.

Soit $\omega \in \Omega$ et $\sigma \in G$. Il existe $N \in \mathcal{N}$ et $\tau \in G$ tel que ω soit la classe de τN dans G/N. Définissons alors

$$\sigma(X_\omega) = X_{\sigma(\omega)}$$

avec $\sigma(\omega)$ la classe de $\sigma\tau N$ dans G/N. On vérifie alors que G est un groupe d'automorphismes de L (exercice).

Le stabilisateur $S(X_\omega)$ de X_ω pour ω classe de τN est N donc est un sous-groupe ouvert de G. Si $R(X_{\omega_1}, \cdots, X_{\omega_n}) \in L$, alors $S(R)$ contient $S(X_{\omega_1}) \cap \cdots \cap S(X_{\omega_n})$ qui est ouvert, donc est ouvert. En appliquant alors la proposition précédente, on en déduit le théorème de Waterhouse.

Chapitre 6

Quelques exemples de groupes de Galois

6.1 Le groupe des Galois absolu d'un corps fini

On considère dans ce paragraphe un nombre premier l et q une puissance entière de l. On note $\mathbb{F}_q$ le corps à q élément. On étudie ici le groupe de Galois absolu de $\mathbb{F}_q$ (qui est égal, puisque $\mathbb{F}_q$ est un corps parfait, à $Gal(\overline{F}_q/\mathbb{F}_q)$) et aux correspondances galoisiennes découlant de cette étude.

Théorème 118.— *Le groupe de Galois absolu de $\mathbb{F}_q$ est isomorphe au groupe $\widehat{\mathbb{Z}}$.*

Preuve : Considérons sur $\mathbb{N}^*$ l'ordre $\leq$ défini par $n \leq m$ si et seulement si $n|m$. On sait que $G = Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ est isomorphe à la limite projective des $Gal(L/\mathbb{F}_q)$ où L est une extension galoisienne finie de $\mathbb{F}_q$. Par ailleurs, on a établi que toute extension finie de $\mathbb{F}_q$ est galoisienne et que ces extensions correspondent exactement aux corps $\mathbb{F}_{q^n}$ pour $n \in \mathbb{N}^*$. On sait aussi que l'on a l'extension $\mathbb{F}_{q^m}/\mathbb{F}_{q^n}$ si et seulement si $n|m$, on en déduit donc que le groupe G muni de la topologie de Krull est isomorphe à la limite projective du système

$$(Gal(\mathbb{F}_{q^n}/\mathbb{F}_q), res_{mn})_{n\in\mathbb{N}^*}$$

où $res_{mn} : Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) \longrightarrow Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$, qui désigne l'application de restriction, est définie pour $n|m$.

On considère maintenant l'élément $\sigma \in Gal(\overline{F}_q/\mathbb{F}_q$ défini, pour $x \in \overline{\mathbb{F}}_q$, par

$$\sigma(x) = x^q$$

On sait que la restriction de σ à $\mathbb{F}_{q^n}$ définit un générateur de $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ que nous noterons σ_n et donc, par conséquent, il existe un unique isomorphisme

$$\varepsilon_n : Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

vérifiant $\varepsilon_n(\sigma_n) = 1$. Soit maintenant n et m deux entiers tels que $n|m$. Il est clair

que l'on a $res_{mn}(\sigma_m) = \sigma_n$, il s'ensuit que le diagramme suivant

$$\begin{array}{ccc} Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) & \xrightarrow{\varepsilon_m} & \mathbb{Z}/m\mathbb{Z} \\ \Big\downarrow{\scriptstyle res_{mn}} & & \Big\downarrow{\scriptstyle \pi_{mn}} \\ Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) & \xrightarrow{\varepsilon_n} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

(où π_{mn} désigne le morphisme naturel) est commutatif. Ainsi la proposition ??? nous permet de déduire que les groupes $\varprojlim \mathbb{Z}/n\mathbb{Z}$ et $\varprojlim Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ sont isomorphes. Le premier n'est rien d'autre que $\widehat{\mathbb{Z}}$ et le deuxième, comme il a été rappelé, est isomorphe à $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. D'où le résultat.

L'isomorphisme que l'on vient d'introduire dans cette preuve montre que l'application σ est un générateur topologique du groupe $Gal(\overline{F}_q/\mathbb{F}_q)$. L'abélianité de $\widehat{\mathbb{Z}}$ assure que tout les sous-groupes (donc tous les sous-groupes fermés) de $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ sont distingués et par suite que toute extension algébrique de $\mathbb{F}_q$ est galoisienne. Ce fait pouvait être obtenu directement en remarquant que si $L/\mathbb{F}_q$ est une extension algébrique alors L est le compositum de toutes ses sous-extensions finies et comme une extension galoisienne finie de $\mathbb{F}_q$ est galoisienne et que le compitum d'extensions galoisiennes est galoisienne, on retrouve bien le fait que $L/\mathbb{F}_q$ est galoisienne.

On veut maintenant regarder à quoi correspond, en termes galoisiens dans cette situation, un isomorphisme entre $\widehat{\mathbb{Z}}$ et $\prod_p \mathbb{Z}_p$. Pour cela on introduit, pour un nombre premier p donné le corps

$$L_p = \bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{q^{p^n}}$$

Il s'agit bien d'une extension puisque la suite $\mathbb{F}_{q^{p^n}}$ est une suite de corps emboités. L'extension $L_p/\mathbb{F}_q$ est galoisienne et comme dans la preuve du théorème précédent, en regardant l'isomorphisme $\varepsilon_{p^n} : Gal(\mathbb{F}_{q^{p^n}}/\mathbb{F}_q) \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, on déduit que

$$Gal(L_p/\mathbb{F}_q) \simeq \mathbb{Z}_p$$

Maintenant, si a et b sont deux entiers premiers entres eux, on a $\mathbb{F}_{q^a} \cap \mathbb{F}_{q^b} = \mathbb{F}_q$ car si $K = \mathbb{F}_{q^a} \cap \mathbb{F}_{q^b}$ alors il existe c tel que $K = \mathbb{F}_{q^c}$ mais comme $\mathbb{F}_{q^a}/\mathbb{F}_{q^c}$ et $\mathbb{F}_{q^b}/\mathbb{F}_{q^c}$ sont des extensions, on doit avoir $c|a$ et $c|b$ ce qui montre bien que $c = 1$. Les extensions $\mathbb{F}_{q^a}$ et $\mathbb{F}_{q^b}$ étant galoisiennes, elles sont, par conséquent, linéairement disjointe. On en déduit donc que le compositun $\mathbb{F}_{q^a} \bullet \mathbb{F}_{q^b}$ est de degré ab sur $\mathbb{F}_q$, c'est-à-dire que

$$\mathbb{F}_{q^a} \bullet \mathbb{F}_{q^b} = \mathbb{F}_{q^{ab}}$$

On en déduit donc, par réccurence, que si m est un entier et si

$$m = p_1^{n_1} \cdots p_k^{n_k}$$

est sa décomposition en facteurs premiers, alors

$$\bullet_i \mathbb{F}_{q^{p_i^{n_i}}} = \mathbb{F}_{q^m}$$

ce qui permet alors d'affirmer que

$$\bullet_p L_p = \overline{\mathbb{F}}_q$$

Pour p premier, notons

$$\widetilde{L}_p = \bullet_{q \neq p} L_q$$

La remarque précédente montre que $F_{q^m} \subset \widetilde{L}_p$ si et seulement si $p \not| m$. Ainsi, on peut en déduire que

$$\widetilde{L}_p \cap L_p = \mathbb{F}_q$$

La proposition ??? permets alors d'affirmer qu'il y a un isomorphisme entre $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ et $\prod_p Gal(L_p/\mathbb{F}_q)$ ce qui donne un isomorphisme entre $\widehat{\mathbb{Z}}$ et $\prod_p \mathbb{Z}_p$. Si l'on veut détailler l'isomorphisme en terme de générateurs canonique, alors l'isomorphisme

$$\theta : Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow \prod_p Gal(L_p/\mathbb{F}_q)$$

est l'application topologiquement définie par l'envoie de σ au produit des restriction de σ aux L_p.

Venons en maintenant à la description des extensions intermédiaires de l'extension $\overline{\mathbb{F}}_q/\mathbb{F}_q$. Soit $L/\mathbb{F}_q$ une extension intermédiaire et pour tout premier p, notons

$$N_p(L) = \left\{ n \in \mathbb{N},\ \mathbb{F}_{q^{p^n}} \subset L \right\}$$

Pour des raisons évidentes, si $m \in N_p(L)$ alors pour tout $n \leq m$ on a $n \in N_p(L)$. On a alors

Corollaire 119.— *Soit G un sous-groupe fermé de $\prod_p \mathbb{Z}_p$. Il existe un ensemble P de nombres premiers et pour chaque p un entier n_p tels que*

$$G = \prod_{p \in P} p^{n_p} \mathbb{Z}_p$$

En d'autre termes, les sous-groupes fermés de $\prod_p \mathbb{Z}_p$ sont les produits des sous-groupes des $\mathbb{Z}_p$.

Preuve :

6.2 Le groupe de Galois de l'extension $\mathbb{Q}^{ab}/\mathbb{Q}$

Nous commencons ce paragraphe en énoncant un théorème fondamental pour l'étude de la clôture abélienne de $\mathbb{Q}$: le théorème de Kronecker-Weber. Nous n'en donnerons aucune preuve, car les preuves connues de ce théorème utilisent des notions que nous n'abordons pas dans ce livre. Pour une preuve nous renvoyons le lecteur à ???

Théorème 120.— (Kronecker-Weber) *Si L/Q désigne une extension abélienne, alors il existe un entier n tel que $L \subset \mathbb{Q}(\xi_n)$ (ξ_n désigne une racine primitive n-ième de l'unité.*

Puisque $\mathbb{Q}(\xi_n)\mathbb{Q}$ est abélienne, on en déduit immédiatement que $\mathbb{Q}^{ab} = \mathbb{Q}^{cycl}$ "la clôture cyclotomique" de $\mathbb{Q}$ (i.e. $\mathbb{Q}^{cycl} = \mathbb{Q}(\xi_n)_n$). Rappelons, sans démonstration, quelques propriétés des extensions cyclotomiques sur $\mathbb{Q}$:

• Pour tout $n \in \mathbb{N}^*$, l'extension $\mathbb{Q}(\xi_n)/\mathbb{Q}$ est galoisienne et

$$Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

Un ismorphisme entre ces deux groupes est donné par l'application ψ qui à $a \in (\mathbb{Z}/n\mathbb{Z})^*$ associe $\sigma_a \in Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ définit par $\sigma_a(\xi_n) = \xi_n^a$ (notons que cet isomorphisme dépend du choix de ξ_n).

• Si n et m sont deux entiers non nul, alors $\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_a)$ avec $a = p.g.c.d.(n,m)$ et $\mathbb{Q}(\xi_n, \xi_m) = \mathbb{Q}(\xi_b)$ avec $b = p.p.c.m.(n,m)$.

Considérons maintenant un système cohérent de racines primitives de l'unité $(\xi_n)_n$, c'est à dire pour tout n une racine primitive n-ième de l'unité telle que si $m = na$, alors $\xi_n = \xi_m^a$. Un tel système existe bien. En effet on peut considérer que la copie de $\overline{\mathbb{Q}}$ dans $\mathbb{C}$ est incluse dans K. On pose alors $\xi_n = exp(2i\pi/n)$.

Pour tout nombre premier p, posons $L_p = \mathbb{Q}(\xi_{p^n})_n$.

Lemme 121.— *L'extension $L_p/\mathbb{Q}$ est galoisienne. Pour tout nombre premier p, $L_p \cap \bullet_{p' \neq p} L_{p'} = \mathbb{Q}$ et $\bullet_p L_p = \mathbb{Q}^{cycl}$. En conséquence de quoi, $G_{\mathbb{Q}^{cycl}} = \prod_p Gal(L_p/\mathbb{Q})$.*

Preuve: Soit $x \in L_p \cap \bullet_{p' \neq p} L_{p'}$, il existe $n \in \mathbb{N}$ tel que $x \in \mathbb{Q}(\xi_{p^n})$ et il existe des nombre premiers $p_1, \cdots, p_k \neq p$ et des entiers $\alpha_1, \cdots, \alpha_k$ tels que $x \in \mathbb{Q}(\xi_{p_1^{\alpha_1}}, \cdots, \xi_{p_k^{\alpha_k}}) = \mathbb{Q}(\xi_{p_1^{\alpha_1} \cdots p_k^{\alpha_k}})$. Comme p^n et $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sont premier entre eux, on en déduit que $x \in \mathbb{Q}(\xi_{p^n}) \cap \mathbb{Q}(\xi_{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}) = \mathbb{Q}$.

Soit $n \in \mathbb{N}$ et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Le nombre complexe $\xi = \xi_{p_1^{\alpha_1}} \cdots \xi_{p_k^{\alpha_k}}$ est une racine primitive n-ième de l'unité (attention, ξ n'est pas forcément ξ_n!). Donc toutes les racines de l'unité sont dans $\bullet_p L_p$ et par suite $\bullet_p L_p = \mathbb{Q}^{cycl}$. L'isomorphisme annoncé découle immédiatement de ces deux propriétés.

Proposition 122.— *Pour tout p premier, $Gal(L_p/\mathbb{Q}) \simeq \mathbb{Z}_p^*$.*

Preuve: On a $\mathbb{Q} \subset \mathbb{Q}(\xi_p) \subset \mathbb{Q}(\xi_{p^2} \subset \cdots$ et $L_p = \bigcup_n \mathbb{Q}(\xi_{p^n})$. Maintenant, si $m \geq n$, alors l'homorphisme $Gal(\mathbb{Q}(\xi_{p^m}/\mathbb{Q}) \to Gal(\mathbb{Q}(\xi_{p^n}/\mathbb{Q})$ correspond (via l'isomorphisme décrit précédemment) à l'homomorphisme $(\mathbb{Z}/p^m\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$ restriction à $(\mathbb{Z}/p^m\mathbb{Z})^*$ de la surjection canonique $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Le groupe $Gal(L_p/\mathbb{Q})$ est donc isomorphe à la limite projective du système $((\mathbb{Z}/p^n\mathbb{Z})^*, \varphi_{mn})_n$, c'est-à-dire à $\mathbb{Z}_p^*$.

On en déduit donc la structure de $Gal(\mathbb{Q}^{ab}/\mathbb{Q})$:

Corollaire 123.— *On a les isomorphismes de groupes topologiques:*

$$\begin{aligned} Gal(\mathbb{Q}^{ab}/\mathbb{Q}) &\simeq \widehat{\mathbb{Z}}^* \simeq \prod_p \mathbb{Z}_p^* \\ &\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \times \prod_{p \geq 3} \mathbb{Z}/(p-1) \times \mathbb{Z}_p \\ &\simeq \mathbb{Z}/2\mathbb{Z} \times \left(\prod_{p \geq 3} \mathbb{Z}/(p-1)\mathbb{Z} \right) \times \widehat{\mathbb{Z}} \end{aligned}$$

Le groupe de Galois $Gal(\mathbb{Q}^{ab}/\mathbb{Q})$ est donc un produit cartésien $G \times \widehat{\mathbb{Z}}$ où G est un produit cartésien de groupe fini. Cette descirption permet de remarquer le fait suivant :

Proposition 124.— *Soit Γ un groupe profini abélien sans torsion de rang ≥ 2. Alors G n'est pas groupe de Galois sur $\mathbb{Q}$ (i.e. il n'existe pas d'extension galoisienne $L/\mathbb{Q}$ telle que $Gal(L/\mathbb{Q}) \simeq \Gamma$).*

Preuve : Si L existait, puisque $Gal(L/\mathbb{Q})$ serait abélien, on aurait $L \subset \mathbb{Q}^{ab}$ et, par suite, il existerait donc un morphisme surjectif continu de $Gal(\mathbb{Q}^{ab}/\mathbb{Q})$ sur $Gal(L/\mathbb{Q})$, donc un morphisme continu de $G \times \widehat{\mathbb{Z}}$ sur Γ que nous noterons φ.

Notons $\widetilde{G}$ la réunion disjointe des facteurs du produit cartésien qui définit G. Les éléments de $\widetilde{G}$ sont donc tous de torsion et il est clair que $\overline{\widetilde{G}} = G$. Comme Γ est sans torsion, il est clait que pour tout $x \in \widetilde{G}$, on a $\varphi(x) = 0$, mais comme $\widetilde{G}$ est dense dans G et que φ est continue, on en déduit que $\varphi(G) = 0$ et par suite que $\varphi(G \times \widehat{\mathbb{Z}}) = \varphi(\widehat{\mathbb{Z}})$. Maintenant, le groupe $\widehat{\mathbb{Z}}$ est de rang 1 alors que Γ ne l'est pas par hypothèse, donc φ ne peut pas être surjective.

Un cas simple d'application est par exemple le groupe $\Gamma = \mathbb{Z}_p \times \mathbb{Z}_p$. Cette proposition souligne la mystérieuse structure du groupe $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. En effet, une vieille conjecture très célébre en arithmétique affirme que tout les groupes finis sont groupes de Galois sur $\mathbb{Q}$ (on appelle cette conjecture le *problème de Galois inverse*). Bien que ce ne soit encore qu'un conjecture, une somme assez conséquente de travaux sur le sujet viennent ettayer l'idée qu'elle soit juste. Le problème de Galois inverse dit donc que le groupe $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ possède "beaucoup" de quotients continus finis, mais la proposition précédente dit au contraire que ce groupe possède très peu de quotients continus profinis...

6.3 Le groupe de Galois absolu de $K((X))$

6.3.1 Le corps des séries de Puiseux

On considère dans ce paragraphe un corps K et pour tout entier $n \geq 1$ le corps $K((X_n))$ des séries de Laurent à coefficients dans K en la "variable" X_n. Sur $\mathbb{N}^*$ on considère le pré-ordre filtrant à droite $n|m$ et si n et m sont ainsi (disons $m = an$ avec $a \in \mathbb{N}$), on définit l'application

$$\varphi_{nm} : K((X_n)) \longrightarrow K((X_m))$$

pour $S \in K((X_n))$, par

$$\varphi_{nm}(S(X_n)) = S(X_m^a)$$

Il est clair que l'application φ_{nm} est un morphisme de corps, ce qui définit donc pour tout $n|m$ une extension $K((X_m))/K((X_n))$.

Lemme 125.— *L'extension $K((X_m))/K((X_n))$ est un corps de rupture sur $K((X_n))$ du polynôme $P(T) = T^a - X_n$. En conséquence de quoi, l'extension $K((X_m))/K((X_n))$ est finie de degré a.*

Preuve :

On peut donc identifier le corps $K((X_m))$ au corps $K((X_n))(X_n^{1/a})$ où $X_n^{1/a}$ désigne une racine a-ième de X_n dans $K((X_m))$. Dans cette situation, on a $X_n^{1/a} = X_m$, ce qui justifie la notation $K((X_m)) = K((X_n^{1/a}))$. Le cas particulier $n = 1$, nous conduit alors à noter plus généralement $X_1 = X$ et $X_n = X^{1/n}$ pour tout entier $n \geq 2$. On remarque que le système $(K((X^{1/n})), \varphi_{nm})_n$ est un système inductif et que les morphismes φ_{nm} sont en fait des $K((X))$-isomorphismes. On

en déduit donc que le corps $\varinjlim K((X^{1/n}))$ est une extension algébrique du corps $K((X))$.

Définition 126.— *On appelle corps des séries de Puiseux à coefficients dans K, le corps $\varinjlim K((X^{1/n}))$ obtenu précédement et on le note $Puis(K)$.*

Si l'on veut confondre $Puis(K)$ à la réunion $\bigcup_n K((X^{1/n}))$, on peut donc représenter un élément $S \in Puis(K)$ sous la forme

$$S(X) = \sum_{k \geq k_0} a_k X^{k/n}$$

où n est un entier fixé. On fera alors attention au fait que, contrairement à la description du corps des séries de Laurent, une série de Puiseux peut s'écrire d'un infinité de facon sous la forme d'une série en la variable $X^{1/n}$.

Une des raisons pour lesquelles on s'intéresse à ce corps est que, dans le cas où K est un corps algébriquement clos de caractéristique 0 (e.g. $K = \mathbb{C}$), le corps $Puis(K)$ est algébriquement clos et constitue donc une clôture algébrique du corps $K((X))$. Nous démontrerons cette propriété dans la quatrième partie de ce livre (prop???).

Examinons maintenant la nature de l'extension algébrique $Puis(K)/K((X))$. Elle est visiblement infinie puisque pour tout entier n, il existe un élément de $Puis(K)$ (à savoir $X^{1/n}$) de degré n. Regardons maintenant l'aspect galoisien de cette extension.

• Supposons que K soit un corps de caractéristique p non nul. Le polynôme $T^p - X$ est donc irréductible sur $K((X))$ et inséparable (puisque de dérivé nulle). Ainsi l'extension $K((X^{1/p}))/K((X))$ et donc l'extension $Puis(K)/K((X))$ est inséparable.

Si maintenant le corps K est de caractéristique nulle, alors l'extension $Puis(K)/K((X))$ est bien sur séparable.

• Supposons maintenant que K contienne, pour tout entier $n \geq 1$, toute les racines n-ième de l'unité. L'extension $K((X^{1/n}))/K((X))$ est alors normale puisque $K((X^{1/n})) = K((X))(X^{1/n})$ et que les conjugués sur $K((X))$ de $X^{1/n}$ sont les $\xi_n X^{1/n}$ où ξ_n parcourt l'ensemble des racines n-ième de l'unité. Comme $Puis(K) = \bigcup_n K((X^{1/n}))$, on en déduit que $Puis(K)/K((X))$ est une extension normale. Réciproquement, supposons qu'il existe un entier $n_0 \geq 1$ tel que K ne contienne pas toutes les racines n_0-ième de l'unité, alors l'extension $Puis(K)/K((X))$ ne peut être normale, puisqu'alors pour toute racine n_0-ième de l'unité, ξ_{n_0}, on aurait $\xi_{n_0} X^{1/n_0} \in Puis(K)$ ce qui, en divisant par X^{1/n_0}, impliquerait que ξ_{n_0} serait dans K.

On a ainsi pour résumer

$$\begin{array}{lcl} Puis(K)/K((X)) \text{ est séparable} & \iff & car(K) = 0 \\ Puis(K)/K((X)) \text{ est normale} & \iff & K^{cycl} \subset K \end{array}$$

Le cas galoisiennement intéressant est donc le cas d'un corps K de caractéristique 0 contenant toute les racines de l'unité. Dans ce cas, on a alors :

Proposition 127.— *Soit K un corps de caractéristique 0 tel que $K^{cycl} \subset K$. L'extension $Puis(K)/K((X))$ est galoisienne et son groupe de Galois est isomorphe au groupe $\widehat{\mathbb{Z}}$.*

Preuve On vient de voir pourquoi l'extension $Puis(K)/K((X))$ est galoisienne.

Par ailleurs, on a

$$Puis(K) = \bigcup_n K((X^{1/n}))$$

L'extension $K((X^{1/n}))/K((X))$ est visiblement galoisienne sont groupe de Galois est alors isomorphe au groupe cyclique d'ordre n, $\mathbb{Z}/n\mathbb{Z}$. En effet, une fois choisie une racine primitive n-ième de l'unité, ξ_n l'application $\sigma_n : K((X^{1/n})) \to K((X^{1/n}))$ définie par :

$$\sigma_n(\sum_{k\geq k_0} a_k X^{k/n}) = \sum_{k\geq k_0} \xi_n^k a_k X^{k/n}$$

est visiblement un élément de $Gal(K((X^{1/n}))/K((X))$ d'ordre n, mais comme le dergé de cette extension est n, cela implique que σ_n est un générateur de ce groupe qui est donc cyclique de degré n. Notons alors (une fois fixée ξ_n)

$$\varepsilon_n : Gal(K((X^{1/n}))/K((X))) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

l'isomorphisme qui à σ_n associe $1 \in \mathbb{Z}/n\mathbb{Z}$.

Considérons maintenant un système cohérent de racines primitives de l'unité $(\xi_n)_n$ et les isomorphismes ε_n associés aux ξ_n. Alors pour $n|m$, le diagramme suivant

$$\begin{array}{ccc} Gal(K((X^{1/m}))/K((X))) & \xrightarrow{\varepsilon_m} & \mathbb{Z}/m\mathbb{Z} \\ \Big\downarrow res_{mn} & & \Big\downarrow \pi_{mn} \\ Gal(K((X^{1/n}))/K((X))) & \xrightarrow{\varepsilon_n} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

est commutatif (les morphismes π_{mn} étant les morphismes canoniques). On en déduit donc (prop???) que les sytèmes projectifs ont des limites projectives isomorphes, ce qui implique bien que $Gal(Puis(K)/K((X)))$ est isomorphe à $\widehat{\mathbb{Z}}$.

6.3.2 Le cas $K = \overline{K}$ de caractéristique 0

On prend un corps K algébriquement clos de caractéristique 0. Comme on l'a annoncé au paragraphe précédent, on a $\overline{K((X))} = Puis(K)$ et, en vertu de ce qui précède, on a

Proposition 128.— *Le groupe de Galois absolu de $K((X))$ est isomorphe à $\widehat{\mathbb{Z}}$.*

Ce résultat constitue une analogie arithmétique entre $\mathbb{F}_p$ et $K((X))$. L'analogue du Frobénius dans $K((X))$ est donc l'automorphisme σ qui à $\sum_{k\geq k_0} a_k X^{k/n})$ associe $\sum_{k\geq k_0} \xi_n^k a_k X^{k/n}$ (un système cohérent de racines $(\xi_n)_n$ étant fixé). De même, la partie $\mathbb{Z}_p$ de $\widehat{\mathbb{Z}}$ correspond alors au groupe de Galois de $\bigcup_n K((\sqrt[p^n]{X}))$.

6.3.3 Cas $\mathbb{Q}^{ab} \subset K$

Si K est un corps de caractéristique nulle non algébriquement clos, alors on a plus $\overline{K((X))} = Puis(K)$, pire, il se peut que $Puis(K)/K((X))$ ne soit plus galoisienne.

Néanmoins, le corps $Puis(\overline{K})$ étant algébriquement clos, on peut regarder la clôture algébrique de $K((X)$ dans $Puis(\overline{K})$. On a alors:

Proposition 129.— *La clôture algébrique, $\overline{K((X))}$, de $K((X))$ dans $Puis(\overline{K})$ est égale à* $\bigcup_{L/K\ finie} Puis(L)$.

Preuve: Si L/K est de degré d, alors $Puis(L)/Puis(K)$ est aussi de degré d, une base de L/K étant aussi une base de $Puis(L)/Puis(K)$. Comme $Puis(K)/K$ est une extension algébrique, on en déduit que $Puis(L)/K$ en est une aussi et par conséquent que $\bigcup_{L/K\ finie} Puis(L) \subset \overline{K((X))}$.

Réciproquement, soit $S = \sum_{k\geq k_0} a_k X^{k/n} \in Puis(\overline{K})$ une série de Puiseux algébrique sur $K((X))$. Considérons le corps $L = K(a_k)_k$ et un K-isomorphisme σ de L. On relève σ à $\overline{K}$ en un K-automorphisme $\widehat{\sigma}$. L'application $\widetilde{\sigma} : Puis(\overline{K}) \to Puis(\overline{K})$ définie par:

$$\widetilde{\sigma}(\sum_{p\geq p_0} \alpha_p X^{p/m}) = \sum_{p\geq p_0} \widehat{\sigma}(\alpha_p) X^{p/m}$$

est visiblement un $K((X))$-automorphisme de $Puis(\overline{K})$ qui relève σ. Soit σ et μ deux tels K-isomorphisme tel que $\widetilde{\sigma}(S) = \widetilde{\mu}(S)$. On a donc $\sigma(a_k) = \mu(a_k)$ pour tout k. Mais comme la famille $(a_k)_k$ engendre L, on en déduit que $\sigma = \mu$.

Supposons que L/K soit de degré infini. Il existe donc une infinité de K-isomorphisme de L et par suite, S admet une infinité de $K((X))$-conjugué ce qui est absurde. Donc L/K est finie et par suite $Puis(\overline{K}) \subset \bigcup_{L/K\ finie} Puis(L)$.

Corollaire 130.— *Si K contient les racines de l'unité (i.e. $\mathbb{Q}^{ab} \subset K$), alors le groupe de Galois absolu de $K((X))$ est isomorphe à $G_K \times \widehat{\mathbb{Z}}$.*

Preuve: Commençons par établir le lemme suivant:

Lemme 131.— *Si L/K est une extension galoisienne de groupe G alors l'extension $L((X))/K((X))$ est galoisienne de groupe $Gal(L/K)$. Ainsi, l'extension*

$$\left(\bigcup_{L/K\ finie} L((X))\right)/K((X))$$

est galoisienne de groupe G_K.

Preuve du lemme: On a $[L((X)) : K((X))] = [L : K]$. Définissons l'application

$$\psi : Gal(L/K) \to Aut_{K((X))}(L((X)))$$

par:

$$\psi(\tau)\left(\sum_{k\geq k_0} a_k X^k) = \sum_{k\geq k_0} \tau(a_k) X^k\right)$$

L'application $\psi(\tau)$ est bien un élément de $Aut_{K((X))}(L((X))$ et ψ est visiblement un homomorphisme de groupe. Soit $\tau, \mu \in Gal(L/K)$ tels que $\psi(\tau) = \psi(\mu)$. On a alors $\tau(x) = \mu(x)$ pour tout $x \in L$ donc $\mu = \tau$. Ainsi ψ est injectif et comme $[L((X)) : K((X))] = [L : K]$, on a finalement $\sharp Aut_{K((X))}(L((X))) = [L((X)) : K((X))]$ et donc $L((X))/K((X))$ est galoisienne, comme ψ est injectif, c'est un isomorphisme.

L'ensemble $\bigcup_{L/K\ finie} L((X))$ est bien un corps, car si L et L' sont de degré fini sur K alors $M = L.L'$ l'est aussi. Comme K est de caractéristique 0, on a

$$\bigcup_{L/K\ finie} L((X)) = \bigcup_{L/K\ galoisienne\ finie} L((X))$$

ce qui prouve bien que

$$\left(\bigcup_{L/K \ finie} L((X)) \right) / K((X))$$

est galoisienne. En vertu de ce qui précède, le système projectif associé à l'extension $\left(\bigcup_{L/K \ finie} L((X))\right) / K((X))$ est le même que celui de l'extension $\overline{K}/K$ (les détails techniques de cette affirmation sont laissé au lecteur). D'où l'isomorphisme entre G_K et $Gal\left(\left(\bigcup_{L/K \ finie} L((X))\right) / K((X))\right)$.

Preuve du corollaire: Considérons les corps $\Omega_1 = Puis(K)$ et $\Omega_2 = \bigcup_{L/K \ finie} L((X))$. Il est clair que $\Omega_1 \cap \Omega_2 = K((X))$ et que $\Omega_1.\Omega_2 = \bigcup_{L/K \ finie} Puis(L)$.

Maintenant, $\Omega_1/K((X))$ est galoisienne (puisque K contient les racines de l'unités) de groupe de Galois $\widehat{\mathbb{Z}}$. Par le lemme précédent, on sait que $\Omega_2/K((X))$ est galoisienne de groupe G_K. On en déduit donc l'isomorphisme indiqué dans le corollaire.

Par exemple, on en déduit l'isomorphisme

$$G_{\mathbb{C}((X_1))\cdots((X_n))} \simeq \widehat{\mathbb{Z}}^n$$

6.3.4 Le cas réel clos

Lorsque K est de caractéristique nulle, mais ne contient pas les racines de l'unité, le calcul de $G_{K((X))}$ est plus compliqué (par exemple quand $K = \mathbb{Q}$). Nous indiquons ici comment se débrouiller quand $K = \mathbb{R}$. Si le lecteur est un familier de la théorie d'Artin et Schreier des corps ordonnables, il verra que ce qui est écrit plus bas est valable pour n'importe quel corps K réel clos.

Proposition 132.— *Le groupe de Galois absolu de $\mathbb{R}((X))$ est isomorphe au produit semi-direct $\mathbb{Z}/2\mathbb{Z} \times_s \widehat{\mathbb{Z}}$ où l'action de $\mathbb{Z}/2\mathbb{Z}$ sur $\widehat{\mathbb{Z}}$ est le passage à l'inverse.*

Preuve: L'extension $\mathbb{C}((X))/\mathbb{R}((X))$ est galoisienne de groupe $\mathbb{Z}/2\mathbb{Z}$. Si c désigne la conjugaison complexe de $\mathbb{C}$, alors c se relève en le générateur de $Gal(\mathbb{C}((X))/\mathbb{R}((X))$ par action sur les coefficient des séries.

L'extension $Puis(\mathbb{C})/\mathbb{C}((X))$ est galoisienne de groupe $\widehat{\mathbb{Z}}$ dont nous avons décrit un générateur topologique σ (modulo le choix d'un système cohérent de racines de l'unité). L'élément c se relève en un $\mathbb{R}((X))$-automorphisme de $\mathbb{C}((X))$ par action sur les coefficients. Ce relevé est d'ordre 2. La suite exacte

$$1 \to G(Puis(\mathbb{C})) \to G(\mathbb{R}((X))) \to Gal(\mathbb{C}((X))/\mathbb{R}((X))) \to 1$$

est donc scindée. On en déduit que $G_{\mathbb{R}((X))}$ est bien le produit semi-direct de $\widehat{\mathbb{Z}}$ par $\mathbb{Z}/2\mathbb{Z}$. Reste à étudier l'action de $\mathbb{Z}/2\mathbb{Z}$ sur $\widehat{\mathbb{Z}}$. On a pour tout $S = \sum_{k \geq k_0} a_k X^{k/n} \in$

$Puis(\mathbb{C})$:

$$\begin{aligned} c\sigma c(S) &= c\sigma c\left(\sum_{k\geq k_0} a_k X^{k/n}\right) = c\sigma\left(\sum_{k\geq k_0} \overline{a_k} X^{k/n}\right) \\ &= c\left(\sum_{k\geq k_0} \overline{a_k}\xi_n^k X^{k/n}\right) = \sum_{k\geq k_0} a_k \overline{\xi_n^k} X^{k/n} \\ &= \sum_{k\geq k_0} a_k \xi_n^{k^{-1}} X^{k/n} = \sigma^{-1}(S) \end{aligned}$$

Le sous-groupe $< \sigma >$ (isomorphe à $\mathbb{Z}$) de $\widehat{\mathbb{Z}}$ est dense. L'action de c sur $< \sigma >$ est le passage à l'inverse. Comme l'application $\mu \mapsto c\mu c$ est continue, on en déduit bien que l'action de c sur $\widehat{\mathbb{Z}}$ est le passage à l'inverse.

On peut décrire assez précisément ce groupe profini au moyen des groupes dihédraux. Notons $D = \mathbb{Z}/2\mathbb{Z} \times_s \mathbb{Z}$ le groupe dihédrale infini et pour tout $n \in \mathbb{N}^*$, $D_n = \mathbb{Z}/2\mathbb{Z} \times_s \mathbb{Z}/n\mathbb{Z}$ le groupe dihédrale d'ordre $2n$. Si pour $m|n$, on définit le morphisme $\tau_{mn} : D_m \to n$, par

$$\tau_{mn}((a, x)) = (a, \varphi_{mn}(x))$$

où $\varphi_{mn} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ désigne la surjection canonique, on obtient un système projectif. On appelle alors groupe pro-dihédrale la limite projective de ce système. On a :

Proposition 133.— *La complétion profinie, $\widehat{D}$, de D est isomorphe au groupe pro-dihédrale* $\varprojlim D_n$.

Preuve: Déterminons les sous-groupe distingués et d'indice fini de D. Soit G un tel sous-groupe.

1er cas : $G \subset \mathbb{Z}$, alors il existe $n \in \mathbb{N}^*$ tel que $G = n\mathbb{Z}$. Il est clair que réciproquement, $n\mathbb{Z}$ est distingué d'indice fini dans D. Si $n = 1$, alors $D/G = \mathbb{Z}/2\mathbb{Z}$ et sinon, $D/G \simeq D_n$.

2ème cas : $G \not\subset \mathbb{Z}$. Il existe $q \in \mathbb{Z}$, tel que $(1, q) \in G$. Comme G est distingué, pour tout entier n, on a $(0, n)(1, q)(0, -n) = (1, q + 2n) \in G$ et par suite pour tout entier n et m, $(1, q + 2n)(1, q + 2m) = (0, 2n - 2m) \in G$, c'est-à-dire $2\mathbb{Z} \in G$. Distinguons trois sous-cas :

a) $(1, n) \in G \Rightarrow n \in 2\mathbb{Z}$, alors $(1, 2\mathbb{Z}) \subset G$, donc $G = \mathbb{Z}/2 \times_s 2\mathbb{Z}$.

b) $(1, n) \in G \Rightarrow n \notin 2\mathbb{Z}$, alors $G = 2\mathbb{Z} \cup (1, 2\mathbb{Z} + 1)$.

c) Il existe $n \in 2\mathbb{Z}$ tel que $(1, n) \in G$ et il existe $m \in \mathbb{Z} - 2\mathbb{Z}$ tel que $(1, m) \in G$. Alors $G = D$.

En résumé, les sous-groupes distingués d'indice fini sont, D, $D^n = (0, n\mathbb{Z})$, $A = \mathbb{Z}/2 \times_s 2\mathbb{Z}$, $B = 2\mathbb{Z} \cup (1, 2\mathbb{Z} + 1)$. Comme D^2 est un sous-groupe de A, de B et de D_1 et que ces trois sous-groupes sont incomparables au sens de l'inclusion, on en déduit que

$$\varprojlim D/G \simeq \varprojlim D/D^n$$

L'application $\pi_n : D \to D_n$ définie par $\pi_n((a, m)) = (a, \overline{m})$ a pour noyau D^n et défini donc un isomorphisme $\epsilon_n : D/D^n \to D_n$. On vérifie immédiatement que pour

$m|n$, le diagramme

$$\begin{array}{ccc} D/D^m & \longrightarrow & D/D^n \\ \downarrow{\scriptstyle \epsilon_m} & & \downarrow{\scriptstyle \epsilon_n} \\ D_m & \xrightarrow{\varphi_{mn}} & D_n \end{array}$$

est commutatif. D'où l'isomorphisme.

Proposition 134.— *Le groupe de Galois absolu de* $\mathbb{R}((X))$ *est isomorphe à* $\widehat{D}$.

Preuve: On a $Puis(\mathbb{C}) = \bigcup_{n\geq 2} \mathbb{C}((X^{1/n}))$ et $Gal(\mathbb{C}((X^{1/n}))/\mathbb{R}((X)))$ isomorphe à D_n. Décrivons une telle famille d'isomorphismes

$$\theta_n : D_n \to Gal(\mathbb{C}((X^{1/n}))/\mathbb{R}((X))$$

Soit $(\xi_n)_n$ un système cohérent de racines de l'unité. L'application

$$f : \mathbb{Z}/n\mathbb{Z} \to Gal(\mathbb{C}((X^{1/n}))/\mathbb{C}((X))$$

définie par la donné de $f(1) = \sigma$ et $\sigma(X^{1/n}) = \xi_n X^{1/n}$ est un isomorphisme. On pose alors $\theta_n((a,q)) = \sigma_{(a,q)}$, avec

$$\sigma_{(a,q)}\left(\sum_{k\geq k_0} \alpha_k X^{k/n}\right) = \sum_{k\geq k_0} \alpha_k^a \xi_n^k X^{k/n}$$

avec $\alpha_k^a = \alpha_k$ si $a = 0$ et $\alpha_k^a = \overline{\alpha_k}$ si $a = 1$. On vérifie facilement que pour $m|n$, le diagramme

$$\begin{array}{ccc} D_m & \xrightarrow{\varphi_{mn}} & D_n \\ \downarrow{\scriptstyle \theta_m} & & \downarrow{\scriptstyle \theta_n} \\ Gal(\mathbb{C}((X^{1/m}))/\mathbb{R}((X))) & \longrightarrow & Gal(\mathbb{C}((X^{1/n}))/\mathbb{R}((X))) \end{array}$$

est commutatif. D'où l'isomorphisme.

On peut en déduire que le groupe de Galois absolu de $\mathbb{R}((X))$ est librement engendré (topologiquement) par deux involutions. En effet, le groupe D est engendré par $(1,0)$ et $(1,1)$, comme $\bigcap D_n = 0$, D s'injecte dans $\widehat{D}$ et comme D est dense dans $\widehat{D}$, on en déduit bien que les deux involution incriminée engendre topologiquement $\widehat{D}$. Le fait qu'il n'y a pas de relation entre ces deux involution est laissé en exercice.